GRIDBRIGHT®

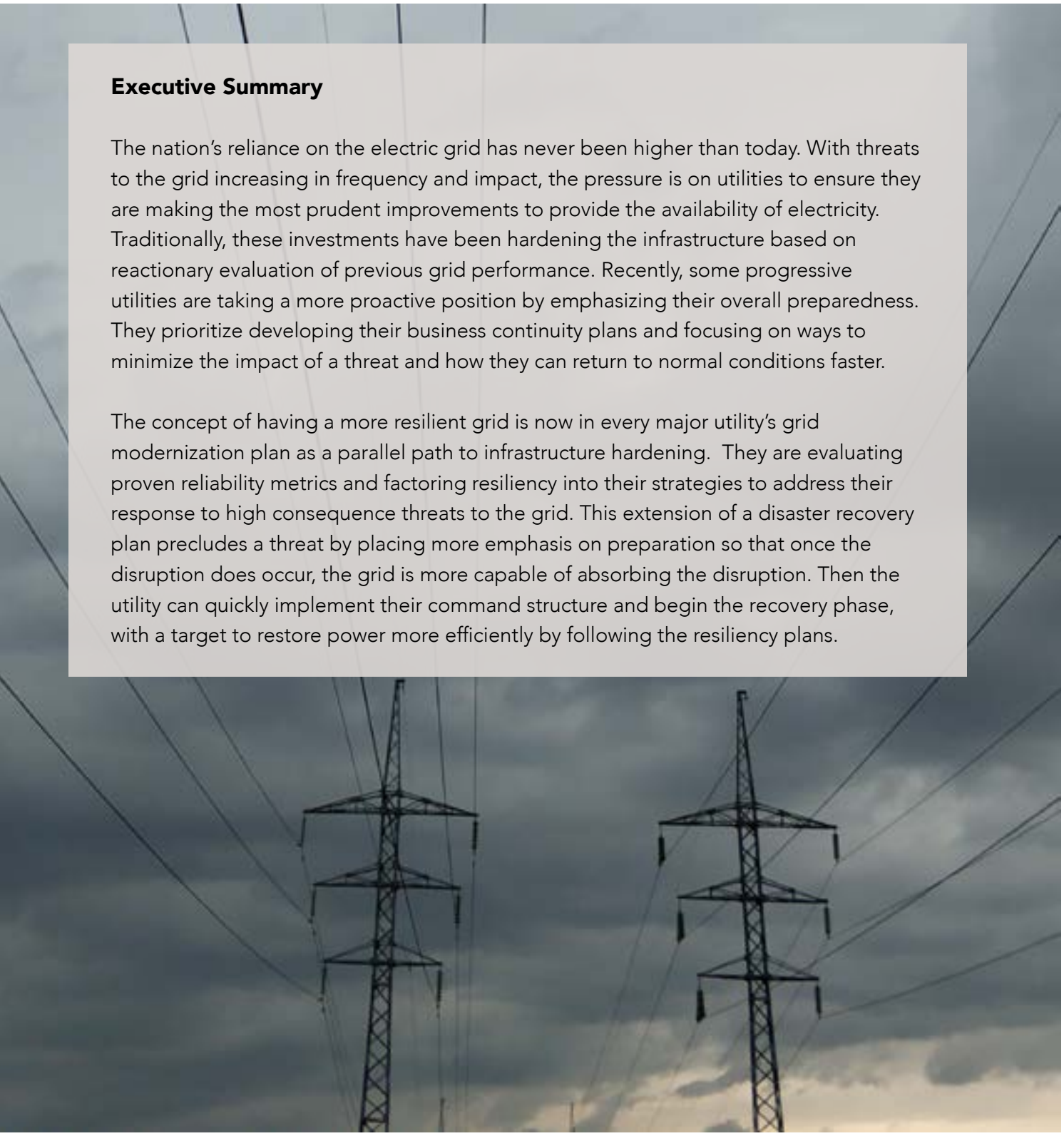
Secure and Sustainable Grid Integration

IMPROVING GRID RESILIENCE THROUGH SITUATIONAL AWARENESS

How using a common operating picture can improve situational awareness and lead to faster and more informed decision-making during threats to the electric grid.

August 1, 2022

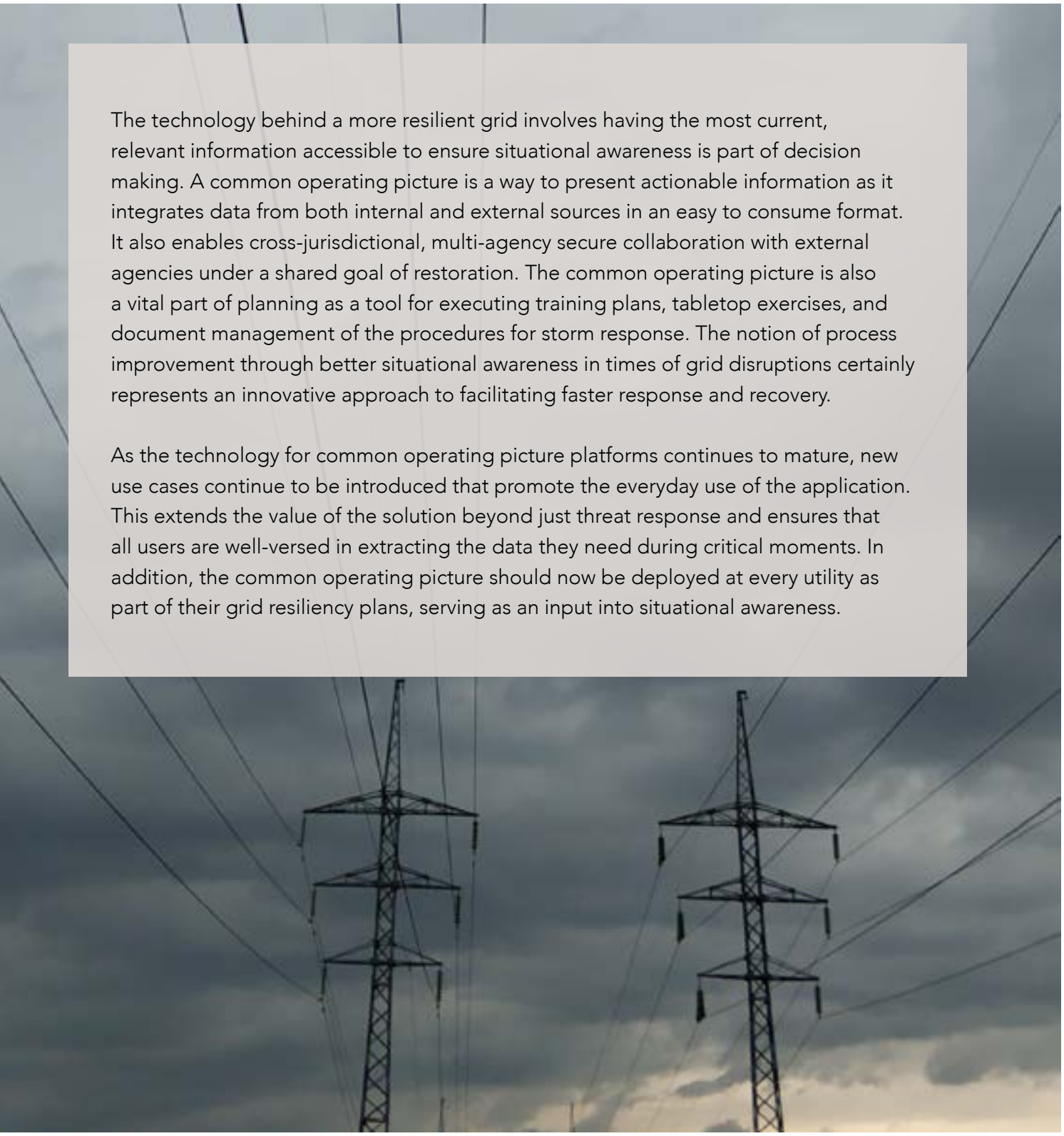
Contents



Executive Summary

The nation's reliance on the electric grid has never been higher than today. With threats to the grid increasing in frequency and impact, the pressure is on utilities to ensure they are making the most prudent improvements to provide the availability of electricity. Traditionally, these investments have been hardening the infrastructure based on reactionary evaluation of previous grid performance. Recently, some progressive utilities are taking a more proactive position by emphasizing their overall preparedness. They prioritize developing their business continuity plans and focusing on ways to minimize the impact of a threat and how they can return to normal conditions faster.

The concept of having a more resilient grid is now in every major utility's grid modernization plan as a parallel path to infrastructure hardening. They are evaluating proven reliability metrics and factoring resiliency into their strategies to address their response to high consequence threats to the grid. This extension of a disaster recovery plan precludes a threat by placing more emphasis on preparation so that once the disruption does occur, the grid is more capable of absorbing the disruption. Then the utility can quickly implement their command structure and begin the recovery phase, with a target to restore power more efficiently by following the resiliency plans.



The technology behind a more resilient grid involves having the most current, relevant information accessible to ensure situational awareness is part of decision making. A common operating picture is a way to present actionable information as it integrates data from both internal and external sources in an easy to consume format. It also enables cross-jurisdictional, multi-agency secure collaboration with external agencies under a shared goal of restoration. The common operating picture is also a vital part of planning as a tool for executing training plans, tabletop exercises, and document management of the procedures for storm response. The notion of process improvement through better situational awareness in times of grid disruptions certainly represents an innovative approach to facilitating faster response and recovery.

