DRAFT

Electric Program Investment Charge (EPIC)

Project Final Report

CYBER-INTRUSION AUTO-RESPONSE AND POLICY MANAGEMENT SYSTEM (CAPMS)

Prepared for: California Public Utilities Commission

Prepared by: Southern California Edison

October 2015

EPIC-1 Program

DRAFT

Sponsoring Office:
California Public Utilities Commission
Los Angeles Office
320 West 4th Street, Ste. 500
Los Angeles, CA 90013

Participant:
Southern California Edison Company – Advanced Technology
2131 Walnut Grove Avenue
Rosemead, CA 91770

Prakash Suvarna – Manager
Tel.: 626-434-6292
e-mail: Prakash.Suvarna@sce.com

Jeff Gooding – Principal Investigator
Tel.: 626-543-6728
e-mail: Jeff.Gooding@sce.com

DRAFT

Acknowledgement

This material was produced with support from the California Public Utilities Commission under the Electric Program Investment Charge (EPIC) program.

Disclaimers

This report was prepared as an account of work sponsored by an agency of the State of California. Neither the State of California, nor any agency thereof, nor any of their employees, affiliates, contractors, or subcontractors, makes any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise does not necessarily constitute or imply its endorsement, recommendation, or favoring by the State of California or any agency thereof. The views and opinions of authors expressed herein do not necessarily state or reflect those of the State of California or any agency thereof.

This report was prepared by Southern California Edison Company (SCE) as an account of work sponsored by the California Public Utilities Commission, an agency of the State of California, under the EPIC program. Neither SCE, nor any employees, affiliates, contractors, and subcontractors, makes any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise does not necessarily constitute or imply its endorsement, recommendation, or favoring by SCE. The views and opinions of authors expressed herein do not necessarily state or reflect those of SCE.

DRAFT

Table of Contents

1 Executive Summary 6
2 Project Background 7
2.1 Threat Identification 7
2.2 Detection 8
2.3 Evaluation 11
2.4 Response 13
3 Project Tasks 14
3.1 Threat Analysis 14
3.2 Use Cases 19
3.3 Requirements 26
4 Project Results 29
4.1 Project Data Summary 29
4.2 Findings 32
4.3 Special Implementation Issues 33
4.4 Principles and Value Proposition 38
4.5 Technology Transfer Plans 38
4.6 EPIC Metrics 40
5 Appendices 43
A. WAMPAC Failure Modes Matrix 43
B. WAMPAC Attack Scenario Matrix 44
C. Test Plan 45

List of Figures

Figure 1: CAPMS Overview Diagram 9
Figure 2: Simple Correlation Logic Definition 12
Figure 3: Example WAMPAC System Architecture 16
Figure 4: CAPMS Threat Analysis Process 17
Figure 5: Threat Matrix Table 18
Figure 6: PMU Data Points 30
Figure 7: Simulated Power Flow during Configuration Attack 31
Figure 8: Demo Data Points Graph 31
Figure 9: Simulated Grid Operator View with CAPMS Indicators 32
Figure 10: Operator Response Approval Flow 33
Figure 11 Bayesian Network of Attack Tree 35
Figure 12 Two Options for Converting an AND Gate 37
Figure 13: CAPMS ATO Network 46

1 Executive Summary

The resiliency of the electric grid of the future will depend on improvements in monitoring, forecasting, coordination, and automation of existing and new equipment. Many of these additions require communications between devices within a geographic area, and to back-office control centers. The Cyber-intrusion Auto-response Policy Management System (CAPMS) project investigated the use of Bayesian decision tree logic to implement configurable security policies into an existing cybersecurity system. The project successfully built and demonstrated a system that can correlate events from secure sensor input points, determine the likelihood of various types of attacks, and respond accordingly.

A cyber-attack might target multiple devices simultaneously across various locations, so it is necessary to build a defense that allows for pre-programmed responses to such attacks. Attacks might come in the form of unauthorized access and changes to equipment, disruption of communications channels, changes to measurements, or even unauthorized control commands. Responses can be notifications to operators, quarantine of certain devices, changes to firewall rules to block traffic, or integrations that send information to existing or new systems and displays.

At the center of the new functionality is a Bayesian decision engine that is continually receiving information from infrastructure components, connected devices, and other systems. For example, given inputs from a physical security system, a work management system, and a network monitoring system, CAPMS can alert operators when there is unexpected access within a secure area such as a substation. This can increase the frequency of security checks and protective scanning functions, or even revoke credentials until operators can confirm the authorization of the access. Such checks could benefit normal operations as well, to ensure coordination and awareness of unplanned changes.

Our finding from this project is that such a system can be useful in providing cybersecurity-related information to operators so they can be aware of potential threats and attacks, as well as to invoke automatic or operator-confirmed responses such as blocking and isolating attacks. The system might also improve adherence to safety and other maintenance procedures by enforcing checks. Another important finding from the project is that for it to be most useful, the cybersecurity system has to be able to take action. In some cases, this will mean blocking communication to some devices. This doesn't mean that grid equipment can stop functioning safely and reliably, so communicating grid equipment vendors must include a non-communicating mode that requires only local measurements.

2 Project Background

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 SCE's successful Common Cybersecurity System (CCS), now being actively deployed and tested in substations. CAPMS uses the CCS product for its base functionality, and SCE worked with the CCS vendor ViaSat to develop and test new functional capabilities that SCE believes will be required to secure the future electric grid. As the vendor, ViaSat was responsible for the design and development of CAPMS. SCE provided practical utility experience to guide ViaSat's understanding of the system's desired functionality and provided the test environment.

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. This project limited the scope of CAPMS demonstration by focusing on the synchrophasor system and the development that had already occurred to support SCE's deployed CCS devices. SCE conducted the following activities in this project:

- A comprehensive analysis of the threats to a synchrophasor system
- Analysis of methods with which CAPMS could be used to detect and react to threats
- Development of attack use cases which could be tested in SCE's laboratory environment
- Development of high level requirements to communicate SCE's desired functionality to ViaSat
- Reviews with ViaSat to provide feedback on interim CAPMS functionality
- CAPMS system testing

2.1 Threat Identification

The three underlying properties of electronic communication that security measures attempt to guarantee are privacy, integrity, and availability. Physical security is required in all locations where attackers could get access to unencrypted data. Cybersecurity systems use cryptographic methods to hide protected information in encrypted communication tunnels, as well as to authenticate the identity of devices and users to prevent unauthorized access. They can also monitor processes, files, and communications to detect and prevent suspicious activity. Ensuring the availability of communications can be difficult, since redundant backup capability requires multiple physical communications paths in case one path is unavailable. Organizations must balance the cost of these protections with the risk of breaches and the damage that an attacker could cause. It can be very expensive to guarantee these properties to a high degree of probability. Utilities can also require that devices have built-in safeguards that protect equipment against unsafe operation, focus on early detection and response, isolation and containment, and ability to continue functioning safely while recovering from attacks, even when communications are not available.

2.1.1 Availability

Denial-of-service attacks can cause problems by flooding a network with disruptive traffic, but many other types of attacks can also block or prevent communications. As mentioned, redundancy is the only way to defend against these types of attacks, but it may be possible also to build tolerance into the system against this type of attack. Network outages occur frequently, and not always because of attacks. Applications and

automation functionality must be able to withstand extended periods of isolation if at all possible. They must be able to operate safely in an isolated state, using only local measurements to perform their function. They must be able to store critical information during outages, and send it later.

2.1.2 Privacy

Ensuring privacy prevents spying on private communications. Attackers can gain financially or strategically by using private information to their advantage. Customers rely on service providers to safeguard their information, including energy usage data, equipment, rate plans, and so on. If an attacker gains access to private communications, it may be necessary to prevent communications until someone removes the threat and the system regains security of the channel.

2.1.3 Integrity

Given access to a network, it can be possible for a device to trick other devices into trusting it, allowing for man-in-the-middle attacks, where a rogue agent could modify or initiate trusted communications. Integrity assurance measures must be able to verify the identity of devices, so that it is difficult for an attacker to gain trusted status. Security systems must also be able to prevent rogue devices or software agents from gaining access to trusted networks.

2.2 Detection

Access to a wide array of information sources is a key element in the CAPMS system's ability to detect anomalous activity (e.g. events) and correlate that activity to determine the appropriate response. In order to establish the required confidence level, implementations must augment existing cyber security monitoring information with numerous sources of data beyond that which is typically the focus of cyber security monitoring with the current philosophy employed by utilities. The complexity of system vulnerabilities and the evolving nature of threats require these additional sources of information, including the systems listed below.

- Operational Applications
- Physical Security Systems
- Workforce Management

Figure 1 provides an overview component diagram of CAPMS system. It includes the central security services provided by the Trusted Network Platform, or TNP, and adds the ability to manage policies that administrators can install on servers in the grid control center as well as on remote hosts. Additionally, adapters to 3rd party security systems and operational systems provide additional sensor inputs and actuator outputs.

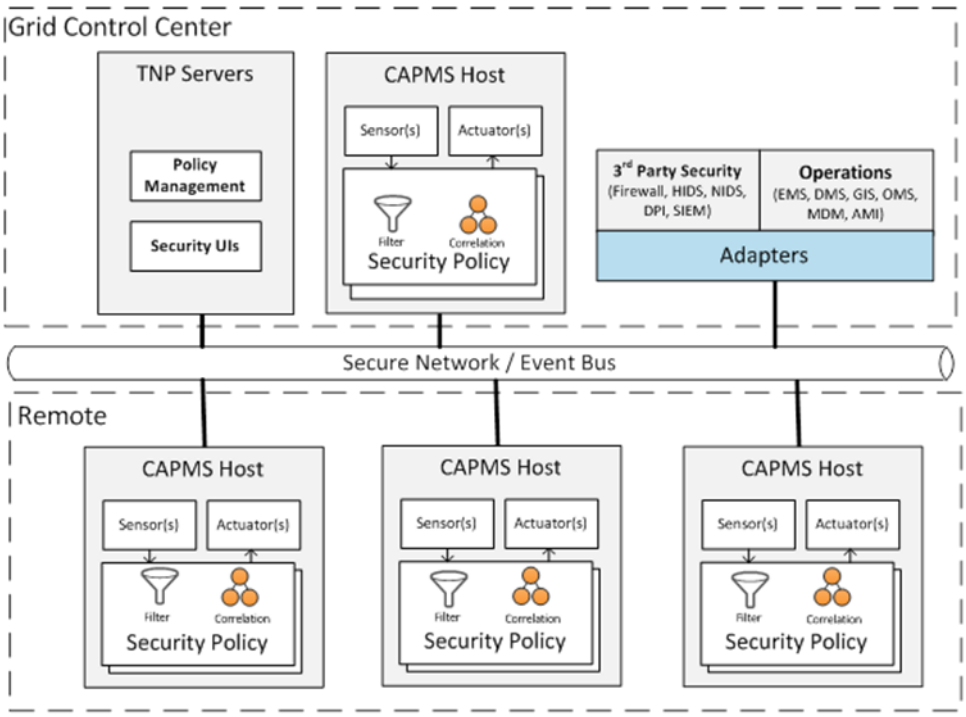

Figure 1: CAPMS Overview Diagram

This section describes several of the sensor input sources of information that may be required. However, the system is highly configurable, so these sources and policies can change at each installation site.

2.2.1 Cyber Security Event Information

Event information typically available within the cybersecurity system continues to play a key role in detecting anomalous system activities.

Monitoring

The cybersecurity system monitors devices using an agent installed on those it is protecting. It can monitor files, running processes, events, and network communications. It can take action locally, such as restarting a stopped process, or preventing unknown processes from starting.

Bill of Health

The system can centrally store a fingerprint (cryptographic signature) of monitored items to identify unauthorized changes. This is included in an overall "Bill of Health" measure of the expected configuration of each device. This adds some overhead in making approved changes, since the operator must compute and store the new approved signature. However, correlation of changed configuration without approval is a reasonable trigger to take action.

Network Alarms

The central security services can receive network alarms through SNMP or other means. The auto-response policies can use this information to correlate events and determine likelihood of attacks or suspicious activity.

Authentication Alarms

The system manages public key infrastructure for device certificates used in authentication and encryption. The system can revoke and manage these credentials through separately protected channels. It can also receive attempted logins, failed logins, and other events from active directory or other LDAP services for use in policies.

