IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 9 May 2023, accepted 3 June 2023, date of publication 14 June 2023, date of current version 20 June 2023.

Digital Object Identifier 10.1109/ACCESS.2023.3286304

TOPICAL REVIEW

A Review of Visualization Methods for Cyber-Physical Security: Smart Grid Case Study

VICTOR COBILEAN[1], (Graduate Student Member, IEEE), HARINDRA S. MAVIKUMBURE[1], (Student Member, IEEE), BRADY J. MCBRIDE[2], BJORN VAAGENSMITH[3], VIVEK KUMAR SINGH[4], (Member, IEEE), RUIXUAN LI[3], CRAIG RIEGER[3], (Senior Member, IEEE), AND MILOS MANIC[1], (Fellow, IEEE)

[1]Department of Computer Science, Virginia Commonwealth University, Richmond, VA 23284, USA
[2]Department of Electrical Engineering, University of Arkansas, Fayetteville, AR 72701, USA
[3]Idaho National Laboratory, Idaho Falls, ID 83415, USA
[4]National Renewable Energy Laboratory (NREL), Golden, CO 80401, USA

Corresponding author: Victor Cobilean (cobileanv@vcu.edu)

This work was supported in part by the U.S. Department of Energy's Office of Energy Efficiency and Renewable Energy (EERE) under the Solar Energy Technology Office under Award DE-0008775, in part by the effort performed through the Department of Energy under U.S. DOE Idaho Operations Office under Contract DE-AC07-05ID14517, and in part by the Resilient Control and Instrumentation Systems (ReCIS) Program of Idaho National Laboratory.

ABSTRACT Cyber-Physical Systems (CPSs) are becoming increasingly complex and interconnected as they attempt to meet the demands of evolving society. As a result, monitoring and maintaining them becomes a more complex and demanding task for control system operators and cyber defenders. While the literature on visualization techniques in the context of cybersecurity is extensive, the same cannot be said for studies on visualization for the security of cyber-physical systems. This paper aims to fill that gap by: 1) defining the main features of a visualizations workflow for security visualizations in cyber-physical systems. The workflow includes the acquisition of cyber and physical data, processing of data, selection, and configuration of both visualization tools and end-user interactions. 2) Providing an overview of cyber-physical security visualization systems, with a focus on smart grids as a case study. Finally, we use the perspectives gained from this analysis to provide insights and directions for future research and design of cyber-physical visualization techniques.

INDEX TERMS Cyber-physical security, cyber-physical system visualization, data visualization, human factors, resilience, situational awareness, grids.

I. INTRODUCTION

Cyber-Physical Systems (CPSs) combine the dynamics of physical processes with those of software and communication. Physical systems, networking, and computers interact in ways that necessitate whole new design technologies [1]. CPSs are increasingly being deployed in critical infrastructures. Prominent applications of CPS include industrial control systems (ICS), smart grids, and intelligent transportation systems (ITS) [2]. As cyber-physical systems become more complex, so do the opportunities for an attacker to interfere with them. The increased interconnection of these systems has resulted in new vulnerabilities and risks. A cyber attack on power infrastructure could cause widespread outages, while one on medical equipment, for example, might harm a patient. Among the prominent applications of CPSs, in this paper, we will focus on smart grid systems.

The smart grid is envisioned as the next generation of the power grid, which has been used for decades to generate, transmit, and distribute electricity. The smart grid offers numerous advantages and cutting-edge functions. It provides improvements in emission control, global load balancing, intelligent generation, and national energy savings. It also gives local consumers more control over how much energy

The associate editor coordinating the review of this manuscript and approving it for publication was Yu-Chi Chen.

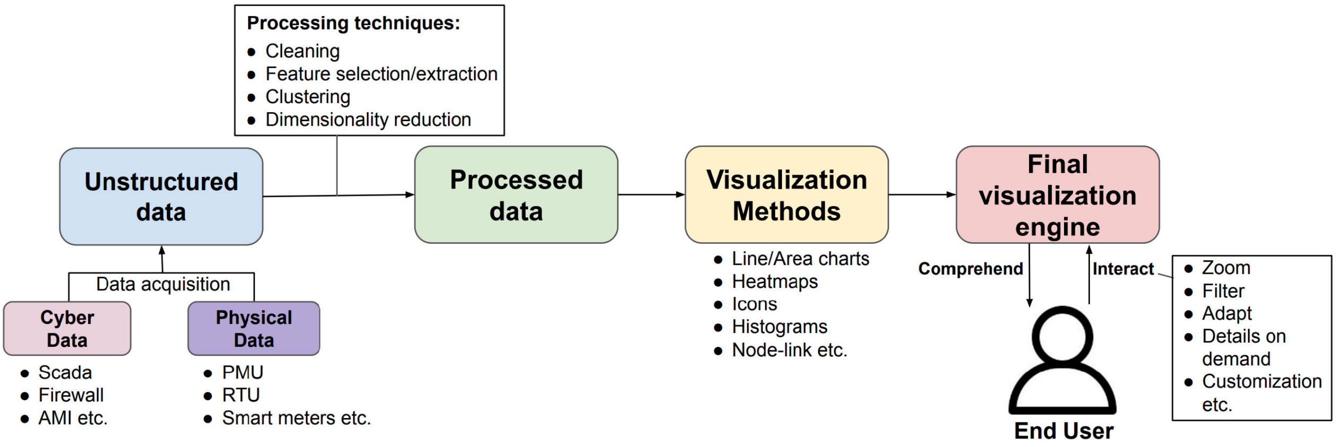


FIGURE 1. Visualization workflow.

they use, which is beneficial to both the economy and the environment [3]. The smart grid is composed of two major parts: 1) power application and 2) supporting infrastructure [4]. The power application manages the main tasks of the smart grid, notably the generation, transmission, and distribution of electricity. The supporting infrastructure, on the other hand, is the intelligent part of the smart grid that is mainly concerned with managing and monitoring the key functions through the use of various pieces of hardware, computer programs, and communication networks.

Smart grids and their security and resilience have been at the core of critical infrastructures for many decades. Even though smart grid system connectivity has resulted in numerous benefits, many challenges have come up, including security, reliability, stability, maintainability, and safety [5]. Malicious attacks have disrupted system operations or resulted in the theft of sensitive data, and these attacks can start with an attack on either the cyber infrastructure or the physical components.

In 2007, the Department of Homeland Security of the USA staged a cyber-attack demonstration code-named "Aurora" resulting in the destruction of a diesel generator that was widely utilized across the US [6]. Recent incidents (e.g., Stuxnet [7], Ukraine power grid outage [8]) have shown that sophisticated and stealthy attacks (and faults) can result in catastrophic consequences to the economy, environment, and even human lives. Thus, it is paramount important to ensure the security of CPSs and smart grids.

A key aspect of detecting attacks is to provide enough information awareness to operators of control systems. To identify attacks and unexpected errors in smart grids and other CPSs an anomaly detection system (ADS) is required. Anomaly detection systems provide information about the detection of attacks, however, visualization of such information will facilitate more understanding of the attack to the system operator [9]. Effective visualizations would achieve a higher degree of operational assurance by providing explainable visual information on abnormal behavior and affected devices of the system. This will provide a better understanding for the system operator about what happened in the system and which actions to take. Therefore, we can infer that visualization tools play a major role in making smart grids secure and resilient. As the reported occurrences of cyber-physical attacks increase exponentially [10], it is imperative to develop and employ tool sets that enhance the user's ability to investigate, understand, and therefore mitigate the impacts of future events on smart grids and other cyber-physical systems.

Visualization tools are intended to be an effective means of communicating data to quickly spur insightful actions through visible patterns, trends, structures, and exceptions, resulting in improved system security [11]. In today's data-driven world, we can collect and use data to help decision-makers make informed and well-founded decisions. The push for renewable energy, increased demand for electric power, and upgraded intelligent power grid equipment (e.g., advanced grid meters, smart relays, etc.), have resulted in increased data streams and complexity of systems, as well as challenges related to controls of such systems [12].

The process of visualizing the state of the cyber-physical system is linked to the process of transforming raw unstructured data into information that can be represented using objects of varying shapes, colors, and dimensions. These objects should help understand the state of the system by facilitating the analysis of large amounts of data [13]. Figure 1 illustrates the various steps and actions involved in the visualization process. This diagram provides a comprehensive illustration of workflow throughout the process of transforming raw data into the final product, which is an interactive visualization designed to improve the security of the system [14].

Because of the clear lack of survey papers on the topic of visualizations for enhancing the cyber-physical security and resiliency of smart grids, we performed an analysis of related literature to provide a synthesized overview of the research on this critical topic. We hope to support both researchers and industry partners by offering an overview of the state-of-the-art techniques and best practices in this field. Our aim is to facilitate a unified understanding of the use of visualizations in CPS security, ultimately promoting more effective and efficient security practices.

The main contributions of the paper are:

- An analysis of the visualization workflow (desired features and characteristics).
- A review of existing work for smart grid security visualization.
- Analyze the challenges and key findings discovered during the review process regarding the visualization's design and implementation for the security of CPS.
- Identifying the potential future research directions for the successful use of the visualization tools.

The rest of the paper is organized as follows. Section II provides an overview of the related work in the field of data visualization. Section III presents in detail the main points and key features of the visualization workflow. An overview of different visualization methods for smart grid case study broken down into two classes (**monitoring** and **planning and discovery**) is covered in section Section IV. Section V discusses current challenges and key findings from the review of cyber-physical visualization research, as well as potential future research directions. The conclusions of the paper are provided in the final section.

II. RELATED WORK

In today's world, we generate and store vast amounts of unstructured data that may help us discover new knowledge and insights in cases we can aggregate into a meaningful picture [15]. The authors of [16] and [17] conducted a comprehensive survey on data visualization tools. This survey not only provided a taxonomy of data visualization papers but also highlighted the most effective techniques for optimizing the performance of data visualizations, as well as discussed the challenges and future opportunities in this field. Similarly, in [18], the authors performed a survey on techniques that can improve the efficiency of data visualization. In some reviews, such as those presented in [16] and [19], the focus is on analyzing the advantages and limitations of software tools used to generate visualizations.

The ability to process, store, and analyze vast amounts of data, commonly known as big data, is an interesting and hot topic in the research community [20]. Numerous surveys have investigated the challenges and solutions associated with visualizing big data [20], [21]. In [22], the authors address the problem of high-dimensional data and explore various solutions for visualizing it. Other papers focus on the visualization of specific types of data: ensemble data [23], event sequence [24], multivariate spatial data [25], graphs [26]. Furthermore, certain surveys concentrate on analyzing papers that focus on a specific domain or task: traffic data visualization [27], security [11], [28], [29], [30], Internet of Things [31], [32]. A promising research direction in visualization involves the integration of machine learning algorithms in the visualization process to automate the processing step of the data or recommend visualizations that are more useful for each user [33], [34], [35].

Given that cyber-physical systems involve a cyber component, an important area of interest is the representation of visualizations for cybersecurity. In [28], the authors presented a survey with a security visualization based on network logs. Similarly, the authors of [11] conducted an extensive review of the field and classified visualization tools into categories such as host/server monitoring, internal/external monitoring, port activity, attack patterns, and routing behavior. Jiang et. al. [29] performed a systematic review on cyber situational awareness visualization. In terms of physical security visualization, we can mention a review that has addressed the visualization of time-series data produced by sensors [36].

After conducting extensive research, it was identified that there is a lack of surveys on visualization methods specifically designed for cyber-physical systems security. This review will concentrate on visualization solutions that can be applied to smart grid security. While there are surveys that target the visualization and analysis of data in smart grids [12], [37], [38], they do not specifically review the security aspect of smart grids, but focus on monitoring other features such as carbon footprint. As a result, this review will rely on papers that provide visualizations for cyber-physical systems but can be applied to smart grids, as well as tools designed specifically for smart grid security. We will extract useful insights from papers that focus on cybersecurity or time-series data monitoring separately to provide a more comprehensive discussion section and to describe the visualization workflow in detail.

