Myth or Reality – Does the Aurora Vulnerability Pose a Risk to My Generator?

Mark Zeller
Schweitzer Engineering Laboratories, Inc.

This paper was presented at the 64th Annual Conference for Protective Relay Engineers and can be accessed at: http://dx.doi.org/10.1109/CPRE.2011.6035612.

For the complete history of this paper, refer to the next page.

Published in
Sensible Cybersecurity for Power Systems: A Collection of Technical Papers Representing Modern Solutions, 2018

Previously presented at the
64th Annual Conference for Protective Relay Engineers, April 2011

Originally presented at the
37th Annual Western Protective Relay Conference, October 2010

Myth or Reality – Does the Aurora Vulnerability Pose a Risk to My Generator?

Mark Zeller, *Schweitzer Engineering Laboratories, Inc.*

***Abstract*—There have been many reports of cyberintrusions, hacking, unauthorized operations, and malicious attacks on the electric power system. Many of these reports are uncorroborated and strengthen the skepticism of the very people in position to prevent these invasions. One vulnerability that has drawn substantial discussion is the Aurora vulnerability, which focuses on electric power generators. Since the dramatic video and interview on the television news in 2007 showing how to cause severe damage to a generator, many generation providers are concerned they could become a victim. This paper discusses the Aurora vulnerability, how it is implemented, what the risk factors are, who is vulnerable, and what steps will mitigate this risk.**

Standard generator protection is not sufficient to thwart a well-executed Aurora attack. This paper presents how the Aurora vulnerability works, what key indicators show a risk, what different methods can be used to initiate an attack, and what modifications can be made to control systems to minimize risk. Many of the recommendations from this paper are low-cost mitigation techniques that can readily be incorporated into standard practices at a generating facility. Comprehensive mitigation techniques include protection and control, electronic and physical security, monitoring, training, risk assessment, and information protection. Making positive changes in these areas can help to maintain control of generators and protect these critical assets.

I. How Can an Aurora Attack Damage a Generator?

Connecting a generation source to the electric grid involves coordinating several key parameters. Frequency, voltage, and phase rotation must be matched for a successful connection. Protective relays monitor both the generator and the main network power systems and allow connections only when these key parameters are within a pre-set tolerance (synchronism). To improve reliability and robust power supply from the generator, these tolerances allow for small variations over short periods without prematurely separating the generation sources. The Aurora attack seeks to use this tolerance in the protection to cause damage to the generator.

The Aurora attack attempts to intentionally open a breaker and close it out of synchronism, as shown in Fig. 1. The resulting mechanical and electrical stress can cause damage to equipment on the system. Generators, motors, transformers, and adjustable frequency drives are all susceptible, with generators on top of the list of most likely targets of attack. Good engineering practice includes synchronism check enabled on relays installed in the power system to prevent out-of-synchronism closing.

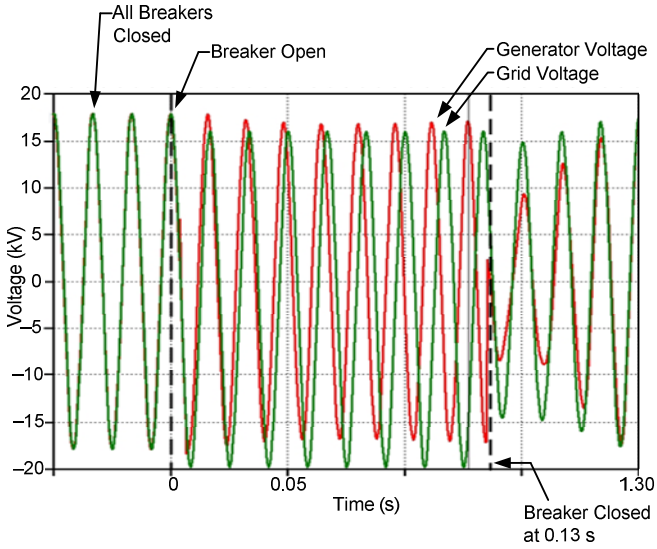

Fig. 1. Aurora attack scenario

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 protection engineers to reevaluate comprehensive generator protection.

