# SECPSIM: A Training Simulator for Cyber-Power Infrastructure Security

Ceeman Vellaithurai, Anurag Srivastava, Saman Zonouz*
Electrical Engineering and Computer Science, *Electrical and Computer Engineering
Washington State University, *University of Miami
*ceeman.vellaithurai@wsu.edu, asrivast@eecs.wsu.edu, s.zonouz@miami.edu*

***Abstract*—Trustworthy critical power grid infrastructures require suitable cyber and power security protection efforts. Expert system operators play a crucial role in protecting complex power-grid networks; however, inefficient training of system operators regarding potential cyber attacks and physical security threats can potentially result in malicious compromises and catastrophic consequences. In this paper, we present SECPSIM, a user-friendly framework based on mathematical models of corrective control actions against various intrusions and failure scenarios. Our experimental results show that SECPSIM can help in learning and provide appropriate corrective cyber-physical control actions efficiently, and provide inexperienced individuals with an effective tutorial user interface.**

## I. INTRODUCTION

The bulk electricity delivery system known as the *power grid* is extremely fundamental to most aspects of modern society. Power grid critical infrastructures form a vast and interconnected cyber-physical network for delivering electricity from generation plants to end-point consumers. Due to their importance, power control networks have been a very attractive attack surface for malicious attackers and nation-state terrorists to penetrate in the network and consequently cause catastrophic physical damage. Remote malicious cyber attacks caused approximately $100 million of damage cost in 2009 [1]. The most recent control system malware called Stuxnet [2] was crafted to sabotage nuclear power plants. Stuxnet specifically raised new questions about power grid security protection which is strictly recommended by the government as destruction of those systems would have a debilitating impact on national security.

Currently, to protect power grid critical infrastructures, expert power system operators, sitting in *control network* rooms, monitor and control the cyber network as well as the underlying physical system in order to guarantee secure energy delivery. Traditionally, power grid operators gain their expertise and experience solely through working with an actual operational power grid where a mistake may result in catastrophic consequences such as large-scale cascading failures and power blackouts. Consequently, a better training and experience transferring solution is needed to make sure that inexperienced operators learn about the potential failures and security incidents as well as how to respond to them and take appropriate recovery actions with minimum effort and without any potential damage on the actual operational power grid. Additionally, there needs to be an assessment method to evaluate whether the operator has gained sufficient amount of expertise and hence can handle real-world conditions before he/she is allowed to work on the actual infrastructure.

The Operator Training Simulator (OTS) [3] simulates the electrical network, user interface and power system behavior. The training simulator simulates the power system in a realistic manner by providing static and dynamic responses to the operators actions which are similar to those observed by the operator in a real control center. The OTS has three distinct functional areas; The Power System Model, the Control Center Model and the Instructor Module. It provides a realistic environment for operators to practice operating under normal, emergency or restorative conditions. However, OTS does not simulate the cyber-side of the power grid and mainly concentrates on simulation of the physical power system.

The objective of this paper is to propose SECPSIM, a conceptual integration of a cyber-attack simulator into the existing OTS, to study the difference in operator response to contingencies with/without the consideration of cyber network configuration. SECPSIM provides a complete simulated power grid infrastructure including the control center environment as well as the physical power system. Additionally, SECPSIM is capable of realistic simulation of malicious cyber-physical attacks that originate at remote cyber assets as well as reactive and proactive corrective control actions to fix cyber exploitations and power contingencies. Furthermore, during an interaction with an expert operator, SECPSIM learns appropriate handling of various attack scenarios by creating mathematical behavioral models. Consequently, SECPSIM makes use of those models during an interaction with an inexperienced operator to perform effective knowledge transfer so that inexperienced operators also learn how to handle various attacks appropriately.

In summary, the contributions of this paper are as follows: 1) We propose an integrated cyber-physical solution to model corrective control actions against malicious intrusions against the power-grid and accidental failures; 2) We introduce an integrated cyber-physical power grid simulator that takes into account cyber asset functionalities, power operations and the cyber-physical interactions during adversarial attack scenarios; and 3) We validate the SECPSIM framework on an emulated cyber-physical power grid network infrastructure by implementing a working prototype of the proposed algorithms.

## II. SYSTEM OVERVIEW

The SECPSIM framework consists of several subsystems that achieve its ultimate overall objective cooperatively. SECPSIM's operation consists of two major phases: 1) learning from simulation; and 2) training operators.

During the first phase, SECPSIM is used by expert operators who go through several cyber-physical failure and intrusion scenarios on the SECPSIM's user friendly graphical interface that is backed up with the cyber-physical system and failure simulation engine. During the expert operator interaction. SECPSIM observes his or her reactions, i.e., corrective control actions, in every system state and calculates a mathematical behavioral model that is a game-theoretic Markov decision process with learned numerical parameters, i.e., state security measures. It is noteworthy that the expert operators could be replaced with a scripted list of appropriate

control actions for various system states; such lists are usually composed during the power grid planning efforts in practice nowadays. More specifically, to accelerate the learning model convergence, SECPSIM calculates a rough system model automatically using the power-based impact index. Later on, during the expert operator interaction, the rough values are further refined to represent the expert knowledge precisely.

