electronics

MDPI

Article

Resilience Evaluation of Demand Response as Spinning Reserve under Cyber-Physical Threats

Anas AlMajali [1,*], Arun Viswanathan [2] and Clifford Neuman [2]

[1] Department of Computer Engineering, The Hashemite University, Zarqa 13133, Jordan
[2] Information Sciences Institute, University of Southern California, Los Angeles, CA 90089, USA; aviswana@usc.edu (A.V.); bcn@isi.edu (C.N.)
* Correspondence: almajali@hu.edu.jo; Tel.: +962-79-8273-087

Academic Editors: Alfredo Vaccaro and Jin (Wei) Kocsis
Received: 20 October 2016; Accepted: 19 December 2016; Published: 28 December 2016

Abstract: In the future, automated demand response mechanisms will be used as spinning reserve. Demand response in the smart grid must be resilient to cyber-physical threats. In this paper, we evaluate the resilience of demand response when used as spinning reserve in the presence of cyber-physical threats. We quantify this evaluation by correlating the stability of the system in the presence of attacks measured by system frequency (Hz) and attack level measured by the amount of load (MW) that responds to the demand response event. The results demonstrate the importance of anticipating the dependability of demand response before it can be relied upon as spinning reserve.

Keywords: resilience; cyber-physical threats; power reserve; demand response

1. Introduction

Utilizing communication, control and computation technologies in the modern smart grid can enhance the reliability of the smart grid, reduce electricity costs and provide new real-time customer services. However, these enhancements create new cyber-physical threats that can be exploited by malicious entities to disrupt smart grid operations on a large scale. Cyber-physical threats are threats that originate in the cyber domain and have an impact on the physical domain of the system [1]. For example, a sudden load drop in the smart grid (physical impact) can be caused by sending malicious remote disconnect commands (cyber attack) to a large number of electric meters [2].

Typically, Demand Response (DR) can be used for many purposes, including energy efficiency, price response, peak shaving, reliability (contingency) response, and regulation response [3]. Many factors determine the type of response a load can provide, such as time of use, duration and speed of response, frequency and magnitude of load required. Based on those factors, there is a growing trend to use DR As Spinning Reserve (DRASR) to provide a reliability response, which is required by many regulations and standards [4]. This functionality of DR is susceptible to cyber-physical threats.

One of the main requirements of the smart grid, as identified by The U.S. Department of Energy (DoE) Smart Grid System Report [5] and other reports from the National Institute of Standards and Technology (NIST) and the National Energy Technology Laboratory (NETL) [6], is to operate resiliently against system disturbances, attacks, and natural disasters. The fundamental problem then is to evaluate the resilience of the smart grid in the presence of system disturbances, attacks, and natural disasters. Evaluating the resilience of such large-scale, complex and heterogeneous system-of-systems in the presence of adverse situations caused by intentional cyber-attacks and random system faults is a non-trivial and challenging task. To simplify resilience evaluation of this complex system, we follow an approach in which the evaluation is focused on one smart grid function at a time. A function here refers to any task or mission of a certain component or system in the smart grid. In this paper, we evaluate the resilience of DRASR (function) in the presence of cyber-physical threats. In this

work, we investigate the question: Is DRASR resilient to cyber-physical threats? DRASR can be considered resilient if the required amount of load to compensate for a contingency is always curtailed within a bounded time. In order to quantify this evaluation, the impact on the smart grid resulting from a cyber-physical attack on DRASR is measured. We use the frequency of the power system (Hz) to measure the impact on the smart grid. On the other hand, the impact of the cyber-physical attack is measured by the amount of load (MW) that responded to the DR request in the presence of cyber-physical attacks. The relationship between the impact (Hz) and the required load (MW) can be used to evaluate the resilience of the smart grid to cyber-physical attacks based on the acceptable level of impact imposed on the power system.

In order to perform this evaluation, the required cyber and physical aspects of the system are modeled and simulated using NS-2 (ns-2.34) [7] and PowerWorld (version 17, PowerWorld Corporation, Champaign, IL, USA) [8], respectively. The setup simulates a system that uses DRASR in the presence of cyber-physical threats. Then, we use this setup to perform a sensitivity analysis of the impact on the system (Hz) and the amount of load (MW) that responds to a contingency. This sensitivity analysis creates a boundary between acceptable and failed DRASR operation. Finally, we demonstrate that at least one cyber-physical attack can cause DRASR failure. As demonstrated in Section 3.2, we follow a systematic methodology that can also be applied to evaluating other smart grid functions. This methodology can be summarized in four main steps:

1. Identify dependencies and failure conditions of the function under evaluation (DRASR in this case).
2. Create an attack tree by exploiting the dependencies identified in the first step.
3. Perform sensitivity analysis based on the first two steps to identify the boundaries between acceptable and failed function operation.
4. Analyze a bottom-up attack scenario to verify that at least one cyber-physical attack is possible.

The rest of this paper is organized as follows: Section 2 discusses smart grid resilience and the concept of demand response as a spinning reserve. Section 3 presents the simulation setup used in the evaluation process. Then, a step by step description of the evaluation process is demonstrated. The results of the evaluation process are discussed in Section 4. Finally, Section 5 discusses the broader implications of our work, and concludes the paper.

2. Background and Related Work

In this section, we first discuss the general notion of resilience and present our definition as applicable to the smart grid. Then, we discuss the motivation, advantages and requirements of using DRASR as a contingency reserve (also known as reliability response).

2.1. Smart Grid Resilience

Many definitions exist in the literature for resilience. Most of these definitions describe resilience as the ability of a system or entity to avoid, absorb and recover from failures [9]. In this work, we adopt the following definition of resilience based on the definition of resilience given by Laprie [9], and the definition of dependability given by Avizienis et al. [10]: *resilience* is the persistent ability of the smart grid to avoid service failures that are more frequent and more severe than are acceptable when facing changes in the environment, and to recover from failures whenever they occur. A number of factors such as cyber-attacks, internal system failures, policy changes, configuration changes, or deployment changes can result in adverse conditions and disrupt system operation. We are specifically interested in evaluating the resilience of the smart grid under cyber-physical threats.

