Out-of-Step Protection System Testing by Means of Communication Network Emulator

Antans Sauhats, Aleksandrs Dolgicers, Andrejs Utans, Dmitrijs Antonovs, Gregory Pashnin
Riga Technical University
Faculty of Power and Electrical Engineering
Riga, Latvia
e-mails: {sauhatas@eef.rtu.lv, dolgicers@eef.rtu.lv, utan@eef.rtu.lv, dantonov@eef.rtu.lv, pashnin@gmail.com}

***Abstract*— This paper presents the testing methodology for out-of-step protection system operation validation. The protection under consideration is a wide-area measurement-based system that consists of several parts: intelligent electronic devices, GPS measurement synchronization and communication network. The entire protection system must be tested in the laboratory before installation on site. The problem is, that communication network is hardly available at the laboratory testing stage and, at the same time, the communication network is a critical part of the system, which directly influences the entire system operation. To overcome this problem, the communication network emulator was elaborated that allows to test the entire protection system in real-time and in the presence of various, potentially vulnerable conditions.**

Keywords-out-of-step regime (OOS) protection; wide-area measurement system; wide-area protection testing; communication network time delay; communication network emulator

I. INTRODUCTION

A modern power system is a very complex structure comprising a huge number of equipments. A power system is a subject to a whole range of disturbances, contingencies and equipment faults that should be eliminated as soon as possible in order to guarantee power system reliable, secure and effective operation [1]. Power system protection's functions are accomplished by means of protection and automation devices. It is possible to subdivide all types of protection and automation systems on two separate groups:

1. Local protection and automation devices, whose main task is to protect only one of the power system objects (generator, transformer, transmission line, substation buses). This type of devices uses only locally obtained measurements (voltages and currents) to accomplish the object protection task;
2. Wide-area protection and automation systems, whose task is to mitigate contingencies, which, if ignored, may lead to power system instability and blackouts. These types of protection systems use the information from several, geographically distant, power system points. High speed communication channels used for real-time information exchange between the local devices comprising the wide-area protection.

Wide-area protection structure can be presented like on Fig. 1. The protection system consists of several elements: Intelligent Electronic Devices (IED) - local devices that measures voltages and currents (U, I), pre-process measurements in vector polar or rectangular form and exchange the information by means of digital communication network [2][6]. Because the physical distance between devices may be too large, the dedicated point-to-point communication channels are not always available. In this case, the private communication network is used for data exchange where switches and multiplexers are access points to the virtual communication circuits. Virtual communication circuits define the logical connection between network clients but the actual data path is defined by the current state of the network and several paths possible for one and the same logical connection.

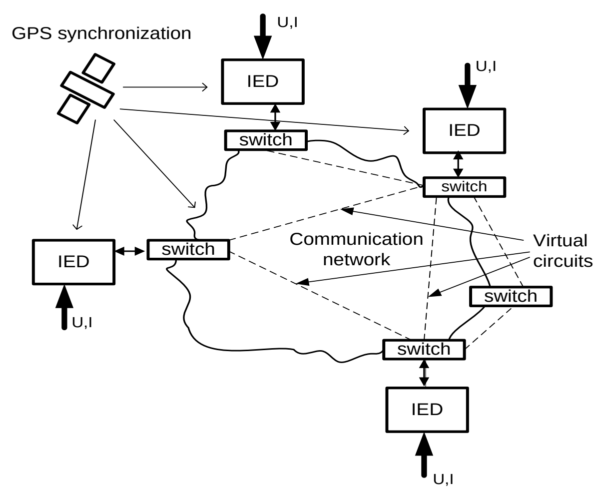


Figure 1. Wide-area protection structure.

To be able to process the measurements of such widespread system, the measurement synchronization should be accomplished. Global Positioning System (GPS) disciplined time sources are used for measurement synchronization. Each IED device receives one pulse per second (1pps) signal from substation GPS receivers [13]. Thus, all measurement are synchronized within several microseconds and supplied with appropriate time tags when transmitted through communication network. Unlike the local protection system, the reliability of wide-area protection systems is highly dependent of the performance and reliability of each element, comprising the system. To guarantee the effective and trouble-free operation of the whole system, the extensive testing should be carried out and all possible functional problems should be identified, preferably, at the system design and laboratory testing stage.