We conducted an extensive literature review by searching four databases: IEEE Xplore, Web of Science, and Scopus. We used the following search query "Visualization AND (security OR cyber OR physical OR CPS)" and "Visualization AND (review OR survey)" to select relevant papers on the topic. Our search yielded a total of 326 publications. From our analysis, we observed that the majority of the articles focused solely on cyber-security, and there is a limited number of papers that tackled the problem of security in cyber-physical systems. We could only identify a limited number of papers that had a finalized prototype of the visualization engine, and these papers were selected for review in Section IV.

III. VISUALIZATION WORKFLOW

The success of a security visualization system will be impacted by a multitude of factors such as the quality of available data and its attributes, the specific tasks that are associated with the visualization, the end-user preferences, habits, and expertise in the domain, the selection of visualization techniques that will be incorporated in the final visualization engine [39]. These steps are illustrated in Fig.1 and are part of a visualization workflow.

TABLE 1. Overview of different types of data.

Data	Applications	Properties	Sources
Cyber Data	Network Monitoring	Network Packets, Port Numbers System logs, Network flow events Proxy logs, Firewall logs Network flow events, DNS data DHCP logs, I/O User authentication activity	Network Switches DHCP servers SCADA systems Firewalls System logs Advanced Metering Infrastructure (AMI) Distribution Man agement Systems (DMS)
Physical Data	Topology visualization, Load/generation forecasting	Ambient temperature, Humidity Wind speed, Direction and geographical area voltage, power irradiance measurements	Smart meters, PMUs, Micro PMUs Field measurement devices programmable thermostats Sensors installed on grid-level equipment (e.g. transformers, network switches) Programmable Logic Controllers (PLCs) Remote Terminal Units (RTUs)

In this section, we will discuss each of these factors in detail and provide an in-depth analysis of their main characteristics. Firstly, we will describe the different types of data and the techniques used for processing raw data, which are typically used in visualizing smart grid security. Then, we will present the most common visualization methods and tools, along with their typical use cases and the associated data. Furthermore, we will outline specific tasks that can be involved in enhancing the security of cyber-physical systems. Finally, we will discuss the adaptability of visualization to the end user, and the expected interactions from the end user.

A. DATA AND PROCESSING TECHNIQUES

Cyber-physical systems generate increasing cyber and physical data. The following paragraphs will define cyber and physical data and how the raw data is processed to visualize such systems.

Cyber data includes items, such as network packets, port numbers, system logs, network flow events, proxy logs, firewall logs, DNS data, DHCP logs, I/O data, user authentication events, CPU, RAM, and other information. Intrusion detection systems (IDS) and intrusion prevention systems (IPS) may generate additional cyber data, such as raw-log insights or specific pattern detection [40]. Moreover, supervisory control and data acquisition (SCADA) systems, Advanced Metering Infrastructure (AMI), Distribution Management Systems (DMS), and Cybersecurity tools such as firewalls are also sources of cyber data [41]. While this data is often monitored and reviewed by experienced analysts, cyber data is one of the most difficult types of data to visualize in real-time. In [42], authors remark that part of this difficulty stems from the technical factors (what mapping strategies are possible for the given data) and the human factors (what type of visualization makes sense to the user). The sheer amount of cyber data that is generated by network and system monitors (scalability) can also make visualization difficult [11]. Despite these challenges, there are a wide variety of tools available for cyber visualization including FlowTag, NVisionIP, security information and event management (SIEM) [43], IDS RainStorm, and Netvis [42]. The most common data types for this type of data are numerical (temporal and multidimensional) and categorical. The logs and reports will frequently imply analyzing text-based information.

Physical data can be defined as data that relates directly to the physical world, such as measurements on ambient temperature, humidity, wind speed, and direction, and geographical area, voltage, irradiance, and cloud cover [44]. Physical data also refers to the current state of a physical system based on the available internal sensor measurements, upon which people, like grid operators, are dependent to make judgment calls about their systems. For physical data measurements, they are often visualized in the system software (i.e. RTAC management software, MATLAB, etc.). This type of data will be described using numerical features in the case of sensor data and categorical features in cases where it is needed to identify the state of a component, e.g., if the switch is on or off. The main data sources are Smart meters, PMUs, Micro PMUs, Field measurement devices, Programmable thermostats, Sensors installed on grid-level equipment, (e.g. transformers, network switches), Programmable Logic Controllers (PLCs) [45]. Table 1 provides a summary of the data types produced by cyber-physical systems which can be included in the security visualization.

Data processing techniques: In this step, we are dealing with the problems related to big data [46]. And the main problem occurs in the cases of real-time security visualization (monitoring) or when the amount of data is so massive that it can overload the buffer. In this case, it is required to compress the size of the data or select the data that is most suggestive and remove the data that is redundant. Data normalization techniques are used to bring the data within a common scale to avoid any bias towards a particular feature. The most used techniques for data processing are feature selection and extraction, clustering, and dimensionality reduction [36], [47]. Moreover, the sliding window technique is an essential method for analyzing time series data [48]. It involves dividing a long time series into shorter, overlapping segments or windows, allowing for a more precise analysis of the data. One of the main advantages of using a sliding window is that it can capture local patterns or trends in the data that may not be apparent when considering the entire time series as a whole.

B. VISUALIZATION METHODS

There are many types of visualization methods that can be used for displaying security-related data and the choice of these types of visualization depends usually on the message that needs to be communicated and the time constraints for the visualization. In this section, we will discuss the most common techniques, the strengths of each display, use cases, and how they are adapted to specific security needs [49].

The most common use cases and types of visualization tools are:

Visualization of data trends: Most of the stored data from CPSs is continuous time-series data, so the most intuitive study that can be performed is noticing changes and changes over time. The most popular techniques are line charts and area charts. As well it is possible to visualize trends in multidimensional data using parallel coordinates [50] or radial displays [51].

Visualization of data correlations: These types of visualization are designed to emphasize the strength of the relationships between displayed variables. The most used visualization are scatter plots [52], bubble plots which represent the variation of scatter plots in three dimensions where the third dimension is the diameter of the bubble, and heatmaps, where the color intensity suggests the strength of the relationship.

Visualization of data distributions: The visualization of distributions is useful for better understanding the data and its characteristics, which can help identify outliers. The most common types of distribution visualizations are histograms for highlighting the frequency of an event [53], box plots for displaying the range of the data, and violin plots for visualizing the shape of the distribution.

Network visualization: This type of visualization is suitable for representing the complex structure of cyber-physical systems and how elements are connected. It is a very useful tool for tracking the overlapping physical and cyber layers of the system. The main idea behind these visualizations is to represent system components as nodes and relationships between components as edges [54].

Hierarchical visualizations: The visualization of this category display the data in a hierarchical structure, where each level represents a different level of abstraction. It can be beneficial for discovering interdependencies between components. Typical choices in this category are treemaps, which consist of nested rectangles of different colors and sizes, and each rectangle represents a node, and the color and size may suggest different properties of the node [55]. For highlighting dependencies between different levels tree diagrams and dendrograms can be used.

Iconic visualizations: An abstraction that aids in data analysis and comprehension is an icon-based representation of high-dimensional data. The attributes of the icons, such as color, shape, and size, are linked to the features of the high dimensional data [56].

Fusion of the methods: In this case multiple cases that were presented before are used simultaneously for providing multiple angles of the available data to transmit more useful information at the same time [57]. For example, a map that shows the status of various components of the system using icons [58]. Additionally, treemaps and icons can be used in combination to display additional information about a component rectangle. Using multiple types of data or visualizations in this manner allows for a more comprehensive understanding of the data.

C. SPECIFIC TASKS RELATED TO VISUALIZATION

It is clear that the main goal of the visualization mentioned in this paper is to enhance the security of the cyber-physical system, but at the same time, we can identify two main tasks that are directly related to this goal: monitoring of the system and situational-aware discovery and planning.

Monitoring: These visualization systems are designed to support the user's decision-making process in real time during the monitoring process. It is important to design the visual aspects of these tools with user efficiency in mind. The data and visual tools should be selected in a way as the decision-maker may identify the affected portion of the system and the possible propagation of the attack through the system.

Discovery and planning: Based on the literature review we can define this task for two subcategories based on the temporal use-case: **1. preemptive use** and **2. root-cause analysis**. These tools are not subject to the same time constraints as real-time monitoring, data processing can be done offline, and more time is available for rendering complex visualizations. These tools heavily rely on the quality of data and algorithms used for extracting features that will facilitate developing hypotheses to identify vulnerabilities before they are exploited or to identify the root cause and develop a recovery plan after an accident happens.

1. Preemptive use: These types of visualizations are designed to assist in the prevention of attacks/events. They are extremely useful during the design process of cyber-physical systems, or vulnerability and/or resilient assessments. This type of visualization will commonly compute a lot of if/then scenarios, to identify vulnerabilities. By providing multiple perspectives, the decision-makers can better identify areas of improvement or weakness in the resiliency and security of the system.

2. Root-cause analysis: This use case intends to aid the user in the investigation of cyber-physical events after they have occurred. The application of the visualization tools aims to provide insights and perspective through visual techniques displaying logged attack data. These insights and perspectives are used to assist the user with the understanding of the cyber or physical event and inform the decision-making process in taking steps to mitigate such events in the future.

D. END-USER EXPERIENCE

In this section, we emphasize the factors that can enhance the overall end-user experience when it comes to visualizations: interactions and adaptability. To ensure the success of a task based on a security visualization, it is important that the end-user can easily understand the information presented through the visualization. However, the time needed to comprehend the presented data can depend on their prior knowledge related to the domain and preferences. This poses a significant challenge, as there can be significant differences between the needs and preferences of cybersecurity specialists, engineers, or higher management who are responsible for the security of a cyber-physical system. To address this issue, end-users should be able to interact with the visualization and the most common interactions described in the literature are: zooming, filtering, details-on-demand, relate, history, extract [59].

Furthermore, the visualization can include the possibility to dynamically adapt to the user based on data gathered from previous interactions. For example, a machine learning recommendation system that uses data from users from the same categories as previous interactions could be implemented to provide a more personalized and efficient experience. By implementing these strategies, end-users can better perceive and understand the information displayed by the visualization.

IV. USE CASE: SMART GRID SECURITY VISUALIZATIONS

In this section, we will discuss the strengths and weaknesses of each type of visualization solution, as well as the important attributes of each analyzed solution. The reason for categorizing the solutions as real-time monitoring and discovery and planning is that the primary task for which the solution was designed, as well as time constraints, will have the greatest influence on the choice of processing techniques, visualization tools, and the amount of data that can be effectively visualized.

Subsection A describes the visualizations for monitoring tailored towards a short-term, immediate decision-making targeted approach (real-time). Subsection B presents the planning and discovery visualization may refer to the two-time categories related to anomalies: 1. visualizations that help to identify vulnerabilities during the design phase of the system and 2. visualization tailored towards forensics, i.e. understanding why certain events have occurred, and finding the reason that led to those events. Table 2 illustrates visualization systems reviewed in this paper.

A. MONITORING TASK

Monitoring is commonly associated with making short-term, real-time decisions. Monitoring visualizations should provide two main tools for the operators: 1) real-time visualizations for identifying anomalous behavior, and 2) meaningful information for fast, short-term decision-making for securing unaffected components of the system and rapidly solving the issue in the system. For example, when a grid is attacked by sensor spoofing, the operator should be able to quickly identify which part of the system is under attack and make decisions to prevent the spreading of the attack to the other parts of the system. Monitoring visualizations should be simple and interactive enough that system operators understand the system state to take rapid operational decisions. The main challenges for the tactical visualizations are 1) high volume and velocity data processing, 2) suggestive representation for taking rapid actions, 3) interdisciplinary representations, and 4) situational awareness.