In recent years, evaluating the resilience of the smart grid has been a topic of interest in different research disciplines. A combination of qualitative and quantitative approaches are used in this evaluation. In the cyber-physical security domain, researchers are interested in evaluating resilience in the presence of cyber-physical threats and/or after adding cyber-security components that should

enhance the resilience to those threats [11–13]. Researchers in this discipline rely on risk assessment methodologies to evaluate resilience, which is considered the goal for risk management, that is, risk management enhances the resilience of the system under study [14]. By definition, risk is the likelihood of an event multiplied by the potential impact of that event. In the cyber-security domain, the risk is usually computed as risk = vulnerability × threat × impact.

While this type of assessment covers likely risks (because of the vulnerability assessment step), it marginalizes unlikely risks (that are still possible), and does not cover unknown risk. While more systematic approaches are being developed in this domain [15], most of the work has been done in an ad hoc fashion.

On the other hand, more systematic approaches have been proposed in the environmental hazards/socio-technical systems discipline to evaluate the resilience of smart grids (and critical infrastructures in general). Resilience is evaluated in this discipline for events like natural disasters (e.g., earthquakes and hurricanes), component failure and human vandalism [16,17]. Because of the nature of the events in this field of research, probabilistic approaches (statistical and stochastic) are used and generalized to do the evaluation. The main problem with this type of analysis is that failure probability models are mainly designed based on statistical data for physical components in the system (e.g., transformers and generators in the presence of an earthquake), or stochastic models of failures for those components. This requires estimates of the probabilities of failures for these events in the system, which are non-trivial to compute [18].

There has been an attempt to use the same probabilistic approaches to analyze smart grids under cyber-attacks in both the cyber-physical security domain and the environmental hazards/socio-technical systems domain [13,19]. However, using the same method to estimate the probability of cyber-attacks (that cause failures) may not be appropriate because it is hard to represent cyber-attacks using probabilistic methods similar to the ones used to model failures because of earthquakes (e.g., what is the probability of a zero-day attack?). In addition, these methods do not capture the behavior of the attacker (attack scenario), which results in unrealistic attack modeling and impact analysis of the attack. For example, assigning a random variable to represent the mean time to attack that will cause a failure of a single power component like a generator neglects the attack scenario and leads to unrealistic impact analysis.

Cyber-physical attacks have different impacts on the smart grid like loss of power, loss of load, loss of information, or damage of equipment [20]. These impacts may propagate and affect higher-level smart grid functions causing high-level function failures. Figure 1 demonstrates how the smart grid can be logically decomposed into a physical power layer, a monitoring and communication layer called Advanced Metering Infrastructure (AMI), and an application layer consisting of higher-level functions such as automated metering, outage management (OM) and DR. In addition to the essential functional layers, there is a need for an orthogonal cyber security layer (CS) for protecting the system against failures and attacks and ensuring the integrity, confidentiality and availability of the system. A resilient smart grid should be able to avoid function failures that are more severe or frequent than is acceptable.

Measuring resilience of critical infrastructure in general has been a topic of interest for researchers [21,22]. Strigini [21] summarizes three main measures that can be used to quantify resilience:

1. Measures of dependability in the presence of disturbances.
2. Measures of the amount of disturbances that a system can tolerate.
3. Measures of the probability of correct service given that a disturbance occurred.

What is common between these three types of measures is that they all require identifying function failures and acceptable degradation levels of smart grid services, which is consistent with the resilience definition presented earlier. In this paper, we quantify resilience by correlating and combining the first two measures listed above.

Our approach in quantifying resilience relies on: (1) measuring the dependability of a smart grid function (DRASR in this case) in the presence of cyber-physical attacks [21], where a failure in this

function is measured by power system frequency (Hz); and (2) the cyber-physical attack measured by the amount of load that actually responds to a DR event.

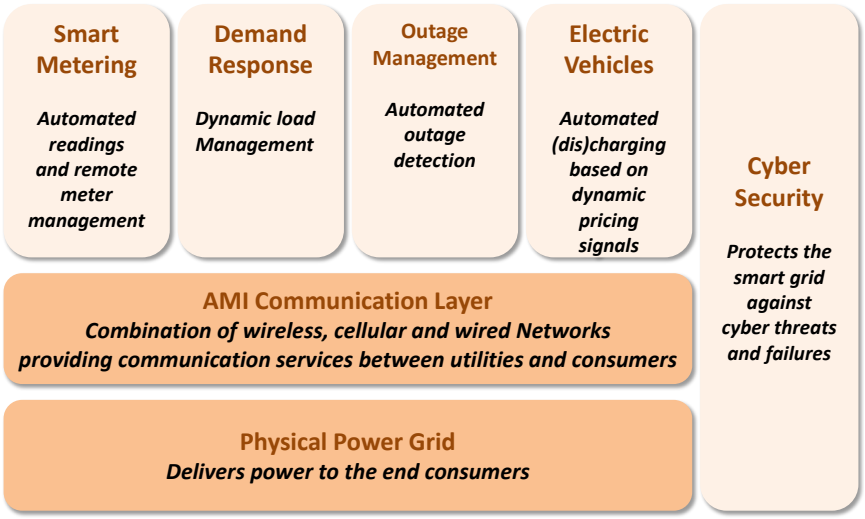

Figure 1. A functional view of the smart grid layers (AMI: advanced metering infrastructure).

2.2. DR as Spinning Reserve

The primary function of the power system is to deliver continuous power. However, a large, complex system such as the power grid faces several threats to its stability in the form of disturbances and contingencies. The power system in North America operates stably at 60 Hz. Minor disturbances and contingencies such as generation loss cause the frequency to fluctuate, but as long as the system is able to prevent the frequency from going out of the optimal operation region (59.97 Hz–60.03 Hz) and quickly recover to 60 Hz, the system operates continuously [23].