As the technology for common operating picture platforms continues to mature, new use cases continue to be introduced that promote the everyday use of the application. This extends the value of the solution beyond just threat response and ensures that all users are well-versed in extracting the data they need during critical moments. In addition, the common operating picture should now be deployed at every utility as part of their grid resiliency plans, serving as an input into situational awareness.

Author

Mr. Eric J. Charette, P.E. currently serves as a Senior Vice President and Executive Consultant for GridBright. His responsibilities include providing consulting services to electric utilities on their grid modernization strategies, specializing in damage assessment and outage management. As part of the GridBright leadership team, Eric contributes are to corporate growth strategies through business development activities and identifying new business opportunities. Previously, Eric was part of the Hexagon leadership team in the role of Executive Technical Director where he was responsible for setting strategic direction within the utilities practice and held roles in business development, sales, and product management. Eric began his career with a distribution power utility and holds a B.S. in Electrical Engineering with an emphasis in Power Systems. As a registered professional electrical engineer, Eric is a proven thought leader and serves on the DistribuTECH Advisory Committee as Grid Modernization track chair.

Contributors

Jody Nemcek serves as the Enterprise Resilience - Emergency Preparedness Manager for Xcel Energy. She has over 20 years of experience working in the utilities industry and specializes in Crisis Management, Emergency Management, and Homeland Security. Jody graduated from Eastern Kentucky University with a master's degree in Safety, Security and Emergency Management.

Stephen J. Callahan is an Executive Vice President for Grid Modernization and Chief Marketing Officer at GridBright, Inc. His Utility Industry experience spans forty years in industry management and consulting. He has led the creation of business and technology strategy and implementation of complex processes and systems for several top global utilities spanning the areas of T&D, network operations, Smart Grid, customer operations, finance, and telecommunications networks. Mr. Callahan is a GridWise Alliance (GWA) Board Member Emeritus and DistribuTECH Advisory Committee member. In addition, he is a frequent contributor to industry conferences and publications focusing on electric utility industry transformation.

A More Resilient Electric Grid

Background

The nation's electric grid constitutes a vital component of our critical infrastructure and our economy [1]. Interruptions in service not only disrupt our lives, but they impede our ability to deliver basic human services such as health care. It serves as an essential foundation for the American way of life.

Yet the electrical grid is prone to multiple hazards and threats which are sorted into four major categories. [2]

- Natural (Geological, meteorological, health, animals)
- Accidental (Equipment failure)
- Intentional (Physical, human, cyber)
- Emerging (Impact of renewable energy)

Average electricity outage frequency in 2020 was
73% HIGHER
than it was in 2019

Specifically, extreme weather events are increasing in frequency and impact and have been shown to have an adverse effect on critical infrastructure including the power grid. The average U.S. electricity customer experienced just over eight hours of electric power interruption in 2020 [3] with an outage frequency of 1.6 – this was 73% higher than it was in 2019 [4]. In 2021, there were 20 weather/climate disaster events with losses exceeding $1 billion each to affect the United States [5]. This is triple the average annual quality during the 41 years that NOAA has been reporting on this statistic. The fiscal impact of those disasters in 2021 was $145B (CPI-adjusted) which was the third-highest since 1980.

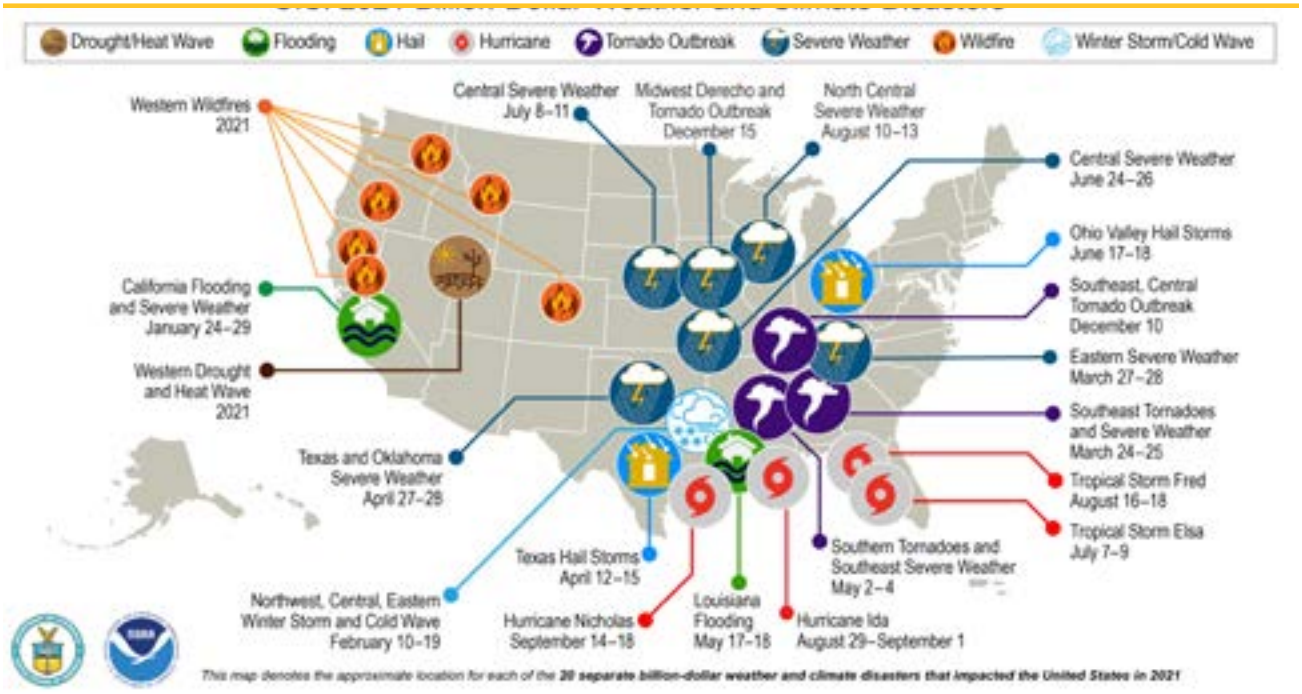


Figure 1: U.S. 2021 Billion-Dollar Weather and Climate Disasters [5]

The focus of local, state and federal government has shifted to processes that the grid can absorb a threat when it does occur.

Utilities invest in preventative measures to decrease the likelihood of outages, but this comes with a price and hazards cannot be completely avoided. The cost of the investments to avoid/minimize outages is weighed against the cost of the outages themselves to determine the return on investment for any increase passed on to ratepayers. Most decisions on which investments to make in what areas are supported by reliability indices that exclude major event days – thus not addressing the impact that a major threat may pose on the grid for a single event.

Predicting when the next major storm, cyber-attack, or cascading equipment failure will happen is impossible. And, since it is not possible to prevent threats to the electrical grid, the focus of local, state, and federal government has shifted to processes that ensure that the grid can absorb a the impact when it does occur. Resiliency strategies have been developed to outline activities and processes to be followed before, during, and after a system disruption. A recent article from Gartner on utility trends noted that 'the need for operational resiliency has never been greater for utilities.' [6]

The U.S. Federal Government is also trying to facilitate resiliency enhancements to the electrical grid through the Advanced Research Projects Agency – Energy (ARPA-E). As an organization from within the Department of Energy (DOE), ARPA-E is chartered by Congress to enhance the economic and energy security of the grid through the development of energy technologies that improve resilience and reliability. ARPA-E funds the research and development of transformative technology solutions in support of the agency's mission. The Seeding Critical Advances for Leading Energy technologies with Untapped Potential 2021 (SCALEUP 2021) program under APRA-E supports the scaling of disruptive technologies and plans to award $1M in cost-share for these high-risk, potentially transformative projects to get off the ground and promote grid resilience. [6a]

The U.S. government is also emphasizing grid resiliency as part of the Infrastructure Investment and Jobs Act (HR 3684) (the "IIJA"). Division D – Energy, Title 1 (Sections 40101 – 40127) outlines how grants are proposed to make the grid more resilient and minimize outages in response to challenges posed by threats [7] [8]. Designated for a five-year period of FY 2022 – 2026, the funds are in three key areas.

1) Preventing Outages and Enhancing the Resilience of the Electric Grid
   - — $5 billion in grants to support grid hardening activities that will reduce the likelihood and consequences of the grid threats
2) Electric Grid Reliability and Resilience Research, Development and Demonstration
   - — $6 billion to fund demonstrations of advancements in grid hardening technology
3) New Funding for the Smart Grid Investment Grant (SGIG) Matching Program
   - — Adds $3 billion in new funding, extending the original $3.4B from the American Recovery and Reinvestment act of 2009 ARRA, a cost matching program to accelerate investments in the smart grid

However, when reading the details of the IIJA, despite the inclusion of the term resiliency, the emphasis is still on infrastructure and not on process improvement. Let us examine the differences between reliability and resiliency as background before discussing how they play a role in situational awareness.

Reliability

According to the U.S. Department of Energy (DOE), reliability is defined as follows.

