SAND2018-7729C

Measurement and Analysis of Cyber Resilience for Control Systems: An Illustrative Example

Nicholas Jacobs
Cyber Resilience R&D
Sandia National Laboratories
Albuquerque, USA
njacobs@sandia.gov

Shamina Hossain-McKenzie
Cyber Resilience R&D
Sandia National Laboratories
Albuquerque, USA
shossai@sandia.gov

Eric Vugrin
Cyber Resilience R&D
Sandia National Laboratories
Albuquerque, USA
edvugri@sandia.gov

***Abstract*—Control systems for critical infrastructure are becoming increasingly interconnected while cyber threats against critical infrastructure are becoming more sophisticated and difficult to defend against. Historically, cyber security has emphasized building defenses to prevent loss of confidentiality, integrity, and availability in digital information and systems, but in recent years cyber attacks have demonstrated that no system is impenetrable and that control system operation may be detrimentally impacted. Cyber resilience has emerged as a complementary priority that seeks to ensure that digital systems can maintain essential performance levels, even while capabilities are degraded by a cyber attack. This paper examines how cyber security and cyber resilience may be measured and quantified in a control system environment. Load Frequency Control is used as an illustrative example to demonstrate how cyber attacks may be represented within mathematical models of control systems, to demonstrate how these events may be quantitatively measured in terms of cyber security or cyber resilience, and the differences and similarities between the two mindsets. These results demonstrate how various metrics are applied, the extent of their usability, and how it is important to analyze cyber-physical systems in a comprehensive manner that accounts for all the various parts of the system.**

***Index Terms*—Cyber Security, Cyber Resilience, Cyber-Physical Systems, Control Systems, Load Frequency Control**

NOMENCLATURE

AMI	Advanced Metering Infrastructure.
DA	Distribution Automation.
CIA	Confidentiality, Integrity, Availability.
SAIDI	System Average Interruption Duration Index.
SAIFI	System Average Interruption Frequency Index.
CVSS	Common Vulnerability Scoring System.
ISC	Impact Subscore, part of the CVSS.
CERT	Computer Emergency Response Team.
CREF	Cyber Resilience Engineering Framework.
IRAM	Infrastructure Resilience Analysis Methodology.
SI	Systemic Impact.
TRE	Total Recovery Effort.
RDR	Recovery Dependent Resilience.
CA	Control Area.
LFC	Load Frequency Control.
BA	Balancing Authority.
SCADA	Supervisory Control and Data Acquisition.
PMU	Phasor Measurement Unit.
FNET	Frequency Monitoring Network.
AGC	Automatic Generation Control.
ACE	Area Control Error.
Δf	Frequency Deviation
ΔP	Power Deviation
v_i	Area Interface
$w(t)$	System Noise
$v(t)$	Measurement Noise
T_{Delay}	Communication delay
DOS	Denial of Service.

This paper describes objective technical results and analysis. Any subjective views or opinions that might be expressed in the paper do not necessarily represent the views of the U.S. Department of Energy or the United States Government. Sandia National Laboratories is a multi-mission laboratory managed and operated by National Technology and Engineering Solutions of Sandia LLC, a wholly owned subsidiary of Honeywell International Inc. for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525.

I. INTRODUCTION

Automated control systems are integral parts of modern infrastructure and have enabled enormous gains in operational capabilities. Increasingly, interconnected power grid infrastructure leverages smart grid technologies such as Advanced Metering Infrastructure (AMI) and Distribution Automation (DA) to further advance efficiencies and control [1]. However, modern control systems are truly cyber-physical systems because they have digital components that control physical processes, which means that the infrastructure community is becoming increasingly concerned about the risks that cyber threats pose to control systems and the infrastructure they support. For instance, malware such as Stuxnet, BlackEnergy, Crashoverride, and Trisis/Trident have been specifically designed and used to attack and cripple control systems [2]–[6]. These attacks have not only increased concerns about cyber risks for control systems but they have also spurred the control community to reconsider cyber security strategies.

Cyber resilience has recently emerged as a strategy that complements security efforts and contributes to cyber risk management. Whereas cyber security activities frequently aim to prevent failures to maintain Confidentiality, Integrity, and Availability (CIA), cyber resilience efforts recognize that it is impossible to guarantee prevention of system degradation

against all cyber attacks. In the event of an attack, cyber resilience efforts aim to ensure essential operations; maintain critical function levels; and rapidly recover. Given that it is impossible to guarantee a network can never be penetrated, cyber resilience efforts frequently do not focus on whether an attack can happen and instead focus on how to react when they do occur. Cyber resilience is especially relevant to control systems and other cyber-physical systems because cyber failures can manifest with immediate and significant physical effects. Policy directives such as Executive Order 13636 "Improving Critical Infrastructure Cybersecurity" and Presidential Policy Directive 21 are evidence of this increasing recognition of the need for system resilience to cyber attacks [7], [8].

Despite the increasing prioritization of resilience, formal approaches for understanding, analyzing, and improving resilience of control systems remain relatively new and under development. These approaches must consider both cyber and physical elements and demonstrate how degradation in one domain affects the other. Ideally, these methods include metrics that enable quantitative analysis and assist system designers, analysts, and decision makers in measuring how resilient their systems truly are. This paper describes a multi-disciplinary approach that integrates information security and control theory to quantify the resilience of control systems to cyber attacks. The remainder of the paper is organized as follows. Section II. describes related metrics for evaluating cyber threats to cyber systems, including metrics previously developed by Biringer et al. to quantify resilience in infrastructure systems [9]. Section III. introduces a notional power system model and how the metrics of Biringer et al. can be extended to measure cyber resilience of the system when under various cyber attacks on the control system. Section IV. details results for quantifying the resilience of the system and compares those results with security metric evaluations. Section V. concludes the paper by discussing opportunities for further maturing and extending this approach.

