AVOIDING UNWANTED RECLOSING ON ROTATING APPARATUS (AURORA)

Working Group J7 of the Rotating Machinery Subcommittee

IEEE PES Power System Relaying and Control Committee

May 12, 2016

Presentation Overview

Working Group

The Issue

Mitigation Measures for AURORA Vulnerability
-System Strength
-High-Speed Synch-Check
-Breaker Closing Delay
-Synchrophasor
-Islanding Detection

Conclusions

Working Group

Chairperson: Mike Reichard

Vice Chairperson: Steve Conrad

Members:

Matt Basler
Gabriel Benmouyal
Zeeky Bukhala
Dale Finney
Dale Fredrickson
Rafael Garcia
Gene Henneberg
Gerald Johnson,
Chuck Mozina
Pratap Mysore
Cristian Paduraru
Phil Tatro
Tom Wiedman
Joe Uchiyama

Working Group Assignment

Deliver a report which discusses the hazards of rotating apparatus out-of-phase circuit breaker closing, scenarios leading to out-of-phase circuit breaker closing, and how to mitigate these findings.

Started September 2010

The Issue

- The Aurora Vulnerability refers to the susceptibility to damage of rotating electrical equipment resulting from a brief separation from, and then a rapid out-of-phase reconnection resulting in large torques imparted to the T-G shaft
- Rapid operation of a breaker control switch (C-O-C) in 100msec is established AURORA Vulnerability
- Devices 21, 24, 32, 40, 51V/C, 64, 78, 87 will not detect attack

Mitigation Measures for AURORA Vulnerability

System Stiffness – Is the system strong enough to cause machine damage?

- Much less likely if Stiffness Ratio < 2
- Stiffness Ratio = Isystem / Igen = X”d / Xsystem
- Example:
- System 345kV, 30kA 3ph fault, 100MVAbase:
  345kV*30kA*√3=17,908MVAsc=179pu;
  X=1/179pu=0.00558pu
- GSU 345/18kV, 100MVA, Zt=10% Generator 100MVA, 18kV, X”d = 0.15pu
  Xsystem = X + Xt = 0.100558

- Stiffness Ratio = X”d / Xsystem = 0.15 / 0.100558 = 1.42

Mitigation Measures for AURORA Vulnerability

System Stiffness – Is the system strong enough to cause machine damage?

Stiffness ratio proportional to ratio of the impedances of generator to GSU plus system.

Most Vulnerable configurations = Highest Stiffness Ratio?
One or more small generators interconnected to the system through a larger GSU.

Least Vulnerable configurations = Lowest Stiffness Ratio?
Generation matches GSU

Most commonly described attack scenario: re-configure the transmission system to make service to the generator radial, then open and rapidly close that remaining radial source.

Mitigation Measures for AURORA Vulnerability

System Stiffness – Is the system strong enough to cause machine damage?

Transmission line switching from steady state condition:

Negligible loss-of-life when $\Delta P \leq 0.5pu$ (C50.13 section 4.2.4.3)

$$\Delta P = \frac{EsEg\ sin\delta}{X}$$

Large angle differences between system (Es) and generator (Eg) voltages created by the AURORA attack would cause the most significant damage.