The reminder of this paper is organized as follows: Section 2 provides background information about out-of-step regime in power system and describes the out-of-step protection system structure and operation principles. The protection system operation in real-time along with the influence of the communication network time delay is analyzed in Section 3. Section 4 describes the methodology of protection system testing using a communication network emulator. Conclusion is drawn in Section 5.

II. OUT-OF-STEP REGIME IN POWER SYSTEM

A power system is always a subject to small or large disturbances and equipment faults. Local faults, such as short-circuits, are successfully mitigated by means of fast disconnection of the faulted object from the healthy grid. But regimes do exist in power system that can lead to much worse consequences than the local equipment faults because of their influence on the stable operation of the power system. Generally, this type of regimes arises as a result of power generation/load imbalance. One of such hazardous regimes is the Out-of-Step (OOS) regime. When generated power cannot be successfully delivered to the load (because of the transmission line limited capacity or short circuit) or, conversely, there is insufficient power (because of the sudden loss of generation or excessive load), then some part of the system generators start acceleration/deceleration in response to the generation/load imbalance. As a result, part of the power system operates asynchronously (loss synchronism) with the remaining part. Fig. 2 shows typical voltage and active power waveforms (effective values) in OOS regime. The situation may become even worse because of the uncontrolled load shutdown in response to the voltage deeps near the power swing electrical center. To avoid equipment damage and widespread power outages, the OOS protection should take appropriate control actions:

1. Try to restore generation/load balance of the system (add generation capabilities or remove excessive load);
2. In case the first step was unsuccessful, the power system should be split in several parts with a goal to preserve power balance within each peninsula. When the power balance within each part is achieved, the power system restoration should be accomplished by the system operator.

The OOS relaying principles are well-known and described [10][11]. At least, several electrical quantities (measured or derived) can be used for power swing detection: power, currents, impedance and impedance rate of change, power swing center voltage.

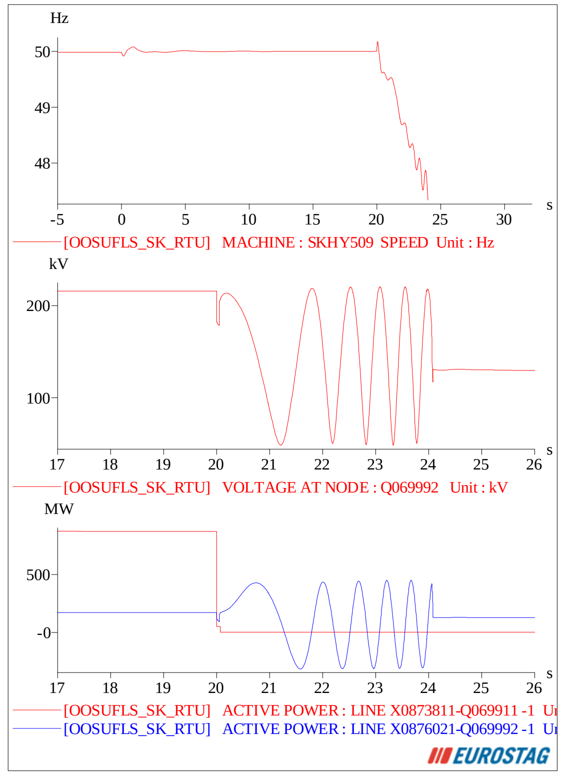
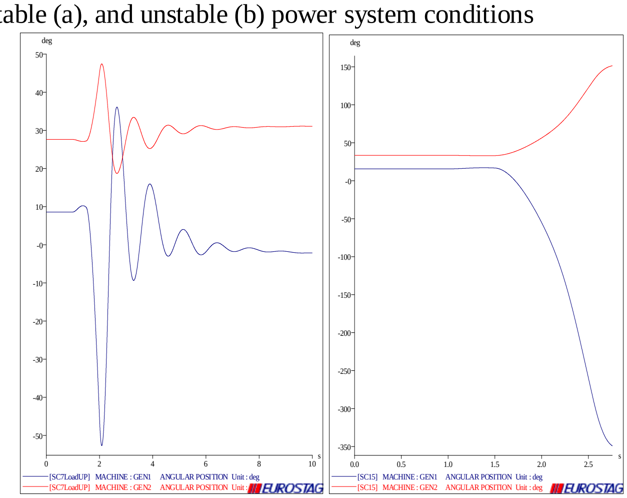