The second phase of the SECPSIM operation aims at training inexperienced operators to consider both cyber and power networks while selecting the corrective control actions. SECPSIM's ultimate goal is to achieve this objective using a simulated environment without the need for interaction with the actual operational critical infrastructure. In particular, SECPSIM with the learned set of system models and parameters can be downloaded and used simultaneously by several (possibly remote) inexperienced trainees. SECPSIM makes use of its hybrid cyber network and power system simulation engines to emulate realistic attack and failure scenarios for the inexperienced who should observe the situation on their screen and decide upon the optimal control action from the list provided by SECPSIM. In the meanwhile, SECPSIM emulates an expert operator internally by implementing a game-theoretic optimization solution to pick the optimal control action according to the created learned system models. Consequently, SECPSIM compares the sequence of actions provided by each trainee and the calculated optimal action sequence, and verifies whether those two sequence match.

**Cyber-Power System Simulator.** To simulate the underlying power system, SECPSIM uses PowerSimulator[1] that simulates the power system under a wide range of conditions including thermal system overload, voltage collapse, off-nominal frequency, Ferranti voltage rise, system islands, large angle variations and cold load pickup. There are three major versions of the PowerSimulator; Custom, Generic and Replica. For our simulation purposes, we use the Generic PowerSimulator that uses a hypothetical generic power system model called the PALCO system to provide realistic power system experience. The supported roles include transmission operator, balancing authority area operator, reliability coordinator, generator operator, distribution operator and substation operator.

The Event Scenario feature in PowerSimulator allows SECPSIM 1) to create a certain power system situation, e.g., a series of line outages representing a situation which could be a result of a storm. The recorded event scenario can be played in any simulation run to train operators for taking control actions related to that situation during light or heavy load periods; and 2) to observe the operator's reaction, i.e., sequence of corrective actions, to create behavioral models of the expert operators and evaluate the inexperienced trainees.

The mathematical power system simulation in SECPSIM consists of algebraic equations that describe the instantaneous relationship between variables and ordinary differential equations that describe the time varying properties of the variables. Since there are many non-linearities in these equations, they are solved numerically. The algebraic equations are typically solved every one to five seconds. This delay serves to induce the delay in data gathering through SCADA systems that receive data by scanning RTUs at specified intervals of time. The real and reaction power injections represented by algebraic equations is given by [4]:

$$P_i = |V_i|^2 G_{ii} + \sum_{n=1, n\neq i}^{N} |V_i V_n V_{in}| cos(\theta_{in} + \delta_n + \delta_i) \quad (1)$$

[1]Available at http://www.powerdata.com/.

$$Q_i = -|V_i|^2 B_{ii} + \sum_{n=1, n\neq i}^{N} |V_i V_n V_{in}| sin(\theta_{in} + \delta_n + \delta_i) \quad (2)$$

where, $P$ - Real power in pu, $Q$ - Reactive power in pu, $G$ - conductance in pu, $B$ - Susceptance in pu, $V$ - Voltage at a bus in pu, $Y$ Admittance in pu, $\theta$ - Admittance angle and $\delta$ - Bus angle. Here $V$ and $\delta$ are unknown variables that are to be computed. This is done using Newton Raphson (numerical method) by solving the following equation,

$$[J][\frac{\Delta\delta}{\Delta V}] = [\frac{\Delta P}{\Delta Q}] \quad (3)$$

where, $J$ is called the jacobian matrix which is composed of partial derivatives. When there is a change in system state, such as the tripping of a line as a corrective action by an operator or a malicious action by an attacker, the values of the admittance matrix change. The power flow is run using the new values to estimate the new state variables $V$ and $\delta$. A contingency is usually associated with dip in voltage and increase in bus angles at certain buses. During a blackout kind of scenario, rapid dip in bus voltages and increase in bus angles are observed, meaning that the system is starting to pull apart. This is visualized in the control center screen of SECPSIM.

SECPSIM modifies the OMNET++ [5] framework to simulate the cyber network of the power grid, the corrective countermeasure actions as well as adversarial intrusions. The simulation includes intra-host network stack simulation and the inter-host communication protocols. Individual packets are simulated and RTT's are exactly emulated. The transferred messages among the hosts include both legitimate messages as well as the malicious exploits that compromise the target host systems stochastically to emulate the success or failure of a compromise attempt by the attackers.