Firewall Activity

Firewalls often block everything except approved connections, possibly by address, port, and protocol. The system can log and collect attempts to initiate unapproved communications for use in correlating events to drive policies and responses. In addition, firewalls can provide the capability to create traffic baselines and then compare the real-time traffic patterns against these baselines. If the difference from a baseline exceeds an operator set threshold, a firewall can send an alert to the CAPMS detection process.

2.2.2 Operational Applications

Operational applications can provide a wealth of information, both at a grid level and an application level, that can be further utilized by the CAPMS system to determine that a cyber-attack is, or is not, occurring. There are numerous systems employed by utilities in this area providing functionality such as Supervisory Control and Data Acquisition (SCADA), State Estimation, Wide Area Monitoring Protection and Control (WAMPAC), Energy Management Systems (EMS), Distribution Management Systems (DMS), Outage Management Systems (OMS), and Advanced Metering Infrastructure (AMI).

Data Validity

Some attacks might attempt to change readings and measurements from grid components to make it look as if something is happening that really isn't, possibly prompting an operator to operate equipment when it isn't necessary. Existing systems may be able to validate readings and determine that someone has altered certain readings or that a device is malfunctioning in some way. Data validity involves assessing the current state or value of a directly observed data point (analog or digital) against the estimated/calculated/expected value. This is typically a dynamic determination driven by a State Estimator or other advanced application that utilizes a power system model to make the determination in the context of current grid conditions. Sending this information to the cybersecurity system can allow it to distinguish between actual grid events and cyber-attacks.

Alarm/Abnormal Condition

Alarm/Abnormal conditions occur when the current state or value of a directly observed data point (analog or digital) is not within a pre-determined range or state. These limits or normal state designations are typically static and done on a point-by-point basis within the operational application and don't vary based on the dynamics of the power grid.

Data Quality

Data quality is an indication to determine/detect if a data point (or points) is not updating or functioning as normal. While the state of the communicating device is the primary driver of data quality, there are some

cases where the device communications are normal but the data quality flags may indicate "bad" data. An example of this might be something such as an RTU reporting that a point is "locally forced" to a value.

Loss of Device Communications Events

Loss of communications events occur when a device that directly supplies data to the operational application (such as a Remote Terminal Unit (RTU) in the case of a SCADA system) loses communications connectivity with the operational application. The system may detect the failure because of failure to receive a reply to a poll (request) from a SCADA master from the device in simple serial system architectures or by a loss of a TCP connection in more advanced systems. This would probably be associated with loss of data but there may or may not be any correlation to the impacted data (if multiple devices are affected, it may be difficult to determine which device corresponds to what data).

Switching Orders/Tags

These include items such as "Hold Orders", "Caution Orders", or other tags, which may communicate ongoing and approved activities or operational constraints on power system devices. These have both operational and safety aspects.

2.2.3 Physical Security Systems

Physical Alarms

If an attacker has physical access to protected assets, those assets are in severe danger of compromise. There may be existing physical security systems in place, but coordinating those alarms with the cybersecurity system can increase the protection of those assets by locking them down against network or local access while investigating and clearing the physical alarm.

Tamper Alarms

Some devices have the ability to send an event when someone attempts to open a protective physical enclosure. The system can use these events in auto-response logic.

2.2.4 Workforce Management

Work Plan / Approvals

One possible strategy for the cybersecurity system is to prevent access and changes to physical or cyber assets unless a scheduled, approved work plan exists. The combination of activity when nothing was scheduled will trigger an alert state, in which the system adopts a heightened security posture, while determining whether or not the activity is an attack.

2.3 Evaluation

Given the ability to detect and collect the required events and conditions, the policy engine provides the ability to correlate information and trigger alarms or to take action. For example, one policy created within the SCE CAPMS system demonstration establishes that when the system detects access to a substation, but no work is scheduled, the system notifies the operator and elevates the alert state, potentially blocking some changes or scanning for changes more often. Eventually, as the system gathers more information about other

related activities, it identifies the most likely targets and can take proactive action if desired. Proactive actions can include investigative actions and other types of responses described in Section 2.4.

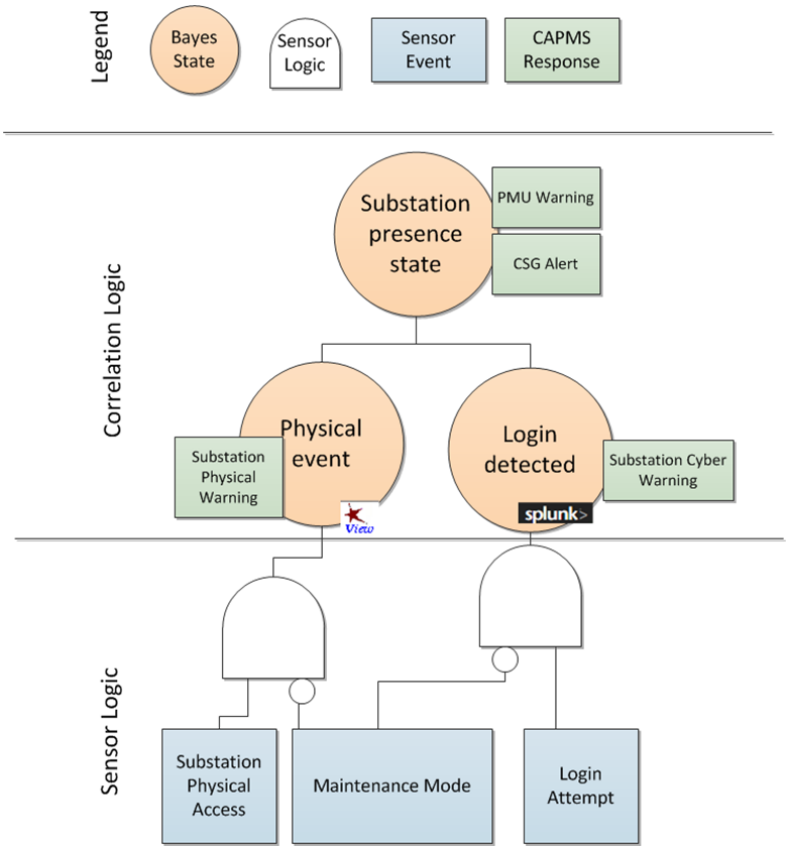

Figure 2: Simple Correlation Logic Definition

2.3.1 Root Cause Analysis

Sometimes it may be difficult to determine the source of an attack. One goal of the system is to gather enough information to identify the cause of alerts and events. With an accurate identified cause, it might be possible to isolate the problem and contain it.

Confidence

The system uses a Bayesian network to model the different attacks and the conditions under which they can be determined. The model can use Boolean logic, with states being either “true” or “false”. It can also compute the probability or confidence of each determination, which allows for tuning of the determinations, filtering alerts by criticality, and other sorts of fine-grained output. The model may limit responses to thresholds in confidence, enabling a tailored response based on how confident the model is that an attacker has achieved their goal.

Extent

One goal of the CAPMS project was to implement the grouping of cybersecurity alert states by location and device. Given this feature, an operator can quickly see the extent of an attack by how many devices and locations are reporting certain conditions.

Consequence

Additionally, operators would like to know what might happen as a result of an attack. System designers could pre-program certain policy result states with this type of information, to alert and notify the operator that a certain condition has been met that will lead to a known consequence.

2.4 Response

The purpose of the CAPMS project is to add functionality to not only gather information and compute the likelihood that observed system activity is the result of a cyber-attack, but also to respond when it has been determined that a cyber-attack has, or is occurring. Responses can take many forms, including simple logged alert events, notifications, or even wipe or quarantine. Obviously, most operators will want the ability to review and confirm automated actions until they feel comfortable with the logic and determinations.

2.4.1 Notification

Logs

Writing a cyber-alert state to a log file is probably the simplest, most basic action. Another system could collect and combine these events with other information in a management console or as input into other processes.

Alerts

The next level of notification is to show the alert state on some sort of display, which could be the security system application.

Programmatic

If desired, the policy engine can send alert state determinations, and potentially the underlying contributing information, to external applications.

2.4.2 Forensic

The system can initiate a forensic response in cases where it suspects an attack but has not identified the specific target. For example, the system could increase the frequency or amount of monitoring and scanning in a suspected attack area to find affected components more quickly.

2.4.3 Isolation / Containment

Once the system gathers enough information to identify the affected components, it is possible to block them from communicating or otherwise contain them to prevent further damage. Or, in cases where someone is using a certain credential inappropriately, the system can revoke it.

Security Association Management

Once the policy engine determines that an attacker has control of a device, it may be desirable to block it from communicating. If the cybersecurity system is managing the security associations used for secure communications, breaking them is very easy. If a different system were managing the security associations, a secure programmatic method of transferring the control message would be required.

Credential Revocation

In the scenario where an attacker is using a valid (but probably compromised) account to make unauthorized changes, the system could revoke the credentials for that account to prevent further changes.

Graceful Degradation

Reliability and safety are very important to energy utilities. If the security system initiates any automatic responses, operators want to ensure that it will not affect the safe, reliable delivery of power. On the other hand, if an attacker gains control of a device, it may be possible to affect the delivery of power and the safe operation of the system. Devices responsible for the operation of the grid must be able to operate safely and effectively with or without communications. Without communications, a device can rely only on local measurements.

Security-Related Operational Modes

Critical components could have redundancies or multiple levels of degradation based on input from CAPMS and other sources to keep them operating safely. Equipment could implement various modes of operation (heightened security states) with local policies as needed.

2.4.4 Contingency Planning

Utilities always strive to be able to handle events where a single piece of equipment fails, so called “N-1” contingencies. It could be possible for CAPMS to predict failures larger than “N-1” and to send those scenarios to a contingency planning system in order to determine the best course of action. For example, if a certain type of equipment has been compromised in a certain area, that list of equipment could be sent to a grid management system for planning, potentially before it is actually taken out of service. The utility could then potentially avoid cascading outages by balancing resources prior to equipment operation.

2.4.5 Cyber-Threat Information Sharing

Another possible response is to notify interested parties about detected cyber-threats and provide them enough information to detect or prevent further attacks.

3 Project Tasks

3.1 Threat Analysis

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 increased connectivity, within the system and external to the system, to adapt to changing business and operational environments. Advances in connectivity, 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 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 technology. To accomplish this, SCE analyzed threats to these systems with a focus on how they could potentially influence a utility’s operational decision-making. The

main components of this approach were examining system characteristics that an attacker could be exploit and the informational impacts from the identified attacks.

3.1.1 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.

