Application Note

Mitigating AURORA Vulnerability with Protective Relaying Basler Electric BE1-25 and BE1-FLEX

Vulnerability to cyber attacks is due in part to steps taken by electric utilities to transfer control of generation and distribution equipment from internal networks to supervisory control and data acquisition, or SCADA, systems that can be accessed through the Internet or by phone lines.

The move to SCADA systems boosts efficiency at utilities because it allows workers to operate equipment remotely, but this access to the Internet also creates more opportunity for cyber attacks. So far, incidents of hackers breaking into control systems to cause damage or outages have been scarce, although the threat of potential damage makes these control systems a target.

Physical threats, in the form of unmanned substations that are several buses removed from generating facilities, also have the potential for damaging generating facilities.

The responsible entities for these assets include the balancing authority, distribution provider, generator owner, generator operator, load-serving entity, reliability coordinator, transmission owner, and/or transmission operator.

NERC Issues AURORA Alert to Industry

The North American Electric Reliability Corporation (NERC) issued a recommendation to the industry on the AURORA vulnerability on Oct 14, 2010. The recommendation provided new sensitive and clarifying information regarding the nature of AURORA. The recommendation requires entities to report on efforts and progress by Dec. 13, 2010 with updates every six months until mitigation is complete.

The recommendation developed by the AURORA Technical Team, working with subject matter experts in the federal community, highlighted detailed engineering data and new understanding of the issue.

The recommended mitigation elements fall into two broad categories:

- Protection and Control Engineering Practices
- Electronic and Physical Security Mitigation Measures

NERC requires that members of the bulk power system implement protections against a vulnerability that could be exploited to cause physical damage to critical systems that provide electricity.

The AURORA Vulnerability

AURORA is a vulnerability to cyber or physical attacks that could sabotage critical systems providing electricity, including the national power grid. This vulnerability included in the NERC alert, involves protection and control systems associated with the operation of rotating machinery such as synchronous generators and motors. The objective of the AURORA attack is to exploit these vulnerabilities and intentionally destroy rotating machinery.

Most of us became aware of "AURORA vulnerability" in September 2007 when CNN (Cable News Network) reported on a test performed at the U.S. Department of Energy's (DOE) Idaho laboratory. CNN reported on Sept. 26, 2007 that a "Staged cyber attack reveals vulnerability in the power grid".

Based on publicly accessible documents produced since the DOE test, Figure 1 represents a one-line diagram of the test setup that may have been used in the DOE test.

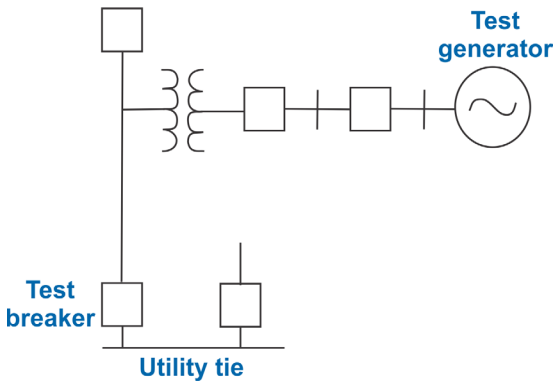

Figure 1 - Example of One-Line of the Test Setup

In the DOE AURORA scenario, the generator is connected to the power grid and carrying load. A hacker gains access to the test (tie) breaker open/close controls and opens the circuit breaker. At that instant, the synchronous connection between the generator and power grid is lost. When the hacker decides to close the breaker, the generator is no longer in phase with the power grid and is electrically "jerked" back into synchronism with the power grid. This condition creates high electrical torque that is converted to stress on the mechanical shaft of the rotating equipment. This stress reduces the life of the rotating equipment and can destroy it. Further, the AURORA scenario, as demonstrated in the DOE test, includes repeated opening and closing of the tie circuit breaker until the generator under test is destroyed. The angle difference between the generator and grid each time the breaker is closed will determine the amount of damage, i.e. 0 degrees no impact, 180 degrees maximum impact.

