



Strategies for complex organizations

Independent Report
Evaluation of the July 2015 Long Beach Network Outages:
Root Cause and Southern California Edison's Response

November 14, 2015

Prepared By:



Table of Contents

1. Executive Summary	5
1.1. Incident Background	5
1.2. Assessment Purpose, Scope and Approach	5
1.3. Summary of Root Cause Analysis	6
1.4. Key Findings and Recommendations	6
2. Introduction	8
2.1. Edison International and Southern California Edison Background	8
2.2. Incident Background	8
3. Assessment Purpose, Scope and Approach	9
3.1. Scope of Assessment	9
3.1.1. Root Cause/Technical Evaluation	9
3.1.2. Emergency Planning, Preparedness, and Response	10
3.2. Approach and Methodology	11
4. Relevant Network Concepts	14
4.1. Electric System Overview	14
4.2. Underground Network Overview	15
4.3. Network Protectors	16
4.4. Network Modeling and Maps	17
4.5. Network Monitoring	18
4.6. Network Customer Outage Counts	19
4.7. The SCE Long Beach Network	19
4.7.1. Overview and History	19
4.7.2. Reliability Performance	19
4.8. Comparing LB1 and LB2 to Other SCE Major Outages	20
5. Incident Responses	22
5.1. Long Beach 1	22
5.1.1. Customer Outages	23
5.2. Long Beach 2	24
5.2.1. Customer Outages	25
5.3. Manhole Fires: Response and Mitigation Plan	26
6. Root Cause Analysis	27

6.1.	Root Cause: Long Beach 1	27
6.2.	Root Cause Long Beach 2	27
6.3.	Sequence of Events	27
6.3.1.	Long Beach 1: Sequence of Events	28
6.3.2.	Long Beach 2	34
6.4.	Contributing Factors to the Incidents	34
7.	<i>Findings and Recommendations</i>	37
7.1.	Underground Network Operations (UNO)	37
7.1.1.	Overview	37
7.1.2.	Findings	38
7.1.3.	Recommendations	41
7.1.4.	Implementation Factors	42
7.2.	Emergency Planning and Preparedness (EPP)	43
7.2.1.	Overview	43
7.2.2.	Findings	43
7.2.3.	Recommendations	46
7.2.4.	Implementation Factors	49
7.3.	Incident Response and Management (IRM)	49
7.3.1.	Overview	49
7.3.2.	Findings	50
7.3.3.	Recommendations	56
7.3.4.	Implementation Factors	58
7.4.	Communications (COM)	59
7.4.1.	Overview	59
7.4.2.	Findings	60
7.4.3.	Recommendations	64
7.4.4.	Implementation Factors	67
7.5.	Information Technology and Operational Technology (ITOT)	67
7.5.1.	Overview	67
7.5.2.	Findings	68
7.5.1.	Recommendations	71
7.5.2.	Implementation Factors	73
7.6.	Corporate Culture (CC)	73

7.6.1.	Overview	73
7.6.2.	Findings	74
7.6.3.	Recommendations	77
7.6.4.	Implementation Factors	78
8.	Appendices	i
8.1.	Appendix A: Detailed Response Timeline	ii
8.1.1.	Long Beach 1	ii
8.1.2.	Long Beach 2	ix
8.2.	Appendix B: Glossary	xii
8.4.	Appendix C: Interviewee Roles	xvi
8.4.1.	SCE Interviews by Position	xvi
8.4.2.	External Stakeholders	xvi
8.5.	Appendix D: Davies Consulting Qualifications	xviii
8.6.	Appendix E: Network Maps	xix

List of Tables

<i>Table 1: Historical Reliability Performance LB Network versus SCE system (2006-2015)</i>	20
<i>Table 2: Event Comparison</i>	20
<i>Table 3: Organization of Findings and Recommendations</i>	37
<i>Table 4: Value Key</i>	37
<i>Table 5: Ease of Implementation</i>	37
<i>Table 6: Recommended Timing of Implementation</i>	37
<i>Table 7: Underground Network Operations Recommendations</i>	42
<i>Table 8: Emergency Planning and Preparedness Recommendations</i>	49
<i>Table 9: Incident Response and Management Recommendations</i>	58
<i>Table 10: Communications Recommendations</i>	67
<i>Table 11: Information Technology and Operational Technology Recommendations</i>	73
<i>Table 12: Corporate Culture Recommendations</i>	78

List of Figures

<i>Figure 1: Approach and Methodology.....</i>	<i>11</i>
<i>Figure 2: The Electric Power System</i>	<i>14</i>
<i>Figure 3: Secondary Overlay in Network</i>	<i>15</i>
<i>Figure 4: Network Protectors.....</i>	<i>16</i>
<i>Figure 5: Monitoring Data Example</i>	<i>18</i>
<i>Figure 6: Long Beach 1 Customer Outages by Day and Time (Source: AMI Data).....</i>	<i>24</i>
<i>Figure 7: Long Beach 2 Customer Outages by Day and Time (Source: AMI Data).....</i>	<i>26</i>
<i>Figure 8: SCE Command and Control Nodes</i>	<i>54</i>
<i>Figure 9: OMS Example.....</i>	<i>69</i>
<i>Figure 10: Screenshot of LPA App</i>	<i></i>
<i>Figure 11: Network Map Example</i>	<i>xix</i>
<i>Figure 12: Status of the Long Beach Network (Northern and Southern Portions) Prior to July 15 Incident .</i>	<i>xix</i>
<i>Figure 13: Status of Network Prior to July 15 Incident According to 2008 and 2012 Long Beach Network Protector Map</i>	<i>xix</i>
<i>Figure 14: Float Circuit Opened at 3:07 p.m.</i>	<i>xix</i>
<i>Figure 15: STEAM Circuit Relayed at 3:32 p.m.</i>	<i>xix</i>
<i>Figure 16: CARGO Circuit De-Energized at 4:22 p.m.....</i>	<i>xix</i>
<i>Figure 17: OCEAN Circuit Relayed at 6:20 p.m.</i>	<i>xix</i>
<i>Figure 18: SCE De-Energizes CHESTNUT, LOOP, TRIBUNE Circuits at 6:21 p.m.</i>	<i>xix</i>
<i>Figure 19: North Network After 6:21 p.m., July 15</i>	<i>xix</i>

1. Executive Summary

1.1. Incident Background

On July 15, 2015, at approximately 3:00 p.m., Southern California Edison (SCE) experienced a network failure on its Long Beach underground secondary network. Based on the completion of an Incident Complexity Analysis, SCE declared Level 2 emergency. At approximately 1:00 p.m. on July 16, outages peaked at 28,895. SCE responded by activating its Electrical Services – Incident Management Team (ES-IMT), communicating the status of the response through the release of more than 50 tweets, staffing Long Beach City’s Emergency Operations Center (EOC) with an executive, providing generator power to customers experiencing outages, and establishing or supporting distribution centers at three different locations. More than 95% of the customers who were out at peak were restored by the evening of July 17, and all customers were restored by 3:34 p.m. on July 20.

On July 30, 10 days after restoration following the July 15 incident, SCE experienced a second failure of its Long Beach network. This failure began at approximately 4:00 p.m., resulting in a peak of approximately 17,500 customer outages. Based on the completion of an Incident Complexity Analysis, SCE declared a Level 3 emergency for the second outage and activated not only the ES-IMT, but also an Incident Support Team (IST). In addition, the Company operated distribution centers at two sites, supplied generator power to customers experiencing outages, and provided personnel to support Long Beach City’s EOC. By August 1, all except for three customers had power restored either through the grid or generators. The remaining three customers were reconnected on August 2 at 5:33 a.m. One additional customer experienced a related outage until August 3 after being temporarily reconnected on July 31 for a period of approximately 22 hours.

In response to the incidents, SCE leadership sought to identify how it could prevent similar occurrences in the future. SCE retained Davies Consulting LLC, a leading management consulting firm with extensive experience in utility emergency response and network operations throughout North America, to conduct an independent assessment. The timeframe of the review was August through October 2015.

1.2. Assessment Purpose, Scope and Approach

The objective of the review was to evaluate the Company’s preparation for and response to the network outages in order to identify potential areas of improvement. The scope included: 1) Determining the root causes of the network failures; and 2) Analyzing key aspects of the subsequent response efforts, such as activation, mobilization, situational awareness, communications, logistics, estimated restoration time, and restoration strategy.

The approach to both the technical root cause analysis and the response assessment involved six key tasks:

1. Mobilize the Project – Confirmed project scope, roles and responsibilities, approach, timeline, milestones and interviewees.
2. Obtain Relevant Data and Documents – Gathered information deemed necessary to conduct the assessment, such as plans, process and network maps, after action reports, etc. (nearly 200 documents)
3. Review Documentation for Each Incident – Analyzed technical data and documents to evaluate SCE's preparedness for and plans implemented during the two separate responses.
4. Conduct Interviews – Held more than 70 interviews with internal and external stakeholders including: incident response personnel, executives, operators, engineers, managers, and field personnel. The purpose of the interviews was to gain a deeper understanding of the Long Beach network design and operations, and how SCE responded to and communicated during the incidents.
5. Develop Preliminary Findings and Recommendations – Identified and documented opportunities for improvement in network maintenance and operations practices, and response processes, procedures, organizational structure, and plans.
6. Summarize Findings – Drafted report of analysis, findings and recommendations.

1.3. Summary of Root Cause Analysis

A primary splice failure on one of the network circuits triggered a series of events that ultimately forced the network to be shut down on July 15. The root causes of the first Long Beach network outage were: SCE operated the Long Beach underground secondary network outside of its optimal design state; did not have processes in place to actively monitor and track equipment that was being operated abnormally; and made operating decisions that resulted in the network shut-down.

The root cause of the July 30 network shutdown was damage sustained during the operation and restoration of the network during the July 15 incident.

1.4. Key Findings and Recommendations

Overall Findings

Over the past 10 years, the reliability of the Long Beach underground secondary network has been significantly better than that of the rest of the SCE system. Notably, the Long Beach network has not had a significant failure for more than 50 years. The number of customers affected during the Long Beach failures was small when compared to other "major" outages in the past; however the restoration was more complex and significant than these numbers suggest due to the nature of the underground system. Following the July 15 network failure, SCE restored all of its customers within five days.

Following the second incident, SCE conducted another efficient response, restoring power to all customers in three days.

The review indicated numerous opportunities for SCE to improve its preparedness for and response to similar incidents. Opportunities for improvement include: enhanced emergency management plans; further implementation and adoption of ICS; enhanced situational awareness; deeper understanding of networks, including the complexities associated with responding to and restoring network failures; expanded communications processes, including development of a comprehensive communications plan that addresses all hazards; updates to the Advanced Metering Infrastructure (AMI) to enable access to better information during large-scale outages; and focused leadership messaging on the importance of preparedness and response.

Key Recommendations

This report details 35 recommendations, across six areas: Underground Network Operations (UNO); Emergency Planning and Preparedness (EPP); Incident Response and Management (IRM); Communications (COM); Information Technology and Operational Technology (ITOT); and Corporate Culture (CC). Key recommendations are:

- Develop and implement a more extensive training and certification program for network operations personnel;
- Develop a network model;
- Deploy ICS below the Region/District Manager level;
- Assign individuals with broad experience to incident leadership positions;
- Create a framework for emergency response plans;
- Develop an underground network restoration process and annex plan;
- Develop an incident communications plan, plan modules, and associated processes to address hazards, threats, and risks;
- Expand the One Voice process to account for different stakeholder needs;
- Formalize the restoration information sharing and vetting process and implement a database/web portal; and
- Update the AMI capabilities for all of SCE's service territory.

2. Introduction

2.1. *Edison International and Southern California Edison Background*

Southern California Edison (SCE) is one of the largest electric utilities in the United States, providing electric service to nearly 15 million people over a 50,000 square mile service territory in central, coastal, and southern California. SCE, which is owned by Edison International, has provided electric service for more than 125 years. Today, SCE serves 180 cities (Long Beach is the largest) and 15 counties. To provide this level of service, SCE maintains grid assets valued at more than \$20 billion, including 1.4 million power poles, 700,000 transformers, and 103,000 miles of distribution and transmission lines.

2.2. *Incident Background*

In July 2015, SCE experienced two extended power outages on the underground network serving the city of Long Beach, California. According to SCE staff familiar with the network, these were the first major Long Beach network disruptions since the 1950s. On July 15, SCE's Long Beach underground network began to experience equipment failures, and was shut down proactively. As a result of the shutdown, approximately 3,800 metered customers¹ (all supplied by the underground network), experienced electric service interruptions. During the four-day restoration that followed, nearly 25,100² discrete additional customers (supplied by overhead distribution circuits), experienced electric service interruptions. SCE's response to this incident was challenged by the media and the City of Long Beach for the length of the outages and for SCE's lack of communication.

Fifteen days later, on July 30, the Long Beach underground network experienced equipment failures again and was quickly shut down a second time. A majority of the underground network was restored that same evening. SCE restored service to all affected customers within three days. This second incident raised additional concerns from the public and Long Beach City officials related to SCE's maintenance of its network systems and the Company's response to these outages. The California Public Utilities Commission (CPUC) is investigating the outages.

¹ In the utility industry, the term meter often means a customer. For example, an apartment building with one meter is one "customer" despite the fact that many individuals reside in that building. A single family home would also be considered a "customer" whether it houses one or multiple individual residents.

² All customer counts which we use for the Long Beach outage are derived from SCE's AMI data. This data is not reliably available in real time to SCE personnel during outages. Therefore, AMI data available *ex post facto* may differ from numbers available to SCE during the outage.

3. Assessment Purpose, Scope and Approach

In response to the incidents, SCE sought to identify how it could prevent similar future occurrences. SCE retained Davies Consulting LLC, a leading management consulting firm with extensive experience in utility emergency response throughout North America, to conduct an independent assessment. Appendix D provides a more detailed overview of Davies Consulting's experience and qualifications³. The timeframe of the review was August through October 2015.

The overall scope of the assessment included: 1) Determining the root causes of the July 15 (hereinafter "Long Beach 1" or "LB1") and July 30 (hereinafter "Long Beach 2" or "LB2") outages; and 2) Analyzing key aspects of the subsequent response efforts, such as activation, mobilization, situational awareness, communications, logistics, estimated restoration time (ERT), and restoration strategy. The objective of the detailed review was to evaluate the Company's preparation for and response to the incidents in order to identify areas for potential improvement. Additionally, the areas of improvement identified were focused on enhancing SCE's performance and meeting or exceeding the expectations of customers and stakeholders.

3.1. *Scope of Assessment*

3.1.1. Root Cause/Technical Evaluation

To determine the root cause of the two incidents, Davies Consulting focused on evaluating the design of the Long Beach network, the state of the network at the time of the incidents, and the technical failures (e.g., in cables, network protectors) that contributed to the occurrence of the incidents. The technical evaluation of the two incidents addressed questions including, but was not limited to:

- How are network operating guidelines implemented and executed on a daily basis?
- What was the cycle for inspection and maintenance of critical network equipment?
- What was the status of the network equipment leading to July 15, specifically related to network protectors and circuits supplying the network?
- Was the network operated within its design state at the time of the outage?
- Was monitoring equipment used to determine the status of the network and identify any anomalies?
- Did the Company have and use a network primary and secondary model to evaluate the impact of different network equipment failure scenarios?

³ Davies Consulting conducted the review of SCE's response to November 2011 wind storm and supported several exercises and process improvement efforts related to emergency management.

- What was the timeline of specific equipment failures that led to the network shutdown?
- What were the causal relationships among the different events during the sequence that led to the shutdown?

3.1.2. Emergency Planning, Preparedness, and Response

In evaluating SCE's emergency planning and preparedness, Davies Consulting concentrated SCE's emergency plans, command structure, roles, procedures, and exercises and training implemented or conducted in advance of these two network incidents. In assessing the response itself, Davies Consulting evaluated the incident complexity analysis, the Company's use and activation of its response organization, coordination among and between functional groups, incident leadership's situational awareness during the outages, communications efforts, the effectiveness of restoration plans, and restoration strategy execution. The response assessment focused on each of the incidents as separate events and included, but was not limited to, the following areas.

- *Emergency preparedness* – How did the Business Resiliency and Transmission and Distribution (T&D) Operating Units prepare for an underground network failure?
- *Training and exercises* – What is the training/exercises plan? What has been conducted?
- *Emergency response plans and processes* – Do comprehensive plans and processes exist to support the restoration of a network incident and all supporting functions? Were plans followed?
- *Situational awareness* – was the complexity analysis designed to create situational awareness in a scenario of this type?
- *Use of Incident Command System* – How did the Company utilize the Incident Command System? Who had responsibility for managing the entire incident and who directed operational restoration? When was the emergency operations center opened and when did restoration resources begin to be committed? How well did SCE obtain and allocate underground network restoration expertise?
- *Emergency response (second roles)* – Are they defined and used effectively? Were the emergency roles assigned, evaluated and trained? Damage assessment – How was damage assessed and how was that information used to develop the restoration strategy and estimated restoration time (ERT)?
- *Restoration priorities* – Were they clearly defined, understood, and followed? How was the restoration sequence executed and how was the problem isolated to protect the rest of the network?
- *Logistics* – How well were logistics managed in support of the restoration?

- *Demobilization* – How was demobilization conducted? How efficient was the process?
- *Communications strategy* – Was a communication strategy developed and implemented? Was information effectively and efficiently disseminated? Communications channels – How effective was social media communication, including Twitter, Facebook, Company website, etc.? How did the Company ensure “One Voice” communication throughout the restoration effort?⁴ Was there a process for ensuring that all of the communications channels had the same information? How well was information communicated internally?
- *Estimated restoration times (ERTs)* – How were they determined? How many times did the ERTs change and how often were they refined? Was there a process to track and update ERTs?

3.2. Approach and Methodology

The approach to both the technical root cause and the response assessments involved six tasks, which are described in detail below.

Figure 1: Approach and Methodology



Mobilize the Project

Davies Consulting team members met with SCE staff to confirm:

- Project scope and objectives;
- Team member roles and responsibilities;
- Davies Consulting’s detailed approach for each task;
- Project work plan timeline, and milestones;
- Interviewees; and
- Interim and final deliverables.

Obtain Relevant Data and Documents

Davies Consulting, with the full cooperation of SCE, gathered information deemed necessary to conduct the root causes analysis and after action assessment. The data requested included response plans, policies, procedures, schematics, outage and other system data, reports and any other written documentation related to the operation of

⁴ One Voice communications is the process by which the company ensures the consistent use of facts, figures, and messaging in all employee and external stakeholder communications.

the underground network and emergency preparedness and response. In all, Davies Consulting gathered close to 200 documents and datasets.

Review Documentation for Each Incident

During this task, Davies Consulting team members reviewed the technical data and documents provided by SCE to analyze the Company's preparedness for and plans implemented during the two separate responses. The review and analysis focused on:

- Overall comprehensiveness/consistency of the plans, including general content and the ability of SCE to respond adequately to a network incident (based on the content of the plans);
- The state of the network system, including maintenance conducted;
- Network practices and procedures;
- Mobilization and network incident levels/categories;
- Organizational structure as it relates to ICS principles, specifically role and responsibility descriptions, span of control, scalability, and terminology used;
- Availability and use of role checklists;
- Interaction with municipal, state, and regional entities and coordination between SCE's various external- and internal-facing communications groups; and
- Integration of communications into the overall event response process.

Examples of the documents reviewed include:

- Outage and communications timelines;
- After action reports;
- Company Twitter posts;
- Long Beach underground network primary and secondary maps;
- AMI data for the customers fed from the Long Beach network prior and throughout the two events;
- Network design standards; and
- Network operating and maintenance procedures and manuals.

Conduct Interviews

Following the data and document review, the Davies Consulting team conducted more than 70 interviews with incident response personnel, executives, operators, engineers, managers, field personnel, and external stakeholders. The interviews included both people who responded to the incidents and individuals who may have influenced the condition of the underground network leading up to LB1 and LB2. The internal interviews covered representatives from all functions involved in the two responses, as well as those responsible for operations and maintenance of the Long Beach network on a day-to-day basis. These interviewees represented all levels of staff from front line employees and crew supervisors to the SCE senior management team.

External interviewees included City of Long Beach elected officials, local emergency managers, first responders, a chamber of commerce leader, and a business improvement district chief executive officer. A complete list of the roles of those interviewed is included in Appendix C to this report. All interviews were conducted on a confidential basis.

Develop and Review Preliminary Findings and Recommendations

The objective of this task was to pinpoint areas where improvement would strengthen the Long Beach network and future response to a network incident. Drawing on information from the interviews and analysis of available documentation, Davies Consulting identified opportunities for improvement in network maintenance and operations practices, response processes and procedures, organizational structure, and emergency response plans. During the assessment, Davies Consulting periodically reviewed its preliminary findings and conclusions with SCE executives, with the objectives of clarifying information and providing progress updates.

Draft Report of Findings and Recommendations

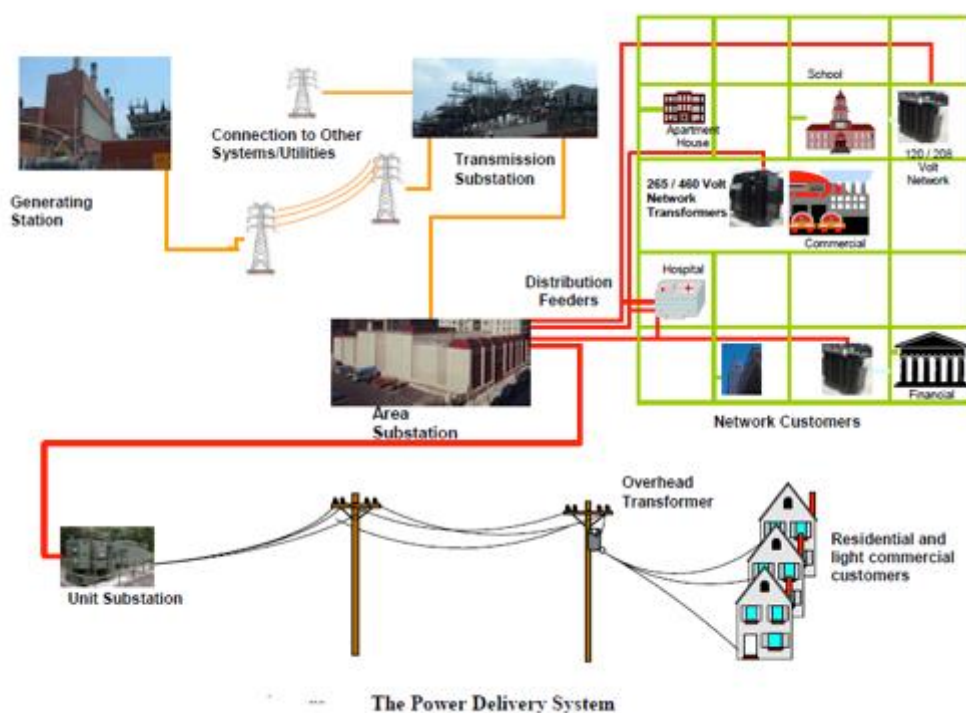
Finally, Davies Consulting summarized its findings and recommendations into a written report. The report includes 36 recommendations across six areas (Underground Network Operations, Emergency Planning and Preparedness, Incident Response and Management, Communications; Information Technology and Operational Technology; and Corporate Culture) along with supporting analysis. For consideration in implementation planning, Davies Consulting assessed the relative value, ease of implementation, and suggested timing of implementation of each recommendation.

