Mitigating the Aurora Vulnerability With Existing Technology

Doug Salmon, Mark Zeller, Armando Guzmán, Venkat Mynam, and Marcos Donolo,
Schweitzer Engineering Laboratories, Inc.

***Abstract*—The Aurora attack may pose a risk to rotating machinery operating under certain conditions on the electrical grid. The Aurora attack involves opening and closing a circuit breaker or breakers, resulting in an out-of-synchronism condition that may damage rotating equipment connected to the power grid. This paper focuses on the Aurora attack on a synchronous generator and the existing technology available to mitigate the attack. The root cause of the vulnerability is a breakdown in security. Defense against the Aurora attack is two-tiered. The first level prevents the attack with sound security practices. The second level protects the equipment in the event that the security level is compromised. The equipment can be protected using several existing methods, including breaker reclosing supervision with a time delay on reclosing, reclosing supervision by a backup protective relay, and rate of change of frequency, or wide-area synchronized phasor measurements.**

I. How the Aurora Attack Causes Damage

The Aurora vulnerability burst into the national spotlight in September 2007, when CNN reported on a test performed at the U.S. Department of Energy's Idaho laboratory [1]. The simplified version of the test setup is shown in Fig. 1. The CNN report sensationalized the potential risk presented by the Aurora attack.

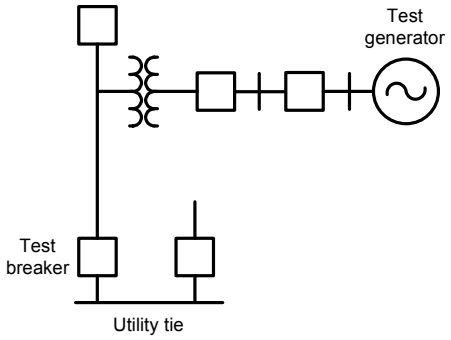

Fig. 1. Test setup for the Aurora attack at the Idaho laboratories

The intent of the Aurora attack is to intentionally open a breaker and close it out of synchronism to cause damage to the connected generators and motors. Good engineering practice includes synchronism-check relays installed in the power system to prevent out-of-synchronism closing. The Aurora attack assumes that these relays could be hacked to defeat their purpose. When an out-of-synchronism close is initiated, the high electrical torque translates to stress on the mechanical shaft of the rotating equipment. This stress reduces the life of the rotating equipment and can destroy it. The U.S. Department of Homeland Security worries that coordinated attacks could cause prolonged outages in large sections of the electrical grid.

Testing acknowledged that in order to initiate an Aurora attack, the attacker would need the following components:

- A device able to open/close breakers
- Access to the open/close device
- Power engineering knowledge
- Power system information
- Hacking skills

The expectation that traditional generator protection can guard against this type of attack has been challenged. By initiating breaker open/close scenarios, unexpected torque can be applied to the rotating machine, as shown in Fig. 2. This threat requires that protection engineers reevaluate how to provide comprehensive generator protection.

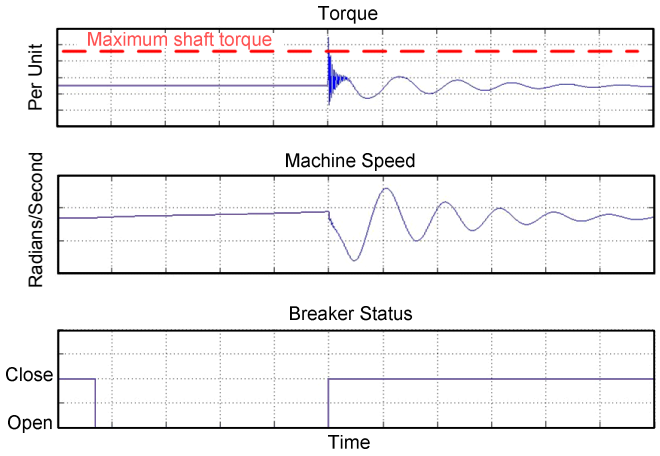

Fig. 2. Relationship of torque, speed, and breaker status

II. Typical Generator Protection

Protection engineers have been building ac generator protection schemes since the first generators were commissioned in 1893. Today's typical ac generator is protected using the following elements (see Fig. 3):