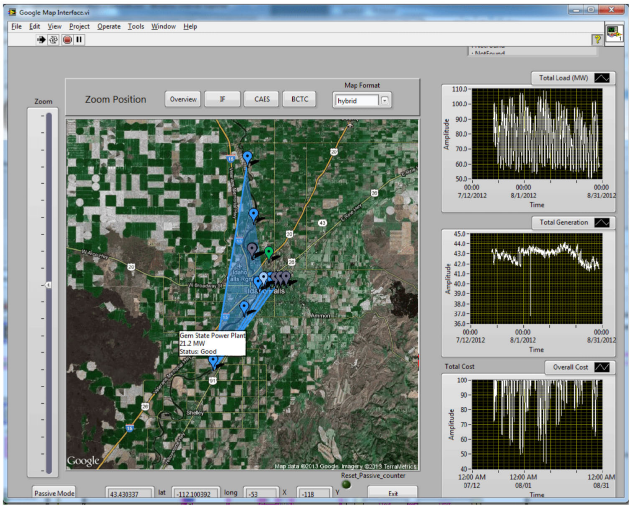


FIGURE 2. Data Fusion Tool - Example of visualization of sources related to a sensor or cyber event based on associated IP Addresses [60].

By leveraging specific data characteristics in smart grid applications, we can create dynamic visualizations that adapt to real-time changes. For example, we can exploit the periodicity of sensor data, including amplitude or frequency, to develop a tool that can detect and highlight any deviations in these measurements. This approach was presented in Data Fusion Tool [60]. The visualization engine highlights the regions affected by cyber-physical events, as presented in figure 2, and assists in the discovery of meaningful correlations that provide operators with useful context.

Node-link diagrams are a powerful tool for visually representing relationships. The authors of [61] used this type of visualization tool to represent the complex interconnections between loads and generators. The main goal of the visualization engine is to draw the attention of the operator to the anomalous subsystems by highlighting the affected nodes (load or generator) in red. This tool facilitates the identification of alternative generators capable of supplying energy to the load.

The work of [63] is focused on using the PMU data for determining the stability boundary of the system and monitoring if the system is in safe working conditions. The visualization [62] determines the safe conditions using PMU data and random bits forest algorithm. The most relevant features

TABLE 2. Overview of visualization systems reviewed.

Visualization system	Data	Data Processing	Visualization methods	End-user adaptability	Year
		Monitoring			
Data Fusion Tool [60]	Alerts from ADS, cyber communication, sensor data	Clustering	Line charts and map with icons	Configuration tools and zoom	2013
Chopade *et. al.* [61]	Power and voltage levels	-	Node-link, maps with icons	-	2012
Liu *et. al.* [62]	PMU	Feature selection, Pearson correlation, Random Bits Forest	Diagram of the system	-	2020
Su *et. al.* [63]	PMU	Computes the stability boundary	2D plot of the stability boundary and current state	-	2017
CyberSAVe [64]	Sensor data	Computing the "cyber trust"	Histogram, bar and line charts, icons	Details-on-demand	2013
MAHIVE [65]	Cyber Communication (DNP3, MODBUS, TCP/IP)	Dimensionality reduction	scatter plots, bar charts, and numerical displays	-	2021
Sundararajan *et. al.* [66]	Unstructured alerts and logs from security tools	Classification with LSTM/RNN, Multiple imputation, linear correlation, linear/polynomial regression,	Bar charts, Histogram	Dynamic customization	2018
Cyber-Energy Emulation (CEE) Platform [67]	Network traffic, Unstructured alerts and logs from security tools	Custom event manager, message-queuing system	3D Visualization engine	Dynamic customization	2020
Saxena *et. al.* [68]	Cyber communication, RTU measurements	Extracting features from DNP3 packets	line graphs, numeric data fields, map	-	2017
Le Blanc *et. al.* [69]	SCADA updates, RTU, IDS alerts	-	Text, icons, node-link	Surveys. analysis of past interactions	2017
Scholtz *et. al.* [70]	Unstructured alerts and logs from security tools	-	Node-Link, Bar, Histogram	Surveys	2018
Lohfink *et. al.* [71]	Cyber communication	Extraction of response frequency	Spiral Chart, Graph representation	-	2020
Vaagensmith *et. al.* [72]	Cyber communication, sensor data	Machine learning	Line graphs, Bar Charts	Multiple displays for different roles	2021
		Discovery and planning			
Bakirtzis *et. al.* [73]	System architecture	Compute the attack vectors	Node-Link	Filtering, search, details-on-demand	2018
Wu *et. al.* [74]	Cyber communications, sensor data	Statistical analysis, machine learning	Radiation Pattern, Scatter Plot	Attacker/defender displays	2020
Jovanovic *et. al.* [75]	Sensor data	Compute resilience level	Line chart, Text, 3-D Matrix Cube, Node-Link	Dynamic customization	2021
Ibrahim *et. al.* [76]	System architecture, known vulnerabilities	Generating attack graphs	Node-link	-	2020
Le *et. al.* [77]	Known vulnerabilities (CVE)	Generating attack graphs, compute security metrics	Node-link	-	2022
PERCIVAL [78]	System architecture	Generating attack graphs	Node-link, text	Zoom, select nodes	2015
Yan *et. al.* [79]	System architecture, load distribution	Graph analysis	Node-Link,map	-	2012
Macedo *et. al.* [80]	Sensor data	Machine learning	Line and Bar charts	-	2021
Kopylec *et. al.* [81]	Geographical information, Unstructured alerts and logs from security tools	Generating attack graphs	Text, graph	Cyber and physical layers displays	2007

are selected using bagging nearest-neighbor and Pearson correlation.

The Cyber Situational Awareness Visualization (CyberSAVe) [64] utilizes several algorithms and visualization techniques to detect various types of attacks on the smart grid. This approach views the complex system as being composed of nodes. This visualization tool solves the problem of the high volume of data by fusing all available data and measuring against the single "cyber trust" metric in order to enable users to make critical decisions. Cyber trust at the level

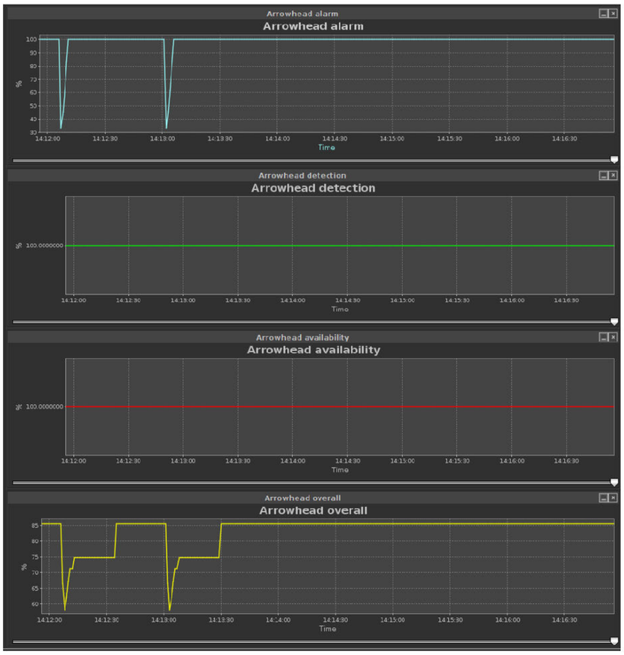
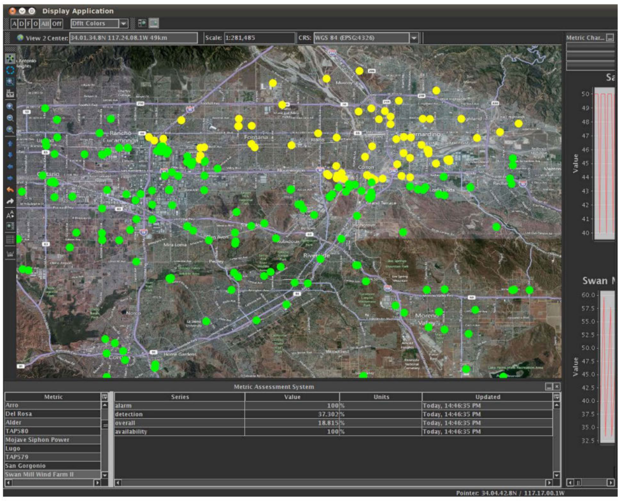


FIGURE 3. CyberSAVe - The Metric Assessment System displaying three components of trust displaying single node metrics (local view) [64].

of nodes (sensors) refers to sensors' availability, ability to accurately detect measured values, produce few false alarms, and how trustworthy future measurements are predicted to be. The calculated level of trust for a particular sensor can be used to isolate a sensor targeted by an attack. Figure 3 demonstrates a time history plot of a single node (sensor) by displaying the three components of the cyber trust metrics (alarm, detection, and availability) and thus the overall trust of the node.

Situational awareness is suggested by the fusion of a geographical map and the nodes in the smart grid that provides information to the system operator about the impacted nodes and their interconnection to the other parts of the system. Individual nodes in the geographical system are represented using a color-coded format. This differentiation by color allows the operator to gain a quick insight into the trust of each individual node while also giving insight into the overall system state. Figure 4 illustrates the holistic view of the visualization tool used for smart grid security from a geographical perspective in the CyberSAVe system.

The Modular Analysis Hierarchical Intrusion Detection System Visualization Event (MAHIVE) [65] displays various data related to intrusion detection such as alerts, logs, and categories of events such as SSL, DNP3, or file-related alerts. The visualization dashboard for the MAHIVE Alert system uses scatter plots, bar charts, and numerical displays to present anomaly detection system-related data. While the presentation of this system is limited in terms of the current state of its visualization capabilities, the authors have identified various topics of future work for improving the system.



View 2 Center: 34.01.34.8N 117.24.08.1W 49km   Scale: 1:281,485   CRS: WGS 84 (EPSG:4326)

Metric Assessment System

Metric
Arro
Del Rosa
Alder
TAP580
Mojave Siphon Power
Lugo
TAP579
San Gorgonio
Swan Mill Wind Farm II

Series	Value	Units	Updated
alarm	100	%	Today, 14:46:35 PM
detection	37.302	%	Today, 14:46:35 PM
overall	18.815	%	Today, 14:46:35 PM
availability	100	%	Today, 14:46:35 PM

Pointer: 34.04.42.8N / 117.17.00.1W

FIGURE 4. CyberSAVe - global view of multiple nodes [64].

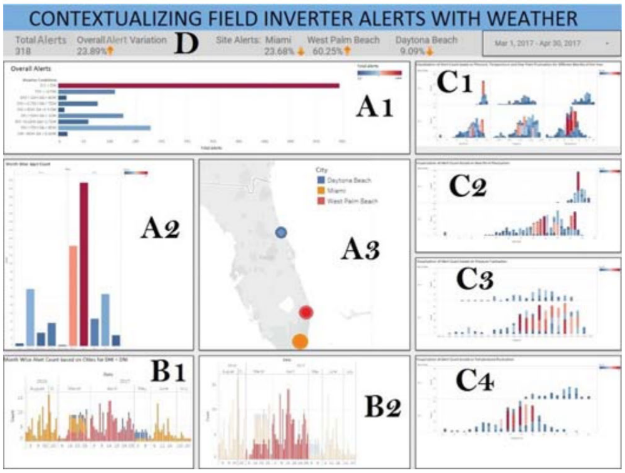
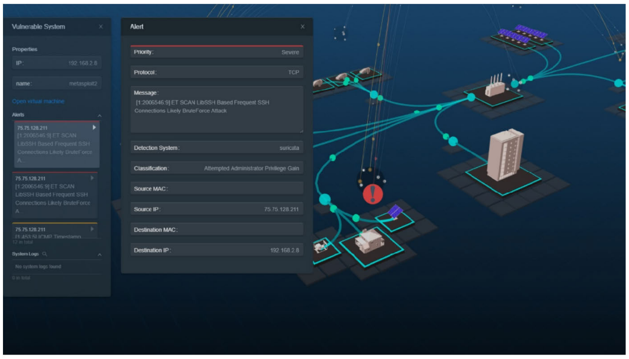


FIGURE 5. Proof of concept dashboard interface presenting descriptive analytics of data for Human-On-The-Loop framework [66].