## III. BEHAVIORAL MODEL CREATION AND LEARNING

To create a behavioral model of how each operator handles various cyber-physical intrusion scenarios, SECPSIM uses the inverse reinforcement learning-based parameter estimation [6]. We first discuss how SECPSIM models rational attackers and defenders (responders) in a power-grid infrastructure using a game-theoretic Markov decision process, and then discuss the interactive parameter estimation algorithm in details.

**Attacker vs. Responder Interaction.** We describe how SECPSIM models the attacker-vs.-defender interaction, i.e., the selection procedures of corrective response and malicious exploitation actions by the operator and the attacker, respectively. SECPSIM uses this model to infer security measure values which the operator's response strategies and the attacker's attack tactics are based on.

SECPSIM solves a competitive Markov decision process (CMDP) to find the optimal action which maximizes the expected accumulative long-run reward measure received after a sequence of response and adversarial actions. Formally, A CMDP $\Gamma$ is defined as a tuple $(S, A, Sec(.), P, \gamma)$ where $S$ is the security state space, assumed to be the set of compromised cyber or power nodes. $A$ is the set of actions, which itself is partitioned into response actions and adversarial actions depending on the player. For every $s \in S$, $A(s) \subset A$ is the set of admissible actions at state $s$. The measurable function $Sec : S \rightarrow [0,1]$ is the security measure calculated for each state, and $P$ is the transition probability function; that is, if the present state of the system is $s \in S$ and an action $a \in A(s)$ is taken, resulting in state transition to state $s'$ with probability $P(s'|s,a)$, an immediate reward $Sec(s')$, i.e., security measure value of the state $s'$, is obtained by the player taking the action. $\gamma$ is the discount factor and is normalized, i.e., $0 < \gamma < 1$.

Using the *infinite-horizon discounted cost* technique, SECPSIM gives more weight to nearer future rewards by recursively adding up the immediate reward, i.e., security measure value $Sec : S \rightarrow [0,1]$ that represents how secure the system is in each state, and the discounted expected game value from then on. SECPSIM computes the optimal policy $\pi^*$ that associates with any state $s \in S$ an optimal action $\pi^*(s)$. SECPSIM formulates the response/adversarial action selection procedure as a game-theoretic *maximin/minimax* problem[2]. Every policy $\pi$ is assigned a value function $V_\pi$ that associates every belief state $s \in S$ with an expected global reward $V_\pi(s)$ obtained by applying $\pi$ in $s$. Bellman's optimality equation (Equation (4)) characterizes the unique optimal value function $V^*$, from which an optimal policy $\pi^*$ can be easily derived:

$$V^*(s) = Sec(s) + \sqrt{\gamma} \cdot \max_{a_r \in A(s)} [\sum_{s' \in S} P(s'|s,a) \cdot \Psi(V^*, s')], \quad (4)$$

where $\Psi$ denotes the value function given that a specific response action is taken:

$$\Psi(V^*, s') = Sec(s') + \sqrt{\gamma} \cdot \min_{a_a \in A(s'_{s,a})} [\sum_{s'' \in S} P(s''|s',a) \cdot V^*(s'')] \quad (5)$$

Briefly, to calculate $V^*$ numerically, SECPSIM uses the value iteration algorithm [7] that applies dynamic programming iterative updates to gradually improve on the value until it converges to the $\varepsilon$-optimal value function [7], i.e. $\mid V_t(b) - V_{t-1}(b) \mid < \varepsilon$. Through improvement of the value, the policy is implicitly improved as well. Once the partially observable decision process is formulated and the $\varepsilon$-optimal value function is calculated, SECPSIM determines the optimal response strategy $\pi^*$ at any given belief state using:

$$\pi^*(b) = \arg\max_{a_r \in A(b)} \Psi(V^*, b, a_r). \quad (6)$$

Next, we discuss how SECPSIM makes use of the operator's responsive behavior at a subset of states during his or her interaction with SECPSIM's simulation GUI to calculate the security measure values $Sec(.)$. The ultimate goal is to make sure that the automatically calculated optimal policy $\pi^*$ (using the calculated security measure values and the optimal response action selection algorithm discussed above) matches the response strategies taken by the expert operator.

**Security Measure Initialization.** Recall that each state represents a set of compromised cyber and power nodes. Out of the possible power compromises (contingencies), we focus on generator contingencies, and other power node incidents can be considered similarly. To initialize the security metric values, SECPSIM makes use of a graph theoretic algorithm to calculate an impact factor (security measure) for each state $Sec_i : S \rightarrow R$ depending on the underlying power grid topology and the set of compromised power nodes in that state. The states where there is no compromised power node, $Sec_i$ is initialized to 0.

The attacker is assumed to know only the topology information of the power system and hence a graph theory based topology analysis is used to rank contingencies [8]. The power system is modeled as a graph $G(V,E)$, where the buses in the power system are treated as a set of vertices $V$ and branch components as a set of edges $E$. The edges are assigned weights to represent the dissimilarity between the branch components. The weights are based on the reactance $X$, since $X$ is usually greater than resistance $R$ of the branch.