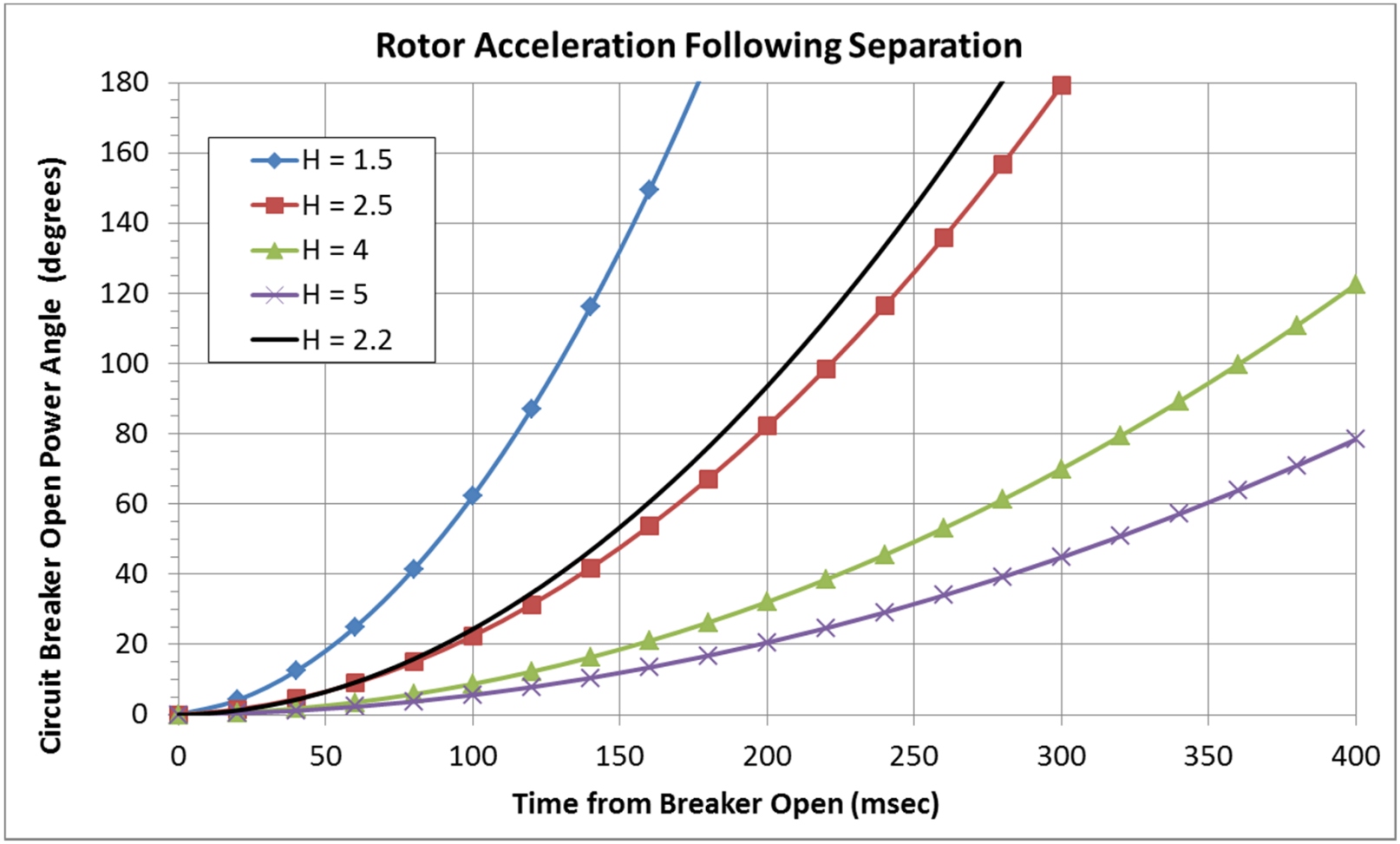
Mitigation Measures for AURORA Vulnerability

High-Speed Synch-Check

- Synchronism check relays ensure circuit breaker closure within voltage and phase angle limits
- If voltage and phase angle are within limits and timer, then 25 contact closes in the “close” path allowing the breaker to close
- Generator Response to System Separation-
  low H = greater angle