II. Cyber Metrics for Evaluating Control and Related Systems

Reliability metrics such as System Average Interruption Duration Index (SAIDI) and System Average Interruption Frequency Index (SAIFI) that measure an infrastructures ability to provide continuous delivery of services (both in quantity and quality) have traditionally been the primary measure for evaluating infrastructure operations [10]. These metrics consider infrastructure to be of a binary nature (i.e., infrastructure is either in a reliable or unreliable state) and require that a specific, restrictive set of conditions be met to apply them. For example, low probability, high-consequence events such as hurricanes, cyber attacks, and other acts of god violate these conditions, invalidating the use of reliability metrics for these situations. Numerous cyber security metrics have been developed in part to address this gap and have been proposed with various goals and use cases. These metrics frequently focus on confidentiality and integrity of data and availability of services. Many focus on basic cyber hygiene (e.g., percentage of users with strong passwords) or the effectiveness of security controls (i.e., firewalls) while others use modeling to evaluate security [11], [12]. Many cyber security metrics have been developed for Information Technology (IT) systems, but these approaches are not directly applicable to cyber-physical control systems [13], [14].

For example, one approach widely used in the field of cyber security is the Common Vulnerability Scoring System (CVSS), which is used to grade the severity of vulnerabilities after they have been discovered [15]. This provides a way to prioritize patching and mitigation efforts so that the most critical vulnerabilities are given priority. The CVSS does this grading through a combination of pre-defined weights and subject matter expert judgment to quantify exploitability and impact for a specified vulnerability and provide an overall score for the criticality of the vulnerability. For example, calculation and weights for the Impact Subscore (ISC) is shown in Equation (1) with numerical values assigned to each impact rating as shown in Table I. We mention the ISC specifically because we will by utilizing it in Section IV to grade the impact of various scenarios to the security of our example system and compare its results with a resilience based scoring approach.

$$ISC_{Base} = 1 - [(1 - Impact_{Conf}) \times (1 - Impact_{Integ}) \times (1 - Impact_{Avail})] \quad (1)$$

TABLE I
ISC Impact

Impact Rating	Numerical Value
None	0.00
Low	0.22
High	0.56

Cyber security efforts frequently focus on controlling access into a system and maintaining CIA. However, they often provide little information on how to plan for or respond to a successful breach of security measures so cyber resilience metrics have received increasing attention to address that gap. The majority of infrastructure resilience analyses and metrics developed over the past 20 years has focused on natural disasters and random events, but several cyber-specific resilience metrics and analysis methods are becoming more prevalent. Though C. S. Holling first introduced resilience as a property of ecosytems and complex systems more than 40 years ago [16], resilience has only emerged as a significant topic of discussion in the national security community over the past 15 years. During that period, a variety of resilience metrics have been proposed, especially for critical infrastructure systems (e.g., see [17], [18], and [19]). Biringer et al. provide an extensive overview of resilience metrics in Chapter 9 of [9]. However, due to the ubiquitous reliance of the electrical power community on reliability as the key measure of grid performance, resilience is relatively new as a performance metric for the grid. Initial grid resilience metrics and analyses

have focused extreme weather and natural disasters (e.g., see [20], [21]), but growing concerns about cyber threats have spurred the development of cyber resilience metrics.

Many cyber resilience metrics are intended to evaluate organizational readiness or potential network designs. One example is the CERT Resilience Management Model, which includes metrics for measuring resilience at organizational levels [22]. MITRE's Cyber Resilience Engineering Framework (CREF) uses qualitative values (very low, low, medium, high, very high) to evaluate cyber resilience goals, objectives, and techniques [23], [24]. DiMase et al.'s cyber physical systems security framework uses a semi-quantitative scorecard to evaluate operational, functional, and architectural levels in critical assets, command and control functions, and cyber physical systems [25], and Linkov et al. describe a cyber resilience matrix with potential metrics that measure a systems ability to plan, absorb, recover, and adapt in physical, information, cognitive, and social domains [26].

Alternatively, another class of metrics use system performance to quantify resilience. Albasrawi et al. use instantaneous measures of cyber resilience in smart grids that compare current functionality of the smart grid relative to catastrophic functionality levels ($[F(t) - F(t_d)]/[F(t_0) - F(t_d)]$) to identify optimal recovery strategies [27]. Clark and Zonouz define game theoretic resilience metrics to develop cyber defense policies that ensure resilience conditions in power systems [28]. Hassel et al. use a set of cyber attack (e.g., percentage of successful attacks, duration of successful attack) and defense measures (e.g., mean number of attack disruptions, defensive efficiency, etc.) to quantify resilience of military systems [29]. Rieger uses a "disturbance and impact resilience evaluation curve" to describe how a cyber attack affects operation of control systems. Rieger defines a set of resilience metrics as properties of the curve (e.g., agility is the derivative of the curve, brittleness is the area under the disturbance curve as intersected by the resilience threshold, etc.) [30]. Wei and Ji use a set of metrics that measure cyber resilience according to the consequence of a cyber attack (e.g., performance degradation and loss) and time (e.g., protection time, recovery time) [31]. Choudury et al. use graph theoretic approaches to integrate latency, authentication request frequency, and other network statistics into a quality of service metric for cyber resilience [32], and Ramuhalli et al.'s metrics focus on continuity of operations, reconstitution of systems, and attacker and defender costs [33].

Though not specifically developed for cyber analysis, the Infrastructure Resilience Analysis Methodology (IRAM) uses a control theoretic approach for quantifying resilience in infrastructure and other systems and has been hypothesized as an approach for quantifying cyber resilience for control systems. The IRAM includes three sets of metrics. Systemic Impact (SI) measures the magnitude and duration of performance loss resulting from an attack, and Total Recovery Effort (TRE) quantifies the resources and associated costs required to fight through the attack and return the system to acceptable performance levels. The Recovery Dependent Resilience (RDR) index combines SI and TRE to provide a comprehensive measure of the impact on the system. Larger RDR values indicate greater impact and thus, lower resilience levels (see Chapter 10 of Biringer et al. for a more detailed description) [9]. Control systems are commonly designed with performance and cost trade-off considerations, so the IRAM metrics show promise for cyber resilience measurement and analysis of control systems. The remaining sections explore how they could be used in the context of an illustrative example.

