Towards Resilient Cyber-Physical Energy Systems

Stefanos Baros[1] Dylan Shiltz[1] Prateek Jaipuria[2]
Alefiya Hussain[2] Anuradha M. Annaswamy[1]

[1] *Department of Mechanical Engineering, Massachusetts Institute of Technology* *
email: {sbaros, djshiltz, aanna} @mit.edu
[2] *Information Sciences Institute, University of Southern California*
email: {jaipuria, hussain} @isi.edu

Abstract

In this paper, we develop a system-of-systems framework to address cyber-physical resilience, the ability to withstand the combined presence of both cyber attacks and physical faults. This framework incorporates a definition of resilience, a resilience metric as well as a resilient control design methodology. The resilient control architecture utilizes a hybrid optimal control methodology combined with a dynamic regulation market mechanism (DRMM), and is evaluated in the context of frequency regulation at a transmission grid. The framework enables the evaluation of both the classical robust control properties and emerging resilient control properties under both cyber attacks and physical faults. The proposed framework is used to assess resilience of a Cyber-Physical Energy System (CPES) when subjected to both cyber and physical faults via DETERLab. DETERLab, a testbed capable of emulating high fidelity, cybersecure, networked systems, is used to construct critical scenarios with physical faults emulated in the form of generator outages and cyber faults emulated in the form of Denial of Service (DoS) attacks. Under these scenarios, the resilience and performance of a CPES that is comprised of 56 generators and 99 consumers is evaluated using the hybrid-DRMM control methodology.

1. Introduction

Cyber-physical systems (CPS) are physical systems whose operations are monitored, coordinated, self-governed and integrated by a system of sophisticated computing and communication algorithms. CPS not only permit but actually mandate synergistic interactions between physical dynamics and computational processes, with the rationale that wide deployment of Information and Communication Technologies (ICT) results in higher reliability and lower operational costs relative to the traditional proprietary and closed systems. Such a deployment introduces new vulnerabilities in the form of security threats due to cyber attacks. A specific class of CPS that we focus on this paper is in the energy sector, which corresponds to smart grids [2], which are end-to-end cyber-enabled electric power systems, from fuel source, to generation, transmission, distribution, and end use.

Cyber-physical Energy Systems (CPES) are not only vulnerable to security threats but also physical outages which may occur due to natural disasters such as hurricanes, earthquakes, and other unforeseen anomalies. A physical outage can be also caused by malicious human physical actions. An example is the "Metcalf sniper attack" on PG&E Corp's Metcalf transmission substation in San Jose, California that happened in 2013 and caused a damage worth over $15 million [38]. Given that the end-goal of CPES is reliable delivery of power to its end-user at all times, cyber-physical resilience of CPES is a necessary requirement, which corresponds to the ability to withstand high-impact disturbances, which may occur due to either physical or cyber causes, and continue to deliver acceptable performance. In this paper, we propose a framework towards such cyber-physical resilience of CPES.

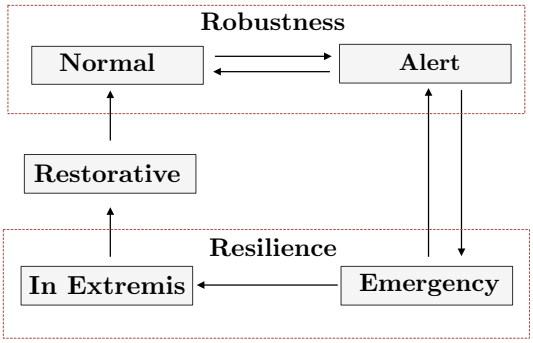

Figure 1: The most critical operating states of a CPES

In order to ensure an efficient yet economic performance, the states of a CPES are often organized into five modes, normal, alert, emergency, in-extremis, and restorative [26] (see Fig. 1). Depending on the mode that the energy system is in, a corresponding set of decisions and actions is pursued to ensure safety and desirable performance. Two points are worth making regarding these five modes. The first is that these CPES are typically designed to be *robust* with their control and protection measures ensuring that they lie in the nominal mode for the most part, and for any perturbations that may cause a transition to the alert stage that a suitable robust action brings the system back to a *nominal* state. And those disturbances that trigger a transition to the emergency mode, or worse still, the in-extremis mode, are assumed to be a high-impact, but low probability event. In the absence of cyber-attacks, while such an assumption is valid, a combined presence of both physical and cyber anomalies can significantly increase the probability of this transition,

*This work was supported by the NSF initiative, Award no. EFRI-1441301.

as well as reduce the time interval of this transition. The second is that the schematic proposed in Fig. 1 also sets the stage for the notion of resilience and its distinction from robustness. CPES can be characterized as robust when they are able to operate normally (which can correspond to the case when the total electricity demand is fully served) under disturbances that only cause transitions between normal and alert states [43, 4]. In contrast, in the presence of high impact disturbances, if the CPES transition to an emergency state and further to an extremis state they can be characterized as being resilient when they can return to an alert or normal state within an acceptable time. A CPES system must therefore be designed to be both robust and resilient, as disturbances can have a range of impact, making the transition to any of the five states mentioned above equally likely. Such a design principle is applicable not only to CPES but any critical infrastructures such as transportation, water, and healthcare [23, 25, 19]. Robustness of systems has been investigated extensively over the past two to three decades including several papers, textbooks, conferences, and journals by the controls community. And more recently, robustness of CPS has been examined in [36, 31, 40]. In contrast, a formal definition of resilience, either in the context of CPS or systems in general, is yet to emerge. Broadly speaking, it is widely accepted that resilience connotes the ability of a CPS to sustain and recover from extreme and severe disturbances that can drive the system to its physical operational limits [26]. In contrast, robustness is a precisely defined notion in control theory that denotes a property that characterizes the system's ability to retain normal operation after being subjected to a range of bounded, and small disturbances or uncertainties [42]. Clearly new tools for analysis and synthesis of resilient control methods for CPES are needed and are currently lacking. The goal of this paper is to examine cyber-physical resilience, and take a first step towards developing a framework for studying this concept for CPES.

The framework that we propose includes a physical network, such as a network of generators, loads, and transmission lines in a power grid, a communication network, that is capable of transmitting information about the physical and cyber variables to agents at various nodes, models of classes of cyber attacks including deception and disruption [27, 14, 8], an overall hybrid dynamic model of a CPES with five modes that correspond to those outlined in Fig. 1, a definition of resilience, a resilience metric, and a methodology for designing a resilient control system for the overall hybrid model. The framework is evaluated in the context of frequency regulation in a power grid at a transmission level. The resilient control system that we propose consists of a Dynamic Regulation Market Mechanism (DRMM) that carries out frequency regulation using a market-based optimization framework, and a supervisory resilient hybrid control layer. The main contributions of this paper are the development of this framework and its validation using a high fidelity testbed, DETER, that is capable of emulating high fidelity, cybersecure, networked systems. DETER is used to construct critical scenarios in the CPES where both physical faults and cyber attacks are assumed to occur.