4. Relevant Network Concepts

4.1. Electric System Overview

As depicted in Figure 2, the electric system is comprised of generation, transmission, and distribution systems. Generation plants serving customers convert energy (from natural gas, hydro, nuclear, or renewable sources) into electric power at high voltages. Transmission lines then deliver that electricity to localized distribution substations. The voltage is reduced at the substations so that primary distribution voltage circuits can distribute the power to customers through the distribution system. Distribution systems, which serve as a connection between the substation and the end-user, serve customers in geographic areas through either overhead or underground primary circuits. They employ transformers to convert the higher distribution voltage to a voltage low enough to be usable by the customer. Some distribution systems include underground secondary networks, which are typically found in a more densely populated areas.

Figure 2: The Electric Power System⁵



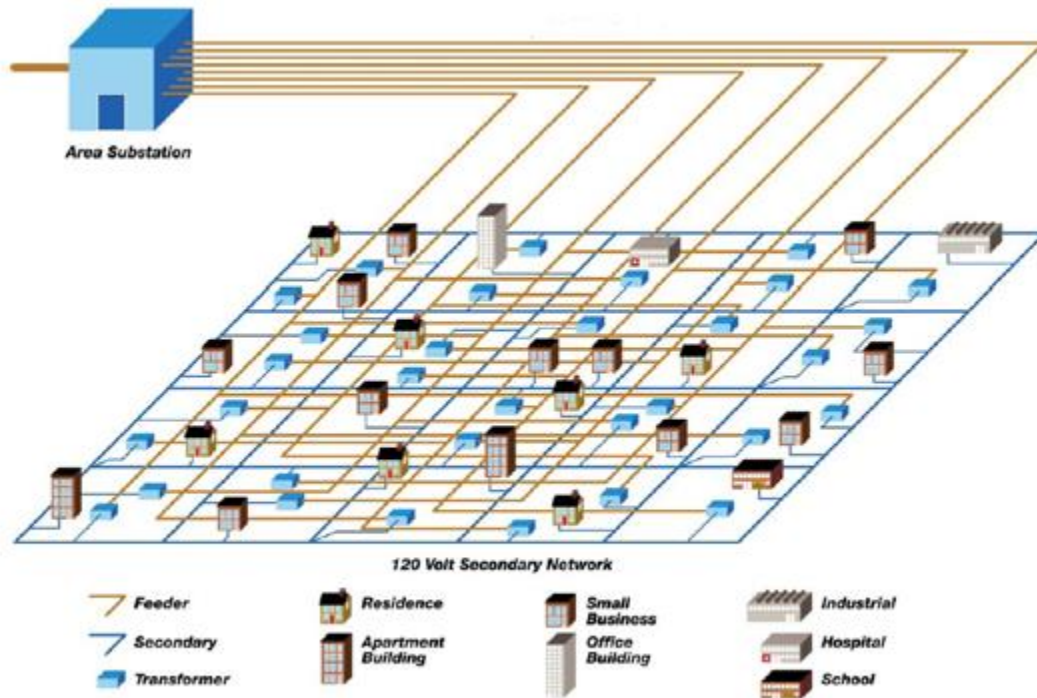
⁵ Overview of Con Edison System and LIC Network, at <http://www.coned.com/messages/licreport/overview.pdf> accessed on October 19, 2015.

4.2. Underground Network Overview

Underground networks are used by electric utilities across the country to supply high density geographic areas with very reliable and safe energy. The supply is generally reliable because the systems are designed to include redundant facilities, meaning that any single equipment failure should not result in an outage to customers.

In an underground secondary network system, primary circuits serve a geographic area by delivering electricity to underground transformers, which lower the voltage to residential or commercial levels. The underground secondary grid typically consists of multiple, low-voltage cables connected in manholes and service boxes. It provides the utility with redundant paths for supplying customers with power (e.g., when a piece of equipment is out of service, another can pick up and complete delivery). The redundancy provided by the combination of the primary and secondary voltages serving a specific geographic area increases the overall reliability of the system. Typically, the primary and secondary systems are inextricably linked and any action on one piece of equipment or segment affects the others.

Figure 3: Secondary Overlay in Network⁶



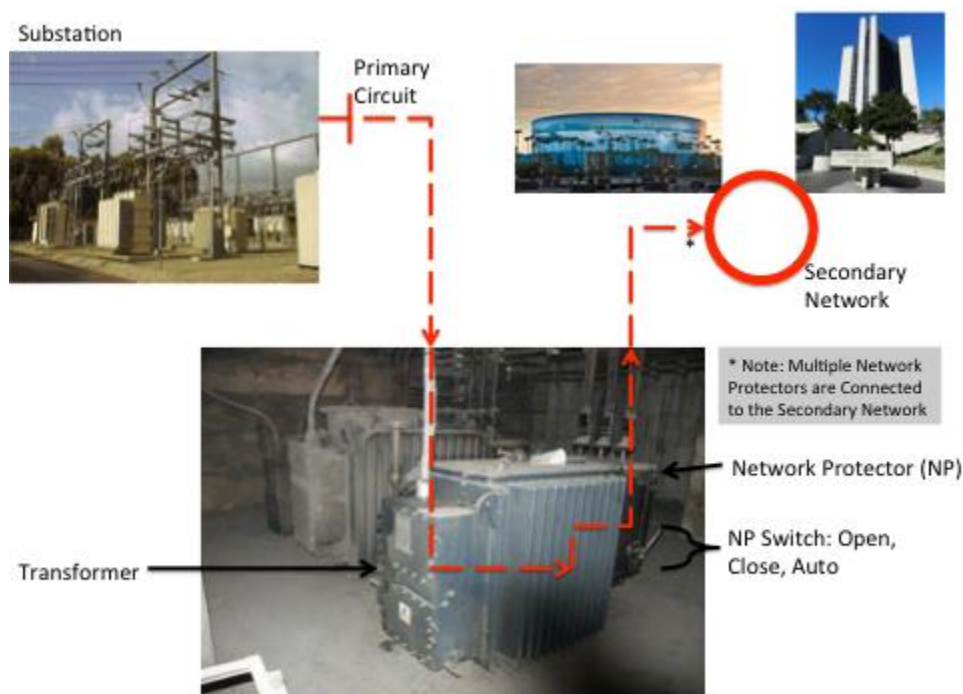
⁶ Ibid.

4.3. Network Protectors

A network protector is an assembly composed of a circuit breaker and its complete control equipment for: (1) automatically disconnecting a transformer from a secondary network distribution system in response to predetermined electrical conditions on the primary feeder or transformer and (2) connecting a transformer to a secondary network through manual or automatic control responsive to predetermined electrical conditions on the feeder and the secondary network distribution system.

The network protector is usually arranged to automatically connect its associated transformer to the secondary network distribution system when conditions are such that the transformer, when connected, will supply power to the secondary network distribution system and to automatically disconnect the transformer from the network when power flows from the secondary network distribution system to the transformer (from IEEE C57.12.44-2000).⁷ Figure 4 depicts the position of the network protectors in relation to the circuits, transformers and network.

Figure 4: Network Protectors



⁷ National Renewable Energy Laboratory, Secondary Network Distribution Systems Background and Issues Related to the Interconnection of Distributed Resources, NREL/TP-560-38079. July 2005.

4.4. Network Modeling and Maps

Maps that accurately depict actual field conditions are necessary for the safe and reliable operation of a distribution system, both overhead and underground. In underground network systems, where equipment cannot be verified easily in the field and conditions can deteriorate quickly in the time it takes to investigate, having accurate maps is particularly vital. As compared to overhead circuits, it is more difficult to inspect, visually, the underground network. Also, it is not as easy to predict the flow of electricity as one can with an overhead, radial system, where electricity flows in one direction.

Underground network maps visually depict the network, providing a record of the status and type of equipment on it (i.e., size and position of cables, transformers, network protectors, circuits). They provide network operators with essential information on the location and status of cables, vaults, manholes, network protectors, and the primary circuits that are supplying the network protectors. All of this information is overlaid on a geographic map that shows the position of the network relative to buildings and streets. Based on this information, network models mathematically simulate the predicted flow of electricity on the primary and secondary portions of the network.

Figure 11⁸ shows the level of detail typically included on a network map, such as the manufacturer of network protectors, the size of cables on a specific run of conduit, the underground space through which the cable runs, and whether the network protector has remote monitoring capabilities. It is important to have accurate data on maps so that field workers, system operators, and the engineers who model the system can operate the system as efficiently as possible.

As mentioned above, a network model is a mathematical depiction of the flow of electricity on the primary and secondary networks. Because a network is designed to continually supply any connected load, regardless of the conditions within the network, a network model that allows engineers and operators to quickly understand what is electrically occurring within the network is needed in order to inform them of the consequences of their actions. Typically, network models are created and maintained by utility engineers based on secondary network maps and primary circuit maps. These models are used by the system operators to mathematically predict the effect of their switching operations on the network and the impact of equipment being in an abnormal state as compared to the optimal state. Network models are used by many (but not all) utilities that operate underground networks.

⁸ Figures containing the Long Beach underground secondary network system are attached in Appendix E, but in order to protect critical infrastructure and sensitive information, this appendix will not be available publicly.

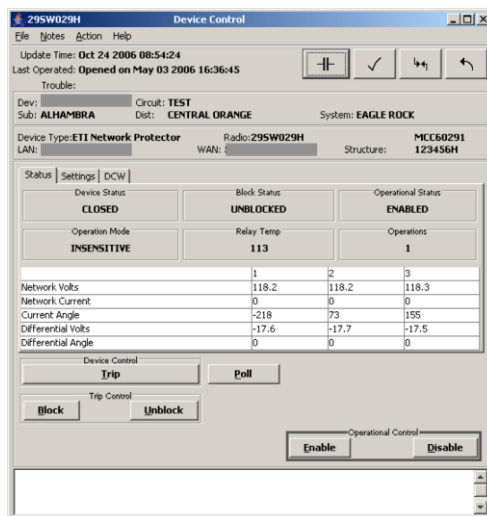
When systems are in their design state (frequently N-0, which is read as N minus zero), network models are less important, since the system is designed with a factor of redundancy or safety. That is, the network is designed to continue providing power safely and reliably even with the loss of one critical piece of equipment (called N-1 or the first contingency). This is similar to other engineering systems (e.g., aviation, mechanical), which are designed to be more robust than minimally necessary.

For a network that is designed as a first contingency network, when it moves from an N-0 to N-1, the network risks becoming unreliable with another failure (a.k.a., contingency). Therefore, when the network is close to its maximum operating condition, specifically when it is operating at N-1, it is important to simulate the impact of each intended action. Network models enable operations personnel to predict the “next worst case scenario” when the system operates with critical pieces of equipment in abnormal states. This helps operators avoid making decisions that further strain the network.

4.5. Network Monitoring

Network monitors provide real-time, near-real-time, or historical information on the status of a network. Network monitoring can include Advanced Metering Infrastructure (AMI), network protector monitoring, and circuit monitoring. AMI and circuit monitoring are used to provide information about both circuits and networks, while network protector monitoring is used primarily on the underground secondary network grid. The extensiveness of network monitoring capabilities and availability of monitoring data to support grid operations varies across the industry. Figure 5 shows an example of information available via network monitoring.

Figure 5: Monitoring Data Example



Where available, network protector monitoring provides information on the status of the network protectors, including but not limited to voltage, current, power, and last

relay. AMI monitors the quality and supply of electricity at the customer delivery point and can be used to provide information on the customer's usage of electricity, usually in hourly increments, as well as the quality of the electricity, normally measured in volts. Due to the design of the AMI communication protocols, this information typically is not available in real-time. Rather, it is often communicated in 24-hour increments, as is done at SCE.

4.6. Network Customer Outage Counts

Outage Management Systems (OMS) are designed to provide a reasonably accurate customer outage count on the overhead radial system. In underground secondary networks, however, the inherent redundancy of the system and the multiple paths by which a customer can receive power means that OMS cannot provide an accurate customer count during an outage. AMI systems can provide accurate customer counts during minor interruptions, but in significant outage events affecting a larger number of customers, the AMI design does not provide for a real-time "pinging" of meters to identify which customers are out of service. These limitations make it difficult to provide an accurate customer outage count during network outages. These limitations are discussed in greater detail in Section 7.6.

4.7. The SCE Long Beach Network

4.7.1. Overview and History

The downtown Long Beach underground secondary network is fed by 9kV and 12kV primary circuits, and supplies service to approximately 3,800 customers. The geographic area covered by the network is slightly less than one square mile of SCE's 50,000 square mile service territory. The primary circuits supplying the underground network also supply overhead customers.

Similar to other networks operated by utilities, SCE's Long Beach network system was built with contingencies through redundant equipment, providing high reliability to customers connected to it. The large number of components and design redundancy, including primary network circuits and secondary mains connecting the network, add to the complexity of SCE's network. The SCE Long Beach network appears to have been designed as an N-1 configuration, which means that a single circuit and its associated network protectors can be out of service and the system should operate at peak load without experiencing any service quality problems.

4.7.2. Reliability Performance

Over the past 10 years, the reliability performance of the Long Beach underground secondary network, as measured by SAIFI and SAIDI, was significantly better than that of the rest of the SCE system (i.e., overhead, radial system). The reliability associated with the Long Beach network shown in Table 1 below includes outages on the overhead sections of the primary circuits that feed the network along with the outages on the

network section. The actual number of outages experienced by the customers served directly by the network is not available; but it is likely that prior to 2015, number is insignificant, since the network had not had a major failure since the 1950s. The two events in July 2015 contributed to a significant number of customer interruptions and minutes of interruption, resulting in poor reliability performance of the network in 2015⁹.

Table 1: Historical Reliability Performance LB Network versus SCE system (2006-2015)¹⁰

SAIDI	2006	2007	2008	2009	2010	2011	2012	2013	2014	2015
Long Beach Network	0.59	1.03	83.27	4.77	38.24	55.31	63.20	1.54	6.33	6061.72
SCE	141.96	151.32	118.78	105.80	140.92	232.39	108.13	102.61	112.25	84.02
SCE Less Long Beach Network	141.96	151.32	118.73	105.79	140.90	232.36	108.09	102.61	112.24	79.96
SAIFI	2006	2007	2008	2009	2010	2011	2012	2013	2014	2015
Long Beach Network	0.03	0.00	0.42	0.10	0.42	0.16	0.47	0.00	0.03	3.63
SCE	1.04	1.10	1.06	0.90	1.05	1.04	0.89	0.91	0.97	0.68
SCE Less Long Beach Network	1.04	1.10	1.06	0.90	1.05	1.04	0.89	0.91	0.97	0.68

4.8. Comparing LB1 and LB2 to Other SCE Major Outages

Table 2 below lists SCE's major outages in the last 10 years, including total affected customers and total days of duration. Notably, this data indicates that SCE experienced no major outages during 2012 and 2013. Of particular note when comparing restoration durations:

- The number of customers affected during the Long Beach failures was small compared to other major outages in the past 10 years; and
- Underground network restorations tend to take longer to complete than similar and some larger overhead events. This is partially caused by limited visibility into underground equipment, confined working space, etc.

Table 2: Event Comparison¹¹

Major SCE Incidents	Date	Total Customers Affected	Total Days
Rain/Wind/Lightning	10/16/2005	251,808	4
Rain/Wind/Lightning	12/31/2005	596,261	9
Heat (Cat 3)	07/13/2006	1,146,824	14
Heat	08/30/2007	644,603	9

⁹ 2015 reliability data is for partial year (through October 19, 2015).

¹⁰ The network reliability numbers include outages related to the overhead portions of feeders that serve the Long Beach underground secondary network. The reliability of the network itself was not available. The numbers for 2015 are year to date as of October 19, 2015.

¹¹ LA County OEM EMERGENCY RESTORATION ACTIONS, December 22, 2011 and supplemental data from SCE

Major SCE Incidents	Date	Total Customers Affected	Total Days
Wind	10/21/2007	599,411	7
Rain/Wind/Lightning	12/15/2008	232,158	12
Rain/Wind/Lightning	06/03/2009	254,627	3
Rain/Wind/Lightning	09/19/2009	262,372	4
Rain/Wind/Lightning	01/17/2010	676,578	9
Rain/Wind/Lightning	10/18/2010	344,764	3
Rain/Wind/Lightning	12/19/2010	498,820	7
Rain/Wind/Lightning	03/20/2011	333,541	4
November 30 Windstorm	11/30/2011	433,945	7
Rain/Lightning	2/28/2014	321,971	3
Wind	4/29/2014	221,310	4
Lightning	7/15/2015	219,522	5
Long Beach Network Failure 1	7/15/2015	28,895	5
Long Beach Network Failure 2	7/30/2015	17,532	3
Rain/Heat	9/8/2015	239,193	3

5. Incident Responses

This section describes, separately, the order of events that occurred immediately before each of the outages and throughout the subsequent responses.¹²

5.1. Long Beach 1

The July 15 incident was first identified by the SCE control center at 3:07 p.m., when the FLOAT circuit opened automatically via relay operation¹³ de-energizing eight network protectors. After two additional circuits supplying the Long Beach network failed and the fire at manhole M5133092 was reported,¹⁴ Grid Operations notified the on-call Storm Manager of the event. After being notified by the Watch Office (the entity responsible for monitoring incidents across the enterprise) of the incident around 5:00 p.m., the on-call Business Resiliency Duty Manager completed an Incident Complexity Analysis by 5:20 p.m. The analysis determined that the incident was a level 2, indicating an “event with little potential for severe harm but which can escalate rapidly if not managed properly.”

The response organization guidance for a level 2 is to rely on manager’s discretion for activation of the IMT/IST/EOC structure. After a series of discussions between the Duty Manager, the Storm Manager, and the acting Grid Operations Director, a consensus decision was reached to have the Storm Manager assume the role of Incident Commander (IC) and monitor the situation remotely. The IC assigned operational responsibility to the Long Beach District Manager. The Duty Manager activated a Liaison to the Long Beach Police Department Operations Center (DOC). The Duty Manager also activated a Public Information Officer (PIO) who operated remotely. In the meantime, in the early evening of July 15, the City of Long Beach activated the Police District Operations Center (DOC).¹⁵ At approximately 6:00 p.m. on July 15, SCE’s Agency Representatives (also known as “AREPs”) arrived at the City’s Police DOC to provide a liaison between SCE and Long Beach.

By the morning of July 16, power had not been restored and as the response lagged, the City of Long Beach Mayor tweeted his frustration with SCE’s approach and

¹² Of note, this section uses AMI and partner data that was not readily available to SCE during the incident.

¹³ A relay is a switch that is either closed or open based upon the level of amperage that is being utilized in a certain segment of a circuit or pieces of equipment. The status of a relay activates other components in the network to operate, usually a primary circuit breaker or a network protector.

¹⁴ It should be noted that SCE refers to its on-call incident commander as a “Storm Boss,” regardless of the type of incident or hazard to which the Company is responding. Similarly, the Company refers to its Corporate Emergency Response Plan as its “Storm Plan.”

¹⁵ Note that the LBPDOC is located in the Police Headquarters. Police Headquarters and the City jail were affected by the power outage although both had limited back-up power generation.

communication. By 3:00 p.m. on July 16, SCE activated the full ES-IMT (Electrical Services-Incident Management Team) response organization at its Lighthipec substation in the city of Long Beach. In order to expedite the restoration to key facilities throughout the affected area, SCE acquired and connected temporary generators.

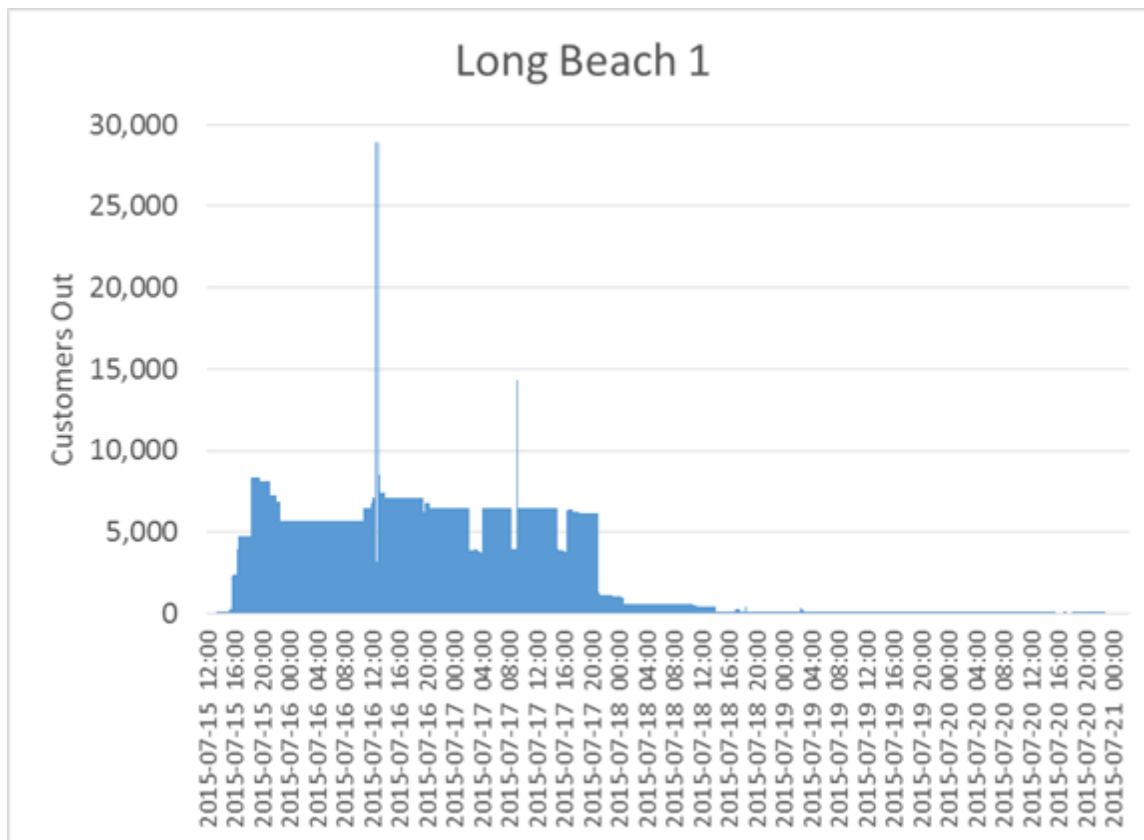
In addition to focusing on service restoration to customers, SCE opened a distribution site at 714 Pacific Avenue to provide water, ice, and flashlights. The American Red Cross also operated a relief site at 240 Chestnut Street. On July 17, both of these locations were closed and a combined site was opened at Cesar Chavez Park, which was then closed on July 18. The Long Beach City EOC and the Police Department Command Posts also closed at approximately 2:00 p.m. on July 18. SCE demobilized its ES-IMT at 2:00 p.m. on July 20, transferring responsibility to the Company's Long Beach District Manager. A detailed timeline of the response is provided in Appendix A.