- Volts/hertz (24)
- Undervoltage (27)
- Reverse or low forward power (32)
- Loss of field (40)
- Negative-sequence overcurrent (50Q)
- Neutral overcurrent (50N)
- Phase overcurrent (50)

- Voltage-controlled or voltage-restrained time-overcurrent (51VC)
- Overvoltage (59)
- Stator ground (64)
- Out of step (78)
- Overfrequency and underfrequency (81)
- Current differential (87)
- Loss of potential (60)

Certainly not all elements are needed for each installation, and a wide variety of details exist on the protection schemes and interconnections.

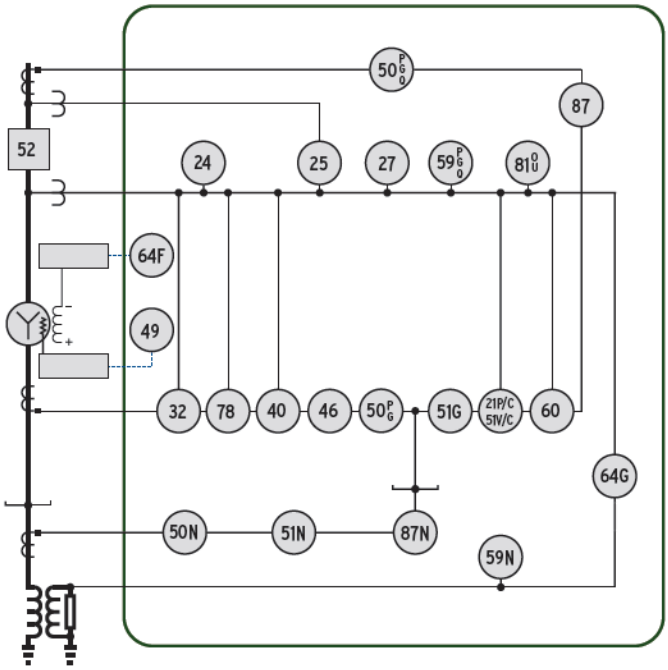

Fig. 3. Typical elements in generator protection system

The generator is protected against closing when the voltage and frequency do not match the corresponding system voltage and frequency. A synchronism check (25) element is used to prevent closing an out-of-synchronism generator to an operating system. Frequency and voltage elements are also used to protect the generator from an unplanned disconnection from the system.

A. Frequency

The generator protective relay provides several steps of over- and underfrequency elements. Each element can operate as an over- or underfrequency element, depending on its pickup setting. If the pickup setting is less than the nominal machine frequency setting, the element operates as an underfrequency element, operating if measured frequency is less than the set point. If the pickup setting is greater than nominal machine frequency, the element operates as an overfrequency element, operating if measured frequency is greater than the set point.

B. Overvoltage and Undervoltage

Generator protection offers over- and undervoltage elements for protection, indication, and control functions.

Typical phase undervoltage elements operate if any single-phase measurement falls below the set threshold. The phase-to-phase undervoltage element operates using the minimum of the measured phase-to-phase voltages. The positive-sequence undervoltage element operates when the measured positive-sequence voltage falls below the set threshold.

Phase overvoltage elements operate using the maximum measured phase voltage magnitudes. Residual overvoltage elements operate using the sum of the three-phase voltage measurements. The positive- and negative-sequence overvoltage elements operate when their respective measurement exceeds their set threshold. The phase-to-phase overvoltage element operates when the maximum phase-to-phase voltage exceeds the set threshold.

III. Why Typical Generator Protection May Be Insufficient

The typical protection of a generator is very robust and has been shown to be both sensitive and secure for operating and protecting the generator during normal and faulted conditions. Typical system protection expects some short-term variations in the operating conditions and system parameters and is set to allow these deviations while still within the operating regions of the generator.

When tested using a real-time digital simulator, the protection schemes discussed in this paper functioned properly but allowed a window of opportunity for a precisely targeted and timely attack (see Fig. 4). A successful attack required a narrow time window, as well as penetrating a number of other system safeguards.