Mitigation Measures for AURORA Vulnerability

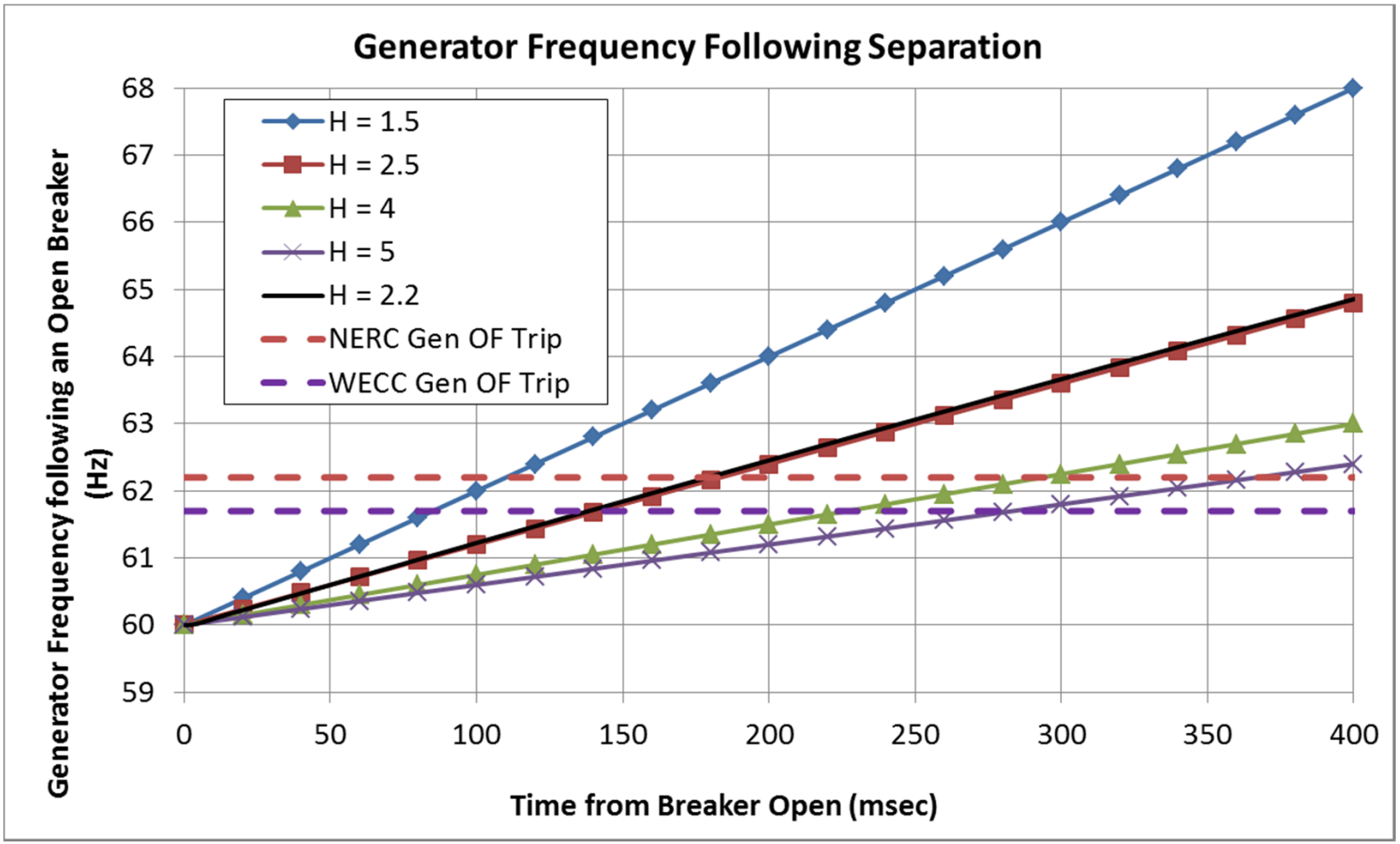
High-Speed Synch-Check



Mitigation Measures for AURORA Vulnerability

High-Speed Synch-Check

Generator Response to System Separation- Slip Frequency (Fs) ∝ H



Mitigation Measures for AURORA Vulnerability

High-Speed Synch-Check

- Typical Slip Frequency settings: 0.1-0.2Hz Transmission, 0.067Hz Generator (>10MVA)

$$Fs = \frac{2xPhaseAngleSetting}{360xTimeDelay}$$

- Fs = 0.067Hz = (2x10°) / (360x0.83s)
-
- EM#1: Fs = 0.30 Hz at an angle setting up to 60° and time dial = 3
- EM#2: Fs = 0.30 Hz at a setting of 40° and time dial =11 (about 0.45 Hz at 60°)
- Solid state synch check relays (SSR) and microprocessor synch check relays (uP Relay) use a specific, fixed slip frequency and timer settings

