A Cyber-Physical Modeling and Assessment Framework for Power Grid Infrastructures

Katherine R. Davis, *Member, IEEE*, Charles M. Davis, *Member, IEEE*, Saman A. Zonouz, *Member, IEEE*, Rakesh B. Bobba, *Member, IEEE*, Robin Berthier, Luis Garcia, and Peter W. Sauer, *Fellow, IEEE*

***Abstract*—The integration of cyber communications and control systems into the power grid infrastructure is widespread and has a profound impact on the operation, reliability, and efficiency of the grid. Cyber technologies allow for efficient management of the power system, but they may contain vulnerabilities that need to be managed. One important possible consequence is the introduction of cyber-induced or cyber-enabled disruptions of physical components. In this paper, we propose an online framework for assessing the operational reliability impacts due to threats to the cyber infrastructure. This framework is an important step towards addressing the critical challenge of understanding and analyzing complex cyber-physical systems at scale.**

I. Introduction

Underlying the electric grid's day-to-day operations and functionality is a vast network of cyber infrastructure composed of layers of computers and communications systems. In some ways, this cyber infrastructure is an unseen backbone of power system operations. Intelligent devices deployed on lines and in substations provide critical services like relaying and system protection through real-time fault detection and clearing. Measurements from sensors in the field as well as commands from power system operators in a control room are relayed over communication networks. The cyber infrastructure touches almost every part of the modern power system.

Power system engineers run thousands upon thousands of studies to understand the behavior of the grid as well as its ability to deal with constantly changing conditions, such as unpredictable outages. Reliability standards in the U.S. require that the bulk electric system be operated in a state that can tolerate any credible contingency, commonly referred to as the $N-1$ reliability criterion. Similar criteria are used in other parts of the world. Typically, the contingencies considered are the loss of electric network components, such as transmission lines, generators, and transformers. Except in special cases, such as transmission lines that share a right-of-way, outages are treated as independent events.

The information, data, or work presented herein was funded in part by the Advanced Research Projects Agency-Energy (ARPA-E), U.S. Department of Energy, under Award Number DE-AR0000342.

K. Davis and C. Davis are with PowerWorld Corporation {kate, matt}@powerworld.com. S. Zonouz and L. Garcia are with Rutgers University {saman.zonouz, l.garcia}@rutgers.edu. R. Bobba is with Oregon State University {rakesh.bobba}@oregonstate.edu. R. Berthier and P. Sauer are with the University of Illinois at Urbana Champaign {rgb, psauer}@illinois.edu.

Part of this work was undertaken while S. Zonouz and L. Garcia were at the University of Miami and R. Bobba was at the University of Illinois Urbana-Champaign.

The grid's cyber infrastructure is not currently subjected to the intense analysis of its electrical counterparts. Analysis is not yet done to understand the impact a cyber outage or compromise might have on the physical system. Intentional cyber attacks and common-mode vulnerabilities break the assumption that contingencies are independent events. If a type of cyber device has a known vulnerability, then a compromise could lead to failures in multiple locations, related only by the use of that device. Multiple outages caused by common vulnerable devices are more probable than the same outages as independent events.

In this paper, we propose a cyber-physical modeling and assessment (CPMA) framework to model the dependencies between the cyber and physical systems and to identify weak points in the system in an online manner. The cyber-physical model captures both the physical power system and the cyber systems connected to it. The cyber-physical threat model captures threats against this infrastructure. The online cyber-physical security analysis algorithm computes security risk metrics considering both cyber and physical power components. It is important to note that this framework is meant to be complementary to security mechanisms in place to protect against attacks and not a substitute. Further, security protections are not infallible and often organizations have to work within the constraints of limited resources for security. The risk analysis enabled by this framework can help prioritize the placement of security controls to better manage risks and improve reliability of the infrastructure.

Our contributions are in, i) identifying what information, and at what level of abstraction, needs to be captured in the cyber-physical model to contribute to a meaningful analysis; ii) defining a cyber-physical threat model that takes into account cyber-physical dependencies and knowledge about known vulnerabilities while accommodating unknown threats and vulnerabilities; iii) defining a cyber-physical modeling framework that take into account both cyber and physical aspects the infrastructure; and iv) developing scalable analysis algorithms for evaluating the system's operational reliability.

II. Framework

The concept of **operational reliability** (formerly called **system security**) and **operating states** were introduced decades ago to indicate the condition of a power system [1]. The operating states are illustrated in Figure 1. The **normal state** is often described as a condition where all equality constraints are met, i.e., all equipment and loads are in service, and all

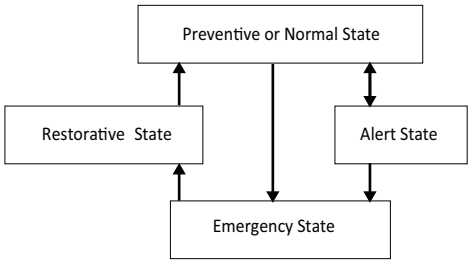


Figure 1. Power system operating states [1] [2]

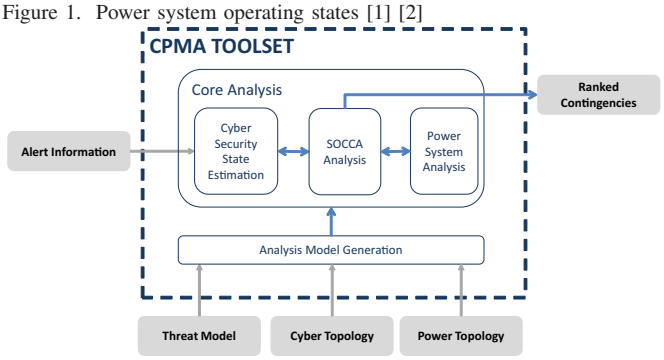


Figure 2. Functional overview of CPMA system integration

inequality constraints are met, i.e., all equipment are within limits. The **alert state** is the condition when one or more inequality or equality constraint would be violated under the occurrence of a credible contingency, such as the loss of a line, transformer, or generator. This alert state is considered "insecure" in an operational reliability sense. The operator is usually required to make dispatch or network changes to eliminate this potential violation.

The **emergency state** is the condition when one or more equality or inequality constraints are violated in real time. This is an insecure state from which emergency action must be promptly taken to move the system into the **restorative state** and then the normal state. The restorative state is a time of transition from having violations in real time (such as bad voltages, line overloads, or load not being served) to having all constraints satisfied. This concept was extended in [2] to include the **in-extremis state** as the state that included the transition from emergency to normal. The goal of CPMA is to extend those concepts of operational reliability to include cyber aspects.