III. Load Frequency Control: A Control System Example

Consider a notional three-bus power system defined by Bevrani and that consists of nine generators distributed across three connected Control Areas (CA) as shown in Figure 1; we focus on the secondary control loop, which performs Load Frequency Control (LFC) (Figure 2) [34], and assume a representative but simplified control system that does not include fast dynamics (e.g., voltage) or nonlinearities. LFC is an important capability for Balancing Authorities (BAs) who are responsible for integrating resources and maintaining load-generation balance for specific areas. Furthermore, BAs are responsible for regulating and stabilizing system frequency—which is an crucial function of LFC. Additionally, we consider the architecture for this example to be the typical Supervisory Control and Data Acquisition (SCADA) system that enables monitoring and control of a variety of devices and components in the grid. Frequency is often a measure of mismatch between the demand and generation, which can be calculated with the SCADA system data. Phasor Measurement Units (PMUs) or Frequency Monitoring Network (FNET) sensors could also be used to obtain frequency measurements for LFC calculations.

Notably, protective measures such as relays are not included in this model which means that actions to limit damage to components are not included in this analysis. Note that as each CA is controlled separately, there is a separate LFC controller for each CA. This results in a three sets of coupled differential equations that are connected through the power flows that exist between the control areas.

In this example, we are primarily interested in the performance of the secondary control loop. The primary controller doing Automatic Generation Control (AGC) for each generator, represented as C_{AGC} in 2, is internal to the dynamics of the secondary controller and is included as part of the state transition matrix $\mathbf{A}$. In each CA the control system is designed to maintain system frequency and tie-line power flows at specified levels (e.g., 60 Hz for frequency), and the equations describing the dynamics for each control area can be written in the general state-space form shown in Equation (2) and with the system state variables shown in Equation (3). The state for each CA, $\mathbf{x}$, is a vector consisting of deviations from the target frequency (Δf), deviation from target power levels (ΔP), and the area control error ACE, defined in Equation (4). The LFC controller uses ACE along with Proportional-Integral (PI) control to calculate the secondary control output

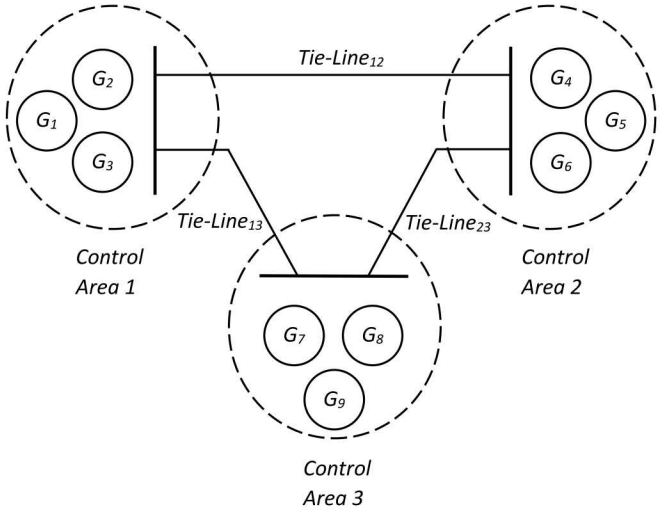

Fig. 1. Example 3-Area Power System, adapted from [34]

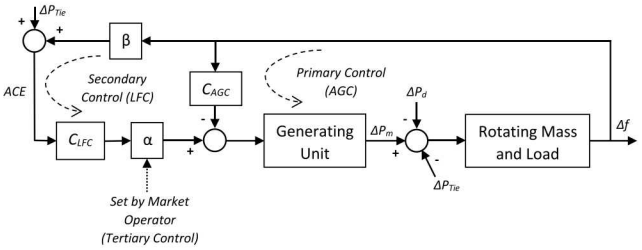

Fig. 2. Power System Frequency Control, adapted from [34]

$u(t)$, as shown in Equation (6) with gains defined in the matrix $\mathbf{K}$, as shown in Equation (5).

$$\begin{aligned}\dot{\mathbf{x}}(t) &= \mathbf{A}\mathbf{x}(t) + \mathbf{B}\mathbf{u}(t) + \mathbf{w}(t)\\ \mathbf{y}(t) &= \mathbf{C}\mathbf{x}(t) + \mathbf{D}\mathbf{u}(t) + \mathbf{v}(t)\end{aligned} \tag{2}$$

$$\mathbf{x}(t)^T = \big[\ \Delta f\ \Delta P_{Tie}\ \Delta P_{m1}\ \Delta P_{m2}\ \Delta P_{m3}\ \Delta P_{g1}\ \Delta P_{g2}\ \Delta P_{g3}\big] \tag{3}$$

$$ACE = \beta\Delta f + \Delta P_{Tie} \tag{4}$$

$$\mathbf{K}^T = \begin{bmatrix}0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & k_p & k_i\end{bmatrix} \tag{5}$$

$$u(t) = -\mathbf{K}\mathbf{y}(t - T_{Delay}) \tag{6}$$

We introduce the T_{Delay} term to represent conditions that introduce latency into the control system. In most instances, T_{Delay} = 2 seconds, to represent some communications delay from the wide area network even under normal conditions.

Note that the power flows across each tie-line are calculated using the area interface, v_i, which links the CAs to each other. The area interface for each control area is calculated in Equation (7), see Chapter 3 of [34] for further details (e.g., parameter settings).

$$v_i = \sum_{j=1, j\neq i}^{N} T_{ij}\Delta f_j \tag{7}$$

We consider a set of attack scenarios that compromise confidentiality, integrity, and/or availability of the control system in Table II. Scenario 1 is the nominal no attack scenario. Scenarios 2 and 3 represent denial of service (DOS) attacks, and we represent the effect of those attacks by setting T_{Delay} to low (8 s in S_2) and high (24 s in S_3) values. Scenarios 3 and 4 represent signal jamming attacks, and we represent the effect of those attacks by injecting zero-mean Gaussian white noise with low (P_n = 0.25 in S_4) and high (P_n = 0.75 in S_5) power levels into the system using our measurement noise $v(t)$ in Equation (2). In Scenarios 6 and 7, we assume a loss of confidentiality provides the adversary with sufficient knowledge to cause a loss of availability by disabling 1 (low in S_6) or 2 (high in S_7) generators, and we represent this effect by modifying $\mathbf{B}$ in Equation (2). Scenarios 8 and 9 represent confidentiality breaches that lead to losses of integrity; specifically, we assume that the adversary uses knowledge of the control system and access to the measurement signals of the secondary control loop to degrade performance, resulting in changes to $\mathbf{C}$.

