A Cyber-Physical Resilience Metric for Smart Grids

Friedberg, I., McLaughlin, K., & Smith, P. (2017). A Cyber-Physical Resilience Metric for Smart Grids. In IEEE Power & Energy Society Innovative Smart Grid Technologies Conference (ISGT) 2017: Proceedings (Power & Energy Society Innovative Smart Grid Technologies Conference (ISGT): Proceedings). DOI: 10.1109/ISGT.2017.8086065

Published in:
IEEE Power & Energy Society Innovative Smart Grid Technologies Conference (ISGT) 2017: Proceedings

Document Version:
Peer reviewed version

Queen's University Belfast - Research Portal:
Link to publication record in Queen's University Belfast Research Portal

A Cyber-Physical Resilience Metric for Smart Grids

Ivo Friedberg, Kieran McLaughlin
CSIT, Queen's University Belfast
Belfast, UK
Email: {ifriedberg01, kieran.mclaughlin}@qub.ac.uk

Paul Smith
AIT Austrian Institute of Technology,
Vienna, Austria
Email: paul.smith@ait.ac.at

***Abstract*—The need for novel smart grid technologies is often motivated by the need for more resilient power grids. While the number of technologies that claim to increase grid resilience is growing, there is a lack of widely accepted metrics to measure the resilience of smart grid installations. The design of effective resilience metrics is made difficult by the diversity of challenges and performance measures that a smart grid is subject to. This work identifies the necessary attributes for a complete and effective resilience metric and shows that previous work falls short. It then proposes a novel approach to measure resilience that focuses on the complex interdependencies between challenges and performances in smart grids.**

I. Introduction

The motivation for smart grid technologies that is often put forward is the increase in system resilience that can be achieved. However, the term resilience is used inconsistently throughout recent work. Terms like robustness, reliability, availability and even security are often used interchangeably with resilience [1]. Recent efforts to explore the definition of resilience for cyber-physical systems in general [2] and power grids in particular [1], [3] were made with the goal to achieve an understanding about resilience that encompasses all aspects of smart grids. However, research on descriptive metrics to quantify resilience cannot keep up with the requirements. New technologies to increase grid resilience are usually focused on limited aspects of smart grids. While this is a valid approach to handle complexity, the metrics used for evaluation are usually limited in the same way. This is a problem as research topics keep isolated and a holistic understanding of resilience in smart grids is prevented.

To overcome this limitation this work identifies seven requirements for a descriptive and holistic resilience metric. It will further show that initial approaches to resilience metrics are limited as significant factors such as time or performance measures are not considered. Based on these findings a resilience metric framework is presented and evaluated. The framework is developed to consider the relationships between various performance measures and challenges within smart grids and related critical infrastructures [4]; something that is most often ignored in existing work. The metric is evaluated in a microgrid use case which is of high relevance as microgrids gain popularity as the go-to technology for grid resilience [5], [3]. The evaluation results show that the metric itself is easy to apply while the underlying framework can be used to identify dependencies and guide system improvements.

II. Resilience Metric Requirements

A metric is defined in the ISO 24765 as *a quantitative measure of the degree to which a system, component, or process possesses a given attribute* [6]. Quantifiability is necessary to enable the **comparison** of two systems with respect to their resilience. Comparison needs to be possible based on **measurements** (comparison of existing installations) and based on system models (**predictions** during design time).

According to work by Arghandeh *et al.* [1], the resilience of a system depends on three potentials. The *absorbing potential* (the ability to withstand negative effects), the *recovery potential* (the ability to recover nominal performance during or after a challenge) and *survivability* (the ability to prevent system collapse). A resilient system needs all three potentials therefore a resilience metric should consider them.