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

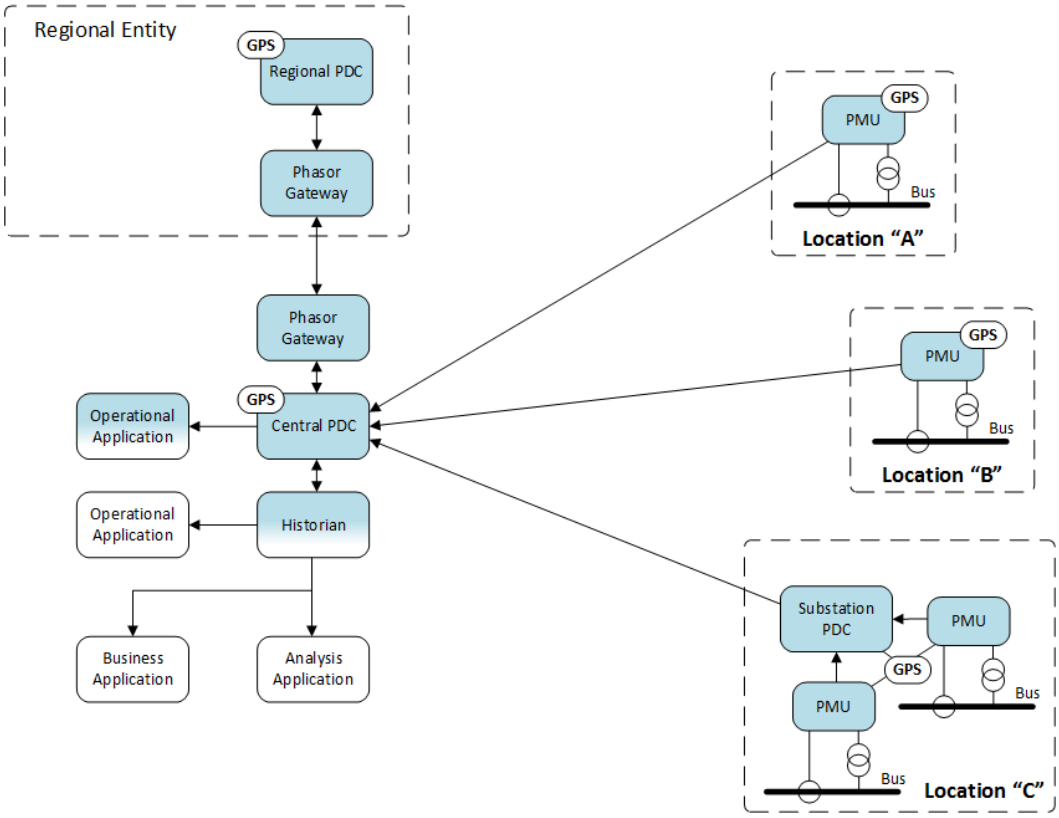

Figure 3: Example WAMPAC System Architecture

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

3.1.2 Process

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

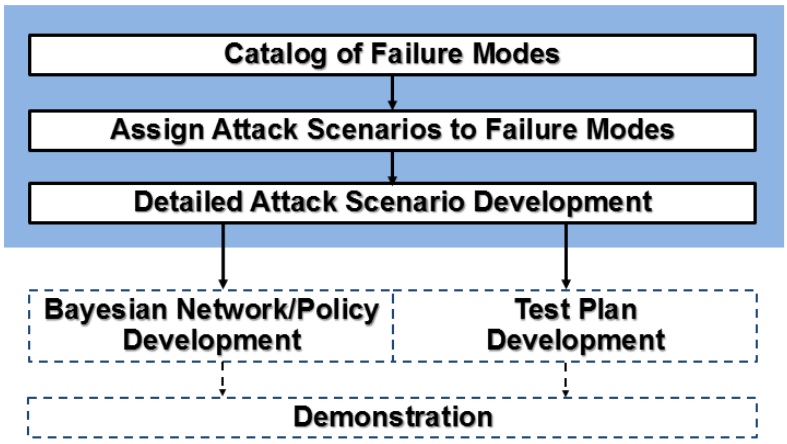

Figure 4: CAPMS Threat Analysis Process

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 as shown in Appendix A. The goal of this step was to identify a good 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 as shown in Appendix B and represented in Figure 5. 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

3.1.3 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 and fall into two primary areas:

- 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.

3.2 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.

3.2.1 Attack Scenario 47: Unauthorized party/system changes DFR/PMU configuration

Narrative

A Threat Agent gains physical access to a remote substation that includes one or more DFR/PMU units. While physically present, the Threat Agent gains logical access to a DFR/PMU unit and modifies the configuration of the unit with the intent of impacting the utility's operational decision making capabilities. Once the Threat Agent has made the intended configuration changes, they reboot the DFR/PMU unit (to ensure configuration changes take effect). The Threat Agent then physically exits the facility.

Assumptions

- Configuration changes to the DFR/PMU unit will take effect immediately (or shortly thereafter the changes are made via reboot of the unit)
- The Threat Agent is knowledgeable of the system, corresponding technology, and has a basic understanding of the operation of the power gird
- Command Frames and Config Frames are exchanged between the PDC and DFR/PMU over TCP
- The DFR/PMU employs the spontaneous data transmission method as described in Annex F of IEEE Std C37.118.2

Pre-conditions

- All communications to the remote substation are functioning normally
- The DFR/PMU has been fully commissioned including functional testing to validate the configuration and communications connectivity
- The PDC at the control center has been configured, functionally tested, and is receiving data (via C37.118 format) from the DFR/PMU

- The CCS client of DFR/PMU has been configured and is monitoring the file associated with the DFR/PMU configuration for changes

Scenario Steps

Step	Description	Possible Sensors
1	The DFR/PMU unit is commissioned	N/A
2	The CCS Client on the DFR/PMU unit begins monitoring target files	N/A
3	A Threat Agent gains physical access to the remote substation where the target DFR/PMU has been installed	Physical security system
4	The Threat Agent gains logical access to DFR/PMU	
	a) Via local console interface of the DFR/PMU interface using compromised credentials or default account	DFR/PMU-Windows log
	b) Via network using RDP and compromised credentials or back door, etc.	DFR/PMU-Windows log
	c) Via network using spoofed USI master software running locally	
5	The Threat Agent modifies the configuration of the target DFR/PMU	1) DFR/PMU-Application log 2) CCS Client (BoH or QoT)
6	The Threat Agent applies the change so that the modified configuration takes effect	DFR/PMU-Application log
7	The Threat Agent terminates logical access	
	a) logs out of DFR/PMU	DFR/PMU-Windows log
	b) Leaves DFR/PMU console open (if that's how he gained access)	
	c) Drops RDP connection	DFR/PMU-Windows log
8	Communications (streaming of the Data Frames) between the affected DFR/PMU unit and PDC are interrupted	PDC-Application log
9	The Threat Agent exits the remote substation	
10	The PDC listens on UDP Port 4713 (default port per IEEE C37.118.2 standard) for Data Frames from the DFR/PMU	
11	The DFR/PMU resumes sending Data Frames to the PDC (via UDP). The DFR/PMU will indicate that a configuration change has been made by asserting Bit 10 of the STAT field within the Data Frame.	C37.118 deep packet inspection (detection of assertion of Bit 10 of the STAT field within the Data Frame)
12	Upon receipt of the Data Frame noting the configuration change (Bit 10 of the STAT field asserted), the PDC sends the Command Frame (Send CFG-1,2, or 3) to the DFR/PMU.	1) PDC-Application log 2) C37.118 deep packet inspection (detection of commands sent from PDC to DFR/PMU)

Step	Description	Possible Sensors
13	The DFR/PMU processes the Command Frame (Send CFG-1,2, or 3) and sends the response (Configuration Frame) to the Threat Agent	1) PDC-Application log 2) C37.118 deep packet inspection (detection of Configuration Frame)
14	Synchrophasor data being received by the PDC is not accurate of current grid conditions	Upstream operational application or system operator
15	The PDC time correlates the incorrect data from the affected DFR/PMU unit along with data from other (normal) DFR/PMU units and forwards the aggregated data to upstream operational application (such as EMS), Phasor Gateway and/or Historian	
16	The operational application detect data anomaly	Upstream operational application log or system operator
17	The Historian stores the received (incorrect) data	
18	The Phasor Gateway forwards the aggregated data to and external entity and/or the Historian forwards the aggregated data to other internal (non-operational) application	1) External Entity (None) 2) Non-operational application log or application owner

3.2.2 Attack Scenario 13: Erroneous IRIG-B output of GPS receiver creates clock error in DFR/PMU

Narrative

A Threat Agent gains physical access to a remote substation that includes one or more DFR/PMU units. While physically present, the Threat Agent gains logical access to the GPS receiver that provides time synchronization to the DFR/PMU via an IRIG-B interface. The Threat Agent modifies the configuration of the GPS receiver with the intent of causing the DFR/PMU to affix incorrect time stamps to the C37.118 data frames and affect the utility's operational decision making capabilities. Once the Threat Agent has made the intended configuration changes, they reboot the GPS receiver unit (to ensure configuration changes take effect). The Threat Agent then physically exits the facility. The incorrect time stamps affixed to the C37.118 Data Frames from the target DFR/PMU to the PDC are perceived as late data by the PDC, and they are flagged as a waiting period violation.

Assumptions

- Configuration changes to the GPS receiver unit will take effect immediately (or shortly thereafter the changes are made via reboot of the unit)
- Communications networks between the remote substation and the utility backbone/core are not interrupted during this scenario
- The Threat Agent is knowledgeable of the system, corresponding technology, and has a basic understanding of the operation of the power gird
- Data Frames from the DFR/PMU are sent to the PDC over UDP
- Command Frames and Config Frames are exchanged between the PDC and DFR/PMU over TCP
- The DFR/PMU employs the spontaneous data transmission method as described in Annex F of IEEE Std C37.118.2

Pre-conditions

- All communications to the remote substation are functioning normally
- The DFR/PMU has been fully commissioned including functional testing to validate the configuration and communications connectivity
- The PDC at the control center has been configured, functionally tested, and is receiving data (via C37.118 format) from the DFR/PMU

Scenario Steps

Step	Description	Possible Sensors
1	The DFR/PMU unit is commissioned	N/A
2	A Threat Agent gains physical access to the remote substation where the target DFR/PMU and GPS receiver has been installed	Physical security system
3	The Threat Agent gains logical access to GPS receiver	Device log
	a) Via web console	
	b) Via serial console port	
4	The Threat Agent modifies the configuration of the target GPS receiver	Device log
5	The Threat Agent restarts the affected GPS receiver unit so that the modified configuration takes effect	
6	The Threat Agent terminates logical access	
7	The IRIG-B output of the GPS receiver is altered as a result of the configuration change and not accurate	
8	The Threat Agent exits the remote substation	Physical security system
9	The DFR/PMU updates its internal clock based on the IRIG-B input from the GPS receiver	Device application log
10	The DFR/PMU utilizes the misaligned internal clock to affix time stamps on C37.118 Data Frames sent to the PDC (via UDP).	
11	The PDC reaches its maximum wait time for collecting data from downstream PMU devices. The PDC aggregates the data from other PMUs, inserts filler values for the missing PMU data, and transmits the aggregated data within the Data Frames being sent to upstream C37.118 clients (phasor gateway, operational applications, historian, etc.). Within the aggregated Data Frame, bits 15 & 14 of the STAT field corresponding to the data block containing the missing PMU data are set to “10” to note that this data is invalid.	1) PDC application log 2) C37.118 Deep Packet Inspection (detection of Bits 15 & 14 in STAT field for corresponding PMU data block of Data Frame set to “10”)
12	C37.118 clients upstream from the PDC receive data frames that contain no data from the target DFR/PMU.	Application log
13	The operational application detect data anomaly	Application logs/alarms
14	The Historian stores the received data	

Step	Description	Possible Sensors
15	The Phasor Gateway forwards the aggregated data to and external entity and/or Historian forwards the aggregated data to other internal (non-operational) application	
16	Non-operational/analysis application detects data anomaly	Application logs/alarms

3.2.3 Attack Scenario 32: Unauthorized device degrades network performance by flooding the network with excessive traffic

Narrative

A Threat Agent gains logical access to a host on the utility substation network infrastructure where the target DFR/PMU is connected. The Threat Agent then utilizes the compromised host to execute a flooding type Denial-of-Service (DoS) attack. The attack results in the available network bandwidth being inadequate for the DFR/PMU to meet the performance requirements for the data frames between the DFR/PMU and PDC. This in turn results in a waiting period violation within the PDC for the specific DFR/PMU.

Assumptions

- The DFR/PMU is currently sending data frames to the PDC.
- The Threat Agent is knowledgeable of the system, corresponding technology, and has a basic understanding of the operation of the power grid.

Pre-conditions

- All communications to the remote substation are functioning normally
- The DFR/PMU has been fully commissioned including functional testing to validate the configuration and communications connectivity
- The PDC at the control center has been configured, functionally tested, and is receiving data (via C37.118 format) from the DFR/PMU

Scenario Steps

Step	Description	Possible Sensors
1	A Threat Agent gains logical access to the substation network where the target DFR/PMU has been installed	Network infrastructure
2	The Threat Agent gains logical access to a host device within the substation network where the target DFR/PMU has been installed	Host logs
	a) Via console interface using compromised credentials or default account	

Step	Description	Possible Sensors
	b) Via network using RDP and compromised credentials, back door, or by brute force	
	The Threat Agent begins a flooding DoS attack from the compromised host	
	a) PING flood attack against the router's local LAN interface	Router log
	b) Smurf attack sent to LAN broadcast address with router's local LAN interface as source address	Router log
3	c) UDP flooding attack against the router's local LAN interface	Router log
4	The available network bandwidth decreases to the point that the DFR/PMU cannot meet its minimum performance requirements for transmitting data frames to the PDC.	1. Network infrastructure 2. Deep Packet Inspection
5	The PDC reaches its maximum wait time for collecting data from downstream PMU devices. The PDC aggregates the data from other PMUs, inserts filler values for the missing PMU data, and transmits the aggregated data within the Data Frames being sent to upstream C37.118 clients (phasor gateway, operational applications, historian, etc.). Within the aggregated Data Frame, bits 15 & 14 of the STAT field corresponding to the data block containing the missing PMU data are set to "10" to note that this data is invalid.	1. PDC application log 2. C37.118 Deep Packet Inspection (detection of Bits 15 & 14 in STAT field for corresponding PMU data block of Data Frame set to "10")
6	The Threat Agent exits/terminates logical access to the compromised host. The DoS attack remains active	Network infrastructure
7	C37.118 clients upstream from the PDC receive data frames that contain no data from the target DFR/PMU.	Application log
8	The operational application detect data anomaly	Application logs/alarms
9	The Historian stores the received data	
10	The Phasor Gateway forwards the aggregated data to and external entity and/or Historian forwards the aggregated data to other internal (non-operational) application	
11	Non-operational/analysis application detects data anomaly	Application logs/alarms

3.2.4 Attack Scenario 26: Unauthorized device intercepts and alters the configuration frame from PMU to PDC

Narrative

A Threat Agent executes a man-in-the-middle (MITM) attack on the data exchange between a DFR/PMU and the PDC located at the utility's control center. After monitoring this data exchange, the Threat Agent then intercepts a Configuration Frame sent from the DFR/PMU to the PDC and alters the time base (TIME_BASE) field within the Configuration Frame. The time base is utilized by a C37.118 client to determine the actual fractional second of the time stamp of the phasor data within the Data Frame. This altered Configuration Frame is then processed by the PDC and used to parse subsequent Data Frames from the DFR/PMU.

