Design of Next-Generation Cyber-Physical Energy Management Systems: Monitoring to Mitigation

Abhijeet Sahu, *Student Member, IEEE*, Katherine Davis, *Senior Member, IEEE*, Hao Huang, *Member, IEEE*, Amarachi Umunnakwe, *Student Member, IEEE*, Saman Zonouz, *Member, IEEE*, Ana Goulart, *Member, IEEE*

***Abstract*—There is a crucial need to enhance the reliability and resilience of our nation's critical energy infrastructure. Electric power systems are cyber-physical critical infrastructure with distinct, interacting networks comprising electrical, communications, and interdependency layers. Resilience requires modeling and monitoring all layers for prevention, early detection, and proactive threat assessment. This paper presents the research and design of a novel energy management system (EMS) called Cyber-Physical Resilient Energy Systems (CYPRES) to accomplish this goal. The CYPRES EMS architecture and methods are all cyber-physical to cohesively model and analyze the power system as a cyber-physical system (CPS). Results are illustrated for this proof-of-concept solution utilizing a 2000-bus cyber-physical synthetic electric grid.**

***Index Terms*—Cyber-physical Modeling, Energy Management System, Risk Analysis, Cyber-physical Vulnerability, Betweenness Centrality, Attack Graph**

I. Introduction

ELECTRIC power systems are mission-critical cyber-physical systems that are persistently targeted by cyber attacks. Attacks and other impending threats occur in new and unforeseen ways as modern technologies are coupled with legacy infrastructure. A range of potential intrusion points can be introduced by integration of new computing technologies that intend to improve capabilities for monitoring and control. The threat landscape is extensive and constantly changing [1]. The challenge this work addresses is to re-envision a unified cyber-aware and physics-aware secure data flow pipeline that extends from end-devices in the field, up through the applications in an energy management system in a control center, and ultimately back out to actuators for secure and resilient control. This paper hence introduces the prototype solution of the power system security defense project, *"Deep Cyber Physical Situational Awareness for Energy Systems: A Secure Foundation for Next-Generation Energy Management,"* with the objective to help energy delivery stakeholders own and maintain a a threat-resilient dataflow pipeline from sensors to actuators. The novelty of this work is the design and demonstration of a next-generation cyber-physical energy management system, giving the resulting required information toward achieving a *secure end-to-end system for managing the energy system, communications, security, and modeling and analytics*.

The major contributions of this paper are as follows.

- We propose a cyber-physical energy management system called **Cy**ber-**P**hysical **R**esilient **E**nergy **S**ystems **E**nergy **M**anagement **S**ystem ***(CYPRES EMS)*** that provides visibility into cyber and physical interdependencies for fast identification of cyber incidents that target physical impact.
- We design an end-to-end system for managing the energy system, communications, security, modeling and analytics in a next generation energy management system.
- We present the requirements, considerations, and lessons, as we extended from theory to lab to practice in security-oriented design, toward implementing this solution at electric power utilities.
- We present algorithms and prototypes to use cyber-physical content in visualizing and aiding grid situational awareness for different yet equally essential roles of grid operation and security personnel.
- We present the integration of data fusion and Bayesian inference to *CYPRES EMS* and its visualizations.
- We present an enhancement called *CyPSA-Live* for live updates on risk evaluation with various metrics and mitigations to patch vulnerabilities.

The paper proceeds as follows. Section II reviews related work. Section III presents the cyber-physical power system models, the model creation process, and the model's usage within the *CYPRES EMS*. Section IV introduces *CYPRES EMS* design, different *CYPRES EMS* functionalities, data source connections, and the enabled capabilities. Section V presents *CyPSA-Live*, a dynamic cyber-physical situation awareness analysis tool with live cyber and physical information. Section VI presents the usage of *CYPRES EMS* and *CyPSA-Live* together for improved situational awareness and risk mitigations. Conclusions and discussions follow in Section VIII.

II. Related Work

A. Extending the Energy Management System (EMS)

A power system EMS is conventionally defined as a collection of computer-aided applications such as topology processor, fault identifier, intelligent alarm processor, etc. [2]; it is used by utilities in the electric sector to monitor, control and optimize power generation, transmission and distribution operations. The expectations of an EMS's capabilities have evolved over time to include decision support, leveraging data analytics through knowledge extraction. Differences arise in

A. Sahu, K. Davis, H. Huang, A. Umunnakwe, and A. Goulart are with the Department of Electrical and Computer Engineering, Texas A&M University (e-mail: *abhijeet_ntpc*, *katedavis*, *hao_huang*, *amarachi*, *goulart@tamu.edu*). S. Zonouz is with Georgia Tech (e-mail: *szonouz6@gatech.edu*)

EMS applications due to factors such as location, system size, ownership, and purpose [2], e.g., whether it serves a single substation, a small control center, or a large utility. There are challenges unique to each of these environments, especially from a cyber-physical security perspective.

Recently, cybersecurity of distribution systems and end-devices, or the 'grid edge,' has been gaining interest by the research community, as it presents a large exposure and unknown risks due to accessibility and heterogeneity of devices that facilitate hidden threat surfaces. Hence, recent works are proposing EMS concepts for those systems, including building or home automation, e.g., an Enterprise Energy Management System (EEMS) in [3] to reduce costs, increase efficiency, and improve energy planning and cost allocation for buildings. Security plays a major role in the future of these systems, especially as advanced analytic and communication technologies with new interactions, such as between a centralized EMS and home automation systems, are being introduced. These needs prompt the EMS to offer consumers actionable information and control features, while ensuring ease of use, availability, security, and privacy [4]. In [5], Luo *et al.* propose a cloud-based information infrastructure for next generation power grids to satisfy requirements of fast reaction to disturbances and faults, wide-area data management, high-performance computing, real-time analysis, and data security. In [6], Howell *et al.* argue a new generation of EMS is required to orchestrate the interplay between dense, diverse, and distributed energy components. A methodology with security quantification, formal methods, and tool creation for advanced metering infrastructure is presented in [7]. In [8], authors propose to apply methods from the internet of things (IoT) to the EMS for energy efficiency, trustworthy data collection, and intelligent security planning for distributed energy systems.

B. Evolution of the Problem with the State of the Art

Traditional technology monitors and controls physical and cyber sides of energy infrastructure separately. Historically, security solutions for energy management systems focused on device and hardware-specific security [9], [10], such as threat mitigation through cryptographic solutions and key management. Protocol and device security has also been extensively studied for Supervisory Control and Data Acquisition (SCADA) and Industrial Control Systems (ICS), e.g., [11]–[13]. In [14] and [15], research on cyber-physical modeling platforms shows that existing abstractions and techniques are inadequate; challenges include multiple models and variants of components, and the need to ensure consistency across models. These works illustrate that current tools are not sufficient to account for cyber-physical interconnections. Hence, while combined research in both power systems and cybersecurity have resulted in myriad improvements in cyber-physical modeling, detection, and response over the past decade, these functions are still done separately and from separate cyber and physical sides. Hence, the research to develop the requirements, design, and implementation of such an EMS on the large-scale cyber-physical power system side has remained largely unexplored prior to this work.

With the integration of multiple features such as data acquisition from diverse sources, latency in communication between physical devices becomes a concern. A persistent challenge is the latency requirement of EMS applications, susceptible to varying data rates of devices and communication link bandwidths affected by network congestion or intrusions. This challenge motivates EMS design, e.g., in temporal and spatial correlation for automatic voltage control, network remodeling, and online decision-making [16]. Delays in addressing transmission, propagation, processing, and queuing are extensively reviewed in [17]. EMS design is also motivated by high renewable energy levels and their operational challenges, driving the need to incorporate uncertainty into EMSs, e.g, [18] that proposes how utility control rooms can consider wind power generation uncertainties. Hence, related works focus on physical operations' optimization in the EMS, while cyber threats are handled through a separate Security Information and Event Management (SIEM) such as *Splunk Enterprise SIEM, SolarWinds SIEM, DataDog*, etc., which monitor Syslog, firewall logs, and other networking device logs for inferring intrusion activities.

However, cyberattacks are emerging issues, such as the threat in European Network of Transmission System Operators for Electricity (ENTSO-E) [19], the Ukraine attacks in energy distribution companies [20], and the Stuxnet compromises of programmable logic controllers [21]. The above cyberattacks all bypass the intrusion detection systems (IDS) and deceive the operators until certain conditions trigger their malicious functions. In [22], the adversary intrudes into the network and can strategically falsify the data and control commands. It is thus an urgent task to equip the EMS with the ability of categorizing, detecting, and defending against threats with the information from both cyber and physical domains.

While the general approach of combined cyber and physical defense has now been proposed in different ways over the past decade, the end-to-end holistic energy management system concept of the proposed *CYPRES EMS* had not been envisioned, proposed, or attempted before. Part of the reason why this had not been done before is that the high fidelity level of details of these models, and the disparate data sources and formats in the real systems, make it extremely challenging. It requires highly detailed model information from traditionally distinct disciplines that 'own' different roles and data within an electric power utility organization (power, protection, security, communications, etc.). These have to come together to establish the automatic and accurate map for these models together, to achieve the large-scale cyber-physical power system model in a mathematical and machine readable format for subsequent analysis of these large scale cyber-physical power systems.

To bridge this separation, our proposed EMS merges the functionalities of the cyber-based SIEM and physical-focused EMS, for secure and resilient control. The foundation of the proposed EMS is based on a hierarchical model, designed considering various data-flow requirements depending on the protocols used by the field devices, SCADA and HMI servers, etc. *CYPRES EMS* focuses on cyber-physical modeling of a large-scale electric grid in detail with communication infrastructures such as routers, switches, relays, RTUs, HMI, PI servers, etc. [23], in addition to security devices such as firewalls and IDSs [24]. By modeling the composed system end-to-end, it is possible to formulate and solve the equations of the subsystems together and avoid superficial solutions that only seek to patch known problems in a one-off manner. *CYPRES EMS* also leverages custom logic in IEC 61131 in the SEL Real Time Automation Controller (RTAC) device to detect and respond [25] and incorporates multi-domain multi-sensor cyber-physical data fusion for intrusion detection [26]. To address uncertainty in alerts from the sensors, *CYPRES EMS* also provides a framework for evidence-theoretic rules of combination [27]. It is important to note that *CYPRES EMS* works well with and complements existing efforts. It is designed to be modular and work with utilities where they are now, with current data sources and tools.

