Common Questions and Answers Addressing the Aurora Vulnerability

Mark Zeller
Schweitzer Engineering Laboratories, Inc.

Presented at the
DistribuTECH Conference
San Diego, California
February 1–3, 2011

Common Questions and Answers Addressing the Aurora Vulnerability

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. One security risk that has drawn substantial attention is the Aurora vulnerability, focused on electric power generators. Since the dramatic video and television news interview in 2007 showing how to cause severe damage to a generator, many generation providers, including distributed 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 mitigate this risk.**

Standard generator protection is not sufficient to thwart a well-executed Aurora attack. This paper addresses commonly asked questions about the Aurora attack, including what is real and what is exaggeration. Each question is answered with commonsense solutions that can be implemented with existing low-cost technology.

I. What Is the Aurora Vulnerability?

The intent of the Aurora attack is to intentionally open a breaker and close it out of synchronism to cause damage to connected power system equipment, such as generators, motors, and transformers. When an out-of-synchronism close is initiated, the resulting high electrical current and torque translate to stress on the mechanical shaft of rotating equipment. This stress reduces the life of the rotating equipment and can possibly destroy it. Fig. 1 shows a typical oscillograph of an Aurora event.

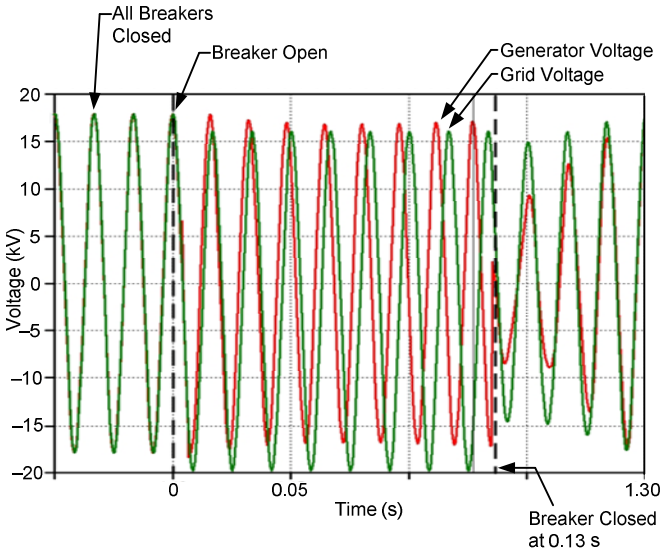

Fig. 1. Aurora attack scenario

The relationship between the breaker, machine speed, and shaft torque during an Aurora event is shown in Fig. 2.

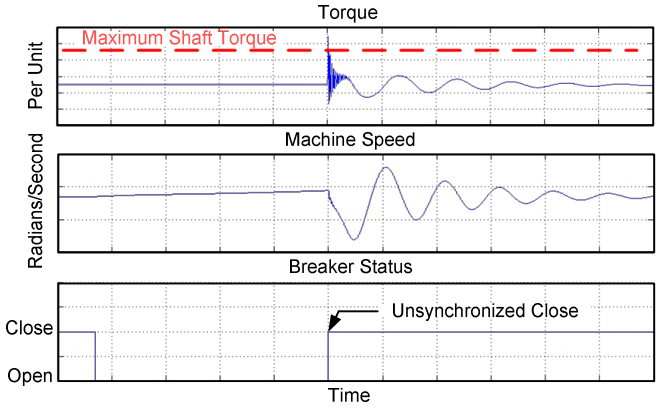

Fig. 2. Aurora attack generator torque, speed, and breaker status

The Aurora vulnerability exists because of an attacker's potential 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 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 open/close switching that is fast enough to operate within the vulnerability window.

II. What Equipment Is at Risk?

Generators, motors, transformers, and adjustable frequency drives are all susceptible, with generators at the top of the list of most likely targets of attack. 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 can 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) require 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.

III. Was the Demonstration Attack Valid?

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 CNN report sensationalized the potential risk presented by the Aurora attack.

The CNN video shows a large diesel engine driving a generator. The Aurora attack is initiated, and the video records the results. Several clearly noticeable physical jolts are observed, and small pieces of the coupling are ejected. The scenario is continued through more than a dozen hits until the room is filled with white smoke that erupts from the coupling. It was reported that accelerometer measurements recorded torque impacts up to five times normal. Both the engine and the generator were damaged. The engine was beyond repair and sold for scrap. The grid surrounding the test was monitored and reported no noticeable effects.