[2]We describe the response action selection procedure here, and one can easily compute the optimal adversarial action similarly.

To determine the most critical generators for a cyber-attack, the concept of vertex centrality is used. Vertex centrality measures assign ranking coefficients to vertices in a graph, from which we can deduce that the most important generators are those located on buses with a high ranked centrality index. Among all vertex centrality indices, evidence of a close relationship between closeness centrality and impact of generator outages has been shown in [8]. The closeness centrality for a $n$ bus system is defined as:

$$C_c(\nu_i) = \frac{\sum_{i \in \nu / i} d(i,j)}{n-1} \quad (7)$$

The above equation relies on the use of shortest path distance $d(i,j)$ between the vertices which is computed using the Dijkstra [9] shortest path algorithm. The closeness centrality index is extended for a $N-X$ case in [10] given by the closeness impact centrality index as:

$$CI_c(V_{cont}) = \sum_{i \in V_{cont}} |C_c(v_i)| \quad (8)$$

where, $V_{cont}$ is the set of generators considered for the $N-X$ case. The security metric value for each CMDP state is initialized as

$$Sec_i(s) = 1 - \frac{CI_c(V_{cont}(s))}{CI_c(V)} \quad (9)$$

where $V$ is the total set of generators, and $V_{cont}(s)$ indicates the set of compromised power nodes, i.e., generator contingencies, in state $s$. Consequently, $Sec_i$ is assigned a real value in $[0,1]$ depending on how critical the generator contingencies in $s$ are. States with higher $Sec_i$ values represent more system security; therefore, the attackers and the defenders takes actions to drive the system towards less and more secure states, respectively.

**Automatic Security Metric Elicitation.** Computation of a security measure function that explains the operator's response policy is essentially an inverse control problem in which $Sec(.)$ is desired given $\pi^*$. SECPSIM employs a game-theoretic inverse reinforcement learning algorithm to consider the operator's policy as evidence, and consequently update the *apriori* security measure values $Sec_i(.)$. Similar to [6], uncertainty of the prior security measure knowledge is modeled using the Laplace density function:

$$P(Sec(s) = r) = \frac{1}{2\sigma} e^{-\frac{|r - Sec_i(s)|}{2\sigma}}, \forall s \in S, \quad (10)$$

where $P(Sec(s) = r)$ denotes the probability that the security measure value for the state $s$ is equal to $r$. As a distribution parameter, $\sigma$ denotes the predefined uncertainty level.

SECPSIM takes the operator's noisy response policy during an attack scenario as well as the above *apriori* knowledge to derive the posterior distribution of the system security measure. In particular, an attack scenario $T$ is represented as a sequence of (state, action) pairs $T = [(s_1,a_1),(s_2,a_2),\cdots,(s_n,a_n)]$ that denotes the system states and the operator's corresponding responses. Due to the Markov property of CMDP, determination of response actions, at each time instant, depends only on the present state. Therefore,

$$P(T|Sec) = P((s_1,a_1)|Sec) \cdot P((s_1,a_1)|Sec) \cdots P((s_n,a_n)|Sec), \quad (11)$$

where $P((s_i,a_i)|Sec)$ denotes the probability that $a_i$ is selected as the optimal policy at state $s_i$ given the security measure function $Sec$. It is important to highlight that the optimal policy value is always unique; however, the above probability distribution encodes the noise in the optimal policy samples due to the operator's expertise level.