5.1.1. Customer Outages

According to SCE's AMI data collected after the incident, there were two customer outage peaks during the incident.¹⁶ The highest of these peaks was at 12:54 p.m. on July 16, when 28,895 customers were without power for three minutes. AMI data also shows that power to all customers was restored by 3:34 p.m. on July 20.

¹⁶ It is important to note that the AMI data used throughout this report was not available to SCE at the time of the incidents and that, as a result, the customer numbers in AMI may be different than those relied upon by the Company during the incidents or in communications at the time of the incidents. AMI data does not include approximately 3% of customers affected who do not have smart meters installed or whose smart meters are not connected to the communications network.

Figure 6: Long Beach 1 Customer Outages by Day and Time (Source: AMI Data)



5.2. Long Beach 2

SCE experienced a second failure of its Long Beach underground secondary network at approximately 4:30 p.m. on July 30. Around 5:00 p.m., the Business Resiliency team completed an Incident Complexity Analysis and determined that SCE should declare a level 3 incident, which is defined as an “event with the potential to result in severe harm to the company, but for which there is a higher level of familiarity or anticipation.” The Company activated its full ES-IMT and an Incident Support Team (IST), following the guidelines for a level 3. The City of Long Beach also activated its EOC to support the incident only to demobilize within 24-hours. As part of its response efforts, SCE sent AREPs to the city’s EOC.

During the response to the second Long Beach network failure, SCE implemented a plan that had three objectives:

- Restore service to customers;
- Inspect underground structures; and
- Develop a manhole tethering solution.

Due to experience gained in its response to the July 15 incident, SCE was able to develop a comprehensive restoration strategy. According to SCE’s AMI data, in just over 12

hours, the outages were reduced to less than 300. SCE operated customer support distribution sites at Cesar Chavez Park and 925 Locust Avenue during the incident. On August 1, all customers were being supplied with power, either through the grid or by generators. SCE demobilized its IST organization on August 1 and closed its distribution sites by August 2. On August 3, the last customer was restored and SCE demobilized the ES-IMT.

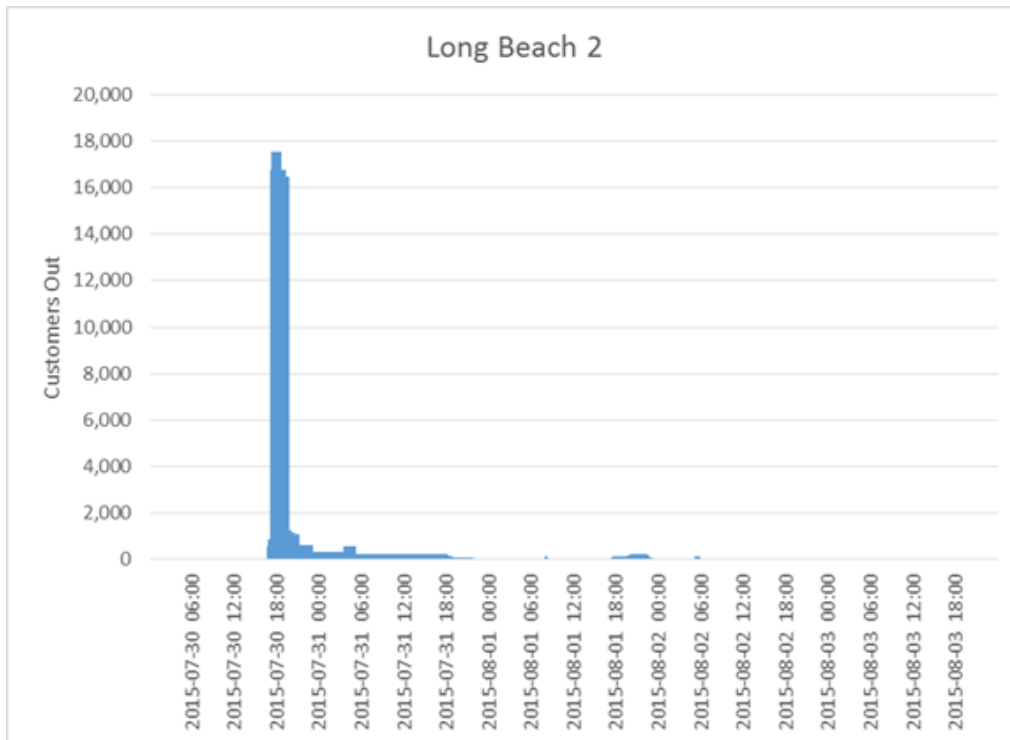
During the incident, SCE also completed inspecting its underground structures, developed and tested a tethering plan for the manhole covers, and reviewed the plan with Long Beach City officials. A detailed timeline of Long Beach 2 response is provided in Appendix A.

5.2.1. Customer Outages

According to SCE's AMI data,¹⁷ at approximately 5:20 p.m. on July 30, a peak of 17,532 customers were without power. Less than 300 customers remained without power by the morning of July 31. By the morning of August 1, AMI data shows that the number was reduced to less than 50. The AMI information available after the fact indicates that by August 1, all except for three customers had power restored either through the grid or generators. The remaining three customers were reconnected on August 2 at 5:33 a.m. One additional customer experienced a related outage until 3:18 p.m. on August 3, after being temporarily reconnected on July 31 for a period of 22 hours.

¹⁷ Customer outage information from SCE's AMI data was not available to the Company in real time during the incident.

Figure 7: Long Beach 2 Customer Outages by Day and Time (Source: AMI Data)



5.3. Manhole Fires: Response and Mitigation Plan

During the two network incidents, the City of Long Beach experienced several manhole fires, sending covers into the air. City of Long Beach 911 records indicate eight reports of fires or smoke with two explosions during the two network outages. SCE mapping data shows four vault fires over the course of both events. In order to reduce future risk of public injury and outages, SCE took immediate action to establish a plan to inspect its underground structures for additional damage or fires and to design and implement a tethering solution for each manhole cover.

By Friday, July 31, SCE had completed the inspection of its manhole structures in the Long Beach underground secondary network. The inspections found no critical issues requiring immediate repairs and discovered lower priority repairs that were to be addressed after the resolution of the outage incident.

SCE also established a task force and charged it to design a manhole cover tether, identify materials, and develop an installation approach. By August 3, the tethering proof of concept had been piloted by SCE, with three installed in the field. SCE retrofitted all structures on the underground network that could be accessed and located by August 10, 2015, and completed the remaining structures on the network by September 15, 2015. In total, SCE retrofitted 278 manhole covers with the tethering mechanisms.

6. Root Cause Analysis

Based upon a review of the incident timelines and available documentation of processes, procedures, and practices at SCE, Davies Consulting identified the root causes¹⁸ of the July 15 event and of the July 30 event. This section also describes other contributing factors.¹⁹

6.1. *Root Cause: Long Beach 1*

SCE operated the Long Beach underground secondary network outside of its optimal design state without having processes in place to actively monitor and track equipment that was being operated abnormally and made operating decisions that resulted in the network shut-down. A primary splice failure on the FLOAT circuit triggered a series of events that ultimately forced the network to be shut down. As the Long Beach network is a first contingency designed network,²⁰ a primary splice failure should not have resulted in a network shutdown. Therefore, the root cause is that the network was outside of its optimal design state.

6.2. *Root Cause Long Beach 2*

The July 30 network shutdown was the result of damage sustained during the operation and restoration of the network during the July 15 incident. The specific operational decisions during the July 15 incident are detailed in Appendix A.

6.3. *Sequence of Events*

As a reference for the following sections, on July 15, the available primary circuit maps being utilized by Grid Operations indicated that there were seven known primary circuits supplying the Long Beach network (i.e., network circuits):

1. FLOAT;
2. STEAM;
3. CARGO;
4. OCEAN;
5. CHESTNUT;
6. LOOP; and

¹⁸ A root cause is identified if its removal from the problem sequence would prevent the final outcome from occurring.

¹⁹ A contributing factor is one which affects the final outcome but was not a root cause.

²⁰ A first contingency design means that any single circuit can be out of service without any disruption of service to customers. As a first contingency design, SCE's Long Beach network is intended to provide safe and reliable service at peak load with any single primary circuit out of service.

7. TRIBUNE.

Additionally, there was a section of the network that was not included on the Long Beach Network Protector map being used by Grid Operations during the response. This additional section of the network is fed from another three primary circuits:

1. AFTON;
2. DUSK; and
3. HOBACK.

6.3.1. Long Beach 1: Sequence of Events

On July 15, the SCE Long Beach network was operating with six distinct locations where the network protectors (NWP 20638, NWP 20670, NWP 20653, NWP 30397, NWP 25509 and NWP 25505) were not supplying the load because they were in the open position or missing fuses, creating six localized first contingencies (see Figure 12, A through F references). As a result, at these locations, rather than the network protectors supplying the load from the primary circuits as they are designed to do, load was being supplied by the secondary grid, which, in turn, was being supplied by nearby network protectors that were in the closed position.

SCE's operations personnel were not aware that the network was being operated beyond its optimal design state because processes were not in place to actively monitor and track equipment that was being operated abnormally. As a result, the abnormal status of equipment was not being taken into consideration when making operational decisions.

In addition to the six locations noted above where network protectors were open and not supplying the network, there were two additional locations where network protectors were closed, but not operational (NWP 20649, and NWP 28113). These network protectors were supplying the underground secondary conductors, but were unable to open due to non-operational or missing relays.²¹ A fully operational network protector is designed to open if the primary circuit that is supplying it opens due to a primary fault on the circuit, or if it is purposefully opened by Grid Operations. Because these network protectors were closed, but not operational, they would not have

²¹ As noted previously, relays are switches that are either closed or open based upon the level of amperage that is being utilized in a certain segment of a circuit or pieces of equipment. The status of a relay activates other components in the network to operate, usually a primary circuit breaker or a network protector.

opened if their supply circuit opened. Instead, the circuit would have become energized-via-backfeed.²²

Of particular concern was one localized first contingency in the area bounded by 3rd and 4th Streets on the south and north and Crystal Court and Virginia Court on the west and east.²³ This load pocket was designed to be supplied by two primary network circuits with secondary voltage main connectivity and support. Both network protectors (OCEAN circuit - NWP 20670 and FLOAT circuit - NWP 20649) that supplied the load pocket from different circuits were in an abnormal state, with NWP 20670 being open with fuses removed and NWP 20649 being closed and non-operational (Figure 13, A and B references). In addition, due to the physical boundaries of the load pocket, the secondary conductors supporting the load pocket through the underground secondary grid were routed through one manhole (M5133092) and were not designed to supply the load created when both of the network protectors were unavailable. It should be noted that the NWP 20649 was manually closed (non-operational because of missing relays) on June 18 to alleviate a low voltage situation in the load pocket and it was not placed back into a normal closed automatic position²⁴ prior to July 15. This network protector had been identified in the SAP equipment log as being non-operational (operating without a relay) since October 14, 2010. Notably, on July 15, this was the only network protector in the SAP system log identified as operating in an abnormal state.

The abnormal status of the other network protectors was identified during vault inspections on or after July 15. Throughout the industry, it is not uncommon to have discrete pieces of equipment out of service or in an abnormal state at any given time. To address this issue, which places an underground network beyond its optimal design state, a leading utility practice is to continually evaluate the status of equipment and

²² A network protector is designed to open automatically when the feeder that is supplying its associated transformer is de-energized. When a network protector is closed manually and is non-operational, it will not open when its associated feeder is de-energized. In this type of situation, a network protector that remains closed when its associated feeder is de-energized will provide an electrical path from the secondary mains of the network back through the network protector, its associated transformer, and into the “de-energized feeder.” If there is a fault on the feeder (which leads to it being automatically de-energized through a relay operation at the circuit breaker) the secondary grid will attempt to supply power to the fault, and the feeder remains “energized-on-backfeed” through the electric path previously described.

²³ A load pocket is an area with discrete boundaries that has defined electrical support consistent with the design criteria for the network and limited secondary main ties to the remaining portions of the underground secondary network.

²⁴ This network protector was not capable of being placed in an automatic position because it was missing its relay.

conduct next worst case analyses.²⁵ In the case of the Long Beach network, given the information that was available to Grid Operations, the next worst case event, when considering the locations, circuit supply, and secondary support within the grid, was the loss of the FLOAT circuit due to a splice or cable fault. A failure of the FLOAT circuit would place the above-described load pocket in a second contingency,²⁶ forcing it to rely on secondary conductors of the network to remain energized.²⁷ Unfortunately, the electrically closest network protector that would have been able to help supply the load pocket was also supplied by the FLOAT circuit (NWP 20650), and with the loss of the FLOAT circuit, it was unavailable to supply the load pocket.

The load pocket also contained a closed, non-operational network protector (NWP 20649), which was supplied by the FLOAT feeder and would remain energized-via-backfeed, supplying the splice or cable fault. To make this next worst case worse, the electrically closest load area which could provide support had three network protectors (NWP 30397, NWP 25509 and NWP 20638) open, non-operational, and not supporting the network (Figure 13, C, D, and E references). Moreover, the secondary conductors that electrically connect this load pocket to the remainder of the network were not designed to carry the load required in a second contingency, especially not the additional load created by the network protectors that were closed and continuing to energize primary circuits via-backfeed. In a next worst case scenario analysis, these factors would have identified the loss of the FLOAT feeder as the next worst case event in the Long Beach network operations.

At 3:07 p.m. on July 15, the FLOAT circuit opened.²⁸ At 3:19 p.m., Grid Operations closed the FLOAT circuit breaker in an attempt to re-energize the circuit, but it immediately re-opened. After electrically isolating portions of the circuit, Grid Operations again attempted to re-energize the FLOAT circuit twice, but was unsuccessful because the breaker it was attempting to close did not respond.

Once the FLOAT circuit was de-energized at 3:07 p.m., the next worst case scenario was realized, causing a fire, which was reported in the 3rd Street and Magnolia area. The fire occurred because the load pocket was in a second contingency but was only designed to handle a first contingency. In addition, the network protector (NWP 20649) that was connected to the FLOAT circuit was backfeeding the primary portion of the network,

²⁵ The next-worst case analysis identifies the next worst event (i.e., loss of a feeder or network protector) that would further challenge the ability to reliably and safely operate a network.

²⁶ Second contingency is when two major components are out of service and the system is designed to work properly with only one component out of service.

²⁷ It should be noted that SCE had no primary or secondary network model to confirm this.

²⁸ The relaying of the FLOAT feeder was due to a failed splice joint that connected two types of primary cable in V5202624.

due to the faulted primary splice, and any electrically connected overhead load, thereby adding load to an already stressed load pocket.

Underground secondary networks will remain energized even when they exceed their design criteria, so in this instance, even with two components being out of service (FLOAT circuit and the open network protector NWP 20670) and the additional load created by the energized-via-backfeed situation, the network attempted to provide service to the load pocket utilizing secondary circuits. Since manhole M5133092 was the connection point to the secondary circuit portion of the underground secondary network, the load would need to be supplied by conductors in that manhole. By design, as a first contingency network, the conductors in manhole M5133092 were not intended to carry the entire load of the load pocket, which was normally supplied by two network protectors from two different primary circuits. As a result, when the additional load was placed on manhole M5133092, the insulation on the conductors began to burn. While the network was struggling to keep the load pocket energized, the remaining portions of the network were also hampered by the loss of the other network protectors supplied by the FLOAT circuit, which are designed to automatically open if the associated circuit is de-energized.

Four network protectors were supplied by the FLOAT circuit, including the closed non-operational one in the load pocket (NWP 20649). Of the three other network protectors supplied by the FLOAT circuit, the most notable was NWP 20650 (See A in Figure 14), which was electrically closest to the load pocket. That network protector was unable to provide support because it opened as a result of the FLOAT circuit failure, so the next closest load area had to provide the electric support to the load pocket. In the next closest load area, three additional network protectors, supplied by the CARGO and CHESTNUT circuits (NWP 30397, NWP 25509, and NWP 20638– B, C, and D references, respectively, in Figure 14) were also open and non-operational. In total, when the FLOAT circuit failed, six network protectors were not supplying the network's secondary grid.²⁹

At 3:32 p.m., the STEAM circuit opened automatically based upon the relays sensing a fault, taking another circuit out of service and de-energizing its six operational network protectors.³⁰ The cause of the STEAM circuit loss was a cable splice failure in manhole V5202624 (See A in Figure 15), the same manhole as the FLOAT circuit splice failure, which was in close proximity to the primary splice fault on the FLOAT circuit. This may have been caused by the continued energy supply that was provided to the primary

²⁹ The number of FLOAT network protectors is derived from the 2012 map with corrections that were identified through switching (i.e., NWP 30397 and NWP 25509 identified as FLOAT circuits as per the 2008 and 2012 maps but identified during switching as being supplied by the CARGO circuit). These numbers are relied upon in the remainder of the report due to discrepancies between maps.

³⁰ While there are six network protectors connected to the STEAM feeder, NWP 25505 was already off-line.

splice failure through the energized-via-backfeed location, NWP 20649, and the attempt to reclose the FLOAT circuit after it initially failed. After the STEAM circuit was de-energized, 12 of the approximately 60 network protectors in the Long Beach network were off-line and unable to support the network. One of the 12 network protectors (NWP 20649, closed and non-operational) was adding stress to the network by supplying energy to the FLOAT circuit primary splice failure from the secondary portion of the underground secondary network. It should be noted that neither of the primary circuits in manhole V5202624 had arc proof taping, which is utilized to protect the primary circuit cable from damage due to local environmental conditions such as fire in close proximity to an existing or on-going fault.

In summary, the primary splice failure on the FLOAT circuit, the subsequent re-energization of the FLOAT circuit, and the energized-via-backfeed situation created environmental conditions that may have caused the cable splice failure on the STEAM circuit.

At 4:22 p.m., as the network continued to provide energy to the burning cables in manhole M5133092, SCE proactively de-energized the CARGO circuit that ran through that manhole. While appropriate to avoid damage to the CARGO circuit, this decision eliminated three more network protectors from service, making the continued service of the network tenuous. However, the removal of network protectors NWP 28113 (9th Street and Pacific Avenue), NWP 25525 (6th Street and Pine Avenue and shown as A in Figure 16), and NWP 25508 (7th Street and Tribune Court and shown as B in Figure 16) resulted in severe low voltage in the area around Pine Avenue and 9th and 10th Streets, initiating the cable fires in manholes M5132735 and X5132734 on 9th Street and Pine Avenue.³¹ Low voltage causes cables to significantly heat, which increases impedance,³² resulting in the insulation on the cable melting and burning. During this period, it becomes more difficult to supply the load.

By design, when the CARGO circuit was de-energized, the network protectors that were operational would have opened, separating the network protectors from the underground secondary network grid. In this instance, however, one network protector (NWP 28113) supplied by the CARGO circuit was closed and non-operational, so NWP 28113 remained energized-via-backfeed, adding to the problem. This placed significant stress upon the remaining network in the northern portion, because it attempted to provide electric service to the remaining non-network load connected to the CARGO

³¹ These locations are not shown on the graphic, which illustrate the system as it appeared to SCE on the maps being used during the response.

³² Impedance is the effective resistance of an electric circuit or component to alternating current, arising from the combined effects of ohmic resistance and reactance.

circuit. This additional load contributed to burning the insulation on the conductors that were attempting to supply the load.

At 5:59 p.m., Grid Operations proactively placed the OCEAN, CHESTNUT, TRIBUNE, and LOOP circuits in a non-reclosing mode so that they would open and not reclose if a triggering event were experienced. This was done to avoid creating any additional damage to the system if another circuit failed.

As illustrated in Figure 17, at 6:20 p.m., the OCEAN circuit failed, eliminating six more network protectors from supplying the network. As previously discussed, one of the six network protectors (NWP 20670, shown as A in Figure 17) already was not supplying the network prior to July 15.

At 6:21 p.m., the southern portion of the network was de-energized by opening circuits CHESTNUT, LOOP, and TRIBUNE. The remaining northern portion above 7th Street (that was not identified as being part of the underground secondary network on the Long Beach Network Protector map) remained energized. At this time, the northern portion of the network was supplied by the DUSK, AFTON, and HOBACK circuits from the Cherry Street substation, so when the underground secondary network was de-energized by opening the network circuits from Seabright and State Street substations, the northern portion was not de-energized. Looking at the northern portion of the network independently, this placed that portion of the network in a second contingency, because it did not have supply from the CARGO and TRIBUNE circuits. At that time, Grid Operations was unaware that the northern portion of the network was still energized.

Due to the loss of the two network circuits in the northern network, significant strain was placed on the secondary circuits, because the remaining circuits supplied by the Cherry Street substation continued to attempt to supply the load for the network as a whole. This was further exacerbated by the fact that the network protector NWP 28113, which was supplied by the CARGO circuit, was closed non-operational. This meant that in addition to the northern portion of the network being in a second contingency, it was also providing electric service to the non-network customers normally connected to the CARGO circuit, through the NWP 28113. As a result, the cables running through manholes M5132735 and X5132734 at 9th Street and Pine Avenue (shown as A in Figure 19) began to burn. The remaining network protector supplying electricity (NWP 30376 at Pine Avenue and 10th Street (shown as B in Figure 19) was north of the area. The secondary cable damage and the two structure fires in manholes M5132735 and X5132734 at 9th Street and Pine Avenue in the northern portion of the network were the result of the underground secondary network attempting to supply the network and non-network load that remained electrically connected. As secondary cables burned clear, disconnecting themselves from the secondary network grid, the remaining cables became more overloaded, likely being further damaged.

6.3.2. Long Beach 2

On July 30 at 4:50 p.m., the HOBACK circuit, which was the circuit providing the most electrical support for the northern portion of the network, relayed and locked out. This resulted from a secondary conductor, running in the same civil structure, burning into the HOBACK primary circuit. The burning of the secondary conductor was likely a result of the damage it sustained during the July 15 incident, wherein its ampacity rating was reduced due to overheating.