In summary, the modeling and control of cyber-physical power systems have warranted increasing attention from the research community. While society recognizes the need to prioritize *resilience* of these systems, significant work remains to fully equip stakeholders to prepare for, endure, and recover from unplanned hazards including cyber attacks [28]. The proposed solution offers a cyber-physical modeling foundation to rebuild energy management systems from the ground-up.

III. Cyber-Physical Power System Modeling Preliminaries

The workflow diagram of *CYPRES EMS* is presented in Fig. 1, with inputs of cyber, physical, and interconnection models. This section presents the models of each layer.

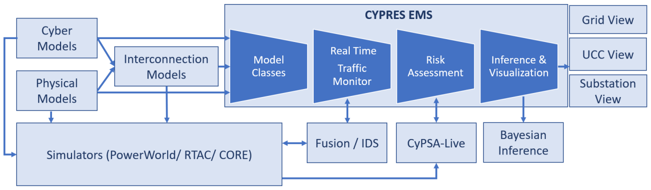


Fig. 1: Workflow diagram for *CYPRES EMS*.

A. Cyber Models

An exemplar case is built and used to study the operations and defense of large-scale cyber-physical power systems. The cyber-physical synthetic model is built from the 2000-bus synthetic electric grid test case [29] based on public information and statistical analysis of real power systems. The communication/cyber model defines networking devices that support power generation, transmission, and distribution operations. Our synthetic communication model [23] defines the models for routers, switches, firewalls, EMS servers, DNP3 Master, ICCP servers, etc., as nodes, while links represent the communication channel types such as microwave, Ethernet, or MPLS/fiber links. DNP3 is employed between substations and between each utility control center (UCC) and its substations, while ICCP is employed between balancing authorities (BAs) and UCCs. The interconnections between cyber and physical exist through substation intelligent electronic devices, such as remote terminal units, protective relays, etc., which directly connect and control physical components and supply data. The cyber models include following:

1) Hierarchical Model of Communication Network: The cyber components are created following a hierarchical communication model of a regional reliability coordinator interacting with electric utilities or market participants, which may include a scheduling entity, load-serving entity, resource entity, or transmission/distribution service provider. The model has three primary levels: BAs, UCCs, and substations as shown in Fig. 2.

- **Balancing Authority (BA)**: BAs handle generation-load balancing via generator dispatch and load control. Most BAs interact with market participants by *coordinating scheduling* such as economic dispatch, unit commitment, and *reserve sharing* to regulate reserves via seconds to minutes transactions. BAs are responsible for frequency control. Hence, a BA consists of a collection of ICCP servers and clients for each market participant and a dedicated firewall to filter ICCP traffic which carries periodic data, e.g., time stamp, status and analog points, block data, and control commands. Routers and switches are deployed for network segregation and VLAN creations.
- **Utility Control Center (UCC)**: A UCC hosts multiple servers for dedicated purposes such as state estimation; post fault analysis; and transient, small signal, and voltage stability in an EMS. In our testbed, to design and test CYPRES, we deploy four nodes: (1) for interacting with the BA using ICCP, (2) for controlling and monitoring substation devices using DNP3, (3) for interacting with the utility's corporate network, and (4) for third parties or vendors through their dedicated Demilitarized Zones (DMZs). A DMZ is a perimeter network to protect an internal LAN from untrusted traffic. For example, a web-server in the DMZ fetches the real-time Area Correction Error (ACE) and frequency information from a database server that gets updated from a Historian server in the SCADA DMZ in the UCC. Further, the UCC hosts an ICCP node that updates reports from the web-server, and forwards the response to the ICCP client's request running in the BA. Threats include XSS and SQL injection for manipulating real-time data that can enforce malicious Automatic Generation Control (AGC) setpoints. For the defense against such threats, at the UCC, the Snort IDS is deployed, in addition to continuous patching of the web server, for validating user-inputs.
- **Substation**: A substation consists of a local control center with devices stationed in three levels. At the station level, an operator workstation, controllers, DNP3 outstations, local database, or web server may be deployed. At the bay level, industrial automation and control devices such as the RTAC, remote terminal units (RTUs), bay controller, and relays are deployed. At the process level, the current and potential transformers, breakers, and isolators are stationed are directly connected to the feeders or transformers. In our model, we deploy one RTAC for each substation, controlling multiple relays. A substation firewall is deployed to filter substation traffic.

Using k-means clustering, the geographical location of the UCC is determined for groups of substations. The green-

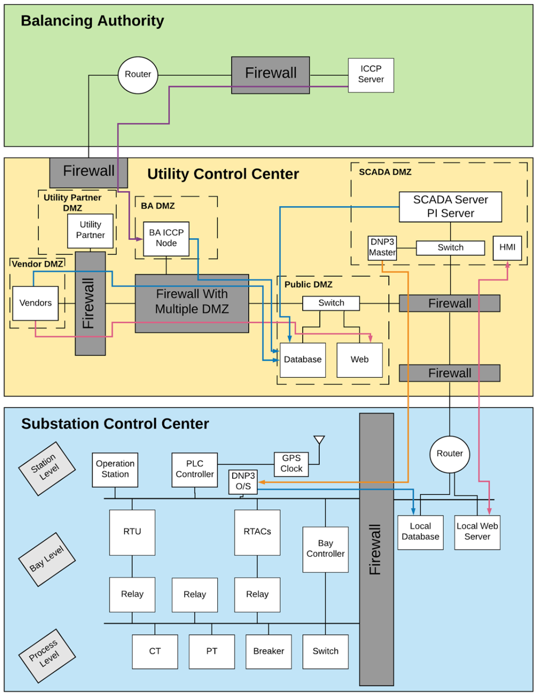


Fig. 2: Hierarchical model of the synthetic communication network [30].

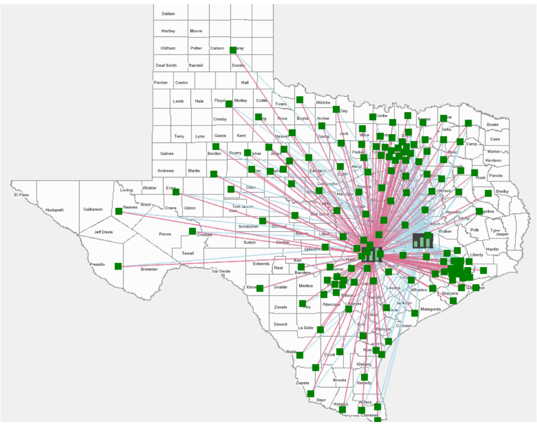


Fig. 3: Power network to node-breaker topology to cyber network connection for a large-scale synthetic electric grid.

colored icons in Fig. 3 map the UCC locations in the communication network. A star topology is considered in all the three levels to simplify configuring static routes and firewall policies. There can be also be hybrid topologies. Under such scenarios, Djikstra's shortest path algorithm is used to compute shortest paths from the substation to the UCC and vice-versa to compute the routing tables with highest priority.

2) IP Schemes: In this work, for IP allocation, depending on the potential systems within a broadcast domain, class A is used for BAs, class B for UCCs, and class C for substations, as elaborately discussed in our previous work [23].

3) Firewall Models: The *BA Firewall* secures BA communication with respective market participants. Currently, these firewalls are configured to allow ICCP requests and response between the ICCP node in the BA and the UCCs. Next, in the *Utility DMZ Firewall* within UCC, five DMZs are configured for: SCADA, corporate network, BA, public, and for vendors to access the public network. Corporate and vendor DMZs are protected by two different interfaces of a shared firewall, also connected to one end of the public DMZ. Furthermore, the ICCP DMZ is behind the *Utility-BA Firewall* connected to the BA, where it only communicates with the BA's ICCP node. On the other side of the public DMZ, the *Utility-Substation Firewall* is also connected to the inside of UCC and the substation, while the substation network includes one *Substation Firewall* which divides it into two subnets with high security levels: one is for the relay network which sends all power information back to the UCC, and the other is for the substation DMZ which includes a local database and web server, which the UCC accesses for historical substation data. The details on the interfaces, object groups and the access control lists are illustrated in our firewall paper [24].

4) Router Models: A *Substation Router* is deployed for communicating with the UCC in the star topology, with substations and UCC in the mesh topology. Next, two *UCC Routers* are deployed in a UCC, where one router interfaces all substations, and the other interfaces the BA. The *BA Router* interfaces with other BAs and their market participants.

5) Intrusion Detection System (IDS) Models: The *CYPRES EMS* modeling environment in the RESLab testbed [31] contains the following IDS models, where additional defenses can be added:

- *Rule-based IDS*: The rule-based IDS are configured to model common industry security controls. The Snort IDS is configured to operate within containers modeled as routers in the CORE emulation network in RESLab. The configured rules are related to ICMP flood, ARP spoof, and DNP3 payload modification attacks. Currently, Snort pipelines alerts to a Logstash server configured in the virtual machine (VM) hosting the CORE emulation, as detailed in [22], [31].
- *Anomaly-based IDS*: A multi-sensor data fusion framework is developed for training machine learning centric anomaly-based IDS using features constructed from both physical and cyber sensors as detailed in our prior work [26].
- *Dempster Shafer-based Fusion IDS*: In [27], this IDS is proposed to address uncertainty in alerts to reduce false alert rates. A location-cum-domain based fusion framework is proposed and evaluated with different combination rules, that fuse multiple evidence from inter-domain and intra-domain sensors.