Typical generator protection schemes will protect the generator under most operating scenarios but have some limitations when the power exchange with the utility is minimal. Protection schemes that depend solely on local measurements do not provide complete protection against the Aurora attack under all operating conditions. Local protection schemes are limited because of the information available. Fig. 5 shows typical operating times of generator protection to detect that the breaker in Fig. 4 has been opened for different power exchange conditions.

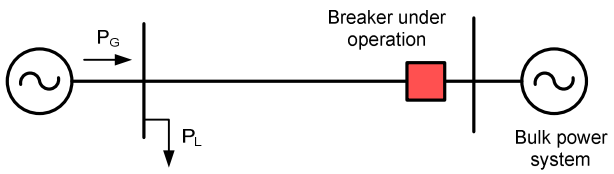

Fig. 4. Performance of the islanding detection methods were tested at varying ratios of P_L to P_G

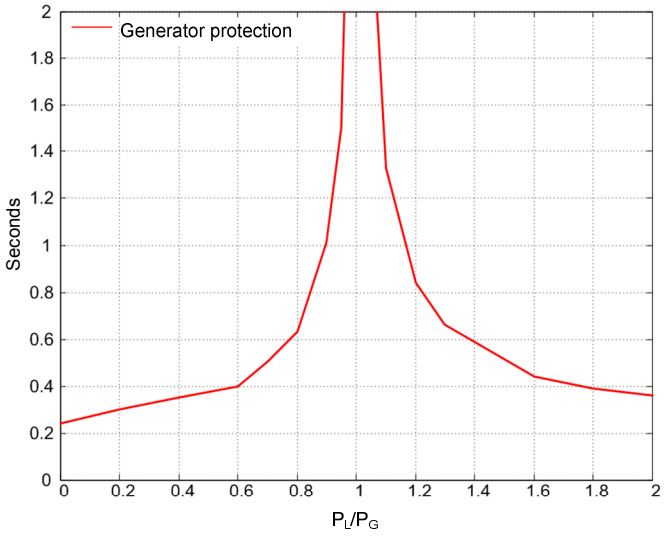

Fig. 5. Typical generator protection response time with respect to power flow

IV. Aurora Vulnerability Root Cause Is Lack of Security

The Aurora vulnerability exists because of an attacker's ability to access key protection and control systems. Any discussion of protection against the Aurora vulnerability must start with a review of security measures. Proper security for any system must be viewed as layers of protection with security in depth.

In order to execute an Aurora attack, the perpetrator must have knowledge of the local power system, know and understand the power system interconnections, initiate the attack under vulnerable system load and impedance conditions, and select a breaker capable of open/close switching that is fast enough to operate within the vulnerability window.

In order to access a protective relay, the attacker would need physical or electronic access to the relay. Assuming the attack initiated via remote electronic access, the perpetrator would need to understand and violate the electronic media, find a communications link that is not encrypted or is unknown to the operator, have no access alarm sent to the operators, know all passwords, or enter a system that has no authentication.

If using a protective relay for the attack, the perpetrator would also need to be able to communicate with the relay for controlling the appropriate circuit breaker, understand the engineering needed to initiate a fast trip and close, and disable any logic and protective elements preventing fast open/close operations. The logic diagram in Fig. 6 shows the conditions that are required for an Aurora attack.