Typical electric utility practice is to include synchronism-check relays between network sources for the purpose of checking the angle and slip rate between, and the voltage of, the two network sources before the circuit breaker can be closed. This prevents closing of a breaker between two systems that are out of phase (synchronism) or have dramatically mismatched voltages. The AURORA attack assumes that the controls that open and close a given circuit breaker can be hacked as well as the synchronism check function of a modern communicating multifunction relay. Ensuring that the synchronism-check relay cannot be hacked is a key element of mitigating the AURORA Vulnerability.

Understanding Synchronism Check Applications

Ensuring that synchronism-check (25) protection and control systems cannot be hacked requires an understanding of the technologies employed for the application. A very real threat exists in applications that employ the technology extremes, i.e. electromechanical on one end and communicating multifunction protection on the other.

Electromechanical products, by design, are slow to open their 25 contact. In applications where voltage is maintained on the 25 relay after a breaker is closed, the 25 contact may not be able to open fast enough to prevent the AURORA scenario. If a circuit breaker is opened by a hacker, contact dwell time, disk and drag magnet, and bearings of the electromechanical 25 relay are inherently slow in allowing the 25 contact to open, resulting in a condition that will not ensure an open 25 contact before the hacker closes the circuit breaker. Also with an open breaker, the generator will be "slipping" at some rate relative to the power grid and, depending on this rate, can ratchet an open 25 contact to the closed position or prevent the reset of a previously closed 25 contact.

The assumption on the communicating multifunction application is that the security of the product can be breached, allowing a hacker to modify the logic, permanently closing the 25 output contact. Figure 2 shows an example of typical multifunction relay logic and how it is assembled to perform the 25 function.

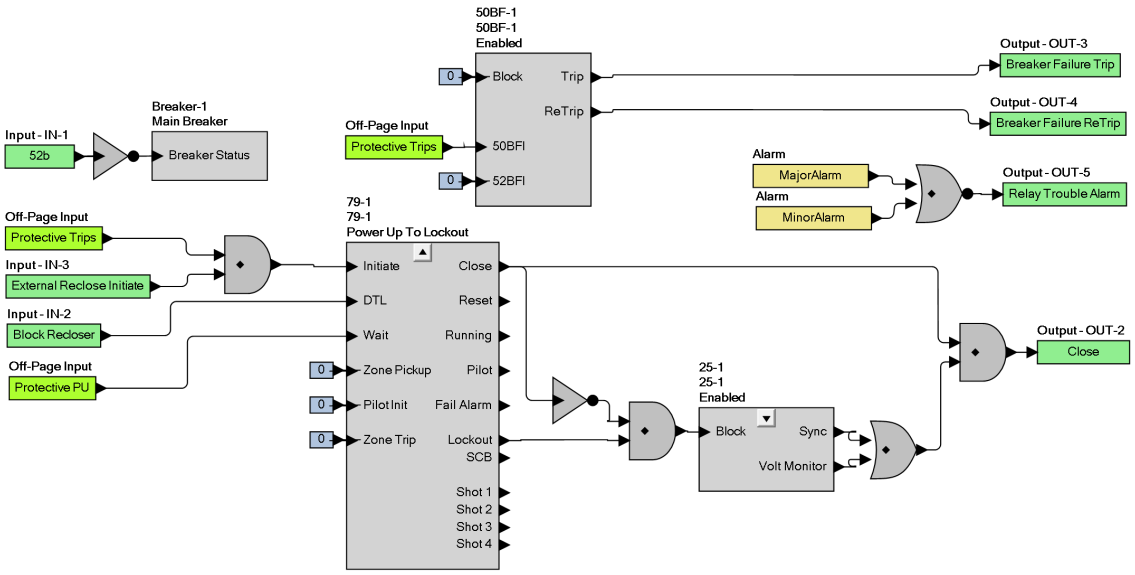

Figure 2 - Example of Multifunction Relay Logic Set Up to Perform the 25 Function

Electric utilities employ thousands of communicating multifunction protective relays because of their flexibility, low maintenance cost, and most importantly, their "remote communicating capability". It has been demonstrated for more than 20 years that remote communications increases the reliability of the protection system by providing instantaneous feedback on the health and well being of the protection system. The AURORA Vulnerability threat requires either "hacker proof" security or a backup 25 function provided by a non-communicating alternative.