The CPMA framework improves grid operational reliability and security through tools for stakeholders to evaluate and rank their system's most critical cyber-physical threats. The toolset for CPMA can be divided into several functional blocks, as illustrated in Figure 2. Each block is responsible for a combination of specialized data handling capabilities, algorithms, and interfaces to establish the core functionality. We list below the inputs required by CPMA:

Cyber topology. The control network, to the extent that it affects the operational reliability of the grid, is the focus of our effort. This network is geographically distributed and encompasses both control center networks and substation networks. Cyber topology modeling is discussed in Section III.

Power topology. Meaningful cyber-physical analysis requires working with the full topology representation of the system, since this is the level where cyber-physical interactions occur. Signals are mapped to devices in the full topology model. Cyber-physical modeling is also discussed in Section III.

Threat model. In order to design and develop cyber-physical analysis tools, it is critical to understand and capture the relevent cyber-physical threats. A cyber vulnerability can compound an electrical system weakness. Cyber induced circuit breaker actions, particularly line outages, are our main focus. Threat modeling is discussed in Section IV.

We now outline the functional blocks of the toolset. There are four primary functions: model generation, cyber security state estimation, power systems analysis, and security-oriented cyber-aware contingency analysis (SOCCA). During online operation, this analysis is run periodically to update the results as the state of both the cyber and power networks change.

Model generation. The model generation step incorporates topology and threat model information and creates a state space representation that is used in subsequent analysis (see Section V). It is done once at the beginning and again when needed based on changes to the system or threat information.

Cyber security state estimation. Detection is an indivisible component of situational awareness. CPMA supports the correlation of data from intrusion detection systems (IDSs) specifically designed to find malicious activities in power grid infrastructures. In an online mode, this function uses the generated analysis model and available alerts to estimate the security state of the system (see Sections V and VI).

Power system analysis. Power system topology and the available power system state are used to compute the impact of contingencies such as line outages induced through cyber-attacks (see Section VI) .

Contingency analysis. SOCCA uses information about the current security state of the cyber system, the threat model, the cyber topology, and the interdependencies between the cyber and the physical systems to assess and rank contingencies potentially induced by a cyber adversary. This analysis is based on [3] (see Section VI).

CPMA can be carried out offline in a planning mode, using a steady-state snapshot of both the cyber and power systems. As the system evolves, CPMA is designed to take into account alerts from monitoring systems and to estimate the security state online. Contingency ranking is thus updated during real-time operations to take prevailing conditions into account.

III. Cyber-Physical Power Infrastructure Model

Cyber-physical topology models of the power infrastructure allow CPMA to determine the most important cyber-induced contingencies as well as perform analysis of their impact. While physical connections are traceable, non-physical dependencies can be much more hidden. We develop our models using object-oriented principles, allowing new information to easily be added as it is known.

A. Power System Model

The power system model describes the configuration and electrical characteristics of the components. The topology

describes how components are connected, while the state refers to the voltage and angle values of the electric power system at a particular instance in time. The model often represents a best guess of what the future will hold or an estimation of the current power system conditions. In an online sense, approximately every 3-5 minutes, a state estimator fits measured data to a power system model to obtain a best guess of the current conditions [4]. The state estimator model can then be used for studies to determine the impact of outages on the present system state. This process is called real-time contingency analysis.

Figure 3 shows a full breaker-level topology diagram, as would be used in a state estimator. Even in a simple model like the one shown in Figure 3, multiple breakers may be involved in isolating a line from the rest of the system. For example, since breaker a1, a2, and b1 are open, Line A is open.

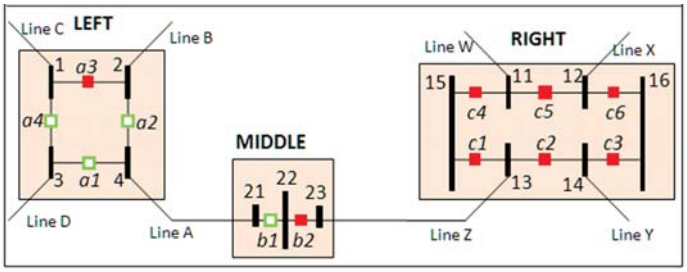


Figure 3. Line status determination from breaker status

Measurements from the SCADA system map to devices in the full topology model. PowerWorld implements a feature called integrated topology processing (ITP) [5] for the purpose of working with full topology models. ITP performs model consolidation only internally as needed to prevent numerical instability. Most EMS systems have a feature to export the full topology model data in a text file format, which can be easily interpreted.

B. Cyber System Model

The cyber system model describes the connectivity and interactions among cyber nodes, as well as existing security mechanisms that can restrict communication between connected hosts. Routers and firewalls determine which hosts on a network are able to communicate, and the cyber system model must represent this logical level. Building and managing cyber network models is a challenging process for an organization. Automated tools can help; the CPMA framework makes use of Network Perception's NP-View software [6], which builds a logical network model by parsing firewall rule-sets.

Figure 4 shows side-by-side views of a sample cyber-physical model in both NP-View [6] (left) and PowerWorld Simulator (right) [7]. The cyber topology shown captures the connections to the substation RTUs allowed by the firewall rules, but it does not capture details in the protection schemes at the substation level.

There is currently no universal format to exchange cyber topologies, yet it is necessary for the future of cyber-physical modeling that we can easily store and accept information in a well-defined, easy to handle format. The CPTL language [8] being developed at the University of Illinois is our candidate for developing models for this framework. CPTL explicitly captures the cyber model information and its connections with the power model. These cyber-physical interconnections are critical to the analysis.