Cyber-physical systems are comprised of three different domains that interact to provide a service [1], [7]: the physical, the cyber and the control (or cyber-physical) domain. In each domain, multiple measures of performance are present. A resilience metric has to be **flexible** in a way that allows the evaluation of resilience with respect to all performance measures. Through interaction the domains become dependent; a decreased performance in one domain, is a potential challenge to performance measures in other domains. An effective understanding of the resilience of a system needs to consider these **interdependencies**. At the same time, not all performance measures are relevant for each evaluation. To make the complexity manageable, a metric needs to be **scalable**; aspects of the system that are irrelevant during evaluation need to be abstracted. However, the metric framework should in general be applicable to all potential performance measures.

Table I presents current approaches with respect to the seven attributes identified for an effective resilience metric. It shows that there are a number of shortcomings where significant factors such as time, the dependencies between performance measures or resilience potentials are ignored which leads to an incomplete view of resilience.

	[8]	[9]	[7]	[2]	[3]	[10]
Comparable	●	●	○	●	●	●
Prediction	●	●	●	○	●	●
Evaluate Measurements	◐	●	●	●	○	○
Resilience Potentials Analysis	●	○	●	●	○	●
Flexibility	○	●	○	○	●	●
Interdependencies	○	◐	●	○	●	○
Scalability	●	●	●	○	◐	●

Table I: Completeness of relevant resilience metrics for cyber-physical systems. Full circle ... requirement fulfilled. Half-full circle ... adaption possible to fulfill requirement. Empty circle ... requirement not considered.

Watson *et al.* [10] propose to measure resilience with respect to probability and impact of adverse incidents. In a similar but more concrete approach Chanda and Srivastava [3] apply percolation theory to a topological graph model of the system and use decision making to quantify the results. However, probability and impact based metrics are generally unable to consider the time dimension of the recovery potential.

Rieger *et al.* [7] specifies a resilience metric based on control loop performance. The metric is computed with the use of game theoretic approaches. A similar approach is taken by Melin *et al.* [8] with a mathematical definition of resilience in closed-loop control systems. The problem with the focus on control systems is the loss of flexibility, as performance measures that are not control loop specific cannot be considered.

In work by Henry *et al.* [9] resilience is defined as the ratio between the initial system state before a disruptive event occurs and the recovered state after a resilience action was taken. This approach is very similar to the approach taken in this work, however important concepts like absorbing potential, or the time it takes to recover are not considered.

III. Resilience Metric Framework

The performance of a system can be described by a vector of all performance measures

$$\vec{p}(t) = \begin{pmatrix} p_1(t) \\ p_2(t) \\ \vdots \\ p_n(t) \end{pmatrix} \tag{1}$$

where each performance measure $p_i(t)$ has a nominal performance p_i^N – the performance in a challenge free environment –, a collapse threshold p_i^T – a performance level from which the system cannot recover on its own – and is bound by $0 \leq p_i(t) \leq p_i^N$. Based on a single performance measure $p_i(t)$ the resilience of the system with respect to this performance measure is defined as $\mathcal{R}_{p_i}$ as given by Eq. 2.

$$\mathcal{R}_{p_i} : \mathbb{R}^+ \to [0;1] : t \mapsto 1 - \frac{\int_{t_0}^{t} p_i(\tau)\mathrm{d}\tau - p_i^T \cdot (t - t_0)}{(t - t_0)(p_i^N - p_i^T)} \tag{2}$$

It describes the ratio between the actual system performance (the area between $p_i(t)$ and p_i^T) and the worst case system performance. This metric is supported by a framework that models each performance measure p_i in dependence to other performance measures, as well as external challenges. The quantitative results from the metric can then be rooted in the complete system. The framework can further be used to predict the resilience of the system through estimation without applying real challenges at runtime. Each performance measure is modeled as a differential equation which is solvable as an initial value problem (IVP). where $p(t_0) = p_0$ (see Eq. 3).

$$\dot{p}_i(t) = [f(t, r, p_i(t), p_i^N) - g(t, \vec{c}(t), \vec{p}(t))] \cdot \Theta_{p_i}(p_i(t)) \tag{3}$$

Here, f represents the recovery potential of a degraded system. It depends on the time t, a recovery rate r which needs to be identified for each system and can be a constant or a complex function, the current performance $p_i(t)$ and the nominal performance p_i^N. On the other hand, g represents the absorbing potential and depends on the time, a set of external challenges $\vec{c}(t)$ and all other performance measures. The dependence on other measures is important as they can pose a challenge to the measure in focus. Finally, $\Theta_{p_i}(p_i(t))$ is a heaviside function that describes the performance threshold p_i^T under which the system is considered collapsed. (see [11] for further details).