Power reserves are the primary mechanism to handle disturbances and contingencies and keep the system operating in its optimal operation region (59.97 Hz–60.03 Hz). Reserves are classified as *spinning* or *non-spinning*, where spinning refers to the unused but synchronized capacity of the system and non-spinning refers to the unconnected capacity. The reserves are used by various response mechanisms such as Governor and Automatic Generation Control (AGC) to balance the frequency of the system. Based on their type, power reserves are classified as regulating reserves and contingency reserves. Mechanisms such as governor response and AGC use the regulating reserves to handle normal operational disturbances in the system. Contingency reserves (also referred to as reliability response) handle supply contingencies such as loss of generation [23].

In the future, automated DR mechanisms will be used as a spinning reserve by utilities to automatically manage load in the system during times of contingencies, or during times of peak demand. For instance, during a contingency such as generator trip, DR will enable an intelligent system controller (or an operator) to send control commands in the form of load reduction requests to selected customers (or customer appliances), who (or which) will comply by shutting off the requested amount of load, thus providing a means to balance and stabilize the system without resorting to more expensive means like buying more energy. DR thus promises to be an efficient, low-cost option for utilities to ensure system stability.

There are several reasons that make DR suitable for this type of reliability response. First, it is infrequently needed (a few times a month) and only needed for a short amount of time (usually 10–15 min). This makes DR less intrusive to customers' daily lives. Second, DR commands can be automatically deployed with the right communication and control technologies that provide fast responses. In addition, DR provides faster responses than generation. Finally, using DRASR may reduce the cost of operating and maintaining typical spinning reserve (synchronized generation) [24].

DR can be considered resilient if the required amount of load is always curtailed within a bounded time, where the required load and time are dependent on utility-specific requirements. Using this definition, we can evaluate if DR was successful in performing its function as a spinning reserve in the presence of a cyber-physical attack (i.e., whether DR was resilient to cyber-physical attacks). Studies have shown that DR signals can be sent from the utility to customers' loads within about 70 s [3]. If DR was not successful in its function as a spinning reserve, then this means that certain requirements were violated, system stability was not maintained and additional actions should be taken to stabilize the system (like increasing generation).

3. Resilience Evaluation of DRASR

To evaluate the resilience of DRASR, we simulate a scenario where DR commands are sent to Air Conditioning (AC) devices of designated customers. There are existing implementations where DR was implemented on ACs [3,25,26]. ACs are suitable for DR activities because turning them off for 10–15 min to compensate for a contingency is not intrusive for customers. Moreover, ACs can satisfy the required amount of load (MW) that can achieve the required balance between generation and load if curtailed. This does not preclude other types of load from being used in the future for the same functionality (e.g., electric vehicles). The ACs should respond by turning off to compensate for certain contingency. In this section, we present the simulation setup that is used to simulate DR (cyber and physical parts of the system). Similar simulation setup was used in our previous work [2]. Then, we use the simulation setup to evaluate the resilience of DRASR in the presence of cyber-physical attacks.

3.1. Modeling and Simulation Setup

Separate simulation tools are used to model the cyber and physical (power) parts of the system. NS-2 is used to simulate the communication network between the utility and the customer side. On the other hand, PowerWorld is used to simulate the power side of the system. Analytical models are used to model how events propagate from the cyber domain to the physical domain. The results we obtained from these models do not apply directly to real world systems; however, more complex and sophisticated representations of real systems can be used by applying the same methodology. For instance, our analysis methodology can be applied to models of existing power systems to obtain specific results pertinent to those systems. A model of the system is represented in Figure 2. This model does not represent the entire smart grid. However, it only represents the parts that are required for DRASR operation. In this case, we assume that the DR commands are transmitted through the AMI network. Next, we describe the details of the system and the models used to represent it.

Head End—The head end represents the central control system of smart meters on the utility side. The head end is responsible for sending DR commands to customers' controllable air conditioners for load curtailment. We assume that DR commands are sent to the smart meters by the head end and smart meters transfer those commands to the air conditioners in the customer premises.

Wireless Mesh Network—This model represents the communication network between the head end and the meters (customer side), which includes wired and the wireless networks. We make the simplifying assumption that wireless network dominates the characteristics of the communication network. The wireless network is actually the Radio Frequency Mesh (RF mesh) in the neighborhood model which consists of wireless smart meters that communicate with the head end in ad hoc fashion through a wireless router placed at the center of the region. Full details of the RF mesh configuration can be found in our previous work [2].

Neighborhood Model—We model 400 smart meters distributed in a region with a wireless router placed at the center of the region. Our preliminary simulation results showed that 400 smart meters is a suitable number for a single wireless router. In a practical implementation, this number may vary and can be enhanced by the use of repeaters that extend the communication range of the wireless router [27]. Our analysis considers 457 RF Meshes [2]. In this neighborhood model, buildings are uniformly distributed in the region with residential, commercial and industrial customer types.

Customer types, percentages, distribution in the neighborhood model, and air conditioner load ratings are assigned based on analytical model of an example neighborhood based on census data for ZIP code area 90057, and real air conditioner load ratings [28]. Customer ratings and air conditioners values are shown in Table 1.