When the HOBACK circuit opened and was no longer able to contribute to supporting the underground secondary network, the load that was previously being supplied by the HOBACK circuit was picked up primarily by the CARGO circuit and its associated network protector. Similar to the incident at Magnolia and 3rd Street during LB1, the configuration of the network and the secondary mains only permitted current to flow along certain corridors. As the CARGO circuit attempted to keep the network energized, the load was primarily funneled through manholes M5132758 and V5132757, causing the cables to burn and creating structure fires. This was exacerbated by conduit damage that occurred between manholes X5132760 and M5132758 during LB1. The conduit damage prevented a pre-July 30 installation of conductors necessary to carry this load pocket within the underground secondary network during a first contingency.

With field reports of structure fires and knowing the potential impact of the CARGO circuit failing, at 5:08 p.m., Grid Operations de-energized the network in order to make repairs. The repairs were made, sections were isolated, and the bulk of the network customers were restored that evening. Customer outage counts increased briefly from 345 to 569 at 3:32 a.m. the next day, but then continued to decrease as damaged secondary cable was repaired.

6.4. *Contributing Factors to the Incidents*

In addition to the root causes of the two incidents, the analysis of the sequence of events detailed above revealed several contributing factors. Any of these, when considered individually, may not have raised concern or caused the network to shut down. When evaluated collectively, they suggest that a network shutdown could have been anticipated.

Lack of a Primary or Secondary Load Flow Model

SCE does not have a primary or secondary model of the underground network. Without a model, it is difficult to optimally operate the network. Specifically, the lack of a model precludes Grid Operations from understanding the consequences of operational decisions (e.g., adding load or re-configuring a circuit) made to react to system events (e.g., circuit contingencies or network protectors being off-line).

Lack of a Process or Tools to Conduct Contingency Analysis

As a result of not having a load flow model, SCE has not undertaken formal engineering analyses to evaluate potential contingencies within the network. Operations personnel operate the system as a first contingency design without knowing what will occur during the contingency – and if the system is actually designed to withstand it. Without this information, a next worst case analysis cannot be undertaken, which increases the risk of a network failure. Effectively, there is no information available to provide guidance regarding the operation of the network during its most vulnerable time period – contingencies.

Network Maps Did Not Accurately Depict Actual Field Conditions

The Long Beach network protector map relied upon at the beginning of the July 15 incident was nearly seven years old and out-of-date. Although response personnel were able to acquire a more recent version of the map from 2012 in the midst of the July 15 incident, that map was missing critical pieces of information necessary to safely and reliably operate the network. Without knowledge of actual system status and configuration, Grid Operations made decisions that added to the likelihood of cascading equipment failures and the ultimate shutdown of the network.

Existing Information on Automated Network Protectors Was Not Being Used

Despite having installed remote monitoring on 18 network protectors within the network, Grid Operations did not have access to information on the network protectors, and therefore, did not use this information to support its decision making process.

Existing Information from AMI Was Not Integrated into Operations

Currently AMI is capable of providing hourly minimum and maximum voltage for every network customer, enabling basic identification of potential network issues. For example, AMI data indicates that there were low voltage situations in the area after the CARGO circuit was proactively de-energized, which persisted along the Pine Avenue corridor in the 9th and 10th streets area, after the primary circuits CHESTNUT, LOOP, and TRIBUNE were de-energized. There is little evidence that this was used to proactively analyze the network prior to July 15th.

Day-To-Day Network System Operational Decisions Increased the Risk of Network Failure

Equipment being out of service or in non-operational states for extended periods of time subjected the network to significant increased risk, particularly because it is designed only as a first contingency network. Further, adding non-network load to network circuits without adequate protection also increases the risk of network circuit failures. Because the majority of network faults are not transient, allowing network circuits to reclose automatically places additional stress on equipment exposed to the fault current. The practice of placing network protectors in closed position manually

without a contingency plan to remedy the situation, as necessary, potentially places additional burden on the secondary grid during energized-via-backfeed situations.

Construction Standards Do Not Minimize Network Operating Risk

There are insufficient standards regarding the installation of primary circuits to minimize risk in SCE's underground structure (i.e., duct positions, racking requirements to avoid cascading faults, position of secondary versus primary, racking on opposing walls, etc.). In addition, arc proof taping was not replaced as part of the removal of previously installed asbestos arc proofing. This potentially increased the probability of a cascading fault, which happened when the STEAM circuit failed.

7. Findings and Recommendations

The findings and recommendations listed in this section were developed through interviews with nearly 80 stakeholders and a review of SCE data and documents provided in response to Davies Consulting requests. They are grouped within the following areas shown on Table 3.

Table 3: Organization of Findings and Recommendations

Acronym	Area Assessed
UNO	Underground Network Operations
EPP	Emergency Planning and Preparedness
IRM	Incident Response and Management
COM	Communications
ITOT	Information Technology and Operational Technology
CC	Corporate Culture

For each recommendation, there is an estimated value, level of difficulty to implement and suggested timing of implementation. The following tables show the associated color codes and definitions.

Table 4: Value Key

Low Value	Moderate Value	High Value
-----------	----------------	------------

Table 5: Ease of Implementation

Difficult to Implement	Moderate to Implement	Easy to Implement
------------------------	-----------------------	-------------------

Table 6: Recommended Timing of Implementation

Critical	In-progress
Immediate	Within 6 months
Mid-term	Within 6-12 months
Long-term	Greater than 12 months

In considering these recommendations, it should be noted that SCE may not choose to act on all of them, or at least not immediately. Some of the recommendations entail significant investment that may require regulatory approval. There may be delays in implementation of these recommendations pending availability of funding.

7.1. Underground Network Operations (UNO)

7.1.1. Overview

The knowledge, skills, tools and technology needed to manage underground secondary networks effectively are substantively different from those used to operate overhead or radial systems. A Company with an underground network needs to have precise maps, use data monitoring and network modeling tools that predict the flow of electricity, and

provide the tools and technologies that system operators, line workers, and engineers need in order to understand how the network is maintained, operated, and restored. Operators also need to understand how to problem solve the network when components fail and move the network away from its design state and closer to a failure state.

As networks begin to fail, they are designed in such a way that they will continue to attempt to serve customers despite the loss of circuits, thereby raising load levels on the cable, which can cause the networks to degrade and potentially fail. Therefore, operators must recognize some of the warning signs of impending failure, as the SCE decision makers did on July 15 and July 30, and take actions to de-energize the entire network before the network collapses. Once de-energized, network systems (i.e., cables, protectors, circuits, and transformers) must be inspected and repaired so that the damaged sections are isolated before the network can be restored as a whole. These are time consuming processes that increase the complexity and extend the duration of restoration.

7.1.2. Findings

The company had limited knowledge of the status of its network and network operations and restoration processes.

System operations, construction and maintenance, and engineering leadership (network decision makers), had limited knowledge of SCE's network status³³ and operations in comparison to their knowledge of the Company's overhead radial system. It appears that SCE's reduced knowledge of network status and operations was attributable to the following:

- SCE's personnel have deep and up-to-date knowledge of the radial system as a result of their frequent work operating and restoring the overhead radial system;
- The network had operated without a significant failure for decades, leading to limited knowledge and experience in resolving network failures as compared to overhead outages; and
- It was thought during these incidents, by many members of incident leadership, that overhead radial restoration techniques could be applied to the underground network operation and restoration.

The level of network expertise exhibited by SCE is not uncommon for companies with only a small portion of their customers on network systems; however SCE did not have the necessary processes in place to overcome this limitation when a failure actually occurred.

³³ Network status means the location and status of the network infrastructure (network protectors, circuits, transformers, and cables).

SCE does not have a primary or secondary underground network model.

The linchpin of network operations and restoration is a network model, which is a mathematical model that establishes the flow of electricity within the network. Decision makers use this model to predict how the system will react to load and system changes. Both leading up to and during the failures, the absence of a network model meant that SCE could not fully understand the impact of each of its decisions on the flow of electricity and the stability of the network. This, coupled with the data quality mentioned below, meant that it was difficult for SCE to effectively restore the network failure.

Network maps and record keeping was not adequate.

The maps and data relied upon by response personnel during the Long Beach failures did not reflect the actual state of the network, and decisions made before and during the response led to additional discrepancies. During the first response, personnel had two maps available to them: one dated 2008 and another dated 2012. While the differences between the two maps were slight, both maps were missing significant information, which appears to have limited the effectiveness of the response.

More specifically, neither the 2008 nor 2012 maps include detail about the network above 7th Street. In addition, the position and status of network protectors and the secondary network were not available to incident leadership. Despite the map data quality issues, the lack of a network model and expertise had a more significant effect on the restoration delays.

System Operators did not use remote monitoring to understand the state of network.

In the days leading up to the first failure and during both incidents, system operations did not use available remote monitoring to understand the state of the network. The focus of system operator training is on operating the predominant radial portions of the system that tend to experience outages more frequently. As a result, their understanding of network operations is limited. When the system operators on duty at Lighthipe at the time of the failures began to see circuits open automatically (relay or de-energize), they attempted to operate the system, but they were not trained to understand the impacts of their decisions and the best actions to take to mitigate risk in the network.

There was no assigned “owner” of the network with dedicated technical, engineering, and operations resources.

Responsibilities for maintaining and operating were carried out by multiple groups within T&D, with none having sole, explicit accountability. A network stakeholder group, including the Long Beach District Manager, a Long Beach Construction and Maintenance General Supervisor (representing line crews), an Engineering Apparatus Manager

(representing the transformers and network protectors), and a System Operator (representing the substation and the primary supply to the network) did meet monthly, as early as 2011, to discuss the network.

In early 2011, SCE conducted an assessment of the risks in its network with the support of the network stakeholder group. This review identified a number of recommendations to reduce the risk of network outages and failures. SCE implemented some of the recommendations from this study, but not all.

SCE did not have adequate knowledge of network operations and restoration.

At the time of the first Long Beach network shutdown, SCE did not have a cadre of personnel who were dedicated to and had experience in network operations, especially in network fault response and restoration. This gap was evident in a couple of operational decisions that increased the possibility of network failure (but did not cause the outages). Specifically, on July 15, SCE personnel decided to add an overhead circuit to be supplied by the FLOAT circuit. This decision increased the exposure of the FLOAT circuit breaker and the probability that the FLOAT relay protection system would operate, de-energizing the FLOAT circuit (the next worst case event).³⁴ Also on July 15, the overhead load of the ADMIRAL circuit was added to the STEAM circuit. These additions, which SCE planned to remove at 5:00 p.m. on the same day, placed non-network load on the FLOAT and STEAM circuits, increasing the possibility that one of them might go out of service. In addition to adding the overhead circuits to the network, SCE undertook non-priority scheduled work to replace a primary switch on the CARGO network circuit. This required the CARGO circuit to be re-configured, placing the network further out of its optimal design configuration.

In a company that operates one network that serves approximately 0.08% of its total customer base and which has not experienced a major network failure since the 1950s, it is not unusual or surprising that this level of institutional network knowledge was difficult to sustain organically. Notably, other utilities, especially those with a small portion of customers served by networks, tend not to have a designated owner for their underground secondary network systems.

³⁴ In doing so, the relay protection system which normally electrically monitored and protected only the FLOAT feeder now had to monitor and protect the FLOAT feeder plus the BOW feeder. While the additional load was not an issue for the FLOAT feeder as designed, the additional feeder increased the amount of cable and equipment that had to be monitored and protected by the relay protection system. Thus, due to the increased amount of equipment and conductors to protect, there was increased probability of an equipment failure that would initiate operation of the relay protection system.

7.1.3. Recommendations

UNO-1: Develop and implement a training and certification program for network operations personnel.

SCE should develop a certification program for network operators, engineers, troubleshooters, and construction and maintenance crews that covers: the theory of network operations, primary and secondary network operating processes and procedures, network restoration strategies (in addition to System Operating Bulletin 310³⁵), and indicators of network problems.

This certification program should ensure that:

- At least one certified system operator is on duty at all times at the Lighthipe substation;
- All permanently assigned construction and maintenance crews in Long Beach are certified;
- There are sufficient engineers with network experience to maintain and operate the equipment on the network and assist with the modeling; and
- Troubleshooters have an awareness of network operations.

In addition to the training and certification program, the network owner should conduct a field exercise on network restorations at least once every three years. This exercise should address a variety of scenarios, including flooding, earthquake, and a complete network burn down.

UNO-2: Develop a network model.

SCE should develop a secondary network model that enables mathematical modelling of the system. This model should be used whenever the network is taken out of design state, whether intentionally or unintentionally.

UNO-3: Develop contingency plans for network operations and conduct a hazard analysis.

Engineers and planners should conduct contingency analyses for the network, modelling next worst case scenarios (e.g., the loss of the FLOAT circuit). Based on these contingencies, the engineers and planners would either consider re-configuring the network to be more reliable or create useful procedures for system operators or field personnel. These procedures would outline what steps they should take in any given contingency.

As SCE increases its proficiency in network operations, it should identify the most consequential hazards and scenarios that could interrupt or affect the network. These

³⁵ System Operating Bulletin 310 has basic information and guidance on the network restoration.

could include tsunamis, earthquakes, major building collapse, and “black start” conditions. SCE should conduct table top exercises and model the system for scenarios similar to the contingency plans above. Based on the contingencies and hazard analyses, SCE should update the plan or network annex identified in EPP-6.

UNO-4: Utilize the available exception report for low voltages on the network.

Network engineers should use the exceptions report that is automatically generated for low voltage conditions on the network. This exceptions report should be provided to system operators, apparatus engineers, and the Long Beach District Manager on a daily basis. Corrective action should be discussed for exceptions.

UNO-5: Improve network monitoring capabilities in system operations and ensure reporting.

SCE should implement network monitoring capabilities within the control room and require all T&D personnel to report when equipment is out of design state. When the network is out of design state the control room should report this to all network operators until it is back in design state.

UNO-6: Conduct planned network maintenance in off-peak seasons.

It is important to minimize the risk to the network by maintaining the network in design state during peak load. Conducting maintenance on the network usually requires it to be placed out of design state. SCE should complete all planned maintenance in the off-peak season to help ensure that the network is in design state when not doing planned maintenance.

UNO-7: Continue the use of underground network system.

Inevitably, the question will be asked about converting the underground network to a radial system. The Long Beach network, when compared to the rest of SCE’s system (including recent outages) is a highly reliable system. The benefits to reliability resulting from the conversion of the network would not justify the cost.

7.1.4. Implementation Factors

Table 7: Underground Network Operations Recommendations

Number	Recommendation	Value	Ease of Implementation	Implementation Timeframe
UNO-1	Network Training and Certification	High	Difficult	Long-term
UNO-2	Develop a Secondary Network Model	High	Difficult	Long-term
UNO-3	Develop a Network Contingency Plan	Moderate	Easy	Mid-term
UNO-4	Report Voltage Exceptions for the Network	High	Easy	Immediate
UNO-5	Improve Network Modeling Capabilities	Moderate	Easy	Immediate

Number	Recommendation	Value	Ease of Implementation	Implementation Timeframe
UNO-6	Complete all Planned Maintenance in Off-Peak Season	High	Easy	Immediate
UNO-7	Continue the Underground Network	High	Easy	Immediate

7.2. Emergency Planning and Preparedness (EPP)

7.2.1. Overview

Over the last decade, many utilities have established formal emergency management programs and organizations. Increasingly, corporate boards and executives are adopting emergency response visions and guiding principles that clearly communicate a focus on emergency planning and response. Similarly, since 2012, SCE has enhanced its emergency management and business continuity capabilities to meet a range of hazards and threats. It has devoted significant resources to the following efforts:

- Corporate Storm Performance Improvement Process and overhead restoration plan;
- Catastrophic earthquake response; and
- Cyber-attack response.

In addition, SCE has increased the number of resources dedicated to emergency management at the enterprise level. Executives have been trained in crisis management and a number of SCE employees have been certified in the Incident Command System.

As emergency management organizations mature, they face many obstacles, including competing for valuable staff time, sustaining funding as one of many corporate priorities, and updating plans in isolation, reducing the likelihood of broader adoption and use.

In the case of these network outages, once SCE fully activated its response organization, the Company improved its response. There was, however, a delay in fully activating some of the Company's response processes and the level of maturity in ICS, specifically the limited penetration of ICS below the region manager level in Transmission and Distribution, reduced SCE's ability to manage a unique incident. The decision to not fully activate ICS before midday on July 16 contributed to challenges early in the response to the first outage.

7.2.2. Findings

SCE's Business Resiliency organization is challenged to effect change across the entire enterprise.

The Business Resiliency (BR) organization at SCE is currently charged with preparing the enterprise for all hazards that it may encounter, with a focus on emergency management and business continuity disciplines. The BR organization and its partners inside the Company have made progress in preparing SCE to respond to all hazards. BR

has faced challenges in its ability to improve preparedness and response capabilities throughout the enterprise.

BR and SCE's Operating Units share responsibility for protecting against, preventing, responding to, recovering from, and mitigating the risks of incidents. Therefore, these entities share responsibility for preparation and response. Emergency management organizations in multiple commodity utilities are most effective when there is clear governance, executive interest and support, parity of influence with executives, and when each Operating Unit takes responsibility for its own preparedness and response capabilities. At SCE, there is some ambiguity around emergency management governance and a lack of accountability across the enterprise for adherence to this governance. Finally, not all of the Operating Units have the resources necessary or have taken full responsibility for preparedness.

Despite these challenges, SCE has made significant progress in its preparedness and response since 2012. The inability to fully implement emergency management structures and processes did affect the early stages of the first incident. While it is impossible to establish whether this had an effect on restoration duration, it did have an effect on collaboration and communication with the City in the first 24 hours of Long Beach 1.

Implementing ICS helped to improve SCE's response efforts.

Implementation of the ICS framework provided a formalized structure and process to establish situational awareness, develop a restoration strategy, and communicate with customers and stakeholders. Once the ICS structure was fully activated by SCE, the response efforts improved.

ICS has not fully matured at all levels of the Company.

The Corporate Emergency Response Plan (CERP) defines the ICS roles and responsibilities below the section chief level, but ICS has not been fully implemented at SCE. There is, however, significant buy-in for the use of ICS among IMT members and executives, who have taken training, are conversant in the principles of ICS, and are ready to employ ICS if they need to activate under the Crisis Management Council. The lack of ICS penetration below the command and general staff level, and specifically below the T&D region managers, however, was a contributing factor to some of the inefficiencies in the LB1 response. More specifically, and as discussed in Appendix A, there was a lack of coordination between the ES-IMT, the War Room at the Long Beach District, and crews in the field.

Current emergency response protocols and plans do not adequately address an underground network failure.

The CERP did not have sufficient information on the restoration of a network to support field personnel. It did, have elements that, if used, could have promoted better decision-

making and coordination between the IMT and personnel at the Long Beach District and in the field. Additionally, System Operating Bulletin (SOB) 310 did not provide sufficient information on how to restore a network system. This is evidenced by the fact that despite following SOB 310, incident leadership did not have key information available through accurate maps, a network model, system monitoring, or a plan to restore the network.

The current state of ICS deployment does not enable suitable collaboration and engagement of field personnel.

During the response, SCE personnel did not consistently or adequately engage engineers, operational personnel, or the apparatus group to create a workable restoration strategy. Unlike responses to similar incidents at other utilities, the collaboration between engineers, system operators, linemen, and apparatus engineers did not exist early in the incident. This was in part due to facility constraints (Lighthipe and NERC access) but was largely a result of SCE's ICS maturity, specifically that SCE has not implemented ICS below the section chief level.

This prevented SCE from organizing its personnel effectively to assess damage, create a restoration plan, and execute the plan. It is important to note that while this would be a problem in overhead radial outages, it is even more so during a network failure because there is no plan or institutional knowledge in place that specifically defines the response to underground secondary network incidents.

SCE has a robust ICS training and exercise program but has not focused on field personnel.

SCE has invested heavily in its emergency response training and exercises since 2012. Recent exercises have covered high consequence events such as earthquakes and cyber incidents and have largely engaged the upper levels of the Company's leadership. This was a prudent and reasonable approach aimed at implementing ICS and emergency management at SCE's leadership level. While this approach has been successful in many respects and has prepared SCE for responding to certain hazards, it has not sufficiently engaged SCE field personnel.

SCE conducts after action reviews regularly.

SCE integrates its action review with its exercise and incident response processes. Business Resiliency is responsible for identifying, tracking, and applying lessons learned wherever possible. The Operating Units appear to be compliant with implementing specific lessons learned, but there is no evidence of a formal process to capture and track risks or gaps identified through the lessons learned process that require capital funding or executive action to mitigate.

SCE lacks sufficient ties between Business Resiliency and Enterprise Risk Management.

SCE is updating its ratemaking, investment strategies, and asset management programs. Prior to 2014, risk was implicitly, but not explicitly, part of the investment management process and SCE did not have a separate asset management program. Even though SCE identified some network risks as early as 2011 and took steps to mitigate them, including replacing network protectors, the risk was not visible at the enterprise level. Had SCE utilized a more comprehensive, integrated risk management program it is more likely that the Company would have identified network failure as a risk and may have chosen to invest more in its network management and restoration capabilities. It did invest in network modeling capabilities in 2012 and the underground facility maintenance program through the 2015 rate case.

7.2.3. Recommendations

EPP-1: Provide additional executive support to the centralized Business Resiliency organization and enhance Operating Units' business resiliency organizations.

SCE should consider combining business resiliency, cyber security, and physical security functions under a single executive (e.g., Vice President). Typically, emergency management and business resiliency organizations are positioned with sufficient organizational influence to drive change, have direct access to the President of the company, report outside of operations, but have strong operational influence. They also have executive support to drive change and ensure that the entire enterprise is capable of managing the complete emergency management lifecycle for all hazards, including cyber, physical threats, natural hazards, and technical or anthropogenic (human caused) failures. SCE should continue to enable the Business Resiliency leaders' direct access to the President of the Company to ensure that this repositioned organization is better able to effect change.

BR should revisit its strategy on how it leads emergency management while getting the Operating Units to take more responsibility for preparedness and response. At the same time, each Operating Unit should have an assigned champion, with adequate resources and influence, responsible for its own preparedness and response capabilities. This champion also must have resources and influence within the Operating Unit to effect change. The operations and response critical Operating Units (Transmission & Distribution, IT, Corporate Communications, and others as identified by SCE) should create or enhance their preparedness and response organizations. BR should not only actively engage staff to advocate for and own their Operating Unit's preparedness and response capabilities, but should also work with Operating Unit leadership to craft position descriptions, interview staff, and make recommendations on the placement of BR leaders within the Operating Units.

Finally, Business Resiliency should consciously enhance its own utility operations knowledge and reinforce its expertise in electric and IT operations through active operational learning. In addition, BR should actively seek out operational leaders to advocate for improved preparedness and response capabilities.