Relaying Alternatives for Mitigating AURORA Vulnerability

One of the best approaches for mitigating the concerns associated with electromechanical synchronism check applications (25) is to replace the products with a Basler Electric single function BE1-25 synchronism check relay. See Figure 3. This is an analog input, microprocessor-based product that is precise in its measurements and function, eliminating the slow reset concern associated with the electromechanical products. Consult Figure 4 for slip frequency and time delay characteristic. Figure 5 details the voltage characteristics.

Figure 3 - Basler BE1-25 Sync Check Relay

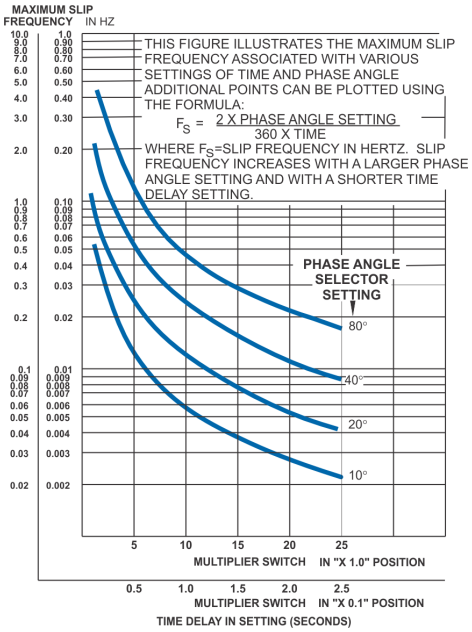

Figure 4 - Slip Frequency vs Time Delay Characteristic

The product is in an S1 case and fits the existing panel cutout of the popular electromechanical 25 relays such as the GE-IJS and ABB CVE.

The BE1-25 product has no remote communications capabilities, so it will work equally well in a backup application for multifunction communicating relays that are subject to AURORA attack.