Very few studies have been carried out in the literature that has focused on an end-to-end formulation of a cyber-physical resilience control problem in a CPES. Notable exceptions include [43] where the authors follow a game-theoretic approach for resilient control design. References [27, 14] and [8] address models of cyber-attacks, but have not addressed resilience metrics or resilient control design. In reference [35], cyber security of power system is addressed through a risk-based approach, but a detailed discussion of resilience of a power grid against physical and cyber attacks has not been provided. In contrast, in this paper we propose an overall framework to evaluate cyber-physical resilience, propose a resilient control method, and validate it using a high fidelity testbed, DETER.

This paper is organized as follows. In Section 2 the problem statement and in Section 3 the proposed system-theoretic framework for resilient CPS are presented, respectively. In Section 4, a resilience analysis of a CPES with a Dynamic Regulation Market Mechanism (DRMM) is conducted with the Section 5 presenting a testbed validation case-study of the CPES using DETER. Finally, Section 6 concludes this paper with some remarks.

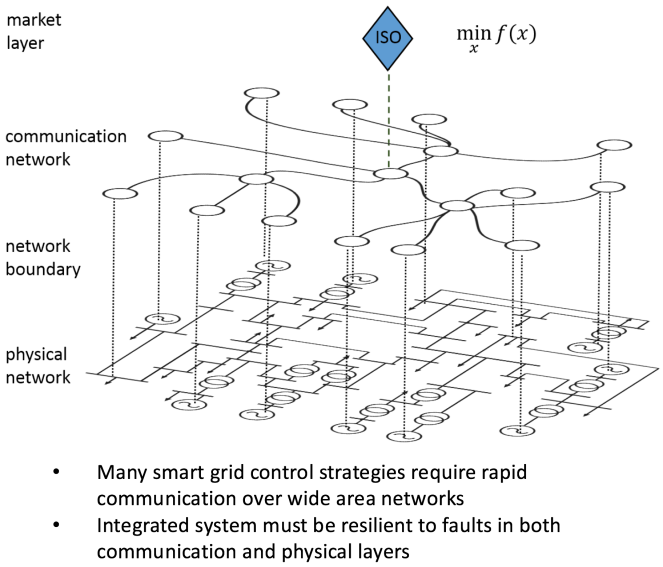

Figure 2: CPES with both physical and cyber layers

2. Problem Statement

An example of a CPES is a power grid with a communication layer, as shown in Fig. 2. The typical problem we consider is one where a large physical outage occurs, which then is followed by a cyber attack. An example of such a physical anomaly is a generator outage in a transmission network, which can lead to large frequency oscillations (see Fig. 3). Depending on the extent of this outage, the overall CPES can transition to either an alert or an emergency state. Suppose that this outage is such that the latter occurs, then typically load shedding is introduced, which ensures that the CPES does not transition to in-extremis. But if at this instance, a cyber attack occurs, then this transition indeed can ensue, as shown in Fig. 3. Our focus is on such a combination of events in this paper. In particular, the objective is to identify how the CPES can be designed to function satisfactorily despite these high-impact disturbances, i.e. be cyber-physical resilient.

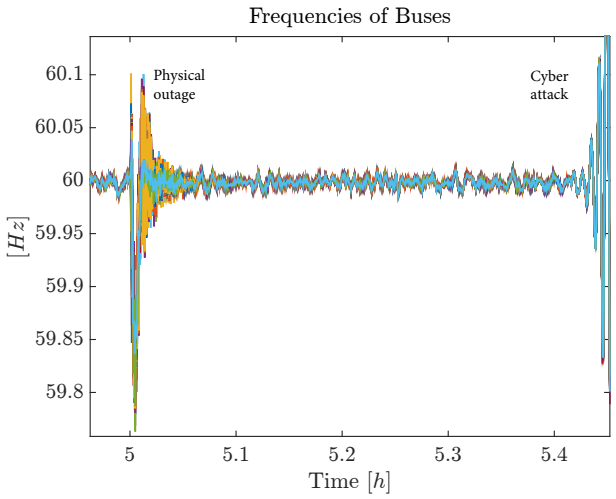

Figure 3: Frequencies of IEEE 118-bus system buses under a physical and a cyber outage

2.1 Models of Cyber-attacks

Malicious attackers can exploit protocol and network insecurities to target energy CPS operations and markets. As wide area energy CPS systems are starting to leverage existing Internet infrastructure, closed dedicated energy networks are being replaced with standard open Internet protocols and shared networks. These shared networks can be used to compromise the three fundamental properties of information in networked control systems, namely, confidentiality, integrity, and availability [41].

Confidentiality concerns the concealment of data, ensuring it remains known only to the authorized parties. *Disclosure attacks* enable the adversary to gather sequences of data $\mathcal{I}_k$ from the calculated control actions u_k and the real measurements y_k . The physical dynamics of the system are not affected by this type of attack.

Integrity relates to the trustworthiness of data, meaning there is no unauthorized change to the information between the source and destination. *Deception attacks* modify the control actions u_k and sensor measurements y_k from their calculated or real values to the corrupted signals $\tilde{u}_k$ and $\tilde{y}_k$, respectively. The deception attacks are modeled as

$$\tilde{u}_k \triangleq u_k + \Delta u_k$$

$$\tilde{y}_k \triangleq y_k + \Delta y_k$$

where the vectors Δu_k and Δy_k represent the manipulation to the respective data channels.

Availability considers the timely access to information or system functionalities. *Disruption attacks* prevent the transmitted data from reaching the desired destination. Such attacks can impact the system by blocking the data or feedback signals, using denial of service attacks, replay attacks, or zero dynamics attacks [27]. The Fig. 4 illustrates the three categories of attacks and how they violate the security properties. In all three cases, the physical plant is sending a measurement vector $y_k = [7, 14]^T$ to the controller through the communication network. This was intended to be a private message to be known only to the plant and the controller. All three forms of attacks affect this message in various forms. In the example shown in Figure 3, a cyber attack was assumed to affect the information sent from a generator about its availability to an Independent System Operator that plays a supervisory role in ensuring power balance across an entire region. Due to this corruption, the ISO carries out an incorrect economic dispatch, which in turn leads to power imbalance and therefore a frequency deviation as illustrated in Fig. 3.

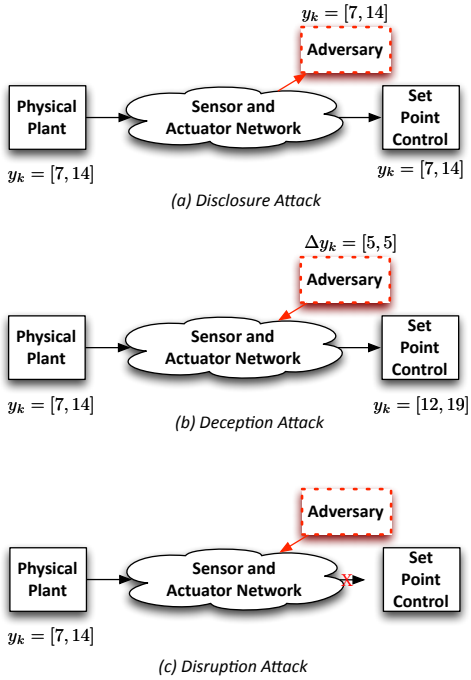

Figure 4: Set point based cyberattacks on the communication network: (a) data confidentiality violation by a disclose attack, (b) data integrity violation by false data injection attack, (c) data availability violation by a denial of service attack.