B. Physical Models

The physical model is the 2000-bus synthetic grid with 1250 substations, 2000 buses, 3206 branches (transmission lines and transformers), and 544 generators. This model facilitates analysis of numerous threat and defense scenarios, from steady-state *N-x* contingencies to transient state fault analysis, without disclosing any real system information.

Below are detailed physical models that enable the mapping between, and the study of, cyber-physical components (e.g. protective relays) for their security and importance. The protective relay location in the detailed power system model is connected with its detailed transient stability model, that may be built from ingested actual settings. The link between the power model, communications model, and the device itself (with its logic and configurations) have crucial cybersecurity implications. To be specific, a protective relay is an interconnection to bridge cyber and physical networks. It also contains both physical network information (e.g., circuit breaker location, connected buses and branches, measurements) and cyber network information (e.g., protocols, IP addresses, local area network gateways, logic configurations), Functionally, relays protect the power system against faults and instability. Relays may also use communication networks through wired or wireless access. Thus, threats include to falsify their settings and their controls or to leverage their vulnerabilities for lateral movement that can cause unexpected disturbances.

- **Identifier Mapping Scheme**: In the electrical system model, each relay type that we model and analyze has a unique set of fields. The linking of the relay to the power system model is based on identifiers in the configuration file, where the naming convention used is crucial. For example, in some SEL 421 relays, the field name is *SID*, and the identifiers can follow a pattern like *"FSUB/BKID/TSUB"*; *FSUB* is the identifier of the "from" substation, TSUB is the identifier of the "to" substation, and BKID is the ID of the protected circuit breaker(s).
- **Distance Relay Modeling**: DISTRELAY models [32] can be automatically built in PowerWorld Dynamic Studio (PWDS) power simulator to simulate relay actions when a fault occurs. To be passed into the power system model, per unit conversion for data fields from the configuration files (shown below) are required:

$$V_{NomHighSide} = PTRY \cdot VNOMY \tag{1}$$

$$Z_{base} = V^2_{NomHighSide}/S_{base} \tag{2}$$

$$Z_{1ReachPrimary} = \frac{PTRY}{CTRX} \cdot Z1P\angle Z1Ang \tag{3}$$

$$Z_{1ReachPU} = \frac{Z_{1ReachPrimary}}{Z_{base}} \tag{4}$$

$$Z_{1PDSec} = \frac{Z_{1PD}}{f_{nomHz}} \tag{5}$$

  where *PTRY* is PT ratio; *CTRY* is CT ratio; *VNOMY* is nominal voltage on PT low side; *Z1P* is zone 1 reach; *Z1Ang* is positive seq line z angle (degrees); and Z_{1PD} is zone 1 pickup. More detailed relay modeling can be incorporated for a thorough transient analyses.

  The modeling uses PowerWorld, and the example Zone 1 (Z_1) calculation is similar for each zone. The extracted fields are passed into PowerWorld, where transient stability relay models are created and available to link with cyber device models and cyber-related information.
- **Device's Power System Importance**: Once the device is modeled, transient stability and power flow studies are possible with the connected relays based on actual device settings. To streamline analysis, critical clearing time (CCT) analysis can identify elements susceptible to short or sensitive CCT. Identifying lines whose CCT is low and linking to the corresponding relays and breakers as well as the cyber network is useful to prioritize relays based on their cyber-attack surface, as shown in [33]. Quantifying a device's importance via its impact allows prioritized monitoring and defenses to be focused around those critical devices.
- **Device's Cyber System Placement**: As opposed to a device's physical power system placement, placing a device in the cyber system can be a more abstract concept. If a device has an IP address, its existence can be modeled in the context of the system control network model. From configuration settings, an entire new realm of cyber-physical analyses exists which, for instance, allow for modeling communication access paths and device commonalities at the settings/logic level that can present common mode failures and vulnerabilities that would otherwise not be known to the system operators.

The following subsection presents the mapping between cyber and physical components to enable a holistic perspective for the end-to-end security analyses.

C. Cyber-Physical Interconnection Models

Protective relays, SCADA, and other substation devices are major interconnection points between cyber and physical models.

1) DNP3 Outstations: For each substation in the synthetic grid, we created DNP3 [34] outstations using Algorithm 1 based on the Substation ID. Then, the DNP3 points for the generators, loads, shunts and branches are grouped into each outstation. Within each DNP3 outstation, Analog Input (AI), Analog Output (AO), Binary Input (BI), and Binary Output (BO) tags are created for each bus, branch, generator, load and shunt, as follows:

- **Analog Inputs (AI)**: AI tags are inserted for substation devices. `Bus:` voltage angle, frequency, and p.u. voltage; `Branch:` real and reactive power flow, current; `Generator:` real and reactive power output; `Load:` real and reactive power; `Shunt:` reactive power.
- **Analog Outputs (AO)**: AO tags are inserted to control generator setpoints. Load MW can be added to represent the ability to do partial load shedding, as well as transformer tap ratios. `Generator:` real power setpoint and voltage magnitude setpoint.
- **Binary Inputs (BI)**: Device status tags (On/Off) are inserted for substations' `Bus`, `Branch`, `Generator`, `Load`, and `Shunt`.
- **Binary Inputs (BO)**: Control tags are inserted for `Bus`, `Branch`, `Generator`, `Load`, and `Shunt` to control (On/Off) status.

Conventional power system studies are based on a bus-branch model, which is an abstract model. It simplifies the substation topology to one or few buses, and ignores the layout of circuit breakers. To include detailed cyber topology, it is necessary to expand the bus-branch model into the node-breaker model that has the layout of circuit breakers and

TABLE I: Example of relay label for branches at substation side.

Relay Label	IP Address	Substation ID	Bus Topology	Identifier Mapping FBus_TBus_CircuitID	Physical Element	Protection Device	Protection Device	Protection Device
$Relay$1_1001_1064_1	10.52.xxx.xxx	1	*Single Bus*	1001_1064_1	$Line$8166_8784_1	$Disconnect$8165_8166_1	$Breaker$8164_8165_1	$Disconnect$1001_8164_1
$Relay$1_1001_1064_2	10.52.xxx.xxx	1	*Single Bus*	1001_1064_2	$Line$8169_8745_2	$Disconnect$8168_8169_1	$Breaker$8167_8168_1	$Disconnect$1001_8167_1
$Relay$1_1001_1071_1	10.52.xxx.xxx	1	*Single Bus*	1001_1071_1	$Line$8172_8830_1	$Disconnect$8171_8172_1	$Breaker$8170_8171_1	$Disconnect$1001_8170_1
$Relay$1_1001_1071_1	10.52.xxx.xxx	1	*Single Bus*	1001_1071_2	$Line$8175_8833_2	$Disconnect$8174_8175_1	$Breaker$8173_8174_1	$Disconnect$1001_8173_1

Notes:Dummy IP Addresses

Algorithm 1 Generate DNP3 Tags For PowerWorld Case and RTAC

```
Collect Case information for Bus, Branch, Load, Generator, Substation
Group devices based on Substation
Identify all Buses within Substation
if The Bus Number of a device is within the Substation then
    Add the device to that Substation
end if
for Each Substation do
    Create DNP3 Outstation with Substation ID
    Create DNP3Object for all devices within the substation with specified DNP3PointType, VariableName, and DNP3PointEventClass
    Create RTAC DNP3 tags for each client with the user-defined pattern: PowerWorld_RTAC_SubstationID_DNP.DNP3PointType_SubstationID_Device_VariableName
    Create RTAC DNP3 tags for tag processor with the user-defined pattern: PWDS_Data.DNP3PointType_SubstationID_Device_VariableName
end for
Note: DNP3PointType specifies data type: AI, AO, BI, or BO. VariableName specifies measurements like bus voltage, branch real power flow. DNP3PointEventClass defines the event class of the data. Device includes the device type, such as bus, branch, generator, etc., and their corresponding key identifier in the case.
```

associated devices, such as switches and bus bar. This allows for mapping the cyber with the physical topology for control relationships, such as protective relays that monitor a branch's current and control its circuit breakers.

To achieve the node-breaker model that would exist in an EMS, based on bus nominal voltage, we expand the bus topology to Single Bus Topology for bus nominal voltage under 200 kV, and Ring Bus Topology for bus nominal voltage over 200 kV. This inserts bus nodes to extend the model to a node-breaker model that represent more detailed substations and cyber-physical scenarios.

To run power system simulations and integrate them with the cyber network, we build and maintain a map that connects the bus-branch with the node-breaker model. In this way, it is possible to simultaneously use the coarse-grained bus-branch model to provide power system data to the cyber network through the DNP3 protocol, while using the detailed node-breaker model to study the physical devices and substation configurations.

2) Real Time Automation Controller (RTAC): In this work, the SEL RTAC is integrated into our models and experiments to control and communicate with substation devices and the UCC [35]. RTAC is an industrial automation and control device used in substation automation systems and SCADA as remote terminal units (RTUs). It supports various ICS communication protocols, such as DNP3, Modbus, IEC 60870, IEEE c37.118, and IEC 61850. Its tag processor converts data between protocols and sends it to an upstream processor for data concentration and management. The functionality of RTAC makes it an ideal device in testbeds. Previous studies have used the RTAC to reconfigure network structure [36], control switches and tap-changers [37], send power setpoints to control battery storage management systems [38], [39], and implement defensive logic against cyberattacks [25]. In [40]–[42], the cyber-physical power system testbeds used RTAC to work as an RTU, to collect data from protective relays, send it to SCADA software, and perform protocol conversion.

3) Relay Types: Three relay types are considered in our model: **Load relays** control disconnects and breakers in the `Load` bus; **Line relays**, consisting of over-current relays and distance relays, protect transformers and transmission lines; **Generator relays** control disconnects and breakers in each `Generator` bus. The detailed model information is available from [43].

Table I shows an example of mapping the cyber and physical systems using protective relays as the interconnection identifier. Each protective relay has an **Identifier** from the physical network and a *relay type*; these are used to create a unique **Relay Label**. In the cyber network, the relay may receive an **IP address**. Each relay is assigned to protect a **Physical Element** and other **Protection Device(s)**, based on the **Bus Topology** from the *node-breaker model*. Through this cyber-physical mapping, we are able to study and analyze the power system through a holistic cyber-physical perspective.