The significance of contextualized data in a human-readable format was emphasized by [66], a human-on-the-loop framework that allows the operator to customize the visualization. The presented framework has the main goal to contextualize data from automated detection, prevention, and mitigation tools. The framework consists of three modules: 1) data analyzer comprising Kafka, Apache Spark, and R, 2) classifier comprising a deep neural network, and 3) decision-maker with situational awareness and cognitive learning model. These modules are used to conceptualize data and then present it via the dashboard interface. The front end of the dashboard interface is segmented into four divisions that the operator can dynamically customize to show data based on system priorities and availability. Such dynamic customization facilitates adjusting to the point of view of a particular operator's background (discipline). The dashboard in Figure 6 presents a theoretical scenario where an operator is monitoring Grid-Tied 3 PV systems.



Vulnerable System ×

Properties

IP:	192.168.2.8
name:	metasploit2

Open virtual machine

Alerts

75.75.128.211
[1:2006546:9] ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce A...

75.75.128.211
[1:2006546:9] ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce A...

75.75.128.211
[1:453:5] ICMP Timestamp

12 in total

System Logs

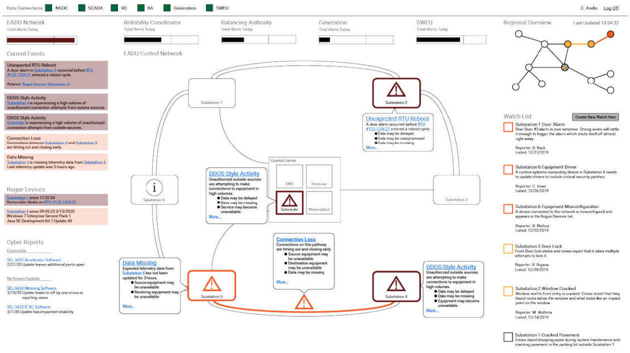
No system logs found

0 in total

Alert ×

Priority:	Severe
Protocol:	TCP
Message:	[1:2006546:9] ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack
Detection System:	suricata
Classification:	Attempted Administrator Privilege Gain
Source MAC:	
Source IP:	75.75.128.211
Destination MAC:	
Destination IP:	192.168.2.8

FIGURE 6. Cyber-Energy Emulation (CEE) Platform [66].



Data Connections 🟩 NSOC 🟩 SCADA 🟩 RC 🟩 BA 🟩 Generation 🟩 SWEU

C. Andor Log Off

EADU Network
Total Alerts Today

Reliability Coordinator
Total Alerts Today

Balancing Authority
Total Alerts Today

Generation
Total Alerts Today

SWEU
Total Alerts Today

Regional Overview Last Updated 13:54:32

Current Events

Unexpected RTU Reboot
A door alarm in Substation 2 occurred before RTU #123.1234.21 entered a reboot cycle.
Related: Rogue Device: Substation 2

DDOS Style Activity
Substation 4 is experiencing a high volume of unauthorized connection attempts from outside sources.

DDOS Style Activity
Scheduler is experiencing a high volume of unauthorized connection attempts from outside sources.

Connection Loss
Connections between Substation 4 and Substation 5 are timing out and closing early.

Data Missing
Substation 5 is missing telemetry data from Substation 4. Last telemetry update was 3 hours ago.

Rogue Devices

Substation 2 since 11:32:54
Removable Media on RTU #123.1234.21

Substation 6 since 09:45:23 3/13/2020
Windows 7 Enterprise Service Pack 1
Java SE Development Kit 7 Update 40

Cyber Reports

Exploitable

SEL-5032 Accelerator Software
2/27/20 Update leaves additional ports open

No Known Exploits

SEL-5630 Metering Software
3/10/20 Update leads to off by one errors in reporting views

SEL-5033 RTAC Software
3/1/30 Update has impacted reliability

EADU Control Network

Unexpected RTU Reboot
A door alarm occurred before RTU #123.1234.21 entered a reboot cycle.
- Data may be delayed
- Data may be compromised
- Data may be missing

More...

DDOS Style Activity
Unauthorized outside sources are attempting to make connections to equipment in high volumes.
- Data may be delayed
- Data may be missing
- Service may become unavailable.

More...

Connection Loss
Connections on this pathway are timing out and closing early.
- Source equipment may be unavailable
- Destination equipment may be unavailable
- Data may be missing

More...

Data Missing
Expected telemetry data from Substation 4 has not been updated for 3 hours.
- Source equipment may be unavailable
- Receiving equipment may be unavailable

More...

DDOS Style Activity
Unauthorized outside sources are attempting to make connections to equipment in high volumes.
- Data may be delayed
- Data may be missing
- Equipment may become unavailable.

More...

Watch List [Create New Watch Item]

□ Substation 1 Door Alarm
Rear Door #3 alarm is over sensitive. Strong winds will rattle it enough to trigger the alarm which shuts itself off almost right away.
Reporter: B. Rook
Listed: 12/27/2019

□ Substation 6 Equipment Driver
A control-systems computing device in Substation 6 needs to update drivers to include critical security patches.
Reporter: C. Imwe
Listed: 12/26/2019

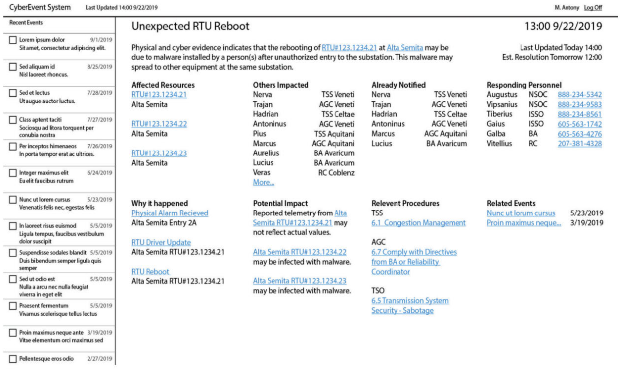
□ Substation 6 Equipment Misconfiguration
A device connected to the network is misconfigured and appears in the Rogue Devices list.
Reporter: B. Malbus
Listed: 12/22/2019

□ Substation 3 Door Lock
Front Door lock sticks and crews report that it takes multiple attempts to lock it.
Reporter: B. Organa
Listed: 12/20/2019

□ Substation 2 Window Cracked
Window next to front entry is cracked. Crews report that they found rocks below the window and what looks like an impact point on the window.
Reporter: M. Mothma
Listed: 12/14/2019

□ Substation 1 Cracked Pavement
Crews report dropping pipes during routine maintenance and cracking pavement in the parking lot outside Substation 1.

FIGURE 7. Wireframe preliminary design concept [69].



CyberEvent System Last Updated 14:00 9/22/2019 M. Antony Log Off

Recent Events

□ Lorem ipsum dolor 9/1/2019
Sit amet, consectetur adipiscing elit.

□ Sed aliquam id 8/25/2019
Nisl laoreet rhoncus.

□ Sed et lectus 7/28/2019
Ut augue auctor luctus.

□ Class aptent taciti 7/27/2019
Sociosqu ad litora torquent per conubia nostra

□ Per inceptos himenaeos 7/26/2019
In porta tempor erat ac ultrices.

□ Integer maximus elit 6/24/2019
Eu elit faucibus rutrum

□ Nunc ut lorem cursus 5/23/2019
Venenatis felis nec, egestas felis

□ In laoreet risus euismod 5/5/2019
Ligula tempus, faucibus vestibulum dolor suscipit

□ Suspendisse sodales blandit 5/5/2019
Duis bibendum semper ligula quis semper

□ Sed ut odio est 5/5/2019
Nulla a arcu nec nulla feugiat viverra in eget elit

□ Praesent fermentum 5/5/2019
Vivamus scelerisque tellus lectus

□ Proin maximus neque ante 3/19/2019
Vitae elementum orci maximus sed

□ Pellentesque eros odio 2/27/2019

Unexpected RTU Reboot 13:00 9/22/2019

Physical and cyber evidence indicates that the rebooting of RTU#123.1234.21 at Alta Semita may be due to malware installed by a person(s) after unauthorized entry to the substation. This malware may spread to other equipment at the same substation.

Last Updated Today 14:00
Est. Resolution Tomorrow 12:00

Affected Resources
RTU#123.1234.21
Alta Semita

RTU#123.1234.22
Alta Semita

RTU#123.1234.23
Alta Semita

Others Impacted	
Nerva	TSS Veneti
Trajan	AGC Veneti
Hadrian	TSS Celtae
Antoninus	AGC Veneti
Pius	TSS Aquitani
Marcus	AGC Aquitani
Aurelius	BA Avaricum
Lucius	BA Avaricum
Veras	RC Coblenz
More...	

Already Notified	
Nerva	TSS Veneti
Trajan	AGC Veneti
Hadrian	TSS Celtae
Antoninus	AGC Veneti
Marcus	AGC Aquitani
Lucius	BA Avaricum

Responding Personnel		
Augustus	NSOC	888-234-5342
Vipsanius	NSOC	888-234-9583
Tiberius	ISSO	888-234-8561
Gaius	ISSO	605-563-1742
Galba	BA	605-563-4276
Vitellius	RC	207-381-4328

Why it happened
Physical Alarm Recieved
Alta Semita Entry 2A

RTU Driver Update
Alta Semita RTU#123.1234.21

RTU Reboot
Alta Semita RTU#123.1234.21

Potential Impact
Reported telemetry from Alta Semita RTU#123.1234.21 may not reflect actual values.

Alta Semita RTU#123.1234.22 may be infected with malware.

Alta Semita RTU#123.1234.23 may be infected with malware.

Relevent Procedures
TSS
6.1 Congestion Management

AGC
6.7 Comply with Directives from BA or Reliability Coordinator

TSO
6.5 Transmission System Security - Sabotage

Related Events	
Nunc ut lorum cursus	5/23/2019
Proin maximus neque...	3/19/2019

FIGURE 8. A proposed display showing that a remote terminal unit (RTU) has rebooted unexpectedly [70].

The Cyber-Energy Emulation (CEE) Platform [67] is used for real-time visualization of large-scale environments involving cyber-physical devices. This approach is quite unique to the field of cyber-physical visualization tools as this platform has the capability to include real and emulated physical devices. The emulated environment allows the user to test parameter changes without the risk of damaging physical equipment. This emulation feature combined with real-time visualization of network traffic, security alerts, and power system states allows the user to improve their overall system state awareness during system operation and parameter experimentation. The CEE real-time environment has the ability to display data from cyber and physical events in a 3D platform while providing the user with a beneficial perspective and utilities for in-depth analysis. An example of a 3D-rendered experimental environment with an ongoing intrusion detection alert can be seen in figure 6 with detailed logs and an interactive user interface.

Cyber-Physical Security Assessment (CPSA) visualization tool was proposed by Saxena et. al. [68] to promote situational awareness in the smart grids. This tool utilizes a Graphical User Interface (GUI) to assist operators in their decision-making process by identifying vulnerable states and measurement errors. The proposed visualization scheme for this tool uses a combination of line graphs, alphanumeric data fields, and the relative geographical location of the infrastructure. Moreover, CPSA can be used to improve understanding of power system monitoring, analyzing the nature of cyber-attacks, malicious command insertion,affected devices, and understanding the impact of attacks on the operation of the power system. Thus, the operator is informed of potential and active threats, as well as the possible fallout from attacks on the power system.

The approach of Le Blanc et. al. [69] is focused on interviewing, observing, and learning about human experiences and interactions with control systems. By developing an understanding focused on human factors, the authors focus on improving user productivity and situation awareness. This paper presents an approach to creating suggestive and interdisciplinary representations by interviewing and including previous observations and experiences of the system operators to determine what information is important to the user. Through observation of team-member interactions and data sharing between cyber and engineering teams, the authors identified informational context and other key features for informed system visualization. The preliminary design concept as seen in Figure 7 was created by observing the reactions of human subjects during the simulated cyber and physical attacks on the power grid.

The work of Scholtz et al. [70] focuses on enhancing situation awareness of individuals from non-overlapping roles to improve the coordinated response of control system engineers. An example of an alert on a remote terminal unit that has rebooted unexpectedly is illustrated by Figure 8. This proposed display allows multiple non-overlapping professionals to be able to provide insights during the monitoring of the system.

