ELECTRIC POWER RESEARCH INSTITUTE

Mitigation of the AURORA Threat Through Protection and Control Engineering Practice

Phase I

1021914

Mitigation of the AURORA Threat Through Protection and Control Engineering Practice

Phase I

1021914

Technical Update, December 2011

EPRI Project Manager

Y. Lu

ELECTRIC POWER RESEARCH INSTITUTE
3420 Hillview Avenue, Palo Alto, California 94304-1338 ▪ PO Box 10412, Palo Alto, California 94303-0813 ▪ USA
800.313.3774 ▪ 650.855.2121 ▪ askepri@epri.com ▪ www.epri.com

DISCLAIMER OF WARRANTIES AND LIMITATION OF LIABILITIES

THIS DOCUMENT WAS PREPARED BY THE ORGANIZATION(S) NAMED BELOW AS AN ACCOUNT OF WORK SPONSORED OR COSPONSORED BY THE ELECTRIC POWER RESEARCH INSTITUTE, INC. (EPRI). NEITHER EPRI, ANY MEMBER OF EPRI, ANY COSPONSOR, THE ORGANIZATION(S) BELOW, NOR ANY PERSON ACTING ON BEHALF OF ANY OF THEM:

(A) MAKES ANY WARRANTY OR REPRESENTATION WHATSOEVER, EXPRESS OR IMPLIED, (I) WITH RESPECT TO THE USE OF ANY INFORMATION, APPARATUS, METHOD, PROCESS, OR SIMILAR ITEM DISCLOSED IN THIS DOCUMENT, INCLUDING MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, OR (II) THAT SUCH USE DOES NOT INFRINGE ON OR INTERFERE WITH PRIVATELY OWNED RIGHTS, INCLUDING ANY PARTY'S INTELLECTUAL PROPERTY, OR (III) THAT THIS DOCUMENT IS SUITABLE TO ANY PARTICULAR USER'S CIRCUMSTANCE; OR

(B) ASSUMES RESPONSIBILITY FOR ANY DAMAGES OR OTHER LIABILITY WHATSOEVER (INCLUDING ANY CONSEQUENTIAL DAMAGES, EVEN IF EPRI OR ANY EPRI REPRESENTATIVE HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES) RESULTING FROM YOUR SELECTION OR USE OF THIS DOCUMENT OR ANY INFORMATION, APPARATUS, METHOD, PROCESS, OR SIMILAR ITEM DISCLOSED IN THIS DOCUMENT.

REFERENCE HEREIN TO ANY SPECIFIC COMMERCIAL PRODUCT, PROCESS, OR SERVICE BY ITS TRADE NAME, TRADEMARK, MANUFACTURER, OR OTHERWISE, DOES NOT NECESSARILY CONSTITUTE OR IMPLY ITS ENDORSEMENT, RECOMMENDATION, OR FAVORING BY EPRI.

THE FOLLOWING ORGANIZATION, UNDER CONTRACT TO EPRI, PREPARED THIS REPORT:

Quanta Technology LLC

This is an EPRI Technical Update report. A Technical Update report is intended as an informal report of continuing research, a meeting, or a topical study. It is not a final EPRI technical report.

NOTE

For further information about EPRI, call the EPRI Customer Assistance Center at 800.313.3774 or e-mail askepri@epri.com.

ACKNOWLEDGMENTS

The following organization, under contract to the Electric Power Research Institute (EPRI), prepared this technical update report:

Quanta Technology LLC
4020 Westchase Blvd., Suite 300
Raleigh, NC 27607

Principal Investigator
J. Holbach

This report describes research sponsored by EPRI.

EPRI would like to express its gratitude to the Protection and Control Task Force and the utility advisors for the support and contribution of this project:

Jim Vespalec	American Transmission Company, United States
Aaron Martin	Bonneville Power Authority, United States
Thomas Roseburg	Bonneville Power Authority, United States
William Winters	Con Edison of New York, United States
Steve Sano	Hawaii Electric Company, United States
Paul Difilippo	Hydro One Networks, Canada
Mohammad Zubair	Hydro One Networks, Canada
Ray Zhang	National Grid, United Kingdom
Michael Cooper	National Grid, United States
Justin Jakub	Nebraska Public Power District, United States
Alex Echeverria	New York Power Authority, United States
Frank Ronci	New York Power Authority, United States
Daniel Zhang	New York Power Authority, United States
Ted Warren	Southern Company, United States

This publication is a corporate document that should be cited in the literature in the following manner:

Mitigation of the AURORA Threat Through Protection and Control Engineering Practice: Phase I. EPRI, Palo Alto, CA: 2011. 1021914.

ABSTRACT

In 2007, Department of Homeland Security officials released a video showing an upsetting experiment result conducted at the Idaho National Laboratory. In the experiment, a circuit breaker connecting a generator to a power grid was opened and then closed out of synchronism intentionally a number of times. The repeated out-of-synchronism closing caused high mechanical stress on the generator and ultimately damaged the generator under test. This "AURORA test" demonstrated a vulnerability of generators and caused industry-wide concerns about the safety of the critical generation assets. The AURORA threat can be initiated from cyber attackers, or equivalently, can be the result of switching misoperation. One of the mitigation directions recommended by subject matter experts is to identify and fill the gap through protection and control engineering practices. The AURORA threat presents a possible gap in existing protection practice for generator and motor. However, the AURORA threat is little known by most utility protection and control staff. This report collects the fundamentals of the AURORA threat, reviews the existing protection and control methods, and explores the applicable and cost-effective AURORA mitigation strategies through protection and control engineering practices.

Keywords

Generator
Hardware mitigation device (HMD)
Out of synchronism
P&C
Reclosing

ACRONYMS AND ABBREVIATIONS

ANSI	American National Standards Institute
DHS	Department of Homeland Security
DOE	Department of Energy
HMD	hardware mitigation device
IED	intelligent electronic device
NERC	North American Electric Reliability Corporation
P&C	protection and control
PMU	phasor measurement unit
REID	rotating equipment isolation device
ROFC	rate of frequency change
SCADA	supervisory control and data acquisition system
SMIB	single machine-infinite bus

CONTENTS

LIST OF FIGURES

LIST OF TABLES

1 INTRODUCTION ADD-ON TEXT

In 2007, Department of Homeland Security (DHS) officials released a video showing an upsetting experiment result conducted at the Idaho National Laboratory. In the experiment, a circuit breaker connecting a generator to a power grid was opened and then re-closed out of synchronism intentionally for a number of times. The out-of-synchronism closing caused high mechanical stress on the generator. After a number of shots, it ultimately damaged the generator under test. The test demonstrated a vulnerability of modern synchronous generators. And it was called the “AURORA vulnerability” or “AURORA threat”. The AURORA threat could be initiated from cyber attackers who can presumably obtain the control of digital relays and enforce the reclosing actions, or equivalently, it could be caused by switching misoperation at substations as well. The DHS video served as a wake-up call for regulators to investigate the threat and mitigation actions for protecting the national power generation infrastructure.

On July 21, 2007, the North American Electric Reliability Corporation (NERC) issued a notification to the industry on the AURORA vulnerability, which was based on the information available at that time. On October 13, 2010, NERC issued another alert in the form of a recommendation to industry on the AURORA vulnerability. The recommendation requires entities (nearly 1900 power utilities and generator asset owners) to report on efforts and progress of AURORA threat mitigation by Dec. 13, and with updates every six months until mitigation is complete.

The mitigation elements that have been recommended by the AURORA technical team in NERC fall into two broad categories: *Protection and Control Engineering Practices* and *Electronic and Physical Security Mitigation Measures*.

In 2011, the EPRI Protection and Control (P&C) task force launched a project to study on the AURORA threat with the following goals:

- Support utilities obtain a good understanding of the AURORA vulnerability from power system and P&C engineering perspectives;
- Perform technical assessment of available protection functions, equipment and tools;
- Recommend mitigation methods and tools from P&C engineering practices;
- Collect and document P&C engineering practices and experience for AURORA mitigation in industry.

However, the project does not intend to cover the following research areas:

- Cyber security and physical security mitigation measures;
- Guide to meet regulatory and compliance requirements;
- Non-technical elements: such as policy and rule making, etc.

On April 28, 2011, the project kick-off webcast was held. The slides and meeting notes can be found in Appendix A. On August 2, 2011, the P&C task force met at New York City and had a half day meeting and discussion on the progress of the project. The meeting notes are provided in Appendix B. This technical update report summarizes the findings and results from 2011 project activities.

2
UNDERSTAND THE AURORA EVENT

Generator separation

Before evaluating various solutions for mitigation or prevention of AURORA threat, it is helpful to review the basics of generator and understand the generator response in the cases of load change and system separation. In the study, the so-called single-machine-infinite-bus (SMIB) model shown in Figure 2-1 is used and it has all necessary components required for the illustration purposes. To simplify the analysis, it is assumed that all components in the SMIB are lossless. In Figure 2-1, a generator with the internal voltage Vg is connected with an infinite bus with terminal voltage Vr. If the load towards the infinite bus is zero, the generator voltage Vg will be in phase with the infinite bus voltage Vr, and no load current flows over the line. As soon as the load on the infinite bus is increased, load current (I_{load}) starts to flow. This current will cause a voltage drop over the generator internal impedance (Zg) and the line impedance (Zl), and cause a phase angle (ϑ) between the generator voltage (Vg) and the infinite bus voltage (Vr) as shown in the voltage vector diagram of Figure 2-1. Under steady state, the mechanical power fed into the generator are balanced with and the electrical load towards the infinite bus.

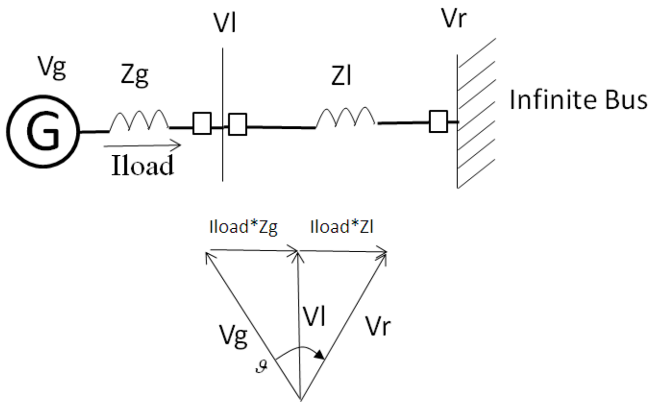


Figure 2-1
Single machine-infinite bus model with voltage vectors shown

The relation between the real power (P_E) over the line and the angle between the generator voltages and the infinite bus voltage can be described as:

$$P_E = \frac{V_g \cdot V_r}{X_g + X_l} \sin(\vartheta)$$

Equation 1

The maximum of the real power transport between the generator and the infinite bus is limited by the sum of the source impedance (X_g) of the generator and the line impedance (X_l).

Theoretically, the maximum power transfer occurs when the voltage angle reaches 90 degree (ϑ=90).

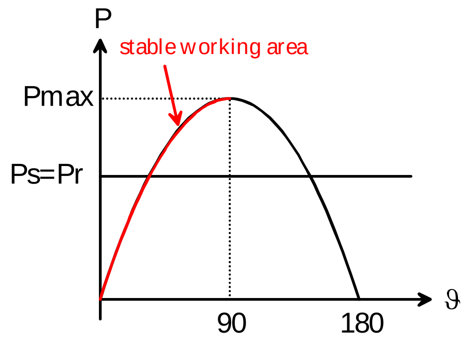


Figure 2-2
Active power in relation to the load angle

Once the voltage angle (ϑ) increases over 90 degree, the real power output decreases as shown in Figure 2-2. And the system becomes unstable because the mechanical power (input) and electrical power (output) cannot be balanced anyhow. The operation area of a generator normally requires voltage angles not larger than a certain degree (for example, 60 degree) to maintenance the system stability. Under steady-state conditions, the mechanical active power into the generator P_M is equal to the electrical active power P_E transmitted over the transmission line, which determines the voltage angle between the generator and the infinite bus. A sudden change of the load or the ability to transmit the load over the line will require the generator to adjust to the new situation by changing the load angle. If the mechanical power is greater than the electrical power transported over the line, the generator will accelerate and increase the frequency and phase angle. If the mechanical power is smaller than the electrical power transports, the generator will decrease the frequency and phase angle. The rate of frequency change (ROFC) depends on the inertia of the generator as well as the difference between electrical and mechanical power, which can be described by the following “swing equation”:

$$\frac{df}{dt} \cdot \frac{2 \cdot H \cdot S_N}{f_N} = P_M - P_E$$

Equation 2

Where:

P_M = mechanical active power going into the generator

P_E = electrical active power transported over the line

f_N = nominal frequency

H = inertia value of machine

S_N = nominal power of machine

For Example:

Generator H = 5s

$$\text{Frequency } f_N = 60Hz$$
$$P_M - P_E = 400MW$$
$$S_N = 800 \text{ MVA}$$

$$\frac{df}{dt} = \frac{P_M - P_E}{2 \cdot H \cdot S_N} f_N = \frac{400MW}{2 \cdot 5s \cdot 800MVA} 60Hz = 3\frac{Hz}{s}$$

Equation 3

If a generator is completely disconnected from power grid, all electrical power transported over the line will suddenly become zero. However, the mechanical power fed into the generator will not be stopped immediately, which causes the generator to accelerate. The acceleration will continue until the governor control of the generator reduces or shut down the mechanical power input. In the analysis of AURORA threat, the responses of governor control can be neglected because it normally takes place on the order of seconds or longer, whereas the investigation focuses on the timeframe of a few hundreds of milliseconds following the AURORA event.

