Journal of Human Performance in Extreme Environments

Volume 14 | Issue 1 Article 4

Published online: 1-24-2018

Employing a User-Centered Design Process for Cybersecurity Awareness in the Power Grid

Jean C. Scholtz
Pacific Northwest National Laboratory, jean.scholtz@pnnl.gov

Lyndsey Franklin
Pacific Northwest National Laboratory, lyndsey.franklin@pnnl.gov

Aditya Ashok
Pacific Northwest National Laboratory

See next page for additional authors

Recommended Citation

Scholtz, Jean C.; Franklin, Lyndsey; Ashok, Aditya; LeBlanc, Katya; Bonebrake, Christopher; Andersen, Eric; and Cassiadoro, Michael (2018) "Employing a User-Centered Design Process for Cybersecurity Awareness in the Power Grid," *Journal of Human Performance in Extreme Environments*: Vol. 14 : Iss. 1, Article 4.
DOI: 10.7771/2327-2937.1094
Available at: https://docs.lib.purdue.edu/jhpee/vol14/iss1/4

Employing a User-Centered Design Process for Cybersecurity Awareness in the Power Grid

Cover Page Footnote

The authors would like to thank the Sierra Nevada Region of the Western Area Power Administration for their support and expertise. We would also like to thank the members of our advisory board: James Ball, Western Area Power Administration; Mark Engels, Dominion Resources, Inc.; Jamie Sample, Ernst and Young. General Electric has also been very supportive of this work especially in providing technical information. This work is sponsored by the Department of Energy, under DOE Project #: M614000331.

Authors

Jean C. Scholtz, Lyndsey Franklin, Aditya Ashok, Katya LeBlanc, Christopher Bonebrake, Eric Andersen, and Michael Cassiadoro

Employing a User-Centered Design Process for Cybersecurity Awareness in the Power Grid

Jean C. Scholtz, Lyndsey Franklin, and Aditya Ashok

Pacific Northwest National Laboratory

Katya LeBlanc

Idaho National Laboratory

Christopher Bonebrake and Eric Andersen

Pacific National Laboratory

Michael Cassiadoro

Total Reliability Solutions

Abstract

In this paper, we discuss the process we are using in the design and implementation of a tool to improve the situation awareness of cyberattacks in the power grid. We provide details of the steps we have taken to date and describe the steps that still need to be accomplished. The focus of this work is to provide situation awareness of the power grid to staff from different, non-overlapping roles in an electrical transmission organization in order to facilitate an understanding of a possible occurrence of a cyberattack. Our approach follows a user-centered design process and includes determining the types of information to display, the format of the displays, and the personnel to whom the display should be shown. Additionally, there is the issue of how much help the tool can provide in the way of assessing the probability of a cyberattack given the current status of various portions of the power grid. Regardless, the ability to provide a common operating picture should enable the various groups to collaborate on a response.

Keywords: cybersecurity, power grid, situation awareness, user-centered design

Introduction

Cybersecurity has become a crucial topic in many, if not all, aspects of modern life. The power grid is no exception. In fact, the power grid is especially vulnerable to attacks as it is an aging infrastructure to which new technologies are being added. Additionally there are three different groups responsible for different aspects of the electrical transmission systems: the cybersecurity group responsible for the enterprise networks, the engineers responsible for maintaining the energy delivery system network, and the dispatchers responsible for the safety and reliable delivery of power. Not only are the groups distinct, they may well be geographically dispersed as well. These three groups are the major players in discovering and dealing with cyberattacks on the transmission power grid. Cyberattacks can start in the enterprise network and spread to the energy delivery system network. If not discovered quickly, the dispatchers may lose the ability to stop the shutdown of the electrical grid. Our work intends to improve the decision-making process by designing and developing displays to provide improved situation awareness (SA) of issues in the system indicative of a potential cyberattack.

Why is the power grid so susceptible to cyberattacks? The bulk electric system (BES) consists of generation, transmission, and distribution systems all of which contain a significant proportion of legacy devices, software, and communication protocols. At the time these systems were installed, physical protection was needed for safe operation. Today these systems are connected, however loosely, to Enterprise and IT (information technology) networks that have much shorter life cycles and are more adept at dealing with modern cybersecurity risks. In addition network substations are often connected by third party communication providers. The result is better communications and operations, but at the expense of expanding the overall attack surface of the energy delivery systems infrastructure. Moreover, the connections between

https://doi.org/10.7771/2327-2937.1094

the different components, even though very loose, mean that bad actors can use such things as "phishing attacks" to enter the Enterprise system and eventually gain access to other components of the system.

Our goal is to analyze the current utility practices and identify how the various sources of information can be combined effectively to provide actionable and timely information to the dispatchers, engineers, and cybersecurity analysts to ensure the reliability and security of the BES. We have assumed that a singular and/or a combination of events already exist in the form of system alerts and that they adequately function as indicators of a cyberattack. Early identification of a cyberattack increases the likelihood that the impact of the attack can be lessened. However, we must make sure that the proper notifications are delivered to the appropriate personnel so that authoritative action can be taken quickly.

The Human Dimension of Cybersecurity Measures

Today's power grid is quite reliable, especially as the BES is designed to tolerate the loss of any single major element, such as a generating station or transmission line, with minimal to no impact on reliability. This is commonly referred to as *N*-1 contingency analysis and covers natural and man-made risks, such as lightning strikes, faults, and maintenance events, and considers the contingencies needed to mitigate those risks. Cyberattacks are a form of man-made risk, with the additional complexity that they could cause unexpected failures of elements across multiple substations within a short amount of time to impact the operation of the BES. Successful cyberattacks typically consist of various techniques executed over a period of time (usually not short). Of the many techniques, some include reconnaissance (learning about the infrastructure, hardware, and software), phishing scams, hardware/software vulnerability exploitation, credential theft, passive monitoring of the network, leveraging exploits to traverse to desired portions of the network, and execution of malicious code/commands. The exact implementation and methods/tools used for cyberattacks are constantly evolving to stay ahead of new defense mechanisms/strategies and take advantage of the latest vulnerabilities. However, it is critical to note that because they involve a progression through several stages, often requiring months or even years from initial launch to final execution, they would leave behind a trail of anomalies that could be used for attack detection and incident response if monitored properly. One issue is how to recognize abnormalities that are indicative of cyberattacks compared to everyday activities and honest mishaps, but of equal importance, and once an abnormality is recognized, who should be notified to take action?

Endsley (1995) defined SA as having three levels. The first level is the perception of elements in the current situation. The second level is the comprehension of the current situation, and the third level is the projection of possible future states. Greitzer, Schur, Paget, and Guttromson (2008) modified the definition in their research on the power grid to include the aspect of sense making. In this perspective, it is about more than providing additional data. Improved technology, information sharing, and the representation of pertinent information are needed to help the decision makers understand if there is a problem and, if so, the probable cause. This would enable the decision makers to resolve the problem more quickly and efficiently. The sense making loop as described by Pirolli and Card (2005) consists of structuring the problem, gathering evidence to confirm or disconfirm various hypotheses, and eventually making the decision. Ericsson and Lehmann (1996) noted that experts select relevant information and encode it in representations they use to reason about the selection of actions. Our goal in developing the tool for SA is to also ensure that it provides relevant information in appropriate representations to expedite decisions.