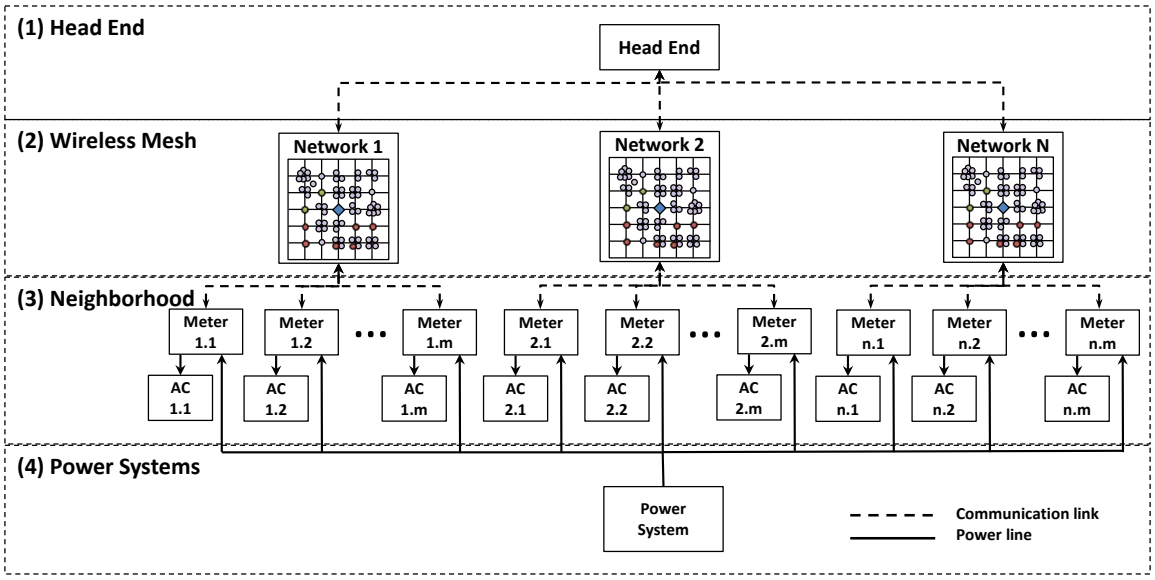

Figure 2. AMI model, that is used to communicate demand response (DR) commands to the air conditioning (AC) units, consists of four elements: (1) the Head End at the utility for smart meter management; (2) "n" Radio Frequency (RF) mesh networks of "m" smart meters each (colored circles) and a wireless router at the center (diamond); (3) a neighborhood model that defines meter and air conditioners; and (4) a model of the power system.

Table 1. Neighborhood model of meter and air conditioner distribution (AC: air conditioning).

Customer Type	Percent of Customers (%)	Num. of ACs	Avg. AC (kW)
Industrial	0.50	2	-
Commercial	12.20	49	3.50
Residential *, 1 unit	5	17	3.50
Residential, 2 units	2	6	3.50
Residential, 3–5 units	5	20	1.44
Residential, 5–9 units	6	21	1.44
Residential, 10–19 units	12	45	1.44
Residential, 20+ units	70	240	0.70
Totals	100	400	-

* Residential type customers have different unit types. For example, '2 units' means one complex that has two apartments.

Power Model—The IEEE 9-bus, three-machine test model, is used to model the power system in this evaluation. This model is used frequently in the literature for stability and frequency control analysis. Starting with the PowerWorld library version of the 9-bus model, the model was configured to include [29], that is, IEEE Type 1 (IEEET1) for the exciter, Steam turbine-governor model (TGOV1) for the governor and IEEL for the load. The IEEE 9-bus model has a load of 315 MW (Figure 3).

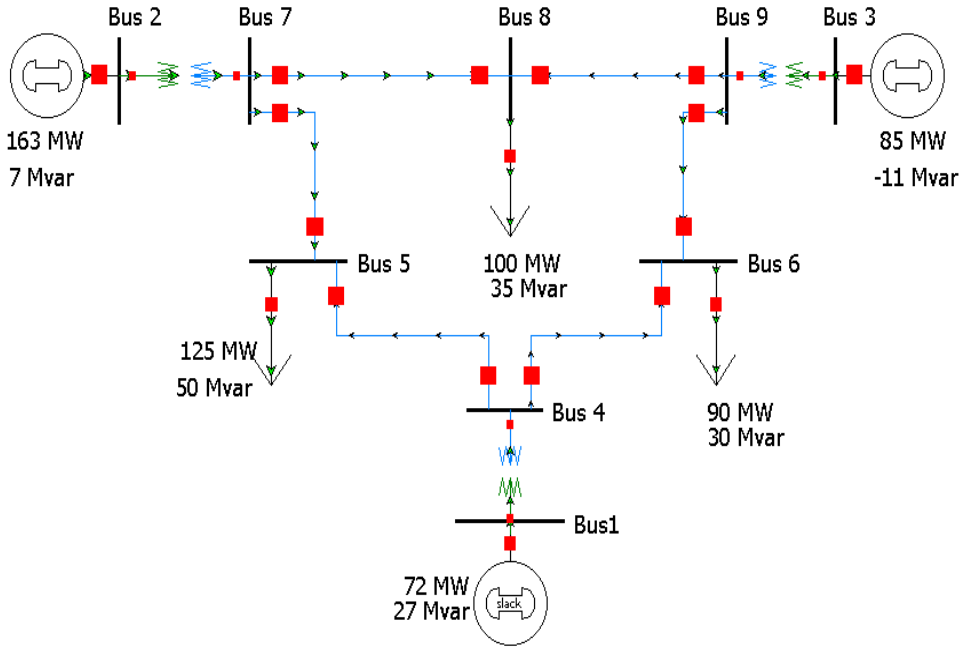

Figure 3. IEEE 9-Bus power model.

3.2. Evaluation Process

DR should respond when there is a contingency by curtailing the required amount of load to stabilize the system to its normal frequency levels (59.97 Hz–60.03 Hz) within the required time (15 min) [23]. DRASR can be considered resilient if the frequency and time requirements are met. By the end of this evaluation, we demonstrate how the resilience of DR in the presence of attacks can be quantified in terms of system frequency (Hz). We next present the step-by-step procedure for evaluation for DRASR.

3.2.1. Identify Dependencies and Failure Conditions

The function under study in this case is DR when used as spinning reserve. By focusing on this single function, we are scoping down the evaluation of this large-scale complex system. The failure conditions of DRASR can be identified based on its requirements. DR is required to stabilize system frequency by curtailing the required amount of load within the required time. The required amount of load is defined based on the size of contingency that happens (e.g., generator failure), whereas time requirements are defined by standards.

DRASR directly depends on the communication network and control devices that transfer, receive and execute DR requests. There are other dependencies related to how DR diagnoses contingencies and makes its decision (e.g., which customers to choose for load curtailment). However, those aspects are out of the scope of this paper. We rely on subject matter experts such as power system operators and contingency planners to identify those dependencies. Cyber-attacks on the communication and control components of the DR system at the time of a contingency may have direct consequences on the amount and timing of load curtailment. Manipulation of system load may impact the stability of the physical system measured by its frequency.

3.2.2. Create Attack Tree

Based on the dependencies identified in the first step, an attack tree is created (Figure 4). The main objective behind creating the attack tree is to increase abstraction in the evaluation process by grouping cyber-attacks that have similar impact.