EPP-2: SCE should create an ICS maturity model and different levels of Incident Management Teams.

An ICS maturity model and implementation of incident management team resource typing will support the development of ICS within SCE. With the ICS maturity model, SCE will be able to communicate what capabilities it currently has while simultaneously being able to create a multi-year maturity plan to expand ICS deeper into the organization and into the culture. In the public sector, IMT typing provides entities with the ability to assign different qualification levels and team sizes based on the complexity of the incident.

For example, in the public sector model, a Type 1 IMT would be called to respond to a Hurricane Katrina level incident while a Type 5 team would be used for routine emergencies in a small town. There is no recognized model in the utility industry, so SCE has the opportunity to adapt other available models to its purpose – understanding the very specific needs of a utility. There is a potential to coordinate this effort with other California or Western Energy Institute utilities.

The IMT resource typing³⁶ will accomplish three things. First, it will lay out a strategy for what qualifications are needed to fill IMT positions and enable responders to understand when they should escalate or deescalate the team. Second, it will shift from a one-size fits all strategy for IMT activation and enable ICS to truly scale from low-level incidents such as routine outages to the truly catastrophic incidents like the 2011 windstorm or the 1994 earthquake. Finally, it will alleviate the burden on the on-call incident management teams by establishing a larger pool of resources, and as a result use the same resources less frequently.

EPP-3: SCE should deploy ICS below the Region Manager level.

With a maturity model and incident typing in place, SCE should develop and implement a strategy for expanding the use of ICS into the field. Operating under the direction and oversight of BR, electrical services should pilot a program for ICS deployment in 2-3 districts. The ICS deployment should focus on how line crews can organize using ICS during an emergency and what resources are required under section chiefs to support a response. Lessons from other utilities suggest that a combination of ICS experts (with industry expertise) and credible electrical services staff who believe in and understand

³⁶ For information on the concept of resource typing see:
https://en.wikipedia.org/wiki/Incident_management_team

ICS work best as instructors. SCE will have to devote increased effort to mapping out a detailed response organization – from incident leadership all the way to the field – and define supporting processes, including information flow from the field to the IMT general and command staff.

EPP-4: Expand on-call Incident Management Teams.

As ICS matures and truly becomes scalable at SCE, there will be an increasing number of SCE personnel who are trained and qualified to fill IMT roles for large-scale incidents. Eventually, it would be wise to have more senior leaders trained and qualified, but that can happen over time, as a requirement of promotion, for example. Eventually, the burden on the on-call team should lessen, since the majority of routine incidents will be managed closer to the front line. Until those capabilities increase, the existing call schedule should be adjusted to minimize the burden on existing members.

EPP-5: Create a framework for emergency response plans at SCE.

SCE should create a logical framework and standards (e.g., NFPA 1600) for its emergency response plans across the enterprise. BR should then identify which of its existing plans is the core plan and which plans are annexes. It should structure a series of annexes that clearly document the processes for responding to key hazards and threats by all response personnel.

Given the need to drive change and provide usable plans, document process, and utilize common processes across the workforce during a response, these response plans must document processes in detail, including process maps, and not just define capabilities.

EPP-6: Develop an underground network restoration process and annex plan.

SCE should create an underground network restoration plan or annex that provides incident leadership with restoration strategies for the underground network. This plan should be more detailed than the existing SOB 310 and should outline the process for network restoration. Most importantly, the annex should address a more catastrophic network failure, including the loss of most network cable and equipment. Also, SCE should review other System Operating Bulletins to understand any gaps that might exist between the SOB and response capabilities.

EPP-7: Transition from training and exercising in-breadth to in-depth.

SCE's focus should be redirected toward engaging front line personnel in training and exercises. Currently, the Company focuses on delivering large-scale training and exercises across the enterprise at the manager and executive level rather than deeper within the organization (down to field personnel). This shift will enable SCE to drive ICS and emergency management more fully into the Company culture.

EPP-8: Review current levels of service during response and update capabilities or expectations.

The following recommendation does not stem from performance during Long Beach. It concerns a risk to SCE's response capabilities moving forward.

As each operating unit creates a strategy for delivering service after organizational restructuring, it should also consider a strategy for emergency response delivery. Business Resiliency should work with affected Operating Units to identify gaps in capabilities and resources, update the service delivery model, work with SCE leadership to fill any strategic gaps, and adjust expectations with stakeholders. Specifically, Business Resiliency should work with leaders in Corporate Communications and Local Public Affairs to:

- Identify strategic risks during a response;
- Update service delivery models to meet customer expectations wherever possible; and
- Work with external stakeholders to adjust expectations or update partnering models before the response.

7.2.4. Implementation Factors

Table 8: Emergency Planning and Preparedness Recommendations

Number	Recommendation	Value	Ease of Implementation	Implementation Timeframe
EPP-1	Support and Enhance Business Resiliency Efforts	High	Easy	Immediate
EPP-2	ICS Maturity Model and 'Typed' Teams	High	Moderate	Mid-term
EPP-3	Implement ICS more fully	High	Difficult	Long-term
EPP-4	Expand On-call Incident Management Teams and Move Toward a More Mature ICS Model	High	Easy	Immediate
EPP-5	Create Plan Framework	High	Easy	Immediate
EPP-6	Develop an Underground Network Restoration Process or Annex	High	Difficult	Long-term
EPP-7	Train and Exercise In-Breadth	High	Moderate	Mid-term
EPP-8	Review Current Levels of Service During Response and Update Capabilities or Expectations	High	Difficult	Immediate

7.3. Incident Response and Management (IRM)

7.3.1. Overview

Incident Management is generally defined as the activities undertaken by the responding entity to identify, analyze, and develop a comprehensive plan for responding to an incident, with the objective of restoring the Company and its

customers/stakeholders to normalcy.³⁷ In leading practice utilities, ICS³⁸ is relied upon as a standardized, on-scene, all-hazard incident management concept, allowing responders to adopt an integrated organizational structure to match the complexities and demands of single or multiple incidents without being hindered by jurisdictional boundaries.

7.3.2. Findings

SCE used lessons learned from LB1 to respond to LB2 more effectively.

The response to the second incident on July 30 was managed more successfully than the first one two weeks earlier. In a short period of time, SCE was able to apply lessons learned from the July 15 incident, including: activating the ES-IMT and IST immediately at the onset of the second event; more effectively deploying generators to critical facilities; and communicating more effectively with local officials from the start of the event.

The response was focused on electrical restoration and did not adequately approach the incident from a community perspective.

SCE's response to the July 15 incident was focused primarily on trying to understand the status of the network and attempting to restore electric service. Responders did not recognize the scope of the incident, especially the community concerns related to public safety and property damage. SCE's incident leadership did not initially integrate the Company's activity with local agencies and did not provide sufficient information so that community leaders could make decisions to better ensure public safety.

The incident complexity analysis did not adequately capture the intricacies of the network failure.

As soon as Business Resiliency was notified of the incident on July 15, it completed an Incident Complexity Analysis. When completed, however, the Analysis did not adequately recognize the complexity of restoring a significant underground secondary network failure, which, as discussed in Section 0, requires a different approach than restoring an overhead failure. Interviewees indicated that the analysis did not sufficiently engage functions outside of Business Resiliency and Operations to assess the complications associated with an incident of this nature. As a result, the Analysis did not

³⁷ Glossary of Terms, The Business Continuity Institute Good Practice Guidelines 2010 Global Edition. thebci.org, accessed on September 28, 2015.

³⁸ ICS is becoming the standard management system in many industries, but it should be noted that ***the complexities present in many private industries make wholesale adoption of ICS, without some modifications, difficult.*** ICS was designed as a system to manage wildfires more effectively and does not necessarily consider the intricacies associated with utilities, such as complex systems and diverse stakeholders with varied expectations.

provide incident leadership with adequate information and guidance to immediately escalate the incident to one requiring a more formal response.

The IMT was not fully implemented and staffed at the onset of LB1.

As noted in Section 5.1.1, the first failure in the LB1 incident was reported at approximately 3:07 p.m. At approximately 6:00 p.m., SCE documentation indicates a partial activation of its IMT, with the full IMT not activated until July 16, more than 12 hours after the initial failure. The partial activation (known as “ICS-lite”) involved remote activation of a limited number of IMT members. The Incident Commander remotely monitored the incident, with no conference calls, and limited interaction between activated individuals.

SCE’s All-Hazards Plan states that the IMT “is comprised of the Incident Commander (IC), the Command Staff, and the General Staff. The General Staff, under the direction of the IC, manages the response to an incident.” While some interviewees indicated that partial activation had been used previously to respond to small incidents, the majority did not have sufficient knowledge of what partial activation entailed – and the definition of what partial activation entailed was not available in any readily accessible plan or document. While ICS is a scalable response structure and does not require an entire IMT to be activated, the use of a telework management system, without adequate conference calls and information sharing, caused confusion, diminished the Company’s situational awareness and lessened the effectiveness of the response.

Some on-duty personnel did not mobilize when activated during LB1.

Business Resiliency is responsible for oversight and management of the Incident Management Program, which includes establishment of response teams, rotation schedules, and coordination and activation. The teams established are aligned with SCE’s operational functional areas and include two qualified people in each position. Business Resiliency has established four Electrical Service IMTs and two Incident Support Teams, each with two qualified individuals staffing each position. Each team is designated A or B, with one qualified person in each position. During the week of July 15, ES-IMT #3 B was on-call. During the week of July 30, ES-IMT #1 A and IST #1 A were on-call. Each individual on-call should be able to meet expectations stated in the Incident Management Program document, including:

- If activated, report to the incident command post;
- When on call, be accessible and available during on-call time 24/7;
- If activated, acknowledge the activation with the Watch Office within one hour, and be en route to the incident command post from within the SCE service territory within two hours;
- If a team member is unable to be on-call for any reason, it is their responsibility to find a willing and qualified replacement to cover the on-call status and send

notification to the team's ICs and the Watch Office no later than 8:00 a.m. on the Wednesday prior to assuming on-call status;

- Team members should go to their counterpart on the same (numbered) team first when a replacement is needed. If that person cannot serve, a qualified replacement should be found on another team; and
- On-call roster changes should be submitted to WatchOffice@sce.com by COB on the Wednesday prior to the Monday shift change.

During LB1, an inaccurate call schedule was relied upon initially by the Watch Office and then multiple on-call personnel did not report when activated and had not found or provided the Watch Office with replacements, leading to difficulty with efficient and timely activation, as well as confusion in shifts/shift transfer and a lack of continuity in positions. The failure to report also created additional confusion because:

- Incident management and response personnel did not have full knowledge about who was filling what position (since it was not aligned with the duty roster);
- There was no clear check-in or resource management process;
- There was a lack of continuity in situational awareness, with more than two individuals (sometimes as many as five) filling a single position; and
- There was no established or defined shift/schedule.

It is important to note that during LB2, incident leadership and Business Resiliency activated both the IMT and the IST and provided SCE personnel with updates regarding who was filling each position.

SCE senior executives largely respected the incident management process and roles and responsibilities.

While SCE officers recognized how the incident management process should work, they did intentionally function outside of process to address problems. More specifically, on the afternoon of July 16, after Long Beach's frustration with the incident had become clear, SCE senior executives were deployed to Long Beach to assess the situation. They quickly realized that the Long Beach stakeholders' expectations were not being met and made a decision to elevate the SCE AREP position to an executive. This was outside of the documented process, yet it was an appropriate decision based on the level of stakeholder dissatisfaction. Overall, the executives did a good job supporting the Incident Management Team, resolving issues, and escalating issues appropriately.

Unity of Command was not achieved.

The Federal Emergency Management Agency (FEMA), defines Unity of Command as "the concept by which each person within an organization reports to one and only one

designated person. The purpose of unity of command is to ensure unity of effort under one responsible commander for every objective.”³⁹⁴⁰

For utilities, successfully achieving Unity of Command means that many response personnel are assigned an incident response role and will shift from their blue-sky reporting hierarchy to the reporting structure in the response organization. An incident response role is defined as a role or task that a person performs during emergency conditions that is different from their normal work activities. Typically, electric utilities assign and train a significant number of employees on second roles that are activated when a major incident occurs.

During a substantial incident, these employees may be required to undertake responsibilities that are different from their day-to-day roles, reporting to individuals not typically their managers. In private sector entities, this shift can be difficult, since it forces both managers and reports to ignore the company’s day-to-day hierarchy and use the reporting structure established in the response organization. As a result, the response organization needs to clearly establish lines of authority and reporting relationships that flow from the field all the way to incident leadership and executives.

SCE has not yet implemented ICS at all levels of the Company, leading to multiple groups reporting outside of the IMT and/or IST. Specifically, a “war room” was established at Long Beach District during LB1 that was led by a District Manager with no direct reporting relationship back to the IMT (personnel reporting through the District Manager were not engaged in the incident management structure). As a result, response personnel (particularly those on the operational side) received conflicting directives and both response personnel and those not engaged in the incident expressed confusion about who was ultimately the Incident Commander. The confusion hampered SCE’s ability to develop a sound restoration strategy.

In addition, some executives did not defer to the Incident Commander or Operations Section Chief, communicated directly with response personnel, and added confusion to the restoration plan, further compromising Unity of Command. Throughout the first response, executives interacted with their reports outside of process. In some cases, executives supported the response with their presence and did not distract or interfere with the unity of command, resulting in better situational awareness for the executives. In other cases, it resulted in confusion as when some T&D leaders interfered with the Unity of Command principle.

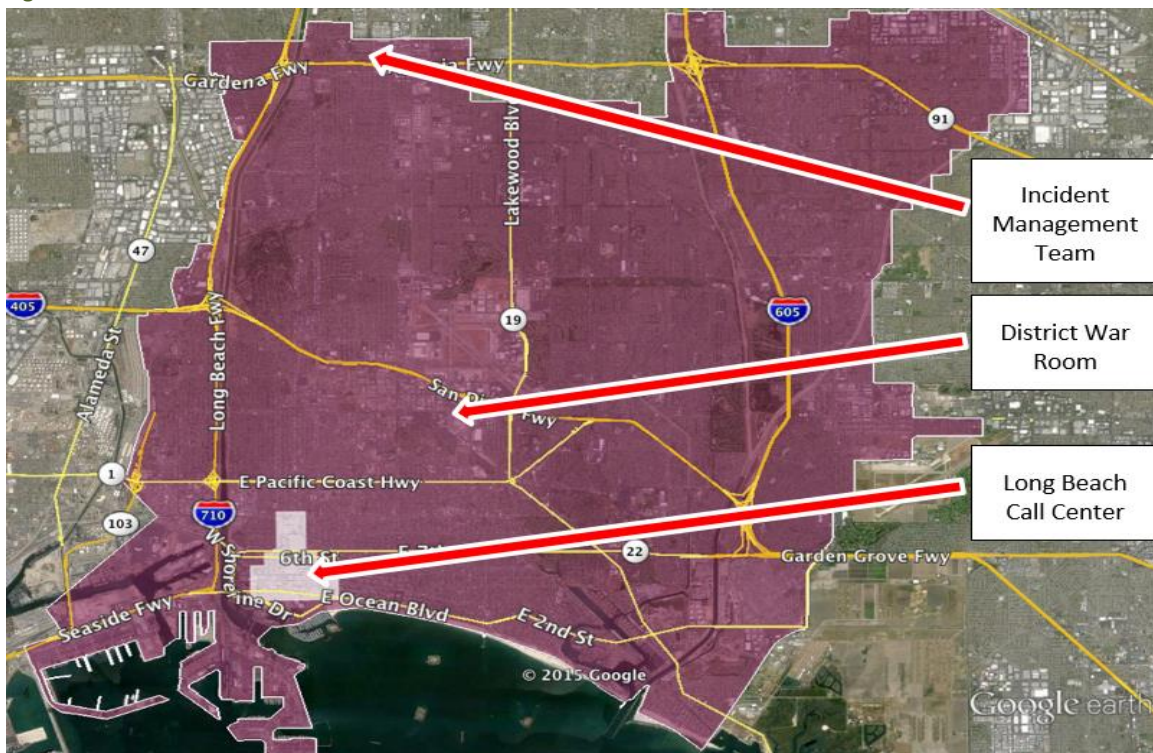
³⁹ FEMA, ICS Glossary, <https://training.fema.gov/emiweb/is/icsresource/assets/icsglossary.pdf>, accessed on September 28, 2015.

⁴⁰ Note that we do not call out chain of command separately though like unity of command, the chain of command was broken.

Disparate command posts contributed to difficulty in collaboration across functions involved in the response.

During the response, leadership (the IMT) was located at Lighthipe substation and District personnel, including operational staff, reported to the Long Beach District war room. Executives spent time at these command nodes as well as the City's various command and control centers (see Figure 8). The use of Lighthipe, according to interviewees, limited effective collaboration due to space constraints. Also, the establishment of a war room without a clear line of authority back to the IMT led to confusion regarding the command structure and which entity was ultimately managing the incident.

Figure 8: SCE Command and Control Nodes



There were other options available to SCE personnel, including the Mobile Command Center (discussed below), the former Long Beach Call Center, or a field Incident Command Post. While responders did not identify the physical spaces as impediments to effective teamwork during the incidents, in hindsight, many did recognize the challenges associated with having disparate or suboptimal command and control centers.

SCE did not utilize its Mobile Command Center.

In its Corporate Emergency Response Plan, SCE notes that it has a Mobile Command Center (MCC), which is “an operationally ready emergency management and communications center held in two 40-foot, self-propelled, and self-contained vehicles,

which can be deployed to the scene of an emergency incident.” According to the CERP, the MCC is designed to provide:

- A highly functional workspace for T&D project managers, offering communications, computer support, office services, shelter, and meeting support;
- A focal point for customers; and
- A venue to coordinate exchange of information with local and emergency authorities, fire agencies, environmental officials, and the media.

SCE failed to activate an MCC at any point during either incident. Having an MCC in place in Long Beach could have provided incident leadership with a functional workspace, Long Beach customers with a sense of SCE’s urgency in responding, and on-site external first responders and elected officials with a space to meet.

SCE did not activate the Incident Support Team during LB1.

The IST, which is typically activated “to manage multiple Incident Management Teams and . . . communicate with the Crisis Management Council,” was never activated during LB1.

Industry-wide, utility executives grapple with their roles in an emergency response. Many executives are eager to contribute during restoration, but, injecting opinions can, if not carefully delivered, disrupt the restoration hierarchy and may adversely affect communication and candor at the middle and lower ranks of an organization. As noted previously, in both LB1 and LB2, SCE’s executives largely respected the incident management structure. However, once the complex nature of the incident and external stakeholder pressure was known during LB1, the activation of an IST with executive engagement would have provided ES-IMT leadership with additional support.

SCE provided emergency supplies at Distribution Centers.

Throughout the two incidents, SCE opened (or supported the Red Cross) Distribution Centers at four locations. These centers provided customers with emergency supplies (water, ice, and flashlights) and safety-related information. In addition, SCE field personnel were tasked with conducting evacuations of affected buildings in Long Beach. Performing first responder responsibilities provides SCE with an opportunity to interact with and provide support to its customers, as well as engage volunteers from non-affected organizations. Since the July 15 and July 30 incidents were localized, SCE could make personnel available to provide this service. However, in a larger (i.e., catastrophic) incident, where every available resource will be needed, manning distribution centers could significantly impede the Company’s response. Therefore, SCE should not commit to providing this service in larger incidents. Rather it should provide this service on a case-by-case basis only.

A utility's primary objective during a restoration should be to efficiently and safely restore power while keeping customers informed. Utilities do not typically utilize valuable resources to undertake activities (such as evacuations or water and ice distribution) that are better left to local/state government agencies (emergency management, health and human services, etc.), or other private and public entities such as the Red Cross. Indeed, in recent years, the industry has almost entirely moved away from distributing these supplies. Before incidents, however, utilities collaborate with government agencies to develop messaging and ensure that coordination is effective during an event. During an event, utilities will work with these agencies to obtain information on distribution centers that the utility can then provide to its customers through pamphlets, etc.

7.3.3. Recommendations

IRM-1: Enhance the incident complexity analysis process.

SCE's complexity analysis should be refined to address additional hazards faced by SCE. The incident complexity analysis relied upon by SCE during the Long Beach incidents considers the following factors:

- Size and scope;
- Resources;
- SCE facility impact;
- Safety-environmental;
- Operations;
- External influences; and
- Evaluation of ongoing response activities.

While the Operations analysis is focused entirely on "storms," other areas of the analysis address questions that apply to all types of hazards. The analysis, however is heavily skewed toward assessing and declaring incident levels for a few hazards, including earthquakes and overhead outage incidents. For example, using the questions included in the complexity analysis to declare a level for other types of hazards or incidents, such as a network failure or a significant cyber data breach, would likely result in declaring a lower level than would truly be warranted. The current complexity analysis should be enhanced to include additional considerations, including, but not limited to:

- Customers/stakeholders impact;
- Expected response duration;
- Impact on essential business functions;
- Impact to Company's brand or reputation; and
- Advisories/directives from government entities.

IRM-2: When the IMT is required, SCE should not rely on remote activation.

Since the Long Beach incidents, SCE has conducted an internal lessons learned process that identified the partial activation as an opportunity for improvement and has already addressed this recommendation.

IRM-3: Use rosters and streamline shifts.

The use of rosters should be required during a response. Where possible, they should be developed and shared in advance of activation/mobilization. SCE should consider enhancements to its incident management support tools that make development and sharing of rosters easier and more seamlessly visible to responders. Further, for non-field response resources, the Company should adopt the industry standard 12-hour shift (understanding that there is a need to conduct transfer of command at the beginning and end of every shift) with a mandatory rest period and pre-defined A/B or day/night shifts to ensure continuity in incident management and response. SCE should enforce this shift schedule for all non-field response resources, including incident leadership. If practical, the callout system should be automatic, tying into the roster or ICS Form 203.

IRM-4: Establish accountability for preparedness and response role activation.

If SCE desires to be a best or leading practice emergency preparedness utility, staff at the Company must be fully engaged in emergency response efforts and activate when on duty. SCE should consider undertaking an internal campaign focusing on emergency response, with executives championing the need for staff to be accountable for responding when they are called upon. SCE also should establish performance metrics for evaluating the response participation and include them as part of performance appraisals.

IRM-5: Consider limitations of existing command and control locations; activate the Company's available Mobile Command Centers during significant incidents.

All responders, including Business Resiliency coaches and executives, should remain sensitive to the limitations of the physical spaces used for command and control. If the ability to team, collaborate, and communicate is impeded by the space being utilized or if there are too many distractions in a designated space, the team should consider relocating to a different facility, a field command post, or a mobile command post. The MCC, while not intended to operate as a decentralized district, can be deployed to demonstrate on-scene presence to SCE's stakeholders.