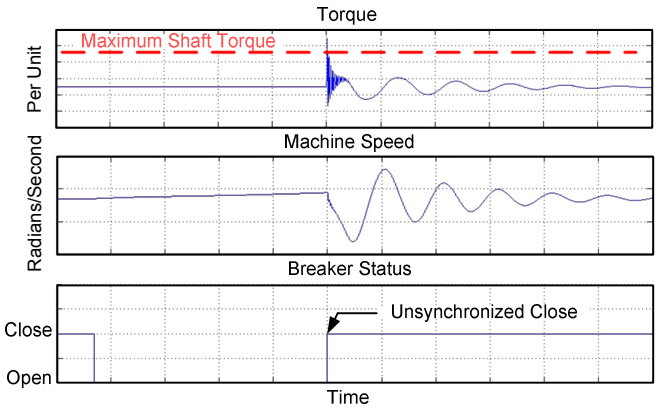

Fig. 2. Aurora attack and generator torque, speed, and breaker status

It is helpful to review typical generator protection elements and response times in order to establish the size of the window of opportunity for an Aurora attack. A typical modern ac generator is protected using the elements in Table I.

TABLE I
TYPICAL ELEMENTS IN A GENERATOR PROTECTION SYSTEM

Protection Element	Typical Response Time	Response to Aurora Attack
Phase distance (21)	Time delay is typically 0.5 to 1.0 s.	Element is sensitive to lower impedance, not higher, of open breaker. Does not operate.
Volts/hertz (24)	Time delay is 1.0 s.	Generator does not overexcite quickly. Does not operate.
Synchronism check (25)	Angle difference is 15 degrees or less.	Local breaker will not see loss of synchronism. Remote breaker with 25 element will respond in less than 3 cycles.
Undervoltage (27)	Time delay is not built into element.	Element action depends on rate and magnitude of voltage decay.
Reverse or low forward power (32)	Time delay is 20 s; prime mover should trip first.	Element may see motoring condition. Does not operate.
Loss of field (40)	No delay on Zone 1. Time delay is 0.50 s on Zone 2.	Element does not operate.
Overcurrent (50)	Response time is dependent on current magnitude and curve selection.	Element does not see overload until after breaker close. Does not operate.
Voltage controlled or voltage restrained time overcurrent (51VC)	Time delay is 3 s, if voltage is less than 80%.	Element does not see overload until after breaker close. Does not operate.
Overvoltage (59)	Time delay is not built into element.	Element does not operate with typical settings. Action depends on rate and magnitude of voltage growth.
Stator ground (64)	Minimum time delay must allow transmission fault-clearing time.	Element does not operate.
Out of step (OOS) (78)	Time delay is 3 s.	Element would not see OOS for action at remote breaker. Does not operate.
Overfrequency (81)	Time delay is 0.03 s minimum.	Element can pick up depending on settings.
Underfrequency (81)	Time delay is 0.03 s minimum.	Element can pick up depending on settings.
Current differential (87)	Minimum time delay must allow transmission fault-clearing time.	Element does not operate. High differential would not be expected on breaker closing.

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

The Aurora vulnerability is not limited to a specific type of generator. All generator types have some risk. The high current impulses applied by an Aurora attack can also have a detrimental effect on other equipment. Surges of current through a transformer reduce its useful life expectancy, and the magnetic fields cause the windings to flex, exposing the transformer to possible failure. When opened under excessive loads, circuit breakers can suffer damage to the contacts. Under certain conditions, the breaker could experience twice the nominal voltage, allowing the possibility of damage or flashover.

The North American Electric Reliability Corporation (NERC) and the Federal Energy Regulatory Commission (FERC) have required all utilities to identify critical infrastructure within their systems. Whether or not generators fit within the identification as critical infrastructure, owners and operators need to evaluate the risk posed by the Aurora attack, decide on the appropriate response, and identify how much risk is acceptable.