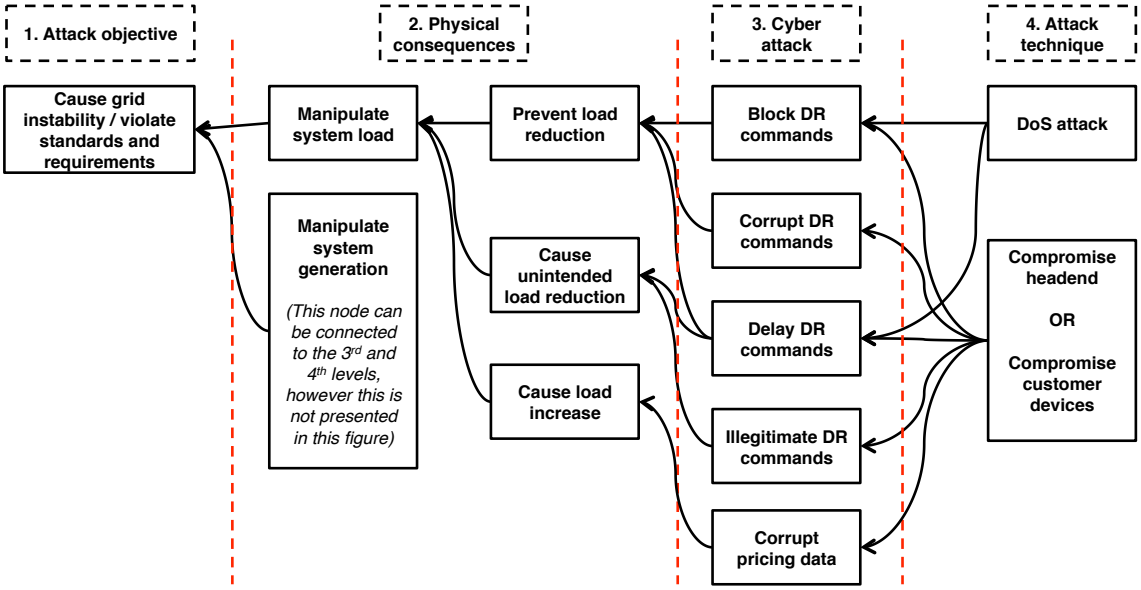

Figure 4. Attack tree for DR as spinning reserve function.

The attack tree is created systematically, although connections to the results are manual. The attack tree is created using a top-down approach with four main steps: (1) setting the attacker's objective for causing failure in the function under study; (2) identifying the physical impacts of the cyber-attacks that cause function failure (load manipulation in this case); (3) identifying the cyber-attacks that may lead to physical impacts; and (4) identifying the attack techniques that may lead to the cyber-attacks.

This attack tree can be divided into four levels. The first level is the function failure (attacker's objective), which is system instability that also includes violating required standards. In this case, the main violation is operating in the under-frequency region. There are several other consequences for operating in the under-frequency region in the system, which results from loss of generation (or increase in load) [23]. For example, under-frequency may have effects on power system equipment like motors and transformers [23].

The second level represents the direct impacts of the cyber-attacks on the physical system which are *manipulate system load* and *manipulate system generation* (Figure 4). One example of manipulating system generation is the famous Aurora generator test [30]. In this paper, we are interested in load manipulation. Similarly, *manipulate system generation* can also be extended to lower levels of the attack tree. Load manipulation may result from causing load reduction, preventing load reduction or increasing load. The physical factor that causes function failure is manipulated at this level. The physical factor in this case is the actual amount of load that responds to a contingency. Manipulating this amount may result in function failure (i.e., system instability).

The third level represents the cyber-attacks that stimulate the physical factors. The cyber-attacks are listed based on the dependencies identified in Section 3.2.1. For example, DR depends on the communication network to transfer its commands. Blocking load curtailment commands results in preventing load reduction (physical factor). This is how the attack propagates from the cyber domain to the physical domain. In Figure 4, the attack tree nodes in the second and third levels do not include all the scenarios through which the top level node (goal of the attack) can be achieved. In addition, there might be faults from non-malicious events that may have the same impact on the smart grid.

The fourth level is the action that the attacker takes to perform the attack (i.e., how the attacker implemented the attack). For example, the attacker may need to compromise the headend or launch a Denial of Service (DoS) attack in order to block DR load curtailment commands. The fourth level of the attack tree can be extended to more detailed levels. For example, the leaf nodes of the attack tree can be extended to demonstrate how the control devices on the customer side are compromised.

However, we stop at the fourth level because we are not concerned about the cause of attack, but rather in evaluating resilience after the attack happens.

In the following two subsections, NS-2 and PowerWorld simulation tools are used to evaluate the consequences of cyber-physical attacks on DRASR by simulating the required components for DRASR operation. The transition from the attack tree to simulation and analysis of results is performed manually here, but the process could be automated with the availability of a comprehensive cyber-physical smart grid testbed that would simulate individual smart grid functions.

3.2.3. Perform Sensitivity Analysis Based on the First Two Steps

The goal of this sensitivity analysis is to quantify the resilience of the system by drawing a boundary between acceptable DRASR performance and DRASR failure in the presence of an attack. The impact of variation of DR responses to variation of contingencies is analyzed. There are two inputs to the sensitivity analysis: (a) the size of the contingency that happens, which is a loss of certain MW of generation; and (b) the amount of load that responds to the contingency through DR. The metric that demonstrates system stability is the frequency of the system (Hz) (i.e., output of the sensitivity analysis). This analysis is performed on the power system to answer what happens if a contingency occurs in the presence of a cyber-attack that eventually reduces the amount of load that responds to the contingency. By performing this analysis at the second level of the attack tree, cyber-attacks with the same impact are abstracted.