IV. Experimental Setup

A. Use Case Description

In recent work, microgrids are proposed in different scenarios to increase grid resilience [5], [12]. One rarely discussed problem with islanded operation of microgrids is their reconnection to the main grid. Among other difficulties the system needs to reliably prevent out-of-sync reclosure. This happens if the difference in phase angle between the microgrid and the main grid is too large and can cause severe damage to power equipment. While the general performance of these approaches was previously evaluated, little research was done on the effects of cyber attacks on these use cases. In this work, we evaluate the resilience of synchronous islanding control which was previously defined in Best *et al.* [13] to prevent out-of-sync reclosure during denial of service attacks that introduce network delay. Phasor measurement units (PMUs) are deployed in the microgrid and the main grid. PMUs periodically measure phase angle (Φ), frequency (ω) and voltage magnitude (X_m). Based on the information from the PMUs, a local controller in the microgrid aims to

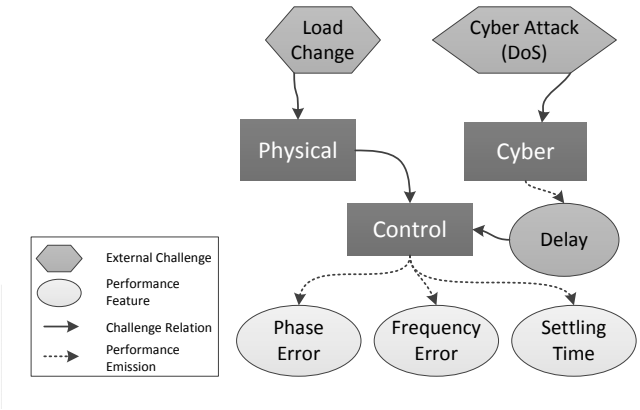


Figure 1: Challenges and performance measures with respect to the system domains. Two external challenges effect the physical and cyber domain; the control domain is challenged internally by load changes and network delay. Three performance measures from the control domain are considered.

minimize the error between the two systems to guarantee that reclosure is safe.

Synchronous islanding is subject to countless challenges. In this work we will focus on step changes in load and denial-of-service attacks that introduce network delay. Figure 1 shows how the three system domains, the challenges of interest and relevant performance measures are connected. This shows the flexibility and scalability of the framework; unnecessary aspects are ignored but various performance measures can be used to compute resilience.

B. System Model

The resilience metric is applied to a power island operated synchronized to an optimal main grid; the system is modeled in Matlab/Simulink. The model is based around a speed controlled synchronous generator rated at 550MW and a frequency of 50Hz. The generator is subject to an initial load of 250MW and an additional step-on load of variable size. The frequency response of the system is measured by a PMU simulation model based on work by Roscoe *et al.* [14]. The simulation model presented here utilizes the P Class PMU with a sampling rate of 10kHz which is compliant to the 2011 version of the IEEE C37.118 standard and is available online[1].

The synchronous generator is controlled by a PI-controller that listens for the measurements from the local (feedback) PMU and the remote (reference) PMU to compute the current error in frequency and phase between microgrid and main grid. The system is subject to common challenges from IT networks like dropped packets, jitter or network delay. These challenges will cause delayed measurements and measurements that arrive out-of-order or not at all. The controller design is based on work by Best *et al.* [13] and improved to handle network challenges by buffering measurements and computing a new set point whenever a new pair of reference and feedback measurements is available.