IRM-6: Collaborate with local agencies in supporting communities affected by incidents.

State, local and other emergency management agencies and groups can manage public needs related to water, ice distribution, and evacuations while SCE focuses on restoring service. As many other utilities do, SCE should develop a comprehensive brochure for distribution both before and during events. It would include information about the

importance of contacting SCE if power is lost, how to find information about safety, dry ice, and water distribution, and where to find cooling or warming centers. This coordination will ensure that SCE is properly engaged with emergency management and response organizations throughout Southern California and is providing customers with essential information in advance and during an incident.

IRM-7: Assign responsibility for determining level of response to Business Resiliency organization.

SCE should assign responsibility for determining the level of emergency response for any incident to the Business Resiliency organization. BR should obtain input from all operating units that are directly impacted by the incident before making determination. This approach should ensure that the response is coordinated across the company and that the organizational siloes are eliminated.

7.3.4. Implementation Factors

Table 9: Incident Response and Management Recommendations

Number	Recommendation	Value	Ease of Implementation	Implementation Timeframe
IRM-1	Enhance the Incident Complexity Analysis Process	High	Moderate	Immediate
IRM-2	Where the IMT is Required, SCE Should Not Rely on Remote Activation	High	Easy	Complete
IRM-3	Use Rosters and Streamline Shifts	High	Easy	Immediate
IRM-4	Establish Accountability for Preparedness and Response Role Activation	Moderate	Moderate	Mid-term
IRM-5	Consider Limitations of Existing Command And Control Locations; Activate the Company's Available Mobile Command Centers During Significant Incidents	Moderate	Easy	Immediate
IRM-6	Collaborate with Local Agencies to Support Communities Affected by Incidents	High	Moderate	Long-term
IRM - 7	Assign responsibility for determining level of response to Business Resiliency organization	High	Moderate	Critical

7.4. Communications (COM)

7.4.1. Overview

Communicating effectively to internal and external stakeholders (customers, regulators, elected officials, media, etc.) during an incident is *at least as important as* the operational/tactical response, including power restoration.

In order to meet stakeholder expectations, help return the community back to “normalcy” in the shortest time possible, and maintain customer satisfaction during major power outages, a utility should:

- Understand the increased expectations of its customer base regarding information sharing;
- Use appropriate and varied communication channels;
- Demonstrate that it knows the customer is without power;
- Convey a sense of urgency about restoring power;
- Provide consistent and accurate information on restoration progress; and
- Provide customers with accurate and reasonable estimated times of restoration.

Leading practice utilities employ a “One Voice” approach for communicating with the media and public. The provision of consistent messaging across all channels minimizes confusion among customer and the community, which can draw resources away from the restoration effort.

The current state of business-to-consumer communications encourages stakeholders to expect immediate and useful information related to their accounts at all times. Due to the complexity of utility systems, however, information that granular is seldom available at the frequency or with the speed that customers or other stakeholders desire, especially during a major incident.

Too often, utilities wait until an incident occurs to educate stakeholders about how they restore service. Then, in the face of an incident, stakeholder expectations have already been set and their focus is on whether the utility can meet those expectations, rather than on if the expectations themselves are reasonable or reflect the reality/complexity of utility operations. During incidents, technologies such as portals are increasingly being used to keep elected officials and other non-residential customers informed in an effective and efficient manner. Portals can also be used to allow communities to actually highlight specific restoration issues that may arise in the midst of an incident (for example, requesting that a specific intersection be restored due to traffic or safety concerns).

7.4.2. Findings

The communication plans relied upon during the Long Beach incidents are missing key components.

The communications plans of leading practice utilities typically include detailed guidelines, processes, procedures, roles and responsibilities, and supporting documentation (e.g., checklist, job aids) for internal and external communication in anticipation of or following an incident. They have an overarching all-hazards plan that describes how the Company communicates regardless of hazard along with sub-plans/modules that describe hazard-specific activities (such as estimated restoration times during an outage or engagement of mailing services following a data breach).

Also, these plans provide the requisite detail and direction to ensure that:

- Communication staff will be accounted for and available for work before, during, and after an incident;
- Team members understand their roles and responsibilities and key communication processes applicable during any incident;
- All channels of communication are up to date and ready for emergency communications;
- Business partners understand how the communication team will interact with them;
- The processes for developing and disseminating a communication strategy, gathering information, developing messaging, and disseminating messaging are easily understood and implemented in anticipation of and during incidents;
- Response personnel understand and support the role of the communications team to gather and communicate information to internal and external stakeholders; and
- The company uses a One Voice approach to communicate with all internal and external stakeholders.

SCE relied on two plans during the two Long Beach incidents: (1) All-Hazards Strategic Crisis Communication Plan; and (2) Public Information Officer and One Voice Team (OVT) Playbook. These two plans, combined, are missing details and process descriptions needed to support a successful communications effort during an incident, including:

- A description of the purpose/scope of each plan and how each will be updated and maintained;
- The organizational structure of the One Voice Team and how that team reports into and collaborates with other activated SCE teams, including the ES-IMT;
- A description of how the One Voice Team is notified and activated in response to an incident; and

- Detailed process descriptions for key communications responsibilities, including, but not limited to:
 - Developing, approving, and disseminating a communications strategy;
 - Developing, approving, and disseminating messaging;
 - Interacting with media, including press conferences; and
 - Using social media and other communications channels.

Also, the overall communications plan framework (i.e., how the All-Hazards Strategy Crisis Communication Plan and Playbook relate to each other and to SCE's other emergency response plans) is not clearly addressed in either plan.

A communications strategy was not established, leading to reactive and delayed messaging.

An essential element of an all-hazards communication plan is the development and dissemination of a clear and documented communications strategy to the entire response team (and affected executives). This strategy considers and describes the phase of the incident, information of general interest, specific information of regional interest, the objectives to be reached, the tools and tactics to be used, and the current status and priorities of the response. The strategy assures a directed approach to data gathering and dissemination that will result in a timely and consistent message to best meet stakeholder needs, keeping in mind that stakeholder groups have different needs and expectations. The strategy serves as a framework to assure a "One Voice" approach to emergency communications. The plan also details how frequently the strategy will be re-assessed and which communications (internal and external) or incident leadership personnel will be engaged in developing the strategy.

During the Long Beach incidents, SCE did not develop a communication strategy. The lack of strategy may have contributed to ineffective information sharing among response personnel, reactive (rather than proactive) messaging, and an over-reliance on fact-based messaging when facts and data were unavailable.

Information was not shared effectively.

There were several reasons for the lack of accurate data and facts, including a failure on the part of SCE's incident leadership to provide communications personnel (Public Information Officer/One Voice Team members and Liaison staff) with requested data and information on a timely basis through incident conference calls. These calls would have, at a minimum, apprised each functional group of restoration and incident status.

Leading practice utilities include conference call schedules, draft agendas, a list of required attendees, and call-in numbers in their response plans. SCE incident leadership did not conduct conference calls during LB1 (or did not adequately notify all response personnel of such). This was exacerbated by the decision to activate the IMT remotely, so the collaborative environment of a co-located team did not exist. Executives also

noted that during LB1, obtaining information (including related to functions within their blue-sky responsibilities) was difficult and that there was no consistent and comprehensive distribution list to keep them apprised of the response progress.

In addition to the lack of formal conference calls, data was being shared outside of the One Voice process and chain of command. For example, interviewees indicated that incident personnel shared key data with executives appearing on camera and/or interfacing with elected officials without providing that same information to communications personnel.

During an incident, many utilities have a team in place to support transparent communications and speak in “One Voice” by ensuring consistency in use of facts, figures, and messaging and by providing timely and accurate information for internal (employee) and external stakeholder communications. In addition, leading practice utilities have implemented databases where facts, figures, reports, and messages are posted and accessible to personnel with internal or external stakeholder communications responsibilities. Currently, SCE does not have a process in place to gather, validate and make available information and data needed by those with communications responsibilities during an incident.

The One Voice approach, as implemented, failed to meet large customer and government information needs/expectations.

An incident requires the affected company to mobilize en masse to respond in a safe and timely manner and to keep stakeholders apprised of its progress. Achieving One-Voice is key to a successful communications response because it:

- Reduces stakeholder confusion;
- Is the most efficient approach to developing and executing communications; and
- Enables the company to present its best image to stakeholders.

To achieve One Voice, leading practice companies establish a centralized communications group with responsibility for developing and releasing all messages, regardless of stakeholder type (internal or external). This group includes representatives from all externally and internally facing business groups to ensure that all stakeholders receive consistent information, understanding that the various stakeholder groups will have different information needs. It is responsible for gathering, fact-checking, and providing timely and accurate information for stakeholder communications.

While SCE has taken significant steps to create a centralized communication group (One Voice Team), the Company failed to meet all stakeholder expectations during Long Beach outages, due to a lack of data and because its approach failed to take into consideration the different information and data needs of diverse stakeholders. Also, the creation of a One Voice Team that is activated during incidents and the use of the same moniker for a blue-sky group creates unnecessary confusion.

The Agency Representative and Liaison functions did not meet partner expectations early in the incident.

During the initial hours of the outage, Long Beach public safety officials were attempting to make their own plans to address community needs and manage their own critical facilities (e.g., the City Jail) that were affected by the failure. These plans addressed how to manage darkened intersections at dusk, vulnerable populations in high rise apartments, fire suppression, and medical emergencies. These officials were frustrated with the lack of transparent communication by SCE. They found that SCE's AREPs were unable to provide an accurate picture of the scope of the outage or to share the SCE's restoration plan.

During blue-sky days, SCE's Local Public Affairs (LPA) program is designed to increase SCE's visibility in the community through a team of dedicated staff responsible for engaging stakeholders. During an incident, the LPA program provides staff to act as AREPs to state and local emergency operations centers. During non-emergency operations, the LPAs are widely lauded for their performance. Unfortunately, during the first 12-18 hours of the response to LB1, the AREPs were unable to obtain needed information from the Incident Commander (as noted above). This left the AREPs unable to provide sufficient operational information about the network or the network restoration plan to meet Long Beach city officials' public safety and public security planning needs. Once the ES-IMT was activated and the complexity of the response and the needs of the City were understood, SCE executives realized that the AREPs were unable to provide sufficient operational information and that executive presence was required. Senior operational executives were appropriately inserted to act as AREPs and provide the City actionable information. While this decision was out of process, it met the needs of the City.

Estimated Restoration Times were not provided or met.

Currently, SCE does not have an effective method for determining how many customers are out within the Long Beach network and, as a result, the Company does not have a process to develop an estimated restoration time. Based on a review of the communications and messaging released by the Company, it is apparent that no ERT was released for LB1 and that the ERT released for LB2 was not met. More specifically, during LB2, at approximately 5:00 a.m. on July 31, the One Voice Team released an ERT of July 31 at 6:00 p.m. At 5:30 a.m. on August 1, an ERT of the afternoon of August 1 was released. The last customer was restored on August 3.

Social media communications did not meet external stakeholders' expectations.

According to SCE's All-Hazards Strategic Crisis Communication Plan, SCE's guiding principles include "communicating proactively in a crisis - early, transparently, and truthfully. Avoid being perceived as dispassionate, detached or passive, which could

provoke critics to tell Edison's story before the Company or its allies.” At the same time, the plan requires that SCE “stick to confirmed facts and steps taken.” Efforts to fulfill these two guiding principles likely contributed to SCE’s social media communications not meeting stakeholder expectations. Specifically, during the first 24 hours of LB1, SCE posted about 16 tweets, with none issued between 10:00 p.m. and 8:30 a.m. on the following day. The tweets sent failed to provide any substantive information due to limited shared situational awareness other than changing customer out numbers (jumping from 2,000 to 4,000 to approximately 2,700 to approximately 3,200). At 4:36 p.m., a tweet was released indicating that somewhere between 200 and 2,700 customers may have been without power.

7.4.3. Recommendations

COM-1: Develop a comprehensive crisis communications plan, plan framework, modules, and associated documentation to address hazards, threats, and risks that SCE faces.

Enhancements to SCE’s current communications plans should include, but not be limited to:

- A description of how the plans integrate with other SCE response and communications plans;
- Communication strategies depending on various incident type and size;
- An incident communications organizational structure; and
- Detailed process descriptions for key communications responsibilities, including, but not limited to:
 - Developing, approving, and disseminating a communications strategy;
 - Developing, approving, and disseminating messaging;
 - Interacting with media, including press conferences; and
 - Utilizing social media and other communications channels.

The plans should clearly assign responsibility for developing a communications strategy during an event and describe the approach used and processes undertaken to communicate during all types of hazards. Sub-plans or modules should address specifics related to different hazards, such as legal requirements related to notifying customers of a data breach. SCE should develop and implement this communications plan framework and associated plans.

COM-2: Enhance the One Voice process to account for different stakeholder needs.

As noted previously, stakeholders have variety of information needs and expectations. This does not mean that SCE should abandon the One Voice approach. Rather, SCE should develop processes, tools, and procedures that consider these differences. More specifically, SCE should create a team responsible for gathering, vetting, and uploading

facts and data and consider creating a database, or similar tool, where vetted and approved data and messaging can be stored and accessed readily. Information in the database can be filed or tagged to indicate where and with whom it may be shared, enabling fulfillment of multiple stakeholder needs.

COM-3: In developing the communications strategy, consider the need to provide stakeholders and response partners with information beyond “confirmed facts.”

The Long Beach communications were hampered, in part, due to an over-reliance on fact-based communications, where no hard facts/data existed due to the nature of the incident. In the absence of facts, SCE provided insufficient information through its social media and other channels. Once the dearth of facts was clear, SCE should have revised its communication strategy to include tactics for developing and disseminating educational and informative messaging – aimed at educating its stakeholders on the nature of networks and the complexities associated with underground network restorations.

Further, SCE should undertake training with agencies that it may interact with during a response. Such training will provide personnel with an opportunity to understand response partner perspectives and needs before the incident and to better manage difficult situations. Finally, the Incident Commanders and Liaison Officers must understand their roles in ensuring the quality of communication with partners and other external stakeholders.

COM-4: Formalize the information sharing and vetting process and implement a database/portal.

SCE should continue implementation and enhancement of its web-based portal for elected official/community access to approved messaging and information. Users and SCE need to agree on the objectives of the portal, how information submitted will be addressed, and how the information in the portal may be shared.

COM-5: Enhance executive distribution lists to ensure executives are apprised of the incident status and response progress.

Executives not engaged in an official capacity during an incident still may need to be apprised of the status of the incident, including any key data, and whether any functions over which he or she has responsibility in blue-sky conditions are affected by the response. Therefore, distribution lists should be established to ensure that executives are provided response-related information prior to its public release.

COM-6: Enhance process for developing and releasing ERTs.

The SCE ERT process should be enhanced in several ways:

- Develop and implement a mechanism to evaluate the accuracy of ERTs and conduct post-incident audits;
- Impose goals for releasing ERTs after the start of an outage, based on incident size and ERT granularity. These ERT goals should be communicated pre-incident to media and customers so that external stakeholders have reasonable expectations about when they will receive an ERT;
- Assign accountability for accurate and timely ERTs to a single role and ensure that the Public Information Officer, who must meet established goals for information release, has information in time to meet deadlines; and
- Establish an “ERT Monitor” position, reporting to the Incident Commander or Planning Section Chief, with responsibility for monitoring ERT status and notifying his/her Event Supervisor of impending expirations or the need to revise the ERT.

COM-7: Assess communication and partnership preparedness and response models.

SCE is currently reorganizing its Local Public Affairs and Corporate Communications organizations. These reorganizations have taken place since the July incidents. The Local Public Affairs organization already has developed a strategy to adapt its service delivery model to be more strategic in its stakeholder engagement on a day-to-day basis. During future incidents, LPA will no longer be able to provide its historical level of service and will have to rely more on staff with operational experience to fill AREP positions. It will expect more engagement by T&D District Managers, specifically expecting them to engage in key relationship management rather than relying predominately on the LPA managers.

Corporate Communications also is in the midst of a reorganization and will have to conduct a similar assessment of its service delivery model. Both LPA and Corporate Communications should assess their preparedness and response capabilities within the new service delivery models. Corporate Communications should look to create a strong emergency and crisis communication capability within the organization, reaching out to qualified personnel outside of Corporate Communications to staff response roles. It should look to enhance its response capabilities and processes based on the future model.

In coordination with EPP-8, LPA and Corporate Communications should work with Business Resiliency to create a Communication and Partnership Strategic Model for Emergencies. Currently, SCE is leading a Public-Private Lifelines Council. Through this council and its engagement of the state and local emergency management agencies, SCE should create, circulate and publish a strategy document that outlines how SCE will communicate with stakeholders during routine and catastrophic emergencies. In routine emergencies, SCE may communicate directly with small businesses, communities, and

customers, while in catastrophic emergencies SCE may rely on county, state, and city EOCs and their Emergency Support Functions.

7.4.4. Implementation Factors

Table 10: Communications Recommendations

Number	Recommendation	Value	Ease of Implementation	Implementation Timeframe
COM-1	Develop a Comprehensive Crisis Communications Plan, Plan Framework, Modules, and Associated Processes to Address Hazards, Threats, and Risks that SCE Faces	High	Difficult	Mid-term
COM-2	Enhance the One Voice Process to Account for Different Stakeholder Needs	High	Difficult	Mid-term
COM-3	In Developing the Communications Strategy, Consider the Need to Provide Stakeholders and Response Partners with Information Beyond “Confirmed Facts”	Moderate	Easy	Short-term
COM-4	Formalize the Information Sharing and Vetting Process and Implement a Database/Portal	High	Difficult	Mid-term
COM-5	Enhance Executive Distribution Lists to Ensure Executives are Apprised of the Incident Situation and Response Progress	Moderate	Easy	Short-term
COM-6	Enhance Process for Developing and Releasing ERTs	Moderate	Moderate	Mid-term
COM-7	Assess Communication and Partnership Preparedness and Response Models	High	Moderate	Immediate

7.5. Information Technology and Operational Technology (ITOT)

7.5.1. Overview

While information and operational technologies serve different purposes for utilities, together they support responders in operating and restoring electrical systems. Both IT and OT systems support the acquisition of information, but OT is different in that it also supports the operation of the electric systems.

Each utility will classify IT and OT slightly differently and give responsibility for the operation and maintenance of such systems to different Operating Units. Broadly speaking, IT systems generally include administrative software applications such as SAP, enterprise resource planning systems, Microsoft Office Suite, engineering design applications, website information, and other software and hardware systems that

support general transfer of information. OT consist of the operational software, including the Outage Management System (OMS), Supervisory Control and Data Acquisition (SCADA) systems, Geographic Information Systems (GIS), Advanced Metering Infrastructure (AMI), and other hardware and software systems that support the operation of a utility's energy systems. There are a number of IT and OT systems that support decision makers during outages. At SCE, these systems include OMS and AMI. Systems that display this information to the public or decision makers include the Outage Map (public) and WebEOC (SCE) on the front end.

Leading up to and during the Long Beach failures, operational technologies did not support decision makers at Lighthipe or in the field. Furthermore, voltage information, which was available to decision makers before the failure, was not used to identify potential problems on the network. Back-end systems highlighted below will need attention to improve information accuracy and decrease lags in data accuracy from the field to front-end user interfaces such as the Outage Map or WebEOC. SCE will need to determine, in coordination with its stakeholders and regulators, the level of investment needed to provide more accurate information to its partners in the public sector and its customers.

7.5.2. Findings

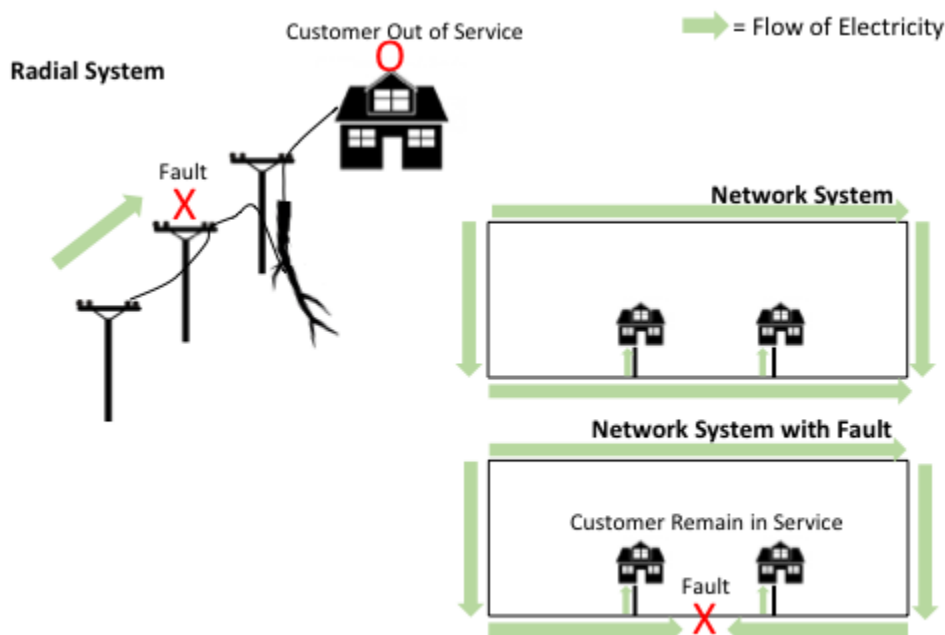
The Outage Management System is not designed for or capable of providing accurate customer outage information for the underground network system.

Across the electric utility industry, OMS is not readily capable of providing accurate information on the status of customer outages for underground networks. Typical outage management systems identify customer outages on radial systems, because customers are tied to a single device or span of wire and algorithms can predict that when a failure occurs to a piece of equipment, a specific customer is out. In a network system, however, OMS is incapable of providing accurate customer outage information because when a failure occurs, the network re-routes power from a different part of the system to continue to provide power to the customer.

During the Long Beach outages, SCE personnel realized that OMS was unable to provide accurate customer counts. As discussed in Section 4, underground secondary networks are essentially pools of electricity rather than arteries, which are typical of overhead radial circuits. Therefore, networks can feed electricity to a customer from multiple paths, making a prediction of which customer is out using OMS logic difficult or impossible.

Figure 9: OMS Example shows how OMS can predict that there is a customer out due to a fault in a radial system. In a network failure, however, even though OMS receives the information that a circuit, device, or section of cable is interrupted, it cannot predict which customers are out, since the customers may still be served through another circuit, device, or a span of cable.

Figure 9: OMS Example



During LB1, when both overhead and underground circuits were affected, SCE personnel estimated the customer counts based on a number of sources, including:

- Information available from AMI;
- Information derived from OMS;
- Customer service;
- Network maps; and
- Nighttime field patrols.

The AMI system is not designed to provide real-time outage information.