Assumptions

- Communications networks between the remote substation and the utility backbone/core are not interrupted during this scenario. The Threat Agent is knowledgeable of the system, corresponding technology, and has a basic understanding of the operation of the power grid.
- Data Frames from the DFR/PMU are sent to the PDC over UDP
- Command Frames and Config Frames are exchanged between the PDC and DFR/PMU over TCP
- The DFR/PMU employs the spontaneous data transmission method as described in Annex F of IEEE Std C37.118.2

Pre-conditions

- All communications to the remote substation are functioning normally
- The DFR/PMU is streaming Data Frames to the PDC.
- The DFR/PMU has been fully commissioned including functional testing to validate the configuration and communications connectivity
- The PDC at the control center has been configured, functionally tested, and is receiving data (via C37.118 format) from the DFR/PMU

Scenario Steps

Step	Description	Possible Sensors
1	A Threat Agent executes an ARP poising attack to intercept traffic between the DFR/PMU and the PDC	
2	The Threat Agent alters the Data Frames from the DFR/PMU to indicate falsely that a configuration change has been made by asserting Bit 10 of the STAT field within the Data Frame.	C37.118 deep packet inspection (detection of assertion of Bit 10 of the STAT field within the Data Frame)
3	The Threat Agent forwards the altered Data Frames to the PDC	
4	Upon receipt of the Data Frame noting the configuration change (Bit 10 of the STAT field asserted), the PDC sends the Command Frame (Send CFG-1,2, or 3) to the DFR/PMU.	C37.118 deep packet inspection (detection of Command Frame being sent to DFR/PMU)
5	The Threat Agent passes the Command Frame (Send CFG-1,2, or 3) through to the DFR/PMU unaltered	

Step	Description	Possible Sensors
6	The DFR/PMU processes the Command Frame (Send CFG-1,2, or 3) and sends the response (Configuration Frame) to the Threat Agent (thinking that the Threat Agent is the PDC)	
7	The Threat Agent then alters the time base (TIME_BASE) within the Configuration Frame received from the DFR/PMU and transmits the altered Configuration Frame to the PDC	C37.118 deep packet inspection (detection of Configuration Frame being sent to PDC)
8	The PDC receives and processes the altered Configuration Frame	
9	The Threat Agent ends the attack	
10	The DFR/PMU begins transmitting Data Frames directly to the PDC (no longer redirected to the Threat Agent)	
11	The PDC parses the Data Frames from the DFR/PMU according to the last received Configuration Frame.	
12	The PDC time correlates the data from the affected DFR/PMU unit along with data from other (normal) DFR/PMU units and forwards the aggregated data to upstream Operational Applications (such as EMS), Phasor Gateway and/or Historian	
13	The Operational Application detect data anomaly	
14	The Historian stores the received data	
15	The Phasor Gateway forwards the aggregated data to and external entity and/or the Historian forwards the aggregated data to other internal (non-operational) application	

3.3 Requirements

The requirements developed for this project are generally at a high level, which is appropriate for a system that is in a research and development phase. These requirements provide an outline of the basic desired functionality and can be further refined to support an actual field deployment.

3.3.1 Functional Requirements

The project used two approaches to develop requirements. The first considered the set of threats and attack use cases developed in sections 3.1 & 3.2. The second approach considered a generalized operational view based on the installation and use of the notional CAPMS system.

1. Installation
2. CAPMS Operational Cycle
    a. Sensing
    b. Policy Application
    c. Response
3. Security

Installation Requirements

A goal for CAPMS is to minimize additional utility resources required to install and configure CAPMS functionality. A future deployed CAPMS system would be installed on many field devices and ease of installation and configuration would be a high priority.

REQ ID	Requirement
1.1	CAPMS shall be installed on target client devices.
	Requirement met.
1.2	CAPMS installation shall be implemented as a CCS upgrade.
	Requirement met. Future system may be integrated into CCS.
1.3	Centralized CAPMS functions shall be installed within the existing CCS system.
	Requirement met.
1.4	CAPMS shall minimize configuration of point-to-point interconnection interfaces with external sensor and actuator actors.
	Requirement met. The project demonstrated a simplified standard interface.
1.5	CAPMS shall support a flexible set of interfaces to support vendor development of CCS/CAPMS clients.
	Requirement met. The JSON interface provides an open standard interface. Additional interfaces are possible.

Sensing Requirements

A goal for CAPMS is to demonstrate an increased level of awareness and policy responses when using data from systems that have traditionally been unavailable to a security system. The CAPMS is designed to use a variety of external data sources that provide additional context to the detection of cyber-physical security events.

REQ ID	Requirement
2.1	CAPMS shall receive and process syslog event messages from client devices and external interfaces.
	Requirement met. CAPMS has an internal log aggregator.
2.2	CAPMS shall receive and process TCP messages from client devices and external interfaces.
	Requirement met. CAPMS receives TCP messages through Splunk.
2.3	CAPMS shall use the Phasor Data Concentrator as a sensor
	Requirement met. CAPMS receives log messages from the Phasor Data Concentrator.
2.4	CAPMS shall use Splunk as a sensor
	Requirement met. Splunk was configured to receive syslog messages from several systems and provide that data to CAPMS.
2.5	CAPMS shall support deep packet inspection of C37.118 messages
	Requirement met. CAPMS monitors C37 messages and is aware of device configuration change messages.
2.6	CAPMS shall detect failed logins to monitored devices
	Requirement met. CAPMS receives failed login notices through the Splunk interface.
2.7	CAPMS shall provide the capability for the CAPMS operator to manually place the CAPMS agent “offline” or in an “online” mode.

REQ ID	Requirement
	Requirement met. Devices with the CAPMS agent can be enabled or disabled.

Policy Application Requirements

CAPMS policies should provide a flexible framework for the utility to configure the monitored data streams, and the responses that it should take upon detection of potential intrusion attempts.

REQ ID	Requirement
3.1	CAPMS shall perform an automated analysis to detect a cyber-intrusion.
	Requirement met. CAPMS uses a probabilistic Bayesian tree to determine the likelihood of intrusion.
3.2	CAPMS shall report the detection of a cyber-intrusion to CAPMS operator.
	Requirement met. The CAPMS GUI reports detected events and the CAPMS system is able to send notifications to other systems.
3.3	CAPMS shall use CCS functionality to assess the health and status of CCS enabled client devices.
	Requirement met.
3.4	CAPMS shall apply policies to detected cyber-intrusions and determine the most appropriate course of action.
	Requirement met. Policy responses provide both user notifications and automatic responses to be made.
3.5	CAPMS shall report the activation/deactivation of a policy and indicate the device(s) impacted to the CAPMS operator.
	Requirement met. Policy deployment and management is managed through a CAPMS GUI. Threat detections and responses are reported through the CAPMS GUI and optionally to other users and systems.
3.6	CAPMS shall provide a summary of all currently policy activations.
	Under development. The CAPMS GUI will provide a summary of detections and responses.
3.7	CAPMS shall provide policy options that require CAPMS operator approval before activation.
	Requirement met. CAPMS responses can be actions that require an operator's approval before being activated.
3.8	CAPMS shall provide the CAPMS operator with the ability to revert (i.e. Cancel) an activated policy.
	Requirement not tested but possible. Actions taken by the CAPMS system can be reviewed by the operator. Additionally, commanded actions taken by CAPMS can include restoration to previous functionality.
3.9	CAPMS shall provide a policy response that is informational only (i.e., Alert Notification).
	Requirement met. Multiple notification options are available.
3.10	CAPMS shall be able to change monitoring levels based on suspicious activity.
	Requirement met. The Bayesian tree allows for levels of certainty and the possibility to take actions as detections are made.
3.11	CAPMS shall be able to initiate new PKI exchange for monitored devices
	Requirement met through CCS functionality.

Response Requirements

The CAPMS response requirements were tailored to the testing environment, but were chosen to test and demonstrate the ability of CAPMS to interact with systems with defined interfaces and use them as part of a security policy's response.

REQ ID	Requirement
4.1	CAPMS shall use eDNA as an actuator.
	Requirement met. The eDNA system was used as a proxy for a Control Center application; CAPMS sends notifications informing an operator that a perceived electric system event are is actually a cyber-attack.
4.2	CAPMS shall support informational messages to external systems and their users as a policy response.
	Requirement met. CAPMS is able to send email and send notifications to systems.
4.3	CAPMS shall support defined interfaces on actuator systems to perform permitted actions as a policy response.
	Requirement met. The eDNA system provided an interface to receive messages from CAPMS.

Security Requirements

CAPMS should support and enhance SCE's ability to implement security policy and assist in meeting federal and state requirements for reporting and auditing.

REQ ID	Requirement
5.1	CAPMS policy engine shall support the implementation of SCE cyber-security policies for substation devices.
	Requirement met. CAPMS policies can support SCE policy guidelines.
5.2	CAPMS shall store logs of all event detections and actions taken to support SCE cyber-security polices for substation devices.
	Requirement met. CAPMS maintains an event log of detections and actions.
5.3	CAPMS shall provide authorized local users the ability to deactivate auto-response functionality.
	Requirement not tested.
5.4	CAPMS shall be able to send its application logs to SCE selected data repository or historian.
	Requirement not tested.

4 Project Results

4.1 Project Data Summary

Unlike many projects, CAPMS was not evaluating the performance, effectiveness, or efficiency of a new type of grid equipment or demand response program. CAPMS developed and demonstrated a new type of security system, one that operators can configure with policies to respond automatically when it detects cyber-intrusions. As such, there are no measurements to report and summarize that one might normally consider "data". However, the project did record several simulated data points. The data historian recorded the measurements from our two PMUs, attached to the grid model simulated by RTDS. SCE recorded the AC

frequency at each PMU, and for each A, B, and C phase at each PMU, SCE recorded the voltage magnitude and phase angle as shown in Figure 6: PMU Data Points.

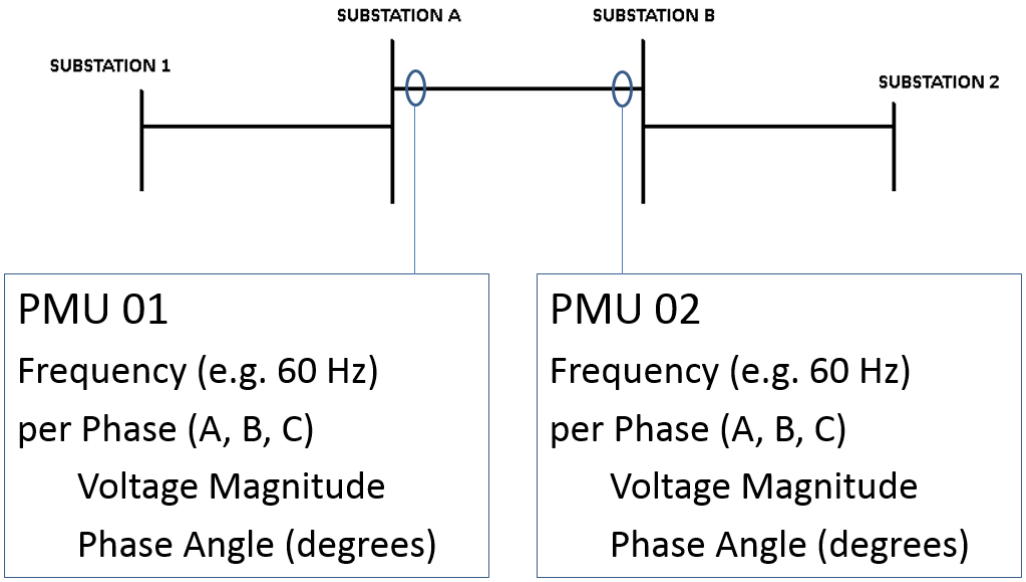

Figure 6: PMU Data Points

In addition to the data points measured directly by the PMUs, the project created several additional data points used to demonstrate inputs and outputs to and from CAPMS, as listed in the table below. The project created similar points for substation B and PMU 2.