We evaluate the impact on the control system using the CVSS ISC and IRAM metrics, as our security and resilience measurements. CVSS ISC calculations are performed according to Equation (1) with the CIA weights assigned according to the previously presented impact ratings as shown in Table I. For the IRAM metrics, we have elected to use the squared error, ACE^2 (relative to ACE^2 in the absence of an attack), and the amount of control expended, u^2 (relative to u^2 in the absence of an attack), to represent as the system performance and cost measures for responding to the attack. IRAM metrics for SI, TRE, and RDR are calculated according to Equations (8), (9), and (10). Note that while we give SI and TRE equal weighting in Equation (10) for this study, the relative weighting of these two terms may be varied according to the analysts risk perspective. Also, the variable s_n specifies the attack scenario, with n = the scenario number as shown in Table II. Note the similarity of these quantities to optimal control formulations such as the Linear Quadratic Regulator and Linear Quadratic Gaussian problems, which both aim to minimize the L2 norm of the tracking error and control effort.

$$SI(s_n) = \sum_{i=1}^{3}\left[\int_0^{100} ACE_i^2(t, s_n)dt - \int_0^{100} ACE_i^2(t, s_1)dt\right] \tag{8}$$

$$TRE(s_n) = \sum_{i=1}^{3}\left[\int_0^{100} u_i^2(t, s_n)dt - \int_0^{100} u_i^2(t, s_1)dt\right] \tag{9}$$

TABLE II
SCENARIO DESCRIPTIONS: C = CONFIDENTIALITY, I = INTEGRITY, A = AVAILABILITY

Scenario	Scenario Type	Definition	Modification to System
S_1	Baseline	Normal Behavior	N/A
S_2	Loss to A, Low	DOS to Communications, Latency / Time Delay	T_{delay} = 8 seconds
S_3	Loss to A, High	DOS to Communications, Latency / Time Delay	T_{delay} = 24 seconds
S_4	Loss to I, Low	Signal Jamming, Addition of Zero-Mean Gaussian White Noise	P_n = 0.25
S_5	Loss to I, High	Signal Jamming, Addition of Zero-Mean Gaussian White Noise	P_n = 0.75
S_6	Loss to C & A, Low	Loss of Generation Capability, Tripping of Relays / Disabling Power Generation	CA 2 Loses 1 Generator
S_7	Loss to C & A, High	Loss of Generation capability, Tripping of Relays / Disabling Power Generation	CA 2 Loses 2 Generators
S_8	Loss to C & I, Low	Manipulation of Measurement Signals for LFC	ACE_2 = 0
S_9	Loss to C & I, High	Manipulation of Measurement Signals for LFC	$ACE_{2,obs} = -ACE_{2,actual}$

$$RDR(s_n) = SI(s_n) + TRE(s_n) \tag{10}$$

$$w_1(t) = \begin{cases} 0 & t < 10 \\ \alpha & t \geq 10 \end{cases} \tag{11}$$

In every simulation, we apply a step load change at t = 10 seconds of α = 0.1 p.u. by modifying $w(t)$ for CA 1 and CA 2 as shown in Equation (11). Since this change in load is affects the system behavior by creating a drop or increase in system frequency, this added load is modeled as a disturbance only to the first element of $w(t)$, as this is the element that will affect the state variable for system frequency. Then, each cyber attack commences by modifying system parameters at t = 20 seconds and ends at t = 80 seconds. At the time the cyber attack ends, the system will revert to conditions with no system degradation but the load of α = 0.1 p.u. will remain for CA 1 and CA 2.

IV. RESULTS & DISCUSSION

Table III shows the results of the SI, TRE, RDR, and ISC calculations for the nine attack scenarios. Lower ranks imply lower attack impacts with respect to either the IRAM RDR or ISC metrics, as shown.

Some similarities can be observed between the IRAM and CVSS rankings. Scenarios 2 and 4 (low latency and low noise) are ranked as the least impactful attacks, and Scenarios 7 and 9 (high loss of confidentiality resulting in loss of availability and integrity) are ranked as the two most impactful attacks. Some notable differences can be observed though, especially for Scenario 8. According to the IRAM RDR metric, Scenario 8 is the 3rd worst scenario, but it is the 3rd least impactful scenario according to the CVSS metrics. Additional minor ranking discrepancies can be seen for Scenarios 5 and 6. Further inspection of the IRAM metrics provides additional insights. The SI, TRE, and RDR results for Scenario 9 are two orders larger than those for Scenario 7, indicating the attack for Scenario 9 is far more impactful and expensive than the attack for Scenario 7. From a resilience perspective, Scenario 9 is far and away the worst scenario and should be prioritized over Scenario 7 for addressing.

Additionally, one can observe that the jamming attacks (Scenarios 4 and 5) have almost no effect on the end performance of the control system (SI is practically 0); the primary effect of these attacks is to increase the amount of control effort required. This controller can still operate effectively in the presence of noise, so the control scheme provides an inherent level of resilience against these attacks. In contrast, the impacts of the DOS attacks in Scenarios 2 and 3 equally affect performance and the cost of responding to the attack, i.e., SI and TRE are approximately equal. Given the nature of the CVSS ISC metrics and their intended use, they provide limited information about the resilience of this control system to the specified attacks. The IRAM metrics provide additional insights that can be informative when analyzing resilience of control systems.