The following section shows how these models enable a comprehensive visualization and analytics of the cyber-physical power systems in *CYPRES EMS*.

IV. *CYPRES EMS*

Building on the cyber and physical models, we now take a design perspective to introduce objects, classes, and functions that comprise the main code library of *CYPRES EMS*. This is a living code base that continues to grow and expand. This section describes the foundational aspects of the current *CYPRES EMS* prototype that allows that growth.

A. Design Guidelines

The design of *CYPRES EMS* is based on the following criteria: (1) OT/IT network visualization of UCC, substations, and BA; (2) critical asset ranking, monitoring and control; (3) intrusion access path visualization; (4) causal/Bayesian inference and structure learning; (5) real-time monitoring of physical and cyber alerts; (6) inter-connection with a network emulation software such as CORE and Minimega; and (7) inter-connection with power system emulator such as PowerWorld Dynamic Studio (PWDS).

B. CYPRES Object-Oriented Class Overview

CYPRES EMS is written in C#, an object-oriented programming language. The code defines several classes that enable the *CYPRES EMS* model, according to the diagram in Fig. 1. These model classes include the `TopologyGeneration` class which uses the other classes to generate the communication model. There are classes that model the BA, UCC, and substations, such as the `BalancingAuthority`, `UtilityControlCenter`, and `Substation` classes. Other classes model devices such as `Firewall`, `Router`, `Switch`, `CyberHost`, `Relay`, and `RelayController`.

C. Grid View

As shown in Fig. 3, CYPRES creates an interactive map. It is created by the built-in `GridCyberView` class which uses the EasyGIS library. A `Start DNP3 Master` button provides access to the DNP3 master's terminal so that users can control the DNP3 outstations. Important functions include `PlaceSubstationControl()`, `PlaceUtilityControl()`, and `PlaceBalancingAuthority()` to allow users to control the substations, UCC, and the BA.

These user control functions can be found in the `CyberUserControls` directory: `CreateLinks()` to create the links between the UCC and the BA, `GetDNP3()` to obtain real-time traffic, and `GetPerformanceCounters()` to collect the traffic and populate it into the charts. A `dnp3Thread` object communicates with the application in another VM, which has an IP address and port number pre-configured in a file. `GridCyberView_Load()` is the main function that populates the entire form. It also starts the back-end threads, draws the charts, and links the map.

D. UCC View and Control

The `UtilityView` class displays the UCC devices (Fig. 4), where the pie charts on the right show the ratio of devices that are compromised, under alert, or in normal state. This is also indicated by the red rectangle around each component. By clicking on each component, its traffic can be observed in real-time in the spline chart shown in the right. The radio button can change the theme from Light to Dark, while the network topology with other alert views can be saved using "Save Utility N/W" menu item. Finally, the small black squares on the right shows the substation view, which is described next.

E. Substation View and Control

The substation view in Fig. 5 allows users to configure cyber and physical nodes. For example, users can modify the substation network's firewall rules (Fig. 6) that filter traffic from the DMZ and UCC networks to the protection devices. For physical devices, users can configure the relay from the RTAC (Fig. 7) by viewing and modifying the breaker controls (Fig. 8).

F. Real-Time Traffic Monitoring

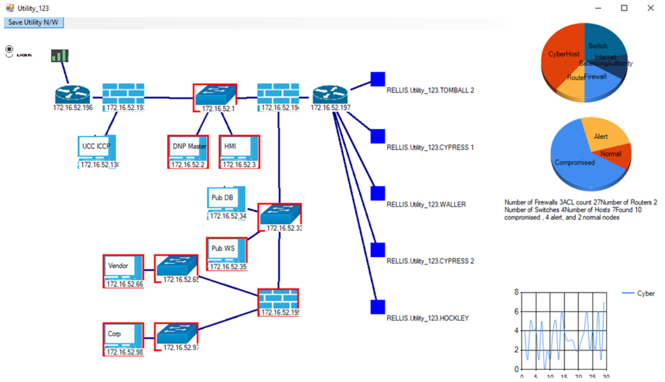
CYPRES monitors the ICS data packets between the substation's network nodes and DNP3 outstations, along with Snort IDS alerts, the cyber network's OSI layer information, and traffic flow information. They are monitored in real-time for cyber-physical data fusion and intrusion detection. The details of this traffic monitoring, the role of our cyber-physical testbed including experiments with various use cases and threat models are shown in Fig. 9. These are described in more detail in Section VII.

G. Bayesian Inference

Deciphering point of intrusion using attack trees has been studied thoroughly for risk assessment, since attack trees or graphs capture the relationships among various vulnerability exploits that an intruder utilizes, along with the privilege escalations to compromise a single or a set of targets. The construction of such data structures depends on the IDS alerts or other sensor logs, which cannot be trustworthy and can have erroneous readings due to random system behavior or faulty sensors. This uncertainty may be *aleatory*, due to random behavior of the system, or *epistemic*, due to lack of complete knowledge of the system, and can be tackled by probabilistic formalism, e.g., a) Monte-Carlo, b) Bayesian, and c) Dempster-Shafer Theory [44]. Among these, the Bayesian formalism based on Bayes Theorem is preferred, as it assists in causal reasoning between each step in the access paths of the adversary's trajectory to compromise the target, and it allows use of prior knowledge from cyber forensic experts from historical data.

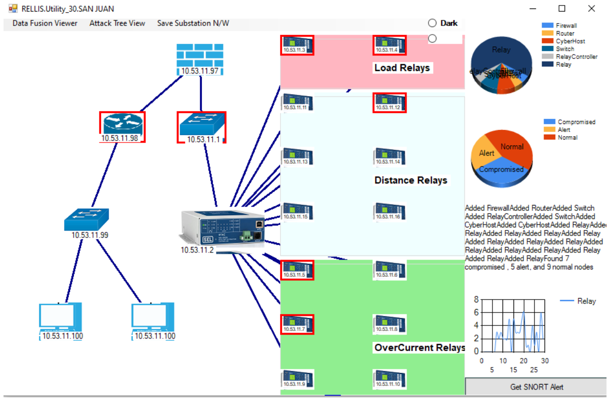
Using Bayes Theorem (Eq. 6), we explore the inference of attack graph structures based on real-time cyber and physical alerts,

$$P(A|B) = \frac{P(B|A) * P(A)}{P(B)} \tag{6}$$



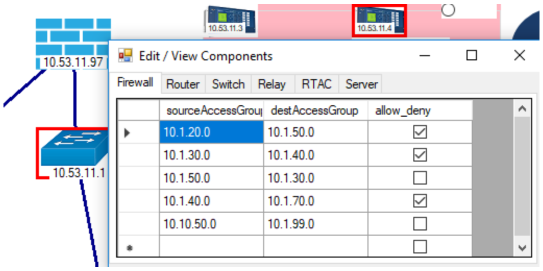
Number of Firewalls 3ACL count 27Number of Routers 2
Number of Switches 4Number of Hosts 7Found 10
compromised , 4 alert, and 2 normal nodes

Fig. 4: Utility control center view.



Added FirewallAdded RouterAdded Switch Added RelayControllerAdded SwitchAdded CyberHostAdded CyberHostAdded RelayAdded RelayAdded RelayAdded RelayAdded Relay Added RelayAdded RelayAdded RelayAdded RelayAdded RelayAdded RelayAdded Relay Added RelayAdded RelayFound 7 compromised , 5 alert, and 9 normal nodes

Fig. 5: Substation view.



	sourceAccessGrou	destAccessGroup	allow_deny
▸	10.1.20.0	10.1.50.0	☑
	10.1.30.0	10.1.40.0	☑
	10.1.50.0	10.1.30.0	□
	10.1.40.0	10.1.70.0	☑
	10.10.50.0	10.1.99.0	□
*			□

Fig. 6: Firewall configuration interface.

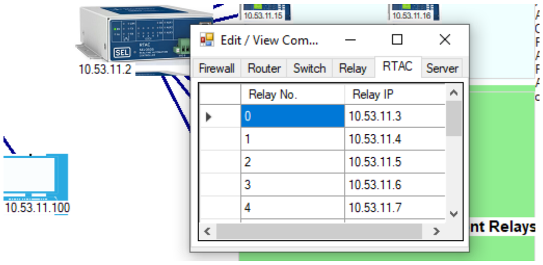
where A and B are events, and $P(A|B)$ is the conditional probability that an event happens, such as the compromise of node A, given that node B is already compromised. $P(A)$ is the *prior*, $P(B)$ is the *evidence*, $P(B|A)$ is the *posterior* probability, i.e., the likelihood that node B is compromised if node A is compromised. The technique of Bayesian inference is used to update the posterior probability when a new evidence is obtained. As the number of network nodes grows, the chain-rule of conditional probability is considered. For instance, an attack graph with three nodes would have the joint probability of multiple evidences computed as in Eq. (7).

$$P(A, B, C) = P(A|B, C)P(B|C)P(C) \tag{7}$$

Thus, the chain-rule as in Eq. (7) is used, where the number of random variables grows with the number of nodes in the attack graph.

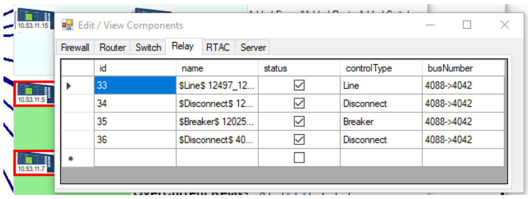
The size of attack graphs can be pruned for faster inference of posterior probabilities, such as $P(B|A)$ in Eq. (6). Inference algorithms such as Pearl's Belief Propagation (BP), Junction tree, and Variable Elimination (VE) have been incorporated in *CYPRES EMS*. To address the zero-day exploit scenarios, *CYPRES EMS* also implements structural learning algorithms for the attack graphs, such as Monte Carlo Markov Chain sampling-based, Chou Liu algorithm, Cooper and Herskovitz algorithms. These algorithms leverage Bayesian inference to detect intrusions in the cyber-physical system modeled in *CYPRES EMS*.