For the above example, the frequency of the generator will continuously increase with a fixed rate of 3 Hz/second as shown in Figure 2-3 and Figure 2-4. As shown in Figure 2-5, the phase angle will increase accordingly, with an accelerated speed that increases with the frequency rate.

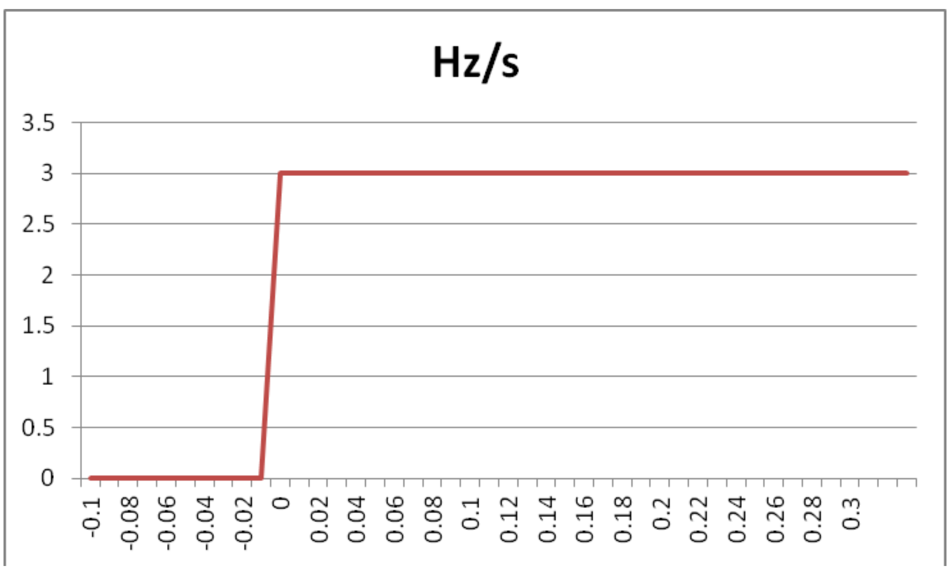


Figure 2-3
Frequency acceleration [Hz/s] over time after generator disconnection (t=0)

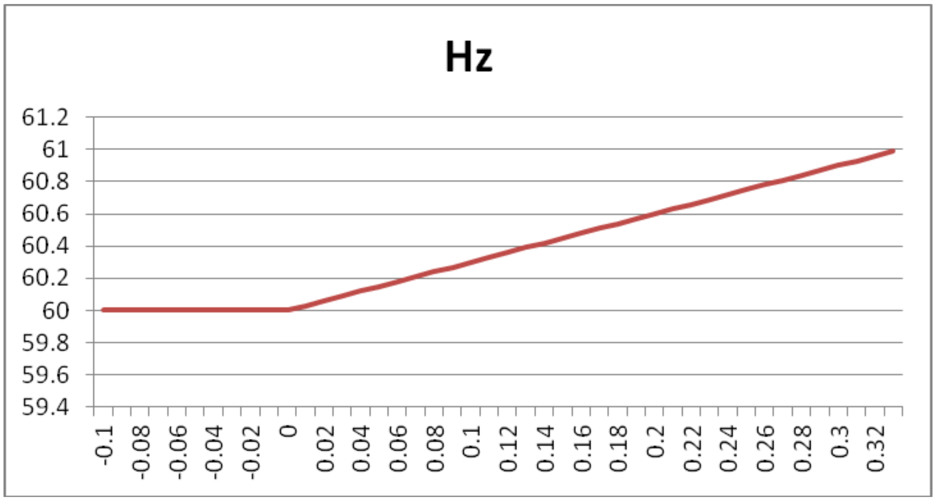


Figure 2-4
Frequency after generator disconnection (t=0)

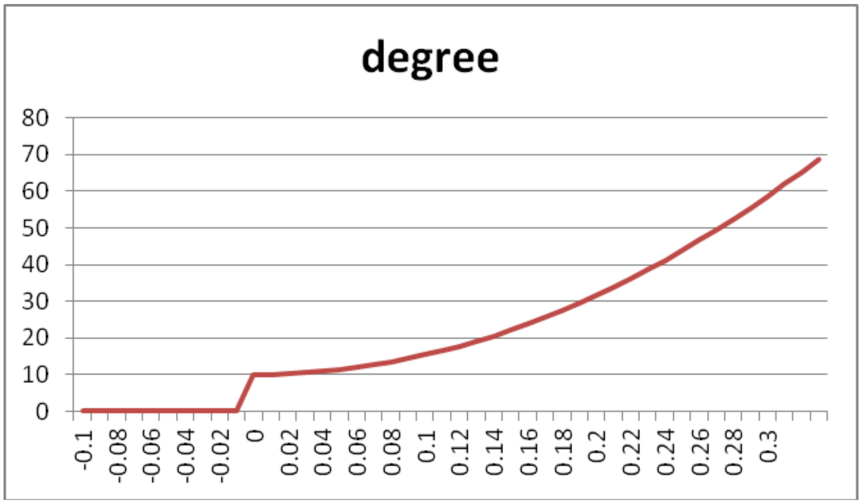


Figure 2-5
Phase shift after generator disconnection (t=0) with vector jump

The method to detect generator isolation can be based on one or a combination of the three related elements: phase shift, frequency and the rate of frequency change.

To use the phase shift directly turns out to be difficult because it requires measuring the voltage on both sides of the interrupting breaker. Depending on the grid network topology, the interrupting breaker may not necessarily be the generator breaker, actually it could be any breaker in the path of connecting generator(s) to load(s). Moreover, interrupting power flow is also possible by opening a group of breakers. In this case, the actual required measurement can be obtained only by a wide area measurement system, instead of a single relaying device.

Separation of a generator from power grid will also cause a voltage vector jump. A vector jump is an immediate change in phase and amplitude of the voltage measured on the generator terminals. It can be caused by a sudden change or interruption of the load current. Figure 2-6 shows the voltage vector jump after a separation.

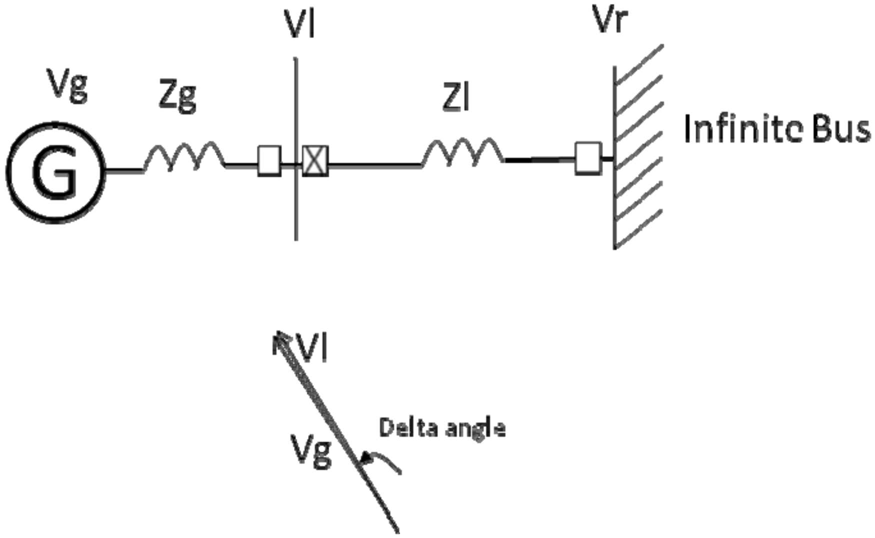


Figure 2-6
Vector jump after separation

If a generator is separated from power grid but form an island or micro-grid, a vector jump can still occur. In this case, the connected load will lead to a lower rate of frequency change compared to the case of a complete separation. However, in certain rare situation, after the separation if the connected load in island happens to be equal to the power supplied by the generator, none of the above elements (voltage, will be observable and the frequency will remain constant, just like nothing happens.

However, it is challenging to distinguish generator separation from large load changes which happens in normal operating conditions. In case of large load change, a generator needs to adjust to this new loading situation by changing the load angle. Therefore, the frequency will either increase or decrease depending on the load change until it reaches the load angle for the new balance. However, even if the generator can reach a new load angle it will not immediately reach it, instead the process will take certain amount of time because of the large inertia of the generator. Depending on the system damping, the load angle may oscillate several times until the target load angle is reached. This phenomenon is known as “power swing”. Power swings may occur when a generator has to adjust to a new balanced operating point. Figure 2-7 through Figure 2-9 show the values of acceleration, frequency, and phase angle for a sample power swing event.

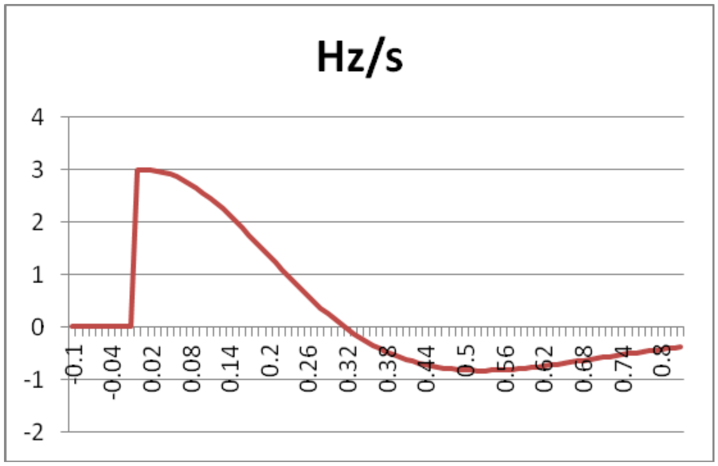


Figure 2-7
A response of the rate of frequency change to a sudden load drop

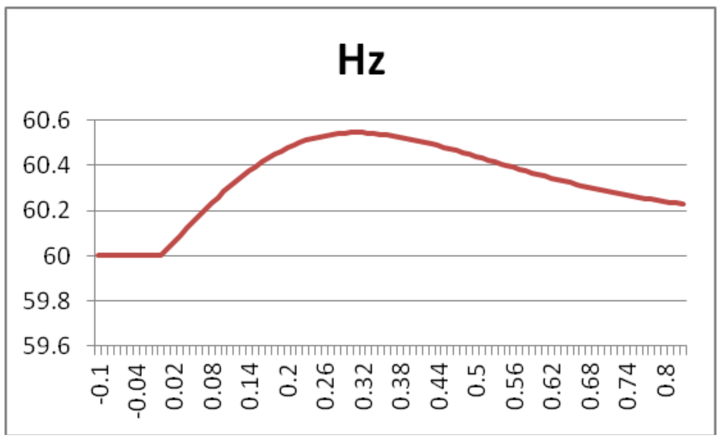


Figure 2-8
A response of frequency to a sudden load drop

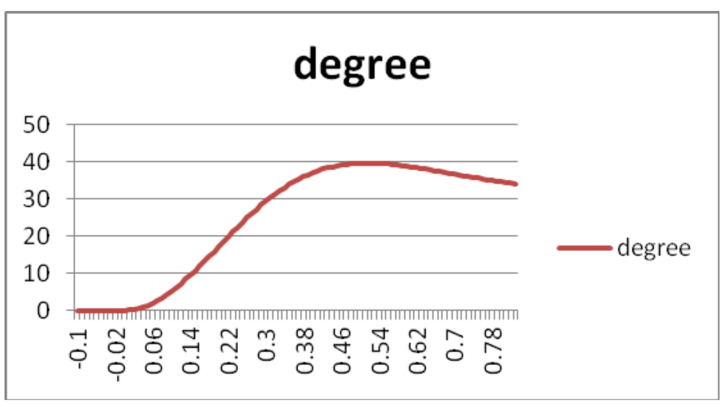


Figure 2-9
A response of phase angle to a sudden load drop

Basics on out of synchronism reclosing

In order to evaluate the risk of AURORA attack, it is necessary to understand the outcomes of an out of synchronism reclosing. In normal operation situation, a generator will be allowed to connect to a power grid only if its voltage is approximately in synchronism with the grid voltage. In general, three elements are monitored by a synchronism check device before a close command is issued. These three elements are voltage amplitude, system frequency and phase angle between the voltages of the generator and that of the grid. If a generator is connected to the power grid and the generator voltage is different either in phase angle or amplitude with the grid voltage, the voltage difference will cause a current flow. This current together with the generator voltage will create an electric torque which applies to the generator shaft. If the suddenly applied torque is too large it could cause damages to a generator.

How much torque can cause what damage to a generator is a very complex question which cannot be answered easily, because a generator is a complex electro-mechanical system. One also needs to take it into account that a generator shaft accumulates certain loss-of-life over its service time due to switching events, fault events or synchronization operations. In such events, sudden changes in torque may already contribute to the material fatigue of a shaft. A detailed discussion of this topic is outside the scope of the report and interested readers can find more information in the reference [1] and [2]. The report will provide a *qualitative* understanding and classification of the electrical torques and associated torsional shaft oscillations caused by power system events.