As Scenario 1 is the baseline of normal behavior, it has no loss to security as represented by an ISC score of 0. However, as we are doing active load tracking and an unexpected load has been added to the system, there is some cost associated with normal error tracking and control. This would be representative of the regular costs of doing business, wear and tear on the system components, and other aspects of doing business in a regular day to day environment. This baseline behavior under normal conditions is shown in Figure 3. Note that in our calculation of SI, TRE, and RDR, we have removed these "normal" costs from the results of all scenarios. This means our resilience costs only measure the impact of the cyber event in each individual scenario.

Recall that Scenarios 2 and 3 represent a loss of availability by increasing amounts of time delay in the measurement communications. To further examine how varying levels of

TABLE III
SIMULATION RESULTS

Scenario	SI	TRE	RDR	ISC	Rank (IRAM)	Rank (ISC)
S_1	0.000	0.000	0.000	0.00	1	1
S_2	0.096	0.102	0.198	0.22	3	2
S_3	0.617	0.673	1.290	0.56	5	6
S_4	0.003	0.100	0.103	0.22	2	2
S_5	0.011	0.297	0.308	0.56	4	6
S_6	0.281	1.489	1.770	0.3916	6	4
S_7	2.213	5.729	7.942	0.8064	8	8
S_8	2.103	1.573	3.677	0.3916	7	4
S_9	269.378	187.315	456.693	0.8064	9	8

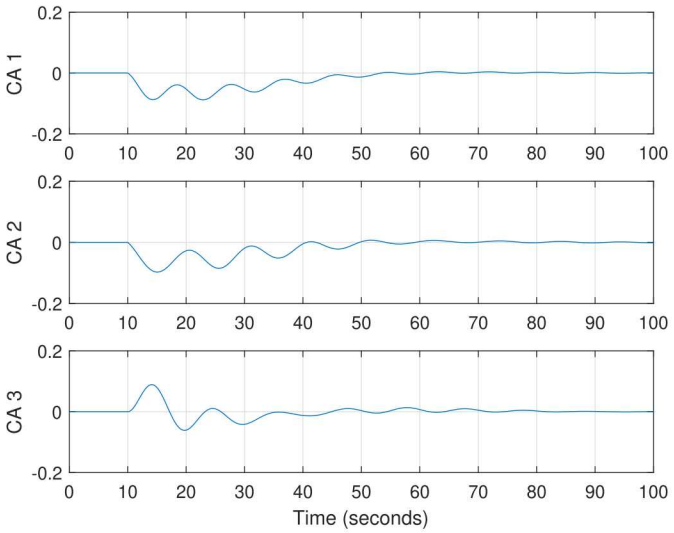

Fig. 3. ACE under Normal Behavior with a Step Load Disturbance at t=10 seconds

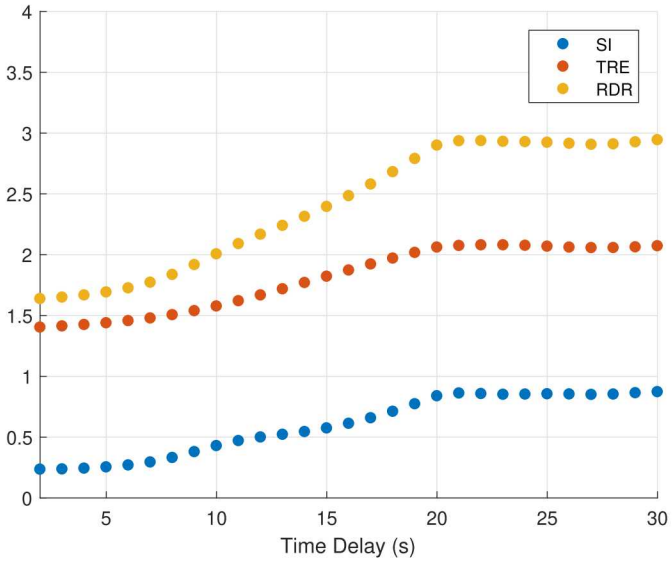

Fig. 4. Resilience costs with various amounts of time delay and a step load change at 20 seconds

time delay affect the performance of this system, several experiments were run where the amount of latency is varied substantially. As may be observed in Figure 4, the resulting performance trend is nonlinear but has several regions with differing behavior. First, as time delay increase so does SI, TRE, and RDR, as would be expected with higher amounts of phase lag between the reported and actual signals. Up to about 20 seconds of delay the cost to resilience increases steadily, but after 20 seconds the cost begins to taper off as the system is only responding to a single step change in load and is not performing additional load tracking. However, if further system disturbances are adding to create more realistic load tracking, the resilience costs should continue to increase. To demonstrate this, see Figure 5 where an additional step load is added at t=40 seconds.

Figure 6 shows a similar result where various levels of measurement noise are applied. Here, the SI, TRE, and RDR costs all increase linearly, but the value of SI increases very slowly. TRE does increase more rapidly, but not enough to correspond with relatively large changes in the ISC score. This shows how the LFC system is robust to measurement noise but must expend significantly more effort to maintain performance.

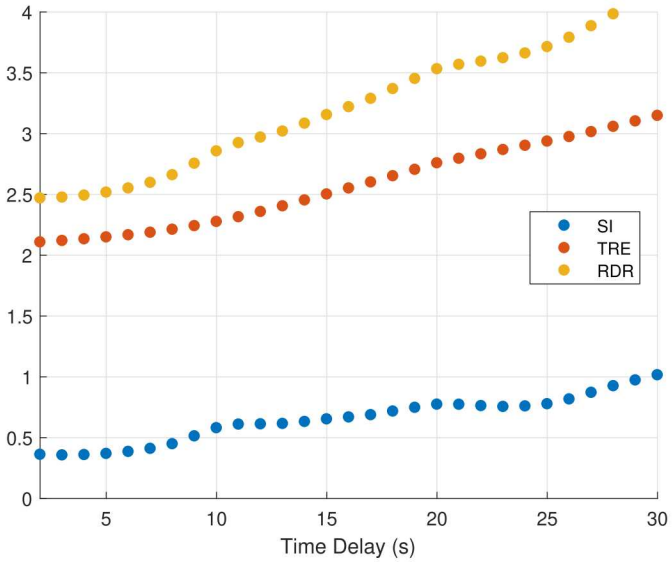

Fig. 5. Resilience costs with various amounts of time delay and a step load change at 20 seconds