For instance, when a user selects the sub-graph of $Utility$ 39 UCC, then selects an inference type and a compromised node as $Firewall$ 1368, *CYPRES EMS* displays a view similar to Fig. 10. It has a table that shows the conditional probability associated with the selected node, i.e., $Utility$ 39..$Firewall$ 1368. For example, the score of 0.5095 shows the conditional probability of $Host$ 2774 being compromised if $Firewall$ 1368 is compromised. The right side of the tool shows the learned structure of the Bayesian Network based on real-time alerts. The graph-based structure learning algorithms are implemented in Python and incorporated in *CYPRES EMS* based on our paper [45].



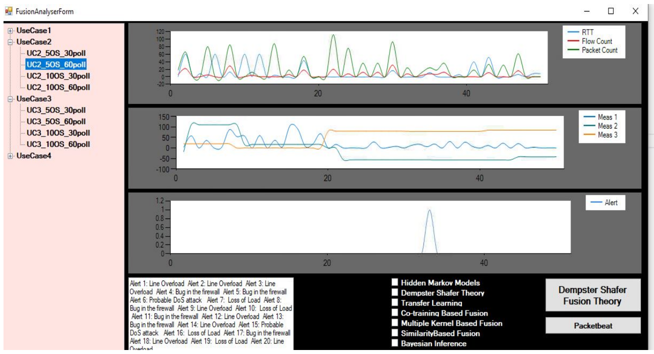
	Relay No.	Relay IP
▸	0	10.53.11.3
	1	10.53.11.4
	2	10.53.11.5
	3	10.53.11.6
	4	10.53.11.7

Fig. 7: Relay controller configuration interface.



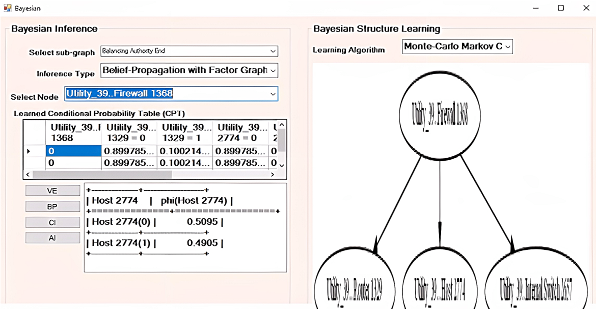
	id	name	status	controlType	busNumber
▸	33	$Line$ 12497_12...	☑	Line	4088->4042
	34	$Disconnect$ 12...	☑	Disconnect	4088->4042
	35	$Breaker$ 12025...	☑	Breaker	4088->4042
	36	$Disconnect$ 40...	☑	Disconnect	4088->4042
*			□		

Fig. 8: Line relay controlling breakers and disconnects through protective relay-based cyber-physical mapping.



Alert 1: Line Overload Alert 2: Line Overload Alert 3: Line Overload Alert 4: Bug in the firewall Alert 5: Bug in the firewall Alert 6: Probable DoS attack Alert 7: Loss of Load Alert 8: Bug in the firewall Alert 9: Line Overload Alert 10: Loss of Load Alert 11: Bug in the firewall Alert 12: Line Overload Alert 13: Bug in the firewall Alert 14: Line Overload Alert 15: Probable DoS attack Alert 16: Loss of Load Alert 17: Bug in the firewall Alert 18: Line Overload Alert 19: Loss of Load Alert 20: Line Overload

Fig. 9: Cyber-physical real-time traffic monitoring for various threat use cases.


Bayesian
Bayesian Inference
VE
BP
CI
AI
Bayesian Structure Learning
Utility_39..Firewall 1368
Utility_39..Router 1329
Utility_39..Host 2774
Utility_39..Internal Switch 3657

Select sub-graph: Balancing Authority End

Inference Type: Belief-Propagation with Factor Graph

Select Node: Utility_39..Firewall 1368

Learned Conditional Probability Table (CPT)

	Utility_39..I 1368	Utility_39... 1329 = 0	Utility_39... 1329 = 1	Utility_39... 2774 = 0	U 2
▸	0	0.899785...	0.100214...	0.899785...	0
	0	0.899785...	0.100214...	0.899785...	0

```
+-----------+----------------+
| Host 2774    |   phi(Host 2774) |
+===========+================+
| Host 2774(0) |          0.5095 |
+-----------+----------------+
| Host 2774(1) |          0.4905 |
+-----------+----------------+
```

Learning Algorithm: Monte-Carlo Markov C

Fig. 10: Bayesian Inferencing using methods such as Variable Elimination, Causal Inference, and Belief Propagation.

There are additional components that are or can be incorporated to the main *CYPRES EMS* code library; however, their discussion is beyond the scope of this paper. For example, the data fusion engine [26] and other techniques mentioned in Section III are co-designed for use in *CYPRES EMS*.

Next we highlight a major application of *CYPRES EMS* for real-time cyber-physical situational awareness and risk analysis.

V. CyPSA-Live

An integral part of the CYPRES EMS is dynamic cyber-physical situational awareness analysis (CyPSA). The previous version of CyPSA# application [46] performed an offline risk analysis, as it depended on NP-View's firewall and network topology files. CyPSA# used these files to to statically construct the attack graph model. Cyber network vulnerabilities were based on the $nmap$ reports, which identified vulnerabilities associated with the open ports. These vulnerabilities were then mapped to an 8-substation power system model [47].

The architecture of *CyPSA-Live* (Fig. 11) provides these new functionalities:

1) Generates an attack graph model in real-time by interacting with the NP-Live server [48].
2) Interacts in real-time with the NVD to obtain cyber vulnerability severity rating, and impact scores.
3) Extracts the list of possible CVEs by integrating *nmap* open ports reports with Nessus [49] alike features.
4) Patches the vulnerabilities and recomputes the paths, critical asset rankings, and security index.
5) Integrates the betweenness centrality (BC) and cyber-physical betweenness centrality (CPBC) metrics [50].

The functionalities incorporated in *CyPSA-Live* will further assist in: a) Integrating the Resilient Energy System Laboratory (RESLab) testbed with the NP-Live server to extract the updated firewall policies computed after a cyber intrusion. This capability will provide dynamic risk assessment to *CyPSA-Live* during real-time operation of the ICS network modeled in RESLab. b) Integrating *CyPSA-Live* into the OpenAI-Gym environment for training a defender agent to take optimal defense action through modifying firewall policies and router configurations to operate the grid under cyber intrusions. The reward model would be based on the scores such as performance index (PI) or Security Index (SI) as introduced previously. c) Integrating Critical Clearing Time (CCT) into critical relay rankings.

The current version of *CyPSA-Live* is not applicable for zero-day exploits since the graphs are constructed based on the existing vulnerability information in the National Vulnerability Database (NVD) [51]. However, *CYPRES EMS* is a platform that monitors the cyber-physical system with additional features such as multi-sensor fusion, the Bayesian framework, and DS rules of combination; it hence addresses the zero-day exploit up to certain extent, depending on how and which real-time data features are extracted.

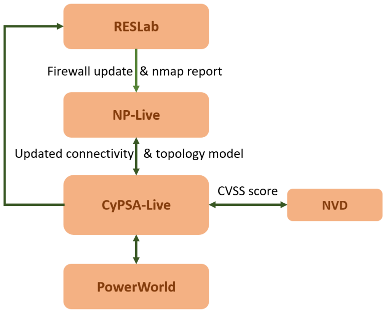
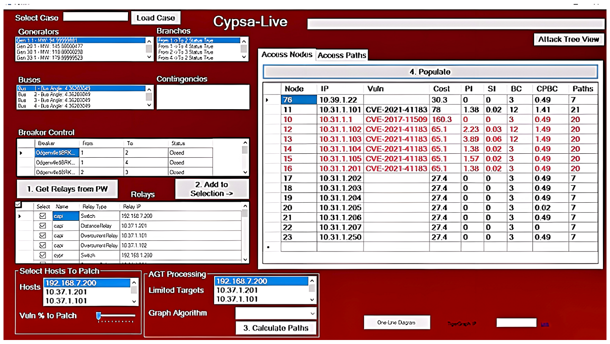


Fig. 11: Framework of *CyPSA-Live*.

Threat scenarios of a false data and command injection attack, using an Address Resolution Protocol (ARP) spoof based Man-in-The-Middle (MiTM) attack in the RESLab testbed [22], as well as communication loss via Denial of Service (DoS) [31], are considered based on the sensor data from different locations in the emulated network. In the scenarios, an adversary has intruded into the communication network, with the capability of falsifying status, measurements, and binary control commands of power components, and flooding traffic to paralyze the communication network.

The *CyPSA-Live* application is presented in Fig. 12. It lists all physical assets such as generators, branches, breakers, and relays. At the right side, there is a table that ranks the critical assets based on metrics such as cyber cost, PI, SI, BC, CPBC and path lengths of the victim nodes from the intrusion points. At the bottom, there is a panel that allows users to patch the vulnerabilities in the compromised nodes, as well as an attack graph template (AGT) processing panel to generate attack tree graphs [50], [52], [53].