IV. Cyber-Physical Threat Model

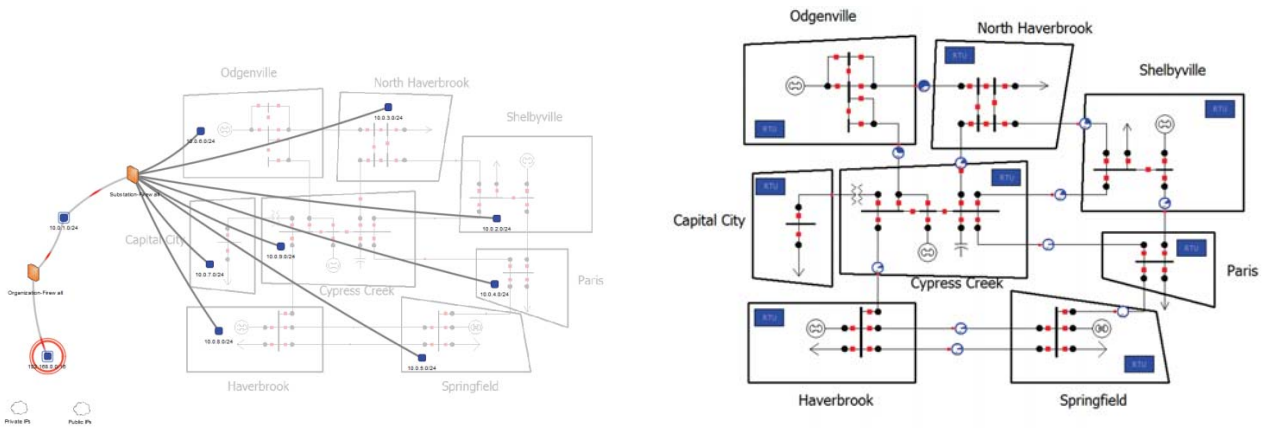
Threat modeling is a structured way of representing threats against a system and is often an integral part of risk assessment or risk modeling for a system. In a cyber-physical system, along with threats to confidentiality, integrity, and availability of data, applications, and other cyber assets, it is also important to i) take into account the threats to integrity, availability, and safety of the physical system, and ii) to understand the interdependence between threats.

A sample attack vector. Here we describe a sample cyber-originated multi-step attack vector that adversely impacts the underlying physical power system, with the potential to cause a catastrophic failure, e.g., an outage or brownout. The attackers are initially assumed to reside outside the power grid control center network. We do not consider physical attacks, e.g., breaking into the control center building. The attackers must penetrate the control center network through cyber vulnerability exploitations. However, not all of the control center computers are accessible from outside due to typical strict firewall rule settings. Often, publicly or semi-publicly accessible computers do exist, e.g., corporate web servers and third-pary access points, that could be hacked into if their software contains vulnerabilities, e.g., buffer overflow. Once such accessible computers are compromised, the adversaries can use those systems as a stepping stone to further penetrate into other accessible systems in the network and get closer to control network and eventually to the power system field devices, e.g., a high voltage transmission relay. Ultimately, an attacker may succeed in penetrating into a computer that controls a relay, and trip the associated line. Such a line trip would cause power flow redistribution over the adjacent transmission lines and potentially lead to line overflows that induce cascading line trips. This could result in the system entering an emergency state.

Attack trees. Attack trees [9] and related attack graphs [10] are a useful way to capture threats against a system. An attack tree is a representation of potential attacks, with the goal of the attack at the root of the tree and the steps to achieve the attack as leaf nodes. In this work, we use attack trees as a primary way to capture our cyber-physical threat model with respect to power system contingencies. In particular, we focus on cyber-intrusions that could lead to line contingencies.

Figure 5 shows a high-level attack tree for line outages. This is modeled after National Electric Sector Cybersecurity Organization Resource (NESCOR) Technical Working Group 1's (TWG1) draft document[1] that presents failure scenarios for the grid with a preliminary impact analysis. As shown in the figure, line outages could be caused by, but not limited to, i) a compromised relay sending unauthorized open commands or a relay acting on compromised settings, or ii) false command

[1] http://www.smartgrid.epri.com/doc/NESCOR_10_25_12.pdf



(a) Cyber Control Network

(b) Power System

Figure 4. Side-by-side views of a sample cyber-physical model as seen in NP-View and in PowerWorld Simulator

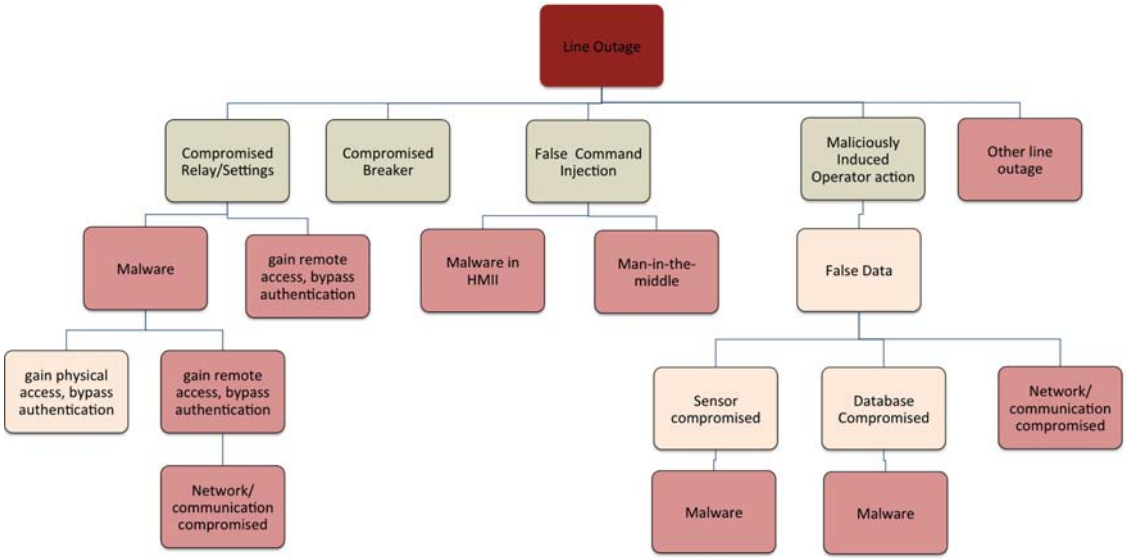


Figure 5. High-level attack tree for line outage

injection (including changing relay settings) by a compromised operator HMI or on a compromised communication link between HMI and relay, or iii) a line open command sent by an operator who was misled by false sensor data, or iv) protection systems kicking in after other potentially maliciously induced line outages, or v) a compromised breaker. The light red color box indicates that a tree below is omitted for brevity. For example, the "Malware" box under "Sensor Compromised" has the same subtree as the "Malware" box under "Compromised Relay or Settings". The number of possibilities and actual feasible attack paths depend on the specifics of the infrastructure such as its components and its vulnerabilities.

Vulnerabilities. There are several sources that provide information on currently known vulnerabilities in existing power grid control and monitoring applications. Industrial control systems cyber emergency response team (ICS-CERT) is one such source. It is a collaborative effort to share control system related security incidents and mitigation measures [11]. The National Vulnerability Database that concentrates on computer vulnerabilities is another source [12]. There are several frequent and easy-to-fix vulnerabilities that appear often in cyber-physical control and monitoring devices such as hard-coded unique passwords across many identical devices [13], weak passwords breakable by brute-force [14], and traditional buffer-overflows [15] since most such firmware are coded using loosely-typed programming languages.