One of the inherent characteristic features of communication within operational technologies (OT) is the frequency with which communication occurs. Sensors within operational technology applications regularly send and receive sensor data at frequent intervals. The goal of the visualization system presented by Lohfink et al. [71] is to utilize these inherent features from sensors to provide insights into the available data using spiral plots. These insights aim to support and inform control operators and cyber defenders of the response strategy, regardless of their experience in the field. The main goal of spiral plots is to map the data dimensions

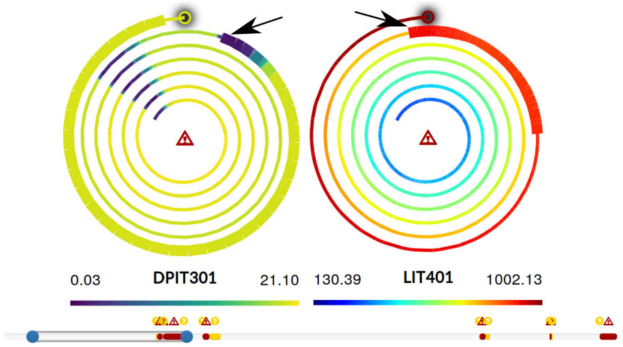


FIGURE 9. Anomaly (left) and disrupted period (right) abrupt increase [71].

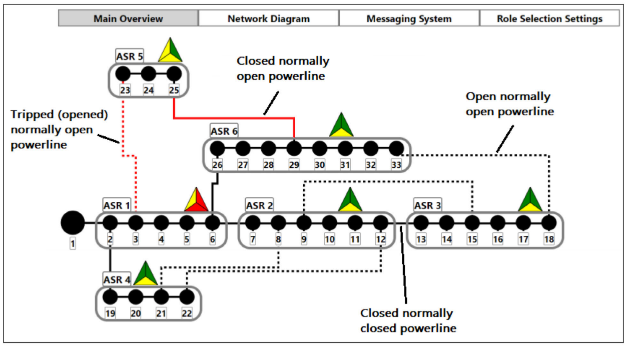


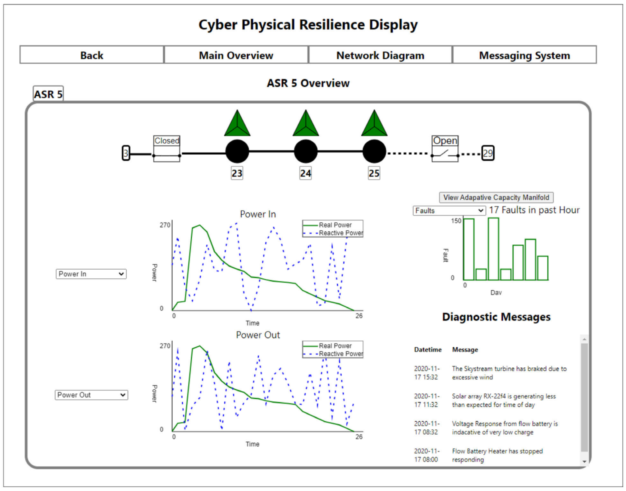
FIGURE 10. Display of attack scenario with the interconnectivity of sensors [72].

to the width and color of the plot, making it more intuitive. The proposed system overview can be seen in figure 9. The final visualization is composed of the spiral plots and icons displaying alerts from the anomaly detection system.

The goal of the display presented in [72] is to aggregate meaningful information together, facilitating rapid operational decisions and complementary context for the roles, as the root cause of events can include both cyber and physical elements. Figure 10 shows an example of the visualization for the IEEE 33 bus system with several of the busses grouped into Aggregated System Resources (ASRs). Each of the different ASR units can be selected to drill down into lower levels that display the ASR's internal components, as shown in Figure 11, where each bus now possesses its own resilience icon. The user can easily locate relevant information by displaying information at a desired resolution. The interconnections between different elements are representing different states, such as normally closed, closed, normally open, or opened (Figure 10).

B. PLANNING AND DISCOVERY TASK

Planning and discovery facilitate the adoption of a long-term plan for securing the cyber-physical system. In the case of these visualizations, the time scale is much more different than in the case of real-time visualizations. In this case, the efficiency of visualization is affected by the quality of the algorithms for data mining and integration of prior knowledge [82]. Based on the time scale of the two types of visualizations, we can consider the following two scenarios: 1. Preemptive visualization for secure design of the system before any exploit occurred, 2. Root-cause visualization for securing the weak points of the system after an attack happened.



Diagnostic Messages

Datetime	Message
2020-11-17 15:32	The Skystream turbine has braked due to excessive wind
2020-11-17 11:32	Solar array RX-22f4 is generating less than expected for time of day
2020-11-17 08:32	Voltage Response from flow battery is indacative of very low charge
2020-11-17 08:00	Flow Battery Heater has stopped responding

FIGURE 11. Overview of each sensor with feature-wise details [72].

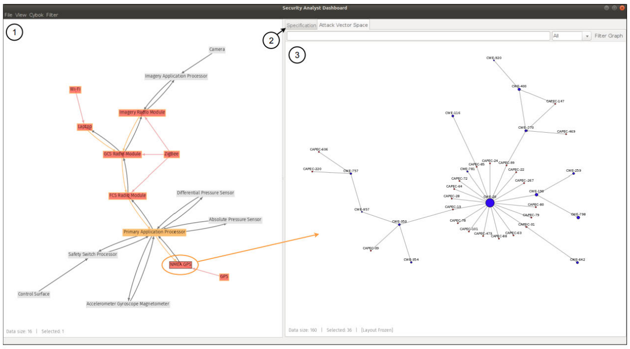


FIGURE 12. Screenshot of the dashboard showing exploit chains in the system topology graph (1) and filtering of the attack vector space per component [73].

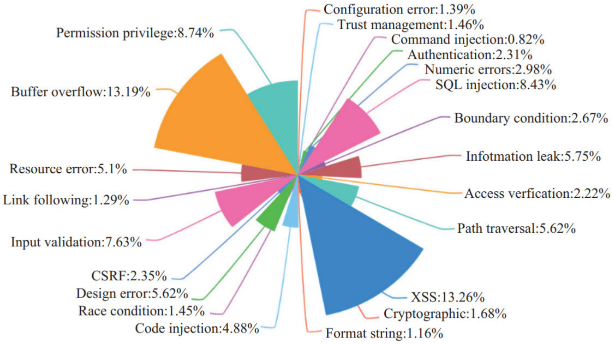


FIGURE 13. Distribution of vulnerabilities [74].

1) PREEMPTIVE VISUALIZATION

The secure design visualization can facilitate the secure-by-design process and apply the zero-trust framework as well as identify risks associated with possible incoming data sources/events [83].

One of the most popular approaches for preemptive visualization is to compute attack graphs [76], [77], [78] in order to better understand the system's vulnerabilities before they are exploited by attackers. In [76], the authors proposed a visualization tool that uses Architecture Analysis and Design Language to model attacks, identify attack vectors, and visualize potential damage. As a result, system operators can use this visualization tool to identify weak points and develop effective solutions for their remediation. The visualization engine presented in [78] evaluates the effectiveness of potential mitigation plans and provides an overview of possible attack evolution by generating attack graphs for specific scenarios that can be simulated directly in the visualization tool.

The work presented by Wu et al. [74] is an example of a visualization system that provides applications for both the attacker's and defender's perspectives. When considering the attacker's perspective, there are multiple types of visualization techniques used for displaying pertinent data. Statistical analysis is performed to identify potential vulnerabilities and display their cause within a nightingale rose diagram as seen in Figure 13. The diagram is used to demonstrate the distribution of threats caused by a corresponding vulnerability. This threat and vulnerability data is used to link corresponding threats to commonly correlated keywords such as ''buffer overflow'' and ''memory''. These keywords are then displayed in a word cloud graph, giving the attacker a sense of potential attack vectors.

An example of a node-link diagram was given by the Bakirtzis et al. [73]. Here, the authors present an interactive security analysis dashboard that displays system requirements and associated attack vectors. As seen in the figure 12, this tool makes it possible to start analysis earlier in the system life-cycle. This system uses node-link diagrams to help inform system designers and security analysts where to improve collaboration during the system design process. The node-link diagrams display system specifications, potential attack vectors, and the resulting attack surface within the system's topology.

Another interesting example of visualization was the ''resilienceCube'' by Jovanovic et al. [75]. This paper presents data via line graphs, tabular data, 3-dimensional matrix cubes, node-link diagrams and maps. The framework was designed to accommodate a wide range of custom tools that monitor three aspects of infrastructure resiliency: Recovery/Adaptation, Robustness, and Preparedness. The ''cube'' plots each of these three values in a 3D space to provide a sense of how well or poor the system is in each area. This assortment of display tools is intended to aid in resilient management strategies by allowing the user to assess, monitor, and benchmark the resilience of a cyber-physical system. The proposed framework set allows for the modeling and analyzing of scenario-based threats, as well as stress-testing the intended system design. This method of identifying potential weaknesses in critical infrastructure allows for the optimization of the initial investment as the resilience of the system can be improved upon.

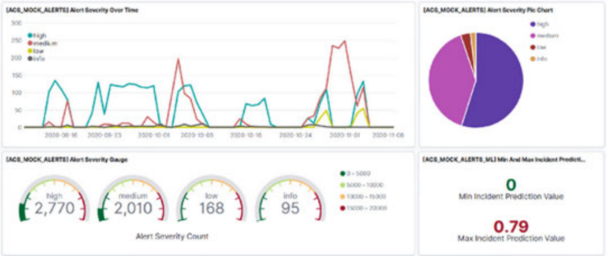


FIGURE 14. Alerts Dashboard - Alert severity monitoring visualizations [80].

2) THE ROOT-CAUSE VISUALIZATION

This class of visualization methods addresses the need for forensics investigation and analysis. Such visualizations are intended to provide insight into the factors that led to a cyber-physical event. These visualizations enable users to learn from past events and come up with a plan to eliminate vulnerabilities that were exploited by the attackers.

Macedo et al. [80] presented a tool that aims to combine an intuitive user interface with machine learning forecasts that display the available data through time-series visualizations. The dynamic user interface of this tool is intended to display pertinent information in supporting the investigation of cyber and physical attacks that are presented in a user-friendly manner. This visualization tool uses line graphs, pie charts, bar charts, and numerical displays, as seen in Figure 14, to display the available data that is generated by threat detection tools.

The work of Yan et al. [79] aims to improve the understanding of how the power grid behaves under complex attacks by combining geographical details of substations with attack and defense data in a simulated environment. This creates a geographically accurate power grid system testbed for which the user can simulate several single-node (substation) attacks. The intent of this visualization system is to provide effective visualization capability of these cyber-physical attacks which will help inform the decision-making process of power system operators regarding their response strategies.

The geographical representations of the power grid during the simulation of an attack are able to display the cascading impact of a cyber-physical attack on the power grid, as seen in Figure 15. The ability to visualize the impact of a cascading attack and how it propagates through the power grid is intended to assist power engineers and operators in the efficient modeling and simulation of these attack scenarios. These scenarios utilize real power grid system data that can potentially help operators to understand grid behavior under certain types of complex attacks with the goal of improving defense strategies through a more informed decision-making process. Another visualization tool for visualizing the cascading failures is presented in [81]. The primary visualization method used is the node-link diagrams with specific node

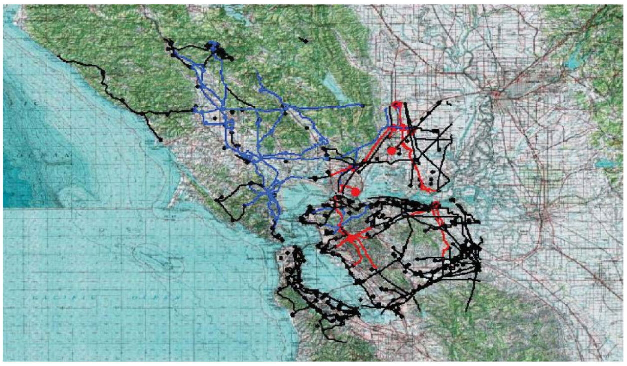


FIGURE 15. Cascading attack example: (Red) currently down, (Blue) previously down, and (Black) normal operation [79].

icons. The proposed solution includes separate displays for the cyber layer and physical hardware.