With support from the California Public Utility Commission (CPUC), SCE was an early adopter of AMI technology. The Edison SmartConnect™ project (AMI's trade name at SCE) was implemented with energy efficiency and reliability in mind. While it was also designed to provide real-time customer outage information to the Company, the AMI design basis was single customer outages and not large-scale outages. Despite upgrades to the AMI system, communication software, the communication backbone, and the Meter Data Management System (MDMS) used by SCE have limited capability to provide real-time outage information during certain large-scale outages.

Voltage Monitoring

In the 2011 windstorm, AMI had limited functionality and was unable to detect low voltages on the meter. In the past three years, SCE's AMI has undergone a significant

software upgrade to provide more functionality to the Company, specifically energy efficiency and maintenance information. Before the Long Beach failures, information was available on low voltages, but it does not appear that SCE identified these voltage abnormalities.

AMI Communication and Backbone Design

The AMI meters are designed to communicate in a self-healing peer-to-peer network, meaning that a group of meters will develop their own path of communication using groups of approximately 500 meters. They will communicate routine information daily from one meter to another through a daisy chain. The last meter in the peer-to-peer group will then communicate to the cellular backbone, which will in turn pass information from all 500 meters to the MDMS. If the last meter in that chain is unable to communicate to the backbone, either because it has no current or because the backbone is not available, it will attempt to communicate again in two hours. If the communication is not re-established within two hours, it will try to rebuild or heal the peer-to-peer network, which could take several hours, sometimes up to 24 hours.

The cellular background or Wide Area Network was optimized for cost savings and was not designed to have either significant overlap in its coverage of the peer-to-peer network or be without power for more than a few hours. If the cellular towers are without power, the cellular backbone is without power for more than four hours, the battery back-ups fail prematurely, or the peer-to-peer network cannot find a cellular node, then the AMI data cannot be transmitted to the MDMS.

In summary, the AMI system was designed for routine, isolated outages and does not currently have the capability to provide real-time accurate AMI data reliably during a large-scale outage.

AMI During the Long Beach Failure

During the Long Beach failures, the peer-to-peer network and/or the communication backbone did not allow SCE to obtain reliable real-time meter information. This limited capability does not allow SCE to use AMI to gather necessary intelligence during other large scale outages, such as those caused by windstorms, earthquakes, and the like. Until the Company is authorized to invest in upgrades to both the meter software and the communication backbone, AMI will not be able to provide either real-time customer outage information to decision makers or accurate customer counts during an emergency.

The Local Public Affairs mobile application to access key outage data had not yet been deployed.

The Local Public Affairs mobile application for state and local governments could have supported better situational awareness for local officials if it had been deployed before the Long Beach outages. Since the Long Beach outages, the mobile application has been deployed to select state and local stakeholders as part of a beta release. While it is an important tool and should answer some stakeholder needs, it will not replace the need for SCE to provide operational information to select public agencies through the Liaison and Agency Representative process.

Figure 10: Screenshot of LPA App



7.5.1. Recommendations

ITOT-1: Ensure that network outages are part of the design basis in the next release of OMS.

As SCE prepares to deploy its next generation outage management system over the next few years, it should ensure that its network is considered in the design of the OMS.

Where possible, OMS should be able to reconcile the status of transformers on the network and provide system operators and other decision makers with logical status of customer. The OMS network limitations should be well-known to system operators and distribution personnel and they should be shared with Corporate Communications and Local Public Affairs staff. During an outage, these shortcomings should be explained to stakeholders so that they are able to manage public safety plans accordingly.

ITOT-2: Update the AMI capabilities for the networked area.

Given that accurate customer counts are more difficult for OMS to derive in networked electrical systems and that the current AMI does not allow for real-time status of AMI customers, SCE should pilot an OMS upgrade for the Long Beach network. This pilot should target upgrades to the OMS software, the MDMS, and the AMI communication backbone. As part of the pilot, SCE should evaluate the costs and benefits of solutions to the communication backbone to support more reliable communication between meters and the MDMS. This should include an evaluation of the distribution and resiliency of the cellular nodes used to communicate between the peer-to-peer network and the MDMS. In cases where the cellular network is not available due to cellular tower outages, SCE should conduct a cost-benefit analysis and provide alternate solutions (e.g., alternate communication pathways on other RF spectrum or mobile communication pathways via SCE vehicles). SCE should also review and update software capabilities for the peer-to-peer communication pathways on meters. This software upgrade should limit the time intervals it takes for meters to recreate communication pathways during outages, enabling faster data flow to decision makers.

ITOT-3: Update the AMI capabilities for the entire SCE service territory.

Pending the AMI upgrade pilot in Long Beach recommended under ITOT-2, SCE should coordinate with the CPUC to evaluate the cost-benefit of upgrades to its entire AMI system to increase the capacity needed to provide real-time meter data gathering during large-scale outages. The design basis for this upgrade should include large-scale outages where large, contiguous areas are damaged by winds or other natural hazards. Between OMS, the Energy Management System (EMS) (circuit breaker status), and upgraded AMI information, SCE should be able to obtain sufficient information to provide customers and stakeholders the status of a majority of its electrical system.

ITOT-4: Work with external stakeholders to affirm the LPA application's usefulness and update it as necessary.

The LPA app is a leading practice in the industry and, despite the fact that it was not available during the Long Beach outages, SCE should be commended for deploying a tool targeted at providing public officials with better information. Invariably, public officials will want more information than is available through an app, so a knowledgeable SCE agency representative will never be replaced by technology. With this in mind, SCE should work with Long Beach and other public sector and public safety officials to user test the LPA app, enhance it, and deploy a second iteration.

It is important to note that SCE's systems and the regulations, laws, and policies under which it operates do not enable SCE to share all available data on its system in real-time with outside parties. Therefore, stakeholders will have to work with SCE to obtain the available data required to make public safety and governmental decisions during an outage. This application should be updated with those requirements in mind.

7.5.2. Implementation Factors

Table 11: Information Technology and Operational Technology Recommendations

Number	Recommendation	Value	Ease of Implementation	Implementation Timeframe
ITOT-1	Ensure that Network Outages are Part of the Design Basis in the Next Release of OMS	Low	Difficult	Long-term
ITOT-2	Update the AMI Capabilities for the Networked Area (at a minimum)	High	Difficult	Long-term
ITOT-3	Update the AMI Capabilities for the entire SCE Service Territory	High	Difficult	Long(er)-term
ITOT-4	Work with External Stakeholders to Affirm the LPA Application's Usefulness and Update as Necessary	High	Moderate	Short Term

7.6. Corporate Culture (CC)

7.6.1. Overview

Culture is based on the shared attitudes, beliefs, and rules that have been developed or allowed to be developed, either formally or informally, over time, that employees consider to be valid. A corporate culture is evident in the way in which:

- The Company conducts its business and treats its customers, stakeholders, and employees;
- Personal expression and decision-making are implemented;
- Communication occurs up and down the organization; and
- Employees are engaged in common objectives.

Leadership has responsibility for reinforcing the type of culture that is desirable. In the absence of that leadership, tradition and informal processes will fill the void and may not reflect the desired attitudes of the leadership. Changing corporate culture is a process and takes time and investment, but that change is necessary in order to meet the needs and demands of customers.

A notable characteristic of many utility cultures is a loyal employee base with long-term, committed service. In many cases, utilities have multiple generations of the same families on their workforces. In addition, much of the work in a utility is functionally oriented, which can lead to formation of organizational siloes.

SCE's corporate culture both helped and hindered the response to the Long Beach incidents. In its approach to the Long Beach incidents, SCE showed that it responds to incidents with a siloed organization that is reluctant to surrender control to a broader/non-operational management entity that engages corporate-wide groups. Also, it is evident that SCE leadership's vision of the Company is not known by everyone involved in the response. Just as evident, however, is the staff's willingness to improve and to understand how it can make changes and learn from its past experiences.

7.6.2. Findings

SCE employees are fully engaged to improve performance, make necessary changes, and learn from experiences.

Davies Consulting completed 70 interviews of SCE employees and Long Beach officials. SCE also has completed its own After Action Review for each of the incidents, identifying opportunities for improvement, some of which were immediately implemented. In addition, SCE already has taken the initiative to make further improvements to its response strategies and organization. Finally, even though SCE has engaged its own process to learn from these experiences, it has been fully cooperative with the Davies Consulting effort. Interviewees have been truthful and candid in their responses, with some employees travelling for several hours, each way, in order to participate in the process. Throughout this effort, a spirit of cooperation and engagement in improving performance was evident. In several interviews, SCE employees asked for input as to how they *personally* could have improved their efforts, in addition to highlighting areas of improvement for the Company as a whole. In other meetings, SCE response personnel (openly and without regard to the potential impact on their positions at SCE) told senior executives that they had made decisions that they realized were not the best decisions, given the benefit of 20/20 hindsight. It is this aspect of its culture that will help SCE develop and integrate an effective corporate culture.

Existing vision and guiding principles do not fully articulate response priorities and may not express executive intent.

An emergency management and response vision should communicate clearly the company's approach to emergency management, including both response and preparedness. Through the process of developing a vision, senior management staff identify, from the company's perspective, the key elements to a successful incident. Then, through internal education campaigns, senior management ensures that all company staff understand the vision and its importance to the company. Having a well-communicated and understood vision prior to an incident helps company personnel understand and internalize that responding effectively to emergencies should be a core competency of the utility.

In its 2014 SCE Corporate Emergency Response Plan, the Company provides a vision and guiding principles to respond to emergencies. SCE's vision is to "... prepare for and respond to emergency incidents as one team using common protocols, terminology and organization that will integrate with the National Incident Management System (NIMS). SCE will partner with the communities they serve in preparing for and responding to emergency events." In this same document, SCE states its guiding principles, listed below.

- SCE will hold ourselves and our teammates accountable for working safely, protecting the public, and each other.

- This plan, the tactics, and the strategies contained in the Plan, are intended to be interpreted and applied by those with appropriate knowledge, training, and experience so that the Plan can flex to accommodate the unique needs of the incident.
- Criteria used to gauge the appropriate level of response are guidelines and are not a substitute for the judgment of personnel that have adequate experience, knowledge, and training to make decisions regarding the escalation or de-escalation of response activities.
- SCE will manage significant emergency incidents using ICS.
- To the extent practical, SCE will activate the plan, or elements of it, in preparation for managing predictable incidents such as weather events.
- The Incident Commander (IC) will establish incident objectives, with input from Command and General Staff members and, as practical, community stakeholders.
- When incident information is shared with customers, the media, elected officials, and regulators, SCE will provide the most accurate information and will speak with One Voice. To this end, the IC will approve all incident communications.
- Restoration of electric service may be only one component of larger public sector response efforts. The IC will, to the extent practical, consider the needs of public sector emergency response agencies and the communities SCE serves, when determining incident objectives.
- SCE will continually improve by critically evaluating our performance and incorporating lessons learned.
- SCE employees will prepare at home and at work because the communities SCE serves depend on us to respond regardless of the circumstances.

While these vision and guiding principles appear to be well-constructed and purposeful, their full implementation and follow-through remain to be completed. The vision and guiding principles define how SCE is to act and respond to an incident. A review of these statements and SCE's response to the Long Beach outages, indicates a gap between intention and action. For example, in SCE's response to the Long Beach incidents, there was a challenge to find resources willing and able to fulfill the roles in the ES-IMT. This resulted in some personnel travelling long distances to participate and work longer shifts than originally planned.

Through interviews of SCE employees, both directly and indirectly involved in the response and identified as members of the response organization, it is apparent that these principles are not well known and some are not fully integrated into the response culture. SCE employees are engaged in serving their customers and want to understand SCE's response identity so that they can successfully approach an incident.

Distribution Operations has a history and culture of handling incidents without recognizing that outages are community events.

As stated by the guiding principles, effective incident response recognizes the need for broader community involvement. The culture at SCE, and the utility industry in general, is that operational functions control every aspect of a response. It is important to understand and recognize that this narrow perspective does not address all stakeholder needs and is not a complete strategy. During the first Long Beach incident, SCE's T&D Operating Unit maintained control of SCE's efforts. Transition to the ES-IMT, especially in the first failure, was delayed with the activation of an ICS-lite response organization. The ICS-lite organization kept T&D in control of the response. The ES-IMT organization, while not activated, was attempting to gain situational awareness behind the scenes to be prepared to act if necessary. The ICS-lite structure, however, was not well-known or understood, and the ES-IMT participants were unsure of their role, lacked situational awareness, and were not engaged in any direct internal communications. The result of this decision was that SCE's broader community responsibility, transparency, and cooperation with its stakeholders was virtually non-existent at the outset of the incident. When the ES-IMT was officially activated, it was already operating at a disadvantage as external stakeholders had already reached their frustration point.

In interviews with SCE employees, it is widely regarded that the ICS-lite organizational decision was not the appropriate response to this incident. The Business Resiliency organization, in conjunction with the affected operational organization, determines the response to an incident.

Chain of command as defined by ICS was not always followed.

Over the last several years, SCE has been investing in improving the way it responds to incidents and emergencies by implementing ICS. This change is being made to better position SCE to address the increasing complexity of incidents and demands of customers, stakeholders, and regulators. SCE has acknowledged that its incident response needs to be broader in scope than its historical operations-only approach. However, the change to ICS and the resulting change to its corporate culture requires time to implement and mature.

As noted in Section 5.1, SCE's response to the Long Beach incidents, particularly LB1, provides several examples of gaps between SCE's approach to ICS in its documentation and in how it was used during the incident:

- In LB1, field operations were communicating directly with the Incident Commander and SCE executive leadership with inadequate engagement of the PIO or LNO within the ES-IMT;
- Involvement and participation by SCE leadership with the ES-IMT was seen as generally positive by participants as it showed their engagement and support; and

- Field personnel were receiving orders from both the ES-IMT and the field leadership and tended to disregard ES-IMT direction in favor of direction from field leadership. With the activation of the ES-IMT, field activities and strategies are to be determined from the ES-IMT, with input and involvement from the field.

7.6.3. Recommendations

CC-1: Fully endorse and communicate the emergency Management vision and guiding principles.

SCE's executive leadership should fully endorse the existing vision and guiding principles or create its own emergency response vision and guiding principles. Developing and sustaining a vision requires executive messaging and ownership to reinforce the way in which SCE integrates and carries out its emergency management as a fundamental element of its emergency response culture. The vision and guiding principle should message that SCE's incident response should be a *core competency*.

Each member of SCE's executive leadership team, along with leaders throughout the Company, should *be personally accountable for integrating emergency management into day-to-day corporate life*, ingraining these principles with SCE's corporate culture. While Business Resiliency's role is to ensure that the Company is focused on emergency preparedness and response, each Operating Unit and executive leader plays a part in raising the character by which SCE will respond to emergencies by asking questions, coaching employees, and ensuring that they, and their organization, are portraying and practicing the principles reflected in the vision and guiding principles. This approach will allow SCE to develop its corporate identity in response and to embed that identity into its corporate culture.

CC-2: SCE should consider assignment of individuals with broad experience to incident leadership positions.

As noted previously, SCE relied too heavily on its traditional approach and culture of assigning an operational individual to act as Incident Commander. This approach does not recognize the broader impact of an incident on the Company, the community, and stakeholders. To reinforce the development of a new corporate culture and ICS response processes as a new core competency, SCE executives and leaders need to be ever-mindful of how the response organization is functioning. To that end, SCE should build on its success with the Incident Support Team and identify and assign individuals with broad experiences to incident command positions, capable of collaborating with stakeholders while understanding the operational requirements of response.

CC-3: Continue to champion a cooperative and transparent relationship with its external stakeholders.

SCE has implemented a strategy that is transforming the way in which it responds to emergencies as a partner in the community and with a transparent after action process.

This strategy recognizes that SCE has a corporate responsibility to partner with external agencies, communicate with its customers, and ensure that its response considers more than the electric system, addressing community needs as well. This transformation benefits SCE, its customers, stakeholders, and regulators. It will be more successful and will sustain itself if it is done with the cooperation and support of SCE’s stakeholders.

Lessons learned from other industries demonstrate the value of an after action process, the willingness to openly share lessons learned, and the willingness to report and manage risks proactively and in a structured manner. The airline, transportation, pharmaceutical, chemical, and food supply industries rely on such positive behaviors, also displayed by SCE, to manage their risks. It is our belief that this culture of transparency, self-reflection, and willingness to share is the right approach.

7.6.4. Implementation Factors

Table 12: Corporate Culture Recommendations

Number	Recommendation	Value	Ease of Implementation	Implementation Timeframe
CC-1	Fully Endorse and Communicate the Emergency Management Vision and Guiding Principles	High	Easy	Immediate
CC-2	Assign Individuals with Broad Experience to Incident Leadership	High	Moderate	Immediate
CC-3	Continue to Champion a Cooperative and Transparent Relationship with its External Stakeholders	High	Moderate	Critical



strategies for complex organizations

Appendices

8. Appendices

8.1. Appendix A: Detailed Response Timeline

8.1.1. Long Beach 1

July 15 (Wednesday)

Network Status and Response Operations

The following is a detailed description of the timeline associated with the July 15 incident:

- At 3:07 p.m. on July 15, the FLOAT circuit opened automatically, de-energizing eight network protectors. Grid Operations attempted to close the circuit multiple times in order to energize the circuit. There was an increasing number of customer interruptions, peaking at 259 customers before the next circuit failed.
- At 3:32 p.m., the STEAM circuit failed, de-energizing an additional six network protectors, resulting in 14 out of 62 network protectors being out of service. At this point in the incident, there were approximately 2,284 customers without power.
- At 3:35 p.m., the Long Beach Fire Department dispatched its units to a reported smoking manhole at 429 West 3rd Street.
- From 3:51 – 3:53 p.m., customer outages increased to 2,408.
- At 3:59 p.m., the Long Beach Fire Department dispatched its units to a reported telephone pole with a manhole smoking beneath it at 4th and Virginia.
- At 4:01 p.m., Long Beach Fire received a report of a smoking manhole at 332 Magnolia Avenue.
- At 4:22 p.m., Grid Operations de-energized the CARGO circuit, removing three additional network protectors and causing severe low-voltage conditions on the network. Simultaneously, two additional fires in the vicinity of 9th and Pine streets occurred, triggering another Long Beach Fire Department response. Customer outages increased to 3,927.
- At approximately 4:30 p.m., following Company procedures, SCE's Grid Operations notified the Storm Manager of the incident. The Storm Manager then contacted Long Beach District Troublemakers (or Linemen) to ascertain details on the manhole fires and the outage.
- At 5:05 p.m., the Long Beach Fire Department responded to a report indicating smoke coming out of the base of a telephone pole at 930 Pacific Avenue.
- At 5:46 p.m., Long Beach Fire units were dispatched to a vault explosion at 9th and Pacific and 9th and Solana Court.
- At 6:20 p.m., the OCEAN circuit failed, de-energizing six additional network protectors, increasing the total number of out of service network protectors to 23 of the 62. Customers out of service increased from 4,736 to 4,928.

- Immediately thereafter, at 6:21 p.m., Grid Operational de-energized all of the remaining network circuits. Customer outages increased to 8,351.
- Precise customer counts were not available,⁴¹ but it was estimated at the time that there were approximately 5,000 customers without service as of 6:30 p.m. There were 4,928 customers out at 6:21 p.m. and by 6:30 p.m. the customer outages were 8,351. The discrepancy was likely due to the lag between when data was pulled and when information was released.
- At 7:04 p.m., Long Beach Fire dispatched crews to Pine Ave and Nardo Way for a vault fire, followed at 7:46 p.m. by two additional reports of smoking manholes.

The fact that there were additional vault fires on the network after 6:21 p.m., when all of the circuits were de-energized, indicates that the network was still energized. Indeed, the existence of additional network sections to the north of what was represented on maps, was not known by SCE personnel at this point in the response.

Activation and Complexity Analysis

The Watch Office notified the on-duty Business Resiliency Duty Manager at approximately 5:00 p.m. that there had been a vault explosion in downtown Long Beach and that several addresses at the Port of Long Beach may have been affected. Upon notification, the Business Resiliency Duty Manager tasked the Watch Office with identifying if the Port of Long Beach was among the approximately 4,000 customers without power. Ultimately, it was determined that the Port of Long Beach did not experience a sustained outage.

The Business Resiliency Duty Manager completed the complexity analysis shortly after 5:00 p.m. to help gauge the level of the response. The complexity analysis determined a score of 5, noting the following:

- Serious public or employee safety threats;
- Observed or potential for claims;
- First responder agencies involved;
- Media interest; and
- Political or regulatory interest or inquiries.

Incident Complexity scores between 3 and 7 equate to an SCE Incident Level of 2. According to the SCE Incident Levels, a Level 3 or above results in activation of the

⁴¹ Information available to decision makers at the time, from OMS, indicated approximately 3,300 customers without power.

Incident Management Team, the Incident Support Team, and the Emergency Operations Center. In an Incident Level 2, it is left to management discretion to activate.

At approximately 5:25 p.m., the Business Resiliency Duty Manager and the Storm Manager discussed the outage. During this discussion, the Business Resiliency Duty Manager and Storm Manager were unable to agree whether to activate the Incident Management Team.⁴² The Business Resiliency Duty Manager agreed to speak with the acting Grid Operations Director. Following that discussion and given that there was confidence that the outages would be resolved overnight, ICS-lite was used, with a Public Information Officer (PIO) and Agency Representative (AREP) activated at 6:00 p.m. The Storm Manager assumed the role of Incident Commander (IC). The IC activated an Operations Section Chief in Long Beach (Long Beach District Manager) and informed a Corporate Communications on-duty officer that there was an incident. There is lack of clarity as to whether the Incident Commander was informed that there was an AREP and PIO activated. Further, based upon different accounts, it is not clear whether the Long Beach District Manager was nominally the Operations Section Chief, or if he actually assumed the Operations Section Chief position.

The Officer-in-Charge (the corporate officer on-call for the enterprise) was notified via voice mail of the incident at 6:05 p.m. Following this notification, at 6:24 p.m., a “Critical Incident Report” was reviewed and released by the Watch Office at 6:36 p.m. Business Resiliency continued to monitor events overnight.

Communications

The July 15 Long Beach outage began at 3:07 p.m. According to SCE’s internal communications timeline, the following messaging was released on July 15:

- 4:51 p.m. – the Company indicated that approximately 2,000 customers were without power in Long Beach and that the Company was investigating;
- 5:05 p.m. – SCE released a safety reminder via Twitter;
- 5:08 p.m. – the Company updated its Twitter feed, posting that approximately 4,000 customers were without power due to the Long Beach failure;
- 5:27 p.m. – SCE tweeted that crews were working to restore power in Long Beach;
- 7:10 p.m. – SCE indicated that crews were assessing the Long Beach outage and that the Company would provide updates as they became available;
- 7:11 p.m. – messaging indicated that SCE crews would work through the evening to restore power to affected customers; and

⁴² Similar incidents had been managed by an ICS-lite approach, which was not defined in applicable plans or procedures, but which involved assigning the Storm Boss to monitor the incident remotely and using crews in the field and a public information officer or agency representative as needed.