- "The ability of the system or its components to withstand instability, uncontrolled events, cascading failures, or unanticipated loss of system components" [9]

Reliability can be quantified and measured by both duration and frequency. As the owners of IEEE standard 1366, The IEEE Distribution Reliability Working Group [10] have defined 12 total indices but the most used metrics for sustained (non-momentary) outages are as follows:

- SAIDI (System Average Interruption Duration Index) indicates the duration an average customer would be without power
- CAIDI (Customer Average Interruption Duration Index) indicates the average duration of an outage
- SAIFI (System Average Interruption Frequency Index) indicates the number of outages an average customer would experience
- ASAI (Average Service Availability Index) indicates the percentage of time that a customer would have power

These commonly used metrics can be calculated by knowing the number of customers interrupted, the duration of the outages, and the customers served (which may be by company, by geographic area, by feeder/circuit). To calculate the lessor used indices, it requires knowing such things as the number of distinct customers interrupted, customers with multiple interruptions, connected load (and duration) of the interruptions, and total load served. Then there is the wrinkle of being able to report data by category which includes (or excludes) major event days or catastrophic days.

The bottom line is that it is straightforward to determine how reliable the grid is because standards have been set. Based on these standards, it is also possible to compare providers against each other and the national averages. Assuming the utilities in the comparison have similar reporting techniques, a SAIDI of 130 (the national average in minutes for investor-owned utilities in 2021 [11]) at Utility A is "better" than a SAIDI of 145 for utility B. This means that the average customer served by utility A would experience 15 fewer minutes of outage than the average customer for utility B during the same period.

Reliability can be improved via technology, and then the improvement can be measured.

Reliability can be improved via technology, and then the improvement can be measured. For instance, ADMS systems can predict outage locations based on customer phone calls can reduce the time to locate trouble and increase reliability. The integration of smart meter last gasp messaging to OMS can lead to faster outage prediction. System reconfiguration after outages occur, either automated/closed-loop or manual/open loop aided by FLISR recommendations to minimize the extent of an outage.

Reliability is a measure of the availability of the power grid. While it is the current standard for measuring grid performance to use reliability metrics, there are issues with basing investment in grid hardening solely on reliability.

- Reliability indices ignore the time of day that the disturbance occurs. Having a power outage while you sleep is much less disruptive than that same outage occurring during the day.
- The indices assume that every minute of duration is viewed equally by a customer. While inconvenient, a 2-hour outage is tolerable. However, those same 2 hours without power at the end of a 2-day outage are agonizing and extremely disruptive.

Expanding the discussion of grid performance to address how the grid (and its operation) reacts and responds when threats occur is part of the current narrative with policymakers and on the minds of many utility executives. Developing a new perspective on grid metrics includes consideration of the preparation to mitigate a threat when it occurs, and then recover from it – which is part of resiliency.

Resiliency

While the North American Electric Reliability Corporation (NERC) provides a much more detailed definition of resiliency [12], the DOE definition is straighter to the point.

- "The ability of a system or its components to adapt to changing conditions and withstand and rapidly recover from disruptions." [13]

Regardless of the definition, resiliency contains two distinct components.

1. The ability of the utility to minimize disruptions (of service)
2. The ability to return to normal operations (as) quickly (and safely as possible.)

Resiliency was introduced as a concept to help describe the behavior of the electrical grid when exposed to threats. It can be visualized by looking at grid stability over a period of time. Under blue sky conditions, the grid operates at a normal state. Under these circumstances, the grid is considered stable despite the possibility that some outages may exist. This state of stability (GSno) continues until the time that a disturbance occurs(tdist). The grid then becomes unstable until it reaches the full extent of the damage at GSmin. The delta between a normal state and the unstable state represents the ability of the grid to absorb the disruption when the maximum delta is reached at tabsb. In other words, GSno (at time tdist) - GSmin (at time tnbsb) = part one of the resiliency definition – how much the grid can absorb the disruption over time. The duration of this cycle from stable, to unstable and return to stable will depend upon the magnitude of the disruption. In the most severe examples such as Superstorm Sandy, it was days to weeks before a stable grid was realized by some of the impacted utilities. In most cases, the time frame is typically in the range of hours to days for a return to normal. When we analyze the use cases to increase resiliency, we will examine what happens if the slope of the line changes, resulting in an increase or decrease in resiliency.

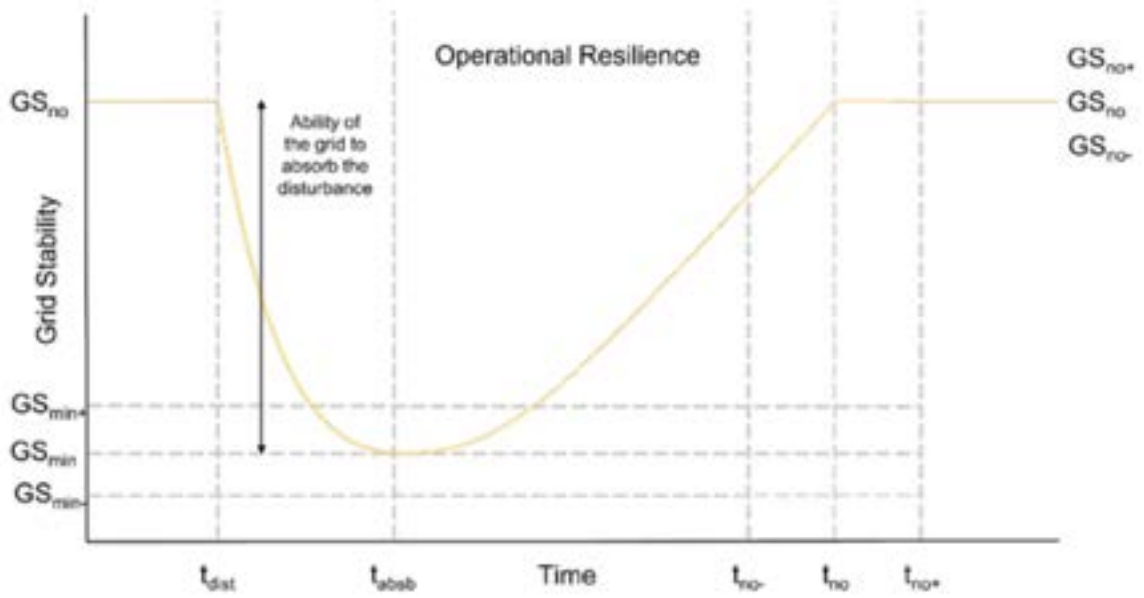
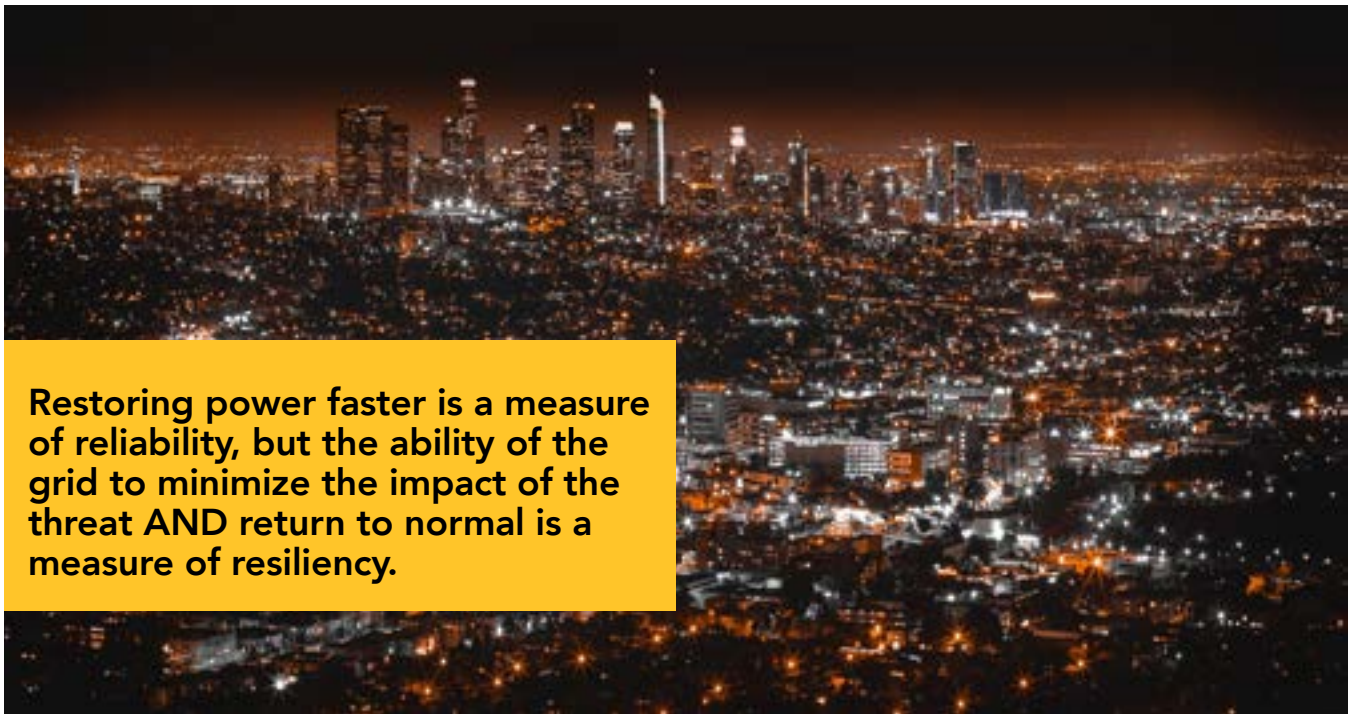


Figure 2: Operational Resilience Represented Graphically with respect to Absorption

The second aspect of resiliency focuses on the amount of time it takes for the grid to restabilize and return to normal conditions. Starting at the time when the grid has reached its minimum stability (GSmin at time tnbsb) until the time when it returns to normal (GSno at time tno) equates to the second part of the resiliency definition. When we analyze the use cases to increase resiliency, we will examine what happens when the return to normal happens faster (or slower) resulting in an increase (or decrease) in resiliency.