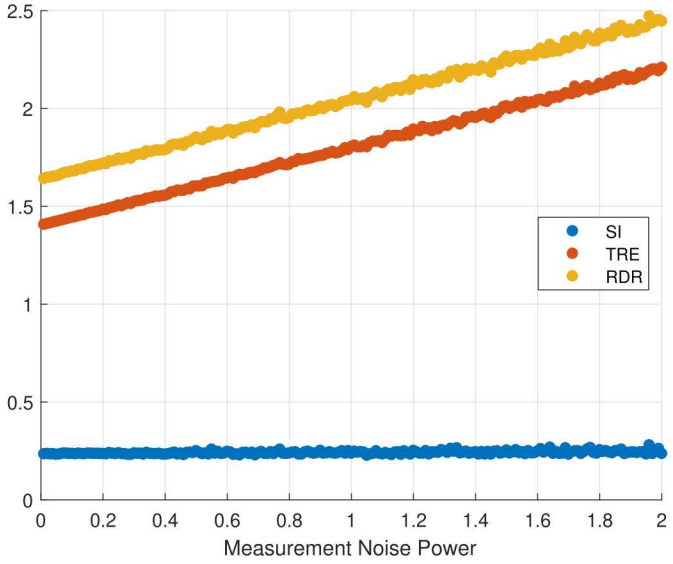

Fig. 6. Resilience costs with various amounts of measurement noise

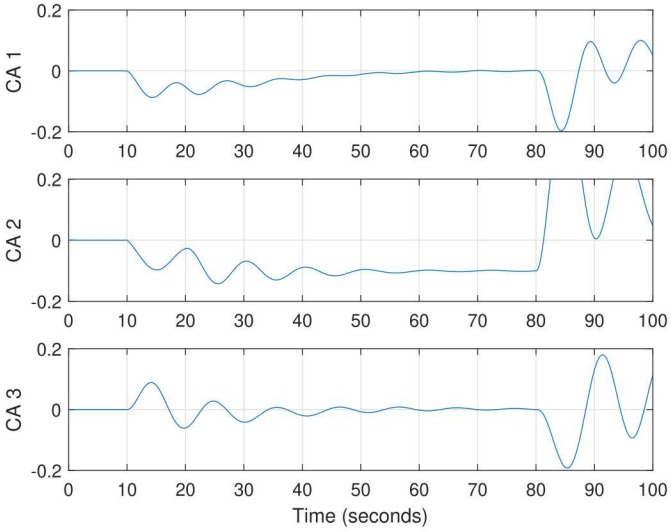

Fig. 7. ACE under Scenario 7 - Loss of Controllability

As Scenarios 6-9 also contain a loss of confidentiality, they all result in higher resilience costs than Scenarios 1-5, with a small anomaly of SI for Scenario 6 being lower than SI for Scenario 3 yet still having a higher cost These higher resilience costs map to the more sophisticated actions that also create greater resilience costs. In comparing Scenario 6 to Scenario 7, we note a very large increase to resilience cost, and a corresponding large increase in security cost. There is also a difference here concerning the controllability of CA 2. Controllability and observability are concepts referring to a systems ability to control and observe its internal state. For a system to be controllable, it must be possible for system inputs to move the states of the systems to any location in the state-space in finite time. For a system to be observable, it must be possible to determine the current state using system outputs in finite time. In Scenario 6, generation capability is lost as represented by modifications to $\mathbf{B}$. However, the system remains fully controllable. Yet, in Scenario 7, both the operating generators in CA 2 are disabled (the third generator is in reserve and is not supplying power), at which point the rank of the controllability matrix for CA 2 becomes zero. In other words, this scenario causes the LFC to lose all ability to control this system. Figure 7 shows this result where CA 2 is not able to recover and reaches a new steady state condition until the cyber event ends.

This is an extreme case: in a real-world environment with thousands of generators, it is highly unlikely one could knock all of them off the grid at once. Islanding conditions are another story though, and research has been done to show how controllability analysis may be used to determine critical components of the grid [35]. Specifically, by processing controller/component sensitivities with clustering and factorization techniques, the components that are critical, essential, or redundant to the overall system controllability are identified. A critical component is necessary for maintaining system control and has no replacement, an essential one is needed for controllability but may be replaced with redundant controller(s), and a redundant controller can be removed without impacting system control. Therefore, in the case of maintaining generation, the loss of critical generators would impact generation levels whereas loss of non-critical generators would not. These roles would change as these losses are incurred and, thus, must be recalculated (though recurrent roles are often discovered for different system conditions, as revealed in [36], [37]).

In Scenarios 8 and 9, the controllability of the system is not an issue but rather the observability of the system is affected. This is seen in Scenario 8, where the adversary has modified the structure of $\mathbf{C}$ by zeroing the feedback to the controller resulting in a loss of rank for the observability matrix. As seen in Figure 8, this results in a similar response to the loss of controllability seen in Figure 7. Incidentally, Scenario 9 does not affect the observability of the system as it does not modify the structure of $\mathbf{C}$, but rather changes the signs of elements inside $\mathbf{C}$. Yet, Scenario 9 is by far the scenario with the highest resilience costs as it is driving the system away from desired operating conditions. While this scenario is tied with Scenario 7 with the highest ISC score of 0.8064, ISC does not show the very large difference in resilience costs and system performance between the two scenarios.