[1]https://goo.gl/7z4uFM (last accessed 14/12/2016)

Step	Frequency			Phase		
MW (%)	t_r (s)	ζ_f	e (Hz)	t_r (s)	ζ_p	e (rad)
10 (1.8)	0.9	0.3595	0.0760	1.94	0.125	0.5878
20 (3.6)	0.9	0.3571	0.1527	1.94	0.1252	1.1767
50 (9)	0.9	0.3509	0.3808	1.94	0.1317	2.9607
75 (13.6)	0.9	0.3467	0.5702	1.94	0.1607	π
100 (18)	0.9	0.397	0.7588	1.94	0.1421	π
125 (22.7)	0.9	0.371	0.9482	1.94	0.1537	π
150 (27.3)	0.9	0.3491	1.1393	1.94	0.1488	π
175 (31.8)	1	0.3301	1.3395	1.94	0.1329	π
200 (36.4)	1	0.4126	1.5349	1.94	0.1757	π
250 (45.5)	1	0.2894	1.9404	1.94	0.1278	π

Table II: Evaluation results of system responses to step-on loads of various size. The load steps are given in MW and in percentage to the power rating of the generator. The table shows the rise time t_r, the damping factor ζ and the maximum error e for frequency and phase. For the rise time and the error, the unit is given in brackets.

The simulation model was used to gather initial information about the system performance. Table II shows the impact of step changes on rise time t_r and maximum error e with respect to frequency and phase. Further, it shows the parameter ζ that defines the asymptotes of the error response to the challenge. All of these measurements will be used to model the system as shown in the next section.

V. Evaluation Results

A. Metric Implementation

The performance of the system under evaluation can be described as $\vec{p}(t)$ with

$$\vec{p}(t) = \begin{pmatrix} p_l(t) \\ p_d(t) \\ p_f(t) \\ p_p(t) \end{pmatrix}$$

where $p_l(t)$ is the load on the microgrid at time t, $p_d(t)$ is the network delay, $p_f(t)$ is the error in frequency and $p_p(t)$ is the error in phase angle. From these, p_l and p_d are internal challenges to p_f which in turn is a challenge to p_p; the difference in frequency between the two systems causes the phase angle to shift. It is possible to abstract the challenge that the cyber-attack imposes, as it is known that only the effect of network delay is of interest (see Fig. 1 in Sect. IV). Then, p_l and p_d can be seen as known functions and don't have to be modeled. The remaining functions will be designed based on the results shown in Tab. II in Sect. III. The measurements show that both, t_r and ζ are independent from the size of the step challenge. In contrast there seems to be a linear relationship between the step size and the maximum error. Thus, the absorption potential of frequency and phase can be described by a