Node	IP	Vuln	Cost	PI	SI	BC	CPBC	Paths
76	10.39.1.22		30.3	0	0	3	0.49	7
11	10.31.1.101	CVE-2021-41183	78	1.38	0.02	12	1.41	21
10	10.31.1.1	CVE-2017-11509	160.3	0	0	3	0.49	20
12	10.31.1.102	CVE-2021-41183	65.1	2.23	0.03	12	1.49	20
13	10.31.1.103	CVE-2021-41183	65.1	3.89	0.06	12	1.49	20
14	10.31.1.104	CVE-2021-41183	65.1	1.38	0.02	3	0.49	20
15	10.31.1.105	CVE-2021-41183	65.1	1.57	0.02	3	0.49	20
16	10.31.1.201	CVE-2021-41183	65.1	1.38	0.02	3	0.49	20
17	10.31.1.202		27.4	0	0	3	0.49	7
18	10.31.1.203		27.4	0	0	3	0.49	7
19	10.31.1.204		27.4	0	0	3	0.49	7
20	10.31.1.205		27.4	0	0	3	0.02	7
21	10.31.1.206		27.4	0	0	3	0.49	7
22	10.31.1.207		27.4	0	0	3	0	7
23	10.31.1.250		27.4	0	0	3	0.49	7

Hosts: 192.168.7.200, 10.37.1.201, 10.37.1.101

Limited Targets: 192.168.7.200, 10.37.1.201, 10.37.1.101

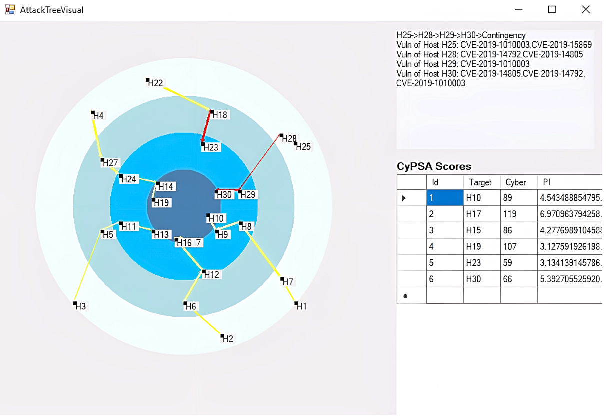
Fig. 12: *CyPSA-Live*: critical asset ranking and other metrics.

The *Attack Tree View* in *CyPSA-Live* shows the intruders' access paths (Fig. 13), which are divided in layers. The outermost layer in the concentric circle represents nodes in the public internet. The next layer represents IT and OT network nodes. The inner circle contains protection devices, such as relays, CTs and PTs. Clicking on a node displays its vulnerabilities, shown as a list in the top right of the *Attack Tree View* window. For instance, the current list shows hosts vulnerabilities beginning at the outermost layer's node $H25$. This host has a web-based vulnerability known as cross-scripting (XSS) obtained from NVD database as CVE-2019-15869, that can propagate to inner hosts $H29$ and $H30$.

VI. Risk Mitigation

CYPRES EMS and *CyPSA-Live* work together to perform situational awareness and risk mitigation. The objective of risk mitigation is to identify the most critical assets in the network.

CyPSA-Live's critical asset ranking, introduced in Section V, assists users to take corrective measures such as



H25->H28->H29->H30->Contingency
Vuln of Host H25: CVE-2019-1010003,CVE-2019-15869
Vuln of Host H28: CVE-2019-14792,CVE-2019-14805
Vuln of Host H29: CVE-2019-1010003
Vuln of Host H30: CVE-2019-14805,CVE-2019-14792,
CVE-2019-1010003

CyPSA Scores

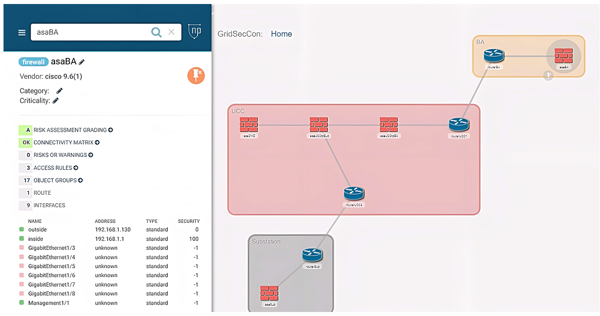
	Id	Target	Cyber	PI
▸	1	H10	89	4.543488854795.
	2	H17	119	6.970963794258.
	3	H15	86	4.277698910458
	4	H19	107	3.127591926198.
	5	H23	59	3.134139145786.
	6	H30	66	5.392705525920.
●				

Fig. 13: Attack tree visualization in *CyPSA-Live*.

installing software patches against vulnerabilities in the hosts (shown in bottom left of Fig. 12), manually operating the relays, or isolating the compromised network.

Based on *CyPSA-Live* asset rankings, we leverage the NP-Live server to define asset criticality and perform stepping-stone analysis:

- Asset criticality: Fig. 14 shows the criticality assignment to the devices, followed by risk assessment grading, and connectivity matrix based on the firewall rules. On the right side of the figure, there are three different criticality zones: one zone for the communication network of a Balancing Authority, another zone for the UCC, and a third zone for the substation network.
- Stepping stone analysis: Fig. 15 shows the stepping stone analysis from the DMZ public network with network ID `172.16.1.32/27` to all reachable networks. These networks are either directly connected, one stepping stone away, or more than two stepping stones away from the DMZ public network. This quantifies risk based on reachability, i.e., if any hosts in the public DMZ, such as the Public_Database or Public_Web_Server, are compromised, then to what extent its neighbors are vulnerable.



asaBA

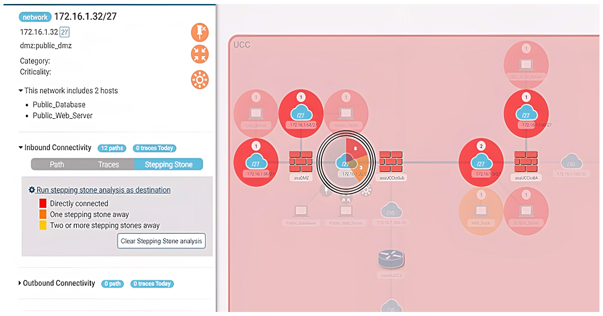
firewall asaBA
Vendor: cisco 9.6(1)
Category:
Criticality:

A RISK ASSESSMENT GRADING
OK CONNECTIVITY MATRIX
0 RISKS OR WARNINGS
3 ACCESS RULES
17 OBJECT GROUPS
1 ROUTE
9 INTERFACES

	NAME	ADDRESS	TYPE	SECURITY
🟩	outside	192.168.1.130	standard	0
🟩	inside	192.168.1.1	standard	100
🟥	GigabitEthernet1/3	unknown	standard	-1
🟥	GigabitEthernet1/4	unknown	standard	-1
🟥	GigabitEthernet1/5	unknown	standard	-1
🟥	GigabitEthernet1/6	unknown	standard	-1
🟥	GigabitEthernet1/7	unknown	standard	-1
🟥	GigabitEthernet1/8	unknown	standard	-1
🟩	Management1/1	unknown	standard	-1

Fig. 14: Device criticality assignment, followed by device-specific summary reports and validating the interfaces.

To complement the asset criticality and stepping-stone analysis, *CYPRES EMS* interacts with the RESLab testbed. The next section shows how this testbed interaction enables inference, tailored based on the high-risk nodes identified in *CyPSA-Live*. They are potential stepping stones for intruders and can reveal vulnerabilities to patch.



network 172.16.1.32/27
172.16.1.32 27
dmz:public_dmz
Category:
Criticality:
This network includes 2 hosts
- Public_Database
- Public_Web_Server

Inbound Connectivity 12 paths 0 traces Today
Path | Traces | Stepping Stone
Run stepping stone analysis as destination
🟥 Directly connected
🟧 One stepping stone away
🟨 Two or more stepping stones away
Clear Stepping Stone analysis

Outbound Connectivity 0 path 0 traces Today

Fig. 15: Stepping-stone analysis of the Public DMZ network within a UCC.

VII. Role in Testbed

The RESLab cyber-physical testbed, shown in Fig. 16, consists of the CORE network emulator, PowerWorld Dynamic Studio (PWDS) as the power system simulator, an OpenDNP3 Master, an RTAC-based master, an intrusion detection system software called Snort, data storage and fusion, and visualization software. A brief overview of some of its components is given in this section while the detailed explanation of RESLab is provided in [22], [31].

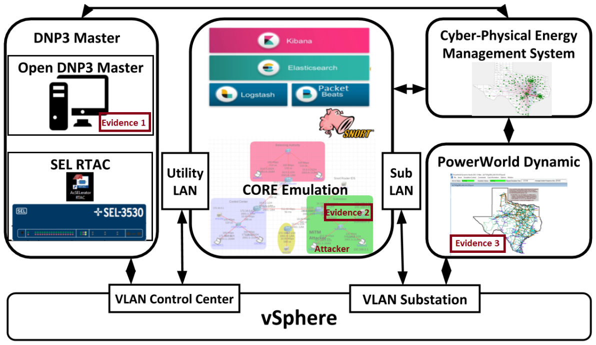
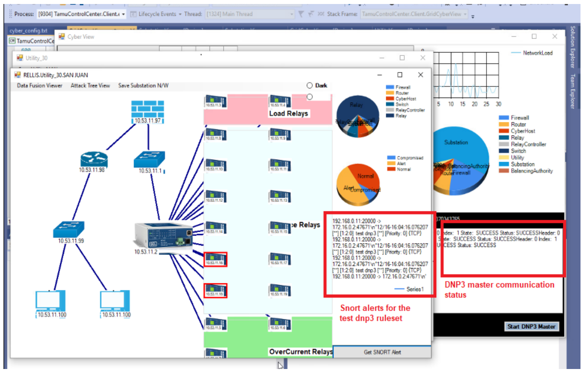


Fig. 16: RESLab emulation testbed architecture showing evidences in three locations: DNP3 Master, *Substation Router*, and PowerWorld DS (PWDS) acting as a DNP3 outstation.

A. *Monitoring Acknowledgement at DNP3 Master*

In the UCC, located on the left side of Fig. 16, the DNP3 Master is controlled via signal from *CYPRES EMS*. The DNP3 Master monitors and controls DNP3 outstations in PWDS, on the right side of Fig. 16. Communication between DNP3 Master and outstations happens through the cyber network emulated in CORE. After the DNP3 Master gets acknowledgment from outstations, it forwards the response to *CYPRES EMS*, which displays this information in the substation view, as in Fig. 17.