As we have already stated, there are three groups, each with their own set of data, that need to communicate with each other to determine if a particular situation may be caused by a cyberattack. We intend to provide each of the three groups with the appropriate information to provide them with Endsley's second level of SA—comprehension of the current situation—not just of each individual piece but of the entire transmission network. If each group has the current SA, then it should be feasible for them to assemble a holistic picture of the entire system and explain any irregularities they see. They should be able to determine if this is due to a cyberattack or can be explained by other irregularities that frequently occur in such large complex systems. For example, an issue that shows up in the Supervisory Control and Data Acquisition (SCADA) network that is used to control transmission is most often due to a cause other than a cyberattack. But if there is also a problem in the Enterprise network, the combination may be indicative of a cyberattack. The ability to see the SA not only of their particular area but the SA of the entire transmission network should facilitate sense makers to determine if a cyberattack is occurring and should help the groups to communicate to mitigate the situation.

Therefore we need to determine: (1) what information is needed, (2) who should see the information, (3) how the information should be displayed, and (4) what, if any, help could a tool provide in assessing the probability of a cyberattack. As there are many anomalies that can occur in these systems, we need to ensure that the new displays do not generate an abundance of false alarms, which could become a distraction or cause personnel to ignore the displays altogether.

There are a number of issues that need to be considered. Personnel at utilities occupy several non-overlapping roles, each with different tasks, responsibilities, tools, and data. Control room dispatchers, IT personnel, and cybersecurity analysts are collectively responsible for the cybersecurity of

the system as a whole. Determining how to display data and establish common ground is challenging when users come to the system with varying expertise and familiarity. To further complicate matters, these roles often work completely different hours with grid dispatchers on duty 24 hours per day, 7 days a week in shifts, and most supporting roles only during traditional business hours during the week. With such different organizational roles, interaction between groups does not usually occur until there is an event. In fact, these groups may lack some of the basic knowledge about types of equipment, possible vulnerabilities, and typical operations of the other groups (Scholtz, Franklin, LeBlanc, & Andersen, 2015).

Control room dispatchers are responsible for maintaining the safe and reliable operation of their portion of the electrical system. Consequently, they already have many displays to monitor. They must respond to alerts and act quickly and responsibly to various conditions, following standard procedures. They monitor the flow of electricity in the network, weather conditions, anticipated power demand, the conditions of equipment, and any scheduled maintenance that will impact the system. Adding more displays to monitor will increase their workload, so the information presented must be useful and easily accessible to them. Additionally, they will most likely need to communicate with others in the event that a cyberattack is suspected, which could result in more time needed to respond to alerts.

Separate from direct grid control, the IT and cyber analysts maintain the cyber tools on the network, do analysis on the large amounts of data from monitoring the network, and provide forensic analysis to determine what caused various incidents. While some aspects of networks are monitored in real time, log analysis is typically done after a problem arises and only on a small subset of logs deemed directly relevant to the apparent problem at hand. The majority of network information is otherwise neglected. Hence, without noticeable effects to draw attention, it might take days to determine that something amiss had happened in the enterprise or energy delivery system network. Meanwhile, energy delivery system network engineers are tasked with maintaining the control systems, incorporating patches, testing out new versions of software, and keeping backup systems, but are not currently tasked with watching the network. Some power utilities are now establishing cyber monitoring capabilities on their energy delivery system networks.

Currently, SA of potentially harmful cyber conditions is not readily available at a higher, regional level. Individual power companies are responsible for reporting issues that would impact the power grid to their assigned reliability coordinator. Reliability coordinators are responsible for identifying issues that impact a wide area and appropriately disseminating information to the impacted parties. These communications are usually accomplished via a phone call or an email. In addition, few utilities are anxious to provide access to their staff or to discuss cybersecurity incidents that may have occurred in their systems.

These factors need to be thoroughly understood as any tool conceived to help in diagnosing and stopping, or at least limiting, the impact of cybersecurity attacks needs to operate within the constraints of the groups. Our procedure for the design and implementation of such a tool takes these factors into consideration and is the basis of this paper.

Prior and ongoing work is being leveraged in support of our display designs. In particular, we are looking at using event reasoning tools to aid in decision making and routing of messages to appropriate individuals for action. Any number of events or alerts can be generated from a vast array of problems on the grid, and any single event may or may not be of interest in the control room. However, a unique combination of events occurring in series or in parallel may indeed be an indicator of cyber activity in a remote asset. An event reasoning tool can be used to quickly aggregate individual alerts or events, analyze the combinations to determine if the threat is legitimate, and then be configured to send a notification to the proper authority for action. Figure 1 depicts a block diagram showing how this might work.

While control alarms are highly accurate, cybersecurity alarms rely on algorithms to detect events. These algorithms can certainly miss events, so developing our event reasoning tool will need to take into account the costs of missing an event versus the costs of false alarms. The reasoning tool will certainly have to be iteratively tested during design and development to ensure that the balance of possible false alarms to missed events is reasonable. As more sophisticated cyberattacks occur the event reasoning system may have to be updated to take new tactics into account.

Method

We have found that a user-centered approach to developing tools is essential to their adoption in the workplace. Therefore our plan was to obtain as much information as possible about the tasks of those involved in the BES. As we work in a technical organization, we are well aware of the tasks of cybersecurity analysts and the tools they use. Some of our team are researchers in the electric grid and understand its functions and the tasks needed to maintain it, including security issues. However, the dispatchers' tasks are relatively unfamiliar to us. Therefore, we decided to start our user-centered work with the dispatchers and then continue to integrate this knowledge with information about the other two groups of users. As a number of the team members have backgrounds in visual analytics, we felt that using some sort of visualizations would be useful to convey the essentials of the SA to our users. As the amount of data is overwhelming, the application of some reasoning tools displayed in one or more visualizations seems to be a reasonable goal. As this

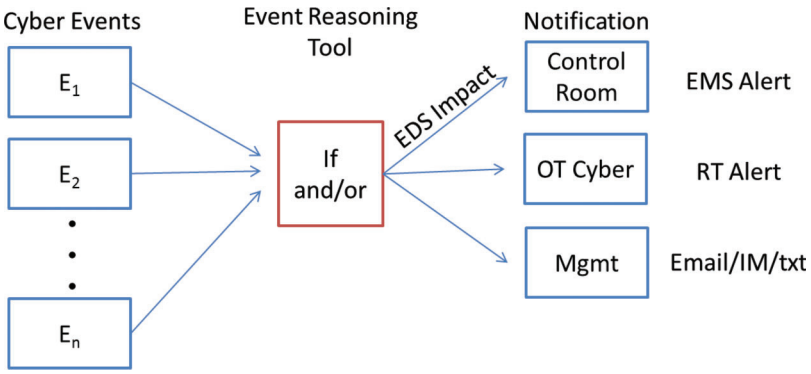


Figure 1. Schematic of an event reasoning tool.

is ongoing work, the discussion of our procedure is separated into completed, partially completed, and planned steps. For the completed steps, we discuss what we did, as well as the information we were able to gather. For the partially completed steps, we discuss the methodology used, the information collected to date, and our next steps. For the planned steps, we discuss what we plan at this point in time and the information we hope to obtain from those steps.

Completed Steps

Our first step was to establish a partnership with a transmission utility so that we could begin our user-centered design process with interviews and observations with utility personnel in a variety of roles. After our partnership was established, we assembled our human factors team and formulated a semi-structured interview procedure, along with some initial questions. We started in the control room with the dispatchers as this was the group we had the least knowledge of at the start.

Interviews and Observations

Three members of the human factors team participated in two sets of semi-structured interviews and observations with the dispatchers. We were able to meet with 12 of the 15 dispatchers during these two sets of interviews. We worked as a team of two, with one person primarily asking the questions and the other taking notes. We interviewed on-duty dispatchers in their control room when they were not actively engaged in tasks. When dispatchers were busy, we observed their procedures, workflows, points of coordination with other utility personnel, and used that opportunity to formulate more questions about their tasks.