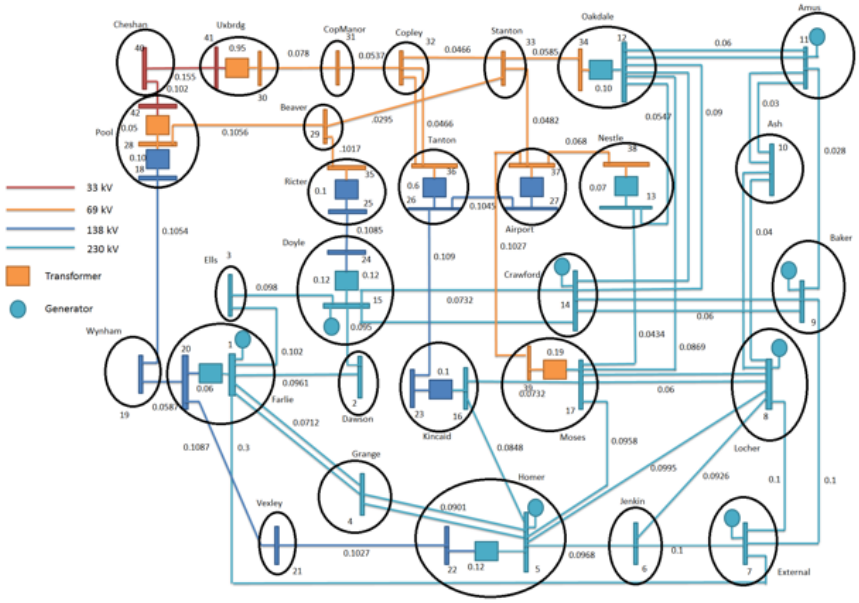



Fig. 1. An Operating Snapshot of a Sample Power System in SECPSIM

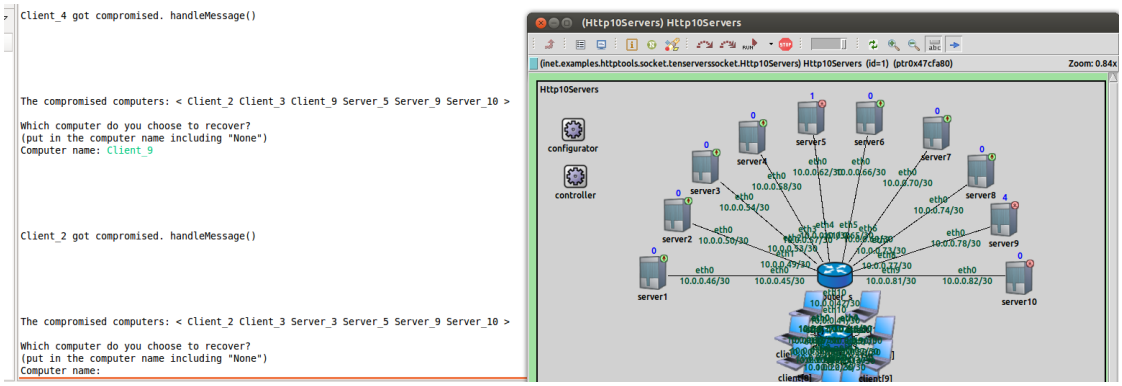



Fig. 2. An Operating Snapshot of SECPSIM with Several Servers Compromised

The optimal policy $\pi^*$ maximizes the $\Psi$ function in Equation (6). Therefore, the larger $\Psi$ is, the more likely it is that the operator would take action $\pi^*(s)$ at state $s$. Additionally, this likelihood increases as we get more confident in the operator's expertise level, i.e., he or she can respond appropriately [6]:

$$P((s,a)|Sec) = \frac{e^{\tau \cdot \Psi(V,s,a)}}{\sum_{a' \in A} e^{\tau \cdot \Psi(V,s,a')}}, \quad (12)$$

where $\tau$ is a non-negative constant, which represents the operator's expertise level. SECPSIM calculates the security measure's posterior distribution using the following equation:

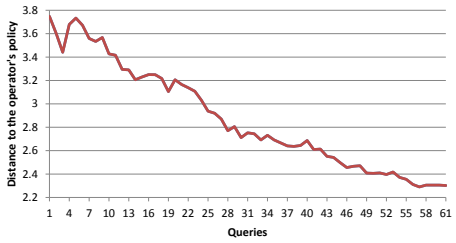
$$P(Sec|T) = \frac{P(T|Sec) \cdot P(Sec)}{P(T)} = \frac{1}{Z} e^{\tau \cdot \sum_{1 \le i \le n} \Psi(V,s_i,a_i)}, \quad (13)$$

which applies the Bayes theorem. $Z$ denotes the normalizing constant, and $n$ is the length of the attack scenario $T$. Consequently, the metric elicitation results in a refined security measure function $Sec$.

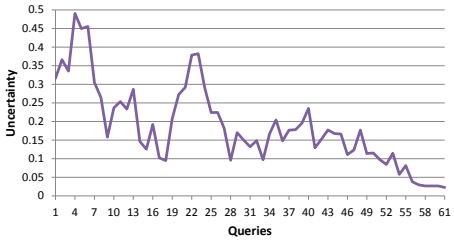
## IV. Simulation Results

**Behavioral Model Creation.** Figure 1 shows our testbed power system topology, and Figure 2 illustrates a simplistic cyber network of the power grid. The operators see such a combined cyber-physical view of the power grid. In the background, SECPSIM simulates both cyber and power networks, and additionally, emulates a multi-step intrusion scenario using the discussed game-theoretic formulation. In case of an attack, SECPSIM provides the operator with a visual and textual detailed information about the attack, and asks for the optimal countermeasure action. During the interaction with an expert operator, SECPSIM uses his/her countermeasure actions to create a behavioral model that is later compared to the action sequence selected by each inexperienced operator. Figure 3(a) shows how the behavioral model creation converges to the optimal policy during the expert operator-vs.-simulator interaction. The horizonal axis represents the number of questions, e.g., in Figure 2, and the vertical axis represents how far the learned model is from the ideal optimal policy. Figure 3(b) shows how the security measure refinement process converges during SECPSIM's interaction with the expert operator. The vertical axis represents the policy uncertainty after every single question. Estimation of the posterior security measure distribution was done using 200 samples, and each query took 7.2 seconds on average to be processed.