V. DISCUSSION

In this section, we will present the main challenges, findings, and future research directions for improving smart grid security visualizations.

The visualization system must be designed to aid in the solving of specific problems and tasks while remaining simple and intuitive to use [70]. By providing significant context to the mined data, it should improve situational awareness and facilitate faster decision-making.

1) CHALLENGES IDENTIFIED IN VISUALIZATIONS OF POWER GRID SECURITY

a: COMBINING CYBER AND PHYSICAL

Major difficulties stem from the differences between cyber and physical data, acquisition process, and difficulties of synchronizing these types of data. Many distributed sensors are used in today's power grid, each using a different communication protocols, hardware, and software resources to generate multidimensional datasets with varying sampling rates, which are then transmitted to the central control center.

b: MISSING HOLISTIC VIEW

Currently, most research is focused on cyber security visualizations, with few proposed solutions for providing a holistic (cyber and physical data combined) view of the security of cyber-physical systems. The visualizations do not have any built-in tools for determining whether a cyber attack caused physical anomalies or whether physical anomalies disrupted communications between system components. As a result, it is entirely up to the end-user to identify cyber-physical causality by correlating the visualizations.

2) BEST PRACTICES

After performing the review, it has been observed that the majority of researchers are focusing their efforts on the development of real-time visualization monitoring tools for security, with relatively fewer efforts dedicated to visualizations designed specifically for tasks such as root cause analysis or system design.

Monitoring - This category of visualization tools should include features in their presentation format that allow the user to interpret them quickly. An effective example would be the ability to highlight important or high-priority alerts in the foreground of the display, while also taking into account the relative size, shapes, and colors in the context of the overall design, in order to quickly capture the attention of the user and provide a clear understanding of the alert's details, achieving a balance between focusing on critical components and comprehending the system as a whole.

Planning and discovery - This class of visualizations relies on prior knowledge and external sources to identify potential attack vectors in order to prevent future attacks. It is critical in this case to stay up to date on newly discovered vulnerabilities. The primary goal of these visualizations is to identify system weaknesses and areas for improvement in terms of resilience and security. The most effective approach is to look at the problem from both the red and blue teams' perspectives and to present information to the end-user via separate visualizations. This type of visualization necessitates analyzing "if-then" scenarios to identify vulnerable system components and predict potential attack outcomes, while also ensuring that a worst-case scenario attack does not cause cascading failures that bring the entire grid down.

3) TOP CHOICES FOR VISUALIZATIONS

The solutions examined in the paper are mostly dashboards that use multiple visualization techniques to provide users with valuable insight into available data from various perspectives. The most common techniques are traditional 2D representations such as line and bar plots. However, icon displays are also popular because they can condense a significant amount of information into a single attribute of the icon, thereby saving display space. Node-link diagrams are used to illustrate the interconnections of a system, where the color or shape of nodes and links may indicate different properties of the system components. Furthermore, most dashboards include a map to help with spatial understanding of the data.

4) INTERDISCIPLINARY ADAPTATION

An additional consideration in the design of visualization for power grids is interdisciplinary visualization. In the modern world of inter-connected and smart systems, users from many different roles as cyber experts, power engineers, etc. are collaborating to secure the grid. Supporting interdisciplinary adaptation and information sharing is imperative to help the end-users communicate and inform the decision-making process for their response strategies. These considerations also help find common ground among data and system feedback, as the available data may be used for many different considerations from role to role.

Allowing end-users to choose relevant information and how it is presented is an effective strategy for optimizing the adaptation process. Another option is to incorporate feedback mechanisms into the system design. The feedback gathered can be analyzed to determine the effectiveness of the visualization system and areas for improvement in future versions.

A. FUTURE RESEARCH DIRECTIONS

1) HOLISTIC CYBER-PHYSICAL HEALTH METRICS

By combining different streams of information into single metrics, the time required to achieve situational awareness can be significantly reduced by presenting single-number displays that holistically describe the system state. These metrics are presented at a level of abstraction that requires no prior knowledge or experience, making them easily adoptable by end-user with diverse backgrounds. Examples of such approaches are presented in [64], where the authors introduce the trust metric, which computes the metric for a single sensor, and [72], where the authors provide a score for the cyber/physical health and resilience of the system.

2) EMPHASIZING INTERDISCIPLINARY ADAPTABILITY

It is imperative to design a tool that does not add additional workload to the user and is capable of providing complete cyber-physical visualization that encompasses the entirety of the monitored system. This design consideration will allow the user to fully utilize the features of the additional data visualization tool while avoiding the idea of adding, ‘‘yet another screen to monitor.’’ While the goal of these visualization methods is frequently to provide the user with a better perspective, literature shows that these tools frequently encourage the integration of multi-disciplinary efforts with the common overarching goal of maintaining and protecting the power grid. The versatility of visualization tools makes it an appealing technology for researchers and industry professionals to pursue in order to further develop this standard.

3) EVALUATION IN REAL-WORLD SCENARIOS AND BENCHMARKING

Some of the solutions studied in this field are still in the early stages of development, and their effectiveness has been tested on experimental setups. As a result, additional testing and evaluation of these proposed solutions in real-world industrial scenarios are required to truly assess their effectiveness and highlight the benefits that they can provide to operators in achieving situational awareness. This testing will allow researchers and industry professionals to better understand the challenges of putting these solutions into practice, as well as identify areas for further improvements. Moreover, to evaluate these solutions effectively, there is a need to develop a benchmark that can help to identify unique criteria for evaluation [84], [85].

4) INTEGRATION OF AI/ML

Overall, the development of visualization tools based on machine learning has the potential to significantly improve the security of smart grids. Recent advancements in machine learning have opened up new horizons in the field of cyber-physical security visualization engines. Some of the benefits are a dynamic adaptable system based on an intelligent recommendation system, universal dimensionality reduction, feature extractors, and an effective intrusion and anomaly detection system for identifying and categorization of anomalies. Machine learning can be seen as a complementary tool for extracting insights from existing data streams.

5) CAUSALITY BETWEEN CYBER AND PHYSICAL

It may be extremely beneficial to shift away from the end-user effort in determining cyber and physical causality and correlation towards the use of algorithms to infer the causality of certain events detected in the system based on available data. This approach can significantly reduce the time required to comprehend the data because the visualization will clearly display whether changes in the system's subsystems or layers are correlated or causal.

VI. CONCLUSION

Visualization methods provide the ability to effectively organize and display complex data, allowing for effective and timely operator decisions, as well as running of ‘‘if-then’’ scenarios.

It is critical to detect anomalous behavior in the power grids as soon as possible, as any delay can have serious consequences to the security and safety of human life and physical assets. The visualization of security aspects of cyber-physical systems has a tremendous effect on the life cycle of complex systems. We looked at preemptive use visualizations that guide and assist users during the design process, as well as vulnerability and resilience assessments. Other solutions are designed to assist users in making real-time decisions during monitoring tasks by providing situational awareness and resolving the issue. Furthermore, some dashboards have been designed to assist users in investigating cyber-physical events after they have occurred and determine the root-cause analysis.

Over the recent years, one can recognize several growing interests when it comes to the visualization of cyber-physical systems with security in mind. The first one is incorporating machine learning algorithms to identify patterns, discover previously unknown relationships, automatically categorize and label incoming data, and reduce data dimensionality. The next one is a shift towards a user-centric focus (adapt to operator need in a given moment). Yet another direction is benchmarking of visualization mechanisms (efficiency evaluation in real-world industrial scenarios).

ACKNOWLEDGMENT

The authors thank Emily Kesler for the contribution to this article while she was a Summer Intern with Idaho National Laboratory.

REFERENCES

[1] J. Shi, J. Wan, H. Yan, and H. Suo, ‘‘A survey of cyber-physical systems,’’ in *Proc. Int. Conf. Wireless Commun. Signal Process. (WCSP)*, Nov. 2011, pp. 1–6.

[2] X. Koutsoukos, G. Karsai, A. Laszka, H. Neema, B. Potteiger, P. Volgyesi, Y. Vorobeychik, and J. Sztipanovits, ''SURE: A modeling and simulation integration platform for evaluation of secure and resilient cyber–physical systems,'' *Proc. IEEE*, vol. 106, no. 1, pp. 93–112, Jan. 2018.

[3] A. Humayed, J. Lin, F. Li, and B. Luo, ''Cyber-physical systems security—A survey,'' *IEEE Internet Things J.*, vol. 4, no. 6, pp. 1802–1831, Dec. 2017.

[4] S. Sridhar, A. Hahn, and M. Govindarasu, ''Cyber–physical system security for the electric power grid,'' *Proc. IEEE*, vol. 100, no. 1, pp. 210–224, Jan. 2012.

[5] H. S. Mavikumbure, C. S. Wickramasinghe, D. L. Marino, V. Cobilean, and M. Manic, ''Anomaly detection in critical-infrastructures using autoencoders: A survey,'' in *Proc. 48th Annu. Conf. IEEE Ind. Electron. Soc. (IECON)*, Oct. 2022, pp. 1–7.

[6] A. Greenberg, ''How 30 lines of code blew up a 27-ton generator,'' Conde Nast, Oct. 2020. [Online]. Available: https://www.wired.com/story/how-30-lines-of-code-blew-up-27-ton-generator/

[7] N. Falliere, L. O. Murchu, and E. Chien, ''W32. Stuxnet dossier,'' *White Paper, Symantec Corp., Secur. Response*, vol. 5, no. 6, p. 29, 2011.

[8] D. Faquir, N. Chouliaras, V. Sofia, K. Olga, and L. Maglaras, ''Cybersecurity in smart grids, challenges and solutions,'' *AIMS Electron. Electr. Eng.*, vol. 5, no. 1, pp. 24–37, 2021.

[9] *Resilient Control and Instrumentation Systems*, Dept. Energy Office Electr., Washington, DC, USA, 2022.

[10] A. Singh and A. Jain, ''Study of cyber attacks on cyber-physical system,'' in *Proc. 3rd Int. Conf. Internet Things Connected Technol. (ICIoTCT)*, 2018, pp. 686–690.

[11] H. Shiravi, A. Shiravi, and A. A. Ghorbani, ''A survey of visualization systems for network security,'' *IEEE Trans. Vis. Comput. Graphics*, vol. 18, no. 8, pp. 1313–1329, Aug. 2012.

[12] B. P. Bhattarai, S. Paudyal, Y. Luo, M. Mohanpurkar, K. Cheung, R. Tonkoski, R. Hovsapian, K. S. Myers, R. Zhang, P. Zhao, M. Manic, S. Zhang, and X. Zhang, ''Big data analytics in smart grids: State-of-the-art, challenges, opportunities, and future directions,'' *IET Smart Grid*, vol. 2, no. 2, pp. 141–154, Jun. 2019.

[13] S. Tee Teoh, K.-L. Ma, S. Felix Wu, and T. J. Jankun-Kelly, ''Detecting flaws and intruders with visual data analysis,'' *IEEE Comput. Graph. Appl.*, vol. 24, no. 5, pp. 27–35, Sep. 2004.

[14] D. Freet and R. Agrawal, ''A statistical comparison of security visualization efficiency compared to manual analysis of IDS log data,'' in *Proc. SoutheastCon*, Apr. 2018, pp. 1–5.

[15] J. F. Rodrigues, A. J. M. Traina, M. C. F. de Oliveira, and C. Traina, ''Reviewing data visualization: An analytical taxonomical study,'' in *Proc. 10th Int. Conf. Inf. Visualisation (IV)*, 2006, pp. 713–720.

[16] H. M. Shakeel, S. Iram, H. Al-Aqrabi, T. Alsboui, and R. Hill, ''A comprehensive state-of-the-art survey on data visualization tools: Research developments, challenges and future domain specific visualization framework,'' *IEEE Access*, vol. 10, pp. 96581–96601, 2022.

[17] S. Liu, W. Cui, Y. Wu, and M. Liu, ''A survey on information visualization: Recent advances and challenges,'' *Vis. Comput.*, vol. 30, no. 12, pp. 1373–1393, Dec. 2014.