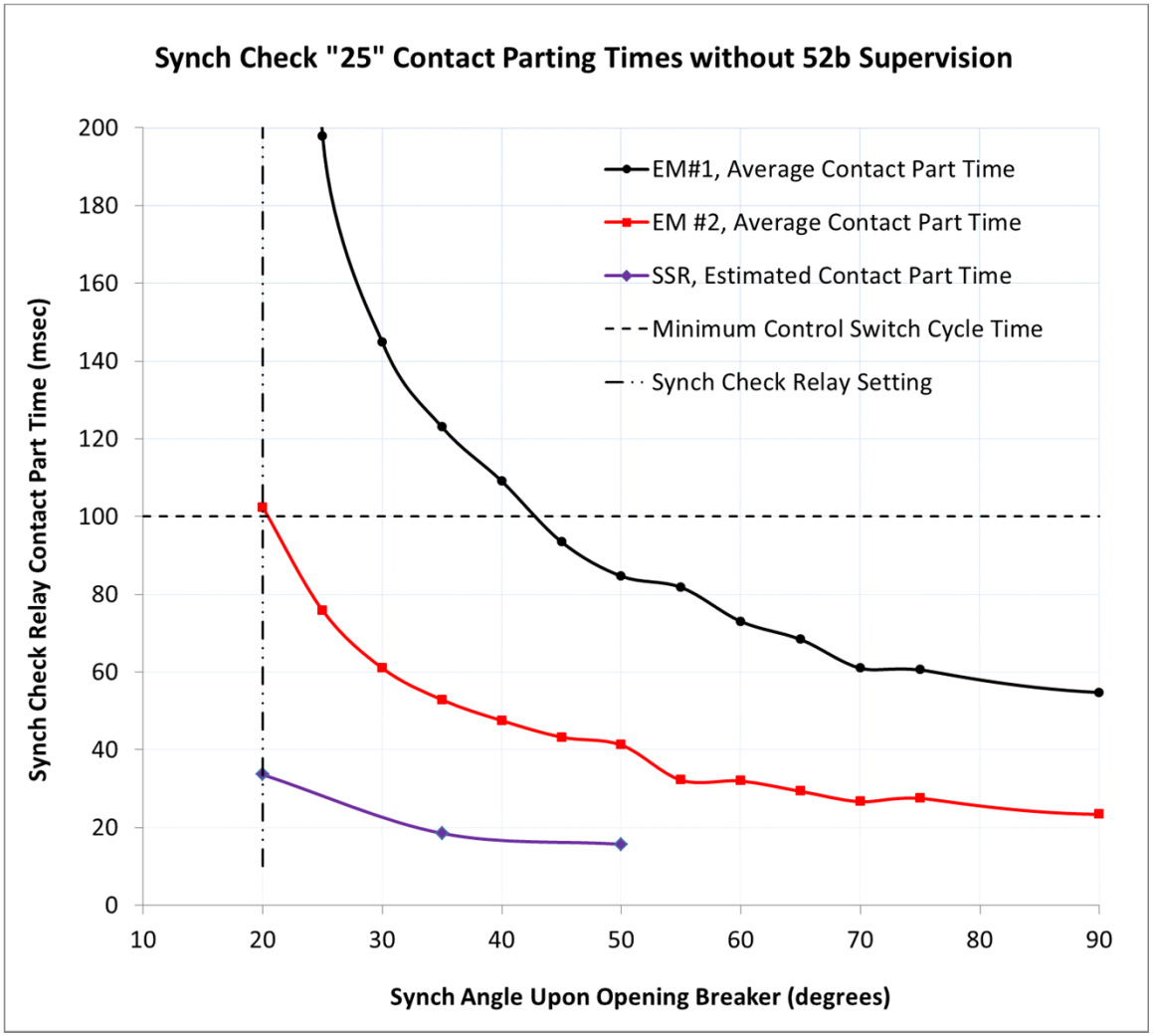
Mitigation Measures for AURORA Vulnerability

High-Speed Synch-Check

- When the synch check relay “25” contact is closed and the breaker is opened, a subsequent attempt to close the breaker before the “25” contact parts will allow the breaker to close, regardless of the actual measured angle
- Synch check relay “25” contact open time a function of the design
- Measurements of the contact parting time for several relays are shown in the table below for the normal application where a breaker auxiliary contact supervises the relay operation

