GE Digital Energy
Multilin

Technical Note

Aurora Vulnerability Mitigation Techniques using UR Technology

GE Publication Number: GET-20039

1. Introduction

The US Department of Energy's Idaho laboratory had conducted "a simulation attack" called "Aurora Generator Test" in March 2007. A 3.8 MVA diesel generator was damaged after multiple open/close breaker operations without a synchronism-check element (25). It was assumed that the synchronism-check control element was hacked by cyber or physical attackers to defeat its purpose. As such, Aurora vulnerability is defined as "the intentional open and close operation (during out-of-synchronism) of a circuit breaker in the vicinity of a generator by hacking synchronism-check element (25)" [1].

Typical generator protection functions are very reliable and secure for generator and power system faults [2]. Generator protection engineering already incorporates synchronism-check element (25), which ensures synchronism between a generator and the power system. However, it was demonstrated that by hacking and disabling the sync-check function in generator relays and conducting several successful Aurora attacks may have detrimental effect on life of a generator/turbine shaft.

One of the solutions provided in the literature is to use islanding detection logic of the generator protection relay to mitigate Aurora vulnerability. Therefore, this technical document provides analysis of the islanding detection logic for Aurora vulnerability as simulated on a Real Time Digital Simulator (RTDS). The limitations of the islanding detection logic to completely address Aurora vulnerability are discussed. Finally, a solution to mitigate Aurora vulnerability is proposed, which not only overcomes the limitations posed by the islanding detection logic, but also enhances cyber securities.

2. Aurora Vulnerability Mitigation using G60 Frequency Element

The Rate of Change of Frequency (ROCOF) element in generator protection is provided to serve two purposes: 1) Islanding protection, and 2) Load shedding [2]. It responds to df/dt, with a good accuracy and flexibility to react to both rising and declining frequencies. The FREQ RATE 1 to 4 PICKUP setting in the GE G60/G30 and other relays allows the protection engineer to set a threshold of pickup, with a trend of increasing (+df/dt), decreasing (-df/dt), or bidirectional (abs(df/dt)). Additionally, FREQ RATE 1 to 4 DELAY allows the protection engineer to set particular time delays to operate the element.

The configured relays issue a trip if the measured ROCOF value stays above the settings for a specified time. The time delay is introduced to secure the ROCOF element during system transients causing frequency changes such as unbalance between generation and load. All four ROCOF elements can be used to obtain the characteristic shown in Fig. 1 below. The figure only shows the characteristic with an increment trend (+df/dt); for a decrement trend, the characteristic will be a mirror image with respect to Y-axis, and for bidirectional, it will be combination of the increment and decrement characteristics. The Frequency Rate pickup settings range from 1 Hz/sec to 4 Hz/sec, and the intentional time delay settings reduces as frequency rate increases, e.g. 0.2 sec, 0.12 sec, 0.09 sec, and 0.04 sec.

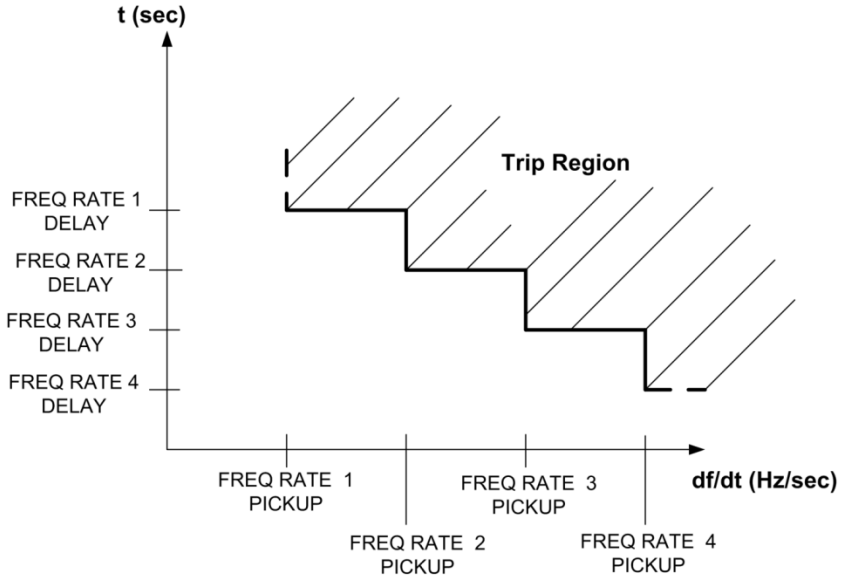

Fig. 1 consolidated characteristic using four ROCOF elements of UR G60.