From the standard [6], there are following findings on the limits of a generator in case of power system faults and switching events:

- "Screening studies have shown that line switching from an initially steady-state condition that results in a ΔP of 0.5 per unit or less will result in zero or negligible loss-of-life per incident. Where the switching ΔP in a specific turbine-generator is expected to exceed the value of 0.5 per unit, it is recommended that the manufacturer be consulted and a possible unit-specific study be performed."
- "A generator shall be designed so that it can be fit for service after experiencing a sudden short circuit of any kind at its terminals while operating at rated load and 1.05 per unit rated voltage, provided that the fault is limited by the following conditions:
  - The maximum phase current does not exceed the phase current obtained from a three-phase sudden short circuit.
  - The stator winding short-time thermal requirements are not exceeded."
- "It should be expected that the most severe faulty synchronizations, such as 180° or 120° out-of-phase synchronizing to a system with low system reactance to the infinite bus, might require partial or total rewind of the stator, or extensive repair or replacement of the rotor, or both."

In summary, a torque produced by a switching event that causes a change of 0.5 per unit (PU) or less will have negligible impact on the life-span of the generator. A torque greater than 0.5 PU, and up to the torque generated by a three phase fault, may reduce the life span of a generator, even though the generator has been designed to withstand such events. In contrast, an out-of-synchronism-closing in the worst case can create a torque which may exceed the limit that a generator is designed for. A generator could be damaged in this case. Whether the torque generated by an out-of-synchronism-closing is larger than that of a three phase fault largely depends on the phase angle between the generator and the grid, and also the system impedance.

Generally, the electrical torque can be calculated by the following formula:

$$T_{electrical} = (i_a \cdot v_a + i_b \cdot v_b + i_c \cdot v_c)$$ **Equation 4**

This calculation is based on instantaneous values. In a switching event, the current will normally be offset by a DC component because the current cannot respond instantaneously in a reactive circuit.

The calculation of the transient current in a dynamic system like a generator after any a grid event is not a simple job. Many papers have been published on modeling and calculation of the currents and the torques under various conditions [3] [4]. This report will focus on the maximum torque produced from various events, and categorize or compare these maximum torques. In [5], there is a simplified method for calculating the maximum electrical torque.

Based on this method, the maximum torque for a three-phase fault can be calculated as:

$$T_{\max(3-phase-fault)} = \frac{E^2}{x_d^{"}}$$ **Equation 5**

The maximum torque for an out-of-synchronism-closing at 120 degree (the worst case) can be calculated as:

$$T_{\max(out-of-synch)} = \frac{3\sqrt{3}}{2} \frac{E^2}{x_d^{"} + x_s}$$ **Equation 6**

where

E= RMS generated voltage
$x_d^{"} =$ *direct axis subtransient reactance*
$x_s =$ *reactance of connected system*

Above equations are helpful to help evaluate the damages associated with the AURORA attack. These equations can be used to determine under what condition the three-phase fault produces a larger torque than that of out-of-synchronism-closing at 120 degree. Also the equation describes the importance of the system impedance relating to the maximum torque.

The calculations shows that the three-phase-fault torque can reach the maximum torque of a out-of-synchronism-closing at 120 degree, which is the worst case, if Equation 7,8,9 are held.

$$\frac{E^2}{x_d^{"}} = \frac{3\sqrt{3}}{2} \frac{E^2}{x_d^{"} + x_s}$$ **Equation 7**

$$\frac{x_d^{"} 3\sqrt{3}}{2} = x_d^{"} + x_s$$ **Equation 8**

$$x_d'' \cdot 1.598 = x_s$$ **Equation 9**

For all applications in which the system impedance is greater than 1.598 times the generator reactance, the three-phase fault torque will be higher than the torque produced by a out-of-synchronism-closing. The system impedance includes all impedances between the generator terminals and the infinite source which represents the power grid.

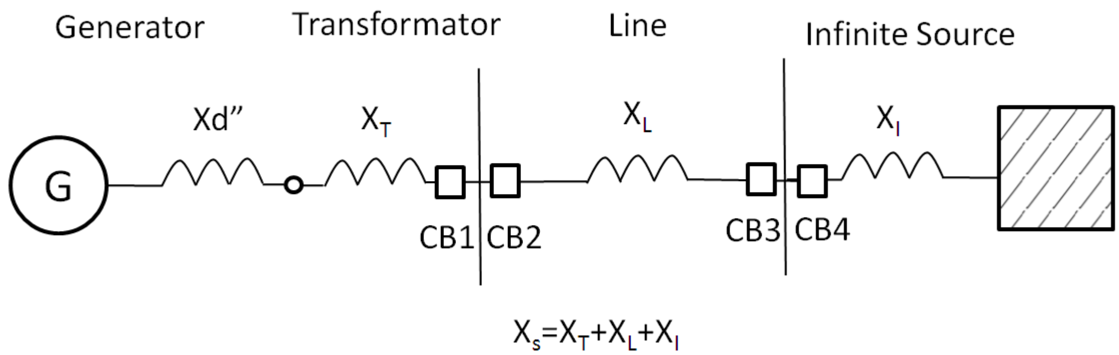


Figure 2-10
System impedance on a serial connection to the power grid

Based on above analysis, it becomes clear that if the system impedance does not change, the location of a circuit breaker **will not have influence** on the torque value. For example, in Figure 2-10 any of the circuit breakers, CB1 through CB4, could be used to initiate an AURORA attack and would generate the same torque on the generator. The maximum torque will be determined by the generator impedance and the system impedance, which includes the transformer impedance, the line impedance and the infinite source impedance. This is important finding. Because the circuit breakers at the generation facility (CB1) normally has well established physical and cyber controls for reducing the risk of AURORA attacks, however, CB2 through CB4 shown in Figure 2-10 could be used to accomplish the same attacks as CB1. These circuit breakers, if located in an offsite unmanned substation, may be more vulnerable as one can gain easier access to them.

Figure 2-11 shows a scenario in which a number of circuit breakers can be combined together to disconnect or reconnect a generator from power grid.

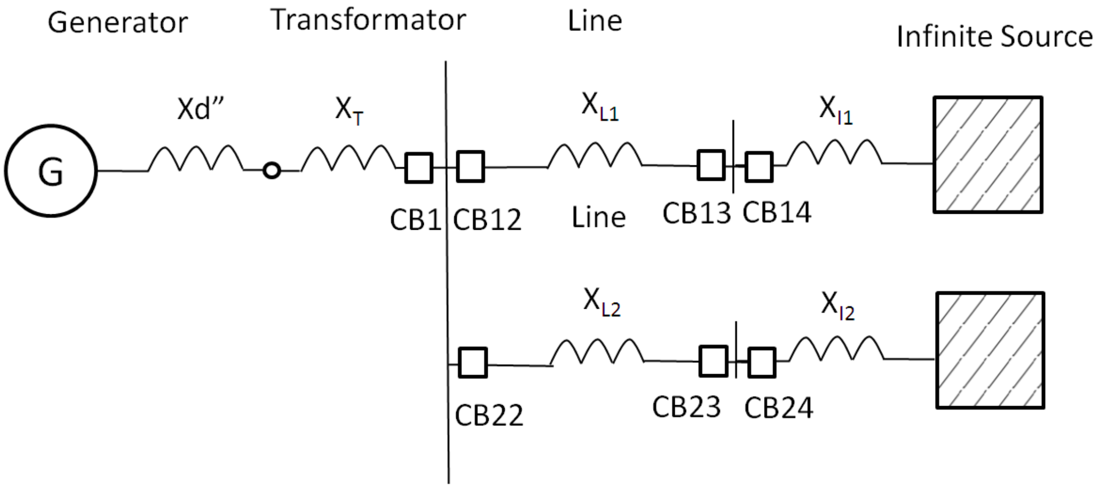


Figure 2-11
System impedance on a parallel connection to the power grid

In Figure 2-11, both CB12 and CB22 need to be opened to disconnect the generator from the power grid. The timing of opening the breaker is critical for a successful AURORA event. To cause the maximum stress to the generator, both breakers (CB12 and CB22) need to be closed at the same time. This is not easy to archive and would require precise coordination, particularly if the breakers are located in different locations. If only one breaker is closed in the AURORA event, the maximum torque produced in this case will be different from the previous case and dependant on the resultant effective system impedance which can be calculated by the impedance from the selected breaker to the infinite bus.

If a generator is connected to a power grid out-of-synchronism at 120 degree, it can produce the maximum electrical torque on the generator. The maximum torque angle (120 degree) is not the same as the maximum load angle (90 degree) because of the additional DC offset in currents (see Figure 2-12).

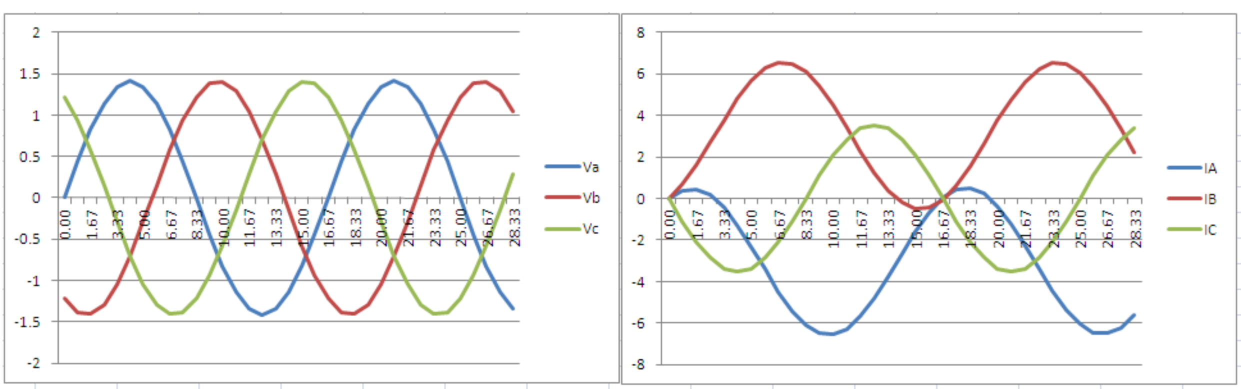


Figure 2-12
Voltages and currents after faulty synchronization

Figure 2-13 shows the calculated torques (in per unit) as a function of the synchronization angle. It also shows different system impedances will have very different impact on the torques. The torques produced by normal loading and three-phase fault also provided in the diagram.

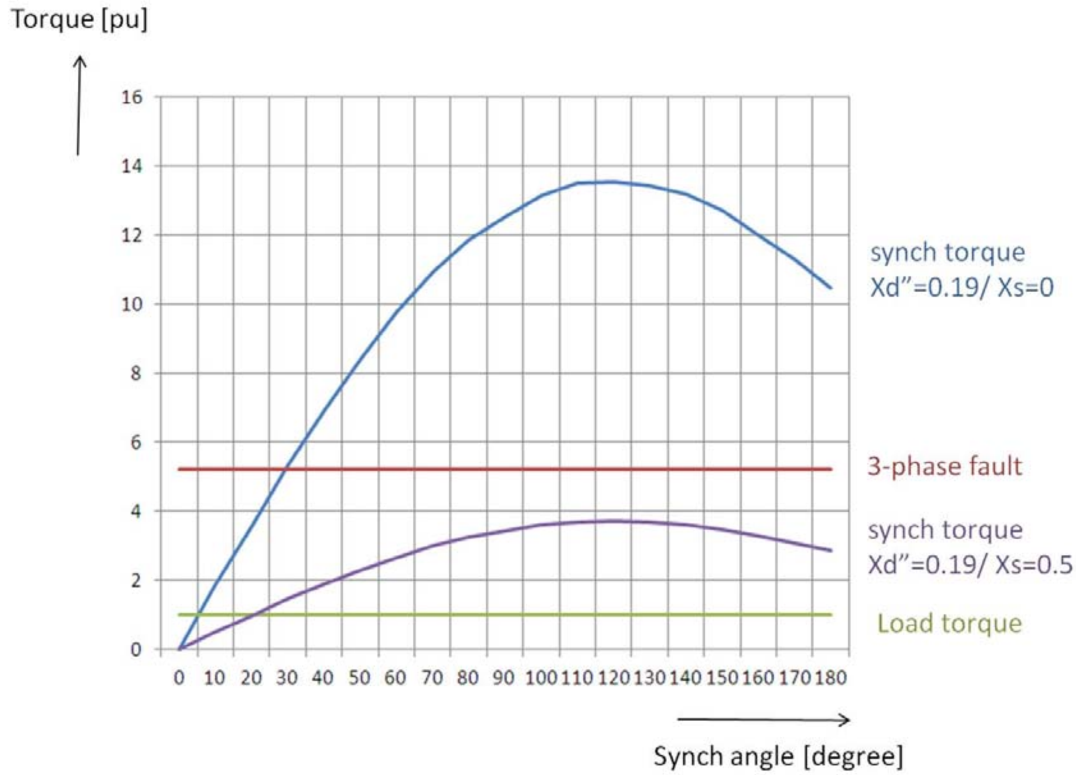


Figure 2-13
Torque versus angle in various scenarios

Special consideration for weak interconnected systems

In the case shown in Figure 2-14, two power systems are connected via a weak tie link. This is a typical case for power systems in islands.