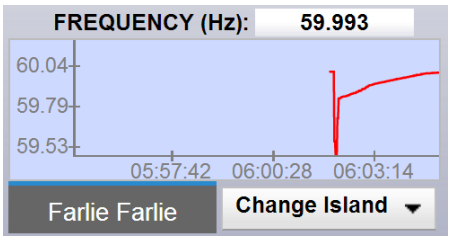
**Evaluation Scenarios.** We evaluate how consideration of both cyber and power network topology in corrective control action selection makes a difference and results in more meaningful countermeasure strategies.



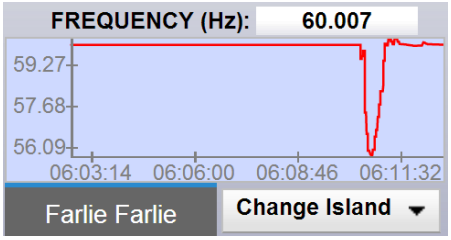

(a) Behavioral Model Generation




(b) Behavioral Model Uncertainty




(c) Frequency response for N-1 Contingency (G8)




(d) Frequency response for N-2 Contingency

Fig. 3. Evaluation Results for SECPSIM

| RANK | $N-1$ Contingencies | | |
|---|---|---|---|
| | GEN | BUS | $C_c$ |
| 1 | G3 | 7 | 0.3136 |
| 2 | G1 | 1 | 0.2926 |
| 3 | G2 | 5 | 0.2648 |
| 4 | G8 | 15 | 0.2645 |
| 5 | G7 | 14 | 0.2468 |
| 6 | G5 | 9 | 0.2465 |
| 7 | G4 | 8 | 0.2320 |
| 8 | G6 | 11 | 0.2287 |

(a) PALCO: N-1 GO CR

| RANK | $N-1$ Contingencies | | |
|---|---|---|---|
| | GEN | BUS | $C_I$ |
| 1 | G8 | 15 | 1 |
| 2 | G4 | 8 | 0.5 |
| 3 | G2 | 5 | 0.16667 |
| 4 | G7 | 14 | 0.125 |
| 5 | G5 | 9 | 0.1 |
| 6 | G3 | 7 | 0.0555 |
| 7 | G6 | 11 | 0.0476 |

(b) N-1 CP CR

| RANK | $N-1$ Contingencies | | |
|---|---|---|---|
| | GEN | BUS | $C_I$ |
| 1 | G8, G4 | 15,8 | 1.5 |
| 2 | G8, G2 | 15,5 | 0.1667 |
| 3 | G8, G7 | 15,14 | 1.125 |
| 4 | G8, G5 | 15,9 | 0.1 |
| 5 | G8, G3 | 15,7 | 0.0555 |
| 6 | G8, G6 | 15,11 | 0.0476 |
| 7 | G4, G2 | 8,5 | 0.6667 |

(c) N-2 CP CR

| | |
|---|---|
| 1 | Shed load Locher A, 271 MW |
| 2 | Shed load Amus A and Amus B, 100 MW each |
| 3 | Shed load Grange A, 172 MW |
| 4 | Shed load Ash A and Ash B, 80 MW each |
| 5 | Shed load Extrnl D, 154 MW |
| 6 | Shed load Jenkin, 21 MW |

(d) CA for N-2 CR

Fig. 4. Evaluation Results for SECPSIM (CP: Cyber Physical; CR: Contingency Ranking; CA: Control Action; GO: Generator Outage)

*1) Physical attack contingency ranking based on incomplete information:* Using the graph theory based ranking algorithm for generator contingency, they were ranked for $N-1$ contingency. The results are shown in Table I for the PALCO system in PowerSimulator. It is to be noted here that the algorithm can be used for finding $N-X$ contingencies and not limited to just $N-1$.

*2) Cyber-physical attack vulnerability ranking:* The N-1 contingency ranking based on the combined cyber-physical ranking metric is given in Table 4(b). The top seven N-2 contingencies are ranked and shown in Table 4(c).

*3) Control action for cyber-physical attack without cyber simulator:* We look at how an operator responds to a contingency without a cyber-simulator associated with the operator training module. $N-1$ *Contingency:* From the contingency ranking given in Table 4(b), $G8$ at bus 15 is chosen to be simulated in the PowerSimulator. For this contingency, it was seen that the system voltage, line loadings and frequency are within acceptable limits. Figure 3(c) shows the frequency curve after the contingency. According to North American Electric Reliability Corporation (NERC) document [11], frequency should be restored to at least 58.5 Hertz in ten seconds or less and to at least 59.5 Hertz in thirty seconds or less. It was observed that the frequency dipped to a minimum of 59.47 Hz and recovered quick enough to satisfy this criterion. $N-2$ *Contingency:* From the contingency ranking given in Table 4(c), $G8$ and $G4$ at bus number 15 and 8 are chosen for this scenario. The generation at $G8$ at the time of tripping is 400 MW, and at $G4$ it is 645 MW. The control actions necessary to prevent under frequency and bring it back into acceptable limits within reasonable time frame is given in Table 4(d). Figure 3(d) shows the frequency response of the system for the $N-2$ contingency case with control actions. The total load at the time the contingency occurs is 3160 MW. A total of 978 MW of load is to be shed in order to bring the frequency of the system within acceptable bounds while the other generators in the system start ramping up their generation to satisfy connected load.

