ASSESSING THE RELIABILITY OF ADAPTIVE POWER SYSTEM PROTECTION SCHEMES

Adrianti*, I. Abdulhadi*, A. Dyśko*, G. Burt*

*University of Strathclyde, UK, adrianti@strath.ac.uk

Keywords: adaptive protection scheme, reliability, failure modes, Bayesian networks.

Abstract

Adaptive power system protection can be used to improve the performance of existing protection schemes under certain network conditions. However, their deployment in the field is impeded by their perceived inferior reliability compared to existing protection arrangements. Moreover, their validation can be problematic due to the perceived high likelihood of the occurrence of failure modes or incorrect setting selection with variable network conditions. Reliability (including risk assessment) is one of the decisive measures that can be used in the process of verifying adaptive protection scheme performance. This paper proposes a generic methodology for assessing the reliability of adaptive protection. The method involves the identification of initiating events and scenarios that lead to protection failures and quantification of the probability of the occurrence of each failure. A numerical example of the methodology for an adaptive distance protection scheme is provided.

1 Introduction

New generation technologies and operational practices are being introduced to electrical power system to alleviate system capacity constraints, and facilitate the integration of greener energy sources. These changes, however, can result in performance issues with existing protection systems.

Increased penetration of distributed generation (DG) for example, can result in failure to detect faults as well as miss-coordination between distribution line protection functions (overcurrent relays, recloser and fuses) [1, 2]. FACTS devices adjust transmission line parameters to control power flow or improve system stability. These can have an effect on the reach of distance protection or can cause malfunction in directional elements [3, 4].

Adaptive protection can offer an effective solution to some of the performance shortfalls experienced by existing protection schemes. Adaptive protection has been discussed widely in technical literature, such as in [5-7], but has not been commonly implemented in practice due to concerns related to the validity of the adaptive scheme operation.

In this paper, a generic methodology for reliability assessment of adaptive protection schemes is proposed as part of the risk assessment process. The method involves the identification of initiating events and scenarios that lead to protection failures and the quantification of the probability of occurrence of each failure [8]. Two stages are involved in the identification of the protection failure modes: Failure mode and effect analysis (FMEA) and Hazard and operability studies (HAZOP). FMEA identifies failure modes of each component of the system and evaluates the severity of the failure modes to the systems. Meanwhile HAZOP identifies hazards which may arise within the system but are not caused by the component failures. For the quantification of the probability of the occurrence of hazards, a Bayesian Networks technique is used. Bayesian Networks is a powerful method used in probability calculations which provides flexibility in modelling of complex systems.

To illustrate the proposed methodology, a case study is presented which assesses the reliability of an adaptive distance protection when applied to transmission lines with quadrature booster transformers.

2 Adaptive protection

Adaptive protection is defined in IEEE std C37.113 as ‘a protection philosophy that permits, and seeks to make adjustments automatically, in various protection functions to make them more attuned to prevailing power conditions’[9]. From the definition, there are three main functions that the adaptive protection must perform:

a. Monitor changes in the power system conditions and determine the system state;
b. Find optimal protection settings, characteristics or logic accordingly;
c. Modify the protection settings, characteristics or logic automatically.

The modifications include pick up thresholds, reach settings and operate/restrain characteristics. Settings can be automatically calculated based on network parameters, such as in [6], or by using look-up tables with several pre-determined setting groups [5, 10].

Changes from one setting to another are not instantaneous; there is always a time delay. If a fault occurs during the time of changeover, the protection is assumed to work incorrectly. Therefore, in order to reduce this risk, the time delay should be as small as possible. The number of setting groups is usually related to the expected variation of power system condition. More setting groups can provide better protection scheme coverage and potentially improved performance. However, this also means that the setting changes take place

more often. This can result in an increased risk of incorrect operation.

3 Failure modes of adaptive protection

Operational modes of adaptive protection can be classified into three categories:

a. Desirable operation;
b. Failure to operate;
c. Unwanted operation.

A desirable operation is when the protection operates for faults in its protected area and does not operate when there is no fault in its protected area. The probability of hidden failures i.e. protection failures during normal system conditions, is assumed to be negligible. This is because components such as relays, circuit breakers, CTs, VTs, dc power sources are equipped with self-testing/supervision functionality. Therefore, this type of failures is not included in the calculations presented in this paper.