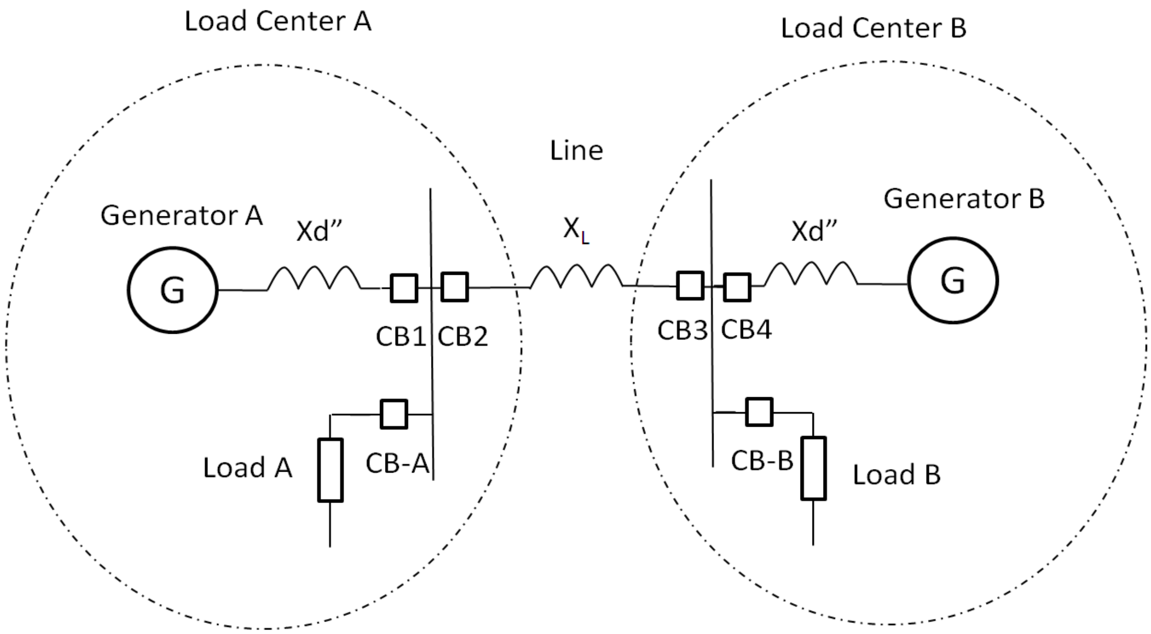


Figure 2-14
Interconnected power systems with a weak link

In Figure 2-14, an attacker could possibly separate the system by opening one of the breakers CB1 through CB4, causing the generators to drift out of synchronism after a certain period of time. The speed of drift depends on how much power deficiency is created. With the help of the swing equation introduced in chapter 2 and the knowledge of the generator inertia, the rate of frequency change can be calculated.

Under normal load condition, opening CB2 or CB3 would not create a large power interruption because the weak intertie line is only lightly loaded in this case. Neither generator would see a large power deficiency, therefore the rate of frequency change would be very small. Both generators would continue to support their local load. It would probably take certain period of time to reach a remarkable phase angle difference between the two systems. And it would be hard for any attackers to predict when the maximum torque angle is archived. However, if the attacked breaker would be closed when both systems are approximately 120 degree apart, an additional torque would be generated on both generators based on the current flow over the transmission line. The current amplitude will depend on the total impedance between the two generators but could be high enough to result in a damaging torque.

The attack of the breaker CB1 or CB4 would change the previous consideration in that now both generators would change their frequency much faster after the opening of the breaker. For example, in the case that CB1 was opened generator A will accelerate as it receives more mechanical power than can export in electrical power (theoretical $P_{elec}=0$) . Generator B is required to support the load at load center A and would slow down as the mechanical power is not sufficient to support the higher electrical power. Both generators would drift apart and would reach the critical 120 degree much faster as than in the previous case. At the closing of CB1 both generators would be exposed to an additional torque caused by the current flow over the transmission line. The current amplitude is determined by the voltage difference between the generators and limited by the total system impedance between the generators. This would be in addition to the actual load difference both generators would see at this moment.

The attack of breaker CB-A or CB-B would not separate the systems and only cause a torque difference based on the load. If the value is above 0.5 PU, it may contribute to a reduction of the life span of the generator.

3
PROTECTION AND CONTROL SOLUTION TO MITIGATE AN AURORA ATTACK

The previous chapter showed that a successful AURORA attack could potentially damage a generator or motor. In this chapter it will be discuss how protection and control functions can be used to prevent or mitigate an AURORA attack. **Note that the physical and cyber security should always be the first line of defense to prevent an AURORA attack and none of the protection and control function will replace them or eliminate their need.** This is particularly true for the circuit breaker at the generator substation as there is hard to prevent an AURORA attack if somebody obtains the control over this circuit breaker. However, the subject of physical and cyber security is out of the scope of this report. For this report, it is assumed that all possible physical and cyber security measures are in place and the circuit breaker inside the generator substation cannot be accessed by unauthorized person. In chapter 3 it was shown that any breaker that is able to disconnect the generator from the power grid can be used to initiate an AURORA attack. This report will discuss protection and control mitigation approaches for the events in which a breaker other than the generator breaker is targeted by an AURORA attack.

Two strategies shown below can be used to mitigate the AURORA threat:

1. Utilize generator protection function(s) to detect any separation of a generator from power grid. Then, trip (open) the generator breaker before the AURORA attacker can reclose a downstream breaker.
2. Design control schemes for vulnerable breakers to prevent any unsynchronized reclosing.

Utilizing of generator protection function to detect generator separation

The techniques for generator-separation detection and tripping have already been studied and applied for distributed generation to prevent harmful effects on the grid and the connected load. In this chapter, various protection functions which can detect generator separation and response fast enough to prevent an unsynchronized reclosing will be discussed. Each function will be evaluated in terms of security and dependability.

Voltage Vector Jump

The voltage vector jump function is the fastest function to detect a separation from the network. The vector jump function utilizes the fact that any load jump will change the voltage drop across the generator impedance. A voltage measured close to the generator terminal will therefore jump by a certain phase angle which is in proportion to the load jump.

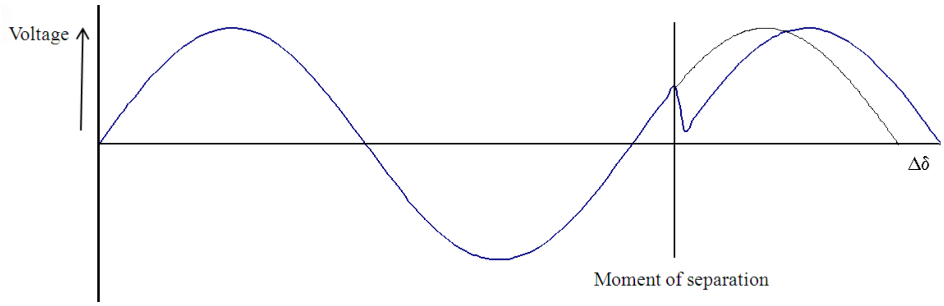


Figure 3-1
Vector jump in voltage

To set the function, the specific power system needs to be carefully studied to find the proper pick-up settings. The settings should not operate on any normal load change condition, while sensitive enough to detect any separation. Such settings may not be possible for all situations, particularly for the situations in which the load is equal to the output of the generator. In such cases, no significant vector jump will happen. In addition, the function needs to be blocked if a power system fault is detected.

Rate of Frequency Change (ANSI 81R)

As explained in chapter 2, a sudden change of load will cause the change of generator frequency with a constant rate assuming the generator governor control has not responded to the load change. The Rate of Frequency Change (ROFC) function has been applied for detection of a load imbalance and for the purpose of load shedding or generation tripping. The ROFC is usually calculated by protective relays over a certain time window. The frequency difference can be calculated from two consecutive measurements of the frequency. The time interval between two measurements can be either fixed or adjustable by settings. A time delay may be added to the ROFC function for protection-security reasons, so the ROFC function will not operate during temporary load imbalance during situations like power swings. Note that in protection terminology, the “security” means a protective function operates if and only if it is necessary. To set the function, the specific power system needs to be carefully studied to find the proper pick-up settings. The settings should not operate on any normal load change condition, while sensitive enough to detect any separation. Such settings may not be possible for all situations, particularly for the situations in which the load is equal to the output of the generator. In such cases, no significant vector jump will happen. In addition, the function needs to be blocked if a power system fault is detected.

In lab tests, it was observed that the ROFC function may have an internal time delay greater than 100 milliseconds, which makes it difficult to use ROFC function for effective protection against AURORA attacks.

Frequency Protection (ANSI 81)

Under-frequency or over-frequency protection functions are designed to protect generators against overload or load rejection. In an AURORA attack, the measured frequency can directly be used to detect a generator separation. Following a separation, the acceleration of the generator will lead to an increase of generator frequency. A generator tripping command will be issued if the measured frequency exceeds the relay pick-up setting. In many generator protection applications, a typical pickup setting of under-frequency or over-frequency is in the range of

±2% respectively, which is between 58.8 Hz to 61.2 Hz for a 60 Hz system. For instance, if an over-frequency pickup is set as 61.2Hz and the rate of frequency change is 3 Hz per second, assuming a generator operates at the nominal frequency (60 Hz) before an AURORA attack starts, it will take 0.4 second for over-frequency to pick up and the phase angle between the generator and the power grid at the moment of closing will be 86.4 degrees. This example shows that the ANSI 81 function can be used to detect generator separation in a "slow way". So an AURORA attacker may still have the chance to close a breaker out-of-synchronism, even though it is not at the maximum torque angle (120 degree).

On the other hand, it is worthwhile to point it out that the ANSI 81 function should not be set too sensitive in order to support the transmission system stability. NERC standard PRC-024 is therefore requiring the following:

> *"Ensure that generator frequency and voltage protective relays are set to support transmission system stability during voltage and frequency excursions"*

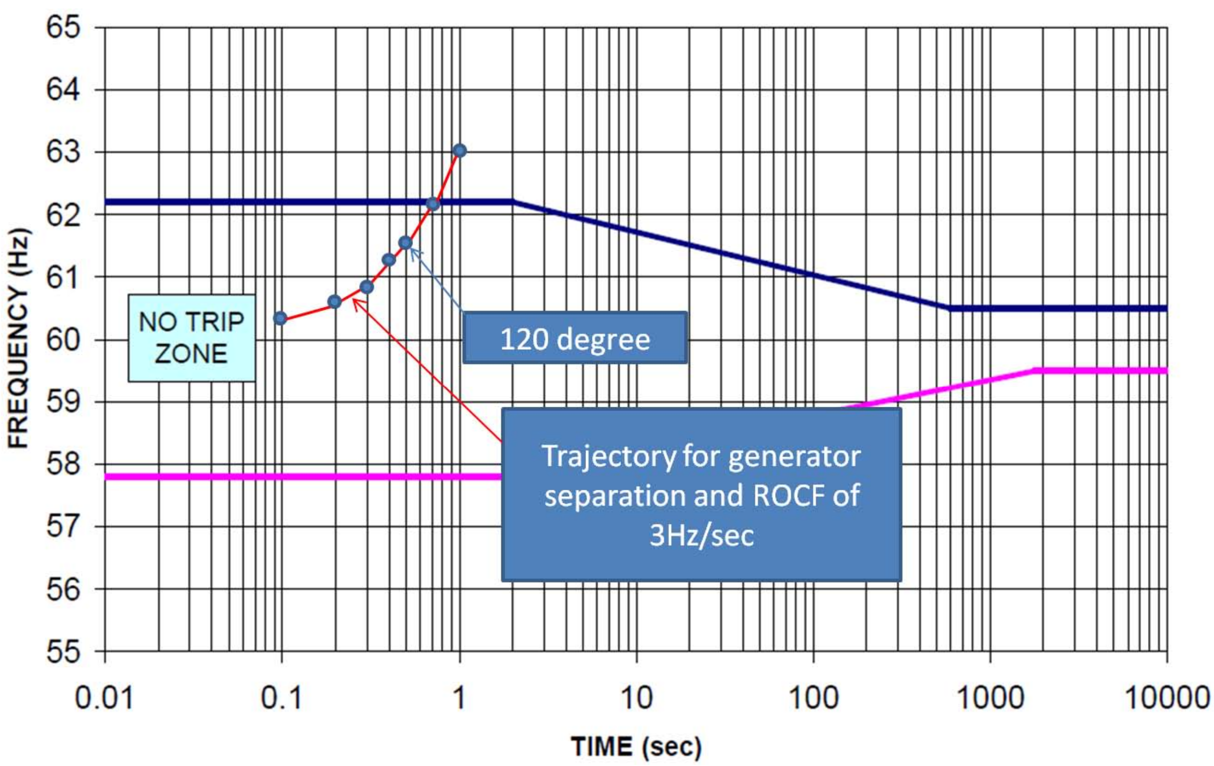


Figure 3-2
Generator frequency deviation after separation versus the NERC PRC-024 off nominal frequency capability curves.

In Figure 3-2, the frequency of a generator is plotted with a rate of frequency change (ROFC) of 3 Hz/s after the separation from the grid. The blue and red curves show the NERC PRC-024 requirements. The research fining is that the ANSI 81 function (under- or over-frequency function) cannot be used **alone** to prevent an AURORA attack because a damaging closing angle can be reached faster than the ANSI 81 function can response.

Over- and Under Voltage Protection (ANSI 59/27)

The ANSI 59 over-voltage protection function and ANSI 27 under-voltage protection function can be used to detect the generator separation. However, an over-voltage or under-voltage may not appear in case the excitation system control is fast enough to regulate the voltage. NERC PRC-024 provides a guideline for setting generator voltage protection functions for the purposes of supporting transmission system stability. However, these suggested settings may make voltage protection functions too slow for protection against the AURORA events.

Wider Area SynchroPhasor Based Protection System

The voltage phasors from phasor measurement units (PMUs) at different locations in power grid can be used to calculate the real-time phase angle between the voltage of the generator terminal and any other locations of the power grid. The generator separation can be detected even in the hard-to-detect situations where the separated generator feeding a balanced load before the separation. However, this wide area protection method relies on the necessary communication infrastructure, phasor measurements from selected locations, and a wide area controller. The speed of this wide area protection method in response to AURORA events is also a challenge.