Figure 2. Out-of-step regime waveforms.

The primary reason of the OOS regime is generator (or group of generators) pole slip with respect to the rest of the system. Fig. 3 shows the generators rotors angle variation for stable (a), and unstable (b) power system conditions



(a) (b)

Figure 3. Generators rotor angle variation for stable (a) and unstable (b) power swing.

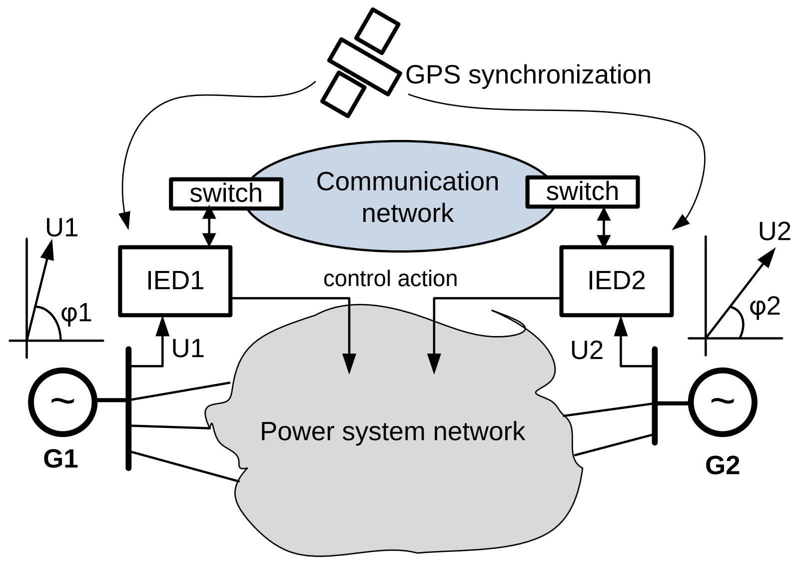


Figure 4. OOS protection system structure.

The generators electromagnetic force (EMF) vectors angle difference value can serve as an indicator of OOS regime. Direct measuring of the generators EMF vectors hardly available, but, the closest available approach is to measure the voltage phasors at the nearest (electrically) nodes. The simplified (with two generation sources G1, G2) OOS protection system structure is shown in Fig. 4. Local devices IED1 and IED2 measure the voltage phasors U1, U2, calculates the voltage phasors angles φ1, φ2 and exchange with information through the communication network. Each IED calculates the angle difference Δφ = φ1 - φ2 and recognize the OOS regime if three conditions are met:

1. The angle difference exceeds the system stability angle setting (derived from the results of power system regimes simulation):

$$\Delta\varphi > const1 \qquad (1)$$

2. The rate of change of the angle difference does not exceed the value of const2 (this condition allows to distinguish OOS regime, when voltage angle changes smoothly, from the short circuit regime, when voltage angle can change abruptly):

$$d(\Delta\varphi)/dt < const2 \qquad (2)$$

3. The negative sequence voltage does not exceed const3 setting value (this conditions allows to distinguish the OOS regime, which is three-phase balanced regime, from all others unbalanced regimes):

$$U2 < const3 \qquad (3)$$

When Δφ starts approaching to the const1 value, the OOS protection should issue the command for load shedding or launch additional generation resources. If Δφ still increases and exceeds the value of const1, then the command should be generated to split the power system in predetermined place.