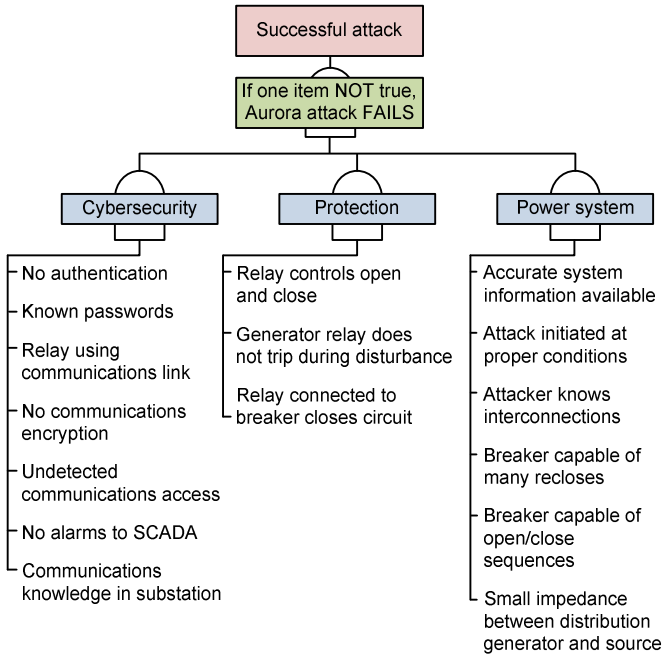

Fig. 6. System information needed to implement an Aurora attack

By initiating proper and prudent security measures, the Aurora vulnerability can be mitigated [2]. Proper security measures include, but are not limited to, the following:

- Know all communications paths to your assets and secure access. These include supervisory control and data acquisition (SCADA), energy management system (EMS), engineering access, maintenance, telephone lines, wireless, Internet, and interconnections and bridges between systems.
- Use strong passwords. Make sure your equipment makes use of strong length and character passwords (e.g., weak: Webster, strong: M$i4fp&r).
- Manage passwords. Do not use default passwords, change them periodically, change them when someone leaves the company, control them, and use different ones in different areas.
- Encrypt communications. Copper wire, fiber-optic and wireless SCADA, engineering, and maintenance all need to be encrypted.
- Practice "need-to-know." Keep your designs safe and secure. Limit access to system details to those who really need to know in order to do their jobs.
- Compartmentalize knowledge. Keep security information localized. Do not use the same security and passwords throughout the system or on multiple systems.
- For key assets, have more than one secure communications path. Minimize the impact of denial-of-service attacks, and send security alarms through a second path.
- Review alarms and access activity. Know which users are on your system and why.

- Do not forget physical security. Keeping the bad guys out of your cyberassets does not help if they can directly access equipment in the field or your data center.
- Guard your access tools. Keep laptop computers locked and encrypted. Keep your system drawings in a secure location with restricted access. Know who has keys, and set up multiple levels of access.

These guidelines help secure information channels and prevent unauthorized access. Be sure to use many of these ideas and develop a security in depth approach. If one security level is penetrated, have other levels between the attacker and your system.

V. Vulnerability Is System Dependent

The level of vulnerability to an Aurora attack is dependent on the configuration and operating characteristics of each system. For example, if the generators on a backup system only operate when disconnected from the main system feed, then there is no risk to the generator. For protection purposes, the risk can also be evaluated based on the power flow at the connection point. Systems can be broken into three groups, as follows:

- Systems with operating generation that still receive power from the grid. Systems like this may include industrial plants that create their own generation but still need to purchase power from the grid.
- Systems that approximately balance the power they generate with the power they need. The result is that little power is imported or exported.
- Systems that export power to the grid. The variations in power flow affect the ability and type of protection needed to detect an undesired disconnection.

VI. Protection Options

Several options for mitigating the Aurora vulnerability can be implemented to improve the protection scheme.

A. Breaker Closing Delay Supervision

Setting the protective relay and/or the open/close control of a circuit breaker to require a delay before closing can circumvent the opportunity window for an Aurora attack. This delay can be implemented either in the protective relay or with a simple time-delay relay installed in the breaker close circuit. This delay can be programmed to allow the mitigation devices to operate. This mitigation system is very low cost and reduces the vulnerability. Delaying the reclose time for a breaker can remove the vulnerability from the Aurora attack, but use of parallel breakers and secondary feed breakers must also be taken into account. Assuming the attacker already has access to the breaker and control switch, changing a timer setting is of low concern because the attacker would have many other options for damaging the system.

B. Breaker Command Supervision

If reclosing of the circuit breaker is required under some conditions, a command-monitoring scheme can be implemented in the protective relay. This scheme allows normal reclosing actions for fault conditions but blocks or delays the reclosing logic when initiated by any source other than the reclosing cycle. If unauthorized access from hacking the communications channel is still a concern, consider a reclosing supervision scheme. This supervision can be implemented in existing digital protective relay logic.