II. TYPES OF AURORA ATTACKS

The intent of the Aurora attack is to disable or destroy critical electrical equipment on the grid; the methods used to initiate the attack can vary widely. The following list of possible attack scenarios is not an extensive or all-inclusive list, but it is intended to encourage the reader to analyze a variety of possible attacks when evaluating system preparedness:

- Manual physical attack. The perpetrator of this attack attempts to use the manual breaker open/close switch at the substation to initiate an attack. Although this type of attack is much less precise and does not specifically target an out-of-phase closing angle, the random and possibly repeated out-of-phase breaker closing could result in torque damage on the generator. Physical access to the open/close controls of the circuit breaker is a growing concern. Typical protection schemes do not always include manual switches in the protection logic. Careful consideration of all sources of open/close commands must be included in any review.
- Compromised communications channel. Using this attack strategy, the perpetrator interrupts the normal communications link to the breaker control device and injects a series of commands intended to open and close the breaker out of synchronism. Any communications channel on the relay should be included in the review process. Unguarded access channels can provide a security breach, enabling an unauthorized series of commands. Many sources of information exist on protecting communications channels; see the references in this paper [1][2][3][4].

- Direct hack into the relay. This attack scenario uses a communications port on the relay as an access point to the protection and control algorithms within the relay. With direct access to the relay, the perpetrator can control the breaker and modify or eliminate the protection algorithms. Most relays provide passwords and access levels that restrict permission to programming and control functions. The first rule of security is: do not use the default passwords.
- Embedded program in the relay. This attack not only compromises the integrity of the relay but also embeds a series of commands within the logic or operating system of the relay, including a trigger set to initiate at a set time or power level or in coordination with other attacks. Checking the file size and modification date at the time of commissioning and during operation can be a valuable indication of unauthorized changes to the relay programming. Programs to check the integrity of files, such as Message-Digest algorithm 5 (MD5), can provide a higher level of security.

III. Why Does Typical Generator Protection Not Mitigate the Aurora Vulnerability?

The Aurora attack seeks to exploit the opportunity to connect two electrical systems out of synchronism. This opportunity could arise from an unprotected system or a system not configured to recognize the threat of an Aurora attack. The Aurora attack seeks to take advantage of the time delay between a protective relay recognizing an out-of-synchronism issue and the initiation of a protection action. Protective relays continuously sample the voltage and current of the power system and calculate other key protection information based on these samples. The relay must be able to separate a bad data sample from a sudden change in the measured variable. This process of sample verification and signal processing is referred to as filtering [5]. One example of filtering is to average a number of inputs together and use the calculated average for protection decisions. This averaging process helps smooth the signal, but it reduces the speed of the relay for recognizing sudden changes in the system. In order to keep the system connected and avoid separating based on variations in the power system, protection engineers also typically add time delays in the trip command sequence. These delays, either from signal processing or intentional design, open a window of opportunity for attack.

As shown in Fig. 3, the Aurora attack is designed to open a circuit breaker, wait for the system and generator to slip out of synchronism, and reclose the breaker, all before the protection system recognizes and responds to the attack. The window of opportunity can be narrowed by analyzing the response time of the generator and circuit breaker protection elements. Traditional generator protection elements typically actuate and block reclosing within 15 cycles (see Table I). Many variables affect this time, but the discussion in this paper uses this estimate for the Aurora window of opportunity.

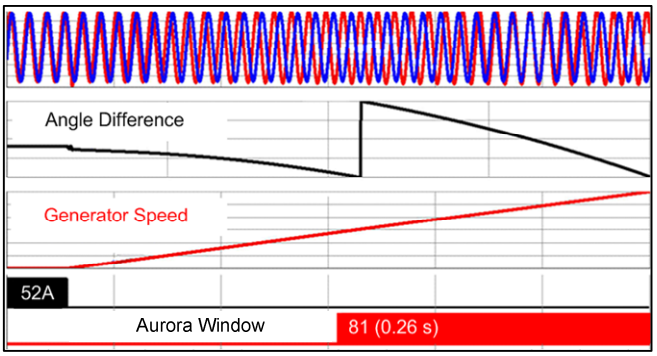

Fig. 3. Aurora window of opportunity

Another contributing factor to why typical generator protection does not guard against an Aurora attack is that the attack may not be initiated at the generator (see Fig. 4). By initiating the attack at a system tie point away from the generator, the synchronism-check element at the generator does not measure a difference between the two systems. This targeting of the tie-in breakers instead of the generator requires the protection engineer to expand the scope of typical generator protection to include the surrounding system tie points.