Our findings with respect to cybersecurity can be summarized as follows:

- The dispatchers cannot be solely responsible for monitoring systems for cybersecurity.
- Dispatchers need operable statements in order to formulate a response.
- Dispatchers rely on well-defined procedures for communications.

GridEx Participation

Additionally, we were offered an opportunity to observe our power utilities' participation in GridEx III (2016). GridEx is a biennial exercise that simulates a cyber/physical attack on the electrical infrastructures across the United States. The exercise lasted two days and several dispatchers, as well as a cybersecurity analyst from our partner utility, participated in the simulation. On the first day of the exercise, a series of physical attacks combined with eventual energy delivery system network and communications compromises caused security deployments to critical substations, evacuations, lines being opened, and substations being islanded. On the second day of the exercise, a plane dragging metal wire took out a substation and malicious code was found in some telemetered data. Our findings from this exercise included:

- There was a safety issue with sending personnel to a substation for investigation. This issue delayed the response that dispatchers would normally make.
- Not all players understood what equipment was in the substations.
- Malicious code was not identified by the tools in place, so the cyber analyst was not aware of it.

It is worth noting that while a utility can be in compliance with North American Electric Reliability Corporation critical infrastructure protection plan (NERC CIP), this does not mean that it will be able to solve the problem. In particular, rolling a truck to the substation could have fixed the issue of malicious code, but would not have provided any indication of how it got there.

Our human factors team, along with some more technical members of our team, visited two other groups of people who are responsible for maintaining and monitoring the networks: the cyber analysts and the information system security officers (ISSOs). From the cyber analysts, we obtained information about a typical day, the tools used to

monitor the business network, the information obtained, and response plans for cyber incidents. Their tasks include:

- Maintenance of network tools (to ensure current picture of network).
- Investigation of "offenses."
- Communication with parties responsible for mitigation.
- Support of network integration activities.

Information was obtained about the cyber alarms and how this group responded to those. An important outcome of these discussions was a confirmation of what the team had observed on the second day of GridEx III. Specifically, the cyber analysts charged with investigation of offenses and anomalies were not trained in grid operations, nor were they familiar with the specialized equipment that appeared in their networks. This reinforces the point that there is a lack of common ground between the grid dispatchers who would encounter the manifestation of cyberattacks, and the cyber analysts who would be called in to assist in remediating the problem.

We visited with the ISSOs, who are in charge of assets which process operational data, such as SCADA (a type of energy delivery system) networks, and ensuring that the systems under their authority meet the Federal Information Security Management Act (FISMA) security requirements. They have specific regions/networks they are responsible for and they coordinate with regional staff as needed. Regional SCADA network managers are utilized for audit evidence collection. The tasks of the ISSOs include:

- Investigating offenses passed to them by the cyber analysts.
- Mitigating vulnerabilities discovered by the cyber analysts.
- Conducting SCADA network assessments for FISMA audits.
- Conducting general support system assessments for FISMA audits.
- Planning for addressing failed audit standards ("Pro-Ams").
- Tool vetting for new additions to monitoring capabilities.
- Handling certificate updates for software.

A list of the tools they use in their daily work was provided to us. While there was some overlap between the ISSOs and cyber analysts in terms of tool availability, we again established a lack of common ground and coordination between the two groups. Particularly, the process of handing partially started investigations from cyber analysts to ISSOs was fraught with communication delays and difficulties in tracking status.

While we were pleased with the information we received from our interviews and observations, we deemed it necessary to determine how well this generalized to other utilities. In the following section, we describe the survey we used to determine this.

Developing Use Cases

Use cases are helpful in user-centered design for clarifying who will be using a system and under what conditions. This aids visual design by providing context, as well as example information to display. Therefore, we needed to identify several combinations of abnormalities that would signify a potential cyberattack as our use cases. Our team, with input from other experts at our organization, came up with three possible scenarios. Before we used these in our early design efforts, we wanted to collect more information from our potential user base. We designed a survey to be sent to a wider base of potential users which asked questions that we had asked in our interviews, as well as feedback on these use cases.

We received 33 responses, of which: 22 participants identified themselves as dispatchers, 8 identified themselves as IT specialists, 2 participants identified as ISSOs, and one participant identified as a cyber security analyst. Not everyone answered every question.

We asked participants to check the North American Electric Reliability Corporation (NERC) functions that their organization handles. The top five NERC roles represented were: Balancing Authority, Transmission Operation, Transmission Owner, Transmission Planner, and Transmission Service Provider. Their organizations provided other functions as well, but the ones listed above were the most prevalent.

Dispatchers noted that their organizations had procedures for dealing with cybersecurity issues that would affect transmission services, but also felt that it was not completely easy to differentiate abnormalities in the system from cyberattacks. They indicated that having a display in the control room to provide awareness of cyberattacks would be useful, and agreed that they would contact the IT specialists, SCADA operations, or cyber analysts when an attack was detected. They felt that more global information would be useful and that they might be the appropriate personnel to determine if a cyberattack was underway. However, there was a lack of agreement as to whether they were the appropriate personnel to mitigate an attack that was underway.

As we only had 8 responses from IT specialists, with only 7 answering the bulk of the questions, we would caution about making generalizations from their responses. We asked the IT specialists if they felt it was important for them to understand how the grid operates. They felt it was very important for them to understand how the grid operates. However, not all of them agreed that they had this understanding. Five of the seven respondents somewhat or completely agreed that the right personnel were involved in handling cyber incidents. All of the respondents somewhat or completely agreed that they communicated directly with

dispatchers on handling incidents. Five of the seven either somewhat or completely agreed that the grid dispatchers had a good understanding of basic security principles. Not all of the IT specialists felt they would be able to support restoring the grid after an attack, and not all were involved in regular training for these incidents or even felt it was important. Not all felt they were kept up to date on changes in the SCADA system and not all felt they had the right contextual knowledge to make many decisions.

We described four different displays and asked the participants which they would find useful and when they would use the display. The four displays were described as:

1. The condition of the control room would be determined by malfunction of breakers, substation alarms, loss of communications from any asset, irregular data coming from any input, and malfunctions of any of the computers available to the dispatchers.
2. The condition of network security would be determined by noticeable traffic increases in and out from a baseline, new IPs accessing or accessed from the system, multiple logins by users, irregularities in the firewall logs, irregularities in the intrusion detection logs, irregularities in the security information and event management system event logs.
3. The condition of the SCADA system would be determined by multiple failed logins, loss of communications from any asset, indications of rogue device(s) on the system, new IPs accessing or accessed from the system, detection of malware on the system.
4. The condition of regional control rooms would be determined by the same set of information as in display #1 from any of the other regional control rooms.

We asked the participants to select all of the displays they would find useful given their area of responsibility. Note that participants could select multiple displays. The results are shown in Table 1.

Table 1
Displays participants found useful—could vote for more than one.

Display one: condition of the control room	11
Display two: condition of the network	18
Display three: condition of the SCADA system	25
Display four: condition of regional control rooms	14

We also asked the participants some questions about using the displays. The questions and results are in Table 2.

We presented all of the participants with three case studies in which three or four events were happening. We asked them to tell us what incidents or combination of incidents would cause them to consider a cyberattack was happening. This section was included to help us design case studies for our initial displays that this audience would find reasonable.