This islanding detection element has been tested with a RTDS simulation of the Aurora vulnerability. A RTDS generator-turbine model is connected to a utility through circuit breakers in order to simulate the Aurora vulnerability event. Fig. 2 shows the results obtained from one of the simulated scenarios, showing quantities from the generator model, such as secondary side voltages and currents, the electrical torque (in per unit), angle difference (in degrees), frequency, and breaker operation. It can be observed from the figure that the shaft toque may exceed or reach close to the maximum limit of the machine if the breaker is operated with open/close commands within 0.25 sec of one another. The synchronism-check (25) was disabled, and open/close operations of the breaker were carried out to isolate the generator from the grid, and re-connect it without synchronization between the generator and the grid. It can be observed from the Fig. 3 that ROCOF-1 element picks-up as soon as df/dt reaches 1 Hz/sec and pickup with delay of 0.2 sec. This intentional pickup time delay prevents operation of the generator protection during load variations (which also causes rate of change of frequency). However, the intentional time delay provides a window of opportunity (between circuit breaker operation and operation of ROCOF element) for

possible Aurora vulnerability attacks. It is recommended that the operation of the ROCOF element subsequently operate a manually resettable lock-out relay on the reclose circuit of the operated breaker.

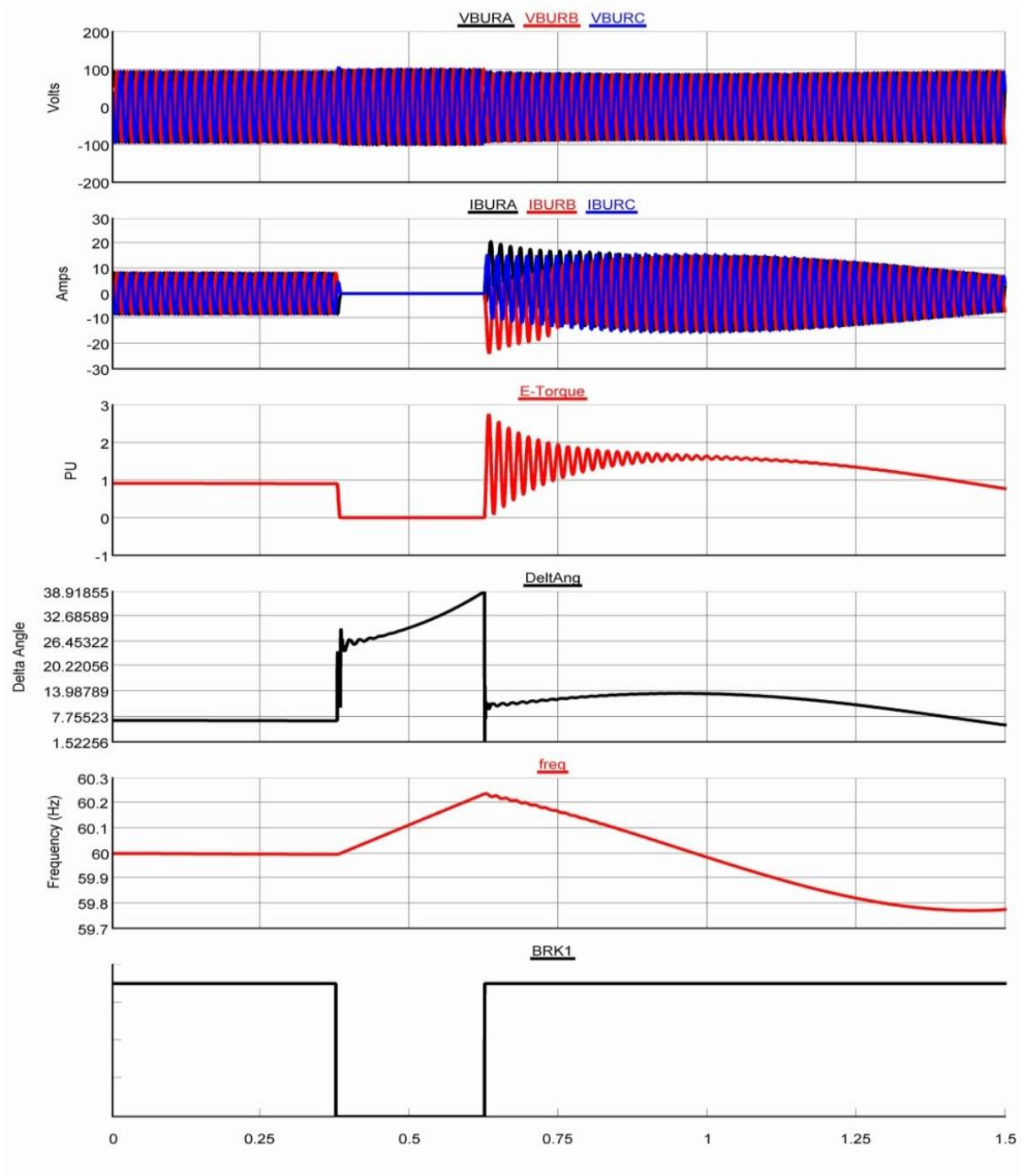

Fig. 2 RTDS simulation of Aurora vulnerability.

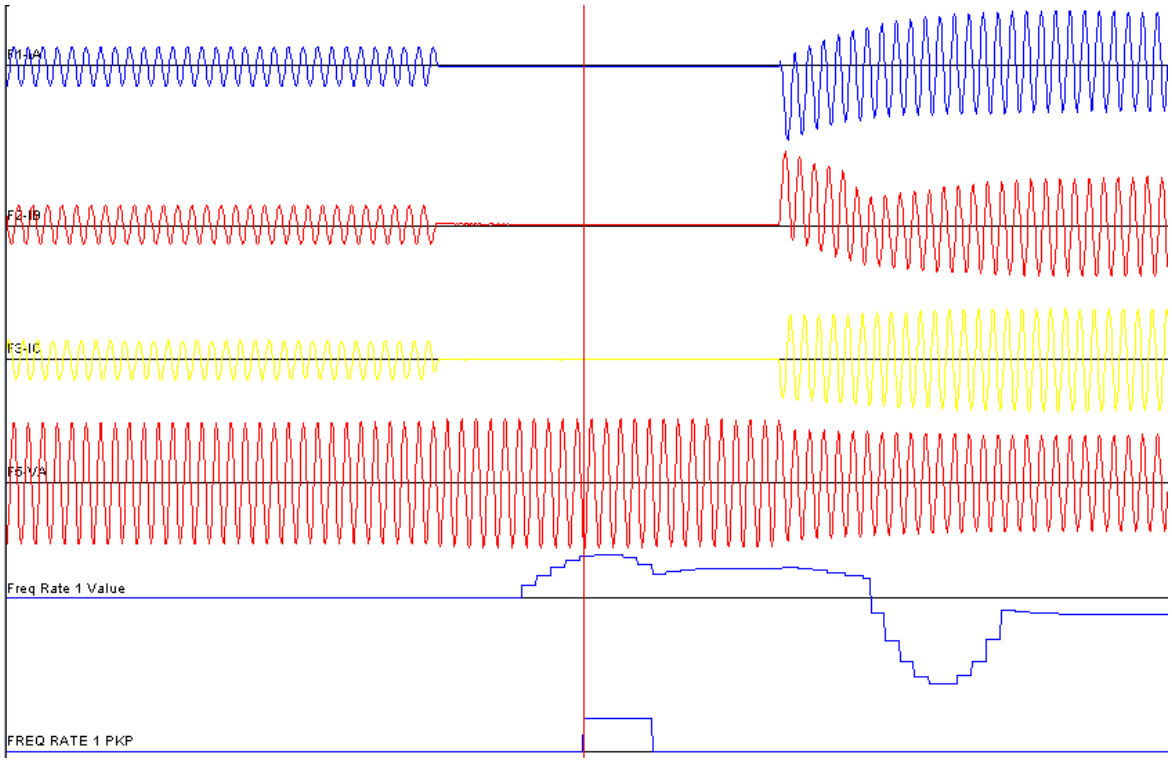

Fig. 3 Testing of ROCOF element of UR G60 during aurora vulnerability.

There are limitations of using this islanding scheme for Aurora vulnerability mitigation:

i. The intentional time delay for ROCOF elements should be set in such way that generator protection remains secure during load variation. However, the intentional time delay introduced to ride through disturbances leaves a window of possible Aurora vulnerability. By reducing this time delay, the Aurora vulnerability window can be narrowed; however, this can make generator more sensitive to the load variation. Therefore, these settings should be done according to utility practice of optimization between dependability and security of generator protection system.

ii. It was argued during Aurora Generator test conducted by Idaho laboratory that for a successful Aurora attack that the synchronism-check element of generator protection device is disabled by a cyber-attack. The argument can also be extended that cyber-attack may include hacking of ROCOF elements as well, in order to inhibit islanding operation.