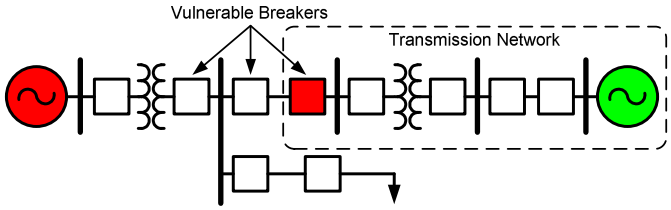

Fig. 4. The target of the Aurora attack is the grid tie-in circuit breaker

IV. Are All Generators at Risk?

The level of vulnerability to an Aurora attack is dependent on the configuration and operating characteristics of each system. For example, if the generator is on a backup system or only operates when disconnected from the main system, there is little Aurora risk to the generator. Generators connected to the grid through a single tie line are the most likely targets. These systems only need a single circuit breaker compromised for an attack to be initiated. In cases where the generating facility and utility are owned or controlled by separate parties, the mitigation protection becomes more difficult. These installations typically lack the communications links that indicate the tie-breaker position. Without this indication, the generating facility must evaluate protection schemes that only require local data. Single-tie generating stations are the applications most likely to benefit from an Aurora hardware mitigation device.

Power flow is an important variable when assessing the Aurora vulnerability. For protection purposes, the risk should 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.

Each of these groups provides a different system response and vulnerability window. System evaluation should analyze an attack under each operating condition.

V. Mitigating the Aurora Attack

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

A. Synchronism-Check Breaker Closing Supervision

Implementing the synchronism-check function in all protective relays that potentially connect two systems together is a key step in the mitigation process. The functionality and speed of the synchronism-check element make it a very effective tool.

Key settings, such as allowable frequency and rate of change of frequency, need to be evaluated and set appropriately. Any point on the system that can potentially connect two sections of the grid should be supervised with synchronism-check protection. The synchronism-check function is fast, reliable protection against connecting together unsynchronized systems. The element works by monitoring the voltage and frequency on both sides of the breaker. The element prevents closing unless the voltage and frequency are within pre-set limited values. Fig. 5 shows the synchronism-check element angle setting range. Additionally, the synchronism-check element monitors the rate of change of frequency and prevents closing above a set rate. Including synchronism check only on the generator breaker does not mitigate the Aurora attack. The addition of synchronism check must also be expanded to all points of possible separation.

Synchronism check in a microprocessor-based protective relay operates very fast. An out-of-synchronism condition can be recognized and used to inhibit breaker closing within 3 cycles. Fast action from the synchronism-check element can be an effective mitigation tool against the Aurora attack if its scope is expanded to include all possible close commands, not just the usual synchronizing close command. Setting the parameters of the synchronism-check element requires a careful review of the power system parameters and consideration of loading and generator performance. A Real Time Digital Simulator (RTDS®) is an excellent resource to model the power system.

One solution is to turn off the synchronism enable logic until it is requested by a trusted source. The synchronism check would only allow closing after this request and the systems are synchronized. This prevents unintended reclosing of the circuit breaker.

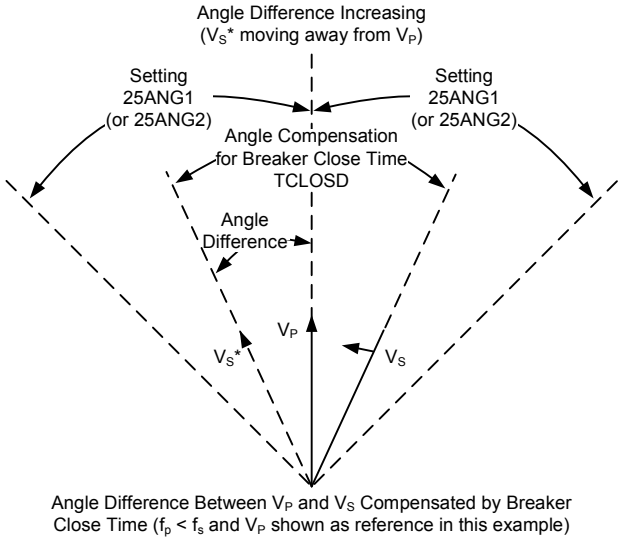

Fig. 5. Synchronism protection functionality

B. Time Delay on Breaker Closing

Setting the protective relay and/or the open/close control of a circuit breaker to require a delay before closing can eliminate the opportunity window for an Aurora attack. Manually switching the pistol grip trip/close switch can be executed in about 100 milliseconds. Installation of a time-delay relay on bus-tie breakers can provide the time needed for the generator protection to implement its own isolation or prevent manually switching the trip/close switch. Implementing a delay on closing mitigates this type of manual attack. This delay can be implemented either in the protective relay or with a simple time-delay relay installed in the breaker close circuit. The circuit shown in Fig. 6 illustrates a simple installation of a time-delay relay installed in a close circuit. The reset can be triggered from several sources, such as the trip/close switch or the breaker position contacts. Be sure to include all switches when deciding where to install the delay contacts.