CASE ONE. The incidents are:

a. A breaker is shown as open, even though a control room dispatcher has not opened it and it has not been scheduled for maintenance. The control room dispatcher is not able to close the breaker from the energy management system (EMS) at the dispatcher's workstation.
b. One of the on-duty dispatchers is logged in from both the control room and from an unknown computer.
c. There is a loss of communications from a substation that has shown an open breaker.
d. Two other control rooms in the regions are reporting similar incidents.

Note that participants could select more than one answer in each case. Figure 2a shows the number who noted that these single incidents would indicate a probable cyberattack. Figure 2b shows the votes for a combination of two of these incidents to indicate a probable cyberattack. Figure 2c shows the number of participants who said which combinations of three incidents might indicate a cyberattack. We also asked if all four incidents would be an indication. Participants selected one or more choices of incidents or none if they felt no conditions were indicative of a cyberattack.

CASE TWO. The incidents are:

a. There is a software error in one of the EMS applications that causes the software to crash.
b. There are corrupt files reported on the EMS server.
c. There is unusually high CPU usage on the EMS server.

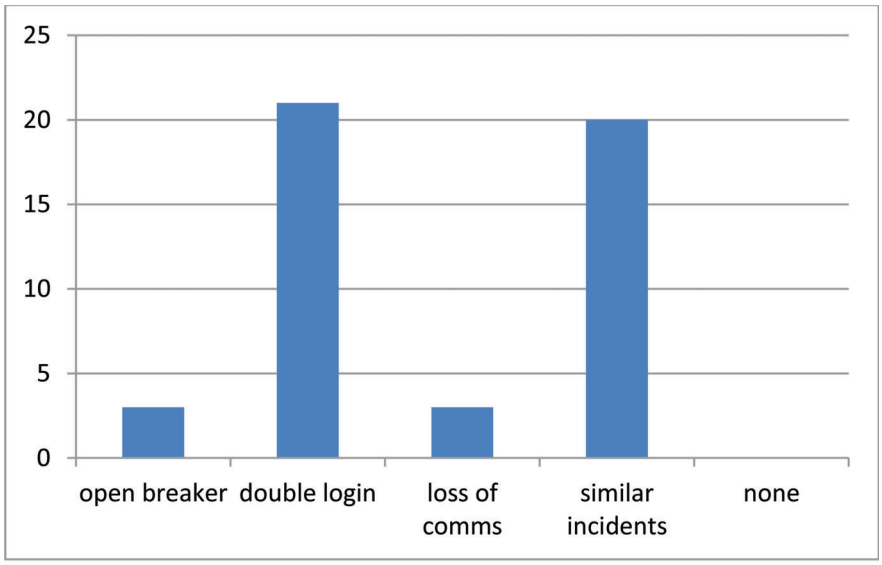
Figure 3 shows the results for this case study. Again, participants could select more than one answer.

CASE THREE. The incidents in this case are:

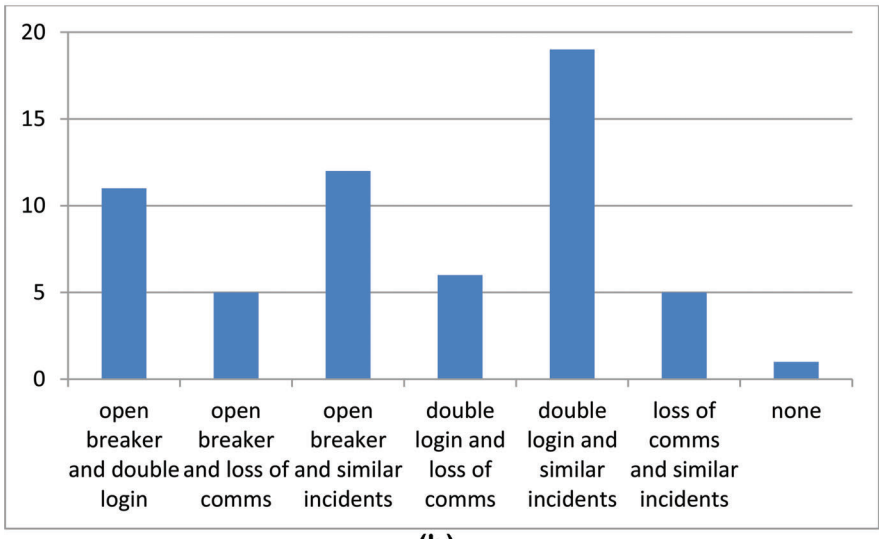
a. There is an indication that there is malware on the EMS server.

Table 2
Questions asked about using the displays.

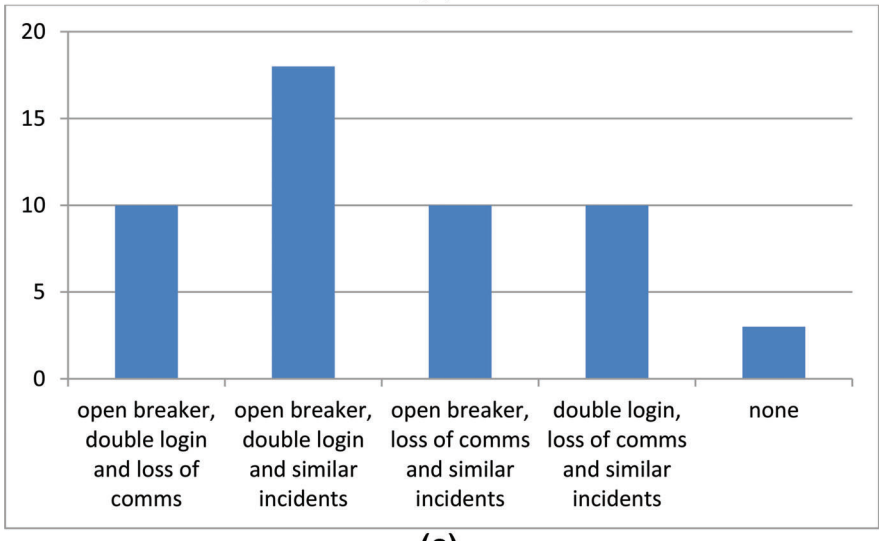
Question	Completely Disagree	Somewhat Disagree	Neutral	Somewhat Agree	Completely Agree
I would only use the display when I encountered a problem in my area	4	6	6	8	5
If I see that another area has a problem as well as my area I will call that area	0	1	3	7	16
It would make it difficult to make a decision if there are indicated problems in multiple displays	4	6	8	7	0



(a)



(b)



(c)

Figure 2. Case study one: (a) one incident; (b) two incidents; (c) three incidents; (d) four incidents. (Figure continued on next page)

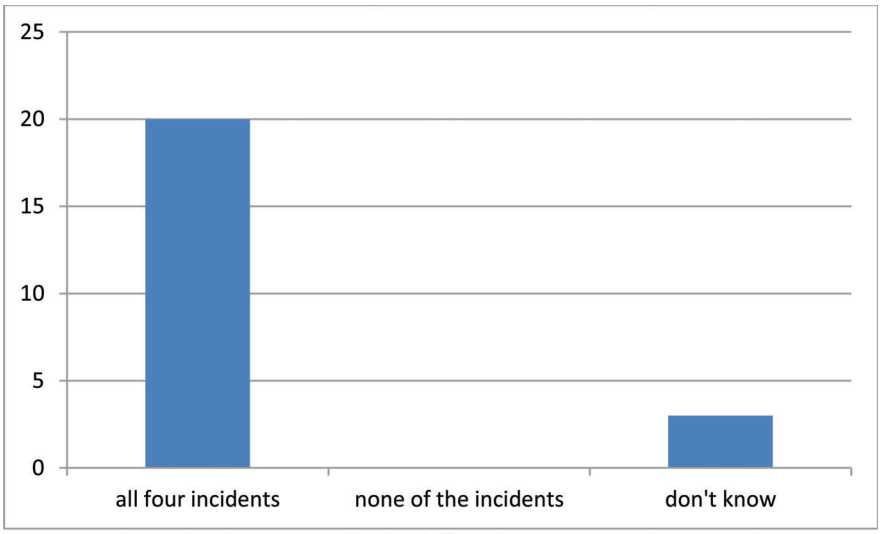


Figure 2b. (Continued)

b. The control room finds that the historian data is incorrect.
c. Another control room in the region has reported an incident.

