A Cyber-Physical Resilience Metric for Smart Grids


Published in:

Document Version:
Peer reviewed version

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

Publisher rights
© 2017 IEEE
This work is made available online in accordance with the publisher's policies. Please refer to any applicable terms of use of the publisher.

General rights
Copyright for the publications made accessible via the Queen's University Belfast Research Portal is retained by the author(s) and / or other copyright owners and it is a condition of accessing these publications that users recognise and abide by the legal requirements associated with these rights.

Take down policy
The Research Portal is Queen's institutional repository that provides access to Queen's research output. Every effort has been made to ensure that content in the Research Portal does not infringe any person's rights, or applicable UK laws. If you discover content in the Research Portal that you believe breaches copyright or violates any law, please contact openaccess@qub.ac.uk.
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.
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...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 ($\Phi$), frequency ($\omega$) and voltage magnitude ($X_m$). Based on the information from the PMUs, a local controller in the microgrid aims to
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 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 \( \zeta \) and the maximum error \( e \) for frequency and phase. For the rise time and the error, the unit is given in brackets.

<table>
<thead>
<tr>
<th>Step MW (%)</th>
<th>( t_r ) (s)</th>
<th>( \zeta )</th>
<th>( e ) (Hz)</th>
<th>( t_r ) (s)</th>
<th>( \zeta_p )</th>
<th>( e ) (rad)</th>
</tr>
</thead>
<tbody>
<tr>
<td>10 (1.8)</td>
<td>0.9</td>
<td>0.3595</td>
<td>0.0760</td>
<td>1.94</td>
<td>0.125</td>
<td>0.5878</td>
</tr>
<tr>
<td>20 (3.6)</td>
<td>0.9</td>
<td>0.3757</td>
<td>0.1527</td>
<td>1.94</td>
<td>0.1252</td>
<td>1.1767</td>
</tr>
<tr>
<td>50 (9)</td>
<td>0.9</td>
<td>0.3599</td>
<td>0.3808</td>
<td>1.94</td>
<td>0.1317</td>
<td>2.9607</td>
</tr>
<tr>
<td>75 (13.6)</td>
<td>0.9</td>
<td>0.3467</td>
<td>0.5702</td>
<td>1.94</td>
<td>0.1607</td>
<td>( \pi )</td>
</tr>
<tr>
<td>100 (18)</td>
<td>0.9</td>
<td>0.397</td>
<td>0.7588</td>
<td>1.94</td>
<td>0.1421</td>
<td>( \pi )</td>
</tr>
<tr>
<td>125 (22.7)</td>
<td>0.9</td>
<td>0.371</td>
<td>0.9482</td>
<td>1.94</td>
<td>0.1537</td>
<td>( \pi )</td>
</tr>
<tr>
<td>150 (27.3)</td>
<td>0.9</td>
<td>0.3491</td>
<td>1.1393</td>
<td>1.94</td>
<td>0.1488</td>
<td>( \pi )</td>
</tr>
<tr>
<td>175 (31.8)</td>
<td>1</td>
<td>0.3301</td>
<td>1.3395</td>
<td>1.94</td>
<td>0.1329</td>
<td>( \pi )</td>
</tr>
<tr>
<td>200 (36.4)</td>
<td>1</td>
<td>0.4126</td>
<td>1.5149</td>
<td>1.94</td>
<td>0.1757</td>
<td>( \pi )</td>
</tr>
<tr>
<td>250 (45.5)</td>
<td>1</td>
<td>0.2894</td>
<td>1.9404</td>
<td>1.94</td>
<td>0.1278</td>
<td>( \pi )</td>
</tr>
</tbody>
</table>

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 \( \zeta \) and the maximum error \( e \) for frequency and phase. For the rise time and the error, the unit is given in brackets.

V. Evaluation Results

A. Metric Implementation

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

\[
\bar{p}(t) = \begin{pmatrix}
  p_f(t) \\
  p_d(t) \\
  p_f(t) \\
  p_d(t)
\end{pmatrix}
\]

where \( p_f(t) \) 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 \( p_d(t) \) is the error in phase angle. From these, \( p_f \) and \( p_d \) are internal challenges to \( p_f \) which in turn is a challenge to \( p_d \); 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, \( p_f \) 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 \( \zeta \) 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
constant factor. The recovery potential can be estimated by the asymptotes of the oscillating control response; they are defined by $\zeta$ 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).

\[ p_f(t) = \frac{L}{1 + e^{-k(t-(t_0-t_s)/2)}} \]  
\[ p_f(t) = \left( (FE_0 - p_f(t)) \cdot \zeta_f \cdot e^{\zeta_f \cdot (FE_0 - p_f(t))} \right) - \left( k_f \cdot \dot{p}_f(t) \right) \]  
\[ p_p(t) = \left( -p_p(t) \cdot \zeta_p \cdot e^{\zeta_p \cdot (-p_p(t))} \right) \cdot \Theta_{FE_T}(p_f(t)) - \left( k_p \cdot \dot{p}_p(t) \right) \]  
\[ \zeta = r \cdot p_d(t) + d \]  

The generic function of $\zeta$ 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, $\Theta_{FE_T}$ is a heaviside function that is 0 if $p_f(t) < FE_T$ 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 $p_f(t)$ 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 ($R_{p_p}$) 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 $p_L$). 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 $10 MW \leq L_S \leq 30 MW$ the absorbing potential ensures that $p_f < FE_T$. As $t_p = t_s = 1 s$, 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 $\text{max}(t_s)$. 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, $\zeta_f$ and $\zeta_p$ need to be analysed. Equation 6 shows that the recovery potential of $p_p$ is dependent on $\zeta_p$ and $p_f$. The recovery potential of $p_f$ depends solely on $\zeta_f$. So to ensure survivability it needs to be ensured that both, $\zeta_f$ and $\zeta_p$ 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 changes. First, $k_f$ defines the absorbing potential, second $\zeta_f$ 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 an 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