3. Systems-theoretic Framework for Resilient CPS

In this section, we first provide a definition of resilience in the context of CPS and present a hybrid systems modeling framework for robust and resilient control design. In addition, we provide a metric for quantifying the resilience of CPS and formulate the optimal resilient control design problem.

3.1 Definition of Resilience

The term resilience is being discussed increasingly of late in the context of CPS, ranging from transportation [19], power [1, 43], control systems [30, 29, 43] as well as other types of systems such as ecological [17, 18] and biological [23]. Resilience is often discussed concomitantly with other system-oriented notions such as robustness, reliability and stability [25] and quite often used interchangeably with the term robustness. We argue however that these two terms are distinct. The reason is that resilience and robustness

characterize fundamentally different system properties. As mentioned earlier, the term robustness applies in the context of small bounded disturbances while resilience, in the context of extreme high-impact disturbances. We offer the following definition of resilience:

Definition 1. *Resilience of a CPS with respect to a class of extreme and high impact disturbances, is the property that characterizes its ability to withstand and recover from this particular class of disturbances by being allowed to temporarily transit to a state where its performance is significantly degraded and returning within acceptable time to a state where certain minimal but critical performance criteria are met.*

With this definition of resilience serving as the cornerstone of our analysis, in the next section we introduce a CPS modeling framework that enables robust and resilient control design.

3.2 CPS Modeling for Robust and Resilient Control Design

In order to analyze and evaluate the resilience and robustness of CPS, as well as for performing resilient and robust control design, a suitable modeling framework should be followed. In this paper, recognizing that CPS are fundamentally hybrid systems, we propose the following *hybrid systems modeling framework*, inspired by that proposed in [43], where a CPS can be modeled as:

$$x_{k+1} = f(x_k, u_k, w_k, q_k(x_k, \alpha_k, d_k, l_k)), \quad x_0 = \mathbb{R}^n \qquad (1)$$

where $x_k \in \mathbb{R}^n$, $u_k \in \mathbb{R}^r$, $w_k \in \mathbb{R}^p$ are the state, the control input and the deterministic disturbance vector at time k, respectively. The variable $q_k \in \mathcal{Q}$ denotes a discrete operating mode and is parameterized by x_k (state), by α_k, that can take any value among a collection of possible cyber attacks $\mathcal{A}$, $d_k \in \mathcal{D}$ that models the possible physical failures, the system operator's action $l_k \in \mathcal{L}$. The complexity of a given CPS and the way through which state variations, cyber and physical failures or discrete control actions by the operator can impact its dynamics, i.e its vector field f, will characterize the function q_k. The model (1) can be viewed as a representation of not only CPES, but general CPS.

3.3 Resilience Metric

We now propose the following metric to quantify the *resilience* of a CPS described in (1):

$$\mathbf{R}(x_k) = \int_{k_1}^{k_2} \left[J_k^* - J(x_k)\right] dk, \quad \mathbf{R} \in \mathbb{R}_+ \qquad (2)$$

where $J(x_k)$ is a function of the CPS state capturing the system's performance and J_k^* is the time-dependent nominal performance that the system should meet, with $\mathbf{R}$ in (2) representing the shaded area shown in Fig. 5 [37]. A few points should be noted about the resilience metric in (2). First, it naturally captures the performance degradation of the CPS but also the time frame for which that occurs. Consequently, the smaller the value of $\mathbf{R}$ for a given CPS and a given set of critical physical or cyber failures [37], the more resilient that system is with respect to these failures. This implies that $\mathbf{R}$ in (2) is an appropriate resilient metric, since a resilient CPS, is one which following a severe disturbance not only does it experience very small performance degradation, $\|J_k^* - J(x_k)\|_\infty$ but it also recovers back to the mode

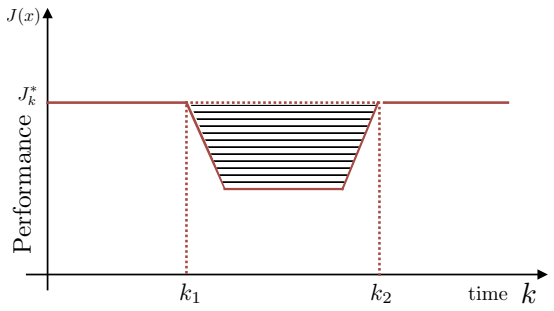

Figure 5: Resilience metric

with nominal performance within an acceptable time i.e with $(k_2 - k_1)$ being small. The performance of a CPS as the one in (1) can be compromised in several ways. High-impact cyber, physical disturbances or actions performed by the system operator can cause the CPS to transit to new operating modes by altering its structure and correspondingly its vector field. In these new modes, the new equilibrium points x^e can lead to $J(x^e) < J^*$ i.e to performance degradation.

3.4 Optimal Resilient Control Design

With respect to the resilience metric defined (2), the optimal resilient control design problem can be now stated as follows:

Optimal Resilient Control Design Problem: Given a control input $\tilde{u}_k$, a deterministic bounded disturbance $\tilde{w}_k$, a physical discrete disturbance $\tilde{d}_k \in \mathcal{D}$ and a cyber disturbance $\tilde{\alpha}_k \in \mathcal{A}$, compute a strategy $\tilde{l}_k \in \mathcal{L}$ which is the solution of:

$$\begin{aligned} \underset{l_k \in \mathcal{L}}{\textbf{minimize}} \quad & \mathbf{R}(x_k) \\ \textbf{subject to} \quad & x_{k+1} = f(x_k, \tilde{u}_k, \tilde{w}_k, q_k(x_k, \tilde{\alpha}_k, \tilde{d}_k, l_k)) \\ & x_0, x_k \in \mathbb{R}^n, \; q_k \in \mathcal{Q} \end{aligned} \qquad (3)$$

Hence, the objective of the resilient controller l_k is to minimize the performance loss $\mathbf{R}(\cdot)$ while driving the system back to its normal operating mode (with nominal performance). On the other hand, the objective of a robust controller would be to achieve optimal performance in each mode q_k in the face of a disturbance w_k. A general solution of the optimization problem that yields a resilient controller is highly challenging. In the next section, we provide one illustration of a resilient controller that approximately solves (3).

4. Resilient CPES with Dynamic Regulation Market Mechanisms

In this section, we address resilience of a particular CPES using a Dynamic Regulation Market Mechanism (DRMM) as proposed in [32, 33]. The DRMM is first described, and how it can be used to achieve frequency regulation in the presence of various disturbances. The supervisory hybrid optimal control layer is then described.