POINTID	Type	LOCATION	I/O	Values
CAPMS.CALCSERV.PFL	Power Flow (from Phasors)	LINE		Analog (Current)
CAPMS.UNIVSERV.PFLABNML	Power Flow Abnormal	LINE	Input	0 = No, 1 = Yes
CAPMS.UNIVSERV.SUBAWORK	Scheduled Work	SUB A	Input	0 = No, 1 = Yes
CAPMS.UNIVSERV.SUBAPACC	Physical Access Alarm	SUB A	Input	0 = No, 1 = Yes
CAPMS.UNIVSERV.SUBANACC	Network Access Alarm	SUB A	Input	0 = No, 1 = Yes
CAPMS.UNIVSERV.SUBAPHYS	Physical Alert State	SUB A	Output	0 = Normal, 1 = Warning, 2 = Alarm
CAPMS.UNIVSERV.SUBACYBR	Cyber Alert State	SUB A	Output	0 = Normal, 1 = Warning, 2 = Alarm
CAPMS.UNIVSERV.PMU1CMBD	Combined Alert State	PMU 1	Output	0 = Normal, 1 = Warning, 2 = Alarm

Figure 8 shows a graph of a typical attack flow. There is no work scheduled, and the simulated attacker triggers the physical access alarm at substation A. This raises the substation alert state to “warning”. The attacker then modifies the configuration of the PMU to map one of the phases to a null input, effectively reducing the calculated power flow by one third (from 521 kW to around 350). This triggers the “power flow

abnormal" point, meant to simulate a validation that a state estimator could produce, flagging measurements that don't seem to fit with the other observed points. Figure 7 shows a graph of the calculated power flow on the line during a simulated attack, including the "PFLABML" calculated point. Note that the blue "Power Flow" line uses the axis on the left (kW) whereas the red "Suspect Readings" line uses the axis on the right. (0 = No, 1 = Yes)

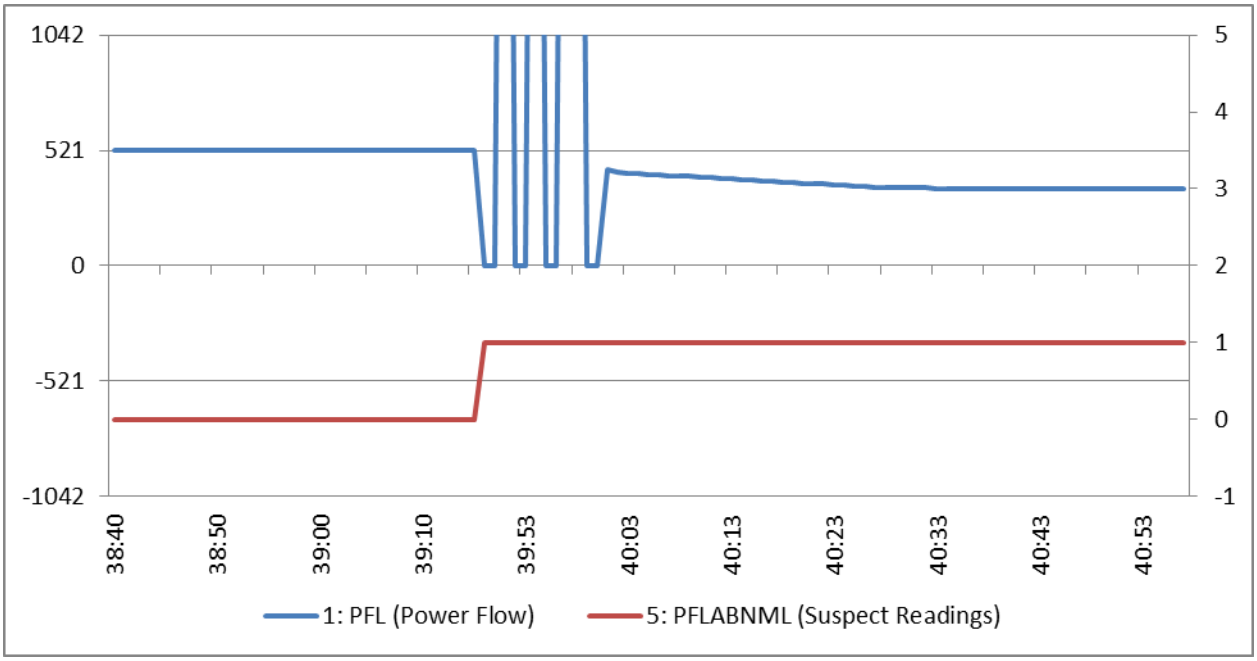

Figure 7: Simulated Power Flow during Configuration Attack

When CAPMS receives the "PFLABNML = 1" event, it raises the substation alert state (SUBAPHYS) to "alarm".

	38:36	38:37	38:42	38:43	38:44	39:18	39:19	39:40	39:41	40:26
8: PMU1CMBD (Device Alert State)	0							0	1	1
7: SUBAPHYS (Physical Alert State)	0			0	1			1	2	2
5: PFLABNML (Suspect Readings)	0					0	1			1
4: SUBAPACC (Physical Access)	0		0	1						1
2: SUBAWORK (Work Scheduled)	1	0								0

Figure 8: Demo Data Points Graph

The CAPMS output alert state points escalate from normal (0) to warning (1) and finally alarm (2) as the attack progresses, resulting in visible indicators on a simulated grid operator screen as shown in Figure 9.

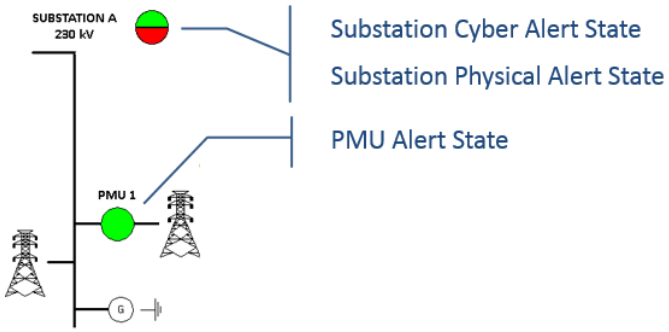

Figure 9: Simulated Grid Operator View with CAPMS Indicators

4.2 Findings

It seems likely that an auto-response policy management system could be effective in preventing and containing attacks. However, there are some potential hurdles that implementers must clear in order to deliver a cost-effective system to the industry.

4.2.1 Value

The value provided to a utility by CAPMS is more than just directly detecting and reacting to a cyber-attack. While this is the primary purpose of CAPMS, there are other potential benefits.

Preventing Operator Error

A cybersecurity system aware of system states could prevent operating errors by alerting Grid Operators that observed power system data within or utilized by an operational application may not be reflective of actual grid conditions. This is especially valuable given that in many cases, operators use power system data to make grid level decisions.

Human Performance Events

The system could detect human performance events, such as a failure to follow an approved process or procedure. Over time, this will improve consistency and adherence to procedures.

System Health Awareness

Such a system can increase awareness of the overall health of the applications, devices, and communications infrastructure utilized for grid operations. Knowing this will allow operators to avoid making changes that could weaken the system when it is in a weakened state.

4.2.2 Challenges

Deployment of CAPMS in an operational environment is not without its challenges.

Policy Definition

Automated responses require definition and integration at each deployment site, potentially requiring significant configuration and custom development effort. It is possible to develop policies that could be re-used, but it will be difficult to balance flexibility, stability, and cost-effectiveness.

Integration

Each deployment of the system must configure not only the policies, but also the inputs and outputs to those policies, with a potentially different set of systems. At this point, these interfaces are not well defined enough to be reusable, which could cause difficulties with maintaining them.

Operator Trust

The operators of the system will not immediately trust the system to make the right response decisions. They will want to understand and be involved in the definition of the policies, and they will want the ability to see the contributing inputs and be able to approve recommended actions before allowing automatic action. The system does include the ability to configure actions to require operator approval, as shown in Figure 10 below. Still, this could slow down response times until the system is tuned and trusted to react automatically.

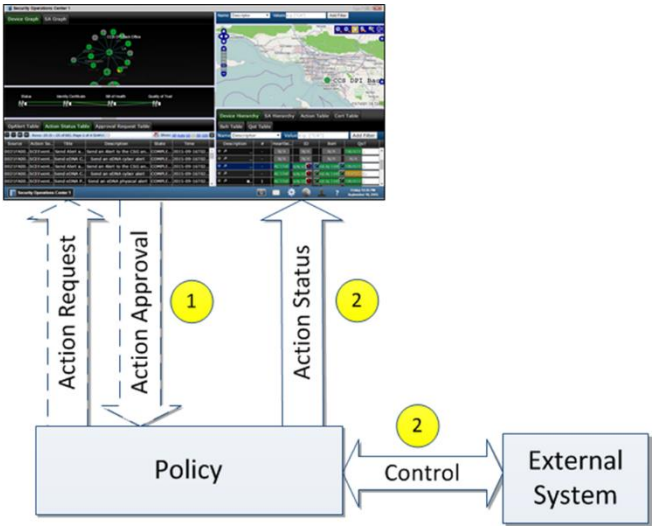

Figure 10: Operator Response Approval Flow

Scalability

The demonstration project implemented a simple policy at a single location. It is likely that management of large numbers of policies at thousands of locations will be difficult. Also, with a large deployment, the policy engine processing would probably need changes to be massively scalable.

Applicability

The system uses openly specified cybersecurity protocols, however most components do not implement them directly. CCS has agents that allow for the protection of Unix/Linux, Windows, and embedded systems, as well as hardware options for terminating protected channels. The protected endpoints do require IP communications.

4.3 Special Implementation Issues

4.3.1 System Integration Challenges

Adapters

Described in the communications architecture of CAPMS, third party adapters can greatly increase the capabilities of a CAPMS policy, benefitting both sensor and response functions. These third party services

may provide both sensing and actuation functions. However, in order to use these third party services, projects must first create adapters.

These adapters can be a barrier of entry for integration with these third party services. It is most feasible for CAPMS policies to integrate with third party services that have a high level of configurability or plugin support.

An example of a sensor service that provides a high level of configurability is Splunk. The CAPMS project leveraged Splunk's support for real-time alert response, which allows for the execution of a script that enables the communication of Splunk-detected events to a CAPMS policy.

An example of an actuation service that provides a high level of configurability is the data historian, eDNA. This product allowed custom interfaces to be constructed that responded to CAPMS policy inputs.

Such configurability features are very important for enabling the use of a CAPMS policy. Services that do not have such integration capabilities can be a barrier from a CAPMS, requiring vendors or project teams to develop integrations with CAPMS policies.

The flexibility of the CAPMS policies in allowing for multiple interfaces does help to mitigate this as a potential issue.

4.3.2 Bayesian Modeling

Selecting Accurate Bayesian Probabilities in Correlative Models

The CAPMS approach describes a Bayesian model for interrelating conditions (both detectable and undetectable). These models accept input events from CAPMS sensors. These models treat these input events as evidence, which allows arrival at conditions that may require multiple inputs to determine whether they have occurred.

The diagram below shows an example of a correlated model in which the system uses the evidence to determine higher-order states.