Failure to operate is a condition when the protection fails to operate for faults in its protected area whereas unwanted operation is a condition when the protection operates when there is no fault in its protected area. These two failure modes are considered in this assessment.

Failure to operate of a protection system can be caused by:

a. Protection components failures, such as relay hardware failure, circuit breaker being stuck and dc supply failure;
b. Special conditions where the protection cannot see the fault, such as high resistive faults.

Unwanted operation modes are initiated by:

a. Protection components' unwanted operation, such as unwanted operation of breaker;
b. Spurious tripping of a relay for an external fault.

Alongside the sources of failure in conventional protection, adaptive features can introduce additional sources of failure. The following is a brief list of them:

a. Primary system event detection
   Sensing the primary system changes is an essential task of the adaptive function. Therefore sensors and detection methods must be reliable. The sensing equipment may suffer some failures and detection methods may provide false information. Thus the impact on the protection performance must be assessed. If sensing equipment is placed remotely from the rest of the adaptive protection functions, then some form of communication is needed. Consequently, their reliability should also be assessed.

b. Adaptive setting selection
   Based on primary system condition, the adaptive functions select or calculate the settings for the relay accordingly. This adaptive calculation or selection may also suffer from the failures. These are mainly caused by hardware failure, software failure or inadequate adaptive scheme design. For assessment of software failure, software reliability engineering methods can be applied, such as in [11].

c. Fault coverage of each setting
   For each setting, the probability of failure to operate and the probability of unwanted operation needs to be assessed.

d. Default settings
   A default setting must be fixed in case of the adaptive function failure. Therefore it's probability of failure to operate and unwanted operation is also need to be assessed for each primary system condition.

4 Methodology for the assessment of adaptive protection reliability

Based on well-known methods for risk assessment [8, 12], a generic method for adaptive protection reliability assessment is proposed. The method is specifically tailored to deal with the issues of adaptive power system protection. The methodology for the adaptive protection reliability assessment is described in the following sections.

4.1 Collection of system information

Information about the protection system and the protected primary system is collected. This includes physical components and their function, layout or interconnection of the components, operating logic, successful operation criteria, embedded software and system operating conditions.

4.2 Identification of initiating events for the protection failure modes

Initiating events of each failure mode can be found using Failure Mode and Effects Analysis (FMEA) and Hazard and Operability (HAZOP) studies [8]. FMEA starts with a list of adaptive protection components and then identifies their failure modes. The effects of these failure modes are then investigated further to obtain their impact on the system.

The FMEA cannot provide all failure modes within the system, because not all of the system failure modes are caused by component failures. For this reason HAZOP is applied. HAZOP identifies initiating events of the system failures which are not caused by components failures. Lists of sources of protection system failures in section 3 can be used to generate the failure modes of the system.

4.3 Quantification the occurrence of each failure

In order to calculate the probability of an occurrence of each failure mode, some well-known methods can be applied such as Fault tree analysis, Markov chains and Bayesian Network. However, Bayesian network method is recommended since it provides flexibility in modelling and simplicity in data requirement [13, 14].

Modelling the reliability problem using Bayesian Network starts with a qualitative part, a directed acyclic graph (DAG). This represents failure modes of the protection in relation to their causes (initiating events). To construct the DAG, network variables (nodes) need to be defined based on the

available data. There are three types of variables: query variables (for which the probability must be calculated), prior variables (input data) and intermediary variables (these model the relation between prior and query variables). The next step is to define the network structure (edges) of the DAG which shows a causal relationship between variables.

After the DAG is constructed, the qualitative part needs to be performed which defines Conditional Probability Tables (CPTs) for each edge. The CPT shows probability of a state occurring for each given cause. Finally, the calculation of the query variable is performed automatically using Bayesian Network software. An example DAG and its CPT is shown in section 5.3.The construction of a DAG for each failure mode can be done separately before being integrated for the whole system.

5 Case study: Adaptive distance protection

The prototype adaptive distance protection scheme proposed in [3, 10], is used to provide a numerical example of the adaptive protection reliability assessment. It is designed to overcome distance protection under-reach problems caused by the presence of a quadrature booster transformer (QBT) in the transmission system. QBT is widely used to control active power flow in the transmission line. The following sections present the application of the proposed methodology for the case study reliability assessment.