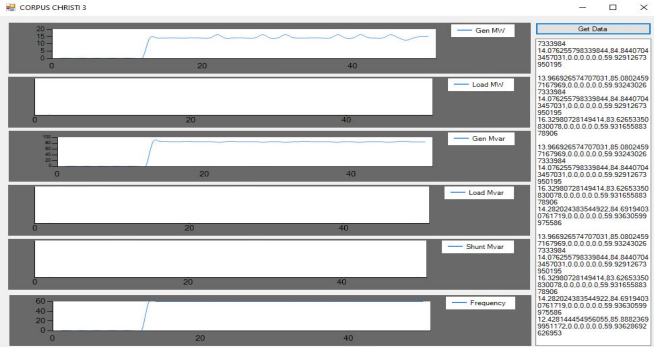
For continuous monitoring of substations' physical data variables, such as net Generation and Load (MW and MVAr), and frequency, PWDS is used, which runs as a background process that acts as a TCP server. It receives queries from *CYPRES EMS*, which acts as a TCP client. The data collected from PWDS is then displayed in *CYPRES EMS*'s substation view (Fig. 18).



```
192.168.0.11:20000 ->
172.16.0.2:47671\n"12/16-16:04:16.076207
[**] [1:2:0] test dnp3 [**] [Priority: 0] {TCP}
192.168.0.11:20000 ->
172.16.0.2:47671\n"12/16-16:04:16.076207
[**] [1:2:0] test dnp3 [**] [Priority: 0] {TCP}
192.168.0.11:20000 ->
172.16.0.2:47671\n"12/16-16:04:16.076207
[**] [1:2:0] test dnp3 [**] [Priority: 0] {TCP}
192.168.0.11:20000 -> 172.16.0.2:47671\n'
```

```
0 Index:  1 State:  SUCCESS Status: SUCCESSHeader: 0
State:  SUCCESS Status: SUCCESSHeader: 0 Index:  1
UCCESS Status: SUCCESS
```

Fig. 17: Receiving Snort alerts from DNP3 master and *Substation Router*.



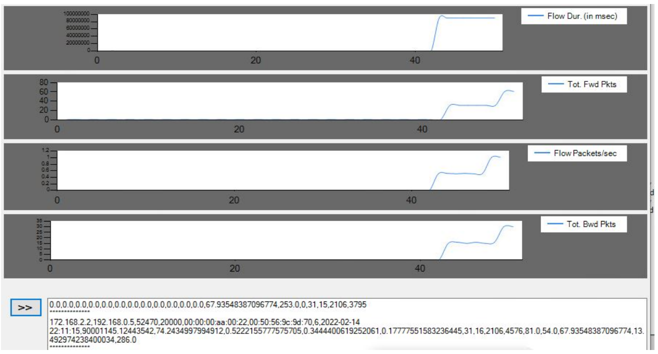
```
7333984
14.076255798339844,84.8440704
3457031,0.0,0.0,0.0,0.0,59.92912673
950195

13.966926574707031,85.0802459
7167969,0.0,0.0,0.0,0.0,59.93243026
7333984
14.076255798339844,84.8440704
3457031,0.0,0.0,0.0,0.0,59.92912673
950195
16.32980728149414,83.62653350
830078,0.0,0.0,0.0,0.0,59.931655883
78906

13.966926574707031,85.0802459
7167969,0.0,0.0,0.0,0.0,59.93243026
7333984
14.076255798339844,84.8440704
3457031,0.0,0.0,0.0,0.0,59.92912673
950195
16.32980728149414,83.62653350
830078,0.0,0.0,0.0,0.0,59.931655883
78906
14.282024383544922,84.6919403
0761719,0.0,0.0,0.0,0.0,59.93630599
975586

13.966926574707031,85.0802459
7167969,0.0,0.0,0.0,0.0,59.93243026
7333984
14.076255798339844,84.8440704
3457031,0.0,0.0,0.0,0.0,59.92912673
950195
16.32980728149414,83.62653350
830078,0.0,0.0,0.0,0.0,59.931655883
78906
14.282024383544922,84.6919403
0761719,0.0,0.0,0.0,0.0,59.93630599
975586
12.428144454956055,85.8882369
9951172,0.0,0.0,0.0,0.0,59.93628692
626953
```

Fig. 18: Real-time generator, shunt, load, and frequency data collected specific to *CORPUS CRISTI 3* substation.



```
0.0,0.0,0.0,0.0,0.0,0.0,0.0,0.0,0.0,0.0,0.0,0.0,0.0,0.0,67.93548387096774,253.0,0,31,15,2106,3795
***************
172.168.2.2,192.168.0.5,52470,20000,00:00:00:aa:00:22,00:50:56:9c:9d:70,6,2022-02-14
22:11:15,90001145.12443542,74.2434997994912,0.5222155777575705,0.3444400619252061,0.17777551583236445,31,16,2106,4576,81.0,54.0,67.93548387096774,13.
492974238400034,286.0
***************
```

Fig. 19: Real-time traffic such as flow duration, number of forward and backward packets per flow collected at the Substation Router at *CORPUS CRISTI 3* substation.

B. Network Telemetry from Substation Nodes

Within the emulated network in CORE, shown in the middle of Fig. 16, the Snort IDS in the *Substation Router* forwards Snort IDS alerts to the respective substation view in *CYPRES EMS*. These alerts are shown in the substation view in Fig. 17.

Similarly, for real-time traffic monitoring within the CORE emulated nodes, *Packetbeat* plug-in in Elasticsearch and *CICFlowmeter* Python package [54] are configured. They forward traffic statistics from each node, such as the *Substation Router*, to the substation view, as the example in Fig. 19.

VIII. Conclusion

CYPRES EMS is a proof-of-concept, next-generation EMS for managing the power system, communication networks, and their security. As a cyber-physical EMS, *CYPRES EMS* allows modeling and data analysis for applications such as situational awareness and cyber threat assessment. Specifically, this paper presents the selected design and methodology decisions based on our research, along with their implementations into automated software tools. The components and functions exemplify how the *CYPRES EMS* would work with utilities' existing networks and be immediately applied.

Future work includes evaluating *CYPRES EMS* for additional cyber attacks such as by adding vulnerabilities to the emulated cyber-physical power system in the RESLab testbed.

IX. Acknowledgement

The work described in this paper was supported by funds from the US Department of Energy under award DE-OE0000895 and the National Science Foundation under Grant 1916142. The authors are grateful for insight and assistance that contributed significantly to the value in theory and implementation of this work: Patrick Wlazlo, Zeyu Mao, Bryan Richardson, Tracy Rolstad, Robin Berthier, Scott Waples, Edmond Rogers, Ben Stirling, Matt Davis, and the rest of the CYPRES team.

References

[1] C.-C. Sun, A. Hahn, and C.-C. Liu, "Cyber security of a power grid: State-of-the-art," *International Journal of Electrical Power & Energy Systems*, vol. 99, pp. 45–56, 2018.

[2] M. Kezunovic and A. Bose, "The future ems design requirements," in *2013 46th Hawaii International Conference on System Sciences*. IEEE, 2013, pp. 2354–2363.

[3] B. Gnerre and G. Cmar, "Defining the next generation enterprise energy management system," in *Web Based Energy Information and Control Systems:*. River Publishers, 2021, pp. 403–434.

[4] S. Aman, Y. Simmhan, and V. K. Prasanna, "Energy management systems: state of the art and emerging trends," *IEEE Communications Magazine*, vol. 51, no. 1, pp. 114–119, 2013.

[5] F. Luo, J. Zhao, Z. Y. Dong, Y. Chen, Y. Xu, X. Zhang, and K. P. Wong, "Cloud-based information infrastructure for next-generation power grid: Conception, architecture, and applications," *IEEE Transactions on Smart Grid*, vol. 7, no. 4, pp. 1896–1912, 2015.

[6] S. Howell, Y. Rezgui, J.-L. Hippolyte, B. Jayan, and H. Li, "Towards the next generation of smart grids: Semantic and holonic multi-agent management of distributed energy resources," *Renewable and Sustainable Energy Reviews*, vol. 77, pp. 193–214, 2017.

[7] T. Yardley, R. Berthier, D. Nicol, and W. H. Sanders, "Smart grid protocol testing through cyber-physical testbeds," in *2013 IEEE PES Innovative Smart Grid Technologies Conference (ISGT)*, Feb 2013, pp. 1–6.

[8] S. Singh, Q. Z. Sheng, E. Benkhelifa, and J. Lloret, "Guest editorial: Energy management, protocols, and security for the next-generation networks and internet of things," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 5, pp. 3515–3520, 2020.

[9] M. D. Schwartz, J. Mulder, J. Trent, and W. D. Atkins, "Control system devices: Architectures and supply channels overview," *Sandia Report SAND2010-5183, Sandia National Laboratories, Albuquerque, New Mexico*, vol. 102, p. 103, 2010.

[10] A. P. Fournaris, L. P. Fraile, and O. Koufopavlou, "Exploiting hardware vulnerabilities to attack embedded system devices: a survey of potent microarchitectural attacks," *Electronics*, vol. 6, no. 3, p. 52, 2017. [Online]. Available: http://www.mdpi.com/2079-9292/6/3/52

[11] P. Jain and P. Tripathi, "Scada security: a review and enhancement for dnp3 based systems," *CSI transactions on ICT*, vol. 1, no. 4, pp. 301–308, 2013.

[12] K. Stouffer, J. Falco, and K. Scarfone, "Guide to industrial control systems (ICS) security," *NIST special publication*, pp. 800–82, 2011.

[13] U.S. Department of Energy, "21 Steps to Improve Cyber Security of SCADA Networks," www.oe.netl.doe.gov/docs/prepare/21stepsbooklet.pdf, 2002.

[14] P. Derler, E. A. Lee, and A. S. Vincentelli, "Modeling cyber–physical systems," *Proceedings of the IEEE*, vol. 100, no. 1, pp. 13–28, 2012.