Although the team executing this demonstration claimed all of the protection was in place, obvious protection measures missing from this demonstration include the following: vibration monitoring limit switches, overspeed limitation on the diesel engine, and synchronism check on the tie breaker. Synchronism check was installed on the protective relay, but as part of the simulated cyberattack, it was disabled during the demonstration.

Some of the topics only briefly mentioned in the demonstration were the levels of security that were breached to achieve the access needed to accomplish the attack. Assuming this was a cyberattack, the perpetrators needed to know the power system connection schematic to target the right breaker. They needed to compromise a communications channel and be fortunate that it was not an encrypted link. After gaining access to the communications channel, they needed to have access to the protective relay settings, which would include at least one password level. In many relays, two separate levels with different passwords are needed to access protective relay settings. Assuming the attack was successful to this point, the protective relay would have alerted the supervisory control and data acquisition (SCADA) operator of programming level access granted by the relay. The demonstration passes these barriers off as trivial, but properly executed, good security practices can prevent this type of attack.

IV. Why Did the Generator Protection Not Work?

Connecting a generation source to the electric grid involves the coordination of 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 from the grid. 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.

The Aurora attack seeks to exploit the opportunity to connect two electrical systems out of synchronism. This opportunity can 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 [2]. 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 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 or 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 curve of the generator and timing of the circuit breaker protection elements. Traditional generator protection elements typically actuate and block reclosing in about 15 cycles. Many variables affect this time, and every system needs to be analyzed to determine its specific vulnerability to the Aurora attack.

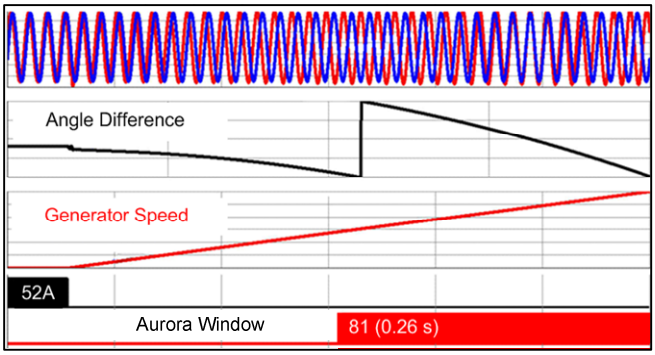

Fig. 3. Aurora window of opportunity

Another contributing factor as 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). If the attack is initiated at a system tie point away from the generator, the synchronism-check element at the generator will 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.

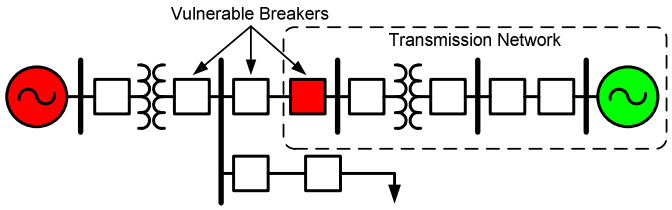

Fig. 4. The target of the Aurora attack is the grid tie-in breaker

V. Is Super Fast Protection Required?

Although the main focus of the Aurora attack is the potential 15-cycle window of opportunity immediately after the target breaker is opened, the overriding issue is how fast the generator moves away from system synchronism. In systems where generation approximately matches the local loading, synchronism match can be maintained for extended periods. Closing the tie breaker while the systems are still synchronized does not provide the current and torque shock needed to damage equipment. Waiting the time needed for the systems to drift out of synchronism provides the opportunity for an out-of-synchronism tie. Protection against the Aurora attack must provide protection for both fast disconnect/close and slow disconnect/close scenarios. The detection method for monitoring the rate of change of frequency from an Aurora attack must be faster than the typical frequency elements that protect equipment.

VI. Are There Many Methods of Attack?

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 can 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 on protecting communications channels exist; see the references in this paper [3][4][5][6][7].
- 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.

VII. How Do I Mitigate an Aurora Attack?

Several options for mitigating the Aurora attack can be implemented to improve the protection scheme. NERC does not endorse any particular solution and leaves the determination as to the best Aurora mitigation to good engineering practices by the entity. Although relay manufacturers have developed individual solutions to mitigate the Aurora threat, no single Aurora protection algorithm exists.