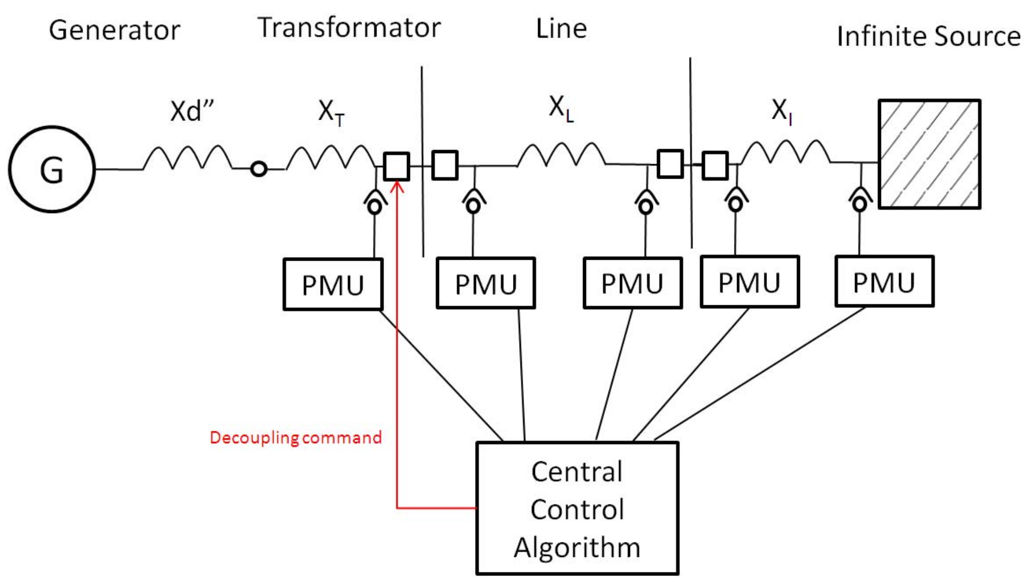


Figure 3-3
Phasor Measurement Unit (PMU) based wide area protection system for detection of generator separation

Figure 3-4 shows an PMU based wide area protection scheme for detection of generator separation. If any of the breakers in Figure 3-3 is opened by an AURORA attacker, the central control algorithm can compare the voltage phasor measurements at the generator terminal and other locations in real time to detect the generator separation. The timing is critical as the scheme includes many steps:

- Measuring the voltages phasors;
- Transmitting the phasor measurements to a central controller;
- Apply the algorithm and initiate appropriate response;

- Sending a decoupling command (generator tripping) via communication links to the Generator breaker;
- Open and lockout the generator breaker.

To effectively prevent an AURORA attack, the scheme has to be fast and secure.

Hardware Mitigation Devices (HMD)

The project investigators evaluated a number of hardware mitigation devices available in market. These products were claimed to be developed specifically for detecting and protecting against AURORA attacks. Following is high level description of the findings.

Approach 1: using rate of frequency change (ROFC) and phase angle

The investigator found that to detect generator separation, one HMD used an approach that uses the rate of frequency change (ROFC) and an estimation of phase angle between the generator and the power system.

Figure 3-4 shows a simplified functional diagram of the HMD algorithm based on the device manual [8].

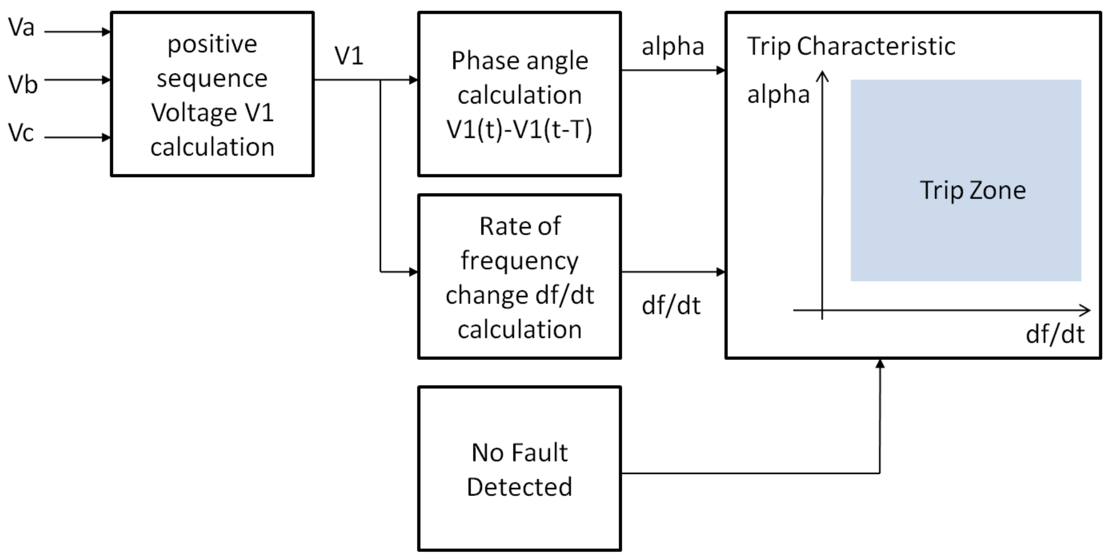


Figure 3-4
Hybrid algorithm using rate of frequency change (ROFC) and phase angle

If a generator is disconnected from the power grid, the generator will accelerate and cause the frequency increase, which will result in an increasing angle difference between the generator and the grid. Before issuing an AURORA tripping command, the relay takes into account of both the rate of frequency change (ROFC) and voltage phase angle difference. The trip command will be issued if the ROFC reaches higher than the setting and the angle is increasing above 40 degrees. For motors, a trip command will be issued if the motor frequency decreases with a settable rate and the angle is decreasing below negative 40 degrees. The hybrid algorithm will be blocked for a period time if a fault is detected using an under voltage protection function.

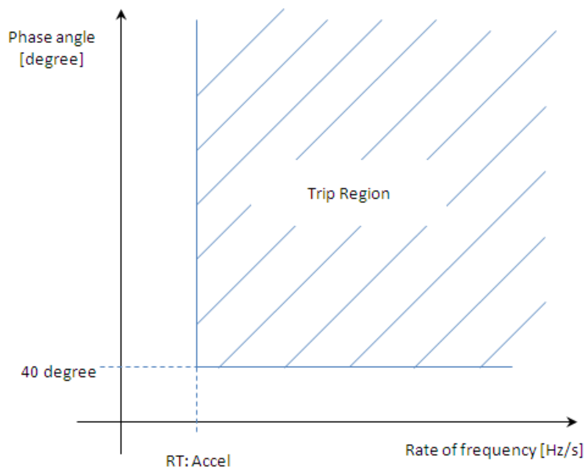


Figure 3-5
Trip characteristic of an HMD

The approach 1 has the advantage that the voltage measurement across the breaker is not needed. However, the approach does not take a possible vector jump into consideration, which could be a very useful element for detecting generator separation. As an example shown in Figure 3-6, if a generator is connected via a long transmission line to the load center, the voltage jump could be a significant criterion for generator separation.

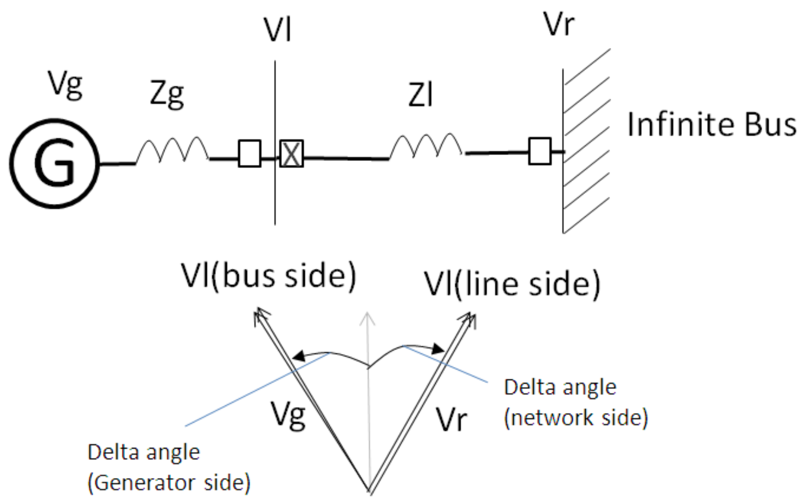


Figure 3-6
Vector jump on both sides of the disconnecting breaker

The uniqueness of the approach 1 is that it evaluates the estimated phase angle between the power grid and the generator to decide the timing of issuing a trip command. In the algorithm, the phase angle was set as a fixed value of 40 degrees because 40 degree is considered as the limit within which closing a breaker out-of-synchronism can still be accepted.

Note that a classical ROFC function (see Section 3.2) with a fixed time delay will not be able to accurately determine the actual phase angle when the trip command is being issued. Therefore, it may not be able to prevent the reclosing at dangerous angles (greater than 40 degree).

Approach 2: using rate of frequency change and the measured frequency

In [9], the author proposed a solution by using the over/under frequency protection function and the rate of frequency change (ROFC) function to detect the separation of the generator. Similar to the approach 1, approach 2 also has built-in automatic time delay settings. The trip characteristic is shown in Figure 3-7. The "cutting out" at the corner of the trip zone is intended to accommodate load change events to avoid potential misoperations.

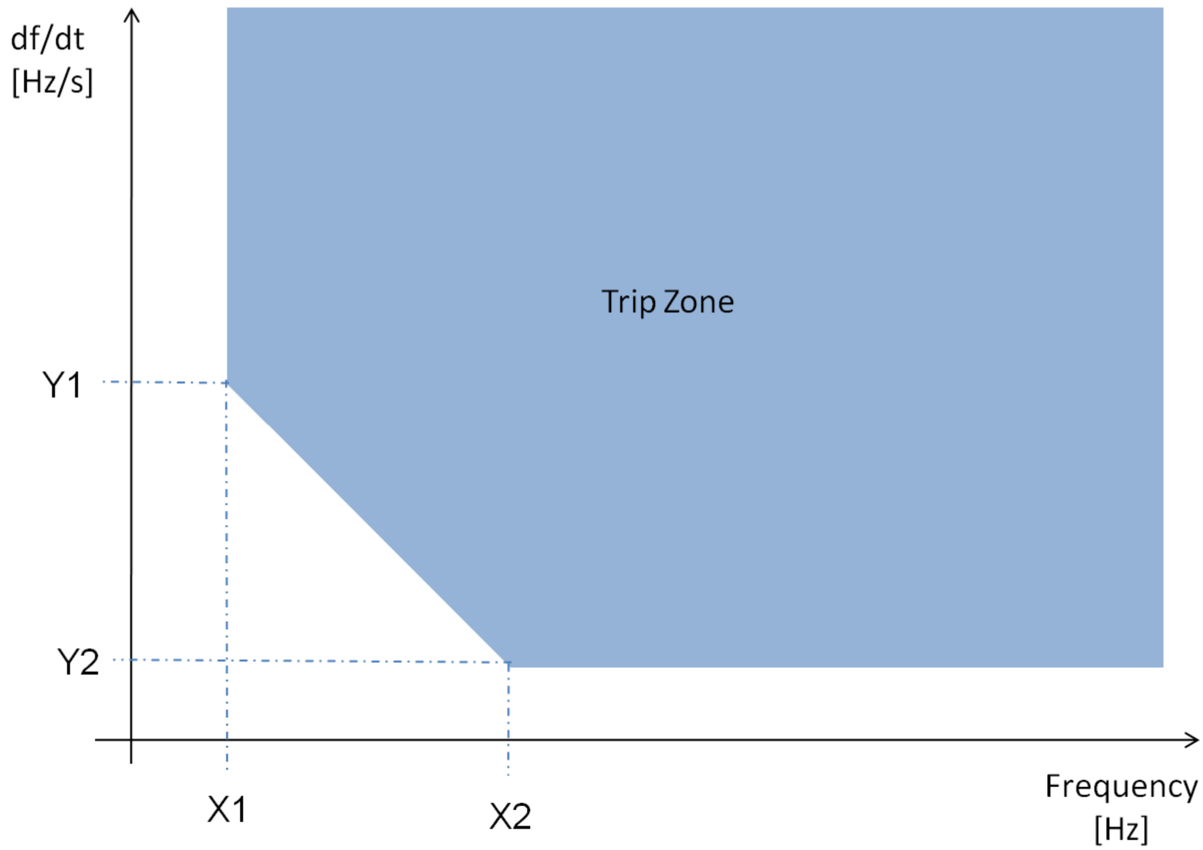


Figure 3-7
Characteristic using change (ROFC) and the measured frequency

The advantage of approach 2 is that the ROFC function can be set very sensitive (at Y2) with little risk of misoperation on load jumps, because a larger frequency deviation is required as a supervisory element. A load jump would start with a certain ROFC value and as the frequency increased, the ROFC value will decrease. The trip zone needs to be properly set so that any load jump will not enter the trip region.

Under-current function (ANSI 37)

As previous discussed the generator separation will not lead to any over current situation, however, the under-current function may apply as the generator separation could result in reduced currents or complete interruption. The research question is whether or not an undercurrent function can be used to detect and trip the generator in AURORA attack.