III. OOS PROTECTION REAL-TIME OPERATION ISSUE

It should be noted that distributed measurements and control systems are already in use in power system utilities. The Wide-Area Measurement System (WAMS) is an example of such system [4]. WAMS structure is very similar to the one presented in Fig. 1, except that instead of IEDs, the Phasor Measurement Units (PMU) are used across the system. PMUs are placed in critical power system points [2]. Each PMU calculates line frequencies, voltage and current phasors and streams those data over the communication network, along with the associated GPS time tags. Data from PMUs are collected in power system utility dispatch center and can be used to create wide-area visibility across the power system in ways that let grid operators understand real-time conditions, see early evidence of emerging grid problems, and better diagnose, implement and evaluate remedial actions to protect power system stability [3]. Several publications [4][5][7][8] dedicated to PMU real-time application for protection and control tasks. Wide-Area Monitoring, Protection and Control systems (WAMPAC) can cope successfully with relatively slow processes like inter-area oscillations, state estimation, under frequency load shedding, power system restoration after islanding. Typical PMU provides output data at rate 10-50 samples per second (for 50 Hz system) [7]. For the proposed OOS protection system, it is mandatory to trace not only the angle value, the voltage phasor rotation should also be tracked with, at least 5 electrical degree resolution (Fig. 5). This requirement could be fulfilled with a signal sampling rate of 500-1000 samples per second (depending on the implemented algorithm), that significantly exceeds the PMU output data rate.

 ISBN: 978-1-61208-319-3

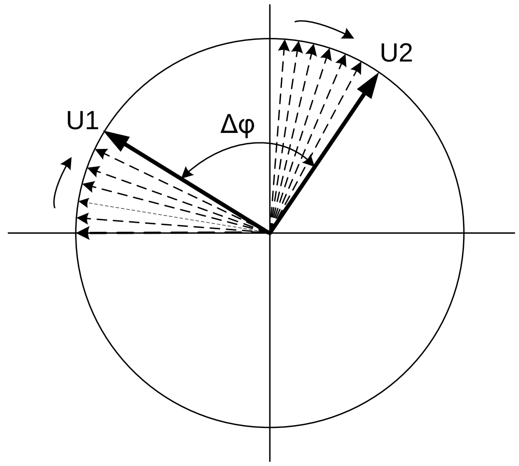


Figure 5. Voltage phasors sampling.

One more factor should be taken into account. WAMS can not be used in the absence of GPS synchronization, but OOS protection should be operable (possibly, with reduced precision) even if the GPS measurement synchronization is not available at the moment. In the absence of synchronization, the data transmission time delay, introduced by the communication network, can be calculated and taken into account before the angle between voltage phasors is calculated. The time delay calculation is based on well-known ping-pong method [12] and the result is valid only if transmitting and receiving time delays are equal (Fig. 6).

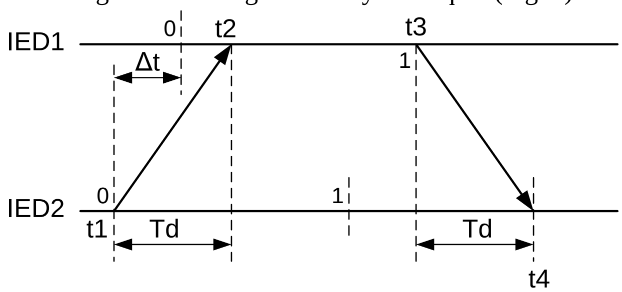


Figure 6. Time delay calculation using ping-pong method.

Then, the measurement synchronization could be achieved in assumption that time delays of the communication network are symmetrical (5). The data transmission time delay *Td* is

$$Td = (t4 - t1 - t3 + t2)/2 \tag{4}$$

Time difference Δt between IED1 and IED2 sampling instances is

$$\Delta t = Td - t2 \tag{5}$$

All time marks: t1, t2, t3 and t4 are local and devices attach these local times to the data frame when data exchange processed. Thus, devices can synchronize their measurements and are operable even without GPS synchronization. Time delay asymmetry will introduce an error in time delay calculations and this error will lead to additional angle error between voltage phasors. To mitigate this effect, IEDs automatically rearranges their settings to less sensitive. Despite the fact that the protection system will operate with lower precision, the system is still capable to detect OOS condition and take appropriate control action. The degree of device settings sensitivity should conform to two requirements:

1. Reliable operation of the protection for the majority of possible OOS regime scenarios;
2. Avoidance of false operation for all possible OOS regime scenarios.