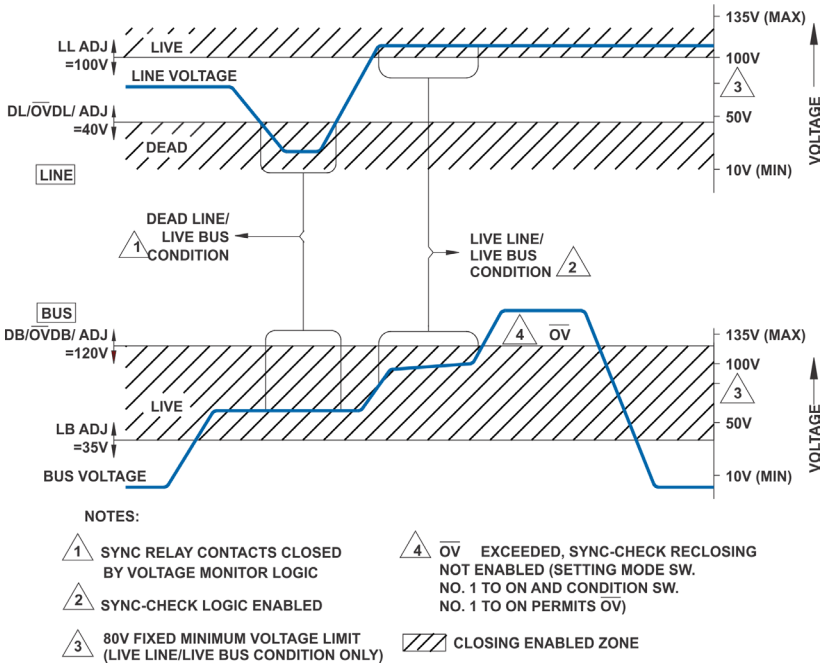

Figure 5 - Voltage Monitor Acceptance Zones

On loss of synchronism between the power grid and the generator, output of the BE1-25 opens in 22ms or under 1½ cycles. Also, the BE1-25 is available with voltage inputs that provide "delta voltage" intelligence to the relay for blocking circuit breaker close when the voltage difference between the two sources representing the grid and generator, are out of limits. In addition, the relay monitors the slip rate of the generator, ensuring that breaker closure cannot occur unless the generator phase angle relative to the grid is within a preset angle window for a specified amount of time. Figure 6 offers an integrated overview of BE1-25 delta angle, delta voltage, and slip characteristics.

For a digital relay with the highest security capabilities, the Basler Electric BE1-FLEX is an excellent choice. This relay has many functions including the 25 element with delta voltage, delta angle, and slip frequency for fast and easy setup. The BE1-FLEX has communications capability if desired, but it is not required in this application. The BE1-FLEX is rare in its ability to be ordered without remote communication ports and encrypted and keyed firmware. For applications that require the advanced recording and protection capabilities of a digital relay without the risk of communications, there is no better choice. Note, the 25 output from the BE1-FLEX or the BE1-25 single function relay is placed in series with the communicating multifunction product, providing a hack-proof 25 backup function.

The BE1-FLEX is supplied in a non-drawout, S1 size case (K option) that fits in a standard S1 case opening (see Figure 7). Adapter plates are sold separately.

Figure 7 - An Inexpensive, Multifunction Option, BE1-FLEX Protection, Automation and Control System

For More Information

To get more information on the products discussed in this note, including product bulletins and instruction manuals, go to www.basler.com or contact Technical Support at 618-654-2341.

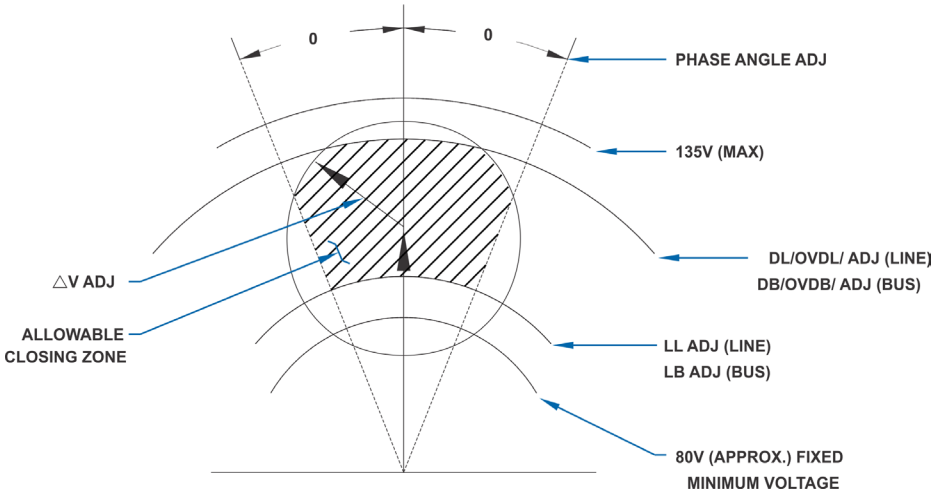

Figure 6 - Closing Zone Using Voltage Difference, Sync-Check, and Line/Bus Voltage Monitor

Basler Electric®

Highland, Illinois USA
Tel +1 618.654.2341
Fax +1 618.654.2351
email: info@basler.com

Suzhou, P.R. China
Tel +86 512.8227.2888
Fax +86 512.8227.2887
email: chinainfo@basler.com

Quality System Certification
Basler
ISO 9001:2015