Scalability. In a large infrastructure there are likely to be a large number of known vulnerabilities. However, it is important to account for vulnerabilities that are actually exploitable and focus only on those attacks paths that can emerge from such exploitation. While it may not be hard to manually come up with attack avenues at a high-level, exploring these avenues at any depth could be a intensive manual effort. An automated way of generating attack trees or graphs for a given infrastructure based on high-level attack tree templates that are created manually would be ideal and would be a good topic for future work. Right now this has to be done manually. One way to keep this tractable is to aggregate multiple vulnerabilities into a probability value indicating how easy or hard it is to transition from one node in the topology representing the infrastructure to another node along an attack path. Probability values can be computed based on the "difficulty" (of exploiting) rating that is included in ICS-CERT advisories. For example, an easy to exploit

vulnerability may be translated to a high transition probability value (say 0.75), where as a hard to exploit vulnerability may be translated to a low transition probability value (say 0.25). Limiting the scope of the threat model to line outages also helps reduce the complexity.

Industry effort. It is encouraging to note that North American Electric Reliability Corporation's (NERC) Critical Infrastructure Protection (CIP) Working Group chartered a task force to develop, maintain, and analyze attack trees for the electric infrastructure. This task force is looking at cyber-physical attacks. Our framework could leverage such industry developed attack trees to power our analysis.

V. Model Generation

Modeling cyber-physical infrastructures concisely is challenging. Accurate hybrid automata models can impact scalability significantly, and traditional discrete modeling techniques do not consider the physical components. Instead, CPMA makes use of an extended discrete state-based model, i.e. a partially observable Markov decision processes (POMDP), that captures sufficient information about the physical system for analyses without causing practical scalability issues. The POMDP enables CPMA to model the underlying cyber-physical infrastructure and estimate its current probabilistic state considering uncertainties in sensor measurements.

Every cyber-physical attack path consists of an escalating series of vulnerability exploitations by the adversary. Initially, the adversary does not have access to the network, but eventually achieves the privilege required to reach his or her attack goals, e.g., causing a power transmission line outage by opening a relay. States in the POMDP capture only the necessary information about the system for our later contingency analyses. Each state is represented as a bit vector where each bit indicates the secure or compromised status of a computing device, e.g., a control center host. Therefore, the initial state is $\varnothing$, in which the attacker does not yet have any privileges over the smart grid network. Each adversarial state transition represents a privilege escalation which is achieved through a vulnerability exploitation. Therefore, any path on the POMDP graph represents an attack path in the power network.

More specifically, each security attack is in a finite set of security states S that cover all of the system's possible security conditions. The system is in one of the security states s at each time instant. From the system's current state, the attacker chooses and takes a malicious action $a \in A$ admissible in s, *i.e.,* an exploitation that is feasible, which leads to a transition to s'. At each transition, the attacker may receive a reward according to a specific reward function for that type of attacker, e.g., a hacker seeking financial gain. The reward function value is the amount of his or her interest in the corresponding state.

Formally, a discrete Markovian decision process Γ is defined as a tuple $(S, A, R(.), P, \gamma)$ where S is the security state space, endowed with the discrete topology. At every time point, the system state is represented as a probability distribution over the state space due to the false positive/negative rates of the IDS alerts. A is the set of adversarial actions. At every $s \in S$, $A(s) \subset A$ is the set of admissible actions. The measurable function $R : S \rightarrow [0, 1]$ is the adversary-driven reward function calculated for each state based on the power system performance index value in that state [16]. For example, if a relay is connected to a circuit breaker, and that relay is compromised, we assume the consequence is measured by the severity of the electrical system impact caused by opening that breaker. The reward is also a function of *ease of attack*, i.e., how easy the target vulnerability is to exploit. P denotes the transition probability function; that is, if the present state of the system is s, taking an action a results in a state transition to state s' with probability $P(s'|s, a)$. γ is the discount factor and is normalized, i.e., $0 < \gamma < 1$.

The smart grid network's access control policies, such as firewall rulesets, are composed of rules about sources (IP and port addresses) that are either allowed or not allowed to reach a destination. CPMA parses the rulesets and creates a binary network connectivity matrix that is a Cartesian product of host systems. The $[i, j]$ entry of the matrix takes on a true value if traffic from host h_i to host h_j is allowed, and a false value if it is not allowed. The connectivity matrix always includes an Internet node representing a group of hosts outside of the network, where attackers are assumed to initially reside. CPMA generates a comprehensive POMDP model of the smart grid network that represents all *possible* attack paths. The generated POMDP by design address all system vulnerabilities and could partilly account for previously unknown exploitations by having a small probability of transition even on paths where no known vulnerabilities exist.

Generation of Markov decision processes (attack graphs) based on the automated extraction and analysis of network firewall rules ensures comprehensive coverage of possible attack paths. Based on the firewall rules, our tools pessimistically consider all the computers that are accessible from a particular host system to be vulnerable, and hence compromisable, by the adversaries. Consequently, the generated attack graphs incorporate every feasible single or multi-step attack vector through the control center network that could potentially cause a physical power system consequence, e.g., a malicious circuit breaker trip.

VI. Cyber-Physical Security Analysis

The core cyber-physical security analysis algorithm used in the proposed framework builds on top of SOCCA [3] which is an *offline* power grid analysis tool. However, for this work on *online* security state estimation and cyber-physical contingency analysis, we use the POMDP that captures potential paths an adversary could take through a network to cause cyber-physical events that we call contingencies. The partial observability is a crucial feature, as during the online analysis, it is infeasible to exactly determine the current state of the system, given the noise and false positive/negative rates of the power and cyber security sensor reports.

Starting from the POMDP's initial state $\varnothing$, an adversary could then reach a state where it is possible to send a command resulting in a physical consequence. As discussed above, the reward to the adversary of taking action a from state s is

$R(s,a)$. The reward function is the following,

$$R(b,a) = \sum_{s\in S} b(s) \cdot \sum_{s'\in S} P(s'|s,a)[\Delta F(s,s') + I(s')] \quad (1)$$

where b is the current *belief* state of the system, i.e., a probability distribution over the state space of POMDP. Clearly at each time instance, we have $\sum_{s\in S} b(s) = 1$. $F(s)$ is a performance index defined in each state. The performance index is computed using the following equation, which measures the severity of a transmission line outage based on the subsequent line overload(s):

$$F(s) = \sum_{l\in L} \big[\max\{\frac{f_s(l)}{f^{MAX}(l)} - 1, 0\}\big]^2. \quad (2)$$

Here, L is the set of all lines, $f_s(l)$ denotes flow on line l in state s, and $f^{MAX}(l)$ denotes the maximum flow allowed on line l.