4.1 CPES with DRMM

We begin by describing the particular CPES, which pertains to an optimal secondary control at the transmission level. Described in more detail in [32, 33], the Dynamic Regulation Market Mechanism (DRMM), achieves frequency regulation in the presence of various physical disturbances in an optimal manner. The starting point for this model is the description of the physical dynamics of a power system. These are, the voltage angle δ_i and electrical frequency ω_i dynamics (swing dynamics) of the synchronous machines buses, the voltage angle δ_i dynamics (swing dynamics) of the load buses, the speed-governor valve position Y_i dynamics of a synchronous generator and its power output $P_{M,i}$ turbine dynamics. Lastly, the power consumption $P_{C,i}$ dynamics of the Demand Response (DR) resourses which are introduced by latencies on their communication with the DR-aggregator. Altogether, they can be compactly stated in discrete-time state-space form as:

$$\psi_{k+1} = \Phi\psi_k + \Gamma_B u_k + \Gamma_E P_{L,k},\ \psi_0 \in \mathbb{R}^{|\psi|} \tag{4}$$

where $\psi = [\omega_G^T\ \delta^T\ Y^T\ P_M^T\ P_C^T]^T$ is the state-vector that denotes deviations of frequencies, phase angles, valve positions, mechanical power generation and flexible consumption from their equilibrium values, and $\Phi,\ \Gamma_B,\ \Gamma_E$ are constant matrices. In (4), the control input is given by $u = [P_G^T\ P_D^T]^T$ where $P_G = (\mathcal{P}_G - \mathcal{P}_G^*),\ P_D = (\mathcal{P}_D - \mathcal{P}_D^*)$ are the secondary control setpoints for the generators and DR units, respectively. In the current practice today in power systems, only regulation of the P_G's of the generators is considered at the secondary control level and its objective is to regulate the frequency of a balancing area back to its nominal value. This is attained by designing the control input P_G as an integral control feedback of the area control error (ACE) which, for an area β, is defined as a weighted sum of the frequency error $\overline{\omega}_\beta$ and the tie line error P_T:

$$e_{C_k}^{(\beta)} = B^{(\beta)}\overline{\omega}_\beta + N_T^{(\beta)} P_{T,k} = N_\psi^{(\beta)}\psi_k \tag{5}$$

where $N_T^{(\beta)},\ N_\psi^{(\beta)}$ are constant matrices. The specific generators that participate in the secondary control and their corresponding regulation capacities are defined through a regulation market which is cleared once every hour. Further, the slow-varying set-points $\mathcal{P}_G^*,\ \mathcal{P}_D^*$ are provided every 5 minutes by the tertiary level which solves an optimal power-flow problem (OPF) in a real-time market setting. In contrast to this practice, DRMM [32, 33] is implemented as an ongoing negotiation process between generators, DR units and the ISO, that allows both generators and DR resources to bid for regulation services in real-time while also ensuring optimal allocation of these services. The negotiations are realized through the iterative market dynamics stated below which, via a Newton-like method, drive the market to the solution of a modified DC OPF with objective the maximization of a Social Welfare. At the same time, through an ACE signal into the power balance equation they realize real-time optimal secondary control while additionally, they guarantee energy payback of the DR units through an additional energy equality constraint. The DRMM iterative dynamics can be expressed as: [32, 33]:

Set-point dynamics

$$\xi_{k+1} = \xi_k - a\hat{H}_\gamma^{-1}(\pi_k + N_h\hat{\lambda}_k) \tag{6}$$

Multiplier dynamics

$$\mu_{k+1} = \max\{0, \mu_k + K_\mu g_k\} \tag{7}$$

$$\nu_{k+1} = K_\nu\nu_k + K_E E_{D,k} + K_\eta\eta_{D,k} \tag{8}$$

Auxiliary dynamics

$$E_{D,k+1} = E_{D,k} + N_E\xi_k \tag{9}$$

$$\eta_{D,k+1} = \eta_{D,k} + E_{D,k} \tag{10}$$

Regulation signal dynamics

$$\rho_{k+1} = \rho_k - K_f N_\psi\psi_k \tag{11}$$

where

$$\pi_k = \nabla_\xi f_k + N_g\mu_k + N_E\nu_k \tag{12}$$

$$\hat{\lambda}_k = (N_h^T\hat{H}_\gamma^{-1}N_h)^{-1}(h_k - N_h^T\hat{H}_\gamma^{-1}\pi_k) \tag{13}$$

The vector $\xi = [\theta^T\ P_G^T\ P_D^T]^T$ represents the set-points and $\mu,\ \nu$ the multipliers of the inequality and equality constraints, respectively. Moreover, the vector E_D represents the energy states of the DR units, η_D the integrals of these states, ρ the regulation signal, π_k a price response signal and $\hat{H}_\gamma$ an estimate of the Hessian of the Lagrangian function. Altogether, equations (6)-(10) can be compactly stated as:

$$\zeta_{k+1} = A_{\zeta_k}\zeta_k + B_\rho\rho_k + B_{P_L}\hat{P}_{L,k} + B_{l_g}l_g,\ \ \zeta_0 \in \mathbb{R}^{|\zeta|} \tag{14}$$

where $\zeta = [\xi^T\ \mu^T\ \nu^T\ E_D^T\ \eta_D^T]^T$. The DRMM for each balancing area is executed as follows. The Independent System Operator (ISO) provides the set-points $P_{G,k}$ and $P_{D,k}$ obtained by the equation (6) to the generators and DR units every Δt_k seconds. When they receive these set-points the generators and DR units use their multipliers $\mu_k,\ \nu_k$ to compute their price response signal π_k which they communicate to the ISO. The ISO, updates the regulation signal ρ_k and h_k by computing the ACE in its area and finally, upon receiving all π_k computes the next set of set-points ξ_{k+1} with the whole process repeating in the same manner. For a CPES where the set of balancing areas is denoted by $\mathcal{B}$, the physical, DRMM and regulation signal dynamics can be stated as [32, 33]:

Physical Dynamics

$$\psi_{k+1} = \Phi\psi_k + \Gamma_B\sum_{\beta\in\mathcal{B}} N_\zeta^{(\beta)}\zeta_k^{(\beta)} + \Gamma_E P_{L,k} \tag{15}$$

DRMM Dynamics

$$\zeta_{k+1}^{(\beta)} = A_{\zeta_k}^{(\beta)}\zeta_k^{(\beta)} + B_\rho^{(\beta)}\rho_k^{(\beta)} + B_{P_L}^{(\beta)}\hat{P}_{L,k}^{(\beta)} + B_{l_g}^{(\beta)}l_g^{(\beta)} \tag{16}$$

Regulation Signal Dynamics

$$\rho_{k+1}^{(\beta)} = \rho_k^{(\beta)} - K_f^{(\beta)}N_\psi^{(\beta)}\psi_k \tag{17}$$

Ultimately, the dynamical model of the CPES with a DRMM can be compactly written as:

$$\chi_{k+1} = A_{\chi_k}\chi_k + B_\chi v_k,\ \chi_0 \in \mathbb{R}^{|\chi|} \tag{18}$$

where $\chi = [\psi^T\ \zeta^{(1)^T}\ \cdots\ \zeta^{(|\mathcal{B}|)^T}\ \rho^{(1)}\ \cdots\ \rho^{(|\mathcal{B}|)}]^T \in \mathbb{R}^{|\chi|}$ and $v = [P_L^T\ \hat{P}_L^T\ l_g^T]^T \in \mathbb{R}^{|v|}$. The cyber component of the CPES in (18) is due to the two-way real-time communication of the set-points ξ and price signals π among the ISO, generators

and DR units. In the next Section, we focus on designing a resilient hybrid control law for the system (18).