- 9:55 p.m. – the Company retweeted a customer tweet thanking the Company for working hard to restore power.

According to SCE’s communications timeline, no additional messaging was released by the Company before the morning of July 16. In addition to the above, SCE’s Agency Representatives (AREPs) were activated and in place at Long Beach City’s EOC and the Long Beach Police Department’s Command Post by 6:00 p.m. on July 15.

Impact on Long Beach

The Long Beach Mayor, City officials, and citizens were not focused on the network failure but on the impacts of the failure. During the initial stages of the incident and in addition to managing the vault fires, Long Beach City officials were directly affected by:

- An outage to City Hall;
- An outage to the City jail;
- A partial outage to the Police Headquarters; and
- An outage affecting Fire Department Station 1.

Indirectly, public officials were responsible for managing:

- Darkened street lights, particularly thoroughfares from the I-710;
- Security in high-rise and multi-unit dwellings;
- Elevator rescues; and
- Vulnerable populations in high rises.

In addition, businesses in the Long Beach Downtown Business Improvement District were affected by the failure, including:

- Several downtown hotel outages;
- An outage at the convention center; and
- Outages at restaurants, bars and small businesses.

Long Beach City Perspective

Long Beach City Officials, in particular the Long Beach Public Safety leaders representing the Long Beach Police and Fire Departments as well as the Disaster Preparedness organization, were notified and activated. In the early hours of the incident on the afternoon of July 15, the Long Beach police activated its Department Operations Center (DOC) in its headquarters and SCE was able to assign an Agency Representative. Eventually, the Fire DOC and the Disaster Preparedness Emergency Operations Center were activated and staffed. Public safety officials had to make decisions on myriad public safety issues, including retaining police officers to staff traffic signals, patrol areas of town without electricity, and support vulnerable populations in high rise

communities. Having obtained insufficient information from the SCE AREP,⁴³ these public safety officials turned to SCE's field resources to obtain information and made staffing decisions assuming that a restoration would not occur overnight.

July 16 (Thursday)

Into the early hours of July 16, SCE personnel developed a restoration plan based on network maps from 2008. SCE planned to restore the network shortly before 8 a.m. and had confidence in their ability to achieve that objective.

Restoration Attempt

At approximately 4:00 a.m., SCE received reports of additional customer outages. At 5:00 a.m., the IC transferred command to the then on-duty Incident Commander at Lighthipe. Concerned about the potential impact on rush hour and additional outages before dawn, Long Beach City requested that SCE not bring the network up before daybreak since the restoration required de-energizing additional portions of the City. Both parties agreed that SCE would wait until after 9:00 a.m. An unsuccessful attempt to restore the network was made at approximately 12:25 p.m. Though switching instructions can be lengthy, it is not clear why there was a several hour delay between 9:00 a.m. restoration target and the attempt at restoration at 12:25 p.m.

Subsequent Response

By early afternoon on July 16, SCE leaders were aware of the complexity and magnitude of the network outage and executives were asked to respond to Long Beach to support Long Beach officials. Once in Long Beach, it was clear to the executives that the Long Beach City officials were not receiving information necessary to manage the City's response. SCE assigned a senior SCE executive as the AREP to the City, bringing substantial operational experience to the table and providing actionable information to city officials.

In the meantime, a decision was made to activate the entire ES-IMT at Lighthipe. According to a review of ICS forms, the ES IMT was fully activated at 3:30 p.m. The activation of the full ES-IMT brought additional personnel and a fresh set of eyes to the response. Additional rigor around response processes provided structure for decision making; and response personnel began to focus on key activities, such as creation of an Incident Action Plan. For the remainder of the day and into July 17, the Lighthipe ES-IMT, the Long Beach District War Room at the Long Beach Service Center, and crews in

⁴³ Early in the response, SCE's Liaison Officer was unable to reliably contact the Storm Boss or obtain an accurate picture of the events. This agency representative relayed frustration with the lack of information, which was making it impossible to understand the magnitude of the incident and the implications on public safety, to their executive.

the field continued to assess damage and develop a plan to restore the network. As it became clear that the network restoration was going to be an extended effort, Business Resiliency connected incident leadership and operational personnel to underground network experts at Consolidated Edison (ConEd) in New York City⁴⁴ and at Pacific Gas and Electric.

Outside of the electrical restoration, SCE decided to open a distribution site at 714 Pacific. The distribution site, which provided water, ice, and flashlights to the public, was only open for 2 hours.

Communications

On July 16, SCE proactively released sixteen tweets (or re-tweets), updated a newsroom story, and developed talking points for a press conference, increasing its social media and communications presence over the first day of the incident.

- 8:23 a.m. – SCE tweeted that “some customers in downtown Long Beach (DTLB) have had power restored overnight. As of 07:30 am, 2,677 customers remain affected by this incident;”
- A minute later, SCE indicated that it would be “testing the underground system later this morning. Working to further reduce the number of impacted customers/begin repairs;”
- 9:39 a.m. – SCE released a tweet indicating that customers in Long Beach could experience outages due to testing;
- 9:56 a.m. – “Crews Continue Repairs and Testing of Underground Systems in Downtown #LongBeach;”
- 11:50 a.m. – “UPDATE: As of 11 am, 3,194 #LongBeach customers continue to be impacted. Crews are continuing to minimize the outage impact;”
- 12:03 p.m. – SCE indicated that restoration efforts were ongoing;
- 1:13 p.m. – SCE reminded customers of the potential for temporary outages;
- 2:12 p.m. – the customer outages were amended to 3,035;
- 3:37 p.m. – a food safety message was provided; and
- 4:36 p.m. – customer outage numbers were revised to between 200 and 2,700

From 7:40 p.m. until midnight, SCE released one tweet re-iterating that crews were testing underground vaults and re-tweeted several messages from customers thanking the Company for restoring power.

⁴⁴ For the reader’s benefit, ConEd experienced an underground network failure in 2006 that was 20 times the size of the Long Beach network outage. The ConEd experts, however, were unable to significantly enhance the network restoration from afar.

July 17 (Friday)

By the early morning of July 17, the ES-IMT began to research the availability of generators to supply electricity to some of the large buildings affected by the failure. In addition, SCE personnel devised a plan to sectionalize the network to enable load to be brought back to sections of the network rather than the entire network at once. At some point during this effort to sectionalize the network, SCE personnel at Lighthipe and in the District recognized that they were using two different maps to manage their response. One map, from 2008, was being used at Lighthipe. The other map, being used at the “War Room” in the District, was dated 2012. Neither map showed the section of the network north of 7th street.⁴⁵

The following actions also took place on Friday:

- At 8:00 a.m., the customer support distribution site was re-opened at 714 Pacific and remained open until 4:00 p.m.;
- At 8:12 a.m., the ES-IMT realized that network customers were not connected to the Company’s Outage Management System (OMS) and that accurate customer counts were not possible;
- At 8:51 a.m., the network was cut into sections, restored, and the Watch Office reported, at 9 a.m. that there were approximately 3,942 customers remaining out of service;
- At 2:00 p.m., SCE opened a customer support distribution site at Cesar Chavez Park and supplied the Red Cross site at 240 Chestnut with ice, water, and flashlights. The 240 Chestnut Site remained open until 4:00 p.m., while the Cesar Chavez Park customer support distribution site remained open until 10:00 p.m.; and
- At approximately 8:50 p.m., SCE was able to restore approximately 5,000 of the 6,100 customers that were out of service.

In addition, SCE increased its social media presence on July 17, releasing (or re-tweeting) approximately 30 tweets and updating an online Newsroom story. The tweets focused on: SCE crews were continuing to work on the restoration; locations for flashlight, ice, and water distribution centers and shelters; locations of generators; safety messages; and re-tweets of thanks from customers.

July 18 (Saturday)

The following key milestones were achieved on July 18:

⁴⁵ A comparison of the differences in the two network maps indicates that the differences between the two maps did not have a material effect on the restoration.

- Shortly after midnight, the number of customers without electricity dropped from 1,000 to approximately 600;
- At 8:00 a.m., the customer support Distribution site was reopened at Cesar Chavez Park and remained open until 10:00 p.m. when it closed for the last time; and
- By 2:00 p.m., customer outages dropped to 148, and around the same time the Long Beach EOC and Police Department Operations Center (DOC) closed.

July 19 (Sunday)

At 12:23 p.m., the service to Long Beach Police Department was switched from generator to network power and customer outages dropped below 100.

July 20 (Monday)

The last customers were restored at 3:34 p.m. At 2:00 p.m., the ES-IMT demobilized and transferred responsibility of the incident to the Storm Manager.

8.1.2. Long Beach 2

July 30 (Thursday)

At approximately 4:30 p.m. on July 30, an outage in downtown Long Beach was reported to SCE affecting a portion of the same area that was affected during the July 15 incident.

- At 3:49 p.m. there was a spike in customer outages plateauing at 56 customers for nearly an hour.
- At 4:33 p.m., the Long Beach Fire Department received information about a vault fire at 10th and Pacific avenues, possibly 10th and Pine.
- At 4:44 p.m. customer outages increase to 567 customers. At 5:14 p.m., the customer outages increase to a count of 893.
- At 4:50 p.m., SCE's Watch Office sent a Critical Incident Report to Company leaders notifying them of the incident.
- At 5:14 p.m., three substations (Seabright, Cherry, and State Street) were proactively de-energized to allow SCE to investigate the outage. SCE's AMI data indicates the peak customer outage number for this second incident to be 17,532.
- At 5:40 p.m., SCE activated its IST and ES-IMT based on the results of the Incident Complexity Analysis completed by Business Resiliency. Both teams were operational at SCE's EOC and Lighthipe by 7:00 p.m.
- At 7:43 p.m., circuits were energized restoring power to all but 1237 customers
- At 7:50 p.m., SCE's Agency Representatives and the IST PIO were in place at the Long Beach EOC.
- At 8:00 p.m., the City of Long Beach and SCE held a joint press conference.

- At 9:00 p.m., SCE opened a distribution site at Cesar Chavez Park Community Center, providing water, ice, and flashlights.

July 31 (Friday)

- At 5:00 a.m., SCE communicated that power would be restored by 6:00 p.m. on July 31 unless additional problems were found. SCE AMI data shows that 239 customers remained without power at 5:08 a.m.
- At 6:00 a.m., the City of Long Beach demobilized their EOC, and the SCE Agency Representative was released.
- At 6:00 p.m., SCE communicated that power would be restored to most of the over 200 customers without electricity by 10:00 p.m., and that approximately 60 customers would remain without power overnight.

SCE continued to operate a customer distribution site at Cesar Chavez Park Community Center during the day. It also established a customer support distribution site on Locust Avenue near affected apartment buildings. At the end of the day, SCE revised its ERT to indicate that there would be a handful of customers who would remain without power through the night. Field personnel completed all but four structure inspections (the four not completed were a result of access issues). These inspections found no critical risks and lower priority repair orders were put into OMS to schedule work.

August 1 (Saturday)

- At 5:00 a.m., SCE reported less than 70 customers without power. The AMI data shows that number to be 18 customers. SCE was using 10 temporary generators to supply power while they worked to reconnect customers to the grid.
- At 5:30 a.m., SCE communicated that all customers were expected to be restored by the afternoon.
- At 4:00 p.m., customer distribution sites at Cesar Chavez Park and Locust Avenue closed.

Later in the afternoon (5:00 p.m.), SCE communicated that all customers were reconnected to power, either through the grid or temporary generators. SCE crews continued to make repairs and test the underground network systems and began transitioning customers off generators to the electric network during the evening and morning hours. At 7:00 p.m., SCE demobilized its IST and transitioned responsibility of the incident to the ES-IMT.

August 2 (Sunday)

At 8:45 p.m., all customers that were on temporary generators were connected to the electrical grid and at 9:00 p.m., the customer support distribution site at 925 Locust Avenue closed. There were two customers without service according to AMI data but it is not clear that this information was available to SCE decision makers at the time.

August 3 (Monday)

At 1:30 a.m., SCE ES-IMT was demobilized, and SCE transitioned to normal operations.

The last customer that experiences a prolonged outage as part of the network failure was restored at 3:18 p.m.

8.2. Appendix B: Glossary⁴⁶

Amperage – a term used to describe the number of electrons moving past a fixed point in a conductor in one second. Current is measured in units called amperes or amps.

Advanced Metering Infrastructure (AMI) – an integrated system of smart meters, communications networks, and data management systems that enables two-way communication between utilities and customers.

Bus – a busbar (also spelled bus bar, or sometimes as buss bar or bussbar, with the term *bus* being a contraction of the Latin *omnibus*, "for all") is a metallic strip or bar that conducts electricity within a switchboard, distribution board, substation, battery bank, or other electrical apparatus. Its main purpose is to conduct a substantial current of electricity, and not to function as a structural member.

Cable - a cable is a group of one or more electrical conductors, used for transmission of electricity https://en.wikipedia.org/wiki/Electric_power. Cables may be underground (as in a network) or overhead. Conductor is generally described as wire in overhead systems but cable in underground systems.

Cascading failure – a cascading failure is a failure in a system of interconnected parts in which the failure of a part can trigger the failure of successive parts. Such a failure may happen in many types of systems, including power transmission and distribution.

Circuit – an electric circuit is a path in which electrons from a voltage or current source flow. For purposes of discussing T&D systems, a circuit is a portion of the distribution system that connects a substation to the end-user. It most typically consists of three-phase and single-phase sections, which are described below. Note that circuit and feeder can be used to describe medium voltage lines.

Conductor – the material through which electric current flows – may also be known as wire or cable. Conductor is generally described as wire in overhead systems but cable in underground systems.

Conduit – a metal, plastic, fiber, or fired clay rigid or flexible tube used to protect and route electrical wiring.

Current – a flow of electric charge. In electric circuits this charge is often carried by moving electrons in a wire. It can also be carried by ions in an electrolyte, or by both ions and electrons such as in a plasma.

Energized-via-backfeed – a network protector is designed to open automatically when the feeder that is supplying its associated transformer is de-energized. When a network protector is closed manually and is non-operational, it will not open when its associated

⁴⁶ The definitions included above are compiled from Davies Consulting subject matter expertise combined with online sources, including www.google.com and www.wikipedia.org.

feeder is de-energized. Thus, in this type of situation, a network protector that remains closed when its associated feeder is de-energized will provide an electrical path from the secondary mains of the network back through the network protector, its associated transformer and into the “de-energized feeder.” And if there is a fault on the feeder, which is why it was automatically de-energized through a relay operation at the circuit breaker, the secondary grid through the electric path previously described will attempt to supply power to the fault – and the feeder remains energized-via-backfeed.

Feeder – medium-voltage lines used to distribute *electric* power from a substation to consumers or to smaller substations.⁴⁷

Fault – a fault or fault current is any abnormal electric current. For example, a short circuit is a fault in which current bypasses the normal load. An open-circuit fault occurs if a circuit is interrupted by some failure.

First Contingency – the condition or state of the network which is one scenarios away from design state (e.g., the loss of a significant feeder would be the first contingency, the loss of a second significant feeder would be the second contingency.)

First contingency design – a first contingency design means that any single feeder can be out of service in the network without any disruption of service to customers.

Incident Action Plan – an incident action plan (IAP) formally documents incident goals, operational period objectives, and the response strategy defined by incident command during response planning. It contains general tactics to achieve goals and objectives within the overall strategy, while providing important information on event and response parameters.⁴⁸

Incident Command System – a standardized approach to the command, control, and coordination of emergency response providing a common hierarchy within which responders from multiple agencies can be effective.

Incident Management Team – a grouping of individuals (typically organized under ICS) responding to an incident.

Load – an electrical load is an electrical component or portion of a circuit that consumes electric power.

⁴⁷ The Free Dictionary, Feeder at <http://www.thefreedictionary.com/feeder>, accessed on October 19, 2015

⁴⁸ U.S. Department of Health and Human Services, Public Health Emergency, What Is An Incident Action Plan, at <http://www.phe.gov/preparedness/planning/mscc/handbook/pages/appendixc.aspx>, accessed on October 19, 2015.

Load pocket – a load pocket is an area where there is insufficient capability to reliably supply 100% of the electric load without relying on additional capacity that is physically located within that area. It is the result of high concentrations of intensive power use inevitable in a big city and limitations, known as constraints, on the system that limit the ability of load to be served by generating resources located remotely.⁴⁹

Manhole – a small covered opening to allow a person to enter, especially an opening in a city street leading to a sewer and network components.

N-1 – a single bus, feeder, or network protector can be out of service and the system should operate at peak load without experiencing any service quality problems.

Network protector – a type of electric protective device used in electricity distribution systems. The network protector automatically disconnects its associated power transformer from the secondary network when the power starts flowing in reverse direction.

Network protector fuse – network protector fuses provide backup protection for clearing faults on the primary feeder in the unlikely event the protector fails to operate.

Outage Management System (OMS) – a computer system used by operators of electric distribution systems to assist in restoration of power.

Primary cable – the portion of underground conductor between the substation and the transformer to the secondary network.

Radial – the type of electrical configuration in which there is one path of electricity from the substation to the customer.

Relay (noun) – a relay is a switch that is either closed or open based upon the level of amperage that is being utilized in a certain segment of a circuit or pieces of equipment. The status of a relay activates other components in the network to operate; usually a primary circuit breaker or a network protector.

Relay (verb) – the automatic opening of a switch from the closed position to the open position.

Second contingency – the condition or state of the network which is two scenarios away from design state (e.g., the loss of a significant feeder would be the first contingency, the loss of a second significant feeder would be the second contingency.)

Secondary cable – the portion of underground conductor between the network protector and the customer.

⁴⁹ Astoria Generating, FAQ, What is a Load Pocket, at <https://www.uspowergen.com/2008/02/27/what-is-a-load-pocket/>, accessed on October 19, 2015.

Secondary network – the underground network that supplies low voltage (120-240V) from the network protector via multiple paths or cables to the customer.

Single-phase – In electrical engineering, single-phase electric power is the distribution of alternating current electric power using a system in which all the voltages of the supply vary in unison.

Splice – the joining of wires.

Spot Network – a spot network supplies a specific load in the network, such as a single large building, and does not provide any secondary voltage support for the secondary portion of the underground secondary network. For purposes of discussing the underground secondary network, it is important to note that “spot networks” do not contribute to providing secondary voltage stability in the secondary portion of the underground secondary network.

Three-phase – a three-phase circuit consists of three different sine wave current flows, different in phase by 120 degrees from each other.

Transformer – an apparatus for reducing or increasing the voltage of an alternating current.

Underground network – the primary and secondary network that is underground.

Voltage – voltage, also called *electromotive force*, is a quantitative expression of the potential difference in charge between two points in an electrical field. The greater the voltage, the greater the flow of electrical current (that is, the quantity of charge carriers that pass a fixed point per unit of time) through a conducting or semiconducting medium for a given resistance to the flow.⁵⁰

Wire – a structure used in [electric power transmission](#) and [distribution](#) to transmit electrical energy. May also be known as a cable or conductor. Conductor is generally described as wire in overhead systems but cable in underground systems.

⁵⁰ WhatIs.com, Voltage, at <http://whatis.techtarget.com/definition/voltage>, accessed on October 19, 2015.

8.4. Appendix C: Interviewee Roles

As noted in the body of this report, Davies Consulting conducted more than seventy interviews with SCE staff and external stakeholders. Individuals interviewed from SCE included those filling the roles and positions listed below (please note that each position may have had multiple individuals filling the role during each incident).

8.4.1. SCE Interviews by Position

Response roles

- Incident Commander (IST)
- Public Information Officer (IST)
- Liaison (IST)
- Incident Commander (IMT)
- Operations Chief (IMT)
- Liaison (IMT) and Agency Representatives
- Public Information Officer (IMT)
- Planning Chief (IMT)
- Business Resiliency Advisor⁵¹

Other

- SCE executive leadership
- Regional Manager
- Distribution AMI
- Grid Control Center (GCC) staff
- Long Beach Operations Supervisor
- Substation Manager
- Substation Supervisor
- Call Center staff
- Crew Supervisor
- Corporate Communications
- Business Accounts
- Underground Network Engineer
- Storm Manager

8.4.2. External Stakeholders

- City Manager, Long Beach
- Chief of Staff, Long Beach Mayor

⁵¹ Not a technical response role but part of the response organization

- Chief of Staff, Vice Mayor
- Chief of Staff, City Councilor
- Public Information Officer, Long Beach
- Deputy Fire Chief and Fire Marshall, Long Beach
- EOC Director, Long Beach
- Commander, Long Beach Police
- Senior Vice President, Long Beach Chamber of Commerce
- President and CEO, Downtown Long Beach Business Improvement District

8.5. Appendix D: Davies Consulting Qualifications

Davies Consulting is an industry leader in utility emergency management. The Company helps utilities throughout North America to continuously improve their emergency response with an all-hazards approach (e.g., weather outages, cyber incidents, infectious disease, system failures, workplace violence, and hostile intruder incidents), enabling utilities to expedite restoration of electrical systems and essential services, and improve cooperation among internal and external stakeholders.

- Davies Consulting experts apply 25 years of experience in power delivery system preparedness, incident and crisis communication, and operational improvement to:
 - Assess program performance using metrics that are based on industry leading practices and Federal Emergency Management Administration (FEMA) guidelines;
 - Identify opportunities to improve preparedness, response processes, and incident communications; and
 - Implement leading practices to ensure effective emergency response.
- The Davies Consulting team includes former utility executives with expertise in utility operations, networks, risk and emergency management, regulatory proceedings, communications, and engineering with many decades of experience assessing and improving utility emergency response planning. This experienced team:
 - Conducts in-depth reviews of existing emergency management programs, including benchmarking against leading practices; and
 - Develops new emergency response programs for the full range of commodities and utility operating units.
- Davies Consulting has conducted more than 40 separate engagements related to utility emergency preparedness, planning, and response, Incident Command System (ICS) implementation, regulatory proceedings, change management, and operational improvement. By improving emergency planning and performance, developing and facilitating training and exercises, and conducting evaluation/results reporting, Davies Consulting helps utilities:
 - Scale their responses to address incidents of any size;
 - Communicate effectively with customers during incidents; and
 - Efficiently restore power to customers.
- Davies Consulting has conducted in-depth assessment studies of underground secondary networks at multiple utilities, identifying and prioritizing risks, recommending and implementing mitigation strategies, and enhancing incident response plans.

The firm brings together utility experience, decision analytics, and process expertise to help utilities break down silos and integrate innovation for long-term, positive results.

8.6. *Appendix E: Network Maps*

(Appendix E Redacted)