

Security Policies for Mitigating The Risk Of Load Altering Attacks On Smart Grid Systems

Tatyana Ryutov, Anas AlMajali, Clifford Neuman

Information Sciences Institute, University of Southern California

Marina del Rey, USA

Acknowledgement

This material is based upon work supported by the Department of Energy under Award Number DE-OE0000192.

Disclaimer

This report was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor any agency thereof, the Los Angeles Department of Water and Power, nor any of their employees, makes any warranty, express or implied, or assumes 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 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.

Security Policies for Mitigating The Risk Of Load Altering Attacks On Smart Grid Systems

Tatyana Ryutov, Anas AlMajali, Clifford Neuman
Information Sciences Institute, University of Southern California
Marina del Rey, USA

Abstract—While demand response programs implement energy efficiency and power quality objectives, they bring potential security threats to the Smart Grid. The ability to influence load in a system enables attackers to cause system failures and impact the quality and integrity of power delivered to customers. This paper presents a security mechanism to monitor and control load according to a set of security policies during normal system operation. The mechanism monitors, detects, and responds to load altering attacks. We examined the security requirements of Smart Grid stakeholders and constructed a set of load control policies enforced by the mechanism. We implemented a proof of concept prototype and tested it using the simulation environment. By enforcing the proposed policies in this prototype, the system is maintained in a safe state in the presence of load drop attacks.

Index Terms— cyber-physical, smart grid, security policy.

I. INTRODUCTION

Demand side management and load shaping programs are aimed to modify the load curve shape of customers by deliberate utility intervention. One of the most common programs is direct load control (DLC) in which a portion of the load (e.g., air conditioning, pool pumps) is under the direct control of the utility. An alternative to DLC is indirect load control, which allows customers to control their loads independently according to the price signals that are sent by utilities. While these programs are intended to achieve various energy efficiency and quality objectives, they can also introduce potential problems into the Smart Grid.

Abruptly dropping the load at certain locations in the grid can cause power quality violations and system failures [1]. Similarly, rapid increase of the load can result in substantial economic costs due to the need to pull power from other regions to meet increased demand, power quality violations and system failures.

The load altering attacks against smart power grids can be categorized as direct and indirect attacks:

1. Direct: fabricating the command messages to affect direct load control command signals, such as switch on/switch

off commands. By simultaneously sending fabricated switch on/off signals to a large number of loads the attacker can cause a major spike or drop in the aggregate load demand.

This can be achieved in two ways: (1) remote disconnect through AMI and (2) direct load control through DR.

2. Indirect: load altering attacks can be triggered by false price injection. By compromising the price signals, the attacker can plan to simultaneously change the energy consumption program in hundreds or thousands of residences and cause major changes in the load profile (increase or decrease). Internet-based load altering attacks against smart power grids can take place in a variety of scenarios.

A key infrastructure component used to automate demand response (DR) programs is the Demand Response Automation Server (DRAS). Figure 1 depicts a conceptual overview of Automated DR infrastructure [Koch]. By compromising the control services (e.g., DRAS) and related Advanced Metering Infrastructure (AMI) services, attacker can send authenticated commands to meters without a need to compromise the meters or communications network. In particular, the adversary can execute the following attacks:

1. Send a sequence of service disconnect commands to aggregators and individual customer meters. This is a direct load drop attack that can cause power quality violations and system failures.

2. Send a sequence of service connect commands to aggregators and customer meters. This is a direct load increase attack that can result in substantial economic costs due to the need to pull power from other regions to meet increased demand, power quality violations and system failures.

3. Broadcast DR Critical Peak Pricing event with very high tariff. This is an indirect load drop attack that can cause power quality violations and system failures.

4. Broadcast Real Time Pricing event with very low tariff. This is an indirect load increase attack that can result in substantial economic costs due to the need to pull power from other regions to meet increased demand, power quality violations and system failures.