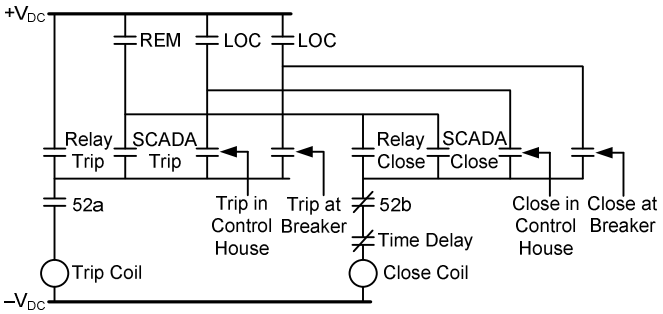

Fig. 6. Simplified circuit breaker control

This delay can be programmed to allow the protection elements to pick up and operate. This mitigation is very low cost and reduces the vulnerability. Delaying the reclose time for a breaker can reduce the vulnerability to the Aurora attack, but use of parallel breakers and secondary feed breakers must also be considered. Implementing a time delay on closing without synchronism check can be bypassed by using one breaker to open the circuit while using a second parallel breaker to close. Aurora mitigation logic, such as close delays and synchronism check, should be implemented on all circuit breakers capable of isolating the generator from the main grid.

C. Breaker Command Supervision

Protective relays not only provide protection and local control, but open and close commands can be initiated remotely through many communications channels. Implementing time delays on breaker closing must also include close commands issued through the communications channels. A command-monitoring scheme can be implemented in the protective relay to monitor the number of close commands received within a fixed time period. This monitor can not only delay closing but also serve as a warning of possible communications issues or unauthorized access. When implementing the close-delay logic, evaluate the system needs and possible use of reclosing actions of the protective relay.

Allow for normal reclosing actions for fault conditions, but block or delay the closing logic when initiated by any source other than the reclosing element. Reclosing should be disabled on the relay if the breaker can be configured in the system as the tie between the generator and the main grid. Be sure to account for all sources of open/close commands, including supervisory control and data acquisition (SCADA), engineering, manual substation, manual breaker, relay logic, and automatic reclosing logic.

D. Redundant Reclosing Supervision

Another method to prevent unauthorized closing of the circuit breaker is to implement a second relay to supervise the main protection and control relay. This second relay should have no communications or external connections, so it cannot be compromised by a communications hacker. Additionally, this second relay should have a different password than the main relay and be physically installed in a location with different physical security. This scenario makes the assumption that the main relay could be compromised. Good security practices are essential to mitigating a cyberattack or physical attack.

E. Local Generator Island Detection Logic

To protect the generator using only local measurements, some protection schemes monitor the rate of change of frequency. This scheme uses a special element to detect an 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. The settings can be tuned to achieve the desired speed and sensitivity.