[18] X. Qin, Y. Luo, N. Tang, and G. Li, ''Making data visualization more efficient and effective: A survey,'' *VLDB J.*, vol. 29, no. 1, pp. 93–117, Jan. 2020.

[19] S. Hirve and C. H. P. Reddy, ''A survey on visualization techniques used for big data analytics,'' in *Advances in Computer Communication and Computational Sciences* (Advances in Intelligent Systems and Computing), S. K. Bhatia, S. Tiwari, K. K. Mishra, and M. C. Trivedi, Eds. Singapore: Springer, 2019, pp. 447–459.

[20] L. T. Mohammed, A. A. AlHabshy, and K. A. ElDahshan, ''Big data visualization: A survey,'' in *Proc. Int. Congr. Hum.-Comput. Interact., Optim. Robotic Appl. (HORA)*, Jun. 2022, pp. 1–12.

[21] I. K. Joy, ''Massive data visualization: A survey,'' in *Mathematical Foundations of Scientific Visualization, Computer Graphics, and Massive Data Exploration*, T. Möller, B. Hamann, and R. D. Russell, Eds. Berlin, Germany: Springer, 2009, pp. 285–302.

[22] A. Kiefer and M. K. Rahman, ''An analytical survey on recent trends in high dimensional data visualization,'' 2021, *arXiv:2107.01887*.

[23] J. Wang, S. Hazarika, C. Li, and H. Shen, ''Visualization and visual analysis of ensemble data: A survey,'' *IEEE Trans. Vis. Comput. Graph.*, vol. 25, no. 9, pp. 2853–2872, Sep. 2019.

[24] Y. Guo, S. Guo, Z. Jin, S. Kaul, D. Gotz, and N. Cao, ''Survey on visual analysis of event sequence data,'' *IEEE Trans. Vis. Comput. Graph.*, vol. 28, no. 12, pp. 5091–5112, Dec. 2022.

[25] X. He, Y. Tao, Q. Wang, and H. Lin, ''Multivariate spatial data visualization: A survey,'' *J. Visualizat.*, vol. 22, no. 5, pp. 897–912, Oct. 2019.

[26] Y. Chen, Z. Guan, R. Zhang, X. Du, and Y. Wang, ''A survey on visualization approaches for exploring association relationships in graph data,'' *J. Vis.*, vol. 22, no. 3, pp. 625–639, 2019.

[27] W. Chen, F. Guo, and F. Wang, ''A survey of traffic data visualization,'' *IEEE Trans. Intell. Transp. Syst.*, vol. 16, no. 6, pp. 2970–2984, Dec. 2015.

[28] Y. Zhang, Y. Xiao, M. Chen, J. Zhang, and H. Deng, ''A survey of security visualization for computer network logs,'' *Secur. Commun. Netw.*, vol. 5, no. 4, pp. 404–421, Apr. 2012.

[29] L. Jiang, A. Jayatilaka, M. Nasim, M. Grobler, M. Zahedi, and M. A. Babar, ''Systematic literature review on cyber situational awareness visualizations,'' *IEEE Access*, vol. 10, pp. 57525–57554, 2022.

[30] J. R. Goodall, ''Introduction to visualization for computer security,'' in *Proc. Workshop Vis. Comput. Secur.*, J. R. Goodall, G. Conti, K.-L. Ma, Eds. Cham, Switzerland: Springer, 2007, pp. 1–17.

[31] A. Protopsaltis, P. Sarigiannidis, D. Margounakis, and A. Lytos, ''Data visualization in Internet of Things: Tools, methodologies, and challenges,'' in *Proc. 15th Int. Conf. Availability, Rel. Secur.*, 2020, pp. 1–11.

[32] E. Karapistoli and A. A. Economides, ''Wireless sensor network security visualization,'' in *Proc. 4th Int. Congr. Ultra Modern Telecommun. Control Syst.*, Oct. 2012, pp. 850–856.

[33] Q. Wang, Z. Chen, Y. Wang, and H. Qu, ''A survey on ML4VIS: Applying machine learning advances to data visualization,'' *IEEE Trans. Vis. Comput. Graphics*, vol. 28, no. 12, pp. 5134–5153, Dec. 2022.

[34] A. Wu, Y. Wang, X. Shu, D. Moritz, W. Cui, H. Zhang, D. Zhang, and H. Qu, ''AI4VIS: Survey on artificial intelligence approaches for data visualization,'' *IEEE Trans. Vis. Comput. Graphics*, vol. 28, no. 12, pp. 5049–5070, Dec. 2022.

[35] R. Priam and M. Nadif, ''Data visualization via latent variables and mixture models: A brief survey,'' *Pattern Anal. Appl.*, vol. 19, no. 3, pp. 807–819, Aug. 2016.

[36] T. Fujiwara, Shilpika, N. Sakamoto, J. Nonaka, K. Yamamoto, and K. Ma, ''A visual analytics framework for reviewing multivariate time-series data with dimensionality reduction,'' *IEEE Trans. Vis. Comput. Graphics*, vol. 27, no. 2, pp. 1601–1611, Feb. 2021.

[37] X. Chen and X. Chen, ''Data visualization in smart grid and low-carbon energy systems: A review,'' *Int. Trans. Elect. Energy Syst.*, vol. 31, no. 7, 2021, Art. no. e12889.

[38] M. Stefan, J. G. Lopez, M. H. Andreasen, and R. L. Olsen, ''Visualization techniques for electrical grid smart metering data: A survey,'' in *Proc. IEEE 3rd Int. Conf. Big Data Comput. Service Appl. (BigDataService)*, Apr. 2017, pp. 165–171.

[39] T. Hanauer, W. Hommel, S. Metzger, and D. Pöhn, ''A process framework for stakeholder-specific visualization of security metrics,'' in *Proc. 13th Int. Conf. Availability, Rel. Secur.*, Aug. 2018, pp. 1–10.

[40] S. Yoo, J. Jo, B. Kim, and J. Seo, ''Hyperion: A visual analytics tool for an intrusion detection and prevention system,'' *IEEE Access*, vol. 8, pp. 133865–133881, 2020.

[41] A. D. Kent, ''Cyber security data sources for dynamic network research,'' in *Dynamic Networks and Cyber-Security*. Singapore: World Scientific, 2016, pp. 37–65.

[42] J. Happa, T. Bashford-Rogers, I. Agrafiotis, M. Goldsmith, and S. Creese, ''Anomaly detection using pattern-of-life visual metaphors,'' *IEEE Access*, vol. 7, pp. 154018–154034, 2019.

[43] V. K. Singh, S. P. Callupe, and M. Govindarasu, ''Testbed-based evaluation of SIEM tool for cyber kill chain model in power grid SCADA system,'' in *Proc. North Amer. Power Symp. (NAPS)*, Oct. 2019, pp. 1–6.

[44] S. Tufail, I. Parvez, S. Batool, and A. Sarwat, ''A survey on cybersecurity challenges, detection, and mitigation techniques for the smart grid,'' *Energies*, vol. 14, no. 18, p. 5894, Sep. 2021.

[45] M. Keshk, B. Turnbull, E. Sitnikova, D. Vatsalan, and N. Moustafa, ''Privacy-preserving schemes for safeguarding heterogeneous data sources in cyber-physical systems,'' *IEEE Access*, vol. 9, pp. 55077–55097, 2021.

[46] K. Kambatla, G. Kollias, V. Kumar, and A. Grama, ''Trends in big data analytics,'' *J. Parallel Distrib. Comput.*, vol. 74, no. 7, pp. 2561–2573, 2014.

[47] H. Yin, ''Nonlinear dimensionality reduction and data visualization: A review,'' *Int. J. Autom. Comput.*, vol. 4, no. 3, pp. 294–303, Jul. 2007.

[48] C.-S.-J. Chu, "Time series segmentation: A sliding window approach," *Inf. Sci.*, vol. 85, nos. 1–3, pp. 147–173, Jul. 1995.

[49] D. A. Keim, "Information visualization and visual data mining," *IEEE Trans. Vis. Comput. Graphics*, vol. 8, no. 1, pp. 1–8, Aug. 2002.

[50] L. Fu Lu, J. Wan Zhang, M. Lin Huang, and L. Fu, "A new concentric-circle visualization of multi-dimensional data and its application in network security," *J. Vis. Lang. Comput.*, vol. 21, no. 4, pp. 194–208, Aug. 2010.

[51] M. Hao, M. Marwah, S. Mittelstaedt, H. Janetzko, D. Keim, U. Dayal, C. Bash, C. Felix, C. Patel, M. Hsu, Y. Chen, and M. Hund, "Visual analytics of cyber physical data streams using spatio-temporal radial pixel visualization," in *Proc. SPIE*, Feb. 2013, pp. 31–42.

[52] X. Suo, Y. Zhu, and S. Owen, "A task centered framework for computer security data visualization," in *Visualization for Computer Security*, J. R. Goodall, G. Conti, K.-L. Ma, Eds. Berlin, Germany: Springer, 2008, pp. 87–94.

[53] C. Muelder, K.-L. Ma, and T. Bartoletti, "Interactive visualization for network and port scan detection," in *Recent Advances in Intrusion Detection*, A. Valdes and D. Zamboni, Eds. Berlin, Germany: Springer, 2006, pp. 265–283.

[54] S. Noel, S. Purdy, A. O'Rourke, E. Overly, B. Chen, C. DiFonzo, J. Chen, G. Sakellis, M. Hegde, M. Sapra, C. Araki, J. Martin, B. Koehler, J. Keenan, T. Coen, W. W. Watson, J. Harper, and K. Jacobs, "Graph analytics and visualization for cyber situational understanding," *J. Def. Model. Simul. Appl. Methodol. Technol.*, vol. 20, no. 1, pp. 81–95, Jan. 2023.

[55] J. T. Langton, B. Newey, and P. R. Havig, "Visualization for cyber security command and control," in *Proc. SPIE*, Apr. 2010, pp. 286–297.

[56] I. Kotenko and E. Novikova, "Visualization of security metrics for cyber situation awareness," in *Proc. 9th Int. Conf. Availability, Rel. Secur.*, Sep. 2014, pp. 506–513.

[57] S. Zhang, R. Shi, and J. Zhao, "A visualization system for multiple heterogeneous network security data and fusion analysis," *KSII Trans. Internet Inf. Syst.*, vol. 10, no. 6, pp. 2801–2816, 2016.

[58] E. Muhati, D. B. Rawat, M. Garuba, and L. Njilla, "CyVi: Visualization of cyber-attack and defense effects in geographically referenced networks," in *Proc. IEEE 17th Annu. Consum. Commun. Netw. Conf. (CCNC)*, Jan. 2020, pp. 1–4.

[59] B. Shneiderman, "The eyes have it: A task by data type taxonomy for information visualizations," in *Proc. IEEE Symp. Vis. Lang.*, May 1996, pp. 336–343.

[60] G. Rueff, B. Wheeler, T. Vollmer, and T. McJunkin, "INL control system situational awareness technology final report," Idaho Nat. Lab. (INL), Idaho Falls, ID, USA, Tech. Rep. INL/EXT-11-23408, Jan. 2013.

[61] P. Chopade, K. M. Flurchick, M. Bikdash, and I. Kateeb, "Modeling and visualization of smart power grid: Real time contingency and security aspects," in *Proc. IEEE Southeastcon*, Jan. 2012, pp. 1–6.

[62] S. Liu, L. Liu, N. Yang, D. Mao, L. Zhang, J. Cheng, T. Xue, L. Liu, G. Yan, L. Qiu, X. Chen, M. Zhang, and R. Shi, "A data-driven approach for online dynamic security assessment with spatial–temporal dynamic visualization using random bits forest," *Int. J. Electr. Power Energy Syst.*, vol. 124, Jan. 2021, Art. no. 106316.

[63] H.-Y. Su and T.-Y. Liu, "A PMU-based method for smart transmission grid voltage security visualization and monitoring," *Energies*, vol. 10, no. 8, p. 1103, Jul. 2017.