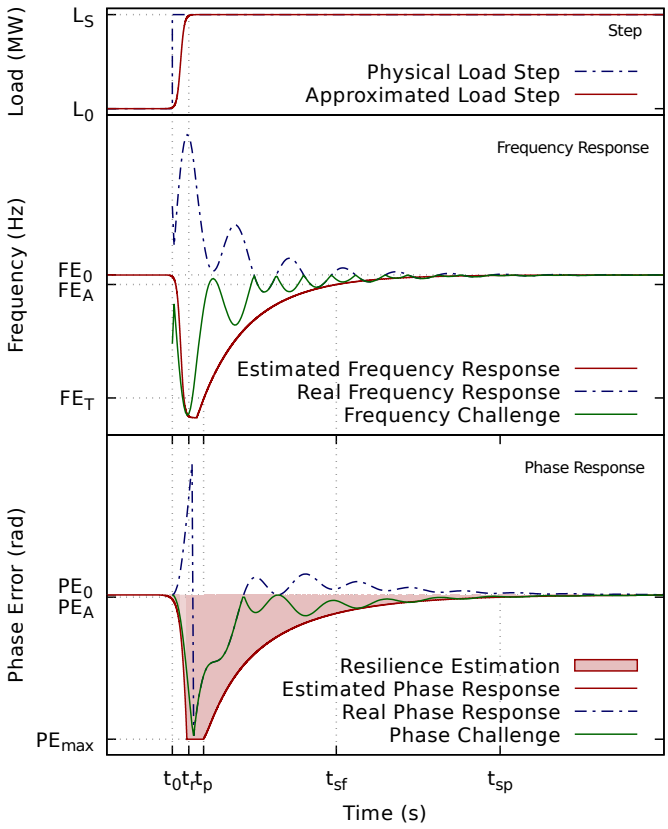
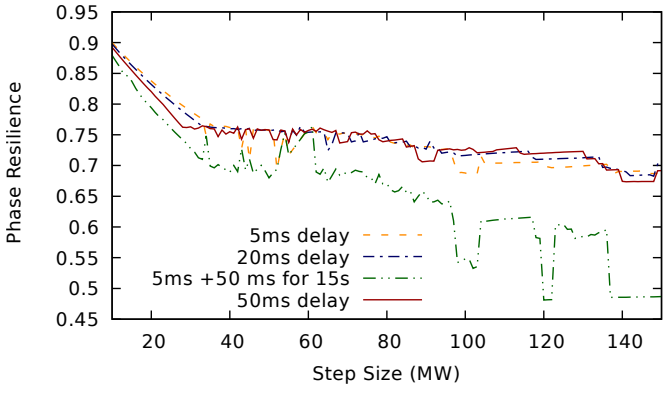
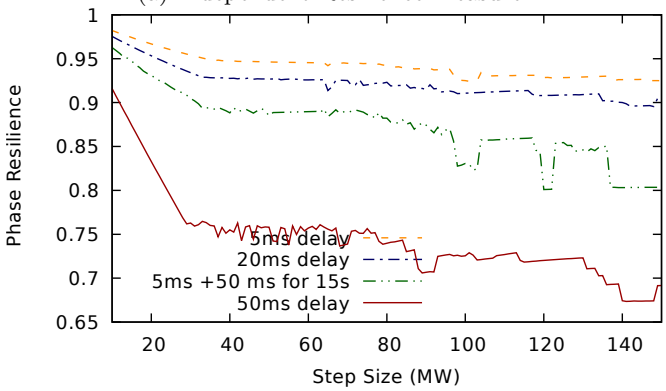


Figure 2: Highlights how Eq. 4 - 6 estimate $\mathcal{R}_{p_p}$. The first figure shows how the step change from L_0 to L_S is estimated by a Eq. 4. For frequency and phase error the real measurements are shown and how they are estimated. Here E_0 are the nominal performances and E_A are the acceptable performances (threshold for settling time). FE_T is the threshold that needs to be passed for the phase to recover. $\mathrm{PE}_{\max}$ is the maximum phase error.



(a) Independent Resilience Measure



(b) Resilience Compared to Worst Case

Figure 3: System resilience under different challenges.

constant factor. The recovery potential can be estimated by the asymptotes of the oscillating control response; they are defined by ζ which is in turn linearly related to the network delay (not shown in Tab. II). Equation 4 - 7 form the system model for the resilience metric. The performance measures $p_f(t)$ and $p_p(t)$ are estimated as a differential equation in the form of Eq. 3. Step changes (like changes in load) need to be estimated to make them integrable; as estimation a logistic function is chosen (see Eq. 4).