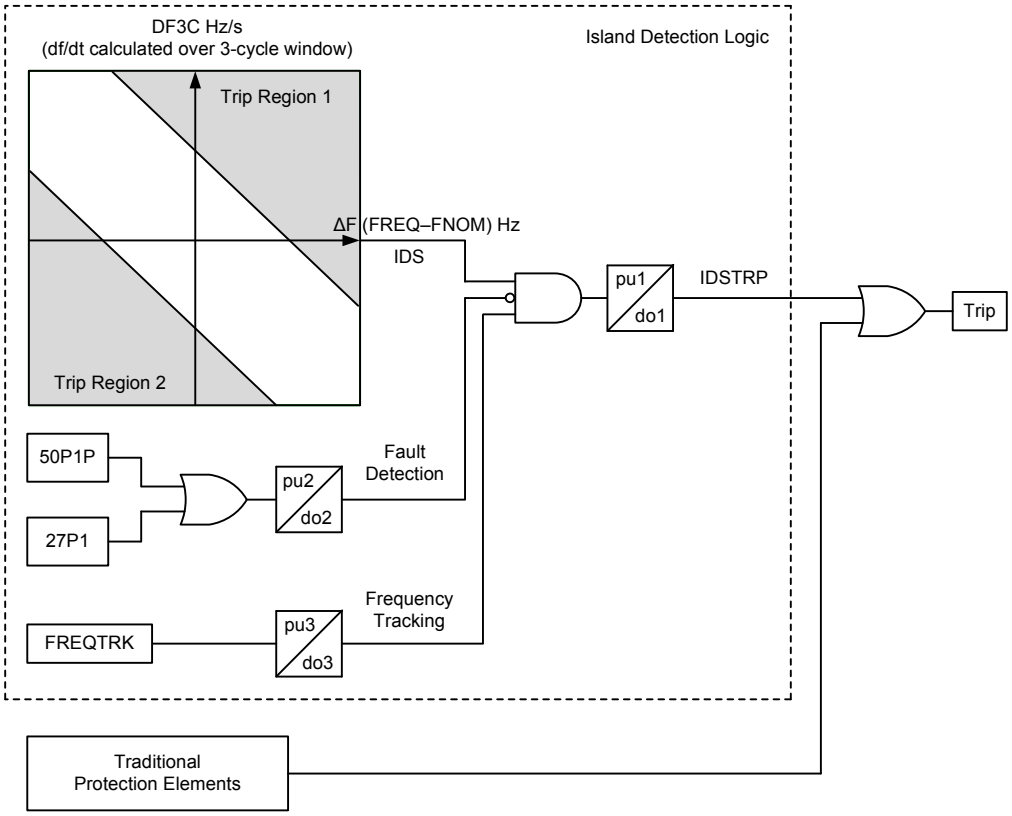

Fig. 7. Island detection logic in existing relay

The addition of time-synchronized phasor measurements 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.

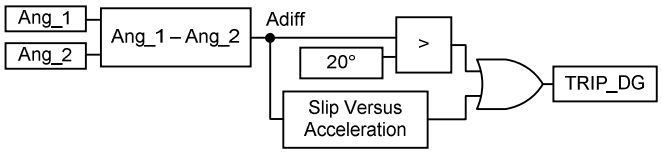

Fig. 8. Protection scheme uses angle difference, slip frequency, and acceleration

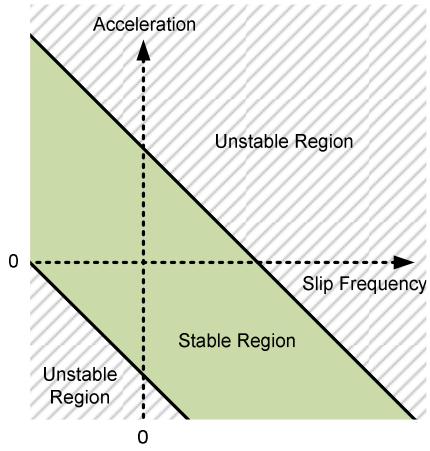

Fig. 9. Stable and unstable generator operating regions

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

VI. Security Considerations to Mitigate an Aurora Attack

The Aurora attack can easily target systems that have little or no security. Take proper security precautions to protect your system from both physical attacks and cyberattacks. Many technical papers are available to show proper methods of securing substations or communications networks [1][2][3][4]. An electric utility communications system is typically isolated from the public Internet system. This isolation provides one level of protection but is insufficient by itself to prevent a cyberattack.

Any assessment 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 [6].

In order to execute a successful 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 opening and closing quickly enough to operate within the vulnerability window.

In order to access a protective relay, the attacker needs physical or electronic access to the relay. Assuming the attack is initiated via remote electronic access, the perpetrator needs to understand and violate the electronic media, find a communications link that is not encrypted or is unknown to the operator, ensure no access alarm is 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 also needs to be able to communicate with the relay to control the appropriate circuit breaker, understand the engineering needed to initiate a fast trip and close, and disable any logic and protection elements preventing fast open/close operations.