Figure 3: Operational Resilience Represented Graphically with respect to time to return to normal



Resiliency and reliability are directly related – a grid cannot be resilient if it is not reliable. And having a resilient grid does not prevent damage – it simply is the ability for a utility to operate or return to operation quickly after damage occurs. Restoring power faster is a measure of reliability, but the ability of the grid to minimize the impact of the threat AND return to normal is a measure of resiliency. Lastly, it is important to note that reliability often deals with many disturbances over a period of time, whereas grid resiliency is typically discussed on single, large-scale events.

While technically not part of the formal definition of resiliency, there is a third component that warrants discussion – this is the public perception that the grid is resilient. With provider of choice options growing, utilities are held more responsible for higher levels of ratepayer engagement. After a major system disruption, a utility can recover and fail to communicate details to the public and they will be perceived as not being very resilient. In the same scenario, the utility could be using its social media channels, holding press conferences, and issuing press releases to communicate their progress and be perceived as having a resilient grid. Some studies have shown that customers are tolerant during power outages that last longer than normal, as long as they have a steady stream of open communication with the utility. Regardless if this is viewed as managing expectations, influencing perception, or controlling the narrative, it is yet another unmeasurable aspect of a resilient grid.

Measuring resiliency is not as standard as measuring reliability. There have been scholarly articles on grid resilience metrics. This includes a paper from NREL that reviewed five different tools on measuring resilience [14], but there is still a lot of active research being conducted on this matter. With the debate that no single metric has yet been developed to measure resiliency, this paper will not focus on the quantification of resiliency improvements. Instead, the concentration will be on how using a common operational picture can provide key input into situational awareness and have an impact on resiliency.

Situational Awareness from a Common Operating Picture

With an understanding of resiliency, now we shift attention to how it can be improved. To do that, we need to first discuss the concept of situational awareness.

The government recognizes the need for a model to enable greater preparedness and response to threats.

Situational Awareness

In 2019, the U.S. DOE began the development of the North American Energy Resilience Model (NAERM) [15]. One of the goals of this effort is to provide a potential solution for real-time situational awareness for large-scale events impacting the energy infrastructure. While this is at a national level, it is an excellent example of the government recognizing the need for a model to enable greater preparedness and response to threats.

The definition of situational awareness can be found within the United States code. The first chapter outlines Homeland Security and under subchapter V for National Emergency Management, Section 321d - National Operations Center, it describes situational awareness as:

- "Information gathered from a variety of sources that, when communicated to emergency managers and decision-makers, can form the basis for incident management decision making." [16]

While not a complex definition, separating it into three parts makes it clear that situational awareness is not making the decision, it is the process of making the decision.

1. Information from a variety of sources
2. Communicated to decision-makers
3. Forms the basis for their decision making

Even though the concept of situational awareness has been around for more than a hundred years [17], more recent models have been developed to help us gain a greater understanding of situational awareness as a thought process. Endsley theorized that situational awareness could be represented as a three-level hierarchical model. [18]

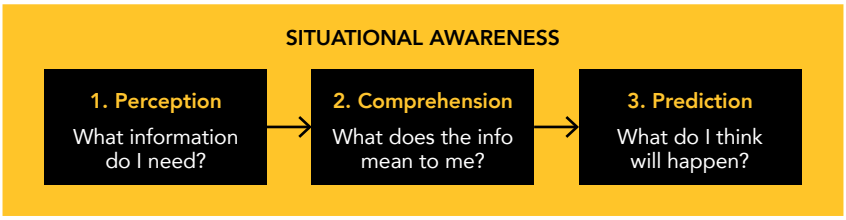


Figure 4: Situational awareness represented as a three-level model

1. **Perception of the elements in a situation within a specified time**

   This can be restated by asking the question "What information do I need?" (to make this decision). This level can be achieved by perceiving the relevant information about a situation. But the decision-maker must have access to the relevant information and recognize that the data is relevant to the situation

2. **Comprehension of the current situation**

   This can be restated by asking the question, "What does the information mean to me?" The level cannot be achieved without the perception of the information and then involves understanding and interpreting the information.

3. **Prediction of the future status**

   This can be restated by asking the question, "What do I think will happen?" Once the information is perceived and understood, the decision-maker can then hypothesize what will happen in the future.

The three-step model for situational awareness outlines the conscious activity of processing information so that a decision can be made. Think of situational awareness as the analysis of data required to be well informed so that a decision can be made, and then this is used as input into making the actual decision. Following this logic, the decision lies outside of the situational awareness model.

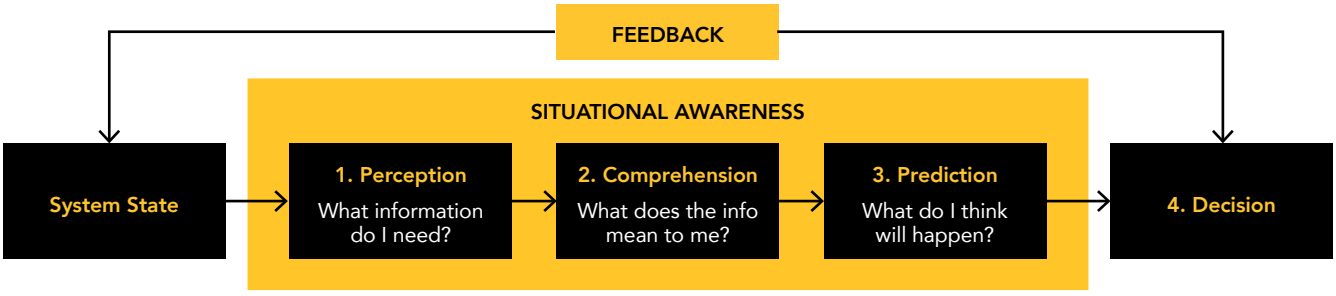


Figure 5: Situational awareness represented as a four-level model

4. Decision Making

The information discovery, comprehension, and consideration of alternatives form situational awareness. This then serves as input to the decision-making. Once the decision is made, that then alters the system state and updates the situational awareness for the next decision. Throughout the event, this process continues to occur until the event is over and no further decisions are required.

It is important to note that there is a difference between making a decision and taking action based on that decision. A person can decide to do something and then not take any action. Therefore we need to expand our model to include a fifth and final level.

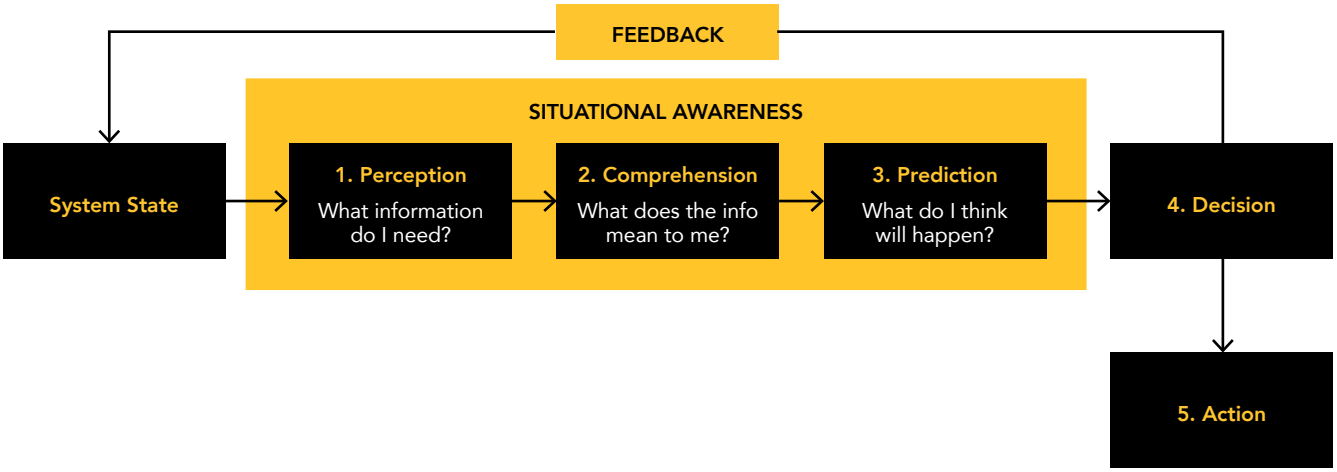


Figure 6: Situational awareness represented as a five-level model

5. Action

Action is the process of acting upon a decision or actually doing something. In our model, taking the information from situational awareness that helped formulate the decision and putting it into motion with activity is the definition of action. This could be updating a system, or communicating the decision to the stakeholders.

Moving this theoretical analysis into practical application for utility emergency response, we need to note where the information (from various sources) originates from that feeds into the situational awareness model. This is where we introduce the concept of a common operating picture.

Common Operating Picture

In utility terms, a common operating picture (COP) is an overview of the state of the power grid based on shared data feeds from both internal and external sources. It represents the single source of truth for real-time intelligence and serves as an essential input for situational awareness to ensure decisions can be made with the most accurate information and the current state of the system. Its purpose is to help coordinate response and promote partnership during a major event or threat to the grid. Collaboration toward a unified goal is needed between different departments within the utility but also extends to external agencies that may play a role in recovery.