Protection blocking was implemented to fulfill the second requirement - protection will be blocked if communication time delay exceed the maximal theoretically possible time delay for a given communication network. Then, a set of experiments should be carried out to be sure that the first requirement is also fulfilled.

IV. OOS PROTECTION SYSTEM TESTING

Any complex control system should be tested to validate the correctness of the implemented algorithms and to define the value of system operation reliability and robustness. This is especially true for protection and automation systems, whose correct and reliable operation largely determine the entire power system operation. Testing procedures for the local protections can be successfully accomplished in the laboratory, prior the device installation on site. Testing of the OOS protection system under consideration is much more complex task because not only each element of the system should be tested. Interaction of individual parts and correct operation of the entire system in the presence of various, potentially vulnerable conditions, should be checked. OOS protection system consists of three main parts: IED units, GPS synchronization system and digital communication network. It should be mentioned, that validation of the system operation on the site could be problematic because system elements are widespread geographically. Correct functioning of the system should be considered under several conditions: presence/loss of GPS synchronization, short-term unavailability of the communication channel, transmitted data integrity violation, operation of the system with different data transmission rates, communication time delay volatility and time delay asymmetry. The communication network is a critical element of the system and, at the same time, it is hardly available at the laboratory testing stage.

Testing of the considered protection system using simulation and modeling technique will not give us the valuable results because of the several reasons:

1. Inappropriate level of details/unavailability of IEDs models.
2. Communication network topology and hardware environment not always defined at the laboratory testing stage.
3. Each element of the system can be a subject to malfunction due to the hard-to-find programming errors, which can not be simulated.

 ISBN: 978-1-61208-319-3

4. Protection system under consideration is a real-time application and assumes that each element of the system should operate in real-time.

An emulator of the Digital Communication Network (CNE) was developed and produced to overcome the problems of protection system testing in real-time. In contrast with a typical communication network simulator, CNE is not hosts/data packets oriented device. Also, the device operation principle is not communication protocol-dependent. CNE emulates communication network parameters and states that can potentially affect the protection system performance and reliability. CNE is a dedicated, microprocessor based device, which internal structure and principle of operation presented in Fig. 7. The input data are sampled and stored inside the memory buffer which is organized in a manner of first-in first-out (FIFO) register. The entire contents of the FIFO memory is shifted at one position prior each next sample. The size of the memory buffer N defines the time delay Δt between data input and data output moments (6). The data transmission time delay is

$$\Delta t = N / Fclk \qquad (6)$$

Two dedicated memory buffers per communication channel were implemented to provide full duplex data exchange. To minimize the jitter effect between the input and output signals, the signal sampling frequency *Fclk* should be significantly greater than data transmission rate *Fdata* (7):

$$Fclk >> Fdata \qquad (7)$$

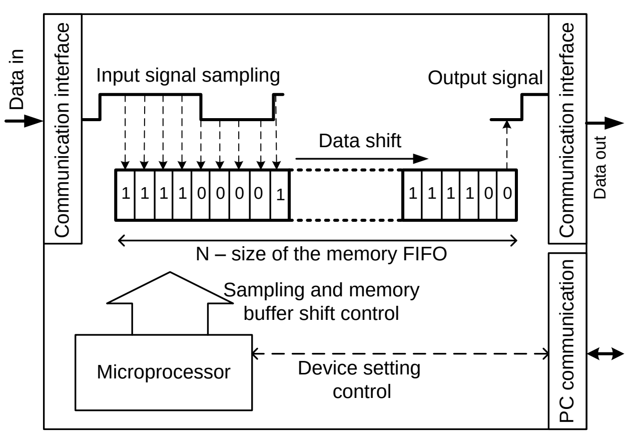


Figure 7. CNE principle of operation.