Some basic security considerations include:

- Know and secure all communications paths to your system assets. These paths include SCADA, energy management system (EMS), engineering access, report collection, maintenance, telephone lines, wireless, Internet, and interconnections and bridges between systems.
- Use strong passwords. Make sure your equipment uses 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 links 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 them 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.
- Have more than one secure communications path for key assets. 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.
- Remember 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 system drawings in a secure location with restricted access. Know who has keys, and set up multiple levels of access.

By initiating proper and prudent security measures, the Aurora vulnerability can be mitigated [7].

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

Commonly used operating systems on personal computers have long been recognized as a security risk. Recent events have also demonstrated vulnerabilities of proprietary operating systems supplied by equipment manufacturers [8]. These attacks reinforce the need to review all system access points, only use trusted sources of code, and validate all program updates with security verification checks.

VII. Conclusion

Does the Aurora vulnerability pose a risk to your generator? The answer depends on the connection and protection details. Is the Aurora vulnerability a myth? Unfortunately, the answer is no; on an unprotected system, the Aurora vulnerability is a reality. Existing technology, much of it very low cost, is available to mitigate this risk.

The best place to start is to review your power system and generator protection schemes, keeping in mind the intent of the Aurora attack. Analyze system tie points, and review the protection logic through all the breaker connection possibilities. Review the power generation and power flow to estimate the rate of change of frequency when a bus-tie breaker opens and optionally closes under load. Make informed decisions to determine if your generator could be susceptible to attack.

If the generator and bus-tie breakers can be operated in a configuration that poses a possible Aurora risk, take proper steps to mitigate the risk. Executing synchronism-check protection on bus-tie breakers is an obvious starting point. Implement proper security, including system information, access, passwords, and encryption, to produce an effective barrier to the Aurora attack.

Additionally, existing protection schemes can be implemented to mitigate the Aurora vulnerability. Schemes can vary in sophistication from simple to complex. Each system and tie arrangement will need individual review.

Do not discount the risk of a manual physical attack. Keep substations well lit, locked, and monitored. Guard your communications channels, including SCADA, engineering, and maintenance PCs. Keep system information secure, and follow defense-in-depth security practices.

While no one solution exists for protection against attack, testing clearly shows existing digital relays with proper protection schemes offer mitigation against Aurora attacks [6].

While standard generator protection does not provide complete protection from the Aurora attack, modifications to the protection scheme can provide mitigation.

VIII. References

[1] D. Anderson, "Securing Modern Substations With an Open Standard Network Security Solution," proceedings of the 11th Annual Western Power Delivery Automation Conference, Spokane, WA, April 2009.

[2] C. Ewing, "Engineering Defense-in-Depth Cybersecurity for the Modern Substation," proceedings of the 12th Annual Western Power Delivery Automation Conference, Spokane, WA, April 2010.

[3] D. Anderson and N. Kipp, "Implementing Firewalls for Modern Substation Cybersecurity," proceedings of the 12th Annual Western Power Delivery Automation Conference, Spokane, WA, April 2010.

[4] D. Dolezilek and L. Hussey, "Requirements or Recommendations? Sorting Out NERC CIP, NIST, and DOE Cybersecurity," proceedings of the 12th Annual Western Power Delivery Automation Conference, Spokane, WA, April 2010.

[5] E. O. Schweitzer, III, and D. Hou, "Filtering for Protective Relays," proceedings of the 47th Annual Georgia Tech Protective Relaying Conference, Atlanta, GA, April 1993.

[6] D. Salmon, M. Zeller, A. Guzmán, V. Mynam, and M. Donolo, "Mitigating the Aurora Vulnerability With Existing Technology," proceedings of the 36th Annual Western Protective Relay Conference, Spokane, WA, October 2009.

[7] E. O. Schweitzer, III, "Ten Tips for Improving the Security of Your Assets," November 2009. Available: http://www.selinc.com.

[8] G. Mintchell, "Siemens Updates Response to Virus Attack," *Automation World Magazine,* July 19, 2010. Available: http://www.automationworld.com/news-7325.

IX. Further Reading

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.

X. Biography

Mark Zeller received his BSEE from the University of Idaho in 1985. He has broad experience in industrial power system maintenance, operations, and protection. He 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. in 2003, he was employed by Fluor to provide engineering and consulting services. He has been a member of IEEE since 1985.

Previously presented at the 2011 Texas A&M Conference for Protective Relay Engineers.

20110217 • TP6452-01