Mitigation Measures for AURORA Vulnerability

High-Speed Synch-Check



Mitigation Measures for AURORA Vulnerability

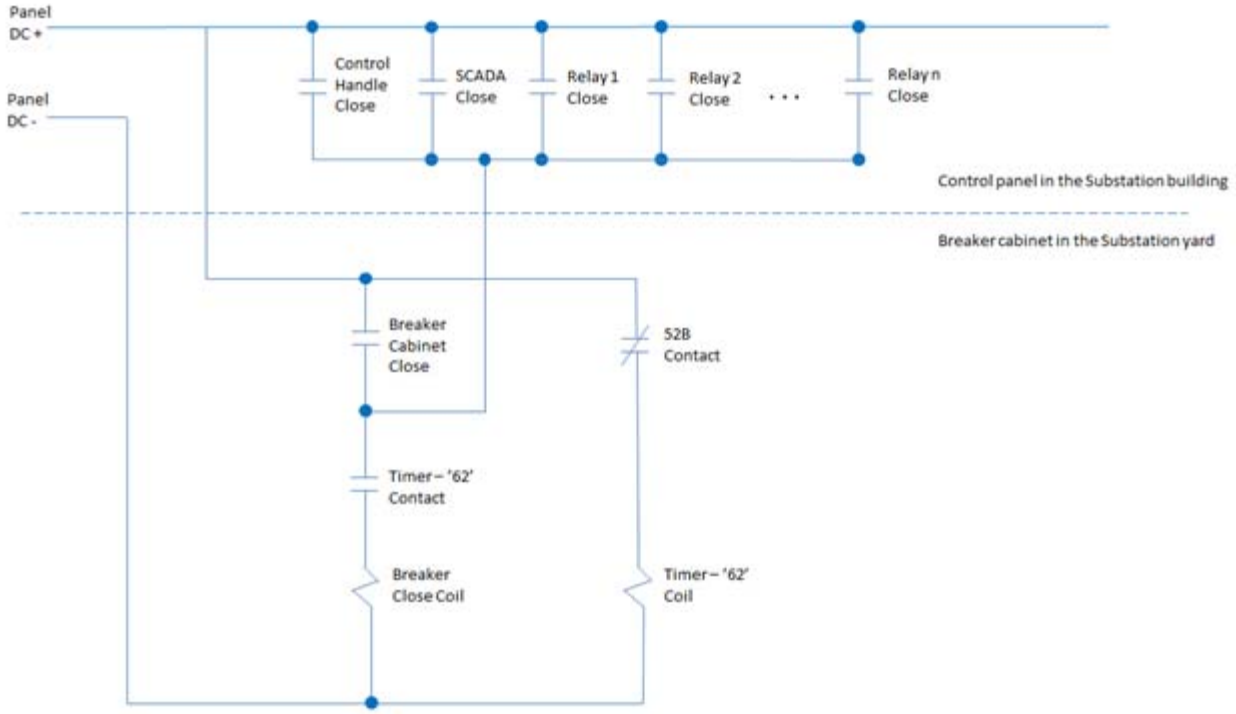
High-Speed Synch-Check

- Conclusions
  - Synch check applications with angle ≥ 10° and at least several tenths of a second delay will not permit breaker closing within the 100 msec vulnerability window for a manual breaker control switch operation when the scheme resets the synch check relay supervision following a breaker close.
  - Synch check relay delayed parting time may cause vulnerability to subsequent breaker closing via the manual control switch or other methods since the relay would not reset rapidly enough to supervise the subsequent breaker close operation.

Mitigation Measures for AURORA Vulnerability

Breaker Closing Delay

- One of the common methods to mitigate against a successful Aurora attack is to block close the breaker(s) for a specific duration after being open, manually or even automatically



- No “High-Speed” reclosing, vulnerable to hacking

Mitigation Measures for AURORA Vulnerability

Synchrophasor

- A phasor measurement unit (PMU) or Synchrophasor is a time-synchronized phasor measurement of power system voltage or current waveform magnitude and phase angle using Global Positioning System (GPS) timing
- PMUs offer the opportunity for real-time protection, control, and operation of the power system
- Synchrophasor could detect an AURORA attack on circuit breakers well into the transmission system and far away from the rotating machine
- A significant barrier to the implementation of this concept could arise from the requirement that Synchrophasor measurement data would need to be shared between generating companies, transmission and/or Independent System Operator companies.

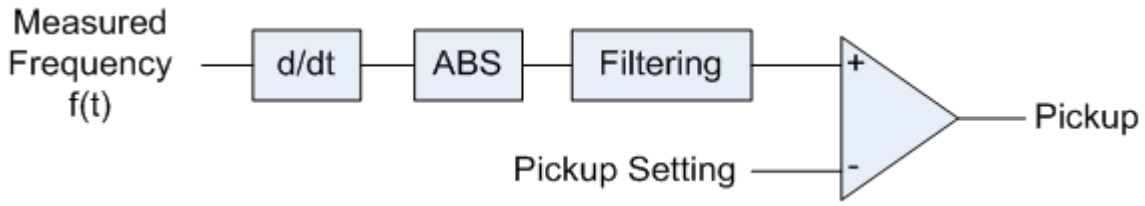
Mitigation Measures for AURORA Vulnerability