Reference [2] shows that the frequency based islanding detection technique has limitations for secure prevention of the Aurora vulnerability. Clearly, the other necessary requirement is the implementation of enhanced security through the addition of user access security.

3. Aurora Vulnerability Mitigation Technique using Stand-alone Relay

The solution for Aurora vulnerability is to apply an additional UR relay for synchronism-check function (e.g. UR breaker control relay C60) with enhanced cyber security. The UR C60

provides two identical synchronism-check elements (25-1 and 25-2). The synchronism check function is intended for supervising the connection of two parts of the system which are to be joined by the closure of a circuit breaker. Synchronism-check verifies that the voltages (V1 and V2) on the two sides of the supervised circuit breaker are within set limits of magnitude, angle and frequency differences.

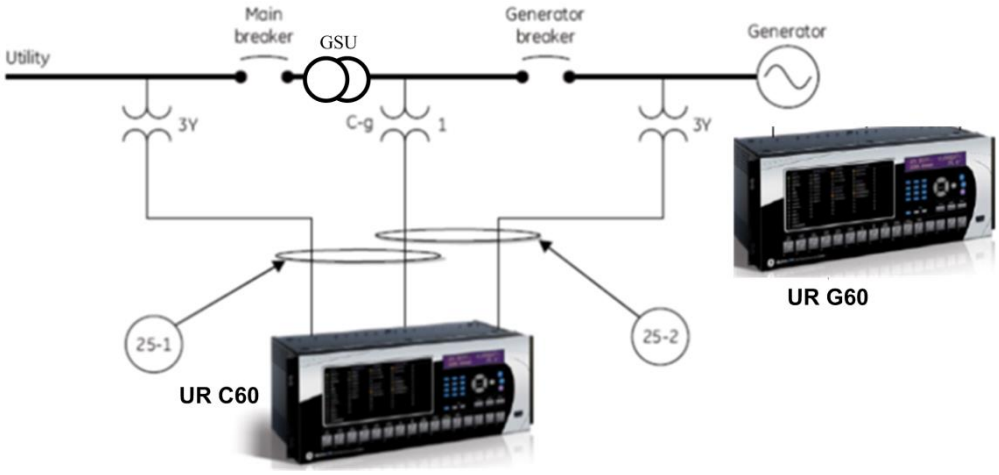

Fig. 4 Implementation of additional security with UR C60 for synchronism-check.

The recommendation for securing the GE C60 Check-sync device:

i. Do not connect to any networks (internet or intranet)
ii. Configure unique password for different access levels
iii. The UR C60 can be installed in physically isolated secured room
iv. Limit access to secured room of the UR C60
v. Implement alarms for circuit breaker operation
vi. Include a manually resettable Reclose Lockout Relay on generator breakers

Advantages of this mitigation technique over islanding detection proposed in literatures:

i. Since UR C60 is not connected to any network connection, there is no threat of a cyber-attack.
ii. Moreover, password of C60 is unique different from other relays. This provides some level of security.
iii. The Islanding detection elements of the generator protection need not be too sensitive, and therefore, there is no compromise with security of generator protection during load variations.

4. Conclusion

This document provides the analysis of the UR ROCOF frequency element (specifically, the G60) through RTDS simulation of the Aurora attack. It is presented that ROCOF element-

based islanding detection logic may only be able to prevent Aurora vulnerability from cyber-attacks if only the synchronism-check element is hacked, and other frequency elements are working normally. Moreover, the addition of a stand-along check-sync element is proposed to further mitigate Aurora vulnerability from cyber-attacks, without increasing the sensitivity of the ROCOF elements due to system disturbances.

5. References

[1]. E.E. Bernabeu, J. Holbach, F. Katiraei, and A. Yazdani, "Aurora" Vulnerability: Reliability Analysis of Hardware Mitigation Devices," proceedings of the 38th Annual Western Protective Relay Conference, Spokane, WA, October 2011.

[2]. GE Digital energy, UR G60 Instruction Manual. Available online: http://www.gedigitalenergy.com/multilin/catalog/g60.htm