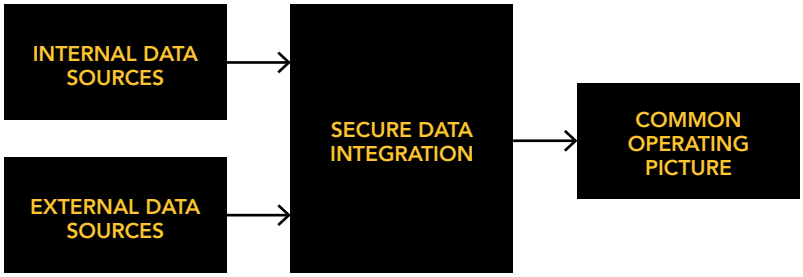


Figure 7: Data inputs for common operating picture

In the response to a large-scale event, there is more than one decision-maker in more than one agency making more than one decision at a time. Therefore, it is imperative that each decision-maker have the most current, relevant, and useful information as input into their cognitive situational awareness approach. In fact, there are hundreds of decisions being made every minute that all require the information found in a common operating picture.

Within the utility, a common operating picture may be used by executives, media relations, engineering, incident command, and field operations. Outside of the impacted area, other utilities thaat may respond with mutual assistance would also need to have access to the information provided by the common operating picture to help them determine how long their resources might be needed.

If the event magnitude is widespread, then the government may be involved. Utilities and government should be working in concert to collaborate on the objectives to protect the safety of the people, stabilize the impact of the threat, and preserve the infrastructure to restore power. However, as noted below, the utility is often on the outside looking inward. The government also has the role of working to reduce obstacles to data access and enable communication from first responders (police, fire, EMS) into the common operating picture. This includes real-time data feeds provided through integration with other systems. Quite often there are barriers that have historically prevented cross-agency collaboration. But to achieve the incident objectives, it requires multi-agency information sharing across all levels of government and the private sector to unstructured data access for contingency planning, collaboration, and coordination of restoration efforts

A typical emergency response approach asserts that emergency response providers are the focal point. In the 3-Tier diagram proposed by Howitt and Makler [19], other agencies (such as utilities) are second-level support for the response.

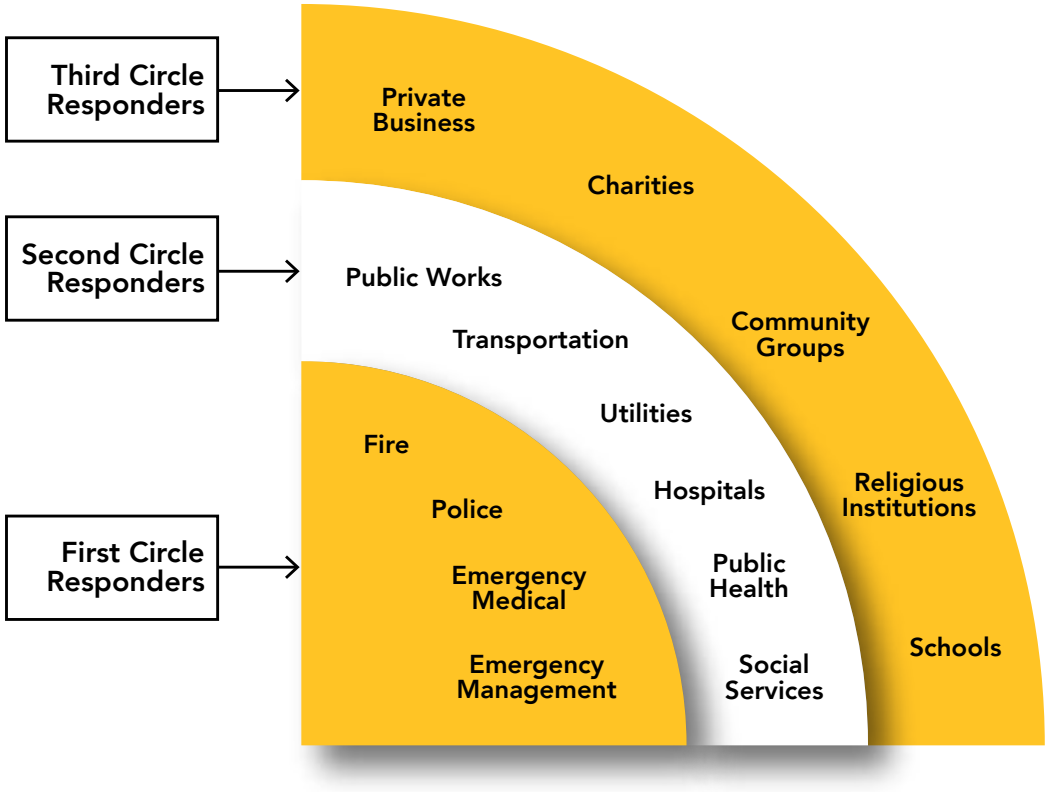


Figure 8: 3-Tier diagram for emergency response providers [19]

While this may be the most widely accepted response approach to a threat that extends beyond the electrical grid infrastructure, it does not prevent the sharing of information across agencies.

While not making decisions on how to safely restore power, the public is making decisions based on the stability of the grid. Depending on the magnitude and duration of the event, the public would have to decide on anything from the refrigeration of food at one extreme to the possible evacuation of the area at the other extreme. The public is performing their own situational awareness to formulate their decisions. The information disseminated to the public may take a different shape and form than what is being used for restoration, but it originates from the same single source of the truth that feeds the common operating picture used by the utility.

Figure 9: Multi-agency information-sharing model

At this point, we can layer together our four-step model for situational awareness resulting in decision making and action taken with our common operating picture. In this graphic, we have grouped all non-utility participants as "stakeholders" in "external agencies."

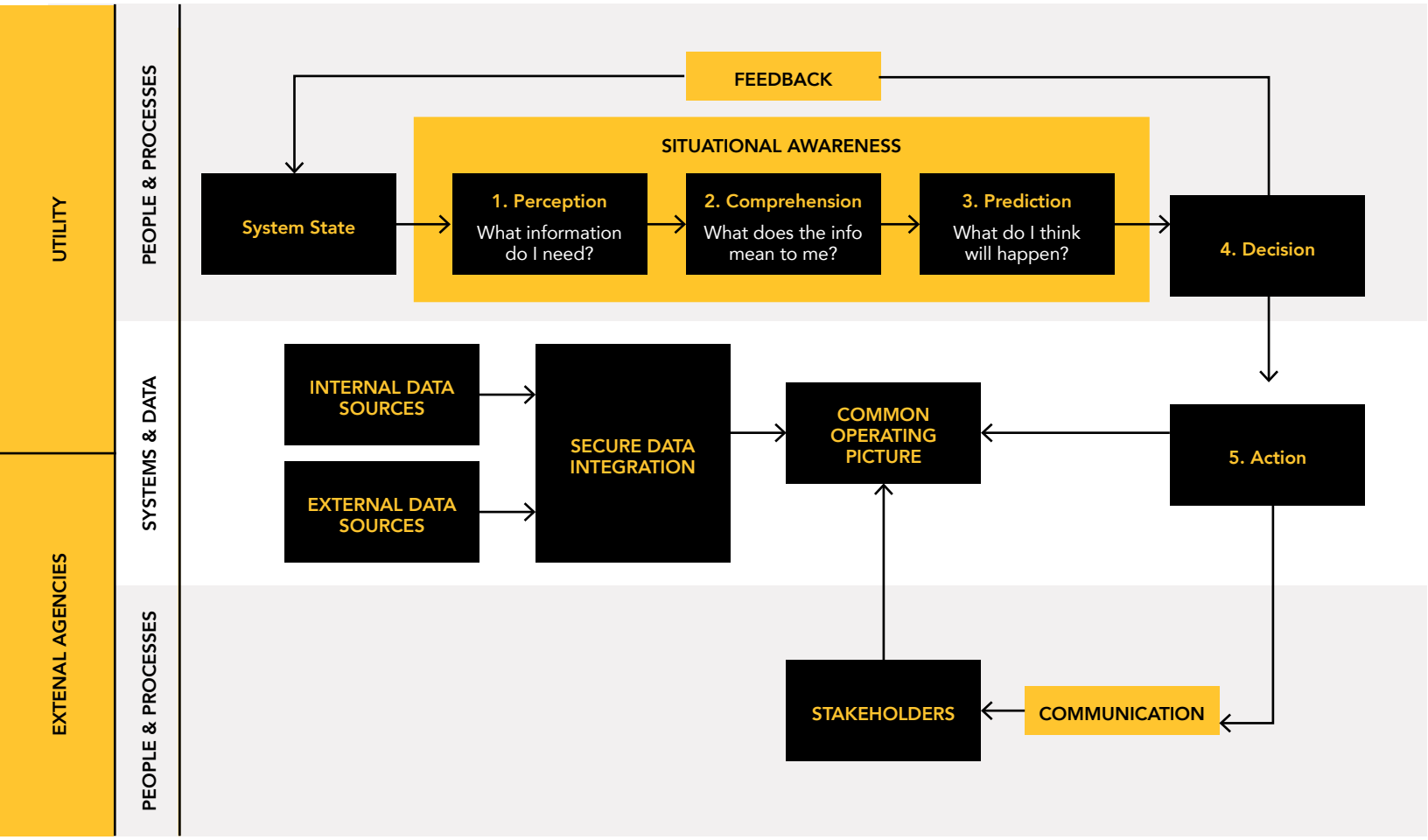


Figure 10: Common operating picture as input into situational awareness

Systems Integration

Having a firm understanding of the concept of a common operating picture, we next dive into the systems that can provide this information. This will not focus on a specific vendor product but on the high-level features and integration points required to provide the current system state for our situational awareness models.