The POMDP's value function for each state is the cyber-physical security index $I(s)$, which is evaluated by solving the following dynamic programming equation:

$$I(s) = \max_{a\in A(s)} \{\gamma \cdot R(s,a)\}, \quad (3)$$

The level of fitness to an adversary of a cyber attack step is represented by the transition probability $P(s'|s,a)$ and the physical impact $\Delta F(s,s') = F(s') - F(s)$.

To evaluate the attack severity in each state, the framework deploys a full power system simulation. We evaluate the effect of each reachable switching action (a breaker opening) and solve the AC power flow equations using the iterative Newton-Raphson algorithm to calculate the line flows. This impact is incorporated into the severity metric in each POMDP state as in Equation 2. Note that modeling variations are possible for the power systems analysis. The appropriate method depends on the needs of the utility and the purpose of the analysis. For example, an approximate DC model may be used, requiring only a non-iterative linear solution, but sacrificing accuracy [17].

It is noteworthy that it is also possible to expand this framework by extending the capabilities of the individual components. For example, modeling a lighting strike that affects power lines as well as communications lines could be done if the power system model is able to simulate electromagnetic transients and the cyber system model contains the physical connections of the communications lines. Also, it is possible to use this framework to evaluate the transient stability of the system due to a cyber compromise by adapting the modeling techniques. While this is beyond the scope of our present work, the framework is extensible to other cyber-physical analysis applications.

A. Result Interpretation

Our framework explores and analyzes potential cyber-physical contingencies according to the current probabilistic cyber-physical state estimate and provides a risk-based ranked list. In particular, for a scalable state space exploration, we make use of the maximum likelihood approximation algorithm, and first pick the state with the highest estimation probability according to the sensor measurements, i.e., $s^* = \arg\max_{s\in S} b(s)$. The analysis results are represented using a three-value tuple for each state (ID, F, I). The first value is an identifier. This identifier corresponds to the specific set of hosts and devices that have been compromised in that state. The second number is the performance index $F(s^*)$, i.e. the immediate physical consequence of being in that state. The performance index is only non-zero for states that are connected to a device such as a relay that is capable of performing a physical action such as opening a breaker. The third number is the security index $I(s^*)$, recursively evaluated for each state. In interpreting the results, the security index represents the best choice from an adversarial perspective. For example, in the below highly simplified POMDP of Figure 6, one can trace the graph by following the greatest values of $I(s^*)$ and determine the three most critical cyber-physical attack paths or contingencies. These are tabulated in Table I.

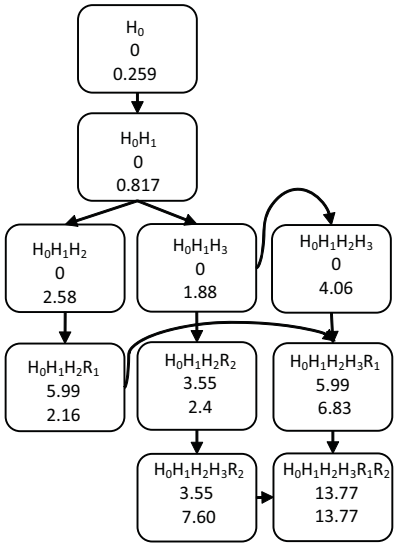


Figure 6. Sample state space graph

Table I
RANKED CRITICAL PATHS

Path 1					
Step	$H_0 \to H_1$	$H_1 \to H_2$	$H_2 \to R_1$		
I(s)	0.817	2.58	2.16		
Path 2					
Step	$H_0 \to H_1$	$H_1 \to H_3$	$H_3 \to R_2$		
I(s)	0.817	1.88	2.4		
Path 3					
Step	$H_0 \to H_1$	$H_1 \to H_3$	$H_1 \to H_2$	$H_2 \to R_1$	$H_3 \to R_2$
I(s)	0.817	1.88	4.06	6.83	13.77

Figure 7 shows these analysis results for a sample system. The first path leads to the most critical line outage for the system in three steps. The second path leads to the second most critical, also in three steps. The third most critical path is the most interesting as it is also the most complex. Here, the adversary's path leads into the control center first, but the adversary does *not* yet open the breaker, which by itself would cause the second most severe contingency. Then, the adversary backtracks and follows steps leading to opening a line in the Haverbrook substation, causing the most severe single contingency. After that, the adversary proceeds to cause

a double line outage and subsequent overloads approximately doubling in severity by taking out the second line, at the control center. He or she could have been dormant waiting for the Haverbrook outage and then knew that would be the most effective time to take out the line in the control center. This example shows how complex attacks can be identified, where these attacks potentially involve more than one action with a physical consequence. Our security analysis thus pinpoints weaknesses in the cyber infrastructure, that through compromise, can lead the system to be in an emergency state, from an operational reliability standpoint. Notice that the highest ranked critical paths share several of the same elements and steps. Thus, targeting protection efforts to the identified common elements can have a system-wide benefit.

It is reasonable to assume that such a double line outage would not normally be considered in a utility's standard planning procedures, as the lines are not geographically close or otherwise coupled. While standard contingency selection methods may miss these contingencies, our framework predicts and flags them for further consideration.

B. Real-World CPMA Stakeholders

Given that the CPMA toolset undertakes cyber-physical analysis and spans both the cyber and power sides of the system, its corresponding stakeholders would be a combination of personnel from the operational technology and information technology divisions of a utility. Support engineers may be responsible for configuration and validation of the toolset while the operational personnel may be responsible for ongoing monitoring and response. Support engineers include both network engineers and SCADA/control engineers. Similarly, operators include both control room operators and network operations center (NOC) staff. To make CPMA accessible to the wide variety of roles, the analysis process is automated so that the end-users will ultimately see only the results applicable for their practical usage and do not have to manually sift through unnecessary low-level details of the system.

Engaging these stakeholders is crucial for us to verify and validate the CPMA toolset. We are presently working with several advisory members including utilities to ensure that our efforts target and solve real-world problems. Part of this effort involves the evaluation of CPMA in a real utility system, which will be reported in future work.

VII. Implementation

This CPMA system is comprised of modules that distribute the work along logical lines and support the implementation of the contingency analysis algorithms as a real-world tool. The functions described have been implemented in real software. While this framework uses information about the current state of the system, it does not interfere with or introduce delays into real-time data streams from sensors or command stream from operators.