Figure 4 shows the results for this case study.

Respondents also gave us alternative explanations for the use cases which referenced other established grid conditions, such as equipment failure and forgotten communications. We will utilize this information in designing initial displays and functionality of the tool.

Semi-Completed

For the next phase of our work, we took the information described above and started turning this into a visual design of what a tool might look like. This step is called prototyping and is used to gather feedback from intended users.

We begin our prototyping process with wireframes. These are drawings of the user interface that have the advantage of having enough fidelity to communicate features, interactions, and workflows, but do not require extensive polish or resources to implement. This allows us to get feedback from potential users early and make improvements early, prior to actual software development. Our utility partners are free to critique wireframes, pick pieces they like, throw pieces away, and even redraw them if they are so inclined. Wireframes also allow us to ask about new ideas: if something has been difficult to communicate in words alone, a simple sketch or wireframe provides something more specific for potential users to revise before time and effort is spent to truly implement it. With wireframes, the cost of iteration is low and so early designs can be refined and would also receive user buy-off without requiring lengthy re-implementation cycles.

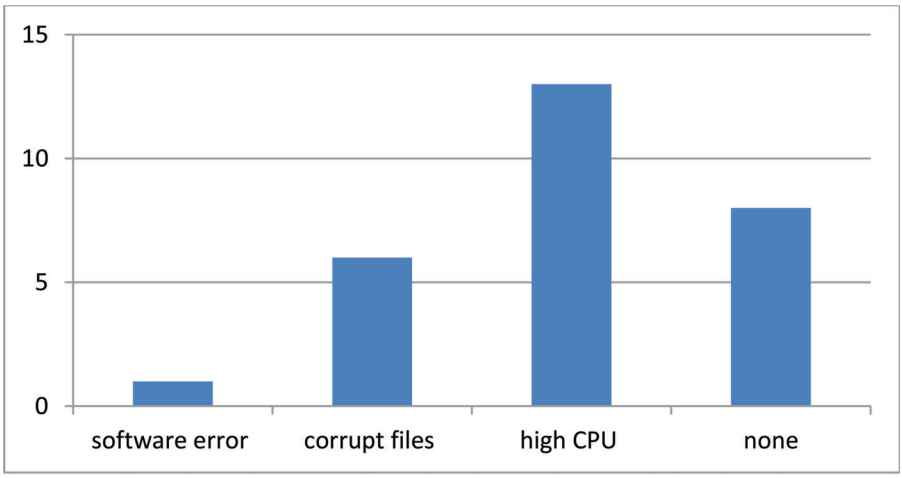
Our first prototypes focused on providing a solution to effectively address a small set of anomalies. Figure 5 shows a wireframe mock-up of the interface we might present to a grid dispatcher to give them information about the events of a use case.

Using the information from our interviews and survey, we felt we had enough information to begin a design of our visualization that would convey information about the real-time status of the enterprise networks, the SCADA network, and the bulk electrical transmission to our three major groups of users.

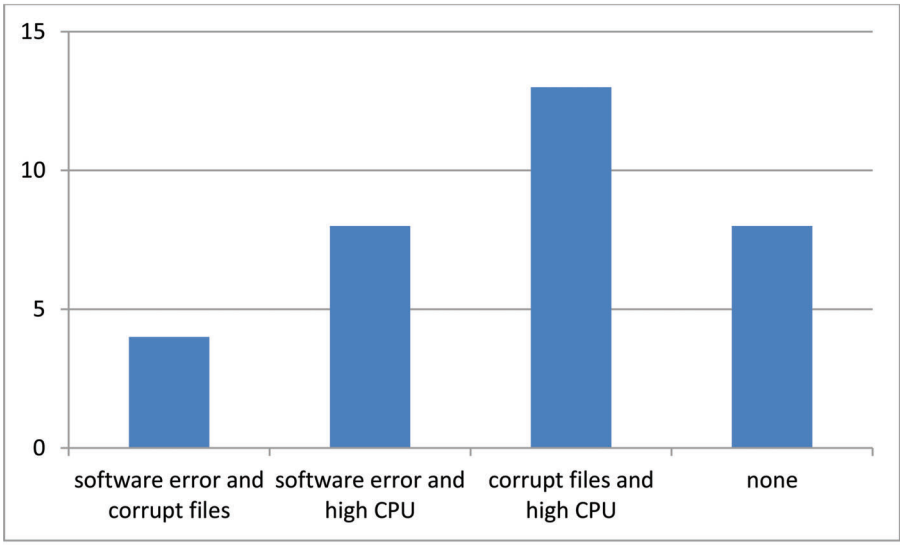
In Figure 5, we provide the dispatcher with a short title and descriptive text to explain the issue detected. In this case, an unexpected remote terminal unit reboot has occurred after a potential substation breach, which makes the reboot suspicious. The dispatcher is also given a list of which resources could be affected or experiencing problems. A list of others in the utility that are also impacted is provided, along with a list of those who have already been notified of the issue and contact information for the personnel responsible for responding to the event. Details about the exact sequence of alarms which brought the event to the dispatcher's attention are provided, along with potential impacts, relevant procedures, and related events.

Figure 6 is a schematic view of a control center and the surrounding substations. This is a second set of wireframes which have also been taken to utility partners for feedback.

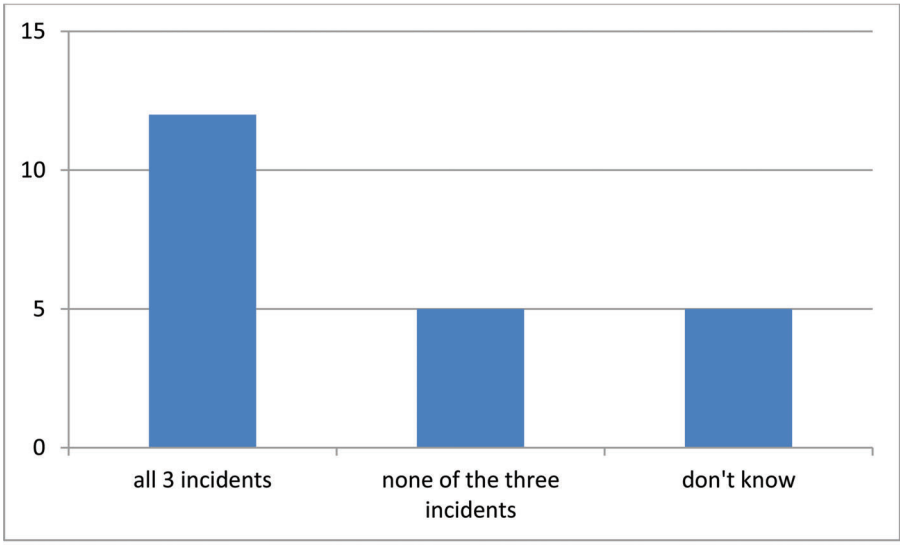
Summary indicators of network activity, alarms, and incidents are provided around the sides of the grid schematic. This wireframe does not directly address a specific use case, but could serve as a high-level view from which a backend system links to details about specific incidents detailed in interfaces such as Figure 5. Feedback was generally encouraging with a few surprises. The primary concerns of our utility partners fell into two broad categories: maintenance of linking information and access to details.