Let us first start with utility systems falling into four categories that should be integrated.

Network Operations

- **Outage Management (OMS)**
  Location, details, and customers impacted by the outage
- **Advanced Distribution Management (ADMS) / SCADA**
  As-operated configuration of the network
- **Damage assessment**
  Images, drone feeds, material requirements of damaged facilities
- **Meter Data Management (MDM)**
  Status of each meter in the network

Assets

- **GIS**
  Asset information of the as-built configuration of the network model
- **Security cameras**
  Real-time video of substations

Resources

- **Mobile Workforce management (MWFM)**
  Details of the workforce
- **Automated Vehicle Locations (AVL) / GPS**
  Real-time positioning of the vehicles, personnel, and equipment
- **Call out system**
  To deploy additional resources and manage schedules

Documentation

- **File management systems**
  Access to libraries containing process and procedure documentation
- **Customer Information System (CIS)**
  Information about key customers in need of special

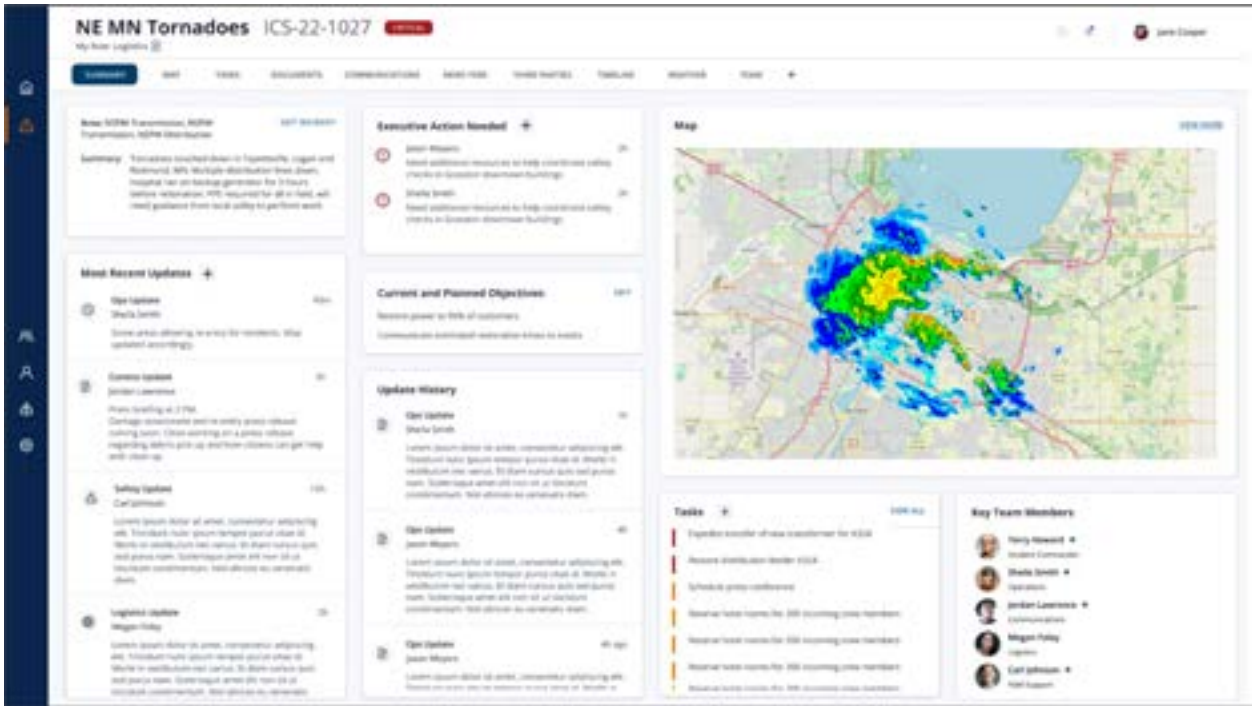
To facilitate common cross-jurisdictional objectives, a common operating picture requires multi-agency information data sharing from both public, private, and governmental sources.

- First responder GPS locations
- Weather (wind speed, lightning strikes, wildfire information)
- Street network
- DOT Road conditions
- Traffic
- Traffic cameras
- Social media
- Other

Common Operating Picture Application Requirements

Now that we have determined all the required information to paint the common operating picture, we need to discuss what the canvas looks like. While not an all-inclusive list of capabilities, this does attempt to outline the key characteristics and features of a common operating picture application.

- Cloud-based environment
- Browser-based accessible
- Device agnostic
- Secure data integration to all systems
- Real-time or near real-time updating
- Instinctive, self-explanatory interface
- Role-based access for inter and intra agency access
- Alerts on changing conditions
- Geospatial map with layer controls



Graphic 1: Example of a common operating picture

Use Cases

Recalling that our definition of resiliency had two distinct components, we will discuss use cases for a common operating picture and how we can minimize the disruptions and then use cases for returning to normal. While we will focus on the positive outcomes, it is also possible that the outcomes of recovery are negative. Examples of these are shown below.

POSITIVE OUTCOME	NEGATIVE OUTCOME
Time to return to normal is reduced	Time to return to normal is increased
Threat absorption is improved	Threat absorbtion is reduced
Post threat state is enhanced	Post threat state is weakened

Table 1: Potential Outcomes for Changes in Resiliency

In reviewing the use cases to improve resiliency, we will start on the second part of the resiliency definition, which will be activities that can be performed during the event to reduce the duration. The reason will become apparent when we propose use cases for limiting impact as that introduces another dimension of complexity.

Use Cases to Reduce Time to Return to Normal

Using our graphic, reducing the time to return the grid to normal is highlighted with the gray box below. Technically, the area could be extended below the grid state normal line but having a weaker (yet stable) grid is undesirable. The mission is to ensure that the time to return to a normal grid stability level that we had before the disturbance occurs at or before the normal time. This can be difficult to quantify in that each threat is unique in the number of incidents that result, and the number of resources required. So that is why we will label a resilience increase for grid stability returning to normal GSno at time tno-. As noted, resiliency and reliability are closely related. Any use case where the time to return to a stable grid occurs before normal is both an increase in resiliency and reliability. We are also assuming in the first set of use cases that the absorption rate remains constant.

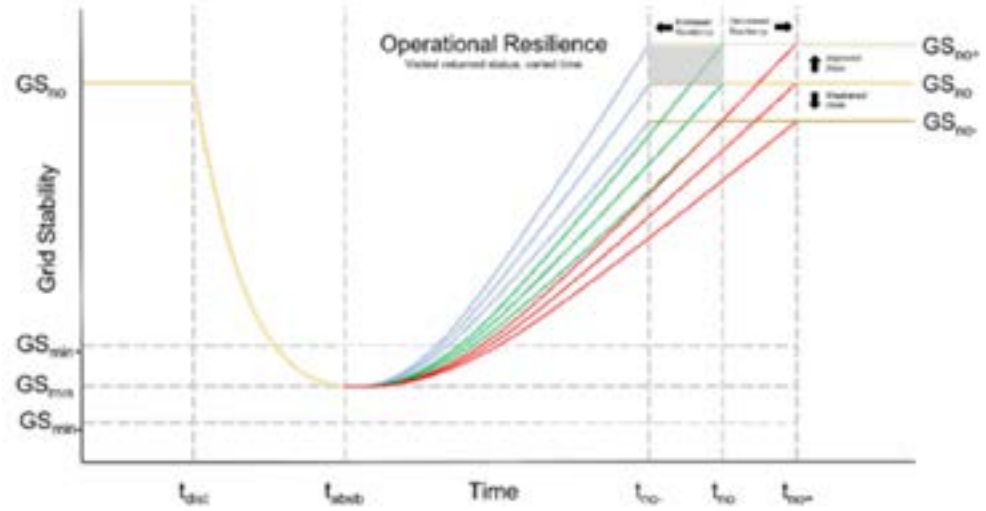


Figure 11: Use Cases to Reduce Time to Return to Normal

As noted above, not all outcomes of recovery are positive. Returning to a normal state can occur faster (improved resilience), normally, or take longer than normal (decreased resiliency). Post threat, the event can be returned to an improved state, to normal status, or to a weakened state. This results in nine potential outcomes that all have been categorized below.