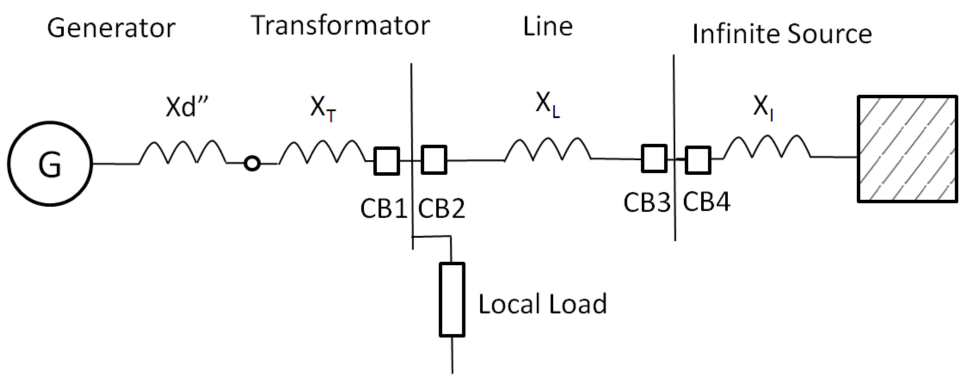


Figure 3-8
Application with local load

The project investigator thinks the utilization of an undercurrent element is difficult, because the function will need the intelligence to guarantee that it will not operate during low load situations. If a generator is separated from the power grid but still supports a local load as shown in Figure 3-8, the currents will not be interrupted and an undercurrent element will be difficult, if possible, to properly set.

In the situations where the separation of a generator will cause the current to be interrupted, the under current may be used with additional control logic and other protection functions.

Summary of generator separation and islanding detection

The project investigator thinks that none of the above protection functions can provide 100% reliable operations for detecting and tripping generator separations or islanding caused by an AURORA attack. The dependability and the security of using each protection function largely depend on the proper scheme design and function settings. It could be a challenge to balance the sensitivity and the security.

A summary of the discussed functions is listed in Table 3-1. An assessment of AURORA attack risks and consequences should be performed to determine which protection function(s) should be used.

Table 3-1
Summary of generator separation and islanding detection functions

Function at the generator	Pick up time	Security	Dependability	Cost
Vector Jump	1 cycle	low	high	low
Rate of Frequency Change (81R)	6-10 cycle	medium	medium	low
Frequency (81)	100 cycle	medium	low	low
Over- and Under Voltage (59/27)	100 cycle	low	low	low
Phasor Measurement Units	10 cycle	high	high	high
Hybrid: Rate of frequency change & phase angle	2 cycle	high	medium	medium
Hybrid: Rate of frequency change & frequency	5 cycle	medium	medium	medium
Under current function	5 cycle	low	medium	low

Possible solutions to prevent unsynchronized reclosing

The project investigator think there is no protective function available which can guarantee a 100% secure and dependable operation of a generator breaker in case that a downstream breaker disconnected the generator from the power grid. The negative impact on power generation reliability by introducing new AURORA protection functions needs to be carefully evaluated.

This chapter will discuss protection functions and procedures which can help prevent a possible AURORA attack in the case that an attacker has obtained the access to a remote substation and control equipment. As it is assumed before, the access to a breaker inside a generator substation is considered as very unlikely, particularly if the generation facility is classified as a critical infrastructure and proper security measures are in already place. However, it is more likely for an attacker to gain access in an unmanned substation which could be many miles away from the generator. Depending on the power system topology, a breaker in a remote substation, which can interrupt the entire or partial connection between a generator and a power grid, could be possibly used to perform an AURORA attack. As discussion in Chapter 2, such remote attacks could result in the same or similar damages as it would be done with the generator breaker.

It is worthwhile to point it out that all approaches discussed below for remote substations can possibly create some challenges for an attack, but may not be able to disable an AURORA attacker with physical access of substation facilities. A capable attacker may be able to bypass all protection and control equipment simply by a jumper. Therefore the goal is to prevent accidental misoperations and to challenge an attacker.

Trip by overcurrent element ANSI 50/51 (on generator or step up transformer)

All previous solutions are targeting to open the generator breaker before an attacker can reclose a generator breaker or downstream breaker(s). It is intended to prevent a generator from any damaging torque caused by an AURORA attack. However, as we can see, the utilization of these functions may possibly have impact on other power system reliability or stability requirement. Moreover, a 100% dependable operation is not always guaranteed.

If a single-shot of unsynchronized reclosing is allowed, the overcurrent protection may be employed to prevent any further AURORA reclosing attempts. As previously discussed, an unsynchronized reclosing can produce large transient currents which can be as high as the maximum emergency load current of a generator. The overcurrent functions for generator protection or step-up transformer protection could be used to trip the generator once the first shot of an AURORA attack is detected.

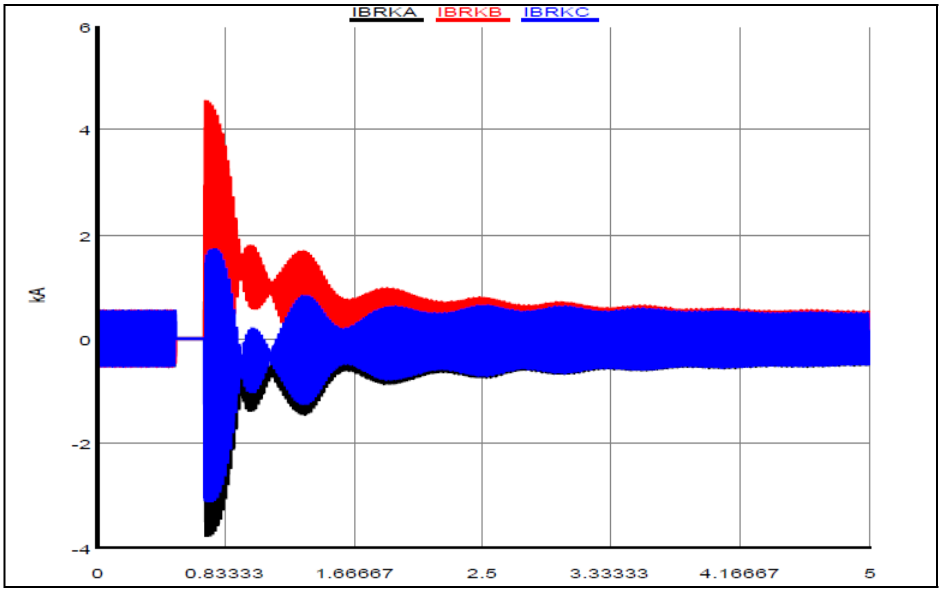


Figure 3-9
Phase currents after unsynchronized reclosing

Obviously, the disadvantage of using ONLY the overcurrent functions is that a generator may have to tolerate a damaging torque produced by one shot of out of synchronism reclosing. Again, whether or not to use overcurrent for AURORA attack protection should be decided on a case by case basis. For certain generators, “one-shot” could be very damaging, particularly in the case that the system impedance is very small and the produced torque can damage the generator even on the first closing. In some cases it may be an option for allowing one-shot of closing without causing a major damage to a generator, however, the incurred large torque can still contribute to reduction of the generator life span. A large system impedance will also limit the transient current, so setting an appropriate current pick up level will be difficult in such cases.

Using synchronism check function on all intertie breaker

The most effective protection function against an out-of-synch reclosing is to supervise the close command by checking synchronism of the voltages across a breaker. A close command should be allowed only if voltages are in synchronism. This is achieved with a so called synch-check relay which compares the amplitude, the frequency and the phase angle of both voltages measured on both sides of the breaker. To allow a close command, all three elements need to be inside of a tolerance range. The angle of 10-20 degree is accepted between the voltages as it does not produce a high transient current, but only a small torque at the generator. If a synch check function is active, an attacker may not be able to close the circuit breaker at any dangerous angle. The synch check contact is normally connected in series with the circuit breaker closing contacts.

The implementation of an electromechanical synch check relay could prevent an AURORA attack initiated via a cyber access. It needs to be checked whether the reset time for the synch check permission is less than 100ms-200ms because this could be a time window for an AURORA attack. The timing depends on rate of frequency change and the phase angle an attacker wants to reach. The phase angle is hereby a function of the time delay and can be described by the following formula:

$$\varphi = \frac{1}{2} ROFC \cdot t^2$$

Equation 10

For example, if the dropped load leads to a rate of frequency change of 3 Hz/s, it will take approximately 500 ms to reach an angle of 120 degrees.

If an attacker gained physical access to the substation he would be able to bypass the supervision contact of the synch-check relay. However he would need detailed knowledge about the scheme and the wiring in the substation.

Lockout breaker after trip

Lockout a breaker after any trip could be an effective way to prevent or disable an AURORA attack. The close command can be issued only after the lockout relay was reset. This may particular be useful to prevent a cyber-initiated attack. Most lockout relays in service are electro-mechanical type, which is inherently immune to any cyber attack.

Even in the case when the attacker is physically in the substation, it will create significant difficulties for the attacker. It takes certain time for an attacker to reset the lockout relays before he could issue the next close command. This may possibly allow generator protection functions to detect the generator separation and take proper protection actions.

The disadvantage is that this approach may impact the operation procedures, or will have to disable automatic reclosing schemes or SCADA remote controls.

Two close contacts in series

An additional close contact can prevent an accidental closing by operators. The operation of two close contacts introduces an additional safety as two independent commands have to be issued at the same time before a breaker can be closed. The second close contact can be supervised by a SCADA controlled signal or by a second switch on the control panel located in the substation.

To prevent an AURORA attack via cyber, it would be helpful that one contact can only be operated locally. An attacker who has physically access to the substation will also be challenged as he/she needs to know the control logic and wiring in order to close a breaker.

The disadvantage is that this impacts the operation procedure and will not permit any automatic reclosing.

Using a close delay for breaker reclosing

To introduce a time delay before an opened breaker can be closed again would prevent a successful AURORA attack as certain timing is required. If the close command is delayed, the system may detect the isolation and take the generator offline. Based on the expected rate of frequency change and the over frequency settings of the generator protection a time delay can be determined.

In the example above with an assumed rate of frequency change of approximately 3 Hz/s following the isolation of the generator, the two voltages could reach an angle difference of 120 degree after approximately 500ms. The AURORA attack needs to issue a close command between 200-700ms to produce a significant torque on the generator. An introduced time delay of approximately 2 seconds would successfully prevent this. The time delay setting should be long enough so that the over-frequency protection function on the generator can detect the isolation and take the generator offline.

Monitor breaker trip/close cycle and lockout

This approach is similar to using the lockout relay after a trip command, but it will permit at least one close command. The disadvantage of this approach is that it allows a single out of synchronism reclosing. And the advantage of this approach is that it will allow at least one auto-reclose cycle. This is an advantage for breaker which is only occasionally able to separate the generator from the power grid but normally work in parallel with other breakers.

4
STRATEGIES FOR AURORA MITIGATION THROUGH PROTECTION AND CONTROL

Economically, it is not feasible to implement all approaches discussed in chapter 3 or apply the approaches to every generators or motors in power grid. A risk assessment should be performed to assist in the selection of mitigation approaches and strategies. Proper criteria need to be developed to assess the level of AURORA risk or vulnerability for each generator or motor. Based on the results of risk assessment, utilities can choose the most suitable and cost-effective way to implement the mitigation strategy.

This chapter will be completed in 2012 (project phase II).

5
SUMMARY

The so-called “AURORA test” revealed a potential gap in generator and motor protection. An intentional or unintentional closing of a circuit breaker out-of-synchronism can create a large torque and therefore damage a generator or motor. The industry and regulators have expressed the concern for the reliability and safety of nation’s critical power generation infrastructure. Two mitigation directions have been identified. One is *protection and control engineering practices*, and another is through *electronic and physical security mitigation measures*. This EPRI project initiated by the protection and control task force in 2011 explores the possible mitigation approaches and options by using *protection and control (P&C) engineering practices*.

Variety of P&C functions and elements have been studied, which include the rate of frequency change (ROFC), frequency, phase angle, over/under-voltage, over/under-current, and emerging synchrophasor technologies.

A study of the hardware mitigation devices (HMDs) has been performed. The P&C principles used by these HMDs to protect against AURORA attacks were explored and explained in the form of high-level functional diagrams.

The project investigator thinks that utility protection and control staff can use two strategies to mitigate the AURORA threat:

- Use proper protection function(s) to detect a separation of a generator from the power grid. Then, trip and lockout the generator breaker before an AURORA attacker can reclose any downstream breaker(s).
- Design proper control schemes for breakers in such a way that they cannot be easily reclosed out-of-synchronism as required for a successful AURORA attack.

To select an appropriate mitigation approach for a specific generator, an assessment of AURORA vulnerability of the generator is normally required. The following factors should be included in the vulnerability assessment:

- The risks and possibilities of potential AURORA attacks
- The consequences from a successfully-executed AURORA attack
- The possible impact of mitigation measures

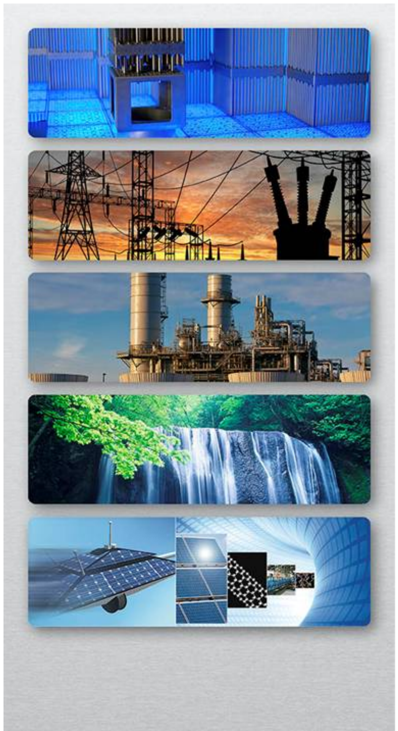
Based on the 2011 findings, the phase II of the project will explore the best strategies and P&C approaches for utilities to consider in the development of their own AURORA threat mitigation programs. It is worthwhile to point it out that the P&C engineering practices cannot replace the physical and cyber security efforts that utilities need to consider in the overall mitigation strategies.