A. Core Analysis Overview

The core analysis and model generation blocks of Figure 2 are implemented in a modified version of Zabbix [18], [19]. Zabbix is a commonly used open source monitoring software package for enterprise networks which can be used to monitor the performance and availability of hosts and network hardware within a network. For our implementation, the Zabbix code has been modified to manage the entire CPMA system, including the data input and output, as well as the functional blocks. One of the components Zabbix manages is an interface to the power systems analysis block of Figure 2, carried out by a modified version of PowerWorld [7].

In CPMA, Zabbix acts as a server and performs the initial contingency analysis based on both the input model as well as the performance indices retrieved from PowerWorld. The input model for the contingency analysis is generated using the NP-View tool, which performs a comprehensive security analysis of the access policy rules and produces the network connectivity matrix according to the control network topology [3]. Zabbix is also configured to respond to detected failures (e.g., a network intrusion or failure of a critical process on a monitored agent) by triggering the analysis to be updated. During the normal course of operation, this includes updating the security state by asking the power system analysis block to calculate a new security index for the predicted next most likely outages. Thus, Zabbix keeps track of the current POMDP state of the system and updates the PowerWorld interface accordingly.

Updating the security state requires knowledge about the location of the host in the network, what other hosts are reachable from the compromised hosts, what vulnerabilities exist on those hosts, and the physical impacts of the compromised hosts on the power system. To that end, CPMA uses a threat model, power system physical model and simulation capability, a cyber network topology model along with the inter-host accessibilities according to the global firewall rulesets, as well as the cyber physical mapping that contains the points of cyber-physical interconnection. The network model allows us to see where in the network misbehaving host is located. The cyber-physical mapping lets us evaluate the potential physical consequences using the power system analysis software. The threat model enables CPMA to assign transition probabilities between the security states.

The time scales at which information must be exchanged determine what data transmission methods are appropriate. Our CPMA implementations use sockets for fast and frequent data exchange and files for less frequent data exchange. The power system side is frequently being asked to gauge the impact of a contingency, so the communications must be relatively fast. Thus, the Zabbix-PowerWorld communication uses network sockets. The threat model, power system model, and cyber network model are parsed from files.

The standard PowerWorld Simulator software package has been heavily modified to allow it to accept and send data over a TCP socket. The original use of this feature was for an operator training simulator [20], where multiple operators interact with the same case. The modifications for the present application allow the software to 1) accept a case sent from a server, 2) accept commands to change data in the model, and 3) return data about the model to the server.

The protocol implementation follows the sequence outlined

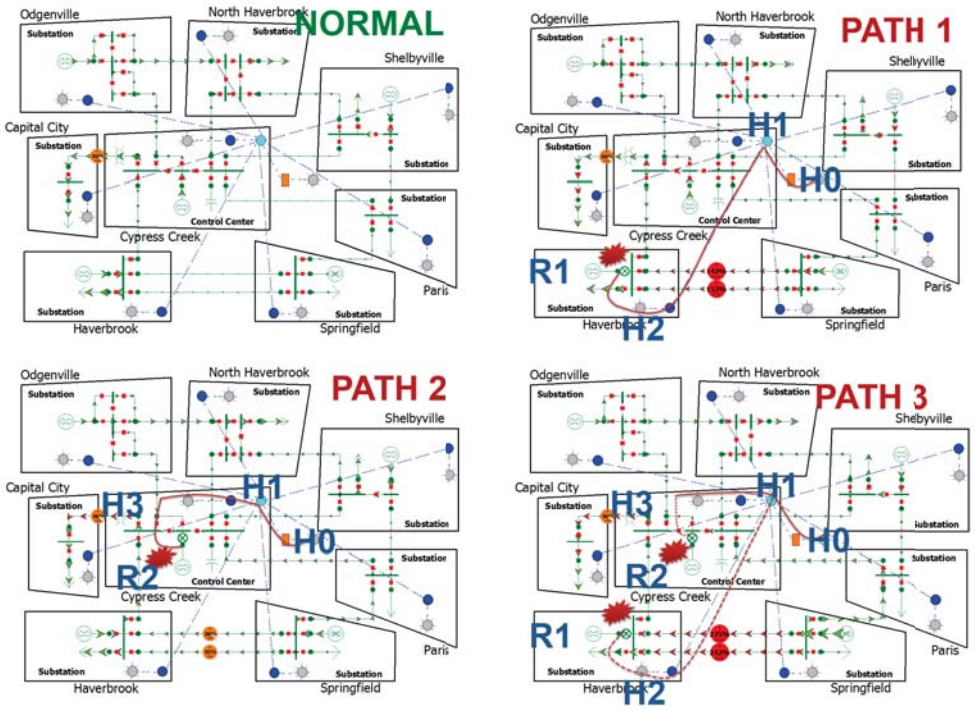


Figure 7. Cyber-originated threats: ranked critical paths for double line outage example

in Fig. 8. Zabbix acts as the server, listening for connections. The modified PowerWorld code connects to the listening Zabbix process and waits for commands. The connection is maintained throughout the process. Once connected, PowerWorld will receive, interpret, and reply to the Zabbix commands. Zabbix is able to formulate the commands and interpret PowerWorld's responses. The payload of a sockets message contains data that is required for the command to be successfully executed. It can be as large as the power system case file, or it may simply be an identifier of a field and a value to retrieve.

PowerWorld and Zabbix must communicate using exactly the same message protocol and data formats. The payload is a byte stream, and PowerWorld and Zabbix must both know how to interpret it. The framework can be adapted to be used with other security event management systems and to integrate with other energy management systems. The Zabbix and PowerWorld implementation presented here provides just one practical example. There are many monitoring and event management systems in use including ArcSight, Synamtec, and Splunk. Similarly, utilities use a variety of energy management systems including those by Alstom, ABB, and OSI. In theory, one could realize a CPMA framework using any combination of the commonly used event manager and energy management systems.

B. Server and Client Messages

A prefix is attached to Zabbix-PowerWorld messages to identify the sending host. Messages sent from the server begin with **tsm**, while those from the client begin with **tcm**. The relevant messages that allow us to implement the client-server communication are described below. The Zabbix process is the server, and PowerWorld is the client.

- **tsmSendCase.** The server sends a message that includes a new power system model.
- **tsmSetData.** The server tells the client to set the specified fields to the specified values for the specified objects. The PowerWorld client will set the specified fields and automatically solve the power flow upon receipt of the message.
- **tsmGetClientState.** The server requests the present values of the specified fields for the specified objects in the case from the client. The PowerWorld client retrieves the values of the specified fields and returns them using a tcmSendData command.
- **tcmSendData.** The client sends specific information about the system back to the server in response to a tsmGetClientState command.