This shows some of the limits to this method of grading cost. That is, the security is graded on a qualitative scale based on the believed cost to the system while the resilience measures only care about system performance. An example of these differences is demonstrated by Scenarios 6 and 8 having lower security costs than Scenarios 3 and 5, even though the resilience costs show these latter cases to be more costly. This demonstrates how security and resilience see these problems differently, how they are complementary ways of looking at this type of problem, and that further work needs to be

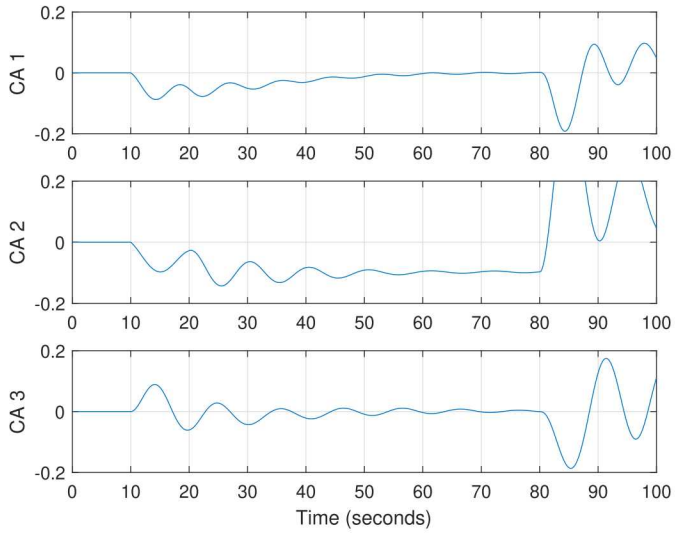

Fig. 8. ACE under Scenario 8 - Loss of Observability

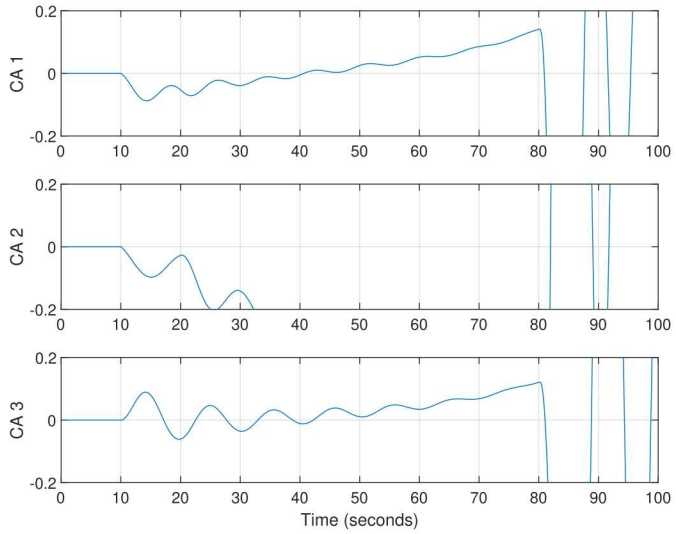

Fig. 9. ACE under Scenario 9 - Loss of Feedback Signal Integrity

completed to achieve a comprehensive approach in evaluating the overall impact of a cyber event.

V. Conclusion

In dealing with control systems, it is important to show both the cyber and physical effects and how various actions are represented and measured in both domains. By studying the security and resilience of grid frequency control, variations between the results of different metrics demonstrate how various measures and approaches have their places in a comprehensive assessment of a system yet each on their own fail to capture the entire picture. For instance, ISC is a security metric and is designed within that context while IRAM comes from study into infrastructure resilience and is solely interested in the ability of the system to meet its objectives and recover from performance degradation. These are different yet complementary ways of looking at this problem, especially when dealing with systems that cross both the cyber-physical domains, and this work shows how deeper insights can be gleaned about the system through inclusion of additional resilience analysis.

The construction of the scenarios and their manipulations in the system equations within this work is rather *ad hoc*, as categorizing cyber events and their impact on a control system is a difficult problem and such discussion is beyond the scope of this work. Further work may extend this by more clearly delineating how cyber attacks appear in and modify these models, which could leverage extensive existing research in such fields as complex systems, cyber-physical systems, and hybrid systems.

References

[1] C. Hawk and A. Kaushiva, "Cybersecurity and the Smarter Grid," *The Electricity Journal*, vol. 27, no. 8, pp. 84–95, Oct. 2014. [Online]. Available: http://dx.doi.org/10.1016/j.tej.2014.08.008

[2] N. Falliere, L. O. Murchu, and E. Chien, *W32.Stuxnet Dossier*. Symantec Security Response, Feb. 2011.

[3] D. Kushner, *The Real Story of Stuxnet*, Feb. 2013. [Online]. Available: https://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet

[4] R. M. Lee, M. J. Assante, and T. Conway, *Analysis of the Cyber Attack on the Ukrainian Power Grid*. SANS Industrial Control Systems, Mar. 2016.

[5] *CRASHOVERRIDE, Analysis of the Threat to Electric Grid Operations*. Dragos INC, 2017. [Online]. Available: https://dragos.com/blog/crashoverride/CrashOverride-01.pdf

[6] *TRISIS, Analysis of Safety System Targeted Malware*. Dragos INC, Dec. 2017. [Online]. Available: https://dragos.com/blog/trisis/TRISIS-01.pdf

[7] *Executive Order 13636 Improving Critical Infrastructure Cybersecurity*. The White House, Office of the Press Secretary, Feb. 2013. [Online]. Available: https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity

[8] *Presidential Policy Directive Critical Infrastructure Security and Resilience*. The White House, Office of the Press Secretary, Feb. 2013. [Online]. Available: https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil

[9] B. E. Biringer, E. D. Vugrin, and D. E. Warren, *Critical Infrastructure System Security and Resiliency*. CRC Press, 2013.

[10] A. Clark-Ginsberg, "What's the Difference between Reliability and Resilience," Stanford University, Tech. Rep., 2016.

[11] G. Stoneburner, *NIST Special Publication 800-33 Underlying Technical Models for Information Technology Security*. National Institute of Standards and Technology, Dec. 2001.

[12] W. Jansen, *NISTIR 7564 Directions in Security Metrics Research*. National Institute of Standards and Technology, Apr. 2009.

[13] A. McIntyre, B. Becker, and R. Halbgewachs, "Security Metrics for Process Control Systems," Sandia National Laboratories, Sandia Report SAND2007-2070P, Sep. 2007.

[14] *A Framework for Assessing and Improving the Scurity Posture of Industrial Control Systems (ICS)*. National Security Agency, Aug. 2010.