Islanding Detection via Rate of Change of Frequency

- AURORA Hardware Mitigation Devices (HMDs) which respond to rate of change of frequency (ROCOF) are available
- ROCOF can be derived from Swing Equation to arrive at…

$$\frac{df}{dt} = \frac{\Delta P f_0}{2HSn} = \frac{\Delta P(pu) f_0}{2H}$$

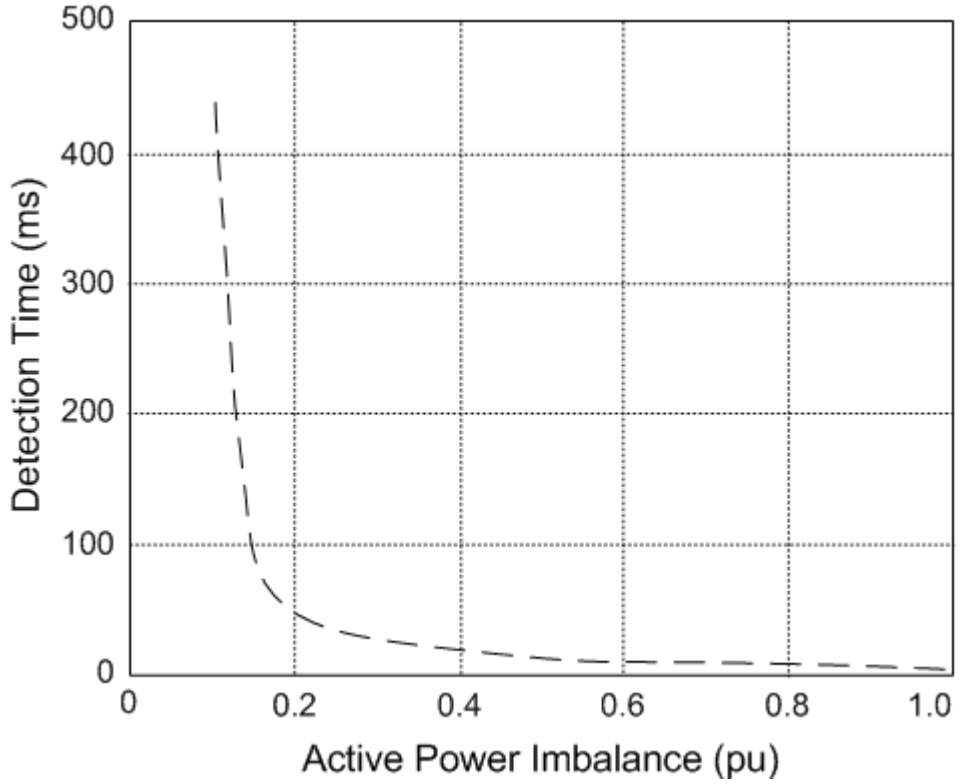
- Thus the initial rate of change of frequency can be calculated if power mismatch and inertia constant are known
- Generic ROCOF



Mitigation Measures for AURORA Vulnerability

Islanding Detection via Rate of Change of Frequency

- Simulation results for a generic ROCOF function taken from a comparative study of HMDs: Sensitivity ∝ Imbalance



Mitigation Measures for AURORA Vulnerability

Islanding Detection via Rate of Change of Frequency

- To improve security, the ROCOF element is often supervised by an undervoltage element and/or overcurrent element
- Detailed study involving ROCOF HMDs found none were able to detect 100% of the simulated Aurora events
- Generally, all HMDs become ineffective as the output power of the generator approaches zero
- One manufacturer incorporates ROCOF and overspeed in the Turbine Control to trip on Remote Open Breaker

Mitigation Measures for AURORA Vulnerability

Islanding Detection via TSR

- A turbine-generator shaft torsional relay (TSR) is a commercially available product that while not specifically designed as an Aurora mitigation device, could serve that purpose
- The TSR is a digital protective relay designed to continuously monitor turbine-generator shafts for torsional oscillations and provide trip output contacts when shaft fatigue reaches predetermined levels
- These relays have traditionally been used where subsynchronous resonance (SSR) due to series capacitors in transmission lines or torsional interaction with HVDC converters has been a concern

Mitigation Measures for AURORA Vulnerability

Conclusions

- Aurora vulnerability window understood to be up to 100 milliseconds
- Generators with stiffness ratios of 1-2 are less likely to be vulnerable to unwanted closing and reclosing of breakers during steady state conditions. Phase angle biggest concern
- Most synch check relay applications will prevent breaker closing within the 100 millisecond vulnerability window . EM may be vulnerable
- Block close supervision timers may be used to defend against unwanted breaker reclosing
- Synchrophasors could be an effective mitigation technique
- ROCOF schemes are effective when power imbalance is high but have security issues
- A combination of techniques would be most effective to preventing an Aurora attack