A. Synchronism-Check Breaker Closing Supervision

Implementing the synchronism-check function in all protective relays that can 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 mitigation tool. Key settings such as allowable frequency deviation 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.

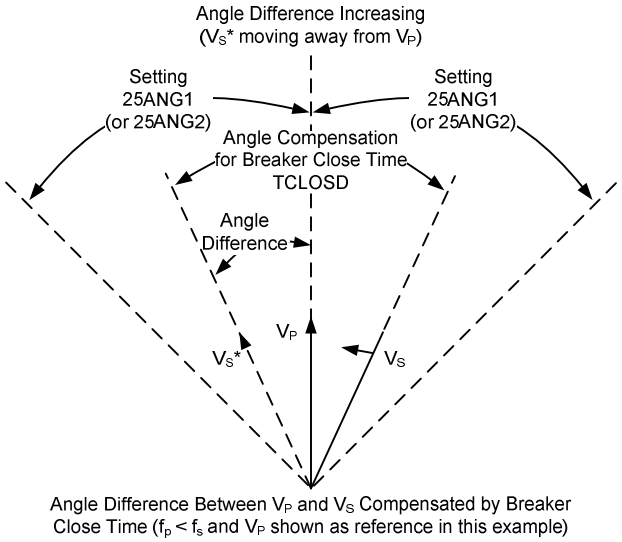

Fig. 5. Synchronism protection functionality

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. Include all manual switches in the synchronism-check logic. 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. Additional security can be achieved by using the logic in the protective relay to prevent breaker closing until synchronism check is initiated and satisfied. For mitigation, the synchronism check is initiated only after completing a sequence of checks that verify the system is prepared for a synchronized tie. These checks can include time delay, other breaker positions, or SCADA approval.

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 time delay can be triggered from several sources, such as the trip/close switch or the breaker position contacts. Be sure to include all manual switches when deciding where to install the delay contacts.

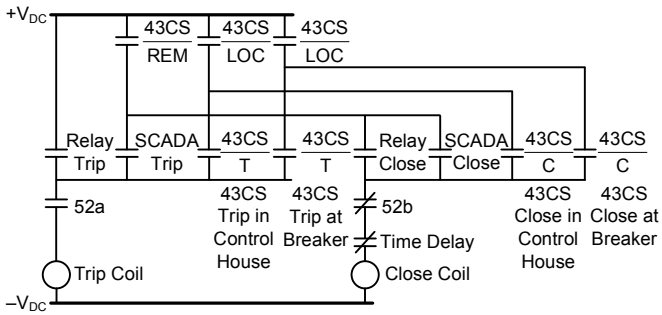

Fig. 6. Simplified circuit breaker control

This delay can be programmed to allow the protection elements to pick up and operate. This mitigation is very low cost and reduces 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 not only delays closing but also serves as a warning of possible communications issues or unauthorized access. When implementing the close delay logic, evaluate the system requirements and the possible use of reclosing logic in 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 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 protective 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 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 (81RF) 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.

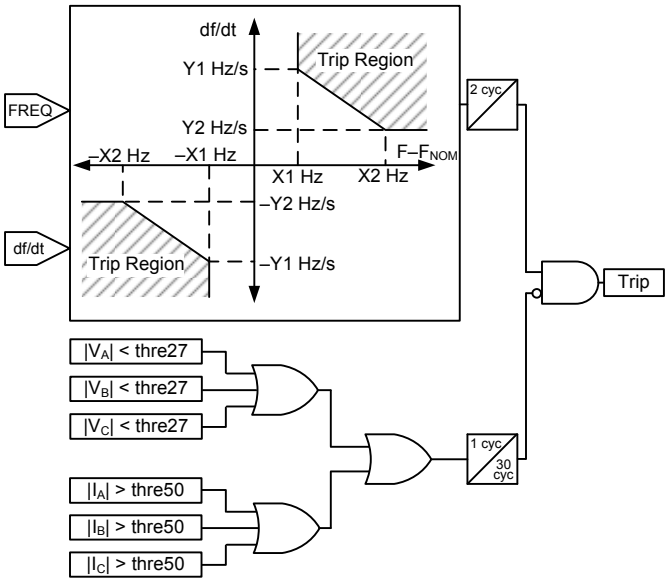

Fig. 7. Island detection logic in existing relay

This scheme is one of the "fence line solutions" discussed in the NERC library of information. Other variants of the rate of change of frequency method include using an average of several frequency measurements as the reference and comparing new measurements to the calculated reference. This method has the disadvantage of using a slower calculated reference; additionally, slow variations in the frequency cause the calculated reference to drift.