This paper presents the Policy Server - a security mechanism that attempts to address the above issues. The mechanism performs the following functions:

1. Monitor DR and AMI commands
2. Control load according to a set of security policies during normal system operation
3. Detect abnormal situations and load altering attacks
4. Respond to the load altering attacks

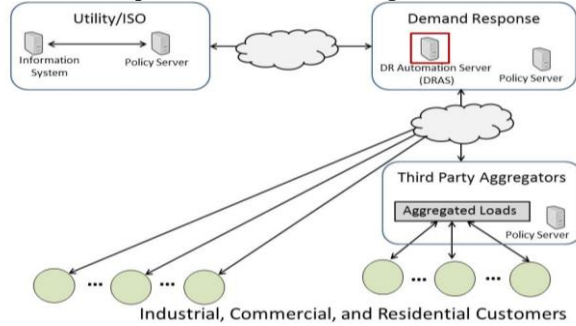


Fig. 1. Conceptual Overview of Automated DR Infrastructure.

The mechanism evaluates received DR and AMI commands to determine whether to authorize the commands and initiate response actions if the system is approaching critical states. This assessment involves evaluation of hierarchical set of policies. We examined security requirements and conducted policy analysis related to load control and defined a set of load control policies evaluated by the Policy Server. We implemented a proof of concept prototype and evaluated it using the simulation environment described in [1]. By enforcing the proposed policies in this prototype, the system is maintained in a safe state in the presence of load drop attacks.

II. RELATED WORK

A number of recent publications have attempted to address the risk of cyber- and cyber-physical attacks against metering infrastructure. **Under construction**

III. LOAD CONTROL POLICIES FOR SMART GRID

Policies that govern Smart grid infrastructure are complex due to a number of involved stakeholders and sources of regulatory controls (e.g., NERC Critical Infrastructure Protection, privacy laws, etc.). Fig. 2 depicts a process whereby concrete (i.e., the policies to be enforced by the system) security policies are produced. Utility, Third Parties, and Customers adopt policies that comply with the Government Regulators' requirements and guidelines. Utility, Third Parties, and Customers establish trust relationships in a form of contracts/agreements, so concrete policies comply with these contracts.

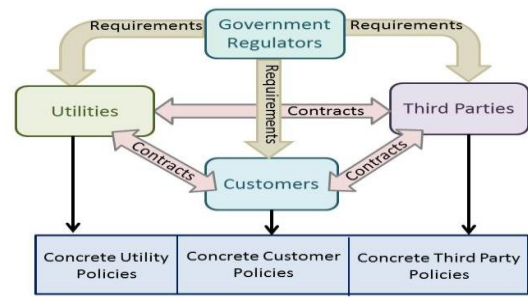


Fig. 2. Smart Grid Policy Specification Process.

We next briefly describe essential requirements and concrete policies related to the load control.

Government Regulator Requirements

1. DR opt-in/opt-out choices. Utilities must allow Customers to opt-out of DR.
2. Voltage regulation. Voltage adjustment at a feeder must be done within the limits allowed by ANSI C84.1. IEEE 1159-200919 defines limits for acceptable power delivery to customers.
3. Building regulation. Building settings must comply with the standards for building temperature and humidity (ASHRAE 55-2010), lighting (CIBSE Code for lighting), and minimum air flow.

Utility Policies

1. Safety policies are constraints expressed as generator protection limits.
2. Power quality policies. Delivered voltage is required to stay in the range $0.9 \text{ pu} < V < 1.1 \text{ pu}$. System frequency is required to stay within $\pm 0.10 \text{ Hz}$ of nominal. The consequences of operating outside of power quality requirements include damage to or degradation of customer and utility equipment.
3. Normal operation policies define constraints on normal operational behavior. Investigation is required if observed behavior falls outside these constraints but that does not rise to violations of power quality and safety policies.
4. Load balancing policies. Power operations contingency plans include pulling power from other regions when generation is insufficient to meet demand. Policies can specify energy price constraints that define maximum acceptable price range as well as energy amount for buying energy from other regions in such cases.
5. Business continuity policies necessitate business activities to function even during cyber-attacks. Such policy may require, for example, DRAS to be constantly operating.