A contingency is simulated in the IEEE 9-bus model in PowerWorld by causing a loss of certain MW of generation. For each contingency, the amount of load curtailed (responded to DR) is varied from 0% to 100%, where 100% represents the required amount of load that should have responded to the contingency. We made sure that the biggest simulated contingency does not cause the frequency to drop below 59.1 Hz. If the frequency drops below 59.1 Hz, other protection mechanisms will intervene like Under Frequency Load Shedding (UFLS) and Under Frequency Generator Protection (UFGP) [23]. These protection mechanisms are out of the scope of this paper. The frequency of the system is monitored after each run as shown in Figure 5.

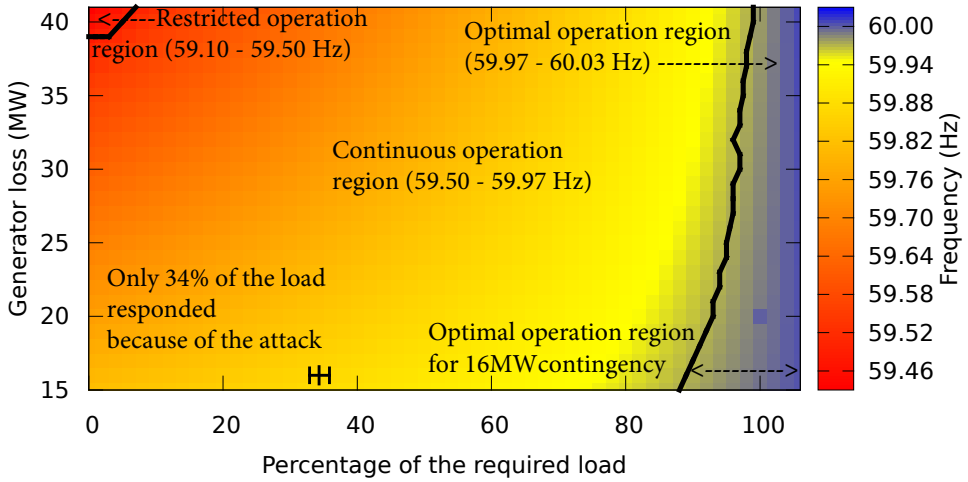

Figure 5. Frequency of the system after 100 s of a contingency (*y*-axis) when varied load responds (*x*-axis) to the DR request. According to the percentage of load that responds, three regions are created: restricted, continuous and optimal. The figure also demonstrated the impact of the DoS attack when DR responds to a 16 MW contingency. On average, 34% of the load responded as shown in the figure.

A boundary for acceptable system performance can be seen in Figure 5 (blue) where the frequency of the system stabilizes to its normal level. This figure also demonstrates the coupling between the physical factor (load that responded to the DR request) and the frequency of the system. The resilience

of DRASR in the presence of cyber-attacks is quantified by system frequency at the end of the simulation. If the frequency deviates from its nominal values (i.e., 60.0 Hz) at the end of the simulation then DR failed in its function as a spinning reserve and the smart grid may be unstable. Based on the values of the frequency, the power system can be operating in one of three regions: optimal operation region (59.97–60.03 Hz), continuous operation region (59.50–59.97 Hz) and restricted operation region (59.10–59.50 Hz). The results are discussed in more detail in Section 4.

3.2.4. Analyze a Bottom-Up Attack Scenario

While the sensitivity analysis done in the third step demonstrates the consequences of the attack in the system, analyzing a bottom-up attack scenario validates that certain attacks can actually propagate to the top nodes of the tree. This step is not intended to validate each and every attack path, but is instead intended to demonstrate (to researchers and stakeholders) that at least one path may succeed, which makes the impact on the root node realistic. As mentioned in Section 3.2.2, there are still unexpected or unforeseen risks that can occur and invoke the same physical consequences that will lead to DRASR failure. The leaf nodes (cyber-attacks) are modeled to verify that they can actually cause failure of DRASR by manipulating system load. Based on the attack tree that is generated in the previous step, many attacks may propagate from the cyber domain to the physical domain.

Customers' control devices are usually susceptible to being compromised, especially if they are connected to the Internet. If these devices are compromised and configured to ignore a DR request, then load reduction will be blocked when needed. The success of this attack path depends on the percentage of compromised devices (ACs) in the serviced area.

In this step, we analyze a DoS attack targeting the wireless router in each RF mesh. If there is a DoS attack targeting the wireless router at the time of DR event, then DR commands may be blocked. As a result of this attack, load curtailment will be blocked. In the attack scenario, we assume that there is a 16 MW (5% of the total generation in the system) contingency in the system (loss of generation). DRASR is used to compensate for the contingency. We assume that, on average, each RF mesh (of the 457) should curtail 35 KW. One way of curtailing this amount in one RF mesh is through the distribution shown in Table 2. Finding the optimal distribution to curtail this amount of load is out of the scope of this paper.

Table 2. Demand response (DR) load curtailment customer and load distribution for a 16 MW contingency in the whole region.

Customer Type	Total Num. of ACs	Avg. AC Load (kW) per Customer	Avg. Load Curtailed (kW)
Commercial	457	3.50	1599.5
Residential *, 1 unit	457	3.50	1599.5
Residential, 2 units	457	3.50	1599.5
Residential, 3–5 units	914	1.44	1316.16
Residential, 5–9 units	457	1.44	658.08
Residential, 10–19 units	2285	1.44	3290.4
Residential, 20+ units	8683	0.70	6078.1
Totals	13,710	-	16,141.24

* Residential type customers have different unit types. For example, '2 units' means one complex that has two apartments.

As a response to this contingency, the head end starts issuing DR commands to the designated customers. Normally, air conditioners should receive those commands through smart meters and curtail the load. However, we assume that two rogue nodes exist in each RF mesh launching a DoS attack at the wireless router by simultaneously generating low bit-rate traffic. Realistically, an attacker can accomplish this attack using different means. For example, an attacker could compromise smart meters in a certain RF mesh and reprogram them to increase the frequency at which they send meter

reads. Alternatively, an attacker could take control of other customer devices such as the service gateway within a Home Area Network (HAN) to send spurious traffic, creating a DoS attack.