[15] *Common Vulnerability Scoring System v3.0: Specification Document*. FIRST. [Online]. Available: https://www.first.org/cvss/cvss-v30-specification-v1.8.pdf

[16] C. Holling, "Resilience and stability of ecological systems," *Annual Review of Ecology and Systematics*, vol. 4, pp. 1–23, 1973.

[17] M. Bruneau, S. Chang, R. Eguchi, G. Lee, T. ORourke, A. Reinhorn, M. Shinozuka, K. Tierney, W. Wallace, and D. von Winterfeldt, "A Framework to Quantitatively Assess and Enhance the Seismic Resilience of Communities," *Earthquake Spectra*, vol. 19, no. 4, pp. 733–752, 2003.

[18] E. D. Vugrin and R. C. Camphouse, "Infrastructure resilience assessment through control design," *Int. J. Critical Infrastructures*, vol. 7, no. 3, pp. 243–260, 2011.

[19] R. Fisher and M. Norman, "Developing measurement indices to enhance protection and resilience of critical infrastructures and key resources," *Journal of Business Continuity and Emergency Planning*, vol. 4, no. 3, pp. 191–206, 2010.

[20] J.-P. Watson, R. Guttromson, C. Silva-Monroy, R. Jeffers, K. Jones, J. Ellison, C. Rath, J. Gearhart, D. Jones, T. Corbet, C. Hanley, and L. Walker, *Conceptual Framework for Developing Resilience Metrics for the Electricity, Oil, and Gas Sectors in the United States*. Sandia National Laboratories, Sep. 2014.

[21] E. Vugrin, A. Castillo, and C. Silva-Monroy, *Resilience Metrics for the Electric Power System: A Performance-Based Approach*. Sandia National Laboratories, Feb. 2017. [Online]. Available: http://prod.sandia.gov/techlib/access-control.cgi/2017/171493.pdf

[22] R. A. Caralli, J. H. Allen, D. W. White, L. R. Young, N. Mehravari, and P. D. Curtis, "CERT Resilience Management Model, Version 1.2," Feb. 2016.

[23] D. J. Bodeau and R. Graubart, *Cyber Resiliency Engineering Framework*. MITRE Corporation, Sep. 2011. [Online]. Available: https://www.mitre.org/sites/default/files

[24] D. J. Bodeau, R. D. Graubart, and E. R. Laderman, "Cyber Resiliency Engineering Overview of the Architectural Assessment Process," *Procedia Computer Science*, vol. 28, pp. 838 – 847, 2014. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S187705091400163X

[25] D. DiMase, Z. Collier, K. Heffner, and I. Linkov, "Systems engineering framework for cyber physical security and resilience," *Environment Systems and Decisions*, vol. 35, no. 2, pp. 291–300, Jun. 2015.

[26] I. Linkov, D. Eisenberg, K. Plourde, T. Seager, J. Allen, and A. Kott, "Resilience metrics for cyber systems," *Environment Systems and Decisions*, vol. 33, pp. 471–476, 2013.

[27] M. N. Albasrawi, N. Jarus, K. A. Joshi, and S. S. Sarvestani, "Analysis of Reliability and Resilience for Smart Grids," in *Proceedings of the 2014 IEEE 38th Annual International Computers, Software and Applications Conference*, 2014.

[28] A. Clark and S. Zonouz, "Cyber-Physical Resilience: Definition and Assessment Metric," *IEEE Transactions on Smart Grid*, vol. PP, no. 99, pp. 1–1, 2017.

[29] S. Hassell, P. Beraud, A. Cruz, G. Ganga, S. Martin, J. Toennies, P. Vazquez, G. Wright, D. Gomez, F. Pietryka, N. Srivastava, T. Hester, D. Hyde, and B. Mastropietro, "Evaluating network cyber resiliency methods using cyber threat, Vulnerability and Defense Modeling and Simulation," in *MILCOM 2012 - 2012 IEEE Military Communications Conference*, Oct. 2012, pp. 1–6.

[30] C. G. Rieger, "Resilient control systems Practical metrics basis for defining mission impact," in *2014 7th International Symposium on Resilient Control Systems (ISRCS)*, Aug. 2014, pp. 1–10.

[31] D. Wei and K. Ji, "Resilient industrial control system (RICS): Concepts, formulation, metrics, and insights," in *2010 3rd International Symposium on Resilient Control Systems*, Aug. 2010, pp. 15–22.

[32] S. Choudhury, L. Rodriguez, D. Curtis, K. Oler, P. Nordquist, P.-Y. Chen, and I. Ray, "Action Recommendation for Cyber Resilience," in *Proceedings of the 2015 Workshop on Automated Decision Making for Active Cyber Defense*. New York, NY, USA: ACM, 2015, pp. 3–8. [Online]. Available: http://doi.acm.org/10.1145/2809826.2809837

[33] P. Ramuhalli, M. Halappanavar, J. Coble, and M. Dixit, "Towards a theory of autonomous reconstitution of compromised cyber-systems," in *2013 IEEE International Conference on Technologies for Homeland Security (HST)*, Nov. 2013, pp. 577–583.

[34] H. Bevrani, *Robust Power System Frequency Control*, 2nd ed., ser. Power Electronics and Power Systems. Springer, 2014.

[35] S. Hossain-McKenzie, K. Davis, M. Kazerooni, S. Etigowni, and S. Zonouz, "Distributed controller role and interaction discovery," in *2017 19th International Conference on Intelligent System Application to Power Systems (ISAP)*, Sep. 2017, pp. 1–6.

[36] S. Hossain-McKenzie, M. Kazerooni, K. Davis, S. Etigowni, and S. Zonouz, "Analytic corrective control selection for online remedial action scheme design in a cyber adversarial environment," *IET Cyber-Physical Systems: Theory & Applications*, vol. 2, no. 4, pp. 188–197, 2017.

[37] S. S. Hossain-McKenzie, "Protecting the power grid: strategies against distributed controller compromise," PhD Thesis, University of Illinois at Urbana-Champaign, 2017.