6
REFERENCES

1. M.C. Jackson, S.D. Umans, R.D. Dunlop, S.H. Horowitz, A.C. Parikh, "*Turbine-Generator Shaft Torques and Fatigue: Part I - Simulation Methods and Fatigue Analysis*", 1978 IEEE Winter Power Meeting, paper F78 038-2.
2. P.C. Krause, W.C. Hollopeter,D.M Tiezenberg, P.A. Rusche, "*Shaft Torques during Out-Of-Phase Synchronization*", IEEE Transactions on Power Apparatus and System,Vol. PAS-96, no. L, July/August 1977.
3. H. S. Kirschbaum , "*Transient Electrical Torques of Turbine Generators during Short Circuits and Synchronizing*", AIEE Transaction, vol. 64, Feb. 1945, pp. 66-70.
4. Park, R. H., "*Two-Reaction Theory of Synchronous Machines*" , A.I.E.E. TRANS., Vol. 48, No. 2, July, 1929, p. 716.
5. V. W. Ruskin, "*Maximum Short Circuit and Faulty Synchronizing Torques on Generator Foundations*", AIEE Transaction vol. 74, pt. III, Aug. 1955, pp. 618-24.
6. ANSI IEEE C50.13 "*IEEE Standard for Cylindrical-Rotor 50Hz and 60Hz Synchronous Generators Rated 10 MVA and Above*" , 2005.
7. ANSI IEEE C37.102 "*IEEE Guide for AC Generator Protection*", 1995.
8. Cooper Power System, "*User and Operations Manual for the iGR-933 Rotating Equipment Isolation Device (R.E.I.D) Idea Relay Scheme*" ,S165-933-1,2009.
9. D. Salmon, M. Zeller, A. Guzmán, V.Mynam, M. Donolo, "*Mitigating the Aurora Vulnerability With Existing Technology*" proceedings of the 36th Annual Western Protective Relay Conference, Spokane, WA, October 2009.

A

TASK FORCE MEETING SLIDES



Mitigation of the Aurora Threat through P&C Engineering Practices

EPRI P&C Task Force Meeting
August 2nd, 2011

Contents

- Proposed scope of work
- Background
- Proposed report outline
- Group discussion and feedback

Proposed scope of work

The objective of this project is to create a report what will lay the foundation to build an AURORA mitigation strategy. The report will consist of 3 major parts.

– Part 1: Basic understanding of the AURORA event

– Part 2: Function analysis of protective relays and Hardware Mitigation Device (HMD)

– Part 3: Risk Assessment and mitigation

EPRI ELECTRIC POWER RESEARCH INSTITUTE

Proposed scope of work

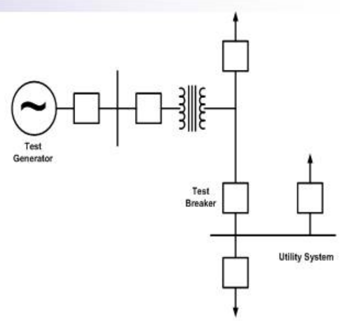
- Literature research on AURORA vulnerability and summarize the findings
- Review and analysis of the state of the art protective relaying for generators and motors protection
  - Research on the state of the art protection philosophy for generators and motors is by reviewing literature and relevant standards.
  - Assist EPRI in hosting a seminar with members about current P&C engineering practices and mitigation methods .
- Study on Hardware Mitigation Devices
- Research on impact of “Aurora Threat” on transformers and breakers
- Development of Risk assessment approaches

EPRI ELECTRIC POWER RESEARCH INSTITUTE

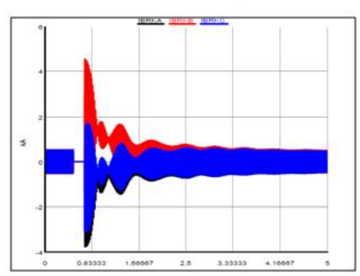
Why is Aurora Getting Attention?

- March 2007 test gained congressional attention
  - Power grid is one of the most critical infrastructures
- Video shown in CNN report September 2007
  - http://www.youtube.com/watch?v=C2qd6xXbySk
- Congressional hearings October 2007 and May 2008
  - Critical of NERC and progress
- NERC issued a notice to industry on June 21, 2007 identifying several measures necessary to mitigate
  - Voluntary with limited reporting on remediation
- New alert issued October 13, 2010
  - Includes greater detail including suggested remediation approaches
  - Requires responses by December 13, 2010; June 13, 2011; and every six months until fully mitigated

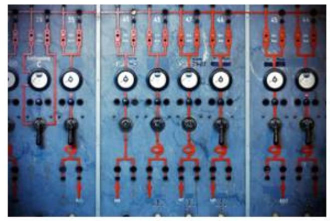
Chapter : Understanding Aurora



- Intentionally opening and reclosing a breaker out of synchronism
- How important is the timing of an Aurora attack?
- Which equipment is effected and why?
  - Generator, Motor, Transformer, Breaker….
- Why are today's protection functions not sufficient?
- How does different system configurations must be considered?



Understanding Aurora

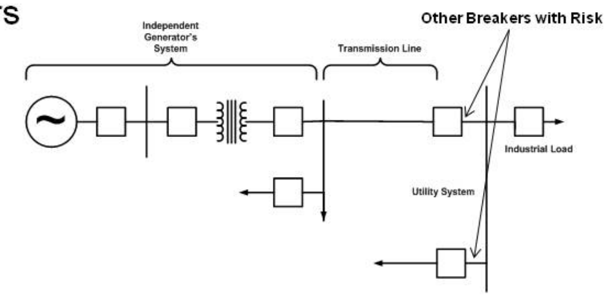


- Protection Elements on Generators
  - Most will not detect
- Others depend on settings
  - Synchronism check (25)
    - Setting allows some degree of separation
  - Undervoltage and overvoltage (27 and 59)
    - Dependent on rate of change and setting
  - Out of Step (78)
    - Time delay generally too long
    - and will not operate for action at remote breaker
  - Over and Under Frequency (81)
    - May operate depending on settings, time delay, and voltage blocking
- Aurora exploits this short time window before classical generator protection function can act – gap in protection

EPRI ELECTRIC POWER RESEARCH INSTITUTE

Understanding Aurora

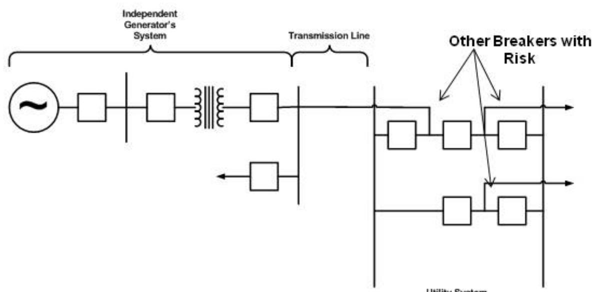
- Dependant on system configuration
- Beyond the generator breaker
  - Protection at the generator will not likely detect
  - Generator is not "out of step" where measurements are taken
- May require opening and closing of combination of several breakers



EPRI ELECTRIC POWER RESEARCH INSTITUTE

Understanding Aurora

- Numerous possible configurations
  - Each situation will have differences
- Three basic perspectives
  - Generation only – only auxiliary loads
  - Co-generation with energy back to grid
  - Co-generation with no energy to grid

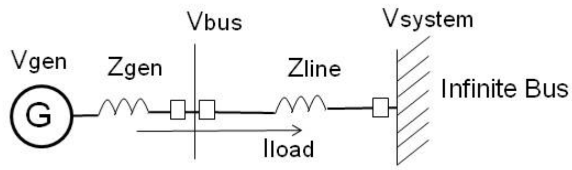


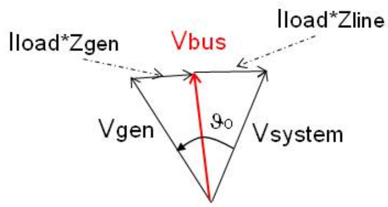
Understanding Aurora

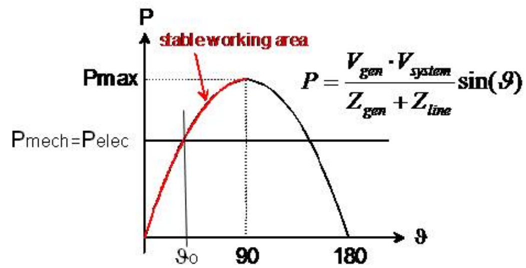
- Aurora initially was demonstrated via a cyber attack requiring
  - Hacking skills
  - Power system knowledge and information
  - Access via communication
- Physical approach is equally possible requiring
  - Access to protective relays and controls
  - Power system knowledge and understanding

What is the problem?

- Normal load situation

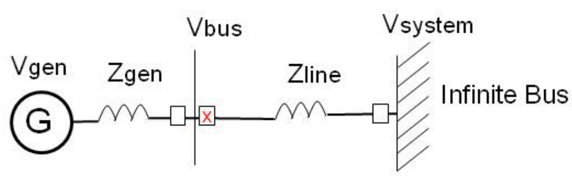


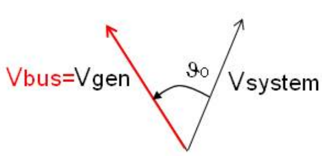


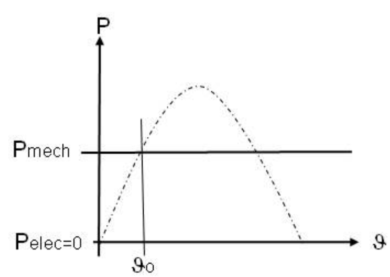


What is the problem?

- Breaker opening and disconnecting generator from grid

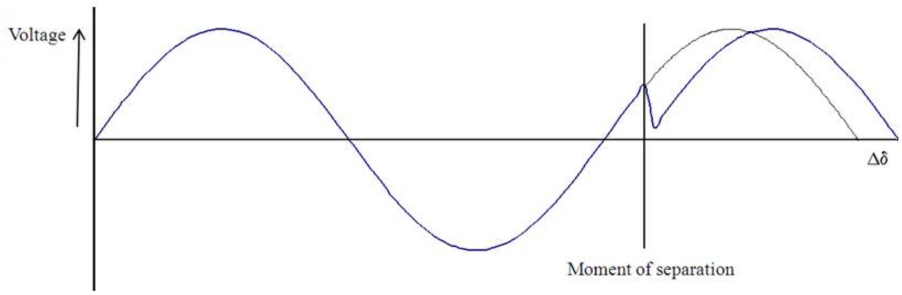






Vector jump

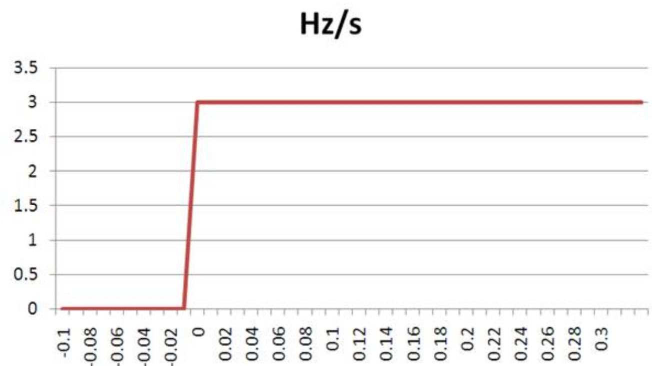
- Vector jump is caused by disappearance of voltage drop across generator impedance
  - Is not a jump of the generator voltage just of the measurement!