In the wireless simulation, we capture which customers received the DR commands and, accordingly, which customers curtailed the load (based on Table 2). Because of the attack, DR was not able to stabilize the system and bring the frequency back to the optimal operation region (59.97–60.03 Hz). Because of the DoS attack, only 34% of load is curtailed, which brings the frequency to 59.86 Hz (continuous operation region). This means that extra actions should be taken to bring the frequency back to the optimal operation region like increasing generation or shedding load. Figure 5 demonstrates the results of the attack on top of the sensitivity analysis.

4. Results

Based on the sensitivity analysis, the operating states of the underlying power system can be divided into three regions (Figure 5).

4.1. Optimal Operation Region (59.97–60.03 Hz)

This is the safe and desired region of operation. In this region, the required amount of load responded to bring the frequency to its normal level within the required time. By analyzing this category, we can identify the level of disturbance that the system can tolerate. The disturbance in this case is the percentage of load that does not respond to the DR request because of the attack. From Figure 5, we can put a lower bound on the percentage of load that should respond to a contingency for the system to be claimed resilient, which varies based on the size of the contingency. For example, 88.0% of the load should respond for a 15 MW contingency in order to maintain the system in the optimal operation region. In other words, the system is resilient to 12.0% disturbance in load response for a 15 MW contingency.

4.2. Continuous Operation Region (59.50–59.97 Hz)

While this region is still safe, it is not the desired region of operation and requires frequency correction. This means that the DR system did not curtail the required amount of load within the required time to bring the frequency back to its normal conditions. Additional actions should be taken to get to the optimal operation region like increasing generation or load shedding. For example, if less than 88.0% of the required load responds to a 15 MW contingency, then the system will be in the continuous operation region.

4.3. Restricted Operation Region (59.10–59.50 Hz)

The system may remain in this region for a restricted amount of time (based on steam turbine off-frequency limits [23]). Being in this region means that the DR system failed to achieve its goal, which directly affects the resilience of the entire smart grid. For example, if only 5.0% of the required load responds to a 40 MW contingency, then the system will be in the restricted operation region. After deploying DR at time of contingency, if the frequency is in the optimal operation region, then DR succeeded and the system is resilient. Otherwise, DR either partially (continuous operation region) or fully (restricted operation region) fails. This demonstrates the importance of anticipating the successful operation of DRASR. An effective situational awareness capability could thus save precious time whenever there is a contingency.

Using our approach, we were able to quantify resilience of DRASR in two ways:

1. The stability level of the system measured by system frequency (Hz) when there is an attack on DR measured by the percentage of load that responds at the time of a contingency.
2. The attack level on DR measured by the percentage of load that responds that the system can tolerate at the time of a contingency, in order to stay in the optimal operation region.

5. Conclusions

By modeling and simulating DR functionality in the smart grid, we quantified the resilience of DRASR by applying a systematic evaluation methodology that can be used to evaluate other smart grid functions as well. The results demonstrate the minimum amount of load (MW) that should respond to a DR event when there is a power contingency for DR to be claimed resilient. They also demonstrate the stability of the system measured by system frequency (Hz) in the presence of variations of attack levels.

This work demonstrates the importance of assessing the resilience of specific functions such as demand response when those functions are used as spinning reserve. The results of this assessment guides the design of security measures and the selection of technologies that improve resilience to all failures. An understanding of the factors affecting smart grid resilience is useful when implementing security policies to protect the systems from cyber-physical attack. We have applied this approach in the assessment of demand response and plan to evaluate the functional resilience of other smart grid components as future work.

Acknowledgments: This research was carried out at the Information Sciences Institute (ISI), University of Southern California, Los Angeles, CA, USA. This material is based upon work supported by the United States Department of Energy under Award Number DE-OE000012, the Los Angeles Department of Water and Power, and by the Department of Homeland Security and the Department of the Navy under Contract No. N66-001-10-C-2018. Neither the United States Government nor any agency thereof, the Los Angeles Department of Water and Power, nor any of their employees make any warranty, express or implied, or assume any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise does not necessarily constitute or imply its endorsement, recommendation, or favoring of by the United States Government or any agency thereof. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States government or any agency thereof. Figures and descriptions are provided by the authors and used with permission. The authors would like to thank our colleagues at ISI, Jet Propulsion Laboratory (JPL) and Los Angeles Department of Water and Power (LADWP) for discussions and feedback that helped develop the ideas and methods expressed in this paper. The authors would also like to thank Mohammed Beshir at USC for the useful discussions that led to this work.

Author Contributions: Anas AlMajali, Arun Viswanathan and Clifford Neuman contributed to the ideas presented in this paper. Anas AlMajali contributed to the design and implementation of the simulation setup. Anas AlMajali and Arun Viswanathan contributed to the analysis of the results. Anas AlMajali, Arun Viswanathan and Clifford Neuman contributed to writing and presenting the paper.

Conflicts of Interest: The authors declare no conflict of interest.

Abbreviations

The following abbreviations are used in this manuscript:

DR	Demand Response
DRASR	Demand Response as Spinning Reserve
AC	Air Conditioning
AGC	Automatic Generation Control
AMI	Advanced Metering Infrastructure
HAM	Home Area Network
DoS	Denial of Service
UFLS	Under Frequency Load Shedding
UFGP	Under Frequency Generator Protection

References

1. Neuman, C.; Tan, K. Mediating cyber and physical threat propagation in secure smart grid architectures. In Proceedings of the IEEE International Conference on Smart Grid Communications (SmartGridComm), Brussels, Belgium, 17–20 October 2011; pp. 238–243.