(a)

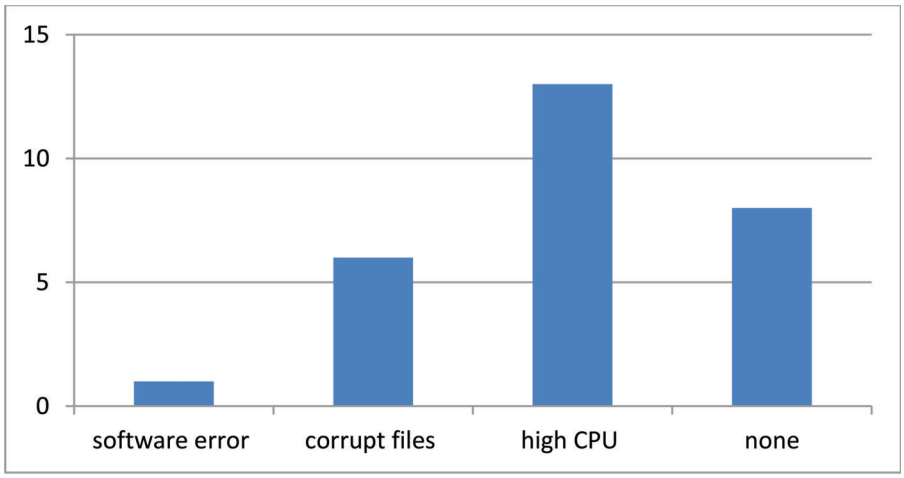


(b)

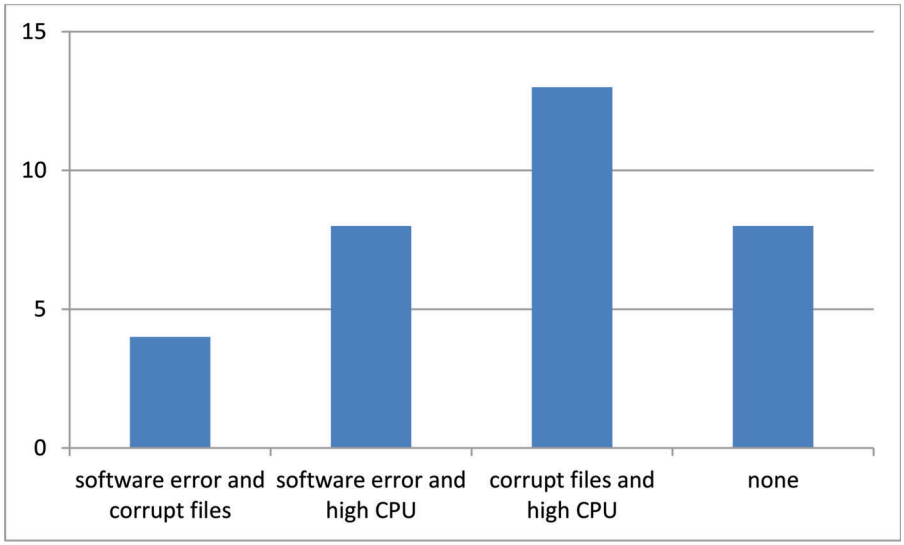


(c)

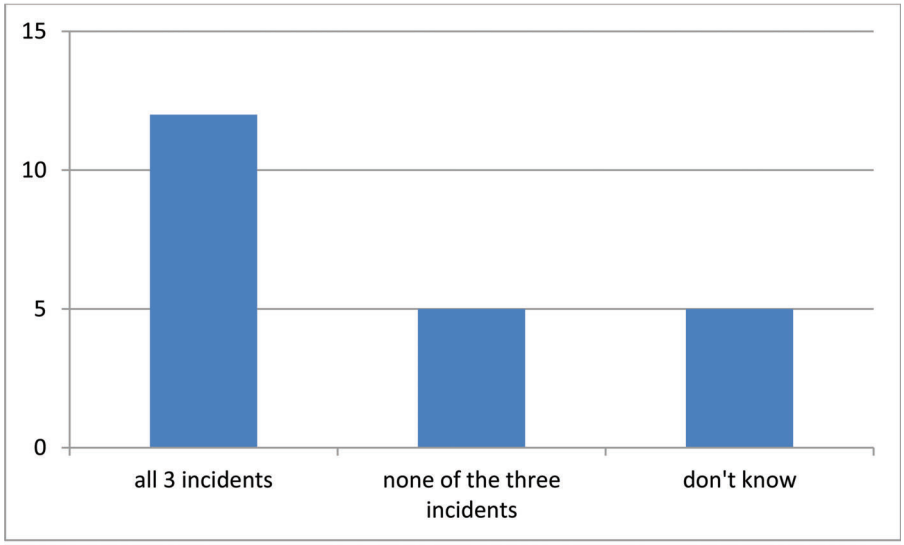
Figure 3. Case study two: (a) one incident; (b) two incidents; (c) three incidents.



(a)



(b)



(c)

Figure 4. Case study three: (a) one incident; (b) two incidents; (c) three incidents.