C. Zabbix-PowerWorld Communication Protocol

The communications are illustrated in Fig. 8, starting with the initial connection. Once the connection is established, it is kept open. When a case is ready for analysis, it is sent to the PowerWorld client, where it is immediately opened and placed in memory. The program below shows the code to send the case. This command is sent at the start of the analysis and periodically as new state estimates become available.

Program 1 Example of sending new case

```
SendFile( std::string("case.pwb"), tsmSendCase,
     true, connectedList[c]->socket());
```

Then, CPMA uses tsmGetClientState and tcmSendData to retrieve data for all of the lines in the case. It is critical for

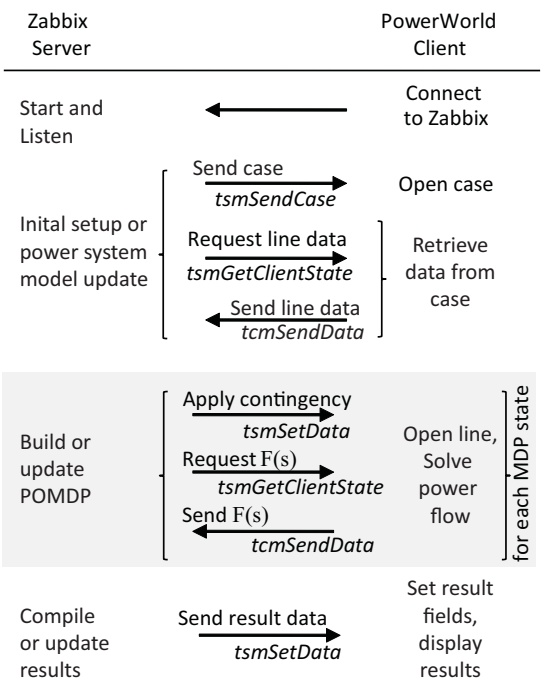


Figure 8. Zabbix-PowerWorld communication

Zabbix to know the correct labels or names of the lines in order to manage cyber-power interconnections as well as line outages. The program below shows the code to open one of the lines, identified by its label.

Program 2 Example of sending command to open line

```
objectID = "BRANCH 'Capital City$BRK$4647'";
FieldID  = "LineStatus";
Value    = "Open";
SendSetDataMessage(tsmSetData, connectedList
     [c]->socket(), ObjectID, FieldID, Value);
```

Program 3 Example of getting performance index

```
objIDs.add("PWCaseInformation");
fldIDs.add("OverloadRank");
SendGetData(tsmGetClientState, true,
     connectedList[c]->socket(), objIDs,
     fldIDs, 1 );
```

During the contingency analysis, the Zabbix server will be sending requests to the PowerWorld Client to evaluate the effects of an outage in order to populate the security states. This is shown as "Build or update POMDP" in Fig. 8. The commands are used to apply an outage and request the security metric.

The program above shows the code that returns the performance index that is used to evaluate the severity of potential outages. This command is sent by the Zabbix server.

The tsmSetData command can also be used for visualization purposes. There are several custom fields in the PowerWorld client that allow users to specify data stored with the objects in the model. For example, a custom floating point field can be used to store post-contingency flows with each line. Setting these fields in conjunction with utilizing other built-in features of PowerWorld allows users to create customized one-line diagrams and results displays.

VIII. Related Work

Over the last few years, design and analysis of cyber-physical systems have received considerable attention in the research community. There has been a lot of work proposing to model and analyze cyber-physical systems in general and in power grids specifically. We review works closely related to our approach and discuss their merits.

In [21], an early paper on the topic, Lee discussed design challenges for cyber-physical systems and argued that existing abstractions and modeling techniques are inadequate for cyber-physical system design. Specifically, he contended that while there are modeling solutions for discrete cyber networks as well as continuous physical plants, the current tools do not sufficiently account for the cyber-physical interconnections and more accurate algorithms and tools are needed in the field. Derler et al. [22] discussed the challenges in modeling cyber-physical platforms. In particular, the authors named intrinsic heterogeneity, concurrency, and sensitivity to timing as the challenging factors. More specific to energy, Ilic *et al.,* [23] proposed cyber-physical models of generation and load components and their interconnection through the electrical network. Their work was focused on load modeling and did not consider the cyber network. Palensky *et al.,* [24] discussed the challenges associated with continuous-time and discrete-time cyber-physical models of energy systems and compared the scalability of these two approaches.

Security and reliability of the cyber-physical energy infrastructures has also received considerable attention (*e.g.,* [25], [26], [27], [28], [3]). A switched systems view of the power grid is used by both [26], [27]. Liu *et al.,* [26] used it to model coordinated cyber-physical attacks, while Dominguez-Garcia [27] used it for reliability modeling. Challenges facing secure control and survivability of cyber-physical systems were discussed in [25]. They suggest as missing an ability to estimate the state of the cyber network along with the state of the physical system and an ability to use that information in improving the physical system's performance. In [28], Zonouz *et al.,* proposed a framework that leverages estimates of security state of the cyber infrastructure to improve electrical system state estimation. In [29], [30], security-oriented techniques for effective steady state cyber-physical abstraction using stochastic control algorithms are introduced. They also discussed how such models could be used for automated decision-making for optimal response actions against adversaries who target safety-critical infrastructures. However, [29], [30] concentrated mostly on the computational assets and did not consider power system dynamics in details in their analyses. This work builds upon cyber-physical power systems analysis by using a POMDP to improve the analysis of cyber-induced contingencies by including an estimate of the security state. Chen *et al.,* [31], proposed a workflow based security assessment framework and demonstrated its use using the case

of Advanced Metering Infrastructure. Their work is limited to the assessment of the cyber-infrastructure and does not take the electrical infrastructure into account. However, their work can be leveraged to improve the scalability of our threat modeling and can be complementary to our framework.

IX. Conclusion

Reliability of the electric grid is tied to the dependability and security of the component systems and parts on which it relies. Presently, the cyber infrastructure and the impact of any failures or compromises in the cyber system are hidden from the power system operators and planners.

This paper extends power system operational reliability assessment with a security-oriented framework for online use with energy management and security event management systems. The proposed CPMA framework captures the possible interactions of cyber networks with physical networks, beginning with a cyber-physical model. This model maps the points of interconnection between the cyber and physical systems, allowing CPMA to determine what physical actions are possible from any given host in the cyber network. Using power system models, cyber system models, threat models, real-time alert information, and the SOCCA algorithm, the CPMA framework implementation provides a way to manage the input data, preform the security-driven operational reliability analysis, and present the results in a meaningful way.