[64] W. J. Matuszak, L. DiPippo, and Y. L. Sun, "CyberSAVe: Situational awareness visualization for cyber security of smart grid systems," in *Proc. 10th Workshop Visualizat. Cyber Secur.*, Oct. 2013, pp. 25–32.

[65] S. Steiner, I. Oyewumi, and D. C. D. Leon, "MAHIVE: Modular analysis hierarchical intrusion detection system visualization event cybersecurity engine for cyber-physical systems and Internet of Things devices," in *Proc. 54th Hawaii Int. Conf. Syst. Sci.*, Jan. 2021. [Online]. Available: http://hdl.handle.net/10125/71475, doi: 10.24251/HICSS.2021.854.

[66] A. Sundararajan, T. Khan, H. Aburub, A. I. Sarwat, and S. Rahman, "A tri-modular human-on-the-loop framework for intelligent smart grid cyber-attack visualization," in *Proc. SoutheastCon*, Apr. 2018, pp. 1–8.

[67] A. Hasandka, J. Rivera, and J. V. Natta, "NREL's cyber-energy emulation platform for research and system visualization," Nat. Renew. Energy Lab. (NREL), Golden, CO, USA, Tech. Rep. NREL/TP-5R00-74142, May 2020.

[68] N. Saxena, V. Chukwuka, L. Xiong, and S. Grijalva, "CPSA: A cyber-physical security assessment tool for situational awareness in smart grid," in *Proc. Workshop Cyber-Phys. Syst. Secur. PrivaCy*, Nov. 2017, pp. 69–79.

[69] K. Le Blanc, A. Ashok, L. Franklin, J. Scholtz, E. Andersen, and M. Cassiadoro, "Characterizing cyber tools for monitoring power grid systems: What information is available and who needs it?" in *Proc. IEEE Int. Conf. Syst., Man, Cybern. (SMC)*, Oct. 2017, pp. 3451–3456.

[70] J. C. Scholtz, L. Franklin, A. Ashok, K. LeBlanc, C. Bonebrake, E. Andersen, and M. Cassiadoro, "Employing a user-centered design process for cybersecurity awareness in the power grid," *J. Hum. Perform. Extreme Environ.*, vol. 14, no. 1, p. 4, Jan. 2018.

[71] A. Lohfink, S. D. D. Anton, H. D. Schotten, H. Leitte, and C. Garth, "Security in process: Visually supported triage analysis in industrial process data," *IEEE Trans. Vis. Comput. Graphics*, vol. 26, no. 4, pp. 1638–1649, Apr. 2020.

[72] B. Vaagensmith, V. K. Singh, R. Ivans, D. L. Marino, C. S. Wickramasinghe, J. Lehmer, T. Phillips, C. Rieger, and M. Manic, "Review of design elements within power infrastructure cyber–physical test beds as threat analysis environments," *Energies*, vol. 14, no. 5, p. 1409, Mar. 2021.

[73] G. Bakirtzis, B. J. Simon, C. H. Fleming, and C. R. Elks, "Looking for a black cat in a dark room: Security visualization for cyber-physical system design and analysis," in *Proc. IEEE Symp. Visualizat. Cyber Secur. (VizSec)*, Oct. 2018, pp. 1–8.

[74] K. Wu, J. Li, Y. Zhu, S. Miao, S. Zhu, and C. Zhou, "Interactive visual analysis on the attack and defense drill of grid cyber-physical systems," *CSEE J. Power Energy Syst.*, vol. 7, no. 1, pp. 45–56, Jan. 2021.

[75] S. Aleksandar Jovanovic, S. Chakravarty, and M. Jelic, "Resilience and situational awareness in critical infrastructure protection: An indicator-based approach," in *Issues on Risk Analysis for Critical Infrastructure Protection*, V. Rosato and A. Di Pietro, Eds. Rijeka, Croatia: IntechOpen, 2021, ch. 4.

[76] M. Ibrahim, Q. Al-Hindawi, R. Elhafiz, A. Alsheikh, and O. Alquq, "Attack graph implementation and visualization for cyber physical systems," *Processes*, vol. 8, no. 1, p. 12, Dec. 2019.

[77] T. D. Le, M. Ge, A. Anwar, S. W. Loke, R. Beuran, R. Doss, and Y. Tan, "GridAttackAnalyzer: A cyber attack analysis framework for smart grids," *Sensors*, vol. 22, no. 13, p. 4795, Jun. 2022.

[78] M. Angelini, N. Prigent, and G. Santucci, "PERCIVAL: Proactive and reactive attack and response assessment for cyber incidents using visual analytics," in *Proc. IEEE Symp. Visualizat. Cyber Secur. (VizSec)*, Oct. 2015, pp. 1–8.

[79] J. Yan, Y. Yang, W. Wang, H. He, and Y. Sun, "An integrated visualization approach for smart grid attacks," in *Proc. 3rd Int. Conf. Intell. Control Inf. Process.*, Jul. 2012, pp. 277–283.

[80] I. Macedo, S. Wanous, N. Oliveira, O. Sousa, and I. Praça, "A tool to support the investigation and visualization of cyber and/or physical incidents," in *Trends and Applications in Information Systems and Technologies* (Advances in Intelligent Systems and Computing), vol. 1368, Á. Rocha, H. Adeli, G. Dzemyda, F. Moreira, and A. M. R. Correia, Eds. Cham, Switzerland: Springer, 2021, doi: 10.1007/978-3-030-72654-6_13.

[81] J. Kopylec, A. D'Amico, and J. Goodall, "Visualizing cascading failures in critical cyber infrastructures," in *International Federation for Information Processing*. Boston, MA, USA: Springer, 2007, pp. 351–364.

[82] Y. Wadhawan, A. AlMajali, and C. Neuman, "A comprehensive analysis of smart grid systems against cyber-physical attacks," *Electronics*, vol. 7, no. 10, p. 249, Oct. 2018.

[83] K. Kaynar, "A taxonomy for attack graph generation and usage in network security," *J. Inf. Secur. Appl.*, vol. 29, pp. 27–56, Aug. 2016.

[84] J. Garae, R. K. L. Ko, and M. Apperley, "A full-scale security visualization effectiveness measurement and presentation approach," in *Proc. 17th IEEE Int. Conf. Trust, Secur. Privacy Comput. Commun. 12th IEEE Int. Conf. Big Data Sci. Eng. (TrustCom/BigDataSE)*, Aug. 2018, pp. 639–650.

[85] I. Sharafaldin, A. H. Lashkari, and A. A. Ghorbani, "An evaluation framework for network security visualizations," *Comput. Secur.*, vol. 84, pp. 70–92, Jul. 2019.

VICTOR COBILEAN (Graduate Student Member, IEEE) received the B.Sc. degree in mechatronics and the M.Sc. degree in mechatronic systems engineering from the Technical University of Cluj-Napoca, Romania, in 2020 and 2022, respectively. He is currently pursuing the Ph.D. degree in computer science with Virginia Commonwealth University, Richmond. His research interests include anomaly detection, informed machine learning, and unsupervised learning.

HARINDRA S. MAVIKUMBURE (Student Member, IEEE) received the B.Sc. degree in computer science from the University of Peradeniya, Sri Lanka, in 2018. He is currently pursuing the Ph.D. degree in computer science with Virginia Commonwealth University, Richmond. He is also a Research Assistant with Virginia Commonwealth University. His research interests include anomaly detection, machine learning, deep learning, and unsupervised learning.

BRADY J. MCBRIDE received the B.S.E.E. degree in electrical engineering from the University of Arkansas, USA, in 2018, where he is currently pursuing the master's degree in electrical engineering. He was an Intern with the Lawrence Livermore National Laboratory and the Idaho National Laboratory, from May 2021 to Mar 2022. His research interests include digital signal processing chips, distributed power generation, and firmware.

BJORN VAAGENSMITH received the B.S. degree in engineering with an emphasis in electrical engineering from Dordt University, Iowa, and the M.S. and Ph.D. degrees in electrical engineering with an emphasis on electronic materials and devices from South Dakota State University. Currently, he is an Electrical Engineering Researcher with Idaho National Laboratory (INL), where he has continued electronic materials projects. He has over five years of experience in building and working with custom power systems data acquisition solutions and performing various power studies. While at South Dakota State University, he was awarded the Integrative Graduate Education and Research Traineeship Scholarship, in 2012, to conduct research on transparent photovoltaics and develop solution processed transparent electrodes. His current research interests include photovoltaics devices, new electronic materials, electrospinning, machine learning, electric grid hardening, transformers, cyber-physical systems, and power grid resilience.

VIVEK KUMAR SINGH (Member, IEEE) is a Senior Researcher with the Cybersecurity Evaluation and Application Group (CEAG), NREL's Energy Security and Resilience Center. He leads a commercialization project with an industry vendor, works on 5G-Securely Energized and Resilient (SER) and NREL's Clean Energy Cybersecurity Accelerator (CECA) Projects. He was with the Power and Energy Systems Group, Idaho National Laboratory (INL), from 2020 to 2021. He has published research papers, patents, software disclosure records (SDRs), and featured in several media articles. His research interests include cyber-physical security for smart grids, wide-area monitoring, protection, and control (WAMPAC), hybrid energy storage systems, and cyber-physical federation testbeds. He has received awards from the U.S. Army Research Laboratory, NASPI, and ISU. He also received awards at Resilience Week 2018–2020 and the 2020 Texas Power and Energy Conference (TPEC).

RUIXUAN LI received the bachelor's degree in safety engineering from the Civil Aviation University of China, the master's degree in industrial engineering from University at Buffalo, and the Ph.D. degree in human factors and ergonomics from the University of Minnesota. She is a Human Factors Research Engineer with the Human Factors and Reliability Department, Idaho National Laboratory (INL). She was a Postdoctoral Research Associate with INL, in August 2019. Prior to that, she was a Graduate Student Researcher with the University of Minnesota, where she helped to develop user-studies for evaluating human factors on motion sickness in virtual reality. Her areas of expertise include research and development, human factors engineering, simulation, motion capture, and ergonomics. Her research interests include affordance perception, system design, visualization, human–machine interaction, human-automation interaction, and risk and resilience in cybersecurity.

CRAIG RIEGER (Senior Member, IEEE) received the B.S. and M.S. degrees in chemical engineering from Montana State University, Bozeman, MT, USA, in 1983 and 1985, respectively, and the Ph.D. degree in engineering and applied science from Idaho State University, Pocatello, ID, USA, in 2008. He is currently the Chief Control Systems Research Engineer and the Directorate Fellow with the Idaho National Laboratory (INL), Idaho Falls, ID, pioneering interdisciplinary research in the area of next-generation resilient control systems. He has 20 years of software and hardware design experience for process control system upgrades and new installations. He was a supervisor and a technical lead for control systems engineering groups having design, configuration management, and security responsibilities for several INL nuclear facilities and various control system architectures. He has authored more than 50 peer-reviewed publications. In addition, he has organized and chaired the 11 Institute of Electrical and Electronics Engineers technically cosponsored symposia and one National Science Foundation Workshop in this new research area.

MILOS MANIC (Fellow, IEEE) is a Professor with the Computer Science Department and the Director of the VCU Cybersecurity Center, Virginia Commonwealth University. He has completed over 40 research grants in AI/ML in cyber and energy and intelligent controls. He has authored over 200 refereed articles and holds several U.S. patents. He has won the 2018 Research and Development 100 Award for Autonomic Intelligent Cyber Sensor (AICS). He is the President Elect of IEEE IES, a fellow of the Commonwealth Cyber Initiative, and an Inductee of the National Academy of Inventors. He is an IES Officer and a Senior AdCom Member. He was a recipient of the IEEE IES 2019 Anthony J. Hornfeck Service Award, the 2012 J. David Irwin Early Career Award, and the 2017 IEM Best Paper Award. He was the Founding Chair of the IEEE IES Technical Committee on Resilience and Security in Industry and the General Chair of the IEEE IECON 2018 and IEEE HSI 2019. He was an Associate Editor of IEEE Transactions on Industrial Informatics and IEEE Open Journal of Industrial Electronics Society. He served as an AE for IEEE Transactions on Industrial Electronics.