C. Reclosing Supervision

Another method to prevent unauthorized reclosing is to implement a second relay to supervise the main protection and control relay. This second relay would have no communications or external connections and could not be compromised via a communications hacker. Additionally, this second relay should have a different password and compartmentally separated access to this information. The second relay could also be physically installed in a separate location with different physical security.

D. Frequency Variation

One existing protection scheme uses a rotor tracking detection algorithm to detect isolation conditions caused by open local or remote breakers. The scheme uses positive-sequence memory voltage as a reference for calculating angular difference (angular displacement with its own reference) and acceleration. The memory is derived from a first order infinite impulse response (IIR) filter.

The relay detects an isolation condition if the angle difference exceeds the preset level, and acceleration/deceleration exceeds the preset threshold.

E. Island Detection Logic

This scheme uses a special element to detect the islanding condition. The characteristic provides a faster response relative to the conventional frequency and rate of change of frequency (df/dt) elements. The response of the element is blocked under fault conditions. Fig. 7 shows the element along with fault detection and blocking logic. This protection scheme can be implemented in existing relay logic.

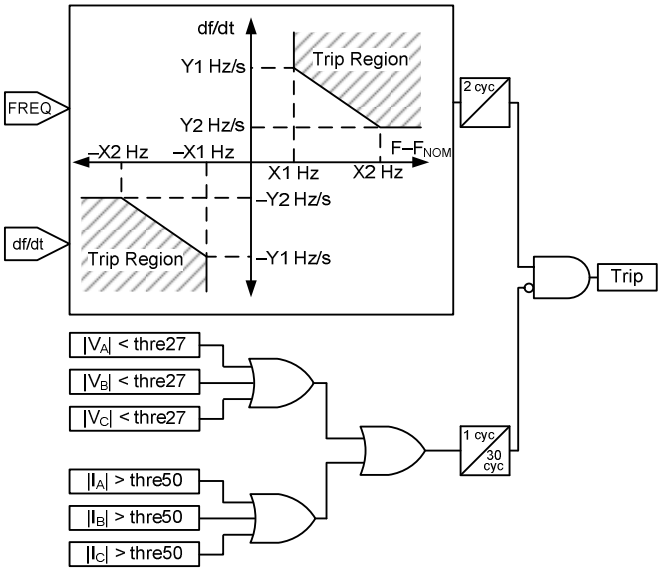

Fig. 7. Islanding detection logic in existing relay

F. Wide-Area Synchronized Phasor Measurement

The addition of time-synchronized phasor measurement within the protective relay has opened a new area of protection. The high-speed communication of phasor data from remote connections allows the application of wide-area measurements as part of the protective relay scheme. Control logic available today in protective relays can implement a fast slip-frequency-acceleration protection scheme, as shown in Fig. 8 and Fig. 9.

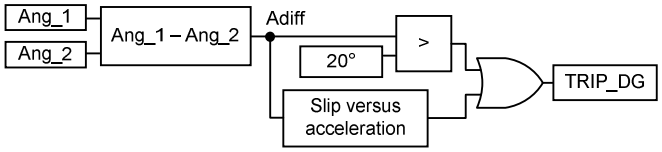

Fig. 8. Protection scheme uses angle difference, slip frequency, and acceleration

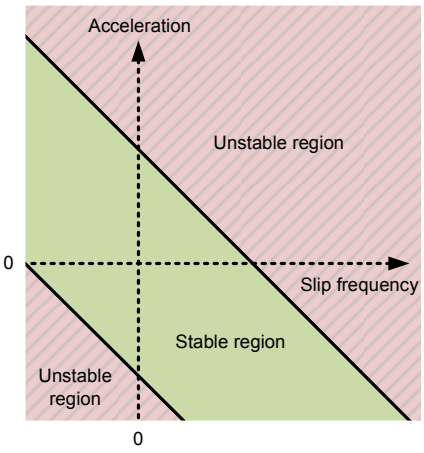

Fig. 9. Stable and unstable generator operating regions

This scheme protects the generator even when the frequency slip between the systems is slow.