4.2 Resilient Hybrid Control Layer of a CPES

In the previous section, we constructed the closed-loop form of a specific CPES (18) with the discrete-time control law defined through the DRMM. In this section, we focus on the design of an optimal hybrid control layer for this CPES. To accomplish that, we first recast the model (18) in the form of a hybrid system as in (1) and use it to formulate an optimal control problem. Let this CPES operate in one of the five well-established modes depicted in figure [12, 26]. We define the set of these discrete operating modes by $\mathcal{Q} := \{q_1, q_2, q_3, q_4, q_5\}$ where q_1 corresponds to the *normal state*, q_2 to the *alert state*, q_3 to the *emergency state*, q_4 to the *extremis state* and q_5 to the *restorative state* [12]. A qualitative description of these operating states and the transitions among them is the following. CPES can transit into an alert state (q_2) when subjected to small state variations χ, to mild cyber α or physical anomalies d or to any other actions performed by the system operator. In this case, CPES can be characterized as robust when they are able to continue operating normally, i.e. serving the total electricity demand, in modes q_1 and q_2 without any performance degradation and despite the reduced stability margins while eventually recovering from the *alert* (q_2) to the *normal* (q_1) mode [26]. On the other hand, large state-variations χ or more severe high-impact cyber α or physical anomalies d, or discrete actions performed by the system operator l, can cause power systems to transit into an emergency state where their performance is degraded, i.e part of the demand is served, while they experience overloads. We emphasize that, large state-variations can cause discrete transitions to a CPES by triggering other protection-type control switches. The series of actions l that might be taken at this stage, any state-variations χ or physical/cyber anomalies d, α that might be incurred, will determine whether the CPES will move to an *extremis* state (q_4) where its performance is significantly degraded i.e a small percentage of electricity demand is served, and it experiences even greater overloads, or it will return back to an alert state (q_2). Finally, the CPES can transit from the *extremis* state (q_4) to the restorative (q_5) and then to the *normal* operating state (q_1) when the system operator performs appropriate control actions l. In summary, the CPES in (18) can be in any of the above modes and can transit between them by experiencing either state-variation χ, exogenous disturbances $d \in \mathcal{D}$ (e.g tripping of a line), Cyber-attacks $\alpha \in \mathcal{A}$ or discrete-time control actions $l \in \mathcal{L}$ which are performed by the system operator. We emphasize that, by definition, these operating modes are generic enough so that in reality they serve as a high-level description of the numerous other discrete operating modes that the CPES (18) can actually operate in. Nevertheless, these are sufficient for the scope of our analysis.

To capture the above complex dynamical behavior of a CPES with the above operating modes, we use a hybrid automaton. The specific example we focus on is frequency regulation in a power grid at a transmission level. This automaton, shown in Fig 6, can be described as the follows [16]:

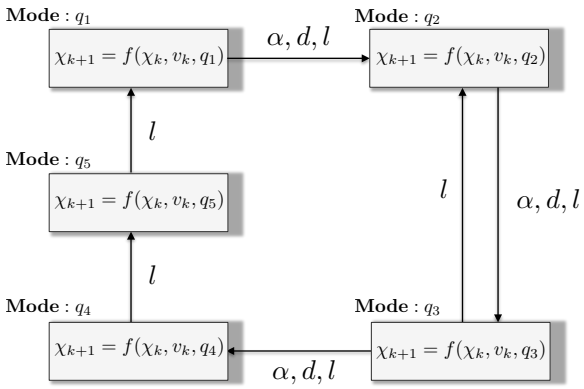

Figure 6: Hybrid automaton modeling the Cyber-physical Energy System (18)

Vector field

$$f(\chi_k, v_k, q_k) := A_{\chi_k}^{q_k}\chi_k + B_{\chi}^{q_k}v_k^{q_k}, \quad f : \mathbb{R}^{|\chi|} \times \mathbb{R}^{|v|} \times \mathcal{Q} \mapsto \mathbb{R}^{|\chi|}$$

Discrete operating modes

$$\mathcal{Q} := \{q_1, q_2, q_3, q_4, q_5\},\ q_k := q_k(\chi_k, \alpha_k, d_k, l_k) \in \mathcal{Q}$$

Discrete transition mapping

$$\phi : \mathcal{Q} \times \mathbb{R}^{|\chi|} \times \mathcal{A} \times \mathcal{D} \times \mathcal{L} \mapsto \mathcal{Q}$$

Note that, v_k in (18) does not correspond to a control input but to the inflexible load which can be controlled by the system operator in emergency situations (e.g via load shedding). Further, realize that, the operating mode $q_k \in \mathcal{Q}$ depends on the state-vector χ_k, the cyber-attacks $\alpha_k \in \mathcal{A}$, the exogenous disturbances $d_k \in \mathcal{D}$ (e.g tripping of a line) and any other discrete-time control actions $l_k \in \mathcal{L}$ performed by the system operator. For the above hybrid automaton model, we proceed to define a function that captures its performance over time. We start by noting that, the generic resilient metric as defined in (2) represents somehow the performance loss of a CPS over time that might occur due to any kind of anomalies. In the case of CPES, their performance loss has to reflect the number of customers (electricity users) not served and/or the amount of electricity demand not served, as well as the duration for which that holds. With this in mind, let $\mathcal{G}$ denote the set of generators and $\mathcal{D}_r$ the set of DR units and consider the following performance function for the CPES in (18):

$$J(\chi_k) = \sum_{i \in \mathcal{G}} P_{M,k}^{(i)} - \sum_{i \in \mathcal{D}_r} P_{C,k}^{(i)} \tag{19}$$

i.e the total generation minus the total power consumption from the DR units of the CPES (18). By denoting the varying inflexible electricity demand as a function of time with J_k^*, we can define the *resilience metric* as:

$$\mathbf{R}(\chi_k) = \int_{k_1}^{k_2} \left[J_k^* - \sum_{i \in \mathcal{G}} P_{M,k}^{(i)} + \sum_{i \in \mathcal{D}_r} P_{C,k}^{(i)}\right] dk, \ \ \mathbf{R} \in \mathbb{R}_+ \tag{20}$$

A resilient CPES should be able to serve the major part of the electricity demand even in the case of emergencies while

also return to a state where it serves the full demand in minimal time. The smaller $\mathbf{R}$ is, the more resilient the CPES in (18) would be. Interestingly, in the context of CPES, the resilience metric (20) has also a physical meaning, it denotes the energy demand not served after a disturbance [37]. With that, we pose the optimal resilient control design problem for the partially closed-loop (secondary control is already through DRMM) CPES (18) as follows:

Optimal Resilient Control Design Problem: Given a physical disturbance $\tilde{d}_k \in \mathcal{D}$ and/or a cyber disturbance $\tilde{\alpha}_k \in \mathcal{A}$, compute a strategy vector $\tilde{l}_k \in \mathcal{L}$ which is the solution of:

$$\begin{aligned} \underset{l_k \in \mathcal{L}}{\textbf{minimize}} \quad & \mathbf{R}(\chi_k) \\ \textbf{subject to} \quad & \chi_{k+1} = f(\chi_k, q_k(\chi_k, \tilde{\alpha}_k, \tilde{d}_k, l_k)) \\ & \chi_0,\ \chi_k \in \mathbb{R}^{|\chi|},\ q_k \in \mathcal{Q} \end{aligned} \tag{21}$$

In the next Section, we use the testbed DETERLab and present a case study on the IEEE 118-bus power system where, a series of physical d and cyber anomalies α take place and the system operator is able to recover its full operation, through a series of suboptimal but effective actions l.