CPMA makes available meaningful data to inform system operators of outages that may be more likely, due to cyber connectivity, than if events were independent. This information also informs system managers of what the most vulnerable portions of their systems are and what paths are most critical to protect.

References

[1] T. Liacco, "The adaptive reliability control system," *IEEE Transactions on Power Apparatus and Systems*, vol. PAS-86, no. 5, pp. 517–531, May 1967.

[2] L. Fink and K. Carlsen, "Power/energy: Operating under stress and strain: This, part two of the blackout series, defines control objectives for various levels and types of emergencies," *IEEE Spectrum*, vol. 15, no. 3, pp. 48–53, March 1978.

[3] S. Zonouz, C. Davis, K. Davis, R. Berthier, R. Bobba, and W. Sanders, "SOCCA: A security-oriented cyber-physical contingency analysis in power infrastructures," *IEEE Transactions on Smart Grid*, vol. 5, no. 1, pp. 3–13, 2014.

[4] A. Monticelli, *State Estimation in Electric Power Systems: A Generalized Approach*. Kluwer Academic Publishers, 1999.

[5] S. Grijalva and A. Roy, "Automated handling of arbitrary switching device topologies in planning contingency analysis: Towards temporal interoperability in network security assessment," *IEEE Transactions on Power Systems*, vol. 28, no. 2, pp. 1523–1530, 2013.

[6] Network Perception. (2014) NP-View. [Online]. Available: www.network-perception.com

[7] PowerWorld Corp. (2005) PowerWorld Simulator. [Online]. Available: www.powerworld.com

[8] G. A. Weaver, C. Cheh, E. J. Rogers, W. H. Sanders, and D. Gammel, "Toward a cyber-physical topology language: Applications to NERC CIP audit," in *Proceedings of the First ACM Workshop on Smart Energy Grid Security (SEGS '13)*. New York, NY, USA: ACM, 2013, pp. 93–104.

[9] B. Schneier, "Attack trees: Modeling security threats," *Dr. Dobb's Journal*, 1999.

[10] R. Lippman and K. Ingols, "An annotated review of past papers on attack graphs. an annotated review of past papers on attack graphs. an annotated review of past papers on attack graphs." MIT Lincoln Laboratory, Project Report PR-IA-1, March 2005.

[11] ICS-CERT Monitor. [Online]. Available: http://ics-cert.us-cert.gov/monitors

[12] National Vulnerability Database. [Online]. Available: http://nvd.nist.gov/

[13] Medical Devices Hard-Coded Passwords. [Online]. Available: http://ics-cert.us-cert.gov/alerts/ICS-ALERT-13-164-01

[14] Offline Brute-Force Password Tool Targeting Siemens S7. [Online]. Available: http://ics-cert.us-cert.gov/alerts/ICS-ALERT-13-016-02

[15] Sielco Sistemi Winlog Multiple Vulnerabilities. [Online]. Available: http://ics-cert.us-cert.gov/alerts/ICS-ALERT-12-179-01

[16] H.-D. Chiang and R. Jean-Jumeau, "Toward a practical performance index for predicting voltage collapse in electric power systems," *IEEE Transactions on Power Systems*, vol. 10, no. 2, pp. 584–592, 1995.

[17] B. Stott, J. Jardim, and O. Alsac, "DC power flow revisited," *IEEE Transactions on Power Systems*, vol. 24, no. 3, pp. 1290–1300, 2009.

[18] ZABBIX SIA. (2014) Zabbix: The enterprise-class monitoring solution for everyone. [Online]. Available: http://www.zabbix.com/

[19] ——. (2014) Zabbix manual. [Online]. Available: https://www.zabbix.com/documentation/2.2/manual

[20] PowerWorld Corp. (2014) PowerWorld Trainer. [Online]. Available: http://www.powerworld.com/products/trainer/overview

[21] 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.

[22] 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.

[23] M. Ilic, L. Xie, U. Khan, and J. Moura, "Modeling future cyber-physical energy systems," in *Power and Energy Society General Meeting - Conversion and Delivery of Electrical Energy in the 21st Century, 2008 IEEE*, July 2008, pp. 1–9.

[24] P. Palensky, E. Widl, and A. Elsheikh, "Simulating cyber-physical energy systems: Challenges, tools and methods," *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, vol. 44, no. 3, pp. 318–326, March 2014.

[25] A. Cardenas, S. Amin, and S. Sastry, "Secure control: Towards survivable cyber-physical systems," in *28th International Conference on Distributed Computing Systems Workshops, 2008. ICDCS '08.*, June 2008, pp. 495–500.

[26] S. Liu, X. Feng, D. Kundur, T. Zourntos, and K. Butler-Purry, "Switched system models for coordinated cyber-physical attack construction and simulation," in *IEEE First International Workshop on Smart Grid Modeling and Simulation*, 2011, pp. 49–54.

[27] A. Dominguez-Garcia, "Reliability modeling of cyber-physical electric power systems: A system-theoretic framework," in *Power and Energy Society General Meeting, 2012 IEEE*, July 2012, pp. 1–5.

[28] S. Zonouz, K. Rogers, R. Berthier, R. Bobba, W. Sanders, and T. Overbye, "SCPSE: Security-oriented cyber-physical state estimation for power grid critical infrastructures," *IEEE Transactions on Smart Grid*, vol. 3, no. 4, pp. 1790–1799, 2012.

[29] S. A. Zonouz, H. Khurana, W. H. Sanders, and T. M. Yardley, "RRE: A game-theoretic intrusion response and recovery engine," in *IEEE/IFIP International Conference on Dependable Systems & Networks, 2009. DSN'09.*, 2009, pp. 439–448.

[30] S. Zonouz, A. Houmansadr, and P. Haghani, "EliMet: Security metric elicitation in power grid critical infrastructures by observing system administrators' responsive behavior," in *IEEE/IFIP International Conference on Dependable Systems and Networks, DSN '12*, 2012, pp. 1–12.

[31] B. Chen, Z. Kalbarczyk, D. M. Nicol, W. H. Sanders, R. Tan, W. G. Temple, N. O. Tippenhauer, A. H. Vu, and D. K. Yau, "Go with the flow: Toward workflow-oriented security assessment," in *Proceedings of the 2013 Workshop on New Security Paradigms Workshop (NSPW '13)*. New York, NY, USA: ACM, 2013, pp. 65–76.