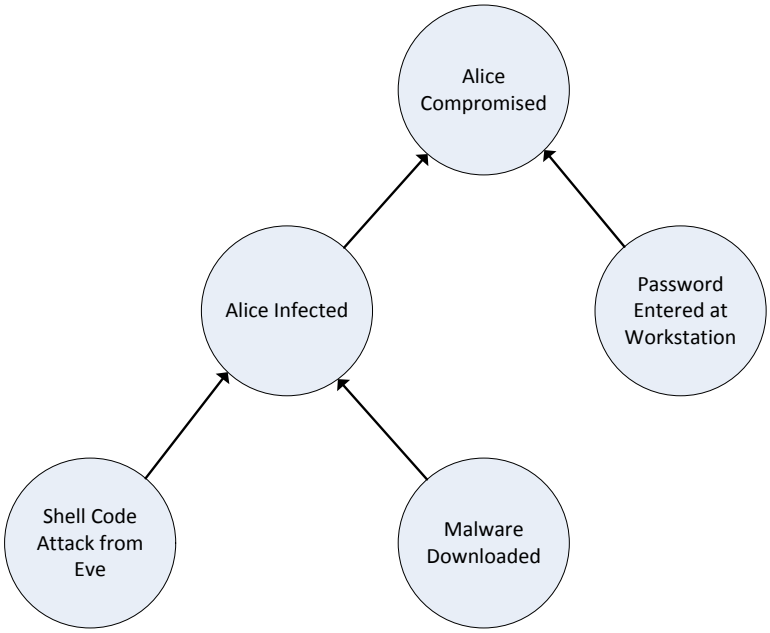

Figure 11 Bayesian Network of Attack Tree

As an example, consider the attack tree converted into the Bayesian network in Figure 11.

- S = "Shell Code Attack from Eve"
- M = "Malware Downloaded"
- W = "Password Entered at Workstation"
- I = "Alice Infected"
- C = "Alice Compromised"

Then SCE needs to define conditional probability tables for the non-leaf nodes, "I" and "C", based on their children. SCE might have the probability tables in Table 1.

Table 1 Conditional Probability Tables for I (above) and C (below)

S	M	P(I = true |S, M)	P(I = false |S, M)
true	true	0.97	0.03
true	false	0.66	0.34
false	true	0.57	0.43
false	false	0.11	0.89

I	W	P(C = true |I, W)	P(C = false |I, W)
true	true	0.82	0.18
true	false	0.60	0.40
false	true	0.48	0.52
false	false	0.14	0.86

Someone with knowledge of the relationship between goals should initialize these probability tables. In the event that this is impossible or impractical, SCE can try training our model with data that is representative of

the state of the system. In the worst case, SCE can initialize our conditional probability tables as truth tables for the gates they may represent and use the Bayesian learning to get estimates that are more accurate.

This can prove to be a challenging element of the use of CAPMS policies. There are a few mitigations for this issue, described in the sections below.

Selection of Simple Probability Tables

The probabilities that the CAPMS project demonstrated upon completion are an example of this approach. CAPMS policies allow for the use of AND and OR logical behaviors so that complex conditional probability tables do not need to be crafted for simple conditions. This simple logic covers more conditions than one may expect.

For example, if CAPMS should enact a response in a condition where there is both a motion sensor detected and a login event, this does not need more complex probability tables for correlating these two conditions.

The use of a hybrid model that combines both simple Boolean logic with more complex probability calculations (when needed) helps to reduce the amount of work needed when assigning probabilities to a CAPMS policy. The approaches described in the sections that follow can aid the determination of these probability tables.

Collection of Data Which Influences Probabilities

The CAPMS platform has focused most of its efforts on the identification of key threats as well as the design of a system that allows for correlated modeling and responses. One of the potential areas for follow-on work would be the investigation of how to better model correlated events. Data that could influence the CAPMS work include:

- Forensics analysis of previous attacks
- Input from domain experts
- Simulation and modeling of attacks on a system reflective of the environment in which a CAPMS policy must reside

Incremental Refinement of Probabilities

CAPMS policies allow for configurable attributes. Conditional probability tables that inform the Bayesian networks may be included in these configurable attributes. This allows a policy to be reused and refined over time without going back to the original developer of the security policy for resubmission.

Operators of a security policy may need to modify these conditional probability tables after observation and testing of a policy. These operators may make an educated determination that a policy's decision is not arriving at the correct conclusions and may modify these conditional probability tables as a way to influence the decision-making. For example, if the "Shellcode Downloaded from Eve" condition described above is incorrectly causing the policy to conclude strongly that Alice is infected, when Alice is known to not be infected, then this is feedback into the behavior of the policy.

4.3.3 Issues with Representing Attack Trees as Bayesian Networks

There is also potential interest in using Bayesian networks for representation of attack trees described in NESCOR[1]. Consider how the With the OR gate, it is straightforward to have the two lower goals feed into the higher goal separately. However, with the AND gate this technique does not necessarily preserve the relationship between the two lower goals. For instance, in this case the AND is used because SCE expects that both "Shell Code Attack from Eve" and "Malware Downloaded" must happen in order for "Alice Infected" to happen. This is because there is some relationship between the two lower goals. It would violate the assumptions of the Bayesian network that "Shell Code Attack from Eve" and "Malware Downloaded" are independent events, when in reality, the fact that one has happened likely indicates that the other has happened or will happen since the attacker is likely trying to cause "Alice Infected."

Depending on the specific events, it may make more sense to use the network on the left of Figure 12. In this way, SCE represents that "Shell Code Attack from Eve" could lead to "Malware Downloaded" which would then lead to "Alice Infected." It also captures that "Shell Code Attack from Eve" by itself might be an indication of "Alice Infected" even without evidence of "Malware Downloaded."

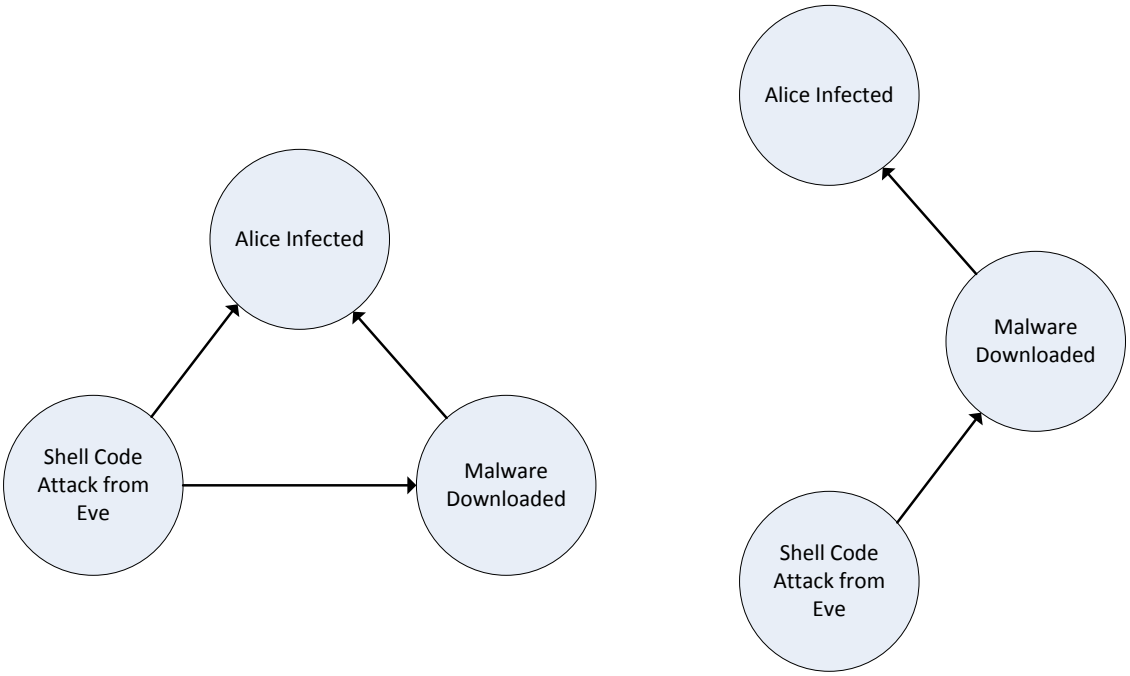

Figure 12 Two Options for Converting an AND Gate

If SCE wants to maintain a tree structure in our Bayesian network, SCE could use the network on the right of Figure 12. This method is proposed in (Qin & Lee, 2004). This preserves the assumption that "Shell Code Attack from Eve" would be a precursor to "Malware Downloaded." It does not completely lose the benefit of having "Shell Code Attack from Eve" influence "Alice Infected" because if "Shell Code Attack from Eve" is

[1] http://smartgrid.epri.com/NESCOR.aspx

detected, this will increase the confidence that “Malware Downloaded” has happened, even if it is not detected, which will in turn raise the confidence that “Alice Infected” is true.

Preserving the tree structure keeps the representation simpler and allows for faster algorithm performance. Nevertheless, the more the Bayesian network reflects the causal relationships in reality, the more accurately it will predict the state of the system. The main issue with this method is that “Malware Downloaded” can block information passing from “Shell Code Attack from Eve” to “Alice Infected.” For example, if SCE knows that “Malware Downloaded” = true, then knowing anything about “Shell Code Attack from Eve” will not affect our belief about “Alice Infected.” This is because the probability table for “Alice Infected” only depends on “Malware Downloaded.” This does not respect the interpretation of an AND gate which should depend on both inputs.

4.4 Principles and Value Proposition

The security of communications is a fundamental underlying technology required for many advanced functions, so the CAPMS project contributes either directly or indirectly to all of the primary EPIC principles. It provides savings over typical solutions by placing cybersecurity primarily in the network infrastructure. This allows multiple grid devices and systems to reuse the network and security features, reducing the cost of communicating equipment and improving overall security and manageability. An effective cybersecurity solution will also provide greater reliability of the electric grid, since it will be able to proactively identify and neutralize threats before they can affect grid components.

Several of the secondary EPIC principles promote implementation of distributed resources programs such as solar, wind, energy storage, demand response, and electric vehicle charging. These programs require secure automated communication of regional forecasts and constraints, directly or indirectly specifying when to increase or decrease load and generation in order to balance supply with demand. Many of these programs will need to communicate with customer and third party energy services provider systems, and while they probably won’t use the same protections and defenses as internal systems, identification and correlation of threats may still be possible and beneficial.

4.5 Technology Transfer Plans

The results of this research show that there are a number of potential benefits to distributed security policies and auto-response to cyber-intrusions identified using correlation of sensor-based events. Future projects at SCE may use these results to inform requirements development for enhanced distributed resources management systems and other future projects. The technology meets several grid security objectives and design characteristics listed below.

- Support new and existing equipment
- Comply with standards and facilitate interoperability
- Implement common services architecture to support reuse
- Support multi-level security and dynamic trust boundary definition
- Provide ability to define automatic response to contain coordinated attacks

The project included a demonstration at SCE as well as one at Duke Energy. The Duke demonstration uses the same TNP foundation, and used much of the same CAPMS code. This helped project teams to identify and distinguish base functionality from configuration and custom code. Effective design and clear delineation of these boundaries should enable more widespread use and deployment of the technology, allowing for more potential savings due to economy of scale.

4.6 EPIC Metrics

D.13-11-025, Attachment 4. List of Proposed Metrics and Potential Areas of Measurement (as applicable to a specific project or investment area in applied research, technology demonstration, and market facilitation)	
5. Safety, Power Quality, and Reliability (Equipment, Electricity System)	
a. Outage number, frequency and duration reductions	See 4.6.1
7. Identification of barriers or issues resolved that prevented widespread deployment of technology or strategy	
b. Increased use of cost-effective digital information and control technology to improve reliability, security, and efficiency of the electric grid (PU Code § 8360)	See 4.6.2
f. Deployment of cost-effective smart technologies, including real time, automated, interactive technologies that optimize the physical operation of appliances and consumer devices for metering, communications concerning grid operations and status, and distribution automation (PU Code § 8360)	See 4.6.2
l. Identification and lowering of unreasonable or unnecessary barriers to adoption of smart grid technologies, practices, and services (PU Code § 8360)	See 4.6.2
8. Effectiveness of information dissemination	
b. Number of reports and fact sheets published online	See 4.6.3
d. Number of information sharing forums held.	See 4.6.3
f. Technology transfer	See 4.5
10. Reduced ratepayer project costs through external funding or contributions for EPIC-funded research on technologies or strategies	
a. Description or documentation of funding or contributions committed by others	See 4.6.4
c. Dollar value of funding or contributions committed by others.	See 4.6.4

4.6.1 Outage Reduction

A system such as CAPMS will help to prevent or reduce duration of outages caused by cyber and physical attacks, as well as other types of unplanned outages. It is difficult to estimate how large of an impact it might have, since it depends heavily on the depth of integration and configuration (how accurately and quickly it can identify attacks and other problems) and how many attacks or other problems occur, and how severe and extensive they are.