5. Case Study

5.1 Attack Generation

The DETERLab facility provides a rich set of resources, tools, and methodologies to conduct high-fidelity, large scale network and cyber security experiments [10, 6]. This facility has been operational since 2003 and is operated by USC/ISI and UC Berkeley. The main thrusts of research on the testbed include cyber attacks and analysis, anomaly detection in networks, and technologies to support privacy and anonymity networks. As of September 2016, the DETER testbed has supported 10,000+ experimenters and students testing a wide range of cyber security technologies. Using DETERLab for evaluation of CPS allows the experimenter to replicate the interactions between the physical and cyber components (plants, controllers, markets, etc.) and the attackers with high-fidelity and accuracy, thus providing a unique balance between experiment control and realism. The attack traffic can be generated using either real–world attack tools or modeled attack tools provided by the DETERLab facility. Several real–world attack tools are available in binary or executable format and can be activated on the required operating systems and end host configuration. DETERLab also provides a range of DoS attack tools that model the various attack methodologies, command and control structures, attack volumes, and attack types, with easy to use graphical user interfaces. There are several experimentation environments available to evaluate networked controlled systems each offering different levels of fidelity and scale [7, 24, 9]. Although these environments have their own benefits, we believe that the DETERLab tools and facilities complement these efforts. In particular, it allows the experimenter to closely replicate the real–world end host and cyber attack models. This enables systematic and consistent resiliency evaluation of physical control systems in such environments.

5.2 Experimentation Framework

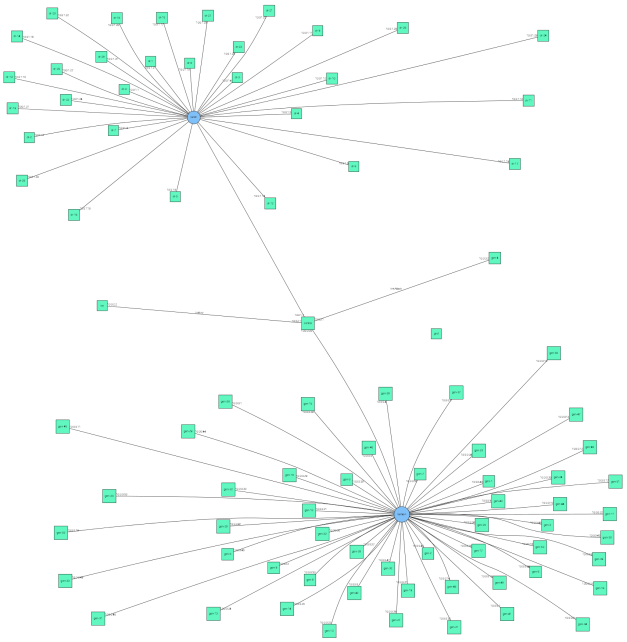

Figure 7: The IEEE 118-bus network overlaid with a communication network (black links) between the DR agents (green boxes) and the Generator agents (green boxes) within the market.

In this section, we discuss the framework for integrating the energy CPES semantics and market dynamics with the DETER testbed to systematically explore the impact of disruption attacks on evolution and stability of such systems. Our approach is to combine CPES and market dynamics tools and simulation with DETERLab tools and methodologies for resiliency evaluations. We build on dynamic market mechanisms developed in [32, 33], and develop additional functionalities needed for security experimentation and testing using the DETERLab facility. The DETERLab emulation architecture is shown in Fig. 7 and has three main components: the physical system dynamics, the physical-to-cyber network interface, and the cyber network dynamics. The *physical system dynamics* provides an interface to the grid agent that computes the power flows and provides primary AGC control in the network. The *physical to cyber dynamics* provides a mapping from the physical systems to the communication network at the various agents within the experiment. It is used to send and receive setpoints at the demand response and generator agents over a TCP/IP network. The *cyber network dynamics* captures the network traffic on the shared network. All cyber anomalies are created in this layer on the network.

Selecting representative topologies for the communication network has been a subject of significant research over the last several years. It is challenging since the Internet structure constantly evolves and deployed CPES systems rarely make their underlying network topologies publicly available due to security reasons [13, 7]. Additionally, the network routing structure is also impacted by the link-level communication technologies, such as wireless, satellite, or wired networks. For example, wireless mobile networks will have a dynamic topological and routing structure that evolves

with the movement of the nodes while wired networks have a static topological structure that does not change frequently. The DETER testbed is primarily a wired testbed and offers several topology generation tools and sample topology catalogs for experimentation [11].

The traffic in the experimentation framework is determined by the various servers, clients, and attackers in the network. To accurately model the wide-area networks and the Internet, cyber security experiments typically model three different types of network traffic; (i) *background traffic*, for example, web server and web client traffic which is congestion reactive, (ii) the *foreground traffic* that is under study, for example, control traffic in the energy CPS and markets, and (iii) *congestion non-reactive traffic* such as, attack traffic in a DoS attack or traffic generated at some constant rate from selfish and malicious nodes. These three types of traffic are interleaved to create a complex set of dynamics discussed in the next section. DETER provides a diverse set of traffic generators, including Harpoon,TCP replay, Apache wget clients for background and foreground traffic, and real and emulated DoS attack traffic and other traffic generators [11].

Modularizing our framework as discussed above enables us to rapidly evolve the cyber network and attack models and the physical energy CPS models to accurately explain the structural and functional improvements to the Internet and address existing security threats, explore new threats, and meet the challenges of scale and complexity. In the next section, we discuss the specific experimentation scenarios along with metrics for resiliency in the presence of faults and attacks on the CPES in the emulated testbed environment.

5.3 Results

In our system, an independent system operator (ISO) broadcasts set-points to each of the generators and demand-response agents every Δt seconds (in this paper $\Delta t = 2$ seconds). Upon receiving their set-points, each generator and DR consumer responds to the ISO the power it can generate and the cost to generate the power. These quantities can be thought of as the marginal cost or marginal utility for each participant at the current set-point. Each generator and DR consumer is responsible for updating its own value cost based on cost curves that are known locally to the generator and demand response agents. The ISO is responsible for measuring system frequency, calculating ACE, and updating the generation of the collective system. Once the ISO receives a response from all the generators and demand response agents, the ISO has everything it needs to compute the next set of set-points and the process repeats. We emulate a period of 24 hours on the DETERLab testbed facility. We simulate the combined primary-secondary control system on a 118 bus grid. We create physical disturbance on the network which results in change in generation capability within the system. For example, faults could be modeled as a rapid drop in renewable generation, a sharp increase in conventional (inflexible) demand, or a generator tripping offline. Our test system is a modified IEEE 118-bus test case, of which 54 are generator buses and the other 64 are load buses modified with a certain amount of flexible consumption. Each bus also experiences a conventional, fixed demand P_L. The system contains a total of 186 transmission lines. Unless otherwise specified, system parameters are taken directly from the test files of MATPOWER. To analyze the resilience of the system, we run