$$p_l(t) = \frac{L}{1 + e^{-k\cdot(t-(t_0-t_r/2))}} \tag{4}$$

$$\dot{p_f}(t) = \Big((\mathrm{FE}_0 - p_f(t))\cdot\zeta_f\cdot e^{\zeta_f\cdot(FE_0-p_f(t))}\Big) - \Big(k_f\cdot\dot{p_l}(t)\Big) \tag{5}$$

$$\dot{p_p}(t) = \Big(-p_p(t)\cdot\zeta_p\cdot e^{\zeta_p\cdot(-p_p(t))}\Big)\cdot\Theta_{\mathrm{FE}_T}(p_f(t)) - \Big(k_p\cdot\dot{p_l}(t)\Big) \tag{6}$$

$$\zeta = r\cdot p_d(t) + d \tag{7}$$

The generic function of ζ is given by Eq. 7 where simulation results suggest that $r_f = -0.003671$, $d_f = 0.3553$, $r_p = -0.00217$ and $d_p = 0.17$. Further, k_f and k_p describe the constant relationship between the maximum performance decrease and the step challenge. Finally, Θ_{FE_T} is a heaviside function that is 0 if $p_f(t) < \mathrm{FE}_T$ and 1 otherwise. This highlights that the phase angle can only recover if the frequency error is within certain limits. The phase error cannot grow indefinitely but instead stays within $[-\pi, \pi]$ rad. As long as p_f is not in a certain range (until t_p), no assumptions can be made about the phase error so the worst case has to be assumed which is $\pm\pi$. Figure 2 highlights how the system resilience with respect to phase error ($\mathcal{R}_{p_p}$) under step changes in load is estimated.

B. System Analysis

Based on the system model, the resilience can now be estimated and computed from measurements. Figure 3 shows the estimated resilience with respect to different load steps and network delays. In Fig. 3a the resilience metric is applied independently for each challenge situation (L_S and p_t). The resilience estimation (the area in red in Fig. 2) is computed from t_0 to t_s where t_s changes for each challenge and evaluation. The results show that for $10\mathrm{MW} \leq L_S \leq 30\mathrm{MW}$ the absorbing potential ensures that $p_f < \mathrm{FE}_T$. As $t_p = t_r = 1s$, the resilience decreases proportional to the change of the load

step. For greater load changes, the resilience stays fairly constant and equal for all constant network delays. The results show that constant challenges to the system do not affect the resilience if the metric is applied in this way. This is an important finding as it shows that constant challenges can be ignored when different grid installations or algorithms are compared; this simplifies the system models needed. However, if the challenge is not constant (see the case where the network delay changes for 15s during the recovery), then the results cannot be compared. The computed resilience drops if the delay is changing over time.

The reason is that the settling time t_s is changed with each evaluation. Challenged by a cyber attack, the network delay will not be constant. The estimation is computed for a shorter time span; however the amount of time in relatively bad performance is longer which leads to a lower resilience. To compare the resilience of different dynamic challenges to the same system, the time over which the integral is taken needs to stay constant. This is done in Fig. 3b where the integral is computed from t_0 to $\max(t_s)$. The results show that network delay has a big impact on system performance and thus resilience.

To analyse the survivability of the system with respect to network delay, ζ_f and ζ_p need to be analysed. Equation 6 shows that the recovery potential of p_p is dependent on ζ_p and p_f. The recovery potential of p_f depends solely on ζ_f. So to ensure survivability it needs to be ensured that both, ζ_f and ζ_p are greater than 0. Otherwise, the recovery potential would be 0 or negative which would lead to a further increase in error. By transforming Eq. 7 the threshold for a positive recovery rate can be computed with 96ms for p_f and 78ms for p_p.

Finally, Eq. 5 and Eq. 6 can be used to identify the most efficient changes to the system to increase resilience. There are two controlling factors for p_f in response to load challenges. First, k_f defines the absorbing potential, second ζ_f defines the recovery potential; both depend on the control implementation. Since load changes are normal operation and can hardly be limited, an improvement of the resilience can only be achieved by improvements to the control design. However, network delay also has a significant impact on performance if the system is already challenged by load changes. This is something that is harder to address with the control design. While control improvements can also increase the resilience to network delay, there is only so much the controller can do as measurements are invalidated by new readings every 100ms (see PMU report rate). Thus, it is necessary to limit network delays in the cyber domain rather than the control domain to effectively increase the resilience. Further, improvements to the recovery potential are more promising in the presented system than changes to the absorbing potential as they improve the resilience with respect to both considered challenges. The absorbing potential is not affected by the network delay.