*4) Control Action for Cyber-Physical Attack with Cyber Simulator:* The cyber-simulator helps in making the operator aware that the attack on the system has been caused by a cyber-attack and not probably due to a physical malfunction/disturbance/attack. The operator is presented with the option of recovering the cyber assets which have been compromised. In this way, the operator is able to retrieve the essential cyber assets first, and restore the physical power system assets to normal operation thereby reducing the effective downtime of a device. *N-1 Contingency*: It has been seen before that there is no control action required from the operator for the N-1 contingency case as the system is able to deal with such a condition. *N-2 Contingency*: Control action taken by the operator will be very different in presence of cyber simulator as operator is aware that the contingency has occurred due to a cyber-attack which needs to be taken care of as well. The load shedding operations would still be needed as stated in Table 4(d) to keep the system frequency within acceptable bounds. However, since the operator knows the cause of the attack, the time in bringing the generators back online is reduced greatly. $G4$ at bus 8 is the bigger of the two generators which were taken out. The operator would recover the cyber assets associated with this generator and bring it back up online first followed by $G8$.

It is to be noted here that in the absence of the cyber simulator, the operator and repair crew will not be aware of cyber-assets being compromised. Even if operators restore the physical system, the attacker will take out generators easily again. In such a situation, the cost associated with the contingency cannot be calculated but will be very high. To compute the savings in cost when the operator is aware of the cyber-attack, we will consider a simple scenario. It is to be noted here that the generator startup and ramping times are still the same, and the time saved in troubleshooting the

root cause is the savings for the utility. When the operator notices the contingency, initial reaction is to shed the load to bring system frequency within acceptable bounds for $N-2$ contingency discussed above. Then the operator tries to bring the generators back into service, however this would not be possible since the cyber assets are compromised. The operator then has to call the maintenance division to take a look at what has happened at the problem location and troubleshoot for the cause. The money lost per hour of troubleshooting is about \$67726 assuming a charge of \$0.06925 per kWh for lost load of 978 MW in this specific case. Assuming the clearance time ranges between an hour to four hours, the total dollar amount lost by the utility for not serving the load could range from \$67726 to \$270906 neglecting generation costs.

## V. Related Work

Cone et al. propose CyberCIEGE [12], a video game as a cyber security awareness and educational tool that can engage typical users in an engaging security adventure. Shumba [13] suggests new tool-based techniques to educate students about cyber-security basics. Tobin et al. [14] introduce AWARE that emulates intrusions on a Windows machine where the user can learn how to detect the on-going intrusion using the system-supplied tools. The above-mentioned proposed solutions are mostly focused on educating general users regarding universal security concepts and does not concentrate on training security administrators regarding advanced tactics to protect a networked system against malicious adversaries. Labuschagne et al. [15] propose an interactive game hosted by social networking sites with the purpose of creating awareness on information security threats and vulnerabilities. Saunders [16] introduces instructional methods for information assurance (IA) using simulation. These proposed techniques can be used for educating a variety of IA constituency including network administrators and functional managers. Although the papers introduce novel ideas, they are neither implemented nor evaluated on simulated or real-world environments.

It is noteworthy that unlike SECPSIM almost none of the past security training or educational software tools has the capability of learning from expert administrators and hence require heavy manual human involvement to design optimal corrective and responsive control actions for different situations. Furthermore, they do not take into account detailed information such as the network configuration of the infrastructure to make the training effort customized for each target infrastructure. Such customization enables SECPSIM to train the system operators more accurately. Finally, SECPSIM targets cyber-physical infrastructures where both cyber assets and power components are emulated.

Some commercially available OTS include Alstoms e-terrasimulator[3], ABBs OTS[4], Open Systems Internationals OpenOTS [5] among others. Each of these simulators share the same three common modules; Power system module, Control center module and Instructor module with varying level of detail. However, almost all of the above-mentioned solutions concentrate on simulation of the power components and the cyber network configuration details are often ignored. The need for a cyber-physical smart grid security approach as well as system requirements and counter measures are highlighted in [17]. CW. Ten et. al propose different ways of modeling cyber intrusions and using the proposed model evaluate impact on SCADA systems in [18]. The fundamental limitations of static and dynamic attack detection, and identification procedures is studied in [19]. Counter measures against arbitrary unobservable attacks on SCADA/EMS using known secure PMUs in the system is studied in [20]. None of the abovementioned solutions aims at training operators regarding the cyber threats and possible countermeasures.