2. Almajali, A.; Rice, E.; Viswanathan, A.; Tan, K.; Neuman, C. A systems approach to analysing cyber-physical threats in the Smart Grid. In Proceedings of the IEEE International Conference on Smart Grid Communications (SmartGridComm), Vancouver, BC, Canada, 21–24 October 2013; pp. 456–461.
3. Eto, J.; Nelson-Hoffman, J.; Parker, E.; Bernier, C.; Young, P.; Sheehan, D.; Kueck, J.; Kirby, B. The Demand Response Spinning Reserve Demonstration–Measuring the Speed and Magnitude of Aggregated Demand Response. In Proceedings of the 45th Hawaii International Conference on System Science (HICSS), Maui, HI, USA, 4–7 January 2012; pp. 2012–2019.
4. North American Electric Reliability Corporation (NERC). WECC Standard BAL-002-WECC-2—Contingency Reserve. Available online: http://www.nerc.com/files/BAL-002-WECC-2.pdf (accessed on 18 December 2016).
5. U.S. Department of Energy. *Smart Grid System Report*; Technical Report; U.S. Department of Energy: Washington, DC, USA, 2009.
6. U.S. Department of Energy. *A Vision For The Modern Grid*; Technical Report; U.S. Department of Energy: Washington, DC, USA, 2007.
7. USC/ISI. Network Simulator—2 (ns-2). Available online: http://www.isi.edu/nsnam/ns/ (accessed on 18 December 2016).
8. Power World Corporation. PowerWorld. Available online: http://www.powerworld.com/ (accessed on 18 December 2016).
9. Laprie, J.C. From dependability to resilience. In Proceedings of the 38th IEEE/IFIP International Conference On Dependable Systems and Networks, Anchorage, AK, USA, 24–27 June 2008; pp. G8–G9.
10. Avizienis, A.; Laprie, J.C.; Randell, B.; Landwehr, C. Basic concepts and taxonomy of dependable and secure computing. *IEEE Trans. Dependable Secur. Comput* **2004**, *1*, 11–33.
11. Cárdenas, A.A.; Amin, S.; Lin, Z.S.; Huang, Y.L.; Huang, C.Y.; Sastry, S. Attacks against process control systems: Risk assessment, detection, and response. In Proceedings of the 6th ACM Symposium on Information, Computer and Communications Security, Hong Kong, China, 22–24 March 2011; pp. 355–366.
12. Huang, Y.L.; Cárdenas, A.A.; Amin, S.; Lin, Z.S.; Tsai, H.Y.; Sastry, S. Understanding the physical and economic consequences of attacks on control systems. *Int. J. Crit. Infrastruct. Prot.* **2009**, *2*, 73–83.
13. Chiaradonna, S.; Di Giandomenico, F.; Lollini, P. Case study on critical infrastructures: Assessment of electric power systems. In *Resilience Assessment and Evaluation of Computing Systems*; Springer: Berlin/Heidelberg, Germany, 2012; pp. 365–390.
14. Sridhar, S.; Hahn, A.; Govindarasu, M. Cyber–physical system security for the electric power grid. *Proc. IEEE* **2012**, *100*, 210–224.
15. Bodeau, D.J.; Graubart, R.D.; Laderman, E.R. Cyber Resiliency Engineering Overview of the Architectural Assessment Process. *Procedia Comput. Sci.* **2014**, *28*, 838–847.
16. Reed, D.; Kapur, K.; Christie, R. Methodology for Assessing the Resilience of Networked Infrastructure. *IEEE Syst. J.* **2009**, *3*, 174–180.
17. Ouyang, M.; Dueñas-Osorio, L. Resilience modeling and simulation of smart grids. In Proceedings of the Structures Congress, Las Vegas, NV, USA, 14–16 April 2011; pp. 1996–2009.
18. Dondossola, G.; Lamquet, O.; Torkilseng, A. Key issues and related methodologies in the security risk analysis and evaluation of electric power control systems. In Proceedings of the 2006 CIGRE Session, Paris, France, 27 August–1 September 2006.
19. Stamp, J.; McIntyre, A.; Ricardson, B. Reliability impacts from cyber attack on electric power systems. In Proceedings of the IEEE Power Systems Conference and Exposition, Seattle, WA, USA, 15–18 March 2009; pp. 1–8.
20. Sridhar, S.; Manimaran, G. Data integrity attacks and their impacts on SCADA control system. In Proceedings of the IEEE Power and Energy Society General Meeting, Minneapolis, MN, USA, 25–29 July 2010; pp. 1–6.
21. Strigini, L. Fault tolerance and resilience: Meanings, measures and assessment. In *Resilience Assessment and Evaluation of Computing Systems*; Springer: Berlin/Heidelberg, Germany, 2012; pp. 3–24.
22. Vieira, M.; Madeira, H.; Sachs, K.; Kounev, S. Resilience benchmarking. In *Resilience Assessment and Evaluation of Computing Systems*; Springer: Berlin/Heidelberg, Germany, 2012; pp. 283–301.
23. Electric Power Research Institute (EPRI). *EPRI Power System Dynamics Tutorial*; Technical Report 1016042; EPRI: Palo Alto, CA, USA, 2009.

24. Kirby, B.J. *Demand Response For Power System Reliability*; Oak Ridge National Laboratory: Oak Ridge, TN, USA, 2006.
25. Eto, J.H.; Nelson-Hoffman, J.; Torres, C.; Hirth, S.; Yinger, B.; Kueck, J.; Kirby, B.; Bernier, C.; Wright, R.; Barat, A.; et al. *Demand Response Spinning Reserve Demonstration*; Lawrence Berkeley National Laboratory: Berkeley, CA, USA, 2007.
26. Eto, J.H. *Demand Response Spinning Reserve Demonstration—Phase 2 Findings from the Summer of 2008*; Lawrence Berkeley National Laboratory: Berkeley, CA, USA, 2010.
27. Lichtensteiger, B.; Bjelajac, B.; Müller, C.; Wietfeld, C. RF Mesh Systems for Smart Metering: System Architecture and Performance. In Proceedings of the 2010 First IEEE International Conference on Smart Grid Communications (SmartGridComm), Gaithersburg, MD, USA, 4–6 October 2010; pp. 379–384.
28. U.S. Energy Information Administration. Electric Sales, Revenue, and Average Price. Available online: http://www.eia.gov/electricity/sales_revenue_price/ (accessed on 18 December 2016).
29. WECC. WECC Approved Dynamic Model Library. 2011. Available online: https://www.wecc.biz/Administrative/Approved_Dynamic_Models_June_2015.pdf (accessed on 18 December 2016).
30. Meserve, J. Staged Cyber Attack Reveals Vulnerability in Power Grid. 2007. Available online: http://www.cnn.com/2007/US/09/26/power.at.risk/index.html?_s=PM:US (accessed on 18 December 2016).