VI. Conclusion

This work presented a descriptive resilience metric framework for smart grids. Seven attributes of a effective metric were extracted from relevant definitions of resilience in the domain and it was discussed how metrics proposed previously fail to fulfill expectations. The results presented in this work suggest that the proposed metric framework can offer a more complete approach to evaluate resilience. The strongest contributions are the ability to analyse resilience with respect to various performance measures (flexibility) while the relationships between the system domains are considered; the two attributes most often left out by existing approaches. Future work will aim to apply the metric to a distribution network use case to allow a more direct comparison to other metrics.

References

[1] R. Arghandeh, A. von Meier, L. Mehrmanesh, and L. Mili, "On the definition of cyber-physical resilience in power systems," *Renewable and Sustainable Energy Reviews*, vol. 58, pp. 1060–1069, may 2016.

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

[3] S. Chanda and A. K. Srivastava, "Defining and Enabling Resiliency of Electric Distribution Systems With Multiple Microgrids," *IEEE Transactions on Smart Grid*, vol. 7, no. 6, pp. 2859–2868, nov 2016.

[4] S. M. Rinaldi, J. P. Peerenboom, and T. K. Kelly, "Identifying, understanding, and analyzing critical infrastructure interdependencies," *IEEE Control Systems*, vol. 21, no. 6, pp. 11–25, 2001.

[5] M. Panteli, D. N. Trakas, P. Mancarella, and N. D. Hatziargyriou, "Boosting the Power Grid Resilience to Extreme Weather Events Using Defensive Islanding," *IEEE Transactions on Smart Grid*, vol. 7, no. 6, pp. 2913–2922, nov 2016.

[6] "Systems and software engineering – Vocabulary," *ISO/IEC/IEEE 24765:2010(E)*, pp. 1–418, 2010.

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

[8] A. M. Melin, E. M. Ferragut, J. A. Laska *et al.*, "A mathematical framework for the analysis of cyber-resilient control systems," in *Resilient Control Systems (ISRCS), 2013 6th International Symposium on*, 2013, pp. 13–18.

[9] D. Henry and J. Emmanuel Ramirez-Marquez, "Generic metrics and quantitative approaches for system resilience as a function of time," *Reliability Engineering & System Safety*, vol. 99, pp. 114–122, 2012.

[10] J.-P. Watson, R. Guttromson, C. Silva-Monroy, R. Jeffers, K. Jones, J. Ellison, C. Rath, J. Gearhart *et al.*, "Conceptual framework for developing resilience metrics for the electricity, oil, and gas sectors in the united states," *Sandia National Laboratories, Albuquerque, NM (United States), Tech. Rep*, 2014.

[11] I. Friedberg, K. McLaughlin, P. Smith, and M. Wurzenberger, "Towards a resilience metric framework for cyber-physical systems," in *4th International Symposium for ICS & SCADA Cyber Security Research 2016 (ICS-CSR 2016)*, 8 2016, pp. 19–22.

[12] S. Liu, X. Wang, and P. X. Liu, "Impact of Communication Delays on Secondary Frequency Control in an Islanded Microgrid," *IEEE Transactions on Industrial Electronics*, vol. 62, no. 4, pp. 2021–2031, apr 2015.

[13] R. J. Best, D. Morrow, D. M. Laverty, and P. A. Crossley, "Techniques for Multiple-Set Synchronous Islanding Control," *IEEE Transactions on Smart Grid*, vol. 2, no. 1, pp. 60–67, 2011.

[14] A. J. Roscoe, I. F. Abdulhadi, and G. M. Burt, "P and M Class Phasor Measurement Unit Algorithms Using Adaptive Cascaded Filters," *IEEE Transactions on Power Delivery*, vol. 28, no. 3, pp. 1447–1459, 2013.