Device settings are controlled by means of PC with appropriate software. User can control the communication time delays for each communication channel and in both directions independently. One of possible features of the device is operation on a basis of predefined scenario: short-term communication interruptions, introducing random errors in transmitted data, abrupt variation of time delays.

The structure of OOS protection system testing using CNE is presented in Fig. 8. After OOS condition simulation by means of power system regimes modelling software (ATP [14], Eurostag [15], ETAP [16]), the data are uploaded into Relay Test Systems (RTS) and analogue signals can be replayed in real time. At least several tens scenarios of OOS regime should be generated to fulfil the requirement of reliable testing. Then, analogue signals (3-phase voltages) are supplied to each IED and replayed by means of RTS - Freja300.

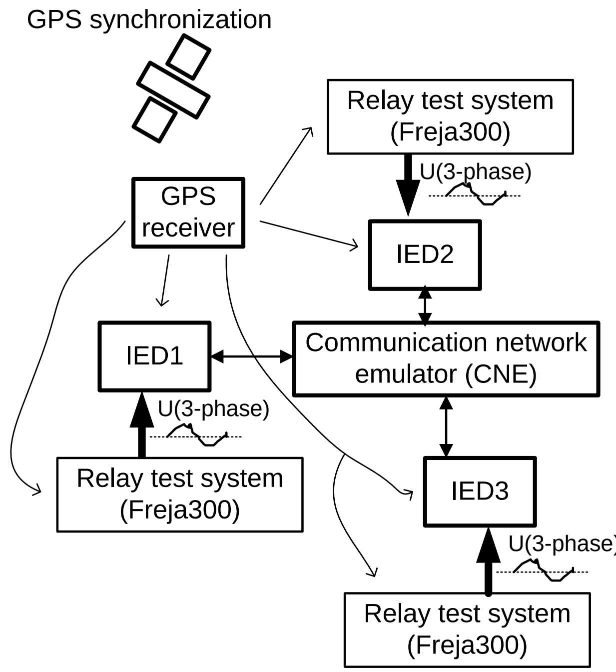


Figure 8. Laboratory testing of the OOS protection system.

IED measurements as well RTS output signals are synchronized by means of GPS receiver. Data exchange between devices is accomplished through the CNE that emulates time delays of the communication network according with predefined scenario. In Fig. 9, we can see an example of one of the experiments.

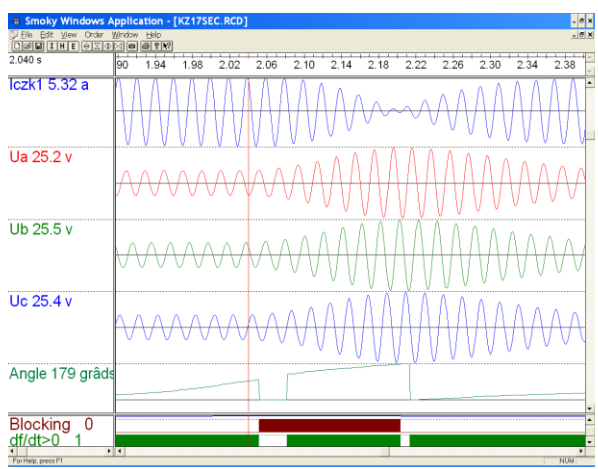


Figure 9. OOS protection system testing example.

CNE abruptly increases the time delay at time 2.05 s and change it back at 2.08 s. Protection operation blocking observable within this time interval in response to time delay variation. This testing structure allows test the whole system in real-time and in close-to-real conditions. After extensive testing, the conclusion is drawn about the validity of protection system settings as also about the entire system operation.

V. CONCLUSION

A secure and reliable operation of the power system is largely determined by correct operation of the protection relay systems. Appropriate testing of relay systems was always performed to evaluate relay reliability, conformance of the settings as also to validate various algorithmic issues, implemented in relays. Relay testing methodology significantly changes with an introduction of wide-area measurements and wide-area protection systems, because several additional components can influence the entire protection system reliability. The GPS measurement synchronization and communication networks now become the critical links and protection system should be tested for several, potentially vulnerable, conditions. Typically, communication network is hardly available to perform the wide-area protection system testing in laboratory. At the same time, it is possible to define communication network parameters, which directly influence the protection system reliability. The communication network emulator was developed and created to provide the OOS protection system testing in the laboratory.