BEGINNING STATE	ENDING STATE	DELTA	RESILIENCE
t_{absb} at GS_{min}	t_{no-} at GS_{no+}	Return to an improved state in less time	Target
t_{absb} at GS_{min}	t_{no} at GS_{no+}	Return to an improved state in normal time	Optimal
t_{absb} at GS_{min}	t_{no-} at GS_{no}	Return to an improved state in less time	Optimal
t_{absb} at GS_{min}	t_{no+} at GS_{no+}	Return to an improved state in more time	Less Optimal
t_{absb} at GS_{min}	t_{no} at GS_{no}	Return to an improved state in normal time	Neutral
t_{absb} at GS_{min}	t_{no-} at GS_{no-}	Return to an improved state in less time	Sub Optimal
t_{absb} at GS_{min}	t_{no+} at GS_{no}	Return to an improved state in more time	Sub Optimal
t_{absb} at GS_{min}	t_{no} at GS_{no-}	Return to an improved state in normal time	Undesirable
t_{absb} at GS_{min}	t_{no+} at GS_{no-}	Return to an improved state in more time	Undesirable

Table 2: Possible outcomes for changes in time to restore

The scenario where the grid is restored to an improved state is noted as either being target, optimal, or less optimal depending on the time to reach that state. Examples of returning to an improved state include:

- New plant that is installed to replace damaged assets has a higher rating to withstand future threats. This may include replacement of wood poles with reinforced concrete structures, enhancing guying, or relocation of overhead facilities to underground.
- New plant that is installed may eliminate code violations that existed previously

The scenario where the grid is restored to a weakened state is noted as either being suboptimal, or undesirable depending on the time to reach that state. Examples of returning to a weakened state include:

- New plant is installed but poor record-keeping results in not having an accurate asset repository for what is in the field.
- Temporary repairs (that are made to the grid to get the power back on in the short term) become long-term parts of the infrastructure, thus the grid is in a worse state than before the threat. This scenario could be sub-optimal short-term but could improve to normal if the short-term fixes were rectified later and the infrastructure was restored to its normal condition.

Use cases for reducing the time to return to normal will outline using the common operating picture after the disruption has occurred.

- Monitor location of all first responders across jurisdictions

  Our resiliency definition notes that it is not just the ability to return to normal operations as quickly as possible, but to do so safely. With all the work that is taking place simultaneously on the grid, knowing where all personnel are located in real-time is a requirement for safe operations. This extends beyond just utility personnel to also include any first responder that might be assisting. Local police might have gotten the first call for a vehicle accident, only to discover that it is a broken pole with potentially hazardous wires on the ground. The communication lines from the police dispatch to the utility dispatchers are open, but police have a responsibility to remain on site until relieved by the utility. If the utility has the visibility of the officer's location from their GPS to the common operating picture, utility dispatchers can guide crews to the correct location. And if immediate relief is not possible, the dispatcher will continue to be reminded of the officer's presence on the scene as to not lose track of them.

- Provide a central location for all reported damage

  During recovery, utility crews continually conduct damage assesssment. However, utility crews are not the only source of insight on damaged facilities. There may be crowdsourced information from social media or smartphone apps where the public is providing useful information. The ability to see damage reports on a map from all sources, combined with outage locations from OMS can help with prioritization of restoration, determine needs for materials and play a key role in resource needs and projections of area power restoration.

- Developing an incident action plan after a threat occurs

  After a disruption occurs, the utility incident command will be responsible for developing an incident action plan (IAP) with objectives reflecting the overall strategy managing the restoration process. As noted by FEMA's guidelines for emergency response, there are five primary phases required to ensure a comprehensive IAP. [20]

  1. Analyze the Situation, Including Future Developments
  2. Establish Incident Objectives and Strategy
  3. Develop the Plan
  4. Prepare and Disseminate the Plan
  5. Execute, Evaluate, and Revise the Plan

  The first phase in planning includes increasing situational awareness of the magnitude, complexity, and potential impact of the threat. A common operating picture with real-time data feeds provides the foundation for this assessment as input into setting the objectives of the plan. Following the "best practices" of an Incident Command System (ICS) will help to establish processes for planning and resource management and coordinate the response among various jurisdictions and agencies.

Use Cases to Reduce Threat Impact

Using our graphic, reducing the impact of a major event on the electric grid is highlighted with the gray box below. The mission is not only to ensure that stability is not impacted MORE than normal (as noted by tno), but to implement tools and processes that reduce the time to restore and move toward tno-

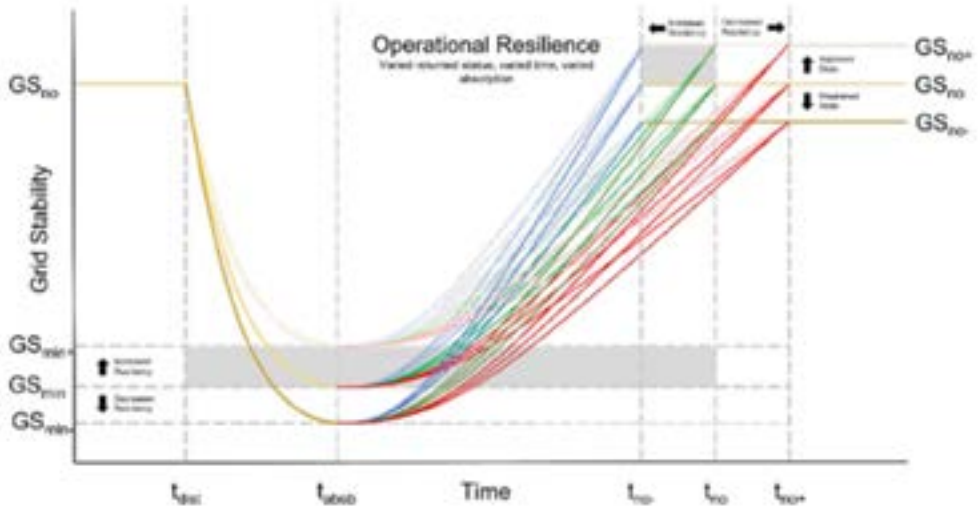


Figure 12: Use Cases to Reduce Threat Impact

As noted above, not all outcomes are positive. The ability to absorb the threat can increase (improved resilience), remain normal, or decrease (decreased resiliency). When combined with the three potential states of the grid post threat (improved, normal, weakened) and three potential times (faster, normal, longer) we end up with 27 different outcomes. For simplicity, we will only categorize the change in absorption here.

BEGINNING STATE	ENDING STATE	DELTA	RESILIENCE
$t_{dist\ at}\ GS_{no}$	$t_{absb\ at}\ GS_{min+}$	Less grid instability after major event	Target
$t_{dist\ at}\ GS_{no}$	$t_{absb\ at}\ GS_{min}$	Normal grid instability after major event	Neutral
$t_{dist\ at}\ GS_{no}$	$t_{absb\ at}\ GS_{min-}$	More grid instability after a major event	Undesirable

Table 3: Possible outcomes for changes in absorption

Use cases for minimizing the overall disruption will outline using the common operating picture before the disruption has occurred.

- Command structure for response

  Having a predefined reporting structure identifying each role during a storm clarifies who is responsible for what tasks. This reduces time to ramp up, resulting in faster response times. As noted in the systems integration section, we identified a touch to file management, which could potentially house the ICS organizational chart that the utility uses in storm response. These are then accompanied by actual resource names capable of performing these functions. If the common operating picture is integrated into the utility call-out system, with a few clicks the entire command structure could be staffed and ready to act.

- Regular testing of response by conducting restoration drills

  Expecting perfect execution during an actual event response without training and preparing is preparing to fail. Running simulations through the common operating picture can help with tabletop exercises to ensure skills are maintained on the software.

- Outage projections using predictive weather

  Historical outage information can be used to predict future damage. Common operating pictures that can leverage historical weather details (wind speed, direction, temperature, lighting strikes per mile) with damage that resulted (and outages that occurred) to apply machine learning techniques to project damage, outages from looming storms. By adjusting input factors, multiple scenarios can be evaluated to optimize resources and materials.

UTILITY CASE STUDY

$500M
in damage incurred across the Twin Cities

In late May 2020, an unprecedented level of civil unrest erupted in the Minneapolis-St. Paul metropolitan area following the death of George Floyd. What started as peaceful protests, turned to looting, arson, and violence resulting in damage or destruction to over 1,500 properties over an intense three-day period [21]. Not since the Los Angeles riots of 1992 had the United States experienced this level of destruction, with over $500M in damage incurred across the Twin Cities [22] [23]. With local law enforcement overwhelmed by the thousands of protesters, Governor Tim Walz deployed over 7,000 members of the Minnesota National Guard to help restore civil order [24].

Incident command was led by the state and after assessing the situation, they set their incident objectives based on the priorities of protection of life, stabilization of the incident, and property preservation. They worked closely with first circle responders (police, fire, emergency management) as the primary agencies required to accomplish the incident objectives. However, there were second and third circle responders who also had responsibilities during the period of unrest, which included local utilities.

For the utilities, their objectives were similar to incident command as they too wanted to ensure their worker's safety and also to protect their critical infrastructure – both their distribution facilities (substations, electric and gas distribution equipment) and their buildings and vehicles. Xcel Energy was an active participant in the incident response as the primary distribution company providing electric service to the impacted area. Xcel quickly ramped up their Emergency Operations Center, which included the Crisis Communication team, Physical Security, and Threat Intelligence personnel, and implemented their incident response.

If all data sources and systems had been integrated into a single common operating picture, the lines between responder circles could have been dissolved and all agencies could have worked together seamlessly.

In the Hot Wash report created by Xcel for their after-action review, they noted the following as areas of potential improvement.

- The City of Minneapolis was using the Homeland Security Information Network (HSIN) – A platform was used for sharing sensitive information between the federal, state, and local agencies to coordinate response to the incident. Xcel did not have access to this network, which resulted in confusion on who exactly was serving as incident commander and created an additional hurdle for Xcel to gain access to real-time information. Xcel was not able to adequately plan resources without the full picture that included projections on the anticipated total duration of the incident.

- Xcel was called upon to disconnect power to homes and businesses that had been maliciously set on fire. But following their priorities of prioritizing the safety of their workers, this required police escorts into the riot zone. This required collaboration with local law enforcement which was difficult to coordinate as they were spread thin across the metro area. In post-event response analysis, Xcel noted that if they would have had better real-time information on first responder locations and arrival times to escort them into these dangerous environments, it would have improved their response.