[3]Available at http://www.alstom.com/grid/e-terrasimulator/.

[4]Available at http://www.abb.us.

[5]Available at http://www.osii.com.

## VI. Conclusions

In this paper, we presented SECPSIM, an enhanced cyber-physical security simulator for training operators. SECPSIM learns mathematically how to protect the cyber-physical infrastructure through its interaction with an operator or scripted list of suitable control actions in various simulated cyber-physical intrusion states. SECPSIM uses the mathematical models to train operator(s) with a user friendly graphical interface that represents a realistic simulated infrastructure. Our results show that SECPSIM can train system operators efficiently with minimal manual effort on a simulated cyber-physical environment, and hence without causing any damaging consequence on an actual operational system.

## References


[1] "Electricity grid in U.S. penetrated by spies, available online at http://online.wsj.com/article/SB123914805204099085.html," 2009.

[2] N. Falliere, L. O. Murchu, and E. Chien, "W32.Stuxnet Dossier," Symantic Security Response, Tech. Rep., Oct. 2010.

[3] A. S. Mulky and S. Mahajan, "Operator training simulator," in *SPE International Production and Operations Conference*, 2012.

[4] J. J. Grainger and W. D. Stevenson, *Power system analysis*. McGraw-Hill New York, 1994, vol. 621.

[5] A. Varga *et al.*, "The omnet++ discrete event simulation system," in *European Simulation Multiconference*, vol. 9, 2001.

[6] 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 Conference on Dependable Systems and Networks*, 2012, pp. 1–12.

[7] R. Bellman, *Dynamic Programming*. Princeton University Press, 1957; republished 2003.

[8] T. A. Ernster and A. K. Srivastava, "Power system vulnerability analysis-towards validation of centrality measures," in *Transmission and Distribution Conference and Exposition (T&D)*. IEEE, 2012, pp. 1–6.

[9] R. Bellman, "On a routing problem," DTIC Doc., Tech. Rep., 1956.

[10] A. Srivastava, T. Morris, T. Ernster, C. Vellaithurai, S. Pan, and U. Adhikari, "Modeling cyber-physical vulnerability of the smart grid with incomplete information," *IEEE Trans. Smart Grid*, vol. 4, no. 1, pp. 235–244, 2013.

[11] "NPCC Document A-03, Emergency Operation Criteria, Northeast Power Coordinating Council (NPCC)," 2004.

[12] B. D. Cone, C. E. Irvine, M. F. Thompson, and T. D. Nguyen, "A video game for cyber security training and awareness," *computers & security*, vol. 26, no. 1, pp. 63–72, 2007.

[13] R. Shumba, "Towards a more effective way of teaching a cybersecurity basics course," in *ACM SIGCSE Bulletin*, vol. 36, no. 4. ACM, 2004, pp. 108–111.

[14] D. L. Tobin Jr and M. S. Ware, "Using a windows attack intrusion emulator (aware) to teach computer security awareness," in *ACM SIGCSE Bulletin*, vol. 37, no. 3. ACM, 2005, pp. 213–217.

[15] W. Labuschagne, N. Veerasamy, I. Burke, and M. Eloff, "Design of cyber security awareness game utilizing a social media framework," in *Information Security South Africa (ISSA), 2011*. IEEE, 2011, pp. 1–9.

[16] J. H. Saunders, "Simulation approaches in information security education," in *Proc. 6th National Colloquium for Information System Security Education, Redmond, WA*, 2002.

[17] Y. Mo, T.-J. Kim, K. Brancik, D. Dickinson, H. Lee, A. Perrig, and B. Sinopoli, "Cyber–physical security of a smart grid infrastructure," *Proceedings of the IEEE*, vol. 100, no. 1, pp. 195–209, 2012.

[18] C.-W. Ten, C.-C. Liu, and G. Manimaran, "Vulnerability assessment of cybersecurity for scada systems," *Power Systems, IEEE Transactions on*, vol. 23, no. 4, pp. 1836–1846, 2008.

[19] F. Pasqualetti, F. Dorfler, and F. Bullo, "Cyber-physical attacks in power networks: Models, fundamental limitations and monitor design," in *Decision and Control and European Control Conference (CDC-ECC), 2011 50th IEEE Conference on*. IEEE, 2011, pp. 2195–2201.

[20] A. Giani, E. Bitar, M. Garcia, M. McQueen, P. Khargonekar, and K. Poolla, "Smart grid data integrity attacks: characterizations and countermeasures π," in *Smart Grid Communications (SmartGridComm), 2011 IEEE International Conference on*. IEEE, 2011, pp. 232–237.