VII. Real-Time Digital Simulator Testing Results

A real-time digital simulator test system, as shown in Fig. 10, was used to test some of the proposed protection schemes. The test cases included creating an intentional islanding condition by opening Breaker BY under different power flow conditions: power import, power export, and zero power exchange. Additionally, a simulation of a change in the positive-sequence voltage phase angle verified the time constant and the performance of the relays under test.

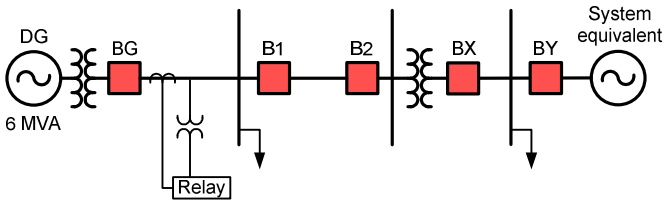

Fig. 10. Configuration of real-time digital simulator test system

Fig. 11 shows the performance of the detection elements for a power import condition. Local load (P_L) is 22 MW, and the local generation (P_G) is around 11.3 MW. Following the breaker opening, generation deficit causes the frequency to drop. The conventional underfrequency element, along with IIR and island detection logic (IDL), detected the event. The island detection logic detected the condition in 82 milliseconds, compared to 205 milliseconds for IIR and 338 milliseconds for the underfrequency element.

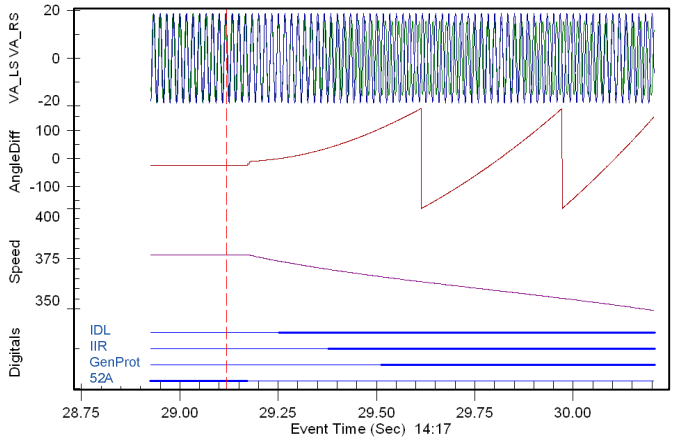

Fig. 11. Island detection logic isolates the rotating machine faster following the islanding condition

Fig. 12 shows the performance of the detection elements for a minimal power mismatch condition. Following the breaker open, generation closely but not exactly matches the load. Island detection logic and the standard generator underfrequency element detected the condition in about 1 second; however, IIR did not operate in a timely manner under this condition.

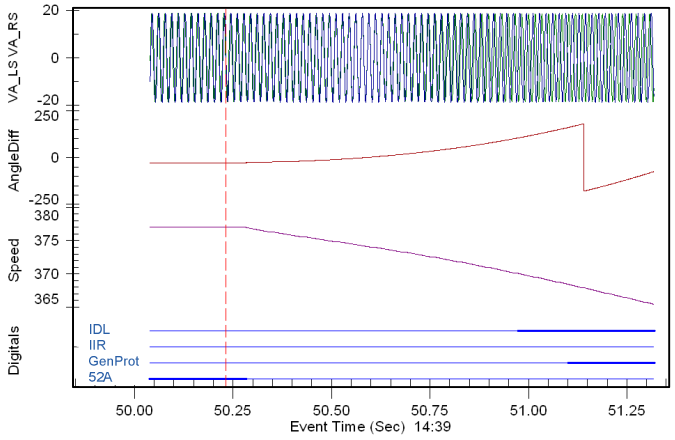

Fig. 12. IIR does not respond in a timely manner under minimal power mismatch conditions

A series of scenarios were simulated to capture the response of the detection elements for different power mismatch conditions. P_L was incrementally changed from 0 MW to 22.6 MW for each load condition. P_G was 11.3 MW.

Response times of the detection elements were recorded. Fig. 13 and Fig. 14 show a comparison of the response times and load variation. All schemes detected the islanding condition when the mismatch between the local generation and the load was significant. When the mismatch was minimal, the schemes that use local measurements did not operate in a timely manner. The wide-area logic scheme detects islanding conditions even under minimal mismatch conditions.