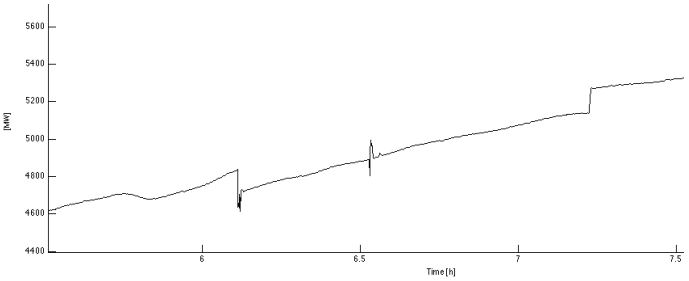

Figure 8: The load shedding at buses 26-28 to arrest the frequency dive and reconnection after lost generation is restored

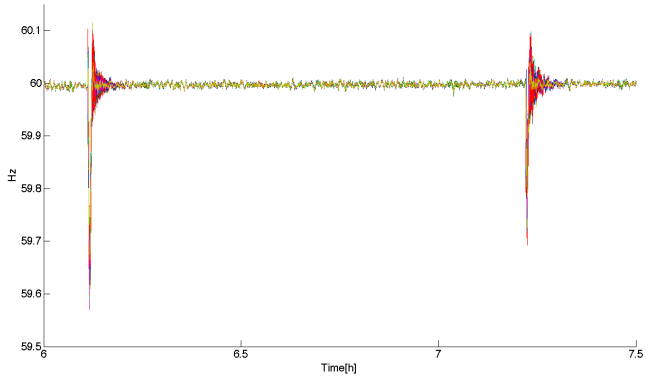

Figure 9: Generator 5 is removed from the market which causes the frequency to be stable during the attack.

two variations of a test. Initially the system is operating at equilibrium when a physical outage causes the generators 11 and 12 to be disconnected as seen in Fig. 10. The frequency starts diving rapidly and the system initially transitions to an alert state. Then, the system operator sheds the loads in the buses 26-28 (328 MW) as seen in Fig.8 causing the system to transition into an emergency state. The system operates in this state until, due to a cyber attack, Generator 5 loses communication with the ISO. This causes the CPES to transition into an extremis state. As shown earlier in Fig. 3, when this happens, the system is highly unstable and the the magnitude of the frequency oscillations increasing. As a resiliency control action, in the next variation, we remove Generator 5 from the dynamic market and observe the system becomes stable again as seen in Fig. 9. Finally, new generation is getting online and the lost load is reconnected. These two resilient control actions enable the system to transition from the restorative back to the normal operating mode (see Fig. 1). In this case study we choose a deterministic control action, first to load shed once generators 11 and 12 were lost and then to reconfigure the market participation once generator 5 was under attack. Each of these actions can be viewed, once again, as a suboptimal solution of (21) for the transition from the in-extremis to the emergency state.

6. Concluding Remarks

With the advanced sensing, communication and compu-

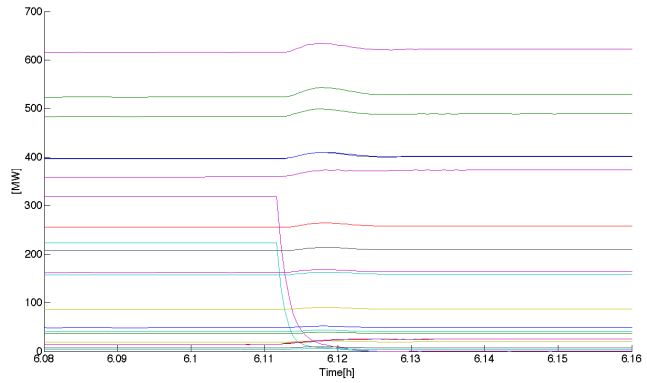

Figure 10: Physical anomaly: Generator 11 and 12 lose power

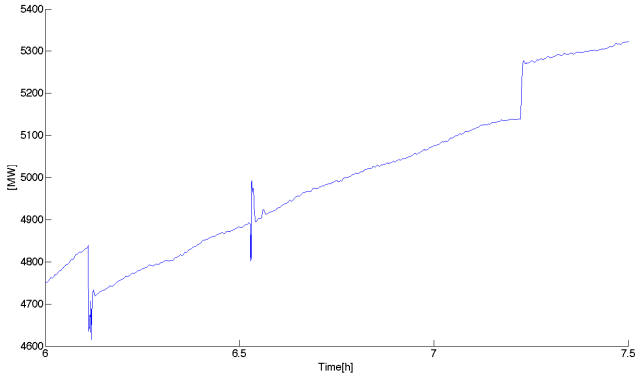

Figure 11: The total power generation shows loss of generation within the system when generators 11 and 12 shut down and the cyber attack starts at generator 5.

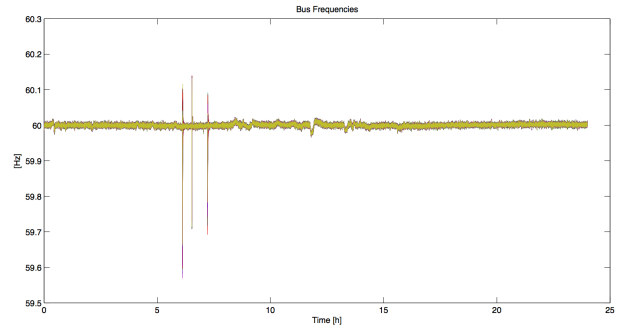

Figure 12: Frequency response under all three events

tation components of a Cyber-Physical System (CPS) intertwined with the physical components, CPS today are vulnerable to both cyber and physical faults. Consequently, resilience with respect to failures, induced in both the cyber and the physical worlds, emerges as a necessary aspect of their secure operation. In this paper, we develop a system-theoretic framework to address cyber-physical resilience that includes a definition of resilience, a resilience metric and a CPS modeling and optimal resilient control design methodology. The proposed framework is exploited to evaluate resilience of a smart Cyber-Physical Energy System (CPES) under both cyber and physical faults through DETERLab, a high fidelity simulations testbed for CPS. Critical scenarios with physical generator outages and cyber Denial of Service (DoS) attacks are constructed for a particular CPES comprised of 56 generators and 99 consumers which adopts our previously proposed Dynamic Regulation Market Mechanism (DRMM) [32, 33] at the secondary control level. The resilience and performance of the CPES under these scenarios and a specific hybrid resilient control strategy are evaluated.

7. REFERENCES

[1] M. N. Albasrawi, N.Jarus, K. A. Joshi, and S. S. Sarvestani. Analysis of Reliability and Resilience for Smart Grids. In *Proc. of 2014 IEEE 38th Annual Computer Software and Applications Conference (COMPSAC)*, 2014.

[2] A. M. Annaswamy. Vision for smart grid control: 2030 and beyond. *IEEE Standards Publication*, June 2013.

[3] A. M. Annaswamy, A. Hussain, A. Chakrabortty, and M. Cvetković. Foundations of infrastructure CPS. In *Proc. American Control Conference*, Boston, MA, July 2016. IEEE.

[4] A. M. Annaswamy, A. R. Malekpour, and S. Baros. Emerging Research Topics in Control for a Smart Infrastructure. *Journal of Annual Reviews of Control*, 2016.