Customer Policies

1. DR opt-in/opt-out preferences that are uploaded to a LADWP information repository for DR application. We assume that if customer selects opt-out no direct

connect/disconnect commands as well as DR event notifications should not reach the customer.

2. Building level policies: certain parts of the buildings (e.g., medical facilities) should receive certain guaranteed power quality to support acceptable levels of lighting, temperature, humidity etc.
3. Price threshold at which to reduce demand - should prices reach or exceed this level, the demand response should be dispatched.

Third Party Policies

Third-party contractors, such as aggregators, can combine loads from certain utilities and make them available for demand response, thus acting as intermediaries between utilities and customers. Third Parties comply with contractual obligations and regulations by enforcing the policies defined by the Utilities (e.g., provide the contracted demand reduction) and Customers (e.g., enforce price threshold at which to reduce demand).

IV. DESIGN DETAILS

Policy Server observes transmitted direct connect/disconnect commands, critical peak events, DR commands and price signals originated by DRAS and sent through AMI infrastructure as well as acknowledgements to DR command signals received through AMI. Policy server can be replicated and deployed in different domains as shown in Fig.1.

Under normal (non-attack) system operation, the Policy server is consulted (e.g., by DRAS) in order to enforce the load control policies before sending an AMI/DR command(s). To determine whether an AMI/DR command is authorized, Policy server evaluates all relevant stakeholders' policies as shown in Fig.3.

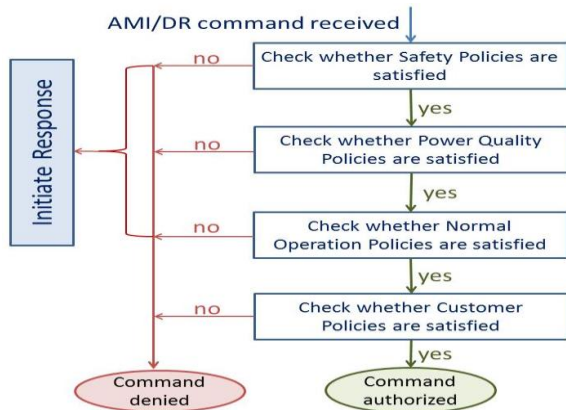


Fig. 3. Policy Evaluation Process.

Note that the policy enforcement can be accomplished in a distributed fashion. For example, enforcement of customer policies can be delegated to an aggregator. In this case, the Policy server at the aggregator's site will determine whether a command authorized by a Policy Server at the Utility or DR site should be forwarded to specific clients.

If the Policy server determines that the system is approaching dangerous state (Safety, Power quality, or

Normal operation policies are about to be violated), it activates response actions, such as:

- Notify operator about ongoing dangerous load drop/increase event involving particular Region(s)
- Drop suspicious messages/commands coming from compromised DRAS by reconfiguring firewall rules
- Shut down the DRAS server if Business continuity policies do not prohibit it

The response actions are also executed in a distributed manner.

Fig. 4 shows concrete Safety, Power quality (purple line), and Normal operation (green line) policies for a load drop attack scenario and two direct load drop attacks. The policies define the boundaries between the three operational regions and demonstrate the correlation between the system variables: the amount of load dropped and time over which load dropped in one hand and the system failure effects in the other hand.