Risk evaluation methodologies can be applied to demonstrate the impact of CAPMS on reducing outages. Traditionally, risk is the product of an event's probability and the consequence of that event.

$$R = P * C$$

Previous academic work has developed methods to quantify expected losses in an attack to better evaluate various benefit options (Carlson, Rutnquist, & Nozick, 2004) and decompose the elements of probability in a manner that is appropriate to control systems (McQueen, Boyer, Flynn, & Beitel, 2006). This second paper characterizes the total probability as a product of conditional probabilities:

$P = P_1 * P_2 * P_3 * P_4 * P_5$ where

P_1 = the probability the system is on an attacker target list

P_2 = probability of being attacked given that the system is targeted

P_3 = probability of a perimeter breach given that the system is attacked

P_4 = probability of a successful attack given that there was a perimeter breach

P_5 = probability of damage given that the system was successfully attacked

Estimating the above probabilities is difficult and outside the scope of the project as is an impact analysis of the consequence of a successful attack. The above formulation does show where CAPMS can reduce the total risk by reducing the last three probabilities. Probabilities P_1 and P_2 are outside the scope of CAPMS and are generally addressed by maintaining a private network with a clear separation from the Internet.

4.6.2 Smart Devices

Utilities have traditionally preferred dedicated private connections for electronic communications with field equipment. Internet technologies offer an opportunity to reduce the cost of "smart" equipment by using routable protocols over virtual private network connections shared by multiple devices. However, cybersecurity systems must protect those communications from unauthorized access. Traditional public key infrastructure (PKI) technologies can manage this aspect, but if an attacker gains control of valid credentials, or finds an unprotected access point, operators need another layer of security to automatically detect and respond to these attacks in a timely manner. Operators must also be aware of cyber-threats that could alter

their view of the grid, in order to prevent responses to false readings. CAPMS provides this higher-level of decision logic and automation, making smart grid and other communicating equipment safe and reliable.

4.6.3 Information Dissemination

Reports and Fact Sheets Published Online

1. **ViaSat Project Award Press Release**
   https://www.viasat.com/news/us-department-energy-award-funds-infrastructure-cybersecurity-development-viasat-and-two-major
2. **Interactive Energy Roadmap Project Effort Overview**
   https://www.controlsystemsroadmap.net/Efforts/Pages/CAPMS.aspx
3. **ieRoadmap Project Description Peer Review Slides**
   https://www.controlsystemsroadmap.net/ieRoadmap%20Documents/ViaSat-CAPMS-CEDS_Peer_Review_2014.pdf
4. **DoE CAPMS Flyer**
   https://www.controlsystemsroadmap.net/ieRoadmap%20Documents/CAPMS_flyer.pdf
5. **ICS SANS Institute Demonstration Slides**
   https://files.sans.org/summit/ics2015/PDFs/Live_ICS_Attack_Demo.pdf
6. **ICS Security Summit CAPMS Demo Video**
   https://www.youtube.com/watch?v=tZDDALpI_yo

Information Sharing Forums Held

1. **10th Annual ICS Security Summit CAPMS Demonstration**
   Orlando, FL | Sunday, Feb 22, 2015 - Mon, Mar 2, 2015
2. **CAPMS SCE Demonstration**
   Westminster, CA | Thursday, Sep 24, 2015
3. **CAPMS Duke Demonstration**
   Charlotte, NC | Tuesday, Sep 29, 2015

4.6.4 Reduced Ratepayer Project Costs

The CAPMS project received half of its funding from a DOE grant. Duke Energy committed approximately $1.2M, and the DOE committed approximately $3M to the overall CAPMS project.

5 Appendices

A. WAMPAC Failure Modes Matrix

				Informational impact of attack				
Failure ID	Attack Target (Funtional)	Attack Type	Possible Result/Failure Mode	Distort	Disrupt	Destruct	Disclosure	Discovery
T1	Network Time Distribution	Spoofing NTP/SNTP server	Clock error within C37.118 server	X				
T2	Network Time Distribution	Spoofing NTP/SNTP server	Clock error within PDC or Phasor Gateway	X	X			
T3	Network Time Distribution	DoS attack on NTP/SNTP server	C37.118 server reverts to alternate time source		X			
T4	Network Time Distribution	DoS attack on NTP/SNTP server	C37.118 server reverts to internal clock		X			
T5	IRIG-B Time Distribution	Substituting/Spoofing IRIG-B input	PMU clock error	X				
T6	IRIG-B Time Distribution	Disrupting IRIG-B input	PMU reverts to internal clock		X			
T7	GPS Signal Reception	GPS jamming	PMU or PDC reverts to internal clock		X			
T8	GPS Signal Reception	GPS spoofing	Clock error within C37.118 server	X				
T9	GPS Signal Reception	GPS spoofing	Clock error within PDC or Phasor Gateway	X	X			
T10	GPS Receiver	Unauthorized configuration change	Clock error within C37.118 server	X				
T11	GPS Receiver	Unauthorized configuration change	Clock error within PDC or Phasor Gateway	X	X			
AL1	C37.118	Spoofing C37.118 server	False data stream transmitted to upstream C37.118 client	X				
AL2	C37.118	Spoofing C37.118 server	False configuration or header message transmitted to upstream C37.118 client	X				
AL3	C37.118	Spoofing C37.118 client	C37.118 server data stream redirected to imposter		X			
AL4	C37.118	Spoofing C37.118 client	Spoofed C37.118 client starts/stops PMU data stream		X			
AL5	C37.118	Man-In-The-Middle	Monitoring/eavesdropping of messages (header/configuration/data stream) from C37.118 server to C37.118 client				X	
AL6	C37.118	Man-In-The-Middle	altered configuration or header message sent to upstream C37.118 client	X				
AL7	C37.118	Man-In-The-Middle	altered data stream sent to upstream C37.118 client	X				
AL8	C37.118	Fuzzing C37.118 protocol	Abnormal behavior or termination of the application on target device		X			
AL9	C37.118	Unauthorized/rouge C37.118 client	Command message from unauthorized C37.118 client starts/stops PMU data stream		X			
N1	Network Infrastructure	Flooding (DoS)	Delayed receipt of data stream by upstream C37.118 client		X			
N2	Network Infrastructure	Flooding (DoS)	Message exchange interupted between C37.118 client and server		X			
N3	Network Infrastructure	ARP spoofing	Message exchange interupted between C37.118 client and server		X			
H1	Network Interface (NIC)	DoS	Device unable to access network		X			
H2	Network Interface (NIC)	DoS	Abnormal behavior or termination of the application		X			
H3	Network Interface (NIC)	Port scanning	Open logical network interface to device discovered (e.g. ftp, telnet, http, etc.)					X
H4	Firmware/OS	Malware	Device utilized to gain access to other protected network resources					X
H5	Firmware/OS	Malware	Unexpected behavior of device		X			
H6	Configuration	configuration	Phasor data within data stream incorrect	X				
H7	Configuration	configuration	Mismatch between header/configuration messages and phasor data within data stream	X				
H8	Database	uauthorized database access	Archieved/historical data modified	X				
H9	Database	uauthorized database access	Archieved/historical data deleted			X		