[5] R. Arghandeh, A. von Meier, L. Mehrmanesh, and L. Mili. On the Definition of Cyber-Physical Resilience in Power Systems. http://arxiv.org/pdf/1504.05916v2.pdf.

[6] T. Benzel. The Science of Cyber Security Experimentation: The DETER project. *Annual Computer Security Applications Conference*, December 2011.

[7] D. C. Bergman. Power grid simulation, evaluation, and test framework. Master's thesis, University of Illinois at Urbana-Champaign, Urbana, Illinois, May 2010.

[8] A. A. Cardenas, S. Amin, and S. Sastry. Secure Control: Towards Survivable Cyber-Physical Systems. In *In Proceedings of the 28th International Conference on Distributed Computing Systems*, 2008.

[9] Andrew Davis. Developing SCADA simulations with c2windtunnel. Master's thesis, Vanderbilt University, Nashville, Tennessee, May 2011.

[10] The DETERLab Facilities. http://www.deter-project.org.

[11] DETER Resources. https://trac.deterlab.net/wiki/DeterResources.

[12] L. H. Fink and K. Carlsen. Operating under stress and strain [electrical power systems control under

emergency conditions]. *IEEE Spectrum*, 15(3):48–53, 1978.

[13] S. Floyd and E. Kohler. Internet Research Needs Better Models. *SIGCOMM Comput. Commun. Rev.*, 33:29–34, January 2003.

[14] A. Ghafouri, Waseem Abbas, Aron Laszka, Yevgeniy Vorobeychik, and Xenofon Koutsoukos. Optimal Thresholds for Anomaly-Based Intrusion Detection in Dynamical Environments.

[15] J. Hansen, J. Knudsen, and A. M. Annaswamy. A Dynamic Market Mechanism for Integration of Renewables and Demand Response. *IEEE Transactions on Control Systems Technology*, 24(3), 2016.

[16] S. Hedlund and A. Rantzer. Optimal control of hybrid systems. In *Proceeding of the 38th IEEE Conference on Decision and Control*, 1999.

[17] C. S. Holling. Resilience and Stability of Ecological Systems. *Annual Review of Ecology and Systematics*, 4:1–23, 1973.

[18] C. S Holling. Engineering Resilience versus Ecological Ressilience. *Engineering with Ecological Constraints*, 1996.

[19] W. H. Ip and D. Wang. Resilience and Friability of Transportation Networks: Evaluation, Analysis and Optimization. *IEEE Systems Journal*, 5(2):189 – 198, 2011.

[20] M. Kezunovic, A.M. Annaswamy, I. Dobson, S. Grijalva, D. Kirschen, J. Mitra, and L. Xie. Energy Cyber-Physical Systems: Research Challenges and Opportunities. Technical report, NSF, 2014.

[21] A. Khodaei. Resiliency-Oriented Microgrid Optimal Scheduling. *IEEE Transactions on Smart Grid*, 5(4):1584 – 1591, July 2014.

[22] A. Kiani, A. M. Annaswamy, and T. Samad. A hierarchical transactive control architecture for renewables integration in smart grids: Analytical modeling and stability. *IEEE Transactions on Smart Grid*, 5(4):2054–2065, 2014.

[23] H. Kitano. Biological robustness. *Nature Reviews*, 5:826–837, 2004.

[24] Idaho National Lab. Idaho National Lab SCADA Test Bed Program. https://www.inl.gov/research-program/critical-infrastructure-protection/.

[25] S. A. Levin and J. Lubchenco. Resilience, Robustness, and Marine Ecosystem-based Management. *BioScience*, 58(1):27–32, 2008.

[26] L. Mili. Taxonomy of the Characteristics of Power System Operating States. In *Proc. of 2nd NSF RESIN Workshop*, 2011.

[27] Yilin Mo, Rohan Chabukswar, and Bruno Sinopoli. Detecting Integrity Attacks on SCADA Systems. *IEEE Transactions on Control Systems Technology*, 22(4), July 2014.

[28] A. Ovens. What resilience means, and why it matters, January 2015. https://hbr.org/2015/01/what-resilience-means-and-why-it-matters.

[29] C. G. Rieger, D. I. Gertman, and M. A. McQueen. Resilient control systems: Next generation design research. In *Proc. of 2nd Conference on Human System Interactions*, pages 632 – 636, 2009.

[30] C. G. Rieger, K. L. Moore, and T. L. Baldwin. Resilient control systems: A multi-agent dynamic systems perspective. In *Proc. of International Conference on Electro/Information Technology (EIT)*, 2013.

[31] M. Rungger and P. Tabuada. A Notion of Robustness for Cyber-Physical Systems. *IEEE Transactions on Automatic Control*, 61(12):2108–2123, August 2016.

[32] D. J. Shiltz. Integrating automatic generation control and demand response via a dynamic regulation market mechanism. Master's thesis, Massachusetts Institute of Technology, 2016.

[33] D. J. Shiltz and A. M. Annaswamy. A Practical Integration of Automatic Generation Control and demand response. In *Proceedings of the American Control Conference*, 2016.

[34] D. J. Shiltz, Miloš Cvetković, and A. M. Annaswamy. An integrated dynamic market mechanism for real-time markets and frequency regulation. *IEEE Transactions on Sustainable Energy*, 7(2):875–885, 2016.

[35] Siddharth Sridhar, Adam Hahn, and Manimaran Govindarasu. Cyber–Physical System Security for the Electric Power Grid. *Proceedings of the IEEE*, 100(1), January 2012.

[36] P. Tabuada, S. Y. Caliskan, M. Rungger, and R. Majumdar. Towards Robustness for Cyber-Physical Systems. *IEEE Transactions on Automatic Control*, 59(12):3151–3163, December 2014.

[37] D. Wei and K. Ji. Resilient Industrial Control System (RICS): Concepts, Formulation, Metrics, and Insights. In *Proceedings of the International Symposium on Resilient Control Systems (ISRCS)*, 2010.

[38] Wikipedia. Metcalf sniper attack. https://en.wikipedia.org/wiki/Metcalf_sniper_attack.

[39] P. Wood, D. Shiltz, T.R. Nudell, A. Hussain, and A. M. Annaswamy. A Framework for Evaluating the Resilience of Dynamic Real-Time Market Mechanisms. *IEEE Transactions on Smart Grid*, 2016.

[40] O. Yagan, D. Qian, J. Zhang, and D. Cochran. Optimal Allocation of Interconnecting Links in Cyber-Physical Systems: Interdependence, Cascading Failures, and Robustness. *IEEE Transactions on Parallel and Distributed Systems*, 23(9), September 2012.

[41] J. Zhang, P. Jaipuria, A. Chakrabortty, and A. Hussain. Distributed Optimization Algorithm for Attack-Resilient Wide-Area Monitoring of Power Systems: Theoretical and Experimental Methods. *In Proceedings of GameSec Conference on Decision and Game Theory*, 2014.

[42] K. Zhou, J. Doyle, and K. Glover. *Robust and Optimal Control*. Prentice Hall, 1996.

[43] Q. Zhu and T. Basar. Robust and Resilient Control Design for Cyber-Physical Systems with an Application to Power Systems. In *Proc. of the 50th IEEE Conference on Decision and Control and European Control Conference*, 2011.