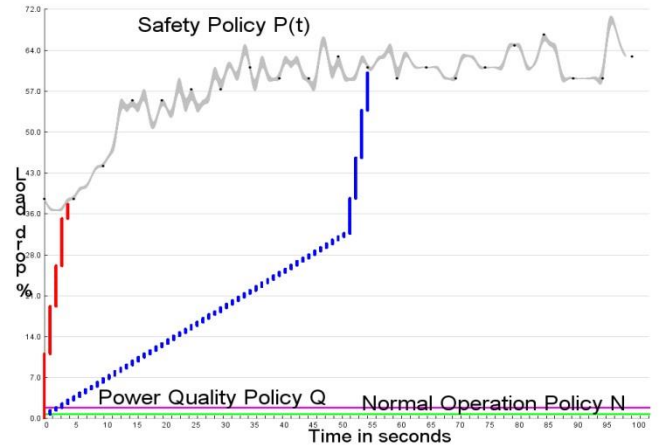


Fig.4. Safety, Power quality, and Normal operation policies for a load drop attack scenario and two direct load drop attacks.

We used the methods and data sources described in [1] to: (1) construct a cyber-physical model of an AMI system connected to a power system, (2) measure the integrated system sensitivity to load drop attacks, and (3) develop the Safety, Power quality, and Normal operation policies for a load drop attack scenario for a modeled region. Power simulations details are described in the next Section.

In our model a **region** represents a set of smart meters served by a given generator. The modeled region consists of 457 neighborhoods. Table shows region customer model.

TABLE I. REGION CUSTOMER MODEL

Customer Type	Region Energy Customer Model		
	Total Number of Meters in a Neighborhood	Average Load (kW)	Total Number of Meters in Region
Industrial	2	19.17	914
Commercial	49	8.51	22393
Residential	349	0.67	159493

Number and average load ratings of the three customer types for a modeled neighborhood were derived from average numbers for the entire Los Angeles Department of Water and Power service area [U.S. Energy]. Each customer in the modeled service area is assumed to have a single smart meter.

Each AMI/DR command includes send time and meter ID. Based on the meter ID Policy server determines the region the meter belongs to and a type of customer. Based on the type of customer and region, the server predicts load drop for each meter that will result in execution of disconnect command. The predicted load drop value is calculated based on the values in Table 1. The time of the effect of the command is assumed to be the send time.

To identify whether the system is in a safe region for the direct load drop case for each DR direct load drop command received at time t_i two conditions must hold:

1. $D(t_i) < P(0)$ defines maximum acceptable load drop completed at once.
2. $\sum_{i=t_d}^{t_e} D(t_i) < P(t_i)$ formula defines the total load drop that involves loads of all meters that are turned off before and at time t_i .

$P(t)$ – function defined for each region that represents Safety policies. It approximates the maximum load that can be safely dropped within time t in certain region.

$D(t_i)$ – total load drop at time t_i , represents the sum of dropped loads of all meters that are disconnected at time t_i .

We use sliding window command stream monitoring approach. The window start time is a certain time $t_s > 0$ in the past that indicates a time boundary to safely discard all observed commands with a time stamps $t_j < t_s$. The value of t_m is calculated based on the state of the system. We assume that t_m is the time required for the system to get back to its normal state after an event (e.g., DR event) after which previous events can be safely discarded. For example, if a DR event causes the frequency of the system to fluctuate then, we wait for the system to get to back its normal frequency which is 60 Hz before discarding previous events.

The window size is 100 seconds, so $t_e = t_s + 100$. A threshold can be added to the above formula in order to report policy violation before it reaches critical value.

Similar approach is used to detect violations of Power quality and Normal operation policies: function $P(t)$ is replaced with the $Q = 1.94\%$ and $N = 0.65\%$ constants defined in Fig.4.

To test the Policy server we executed a number of direct load drop attack scenarios following the procedure described in [1]. Fig. 4 shows two attack scenarios fastest (red) and slow (blue). An attack generates a series of service disconnect commands in a round robin fashion (from the DRAS) addressed to each meter in a single neighborhood. Predicted load drop in one round robin cycle are aggregated (i.e. the load connected to a single meter in each neighborhood). The time spacing between two subsequent command rounds was fixed at 150 milliseconds. Slow attack targets first Industrial next Commercial and finally Residential customers. The order is

reversed for the slow attack execution. The Policy server detects violations of the policies and initiates response measures briefly outlined above. The response is not shown in Fig.4.