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.

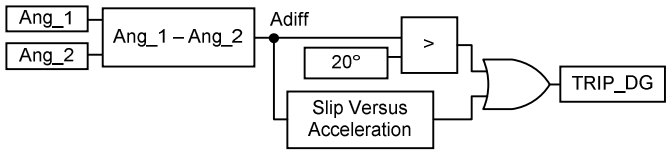

Fig. 8. Protection scheme uses angle difference, slip frequency, and acceleration

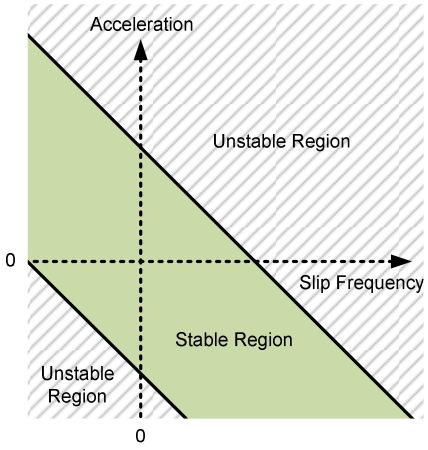

Fig. 9. Stable and unstable generator operating regions

This wide-area synchrophasor scheme protects the generator even when the frequency slip between the systems is slow. The example shown in Fig. 8 uses two measurements. A more robust design brings in measurements from many sources and provides more data for more advanced protection schemes.

VIII. Is a Hardware Mitigation Device Necessary?

NERC recommendations include the consideration of a hardware mitigation device (HMD) and outline key parameters needed in the event an HMD is selected as a mitigation tool. The recommendations *do not* specify the need for an HMD. Many times, if not always, existing protection and good security practices can mitigate the Aurora vulnerability. An HMD should be considered when existing protective relay schemes are unable to provide the level of protection required.

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 [3][4][5][6]. 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 an out-of-synchronism trip and close, and disable any logic and protection elements preventing damaging open/close operations. By initiating proper and prudent security measures, the Aurora vulnerability can be mitigated [8][9][10].

IX. Can an HMD Actually Make My System Less Reliable?

Frequently, if not always, the Aurora vulnerability can be mitigated by existing protection schemes and good security practices, as described in the references [3][4][5][6][9]. Owners should first determine if their security practices mitigate any possible Aurora risk on a case-by-case basis. When security practices suffice, the addition of another relay or HMD can be avoided, saving costs and the additional risk of misoperations that can lead to unintended shutdowns. Special consideration should be given any time an additional device is considered for connection to the trip bus of critical assets, such as generators. Even with the best HMDs or relays and with the best studies and installation, misoperations can arise from testing, installation, maintenance, bad settings, and so on. Although the risk is small, the consequences of tripping a unit are significant enough that, when alternatives are available, they should be considered.

Documentation in the Aurora information library set up for owners by NERC cautions owners about the risk of extended outages caused by the installation of HMDs.

X. Are Good Security Practices Sufficient to Meet the Aurora Mitigation Requirements?

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. This includes paths for SCADA, energy management systems (EMSs), 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 links and 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 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.

XI. Conclusion

Does the Aurora vulnerability pose a risk? The answer depends on the connection and protection details. On an unprotected system, the Aurora vulnerability does exist. Current 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. Implementing proper security, including system information, access, passwords, and encryption, can 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 needs 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, security, and monitoring offer mitigation against Aurora attacks [8].

XII. References

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

[2] 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.

[3] 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.

[4] 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.

[5] 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.

[6] 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.

[7] E. O. Schweitzer, III, D. Whitehead, A. Risley, and R. Smith, "How Would We Know?," proceedings of the 37th Annual Western Protective Relay Conference, Spokane, WA, October 2010.

[8] 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.

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

[10] M. Zeller, "Myth or Reality – Does the Aurora Vulnerability Pose a Risk to My Generator?," proceedings of the 37th Annual Western Protective Relay Conference, Spokane, WA, October 2010.

XIII. Further Reading

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

XIV. Biography

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 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 held positions in research and development, marketing, and business development. Mark has authored several technical papers and has patents pending through SEL. He has been a member of IEEE since 1985.