- The ability to gain access to the airspace around the riot zone was not available. Xcel would typically fly over an area with a drone to obtain intel on the damage. Xcel can then determine what resources, materials, equipment, and personnel are needed for restoration. Not having the ability to use this technique to evaluate the situation did not prove to delay response, but that was not known until after the fact.

The main theme from the Hot Wash was the lack of information and the need for better communication between inter and intra agency. Xcel noted that they were making decisions based on incomplete information throughout the incident. In each of the scenarios above, if all data sources and systems had been integrated into a single common operating picture, the lines between responder circles could have been dissolved and all agencies could have worked together seamlessly.

Xcel felt prepared for potential threats to its infrastructure, especially on the heels of dealing with an unprecedented pandemic. However, they noted that the unpredictability of the rioters and public outrage created a response scenario that they were not fully prepared to handle. To their credit, no agency or department could have predicted the impact that the civil unrest caused. But since then, Xcel has worked to improve its working relationship with the municipal agencies, has developed annual tests for how they may respond to future civil unrest, and have planned to deploy a vendor-supplied common operating picture. This will include features such sharing of outage information with local law enforcement, and two-way sharing of responder locations with those agencies.

The threat levels were reduced fairly quickly in Minneapolis, but unfortunately, similar protests erupted elsewhere and put other American cities under siege. While natural threats to the electrical grid (geological, meteorological, health, animals) can be regionalized, the accidental, intentional, and emerging threats can happen anywhere, at any time. Having real time common operating picture opens up the channels of communication for cross agency collaboration regardless of who is providing incident command.

Barriers to Success

If a common operational picture is a key to situational awareness, what are the barriers to achieving this? Foundational for our definition of situational awareness is the information from a variety of sources. Presented here are the data issues that limit the effectiveness of a common operating picture.

Access:

The information required must be accessible in a form that can be consumed

Gaps:

There should not be key missing information that would impact decision making

Outdated:

The information needs to be real-time / near-real-time and note when it was last updated

Irrelevant:

Only the information that is needed to make informed decisions should be included

Redundant:

Data should not be duplicated and or overlap of information from sources should be minimized

Overload:

There should not be too much information to process given the time allotted to make a decision

Once the data issues are addressed, the administration of the system should not become a barrier to leveraging the common operating picture. These would be things such as how difficult it is to ensure the system is up to date and that users have adequate time for training to maintain their skills. Remember that most personnel working major events have regular "day" jobs that do not require the same skill set as their role in the hierarchy of the incident organizational chart. It should also not be more difficult to maintain and use the common operating picture than managing the response to the actual event itself.

Summary

Threats to the electrical grid are increasing in frequency and impact, which have a crippling effect on human safety, the economy, and simple daily life. Utilities are still making investments to harden the infrastructure mostly based on reliability due to the lack of accepted models and tools to quantify resiliency. Other cost-effective strengthening options are being pursued by progressive utilities in parallel to improve their ability to rapidly recover from major events and enhance resiliency. The target of a more resilient grid should be to have a greater level of absorption (minimize the impact), followed by returning to normal conditions faster. If the returned state has greater stability than before the disruption, it is viewed as favorable.

The concept of presenting actionable information in the form of a common operating picture for incident command structure ensures situational awareness is part of decision making. Integrating data sources via modern, secure architecture ensures that utilities have the information readily available and easy to consume. Theoretical use cases have been documented as to how utilities can leverage technology and process improvement to improve grid resiliency. These use cases have been evaluated in real-world examples which prove how using a common operational picture can improve situational awareness increase grid resiliency.

Works Cited

[1] Executive Office of the President, "ECONOMIC BENEFITS OF INCREASING ELECTRIC GRID RESILIENCE TO WEATHER OUTAGES", August 2013. [Online]. Available:

https://www.energy.gov/sites/prod/files/2013/08/f2/Grid Resiliency Report_FINAL.pdf

[2] T. Huang, S.L. Voronca, A.A. Purcarea, A. Estebsari, E. Bompard "Analysis of Chain of Events in Major Historic Power Outages". [Online]. Available:

https://core.ac.uk/download/pdf/323101459.pdf

[3] U.S. Energy Information Administration, "U.S. electricity customers experienced eight hours of power interruptions in 2020", TODAY IN ENERGY, November 10, 2021. [Online]. Available:

https://www.eia.gov/todayinenergy/detail.php?id=50316

[4] Tara Energy "Power Outages 101: What Causes Them and What to Do About It" 2022. [Online]. Available: https://taraenergy.com/blog/power-outages-101-what-causes-them/

[5] NOAA National Centers for Environmental Information, "2021 in Context", 2022. [Online]. Available: https://www.ncdc.noaa.gov/billions/

[6a] Advanced Research Projects Agency – Energy (APRA-E), U.S. Department of Energy, "The SCALEUP Program," 2022. [Online]. Available:

https://arpa-e.energy.gov/technologies/scaleup/scaleup-2021

[7] 117th Congress, "H.R.3684 - Infrastructure Investment and Jobs Act", 2022. [Online]. Available:

https://www.congress.gov/bill/117th-congress/house-bill/3684

[8] US Department of Energy "Fact Sheet: The Bipartisan Infrastructure Deal Will Deliver For American Workers, Families and Usher in the Clean Energy Future" November 9, 2021. [Online]. Available:

https://www.energy.gov/articles/doe-fact-sheet-bipartisan-infrastructure-deal-will-deliver-american-workers-families-and-0

[9] J. Eto, Grid Modernization Laboratory Consortium, "Grid Modernization: Metrics Analysis (GMLC1.1) – Reliability", Volume 2 April 2020. [Online]. Available:

https://gmlc.doe.gov/sites/default/files/resources/GMLC1.1_Vol2_Reliability.pdf

[10] IEEE PE/T&D - Transmission and Distribution, "IEEE P1366: IEEE Draft Guide for Electric Power Distribution Reliability Indices", 2018-02-15. [Online]. Available:

https://standards.ieee.org/ieee/1366/7243/

[11] U.S. Energy Information Administration "Annual Electric Power Industry Report, Form EIA-861 detailed data files". October 7, 2021 [Online]. Available:

https://www.eia.gov/electricity/data/eia861/

[12] NERC Reliability Issues Steering Committee, "Report on Resilience", November 8, 2018. [Online]. Available:

https://www.nerc.com/comm/RISC/Related%20Files%20DL/RISC%20Resilience%20Report_Approved_RISC_Committee_November_8_2018_Board_Accepted.pdf

[13] F. Petit, V. Vargas, Grid Modernization Laboratory Consortium, "Grid Modernization: Metrics Analysis (GMLC1.1) – Resilience", Volume 3 April 2020. [Online]. Available:

https://gmlc.doe.gov/sites/default/files/resources/GMLC1.1_Vol3_Resilience.pdf

[14] C. Murphy, E. Hotchkiss, K. Anderson, C. Barrows, S. Cohen, S. Dalvi, N. Laws, J. Maguire, G. Stephen, E. Wilson, NREL, "Adapting Existing Energy Planning, Simulation, and Operational Models for Resilience Analysis", February 2020. [Online]. Available:

https://www.nrel.gov/docs/fy20osti/74241.pdf

[15] U.S. DOE Office of Electricity, "North American Energy Resilience Model," Washington, DC, July 2019. [Online]. Available: https://www.energy.gov/sites/prod/files/2019/07/f65/NAERM_Report_public_version_072219_508.pdf

[16] U.S. Government Publishing Office, United States Code, Title 6 - DOMESTIC SECURITY, CHAPTER 1 - HOMELAND SECURITY ORGANIZATION, SUBCHAPTER V - NATIONAL EMERGENCY MANAGEMENT, Sec. 321d - National Operations Center, 2011 Edition. [Online]. Available:

https://www.govinfo.gov/content/pkg/USCODE-2011-title6/html/USCODE-2011-title6-chap1-subchapV-sec321d.htm

[17] and [18] N. Stanton, P. Chambers, J. Piggott, "Situational awareness and safety" Safety Science 2001. [Online]. Available:

https://bura.brunel.ac.uk/bitstream/2438/1804/1/Situation_awareness_and_safety_Stanton_et_al.pdf

[19] N. Hambridge, A. Howitt, D. Giles. "Coordination in Crises: Implementation of the National Incident Management System by Surface Transportation Agencies." Homeland Security Affairs 13, Article 2, April 2017. [Online]. Available: https://www.hsaj.org/articles/13773

[20] E. Zimmerman, FEMA, U.S. Dept of Homeland Security "FEMA Incident Action Planning Guide" Revision 1, July 2015. [Online]. Available: https://www.fema.gov/sites/default/files/2020-07/Incident_Action_Planning_Guide_Revision1_august2015.pdf

[21] [22] [23] N. Williams, Star Tribune, "Out of the Ashes," May 30, 2021. [Online]. Avalable:

https://www.startribune.com/twin-cities-businesses-saw-damage-for-miles-last-summer-they-face-a-long-road-back/600060651/

[24] B. Bakst, Minnesota Public Radio News, "Guard mobilized quickly, adjusted on fly for Floyd unrest," July 10, 2020. [Online]. Avalable:

https://www.mprnews.org/story/2020/07/10/guard-mobilized-quickly-adjusted-on-fly-for-floyd-unrest