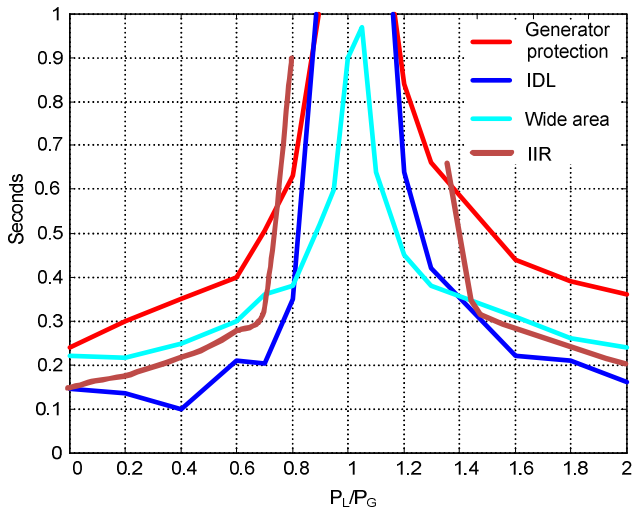

Fig. 13. Relay response time for detecting the islanding condition

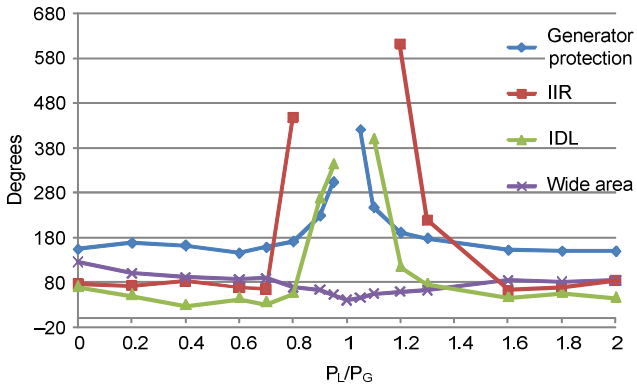

Fig. 14. Response to island condition measured in degrees of slip

Fig. 15 shows the response times during power export conditions ($P_L/P_G < 1$), while Fig. 16 shows the response times during power import conditions ($P_L/P_G > 1$).

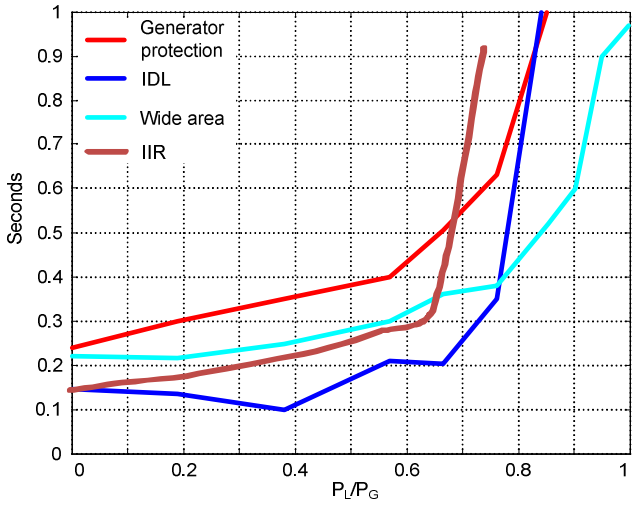

Fig. 15. Response times for power export conditions

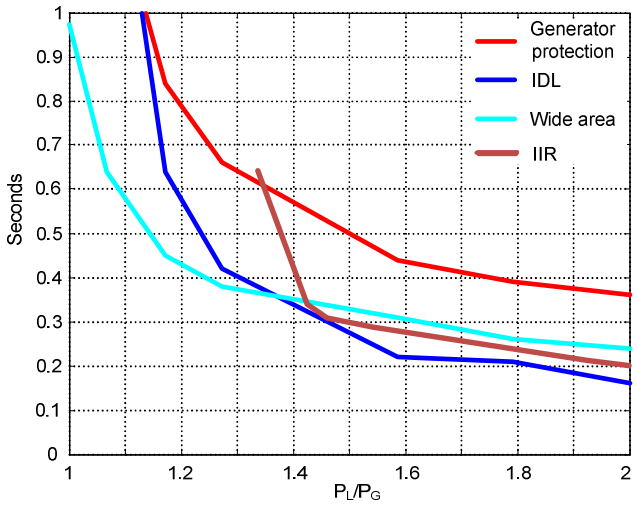

Fig. 16. Response times for power import conditions

VIII. Conclusion

System owners must contend with not only accidental faults to the system but also targeted attacks seeking to damage equipment. Proper security must become a standard operating policy.