V. POWER SIMULATION DETAILS

Power Model: The power system is simulated using the IEEE 9-bus, 3-machine test model, shown in Figure [1]. This model is used frequently in the literature for stability and frequency control analysis. Starting with the PowerWorld library version of the IEEE 9-bus model, the model was configured to include [1]: IEEE1 for the exciter, TGOV1 for the governor and IEEL for the load.

To provide semi-realistic stability in the model, over-frequency protection was enabled with a threshold of 61.80 Hz and a pickup of 0.25 seconds [2], and under-frequency protection was enabled with a threshold of 57.60 Hz and a pickup of 2 seconds.

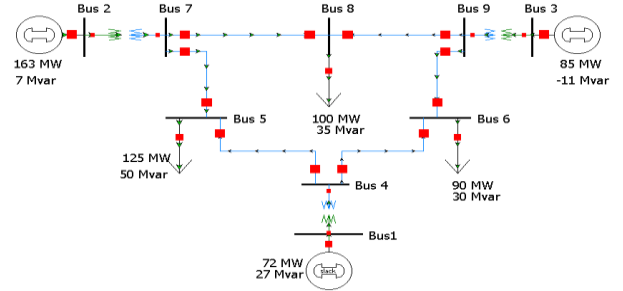


Fig. 5. IEEE 9-bus power model.

Sensitivity Analysis: The policy engine needs to correlate between the system variables and the failure effects on the system in order to make its decisions. The transient stability add-on in PowerWorld was used to implement this analysis (the same analysis was used by AlMajali et al. [3] and Rice et al. [4]). Two inputs were varied to inject a load drop in the simulations: 1) the amount of load dropped which was varied between 20% and 80% of the total load in the system; 2) the duration over which the load was dropped was varied between 0 and 100 seconds. As characterized by Rice et al. [4], the failure effects on the system can be divided to four categories:

1. System shutdown: All generators in the power model tripped as a result of over-frequency protection. This is measured as zero power output from all generators at the end of the simulation. This case corresponds to the violation of Safety policy $P(t)$ depicted in Fig.4.

2. Power quality violation: As defined in IEEE 1159-2009, system frequency is required to stay within ± 0.10 Hz of nominal. Operating outside this range may results in electrical equipment damage [2] [5] (i.e. $60.10 \text{ Hz} < \text{frequency} < 61.80 \text{ Hz}$). This case corresponds to the violation of Power Quality policy Q shown in Fig.4.

3. Anomalous operation: In this category the system is not operating within its normal operation range but still not violating standards (i.e. $60.03 \text{ Hz} < \text{frequency} < 60.1 \text{ Hz}$). This case corresponds to the violation of Normal operation policy N depicted in Fig.4.

4. Normal operation: In this category the system is within its normal operation range (i.e. ± 0.03 Hz).

VI. DISCUSSION

We studied load drop attack scenarios. Our next step is to study direct load increase attacks. There are some issues that can make this attack ineffective. If a meter is disconnected from the grid, then this most likely means that no load is attached to it (e.g., the apartment is empty because someone moved out). So sending a remote connect command that will connect the meter may not increase the load. We need to estimate the percentage of disconnected meters with loads out of the whole number of meters. This information

Simulation of the load increase attack scenario is more complicated because it involves other protection mechanisms beside generator governors like Under Frequency Load Shedding (UFLS) and Under Frequency Generator Protection (UFGP) [EPRI].

Indirect load drop and increase attack scenarios require further examination to determine potential feasibility of such attacks and understanding of conditions that contribute to the effectiveness of the attacks.