REFERENCES

[1] P. J. Moore, "Power system – Protection," London: The Institution of Electrical Egineers, 1995.

[2] A. G. Phadke, "Synchronized phasor measurements in power systems," IEEE Computer Applications in Power, vol. 6, pp. 10 –15, April 1993.

[3] A. G. Phadke, J. S. Thorp, and K. J. Karimi, "State estimation with phasor measurements," IEEE Transactions on Power Systems, vol. 1, February 1986, pp. 233-238.

[4] NERC (North American Reliability Corporation), "Real-time application of synchrophasors for improving reliability", www.nerc.com/docs/oc/rapirtf/RAPIR%20final%20101710.pdf. [retrieved: December 2013].

[5] E. O. Schweitzer, A. Guzmán, H. J. Altuve, and D. A. Tziouvaras, "Real-time synchrophasor applications for Wide-Area Protection, Control, and Monitoring," http://www.google.lv/url?q=https://www.selinc.com/WorkArea/DownloadAsset.aspx%3Fid%3D6388&sa=U&ei=HomlUoi2E6bNygPN84CwDQ&ved=0CCAQFjAA&usg=AFQjCNFk6xRLyW-FRX9aNB4GfDv4mhvDiw [retrieved: December 2013]. "

[6] J. Bertsch, C. Carnal, D. Karlson, J. McDaniel, and Khoi Vu, "Wide-area protection and power system utilization," Proceedings of the IEEE, vol. 93, Issue 5, May 2005, pp. 997-1003.

[7] B. Singh, N. K. Sharma , A. N. Tiwari , K. S. Verma, and S. N. Singh, "Applications of phasor measurement units (PMUs) in electric power system networks incorporated with FACTS controllers," International Journal of Engineering, Science and Technology, vol. 3, no. 3, 2011, pp. 64-82.

[8] B. Bhargava and A. Salazar, "Use of synchronized phasor measurement system for monitoring power system stability and system dynamics in real-time," IEEE Power and Energy Society General Meeting - Conversion and Delivery of Electrical Energy in the 21st Century, July 2008, pp. 1-8.

[9] M. Begovic, D. Novosel, D. Karlsson, C. Henville, and G. Michel, "Wide-area protection and emergency control," Proceedings of the IEEE, vol. 93, no. 5, May 2005, pp. 876-891.

[10] Power Swing and Out-of-Step considerations on transmission lines, IEEE PSRC WG D6, http://www.pes-psrc.org/Reports/Power%20Swing%20and%20OOS%20Considerations%20on%20Transmission%20Lines%20F..pdf, [retrieved: December 2013].

[11] D. A. Tziouvaras and D. Hou "Out-of-Step protection fundamentals and advancements," Schweitzer Engineering laboratories, Inc. Vacaville, CA USA Daqing Hou Schweitzer Engineering Laboratories, Inc. Boise, ID USA.

[12] M. G. Adamiak, Dr. W. Premerlani, and G. E. Alexander, "A new approach to current differential protection for transmission lines," GE Corporate GE Power Management Research and Development Malvern, PA Schenectady, NY, Protective Relaying Committee Meeting October 22-23, 1998 Portsmouth, NH.

[13] White paper – data communication in substation automation system, WP-1004HE – Part4, Time synchronization in substation automation, http://belden.picturepark.com/Website/Download.aspx?DownloadToken=c816280d-b9d5-433f-815a-da4fbc61714f&Purpose=AssetManager&mime-type=application/pdf, [retrieved: December 2013].

[14] Alternative Transient Program, http://www.emtp.org/, [retrieved: December 2013].

[15] Eurostag, http://www.eurostag.be/, [retrieved: December 2013].

[16] ETAP, http://etap.com/index.htm, [retrieved: December 2013].