ELECTRIC POWER RESEARCH INSTITUTE

Rate of frequency change

- Generator cannot export all electrical energy anymore but receives still same mechanical energy assuming govoner is slow (> 1s)
- Mechanical Energy causes acceleration of generator



ELECTRIC POWER RESEARCH INSTITUTE

How to calculate rate of frequency change?

$$\frac{df}{dt} \cdot \frac{2 \cdot H \cdot S_N}{f_N} = P_M - P_E$$

with

P_M = mechanical active power going into the generator

P_E = electrical active power transported over the line

f_N = nominal frequency

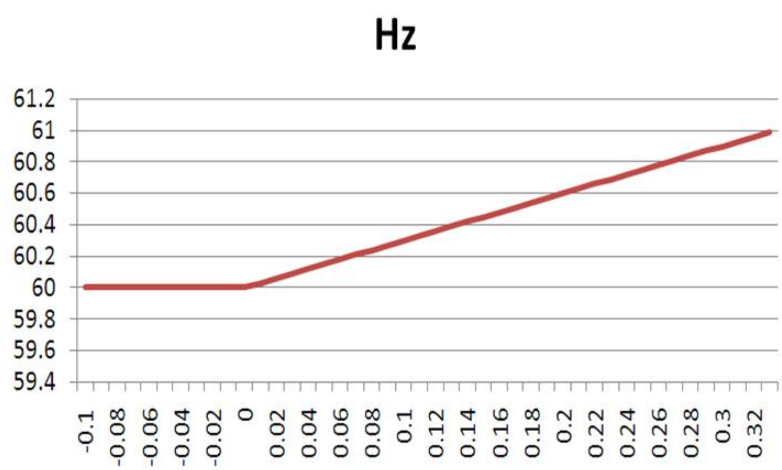
H = inertia value of machine

for hydro generators	: 1.5.....6.0
for turbine - driven generators	: 2.0.....10.0
for industrial turbine generators	: 3.0.....4.0

S_N = nominal power of machine

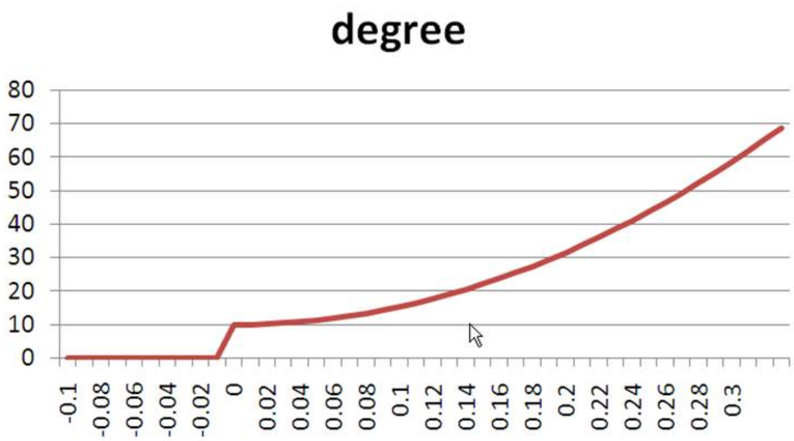
Frequency

- Acceleration causes the frequency to increase



Voltage angle change

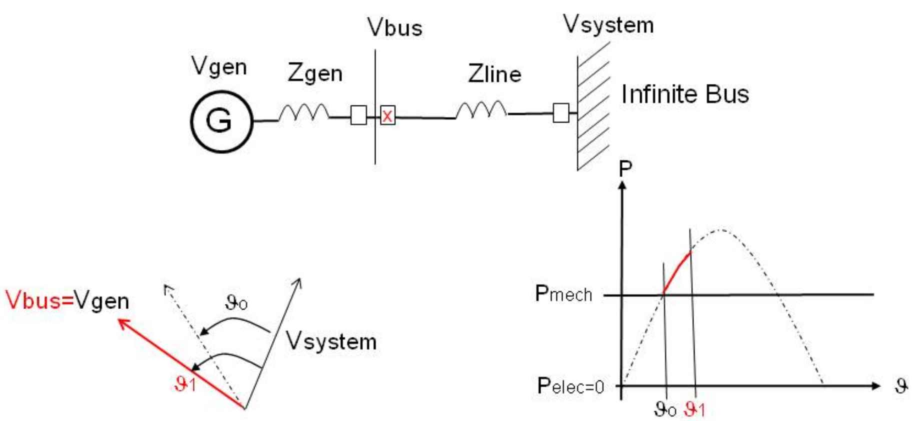
- Acceleration and frequency change causes voltage angle to increase



ELECTRIC POWER RESEARCH INSTITUTE

What is the problem?

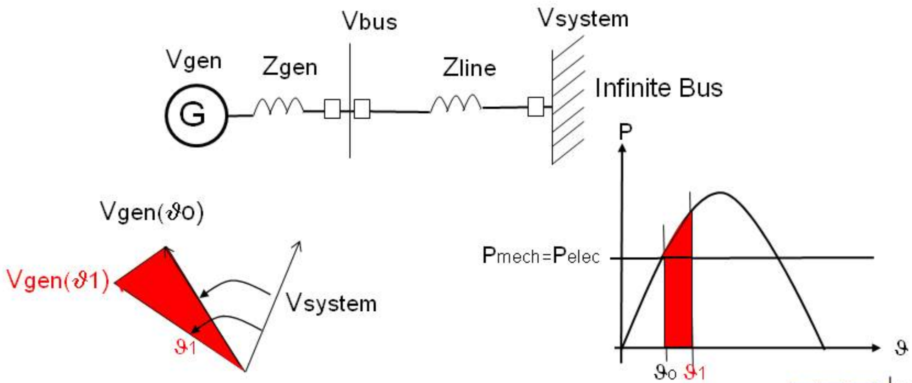
- During breaker-open time:
  - generator voltage shifts in relation to the grid voltage



ELECTRIC POWER RESEARCH INSTITUTE

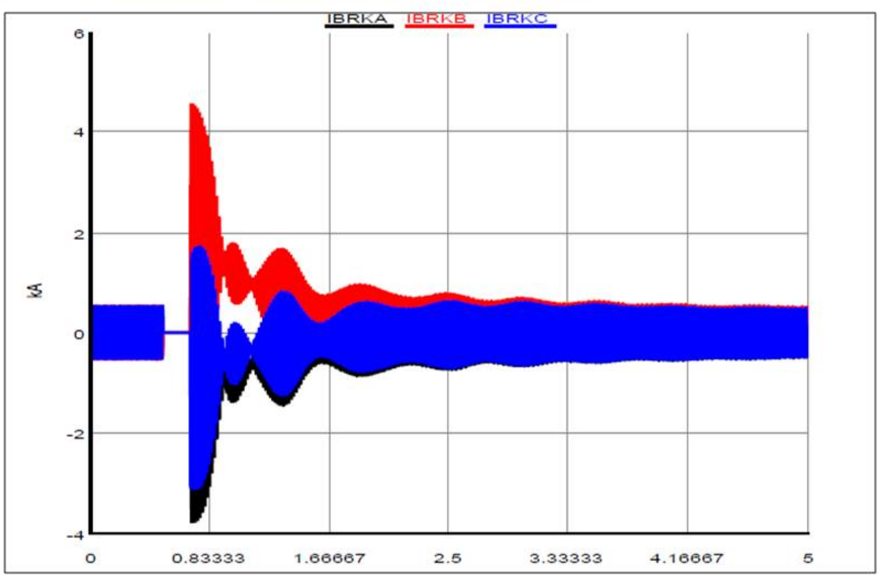
What is the problem?

- Closing the breaker:
  - Close circuit breaker and connect generator out of synch to the load angle not the grid!
  - Similar to 3 pole autoreclose without a fault



ELECTRIC POWER RESEARCH INSTITUTE

Currents caused by AURORA attack



ELECTRIC POWER RESEARCH INSTITUTE

Torque in Relation to Switching Angle

- Torque has maximum by 120 degree switching angle
- Torque at 180 degree is same as for 3 phase fault

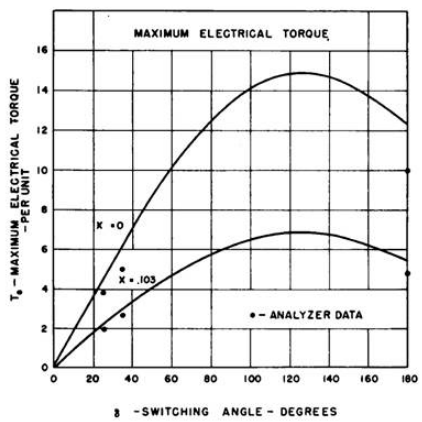


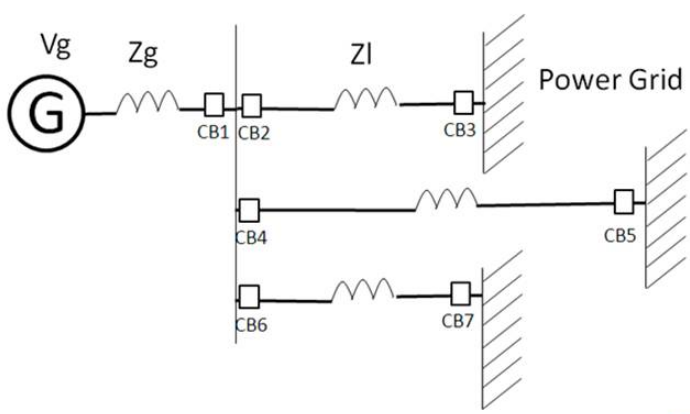
Fig. 1. Maximum electrical torque as a function of switching angle for synchronizing two identical large turbine generators. The upper curve is for switching at the alternator terminals while the lower curve assumes a 10.3-per-cent system reactance

Source: A.J Wood, "Synchronizing Out of Phase", AIEE 1957

EPRI ELECTRIC POWER RESEARCH INSTITUTE

What is the problem?

- Combination of breaker operation can also cause AURORA attack
  - Trip Bus by simulating bus fault (CB1,CB2,CB4 and CB5) and close CB1 and CB2



EPRI ELECTRIC POWER RESEARCH INSTITUTE

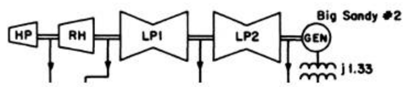
What is at risk

- A successful AURORA attack will reduce the lifespan of **generators** and **motors**
  - For a single "shot" a reduction between 1- 100% is possible
    - Detailed investigation needed
  - Several "shots" could cause mechanical resonance and destroy the generator

Degrees Out of Phase	Shaft Section	% Life Lost
120°	HP-RH	.007
	RH-LP1	.3
	LP1-LP2	.7
	LP2-GEN	.8
180°	HP-RH	0
	RH-LP1	.009
	LP1-LP2	.03
	LP2-GEN	.03

Table 4 Results of Out of Phase Synchronization Tests

M.C. Jackson, S.D. Umans, "TURBINE-GENERATOR SHAFT TORQUES AND FATIGUE: PART III - REFINEMENTS TO FATIGUE MODEL AND TEST RESULTS" IEEE Transactions on Power Apparatus and Systems, Vol. PAS-99, No. 3 May/June 1980, page 1259-1268



Notes of the Kick off Meeting

- Perform a survey of industry experience with installation of Hardware Mitigation
- Device (HMD). How do the utilities justify the use of HMD? Do they do a sophisticated testing before apply HMD? How to do the risk assessment?
- There might be a legal/policy limit in answering the survey of this nature.
- Instantaneous over current element for transformer protection may trip on an AURORA attack.
- There might be some solutions allowing a single shot. What's the impact of single shot? % of generator life span that a single shot could possibly reduce?
- Will the report discuss associated issues like syncheck, breaker close timing?
- Investigate under-excitation function (Impedance based) as a possible solution.
- What is the impact of AURORA threat on wind farms?

Proposed Outline

Chapter: P&C methods for mitigating the AURORA threat

- Allow one unsynchronized shot
  - Trip of over-current element on generators or GSUs
  - Monitor breaker trip/close cycle and lockout
- Prevent any unsynchronized closing
  - Apply syncheck functions on all intertie breakers
  - Two close contacts in series
  - Use generator excitation system protection
  - Lockout after trip
  - Add a time delay for breaker reclosing
  - Use Hardware Mitigation Devices (HMDs)

Proposed Outline

Chapter: Strategy and selection of AURORA mitigation solutions

- Risk assessment
  - Evaluation of generator size and its impact on grid reliability
  - Black start
  - Generator connection with grid
  - Costs of mitigation solutions
  - Impact of mitigation solutions on operation
  - Impact of mitigation solutions on reliability

- Selection of mitigation solutions
  - Which solution will be a good choice?

Export Control Restrictions

Access to and use of EPRI Intellectual Property is granted with the specific understanding and requirement that responsibility for ensuring full compliance with all applicable U.S. and foreign export laws and regulations is being undertaken by you and your company. This includes an obligation to ensure that any individual receiving access hereunder who is not a U.S. citizen or permanent U.S. resident is permitted access under applicable U.S. and foreign export laws and regulations. In the event you are uncertain whether you or your company may lawfully obtain access to this EPRI Intellectual Property, you acknowledge that it is your obligation to consult with your company's legal counsel to determine whether this access is lawful. Although EPRI may make available on a case-by-case basis an informal assessment of the applicable U.S. export classification for specific EPRI Intellectual Property, you and your company acknowledge that this assessment is solely for informational purposes and not for reliance purposes. You and your company acknowledge that it is still the obligation of you and your company to make your own assessment of the applicable U.S. export classification and ensure compliance accordingly. You and your company understand and acknowledge your obligations to make a prompt report to EPRI and the appropriate authorities regarding any access to or use of EPRI Intellectual Property hereunder that may be in violation of applicable U.S. or foreign export laws or regulations.

The Electric Power Research Institute Inc., (EPRI, www.epri.com) conducts research and development relating to the generation, delivery and use of electricity for the benefit of the public. An independent, nonprofit organization, EPRI brings together its scientists and engineers as well as experts from academia and industry to help address challenges in electricity, including reliability, efficiency, health, safety and the environment. EPRI also provides technology, policy and economic analyses to drive long-range research and development planning, and supports research in emerging technologies. EPRI's members represent more than 90 percent of the electricity generated and delivered in the United States, and international participation extends to 40 countries. EPRI's principal offices and laboratories are located in Palo Alto, Calif.; Charlotte, N.C.; Knoxville, Tenn.; and Lenox, Mass.

Together…Shaping the Future of Electricity

1021914

Electric Power Research Institute
3420 Hillview Avenue, Palo Alto, California 94304-1338 • PO Box 10412, Palo Alto, California 94303-0813 • USA
800.313.3774 • 650.855.2121 • askepri@epri.com • www.epri.com