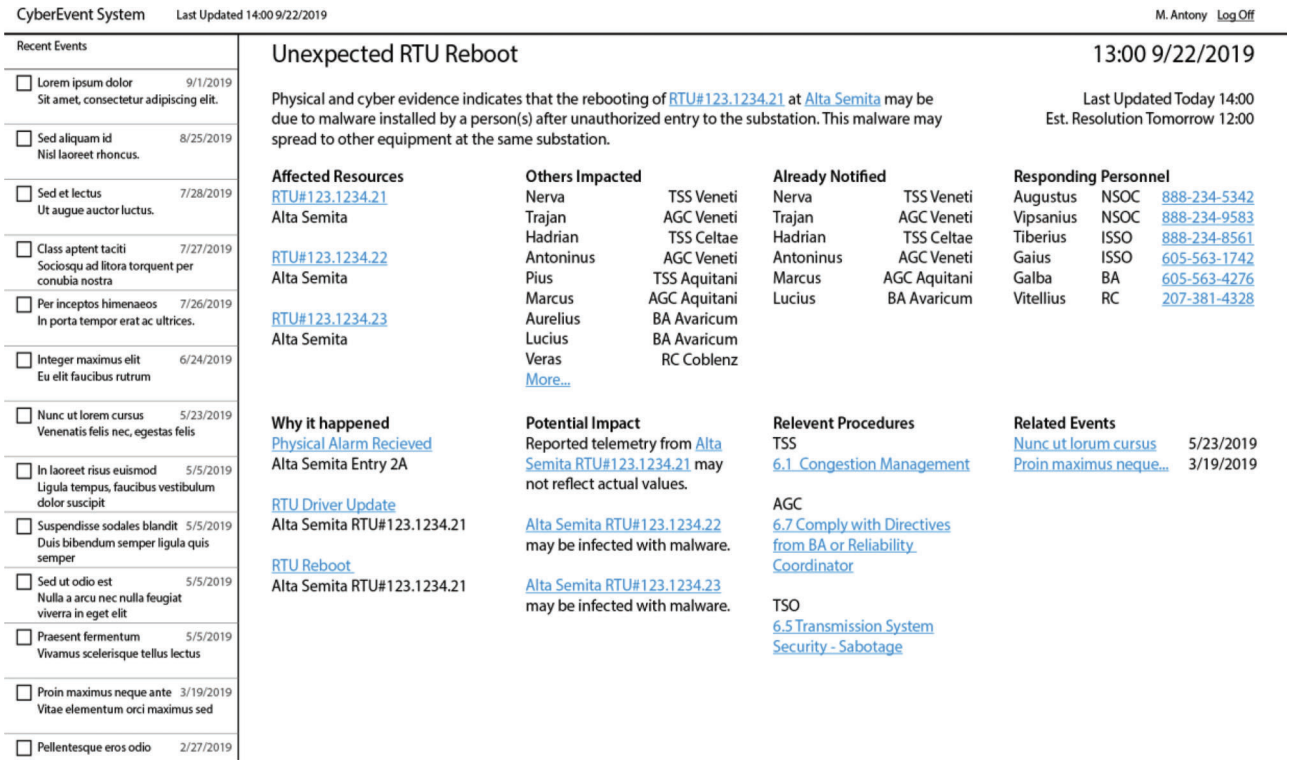


Figure 5. A proposed display showing that a remote terminal unit (RTU) has rebooted unexpectedly.

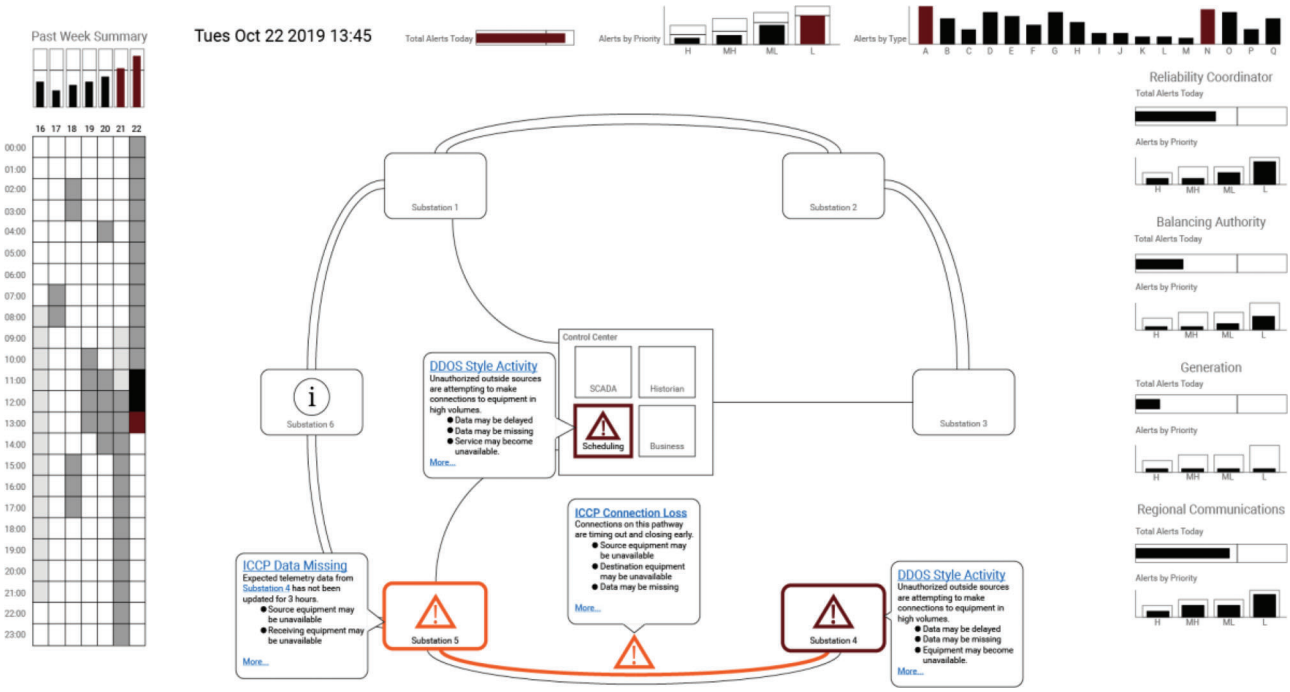


Figure 6. A schematic view of a control center and substations.

Concerns about the maintenance of linking information were focused on the technical feasibility of providing the information to populate the wireframe interfaces and the amount of effort it would require of the technical personnel at the utility to maintain the accuracy of the information. For example, our wireframes provided contact information, such as names and phone numbers of specific personnel who were responding to an event. However, our utility partners were concerned with how this information could be populated and kept up to date, especially in real time.

They had similar concerns with the listing of relevant procedures and the ease of linking procedures to affected equipment in real time.

A somewhat unexpected concern was the dispatchers' interest in making sure that they had access to all the available details through the interfaces. While our field observations and interviews seemed to indicate that dispatchers would prefer an action-oriented set of displays that abstracted all but the most important details, dispatchers specifically asked how they could get specific, detailed, and low-level information when presented with the wireframes. This resulted in a discussion about the need for complete transparency in any system automation and an inherent distrust of the dispatchers towards "simplified" displays. From this discussion, new design ideas arose which imply another round of iteration on our wireframes. Our original idea was to customize information displays by role, and provide grid dispatchers with a simplified view while those personnel directly working on resolving an issue had more details in their displays. Our next iteration will instead feature a shared, collaborative space with clear role-based indications of who is actively working on resolving an issue. All information available will be presented to each person who makes use of the display, rather than separating content by role. This will provide more common ground for occasions when grid dispatchers need to contact other personnel.

The schematic view of the grid in Figure 6 was well received. Grid dispatchers again asked for more detail, specifically the inclusion of additional communication structures in the grid that were not present in the original schematic. They viewed the schematic wireframe as a starting point for alerts generated by the system and envisioned navigating from the schematic "down" to the more detailed wireframe of Figure 5. The additional information around the schematic of Figure 6 was not as well received. Utility partners considered it "noise" that would be ignored most of the time and did not see a need or use for it immediately. Instead, they asked about including information from a higher, regional level to help them detect when problems they were experiencing were affecting the larger grid network.

We will be using this information to iterate on our design and collect feedback on the new design from potential users. Once we have wireframes that are acceptable to our users we will precede to the next step of implementing a prototype and evaluating it on a realistic testbed environment.

Planned Steps

In addition to continuing to refine our prototypes and obtain feedback on the displays, we have three additional steps to undertake. We need to determine the appropriate level of intelligence the tool should have to facilitate sense-making, and then we need to evaluate the utility and usability of the tool functionality and the displays. We need to provide a prototypical testbed to use in this evaluation.

Intelligence in the Tool

In order to provide actionable information for grid dispatchers and cybersecurity analysts at the control center during cyberattacks, the proposed tool should have the ability to ingest, organize, and correlate various information feeds from individual IT and operational technology (OT) monitoring tools that are deployed across the control network. One of the ways to organize this information is to use a structured knowledge representation format. Specific tool information would be organized into "ontologies" that allow the information to be stored and queried efficiently in a graph database. This graph-based representation of information serves as a basis for alert correlation by analyzing the incoming data streams with past data streams to identify emerging patterns and commonalities that point to potential cyberattacks. This framework would enable the replication of the behavior of expert analysts by translating them into well-defined rulesets for query and correlation to discover patterns that may not be obvious to dispatchers and analysts right away. As an extension, the same framework could be used to obtain high-level summaries of information and alerts similar to the ones presented in Figures 5 and 6 that could indicate potential cyberattacks. In addition, this type of knowledge representation would provide the capability to drill down from a high-level summary to the individual alerts that were triggered as part of the individual monitoring tools to further assist the dispatchers and analysts in their decision-making.