DR programs offer customers the opportunity to reduce demand in response to a price signal or financial incentive. A DR event is defined as, "The time periods, deadlines and transitions during which Demand Resources perform." [cite] Typically the request to reduce demand is made for a specific time period on a specific day which is referred to as a demand response event [cite]. Each event has three key measurement components [cite] depicted in Fig. 6:

Load Reduction = Baseline Demand – Actual Demand

Baseline – The amount of energy the customer would have consumed absent a request to reduce.

Actual Use – The amount of energy the customer actually consumed during the event period.

Load Reduction – The mathematical difference between the baseline and the actual use.

The load reduction value can be used to estimate potential change in load during a DR event and determine whether it poses risks such as violation of Safety, Power quality and Normal operation policies.

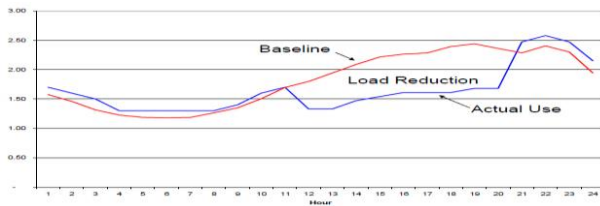


Fig. 6. Demand response event and baseline.

Demand Response Event involves several periods: advance notification, deployment, reduction deadline, release and normal operation. DR Critical Peak Pricing and Real Time Pricing are candidate programs to stage indirect load drop

attacks executed during the ramp up period that starts at the deployment time and ends at the reduction deadline.

Indirect load drop can be calculated based on the previous formula: $\sum_{i=t_s}^{t_e} D_i(t_i) < P(t_i)$, where $D(t_i)$ represents the sum of load reduction values of all meters that are executed at time t_i , t_s is event deployment time and t_e is reduction deadline time. Due to inability to acquire actual customer load reduction data for our modelled region, we experimented with simulated data.

The safety policy violation requires 70% load reduction to be executed by 100% of the industrial, commercial and residential customers, which might not be realistic. However, power quality violations are observed at 10% load reduction on behalf of 20% of the customers making this threat quite feasible.

VII. CONCLUSION

This paper presented a security mechanism that monitors and evaluates DR and AMI commands to determine whether to authorize the commands and initiate response actions if the system is approaching critical states. The detection is based on a set of security policies security requirements defined by various Smart Grid stakeholders. We implemented a proof of concept prototype and evaluated its effectiveness to detect and respond to direct load drop attacks using the simulation environment. Our future work involves studying direct load increase attacks.

ACKNOWLEDGMENT

The authors would like to thank our colleagues at JPL, ISI, and LADWP for discussions and feedback that helped develop the ideas and methods expressed in this paper.

REFERENCES

- Anas AlMajali et al A Systems Approach to Analysing Cyber-Physical Threats in the Smart Grid , IEEE SmartGridComm
- A.H. Mohsenian-Rad and A. Leon-Garcia, Distributed internet-based load altering attacks against smart power grids, *IEEE Transactions on Smart Grid*, vol. 2, no. 4, pp.667–674, December 2011.
- Mitigating The Risk Of Cyber Attack On Smart Grid Systems, Eric B. Ricea, Anas AlMajali Conference on Systems Engineering Research, CSER 2014.
- Demand Response Measurement & Verification, AEIC Load Research Committee, March 2009, www.aeic.org
- Evaluating Baselines for Demand Response Programs, AEIC Load Research Workshop, February, 2008, www.aeic.org
- 8 F. Pasqualetti, F. Dorfler and F. Bullo Attack detection and identification in cyber-physical systems.
- E. Koch and M.A. Piette, "Architecture Concepts and Technical Issues for an Open, Interoperable Automated Demand Response Infrastructure," presented at the Grid Interop Forum, Albuquerque, NM, Nov. 2007
- Electric Power Research Institute, "EPRI Power System Dynamics Tutorial," 2009.
- U.S. Energy Information Administration, "Electric Sales, Revenue, and Average Price," [Online]. Available: http://www.eia.gov/electricity/sales_revenue_price/.