B. WAMPAC Attack Scenario Matrix

Scenario ID	Associated Failure ID	Attack Category	Attack Target (Funtional)	Attack Type	Possible Result/Failure Mode	Possibe Attack Scenario	DFR/PMU	GPS (Substation)	USI Master	PDC	GPS (Control Center)	Historian	Phasor Gateway	Network
1	T1	Timing	Network Time Distribution	Spoofing NTP/SNTP server	Clock error within C37.118 server	Spoofed NTP/SNTP server creates clock error in PMU	x	x						
2	T2	Timing	Network Time Distribution	Spoofing NTP/SNTP server	Clock error within PDC or Phasor Gateway	Spoofed NTP/SNTP server creates clock error in PDC and causes waiting period violation for incoming data stream(s)				x	x			
3	T3	Timing	Network Time Distribution	DoS attack on NTP/SNTP server	C37.118 server reverts to alternate time source	Unavailable NTP/SNTP server causes PMU to revert to alternate time source	x	x						
4	T3	Timing	Network Time Distribution	DoS attack on NTP/SNTP server	C37.118 server reverts to alternate time source	Unavailable NTP/SNTP server causes PDC to revert to alternate time source				x	x			
5	T4	Timing	Network Time Distribution	DoS attack on NTP/SNTP server	C37.118 server reverts to internal clock	Unavailable NTP/SNTP server(s) cause PMU to revert to internal clock	x	x						
6	T4	Timing	Network Time Distribution	DoS attack on NTP/SNTP server	C37.118 server reverts to internal clock	Unavailable NTP/SNTP server(s) cause PDC to revert to internal clock				x	x			
7	T5	Timing	IRIG-B Time Distribution	Substituting/Spoofing IRIG-B input	PMU clock error	Rouge IRIG-B source connected to DFR/PMU creates clock error	x	x						
8	T6	Timing	IRIG-B Time Distribution	Disrupting IRIG-B input	PMU reverts to internal clock	Interuption of IRIG-B signal input causes DFR/PMU to revert to internal clock.	x	x						
9	T7	Timing	GPS Signal Reception	GPS jamming	C37.118 server reverts to internal clock	Error in the IRIG-B output of the GPS receiver causes PMU to revert to internal clock	x	x						
10	T7	Timing	GPS Signal Reception	GPS jamming	C37.118 server reverts to internal clock	Error in the NTP/SNTP output of the GPS receiver causes PDC to revert to internal clock				x	x			
11	T8	Timing	GPS Signal Reception	GPS spoofing	Clock error within C37.118 server	Spoofed GPS signal creates clock error GPS and PMU	x	x						
12	T9	Timing	GPS Signal Reception	GPS spoofing	Clock error within PDC or Phasor Gateway	Spoofed GPS signal creates clock error in PDC and causes waiting period violation for incoming data stream(s)				x	x			
13	T10	Timing	GPS Receiver	Unauthorized configuration change	Clock error within C37.118 server	Erroneous IRIG-B output of GPS receiver creates clock error in DFR/PMU	x	x						
14	T11	Timing	GPS Receiver	Unauthorized configuration change	Clock error within PDC or Phasor Gateway	Erroneous NTP/SNTP output of GPS receiver creates clock error in PDC and causes waiting period violation for incoming data stream(s)				x	x			
15	AL1	Application Layer	C37.118	Spoofing C37.118 server	False data stream transmitted to upstream C37.118 client	Spoofed PMU (C37.118 server) transmits incorrect data to PDC (C37.118 client)	x			x				
16	AL1	Application Layer	C37.119	Spoofing C37.118 server	False data stream transmitted to upstream C37.118 client	Spoofed PDC (C37.118 server) transmits incorrect data to Historian (C37.118 client)				x		x		
17	AL1	Application Layer	C37.120	Spoofing C37.118 server	False data stream transmitted to upstream C37.118 client	Spoofed PDC (C37.118 server) transmits incorrect data to Gateway (C37.118 client)				x			x	
18	AL1	Application Layer	C37.121	Spoofing C37.118 server	False data stream transmitted to upstream C37.118 client	Spoofed Phasor Gateway (C37.118 server) transmits incorrect data to external entity (C37.118 cleint)								
19	AL2	Application Layer	C37.118	Spoofing C37.118 server	False configuration or header message transmitted to upstream C37.118 client	Spoofed PMU (C37.118 server) transmits incorrect header or configuration to PDC (C37.118 client)	x			x				
20	AL2	Application Layer	C37.119	Spoofing C37.118 server	False configuration or header message transmitted to upstream C37.118 client	Spoofed PDC (C37.118 server) transmits incorrect header or configuration to Historian (C37.118 client)				x		x		
21	AL2	Application Layer	C37.120	Spoofing C37.118 server	False configuration or header message transmitted to upstream C37.118 client	Spoofed PDC (C37.118 server) transmits incorrect header or configuration to Phasor Gateway (C37.118 client)				x			x	
22	AL2	Application Layer	C37.121	Spoofing C37.118 server	False configuration or header message transmitted to upstream C37.118 client	Spoofed Phasor Gateway (C37.118 server) transmits incorrect header to external entity (C37.118 client)								
23	AL3	Application Layer	C37.118	Spoofing C37.118 client	C37.118 server data stream redirected to imposter	Spoofed PDC (C37.118 client) intercepts data stream from PMU (C37.118 server)	x			x				
24	AL4	Application Layer	C37.118	Spoofing C37.118 client	Spoofed C37.118 client starts/stops PMU data stream	Spoofed PDC (C37.118 client) sends command message to stop data stream from PMU (C37.118 server) to authorized PDC	x			x				
25	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	Unauthorized device monitors data stream between PMU and PDC and provides power system data to an unauthorized party.	x			x				
26	AL6	Application Layer	C37.118	Man-In-The-Middle	altered configuration or header message sent to upstream C37.118 client	Unauthorized device intercepts and alters the configuration frame from PMU to PDC.	x			x				
27	AL7	Application Layer	C37.118	Man-In-The-Middle	altered data stream sent to upstream C37.118 client	Unauthorized device intercepts and alters the data frame from PMU to PDC.	x			x				
28	AL8	Application Layer	C37.118	Fuzzing C37.118 protocol	Abnormal behavior or termination of the application on target device	Spoofed PMU (C37.118 server) sends malformed C37.118 data frames to PDC (C37.118 client)	x			x				
29	AL8	Application Layer	C37.119	Fuzzing C37.118 protocol	Abnormal behavior or termination of the application on target device	Spoofed PMU (C37.118 server) sends malformed C37.118 configuration frames to PDC (C37.118 client)	x			x				
30	AL9	Application Layer	C37.118	Unauthorized/rouge C37.118 client	Unauthorized C37.118 client starts/stops PMU data stream	Unauthorized C37.118 client sends command message to stop data stream from PMU to PDC	x			x				
31	N1	Network	Network Infrastructure	Flooding (DoS)	Delayed receipt of data stream by upstream C37.118 client	Unauthorized device degrades network performance by flooding the network with excessive data. Data frames sent from the PMU to the PDC are received late.	x			x				x
32	N2	Network	Network Infrastructure	Flooding (DoS)	Message exchange interupted between C37.118 client and server	Unauthorized device degrades network performance by flooding the network with excessive data. Data frames sent from the PMU to the PDC are interupted.	x			x				x
33	N3	Network	Network Infrastructure	ARP spoofing	Message exchange interupted between C37.118 client and server	Unauthorized device executes ARP spoofing attack causing data frames sent from the PMU to the PDC to be redirected to new target.	x			x				x
34	H1	Host	Network Interface (NIC)	DoS	Device unable to access network	Unauthorized device perfroms DOS attack on external interface of the Phasor Gateway.							x	
35	H1	Host	Network Interface (NIC)	DoS	Device unable to access network	Unauthorized device perfroms DOS attack on PDC.				x				
36	H1	Host	Network Interface (NIC)	DoS	Device unable to access network	Unauthorized device perfroms DOS attack onDFR/PMU.	x							
37	H2	Host	Network Interface (NIC)	DoS	Abnormal behavior or termination of the application	Unauthorized device perfroms DOS attack on PMU resulting in PMU malfunction	x							
38	H3	Host	Network Interface (NIC)	Port scanning	Open logical network interface to device discovered (e.g. ftp, telnet, http, etc.)	Unauthorized device perfroms port scan against DFR/PMU and gains access to DFR/PMU via open port.	x							
39	H3	Host	Network Interface (NIC)	Port scanning	Open logical network interface to device discovered (e.g. ftp, telnet, http, etc.)	Unauthorized device perfroms port scan on external interface of the Phasor Gateway and gains access to Phasor Gateway via open port.							x	
40	H3	Host	Network Interface (NIC)	Port scanning	Open logical network interface to device discovered (e.g. ftp, telnet, http, etc.)	Unauthorized device perfroms port scan against the PDC and gains access to PDC via open port.				x				
41	H4	Host	Firmware/OS	Malware	Device utilized to gain access to other protected network resources	Infected test device/laptop spreads malware to DFR/PMU. Malware then utilized to gain access to protected reources on the same network.	x							
42	H4	Host	Firmware/OS	Malware	Device utilized to gain access to other protected network resources	Malware passed to DFR/PMU via USI master	x		x					
43	H4	Host	Firmware/OS	Malware	Device utilized to gain access to other protected network resources	Infected portable USB storage device spreads malware to DFR/PMU. Malware then utilized to gain access to protected resources on the same network.	x							
44	H5	Host	Firmware/OS	Malware	Unexpected behavior of device	Rouge DFR/PMU application software inserted in supply chain to utility.	x							
45	H5	Host	Firmware/OS	Malware	Unexpected behavior of device	Rouge PDC application software inserted in supply chain to utility.					x			
46	H5	Host	Firmware/OS	Malware	Unexpected behavior of device	Rouge Phasor Gateway application software inserted in supply chain to utility.							x	
47	H6	Host	Configuration	configuration	Phasor data within data stream incorrect	Unauthorized party/system changes DFR/PMU configuration (e.g. CT and/or VT ratio's).	x							
48	H6	Host	Configuration	configuration	Phasor data within data stream incorrect	Unauthorized party/system changes DFR/PMU internal clock parameters	x							
49	H6	Host	Configuration	configuration	Phasor data within data stream incorrect	Unauthorized party/system disables DFR/PMU IRIG-B input.								
50	H6	Host	Configuration	configuration	Phasor data within data stream incorrect	Unauthorized party/system changes PDC internal clock parameters				x				
51	H7	Host	Configuration	configuration	Mismatch between header/configuration messages and phasor data within data stream	Unauthorized party/system changes DFR/PMU configuration (e.g. changing phasor identifiers).	x							
52	H8	Host	Database	uauthorized database access	Archieved/historical data modified	Unauthorized party/system gains access to Historian and modifies historical data						x		
53	H9	Host	Database	uauthorized database access	Archieved/historical data deleted	Unauthorized party/system gains access to Historian and deletes historical data						x		

C. Test Plan

Testing Goals

The overall goal of the testing outlined in this test plan is to validate the proof of concept for CAPMS functionality within the context of a utility operational environment. The team built the test plan around an attack scenario selected that represents an unauthorized change to a device configuration, a DFR/PMU unit in this specific case. Within this scenario, the project identified several variants to examine behavior under select conditions as follows:

- Variant 0 - This testing scenario executes the selected attack without CAPMS functionality enabled. This establishes a baseline for typical current monitoring and detection in a utility operational environment.
- Variant 1 - This variation of the testing installs a basic CAPMS policy and executes the selected attack. This demonstrates the basic behavior of the sensor logic and correlation logic within the CAPMS policies.
- Variant 2 - This variation of the test plan involves installing a more advanced CAPMS policy and executing the selected attack. This advanced policy supports complex decisions based on variations in the identified sensors (e.g. attacker physically present at the substation vs. remotely located).
- Variant 3 - This variation involves tuning exercises on the CAPMS policy utilized in variant 2 to optimize performance/effectiveness of the system. In this case, the tuning involved will account for authorized maintenance activities on the DFR/PMU unit. The tuning will take into consideration the subtle differences between an actual attack and authorized activities to accurately detect and react to the first while not inadvertently reacting to the latter.

Furthermore, specific goals during all of these testing variants are to:

- Demonstrate that the additional CAPMS functionality does not negatively impact the current or planned SCE CCS deployment
- Evaluate the CAPMS user interfaces
- Evaluate the dynamic behavior of CAPMS policies as sensor information and other inputs change
- Validate CAPMS ability to correlate inputs and make the proper decisions given the available sensors
- Identify and any unexpected behaviors of the CAPMS functionality that might inadvertently affect system functionality
- Understand how tuning can be utilized to minimize the risk of a false positive detection or reaction within the CAPMS functionality

Test Environment

The Southern California Edison facility consists of a setup depicted in Figure 13.

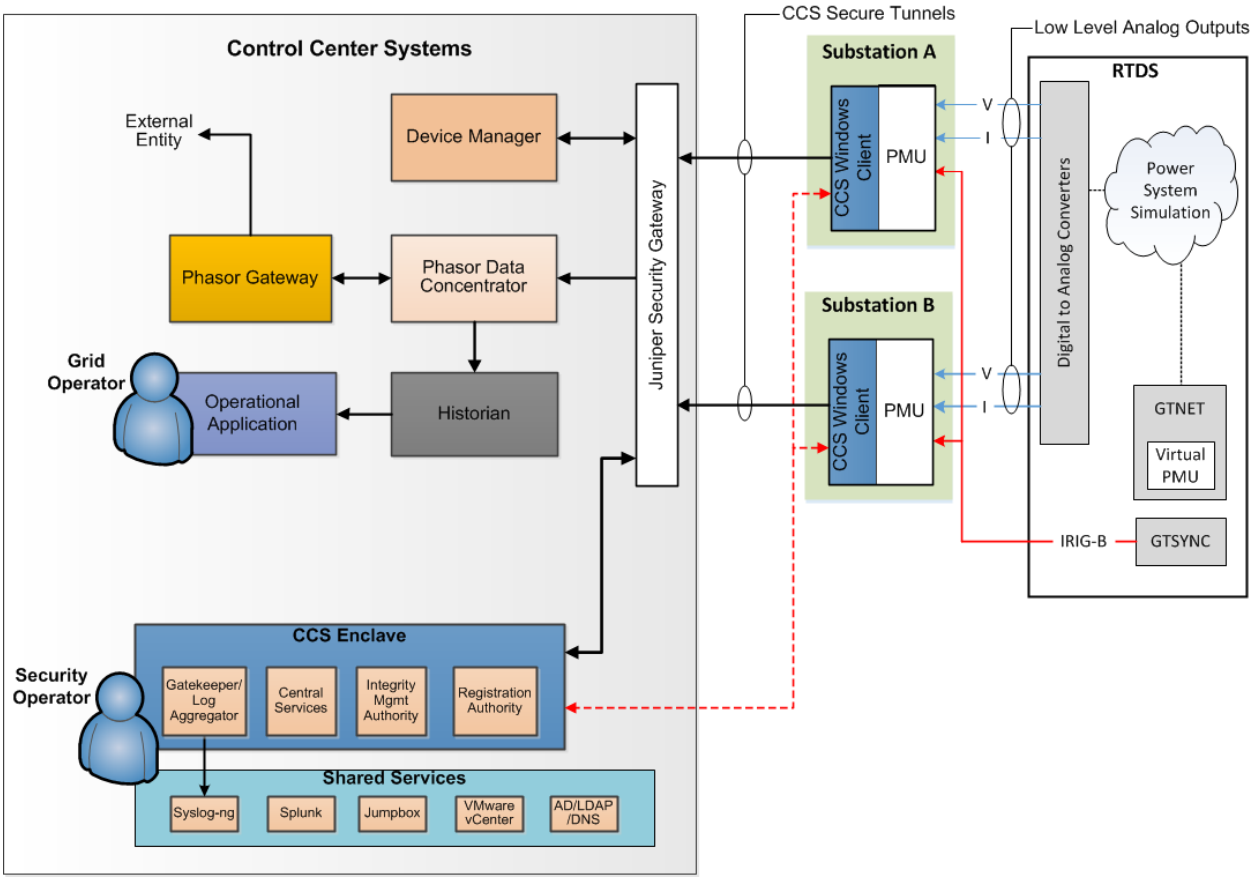

Figure 13: CAPMS ATO Network

This network contains three primary networks:

- Control Center Services – Contains the server-side components for PMU management and aggregation of data (eDNA, ePDC)
- CCS Enclave– Contains the CCS servers for security and policy management.
- Substation Network – This network contains two CCS-enabled Phasor Measurement Units (PMU) connected to the RTDS system.

Application-level communication occurs between each PMU and the Phasor Data Concentrator (ePDC) using the C37.118 protocol, a protocol for exchanging Phasor measurement values. The ePDC aggregates these measurements and sends them on to the eDNA Historian service using the C37.118 protocol. The eDNA Historian service provides the ability to graph and visualize the measurements which have been collected. For the purposes of the CAPMS grant, the eDNA Historian plays the role that an Energy Management System (EMS) or State Estimator (SA) would in a more complete system.

Communication between the PMUs and the ePDC is over a VPN connection provided by CCS, terminating at the edge of the CCS-BACKOFFICE network. Within the CCS-BACKOFFICE network, the CAPMS deep packet

inspection (DPI) capabilities perform inspection on the C37.118 protocol traffic, inspecting for data anomalies or significant events.

Detailed attack steps and scenarios may be disclosed under NDA. Contact SCE for more information.