Testbed Implementation and Validation

In order to perform proof-of-concept testing and performance evaluation of the proposed prototype displays for dispatchers and cybersecurity analysts, we plan to leverage the Electricity Infrastructure Operations Center (EIOC) and powerNET testbed capabilities at the Pacific Northwest National Laboratory (PNNL, 2016). As part of the EIOC at PNNL, we plan to leverage a commercial EMS software platform that is commonly used across several utilities in North America. We are currently in the process of upgrading this EMS platform to the latest version available, so that we can configure it to perform realistic experimentation.

In order to perform a proof-of-concept and performance evaluation of the proposed tool prototype for enhancing SA, we need to develop, configure, and deploy several resources that are part of a prototypical SCADA environment, such as remote terminal units, intelligent electronic devices, network components (such as communication gateways and routers), and cybersecurity components (such as firewalls, intrusion detection systems, security information and event

management systems, etc.). In addition to deploying several resources, we need to configure these various IT and OT cybersecurity tools to ensure that appropriate data streams are available to the proposed prototype tool for performing advanced analytics to detect anomalies.

Figure 7 shows the conceptual testbed architecture for our experimental evaluation and validation of the developed prototype tool. In Figure 7, the dotted lines represent the security monitoring tools (communication network health, firewall logs, IDS logs). The solid lines indicate control signals and mission tools (SCADA). We plan to leverage the capabilities of the powerNET testbed environment, in conjunction with our EMS platform that is part of the EIOC, to create a prototypical testbed environment for our initial testing and performance evaluations. We will be able to feed in information from the IT and OT cybersecurity monitoring tools into the proposed prototype tool for SA during simulated experimental conditions that would be indicative of a cyberattack as part of our field testing. This prototypical environment, coupled with the subject matter expertise about the various cybersecurity and EMS tools, will enable the iterative design and refinement of potential approaches that present information as part of the developed displays in an effective manner.

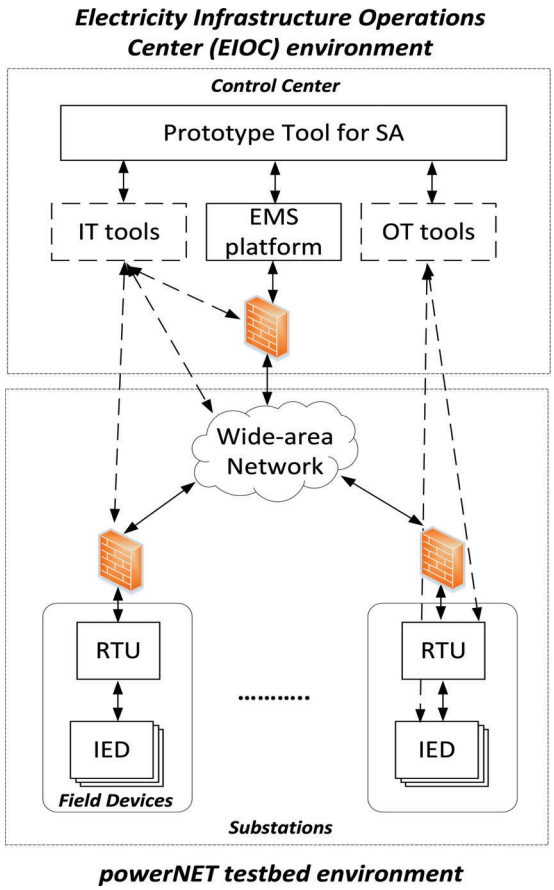


Figure 7. Conceptual testbed architecture for experimental evaluation and validation.

Once we have finalized our prototype of the various displays, our next task will be to use a refined version of the use cases and implement the designs enough to conduct some laboratory testing. Once the EMS system is configured and our displays are installed for the various users, we will invite participants to come and work in a simulated environment in which our SA displays will be featured. After an initial training session about the displays, we will feed in data, and at some point the conditions for a possible cyberattack will appear. We will see if and how long it takes participants to recognize that an attack is occurring. Assuming we are able to get participants representing dispatchers, IT staff, and ISSOs, we are interested in which types of participants notice the conditions first and the communications that occur between the various roles.

While our charter in this work is the design and implementation of the visualization tool, we anticipate that the use of this tool may bring about some organizational changes as well. While our visualization tool can provide the necessary data for communication, additional training and exposure of individuals in the different user groups to the procedures and tasks of the other groups are necessary as well. We suspect that the usability and utility testing we conduct will help to highlight this need.

Conclusion

At this point in time, we have just developed the initial display prototypes and received the first round of feedback on them. Based on that feedback, we are working on a second set of wireframes that we will take back to the customer for feedback.

We found the staff we spoke to very supportive of our work, especially as we were highly engaged in trying to ensure that any additional information we were going to provide was useful to them and would be as unobtrusive as possible to their current responsibilities. While we have had an excellent working relationship with our utility partner, making that initial connection was a long and arduous task. Utilities are skeptical about providing researchers access to their staff due to their workloads, as well as privileged information. We are hopeful that employing the user-centered design process will produce a tool that facilitates the process of rapidly identifying probable cybersecurity attacks and that utilities will find value in this method of tool development.

Our next steps are to further refine our display prototypes and to develop an acceptable level of intelligence for the tool. Once that is done, we will use our testbed to evaluate the usability and utility of the tools using representatives from the power grid in simulated conditions.

One further step that could be extremely valuable is to use our application in a future GridEx study to determine if participants could detect any cybersecurity attacks more quickly using this application. Of course, this would depend on the different injects designed for the GridEx study.

Eventually, we would like to obtain feedback on how many utilities actually install and use the software application. We feel that the human-centric design process has given us insights into a design that provides users with useful and usable software applications.

Acknowledgments

The authors would like to thank the Sierra Nevada Region of the Western Area Power Administration for their support and expertise. This work is done sponsored by the Department of Energy, under DOE Project #M614000331.

Reference

Endsley, M. R. (1995). Toward a theory of situation awareness in dynamic systems. *Human Factors: Journal of the Human Factors and Ergonomics Society*, *37*(1), 32–64. https://doi.org/10.1518/001872095779049543

Ericsson, K. A., & Lehmann, A. C. (1996). Expert and exceptional performance: Evidence on maximal adaptations on task constraints. *Annual Review of Psychology*, *47*, 273–305. https://doi.org/10.1146/annurev.psych.47.1.273

Greitzer, F. L., Schur, A., Paget, M., & Guttromson, R. T. (2008, July). A sensemaking perspective on situation awareness in power grid operations. In *Power and Energy Society General Meeting: Conversion and Delivery of Electrical Energy in the 21st Century* (pp. 1–6). Piscataway, NJ: IEEE.

Pacific Northwest National Laboratory (PNNL). (2016). Electricity Infrastructure Operations Center (EIOC). Retrieved from http://eioc.pnnl.gov

Pirolli, P., & Card, S. (2005, May). The sensemaking process and leverage points for analyst technology as identified through cognitive task analysis. In *Proceedings of International Conference on Intelligence Analysis* (Vol. 5, pp. 2–4).

Scholtz, J., Franklin, L., LeBlanc, K., & Andersen, E. (2016, July). Cybersecurity awareness in the power grid. In D. Nicholson (Ed.), *Advances in human factors in cybersecurity* (pp. 183–193). Cham, Switzerland: Springer. https://doi.org/10.1007/978-3-319-41932-9_15