[15] E. A. Lee, "Cyber physical systems: Design challenges," in *11th IEEE International Symposium on Object Oriented Real-Time Distributed Computing (ISORC)*. IEEE, 2008, pp. 363–369.

[16] B. Zhang, H. Sun, and W. Wu, "A new generation of ems implemented in chinese electric power control centers," in *2008 IEEE Power and Energy Society General Meeting - Conversion and Delivery of Electrical Energy in the 21st Century*, 2008, pp. 1–3.

[17] P. Kansal and A. Bose, "Smart grid communication requirements for the high voltage power system," in *2011 IEEE Power and Energy Society General Meeting*, 2011, pp. 1–6.

[18] Y. V. Makarov, P. V. Etingov, J. Ma, Z. Huang, and K. Subbarao, "Incorporating uncertainty of wind power generation forecast into power system operation, dispatch, and unit commitment procedures," *IEEE Transactions on Sustainable Energy*, vol. 2, no. 4, pp. 433–442, 2011.

[19] E. Targett. (2020, March) High Voltage Attack: EU's Power Grid Organisation Hit by Hackers. [Online]. Available: https://www.cbronline.com/news/eu-power-grid-organisation-hacked

[20] D. U. Case, "Analysis of the cyber attack on the ukrainian power grid," *Electricity Information Sharing and Analysis Center (E-ISAC)*, vol. 388, 2016.

[21] R. Langner, "Stuxnet: Dissecting a cyberwarfare weapon," *IEEE Security & Privacy*, vol. 9, no. 3, pp. 49–51, 2011.

[22] P. Wlazlo, A. Sahu, Z. Mao, H. Huang, A. Goulart, K. Davis, and S. Zonouz, "Man-in-the-middle attacks and defence in a power system cyber-physical testbed," *IET Cyber-Physical Systems: Theory & Applications*, vol. 6, no. 3, pp. 164–177, 2021.

[23] P. Wlazlo, K. Price, C. Veloz, A. Sahu, H. Huang, A. Goulart, K. Davis, and S. Zounouz, "A cyber topology model for the texas 2000 synthetic electric power grid," in *2019 Principles, Systems and Applications of IP Telecommunications (IPTComm)*, 2019, pp. 1–8.

[24] N. Gaudet, A. Sahu, A. E. Goulart, E. Rogers, and K. Davis, "Firewall configuration and path analysis for smartgrid networks," in *2020 IEEE International Workshop Technical Committee on Communications Quality and Reliability (CQR)*, 2020, pp. 1–6.

[25] H. Huang, P. Wlazlo, Z. Mao, A. Sahu, K. Davis, A. Goulart, S. Zonouz, and C. M. Davis, "Cyberattack defense with cyber-physical alert and control logic in industrial controllers," *IEEE Transactions on Industry Applications*, vol. 58, no. 5, pp. 5921–5934, 2022.

[26] A. Sahu, Z. Mao, P. Wlazlo, H. Huang, K. Davis, A. Goulart, and S. Zonouz, "Multi-source multi-domain data fusion for cyberattack detection in power systems," *IEEE Access*, vol. 9, pp. 119 118–119 138, 2021.

[27] A. Sahu and K. Davis, "Inter-domain fusion for enhanced intrusion detection in power systems: An evidence theoretic and meta-heuristic approach," *Sensors*, vol. 22, no. 6, p. 2100, 2022.

[28] Y. Sheffi, *The Power of Resilience : How the Best Companies Manage the Unexpected*. Cambridge, Massachusetts: The MIT Press, 2015.

[29] A. B. Birchfield, T. Xu, K. M. Gegner, K. S. Shetye, and T. J. Overbye, "Grid structural characteristics as validation criteria for synthetic networks," *IEEE Transactions on Power Systems*, vol. 32, no. 4, pp. 3258–3265, 2017.

[30] N. Gaudet, A. Sahu, A. E. Goulart, E. Rogers, and K. Davis, "Firewall configuration and path analysis for smartgrid networks," in *2020 IEEE International Workshop Technical Committee on Communications Quality and Reliability (CQR)*. IEEE, 2020, pp. 1–6.

[31] A. Sahu, P. Wlazlo, Z. Mao, H. Huang, A. Goulart, K. Davis, and S. Zonouz, "Design and evaluation of a cyber-physical testbed for improving attack resilience of power systems," *IET Cyber-Physical Systems: Theory & Applications*.

[32] "Generic distance relay model for the western electricity coordinating council," Western Electricity Coordinating Council, Tech. Rep., 2013.

[33] H. Huang and K. Davis, "Power system equipment cyber-physical risk assessment based on architecture and critical clearing time," in *2018 IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids (SmartGridComm)*. IEEE, 2018, pp. 1–6.

[34] G. Clarke, D. Reynders, and E. Wright, *Practical modern SCADA protocols: DNP3, 60870.5 and related systems*. Newnes, 2004.

[35] H. Huang, C. M. Davis, and K. R. Davis, "Real-time power system simulation with hardware devices through dnp3 in cyber-physical testbed," in *2021 IEEE Texas Power and Energy Conference (TPEC)*. IEEE, 2021, pp. 1–6.

[36] F. Shariatzadeh, C. B. Vellaithurai, S. S. Biswas, R. Zamora, and A. K. Srivastava, "Real-time implementation of intelligent reconfiguration algorithm for microgrid," *IEEE Transactions on Sustainable Energy*, vol. 5, no. 2, pp. 598–607, 2014.

[37] J. Leonard, R. Hadidi, and J. C. Fox, "Real-time modeling of multi-level megawatt class power converters for hardware-in-the-loop testing," in *2015 International Symposium on Smart Electric Distribution Systems and Technologies (EDST)*. IEEE, 2015, pp. 566–571.

[38] D. Watson, T. Chakraborty, and M. Rodgers, "The need for scada communication in a wind r&d park," *Sustainable Energy Technologies and Assessments*, vol. 11, pp. 65–70, 2015.

[39] D. Watson, C. Hastie, and M. Rodgers, "Comparing different regulation offerings from a battery in a wind r&d park," *IEEE Transactions on Power Systems*, vol. 33, no. 3, pp. 2331–2338, 2017.

[40] I. A. Oyewumi, A. A. Jillepalli, P. Richardson, M. Ashrafuzzaman, B. K. Johnson, Y. Chakhchoukh, M. A. Haney, F. T. Sheldon, and D. C. de Leon, "Isaac: The idaho cps smart grid cybersecurity testbed," in *2019 IEEE Texas Power and Energy Conference (TPEC)*. IEEE, 2019, pp. 1–6.

[41] H. Albunashee, C. Farnell, A. Suchanek, K. Haulmark, R. McCann, J. Di, and A. Mantooth, "A testbed for detecting false data injection attacks in systems with distributed energy resources," *IEEE Journal of Emerging and Selected Topics in Power Electronics*, 2019.

[42] T. Becejac, C. Eppinger, A. Ashok, U. Agrawal, and J. O'Brien, "Prime: a real-time cyber-physical systems testbed: from wide-area monitoring, protection, and control prototyping to operator training and beyond," *IET Cyber-Physical Systems: Theory & Applications*, vol. 5, no. 2, pp. 186–195, 2020.

[43] "Deep Cyber Physical Situational Awareness for Energy Systems: A Secure Foundation for Next-Generation Energy Management Cybersecurity," 2022. [Online]. Available: https://cypres.engr.tamu.edu/

[44] Y. Li, J. Chen, and L. Feng, "Dealing with uncertainty: A survey of theories and practices," *IEEE Transactions on Knowledge and Data Engineering*, vol. 25, no. 11, pp. 2463–2482, 2013.

[45] A. Sahu and K. Davis, "Structural learning techniques for bayesian attack graphs in cyber physical power systems," in *2021 IEEE Texas Power and Energy Conference (TPEC)*, 2021, pp. 1–6.

[46] A. Sahu, H. Huang, K. Davis, and S. Zonouz, "A framework for cyber-physical model creation and evaluation," in *2019 20th International Conference on Intelligent System Application to Power Systems (ISAP)*, 2019, pp. 1–8.

[47] G. A. Weaver, K. Davis, C. M. Davis, E. J. Rogers, R. B. Bobba, S. Zonouz, R. Berthier, P. W. Sauer, and D. M. Nicol, "Cyber-physical models for power grid security analysis: 8-substation case," in *2016 IEEE International Conference on Smart Grid Communications (SmartGridComm)*. IEEE, 2016, pp. 140–146.

[48] "NP-Live." [Online]. Available: https://www.network-perception.com/np-live/

[49] "Nessus : A security vulnerability scanning tool." [Online]. Available: https://www.cs.cmu.edu/~dwendlan/personal/nessus.html

[50] A. Umunnakwe, A. Sahu, M. R. Narimani, K. Davis, and S. Zonouz, "Cyber-physical component ranking for risk sensitivity analysis using betweenness centrality," *IET Cyber-Physical Systems: Theory & Applications*, vol. 6, no. 3, pp. 139–150, 2021.

[51] "National vulnerability database." [Online]. Available: https://nvd.nist.gov/

[52] K. R. Davis, C. M. Davis, S. A. Zonouz, R. B. Bobba, R. Berthier, L. Garcia, and P. W. Sauer, "A cyber-physical modeling and assessment framework for power grid infrastructures," *IEEE Transactions on Smart Grid*, vol. 6, no. 5, pp. 2464–2475, 2015.

[53] K. Davis, R. Berthier, S. Zonouz, G. Weaver, R. Bobba, E. Rogers, P. Sauer, and D. Nicol, "Cyber-physical security assessment (cypsa) for electric power systems," *IEEE-HKN: THE BRIDGE*, 2016.

[54] A. Habibi Lashkari, "Cicflowmeter-v4.0 (formerly known as iscxflowmeter) is a network traffic bi-flow generator and analyser for anomaly detection. https://github.com/iscx/cicflowmeter," 08 2018.