Implementing proper security, including system, information, access, passwords, and encryption, produces an effective barrier to the Aurora attack.

Additionally, existing protection schemes can be implemented to mitigate the Aurora vulnerability. Protective relay schemes were modeled using a real-time digital simulator, and the results compared. While no silver bullet exists for perfect protection, this testing clearly shows existing digital relays with proper protection schemes offer protection against Aurora attacks.

While the standard generator protection did operate well under most conditions, it did not operate in a timely manner under near balanced load conditions. Three protective relay schemes were evaluated. Wide-area synchronized phasor measurement, island detection logic, and IIR were directly compared. Wide-area synchronized phasor measurement had

the best overall performance under all operating conditions. Island detection logic provided the fastest protection but was slow near balanced operating conditions. IIR operated in most conditions but was slow with minimal power exchange.

IX. References

[1] J. Meserve, "Staged cyber attack reveals vulnerability in power grid," CNN, September 26, 2007. Available: http://www.cnn.com/2007/US/09/26/power.at.risk/index.html.

[2] E. O. Schweitzer, III, "Twelve Tips for Improving the Security of Your Assets," August 26, 2006. Available: http://www.selinc.com.

X. Biographies

Doug Salmon graduated from the U.S. Air Force Academy in 1978 with a degree in aeronautical engineering. He was a special operations helicopter pilot and commanded at the squadron and group level in Europe and Asia. He had two tours in the Pentagon in the Office of Secretary of Defense and Headquarters Air Staff. He has a masters degree in systems management from the University of Southern California and a masters degree in national resource strategy from the National Defense University in Washington, D.C. Prior to joining Schweitzer Engineering Laboratories, Inc. (SEL) in 2008, he was the Air Force ROTC Commander at Washington State University and the University of Idaho and retired from the military after 30 years of service to his country. Doug is currently the director of government engineering solutions in the government services division of SEL.

Mark Zeller received his BS from the University of Idaho in 1985. He has broad experience in industrial power system maintenance, operations, and protection. He has worked over 15 years in the paper industry, working in engineering and maintenance with responsibility for power system protection and engineering. Prior to joining Schweitzer Engineering Laboratories, Inc. (SEL) in 2003, he was employed by Fluor to provide engineering and consulting services. He has been a member of IEEE since 1985.

Armando Guzmán received his BSEE with honors from Guadalajara Autonomous University (UAG), Mexico. He received a diploma in fiber-optics engineering from Monterrey Institute of Technology and Advanced Studies (ITESM), Mexico, and his MSEE from the University of Idaho, USA. He lectured at UAG and the University of Idaho on power system protection and power system stability. Since 1993, he has been with Schweitzer Engineering Laboratories, Inc. in Pullman, Washington, where he is presently research engineering manager. He holds several patents in power system protection and metering. He is a senior member of IEEE.

Mangapathirao "Venkat" Mynam received his MS in electrical engineering from the University of Idaho in 2003 and a BS in electrical and electronics engineering from Andhra University College of Engineering, India, in 2000. He is presently working as a research engineer with Schweitzer Engineering Laboratories, Inc. He is a member of IEEE.

Marcos Donolo received his BS in electrical engineering from Universidad Nacional de Rio Cuarto, Argentina, in 2000, and his masters degree in electrical engineering (2002), his masters degree in mathematics (2005), and his Ph.D in electrical engineering (2006) from the Virginia Polytechnic Institute and State University. Since 2006, he has been with Schweitzer Engineering Laboratories, Inc. in Pullman, Washington, where he is presently a research engineer. He is a member of IEEE.