5.1. Collection of system information

The primary system consist of two identical lines, with substation B in between as shown in Figure 1 [3]. The QBT is placed at substation B, and the adaptive protection is located at the beginning of transmission line AB (R1). Transmission and protection data are given in the Appendix.

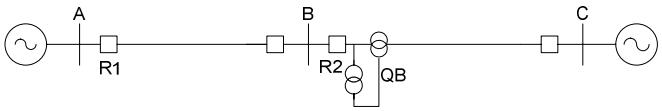

Figure 1: Transmission line with a QBT and an adaptive distance protection at R1 [3]

The boost and buck operation of the QBT results in zone 2 protection under-reach if conventional distance protection is installed at R1 as reported in [3]. Therefore, an adaptive distance protection is installed at R1 to compensate for the under-reach according the QBT operational states. The adaptive distance protection scheme has two pre-determined setting groups, setting group 1 (SG1) is used when the QBT is in the bypass state and SG2 for boost or buck states. The difference between the two setting groups is only in the zone 2 reach setting (refer to the Appendix). At R2, a non-adaptive conventional distance protection is installed, because there is no effect of the QBT on the performance of this protection. The QBT has 20 taps for boost and 20 taps for buck mode of operation, and each tap position results in a different level of protection under-reach which also depends on the type of fault in the line. To quantify this impact and verify the protection operation the scheme was simulated using Real Time Digital Simulator (RTDS) [15].

The operating logic of the adaptive scheme is shown in Figure 2. The QBT operation states are controlled using a set of switches, which enables bypass or buck-boost operation. The QBT state information is obtained from the switches' status indications. The QBT state information is sent to the adaptive protection controller (ABB COM600 substation gateway) through a communication network. This information is used to select a relay setting group from the setting group pool. Once the setting group has been chosen, then it is sent to the distance relay to be activated.

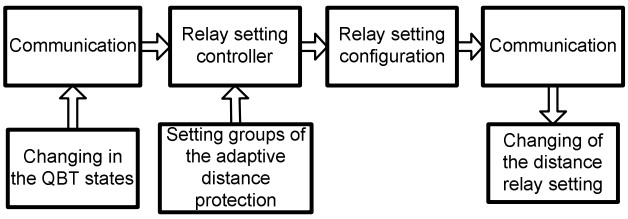

Figure 2: The operating logic of the adaptive distance protection.

5.2 Identification of the initiating events of the protection failure modes

The initiating events of the protection failure modes are identified using FMEA and HAZOP techniques. The failure modes and their initiating events are summarized as follows:

a. For failures to operate the initial causes are:

For zone 1
- Protection component failures.

For zone 2 (if primary protection fails)
- Protection component failure;
- Adaptive function failure;
- QBT operational states indication failure
- Faults occurring during the time of setting switchover from SG1 to SG2 (causing protection under reach).
- Zone 2 protection under-reach for phase-to-phase faults when SG2 is applied as shown in Table 1.

QBT state	Tap	Non detected L-L faults starting at (% of line AB)
Boost	20	148
Buck	11	148
Buck	12	147
Buck	13	145
Buck	14	143
Buck	15	140
Buck	16	136
Buck	17	134
Buck	18	130
Buck	19	126
Buck	20	122

Table 1: Zone 2 reaches when SG2 is applied to relay R1.

b. For spurious tripping, the initial cause is:

- unwanted operation of protection components

5.3. Quantification the occurrence of each failure

The reliability assessment for failure to operate is only conducted on zone 2 of the distance scheme since there is no requirement to adaptively alter zone 1 reach. A fault tree illustration for this failure mode is shown in Figure 3. The fault tree shows that the scheme will fail to clear a fault in zone 2 when both primary protection and the distance protection fail. The adaptive protection can fail to operate because one of these causes: the protection component failure, the adaptive function fails, under-reach during SG2, under-reach during switchover from SG1 to SG2 or the QBT state indicator failure. However, in this paper, only the 'under-reach during switchover from SG1 to SG2' cause is described in detail.

.

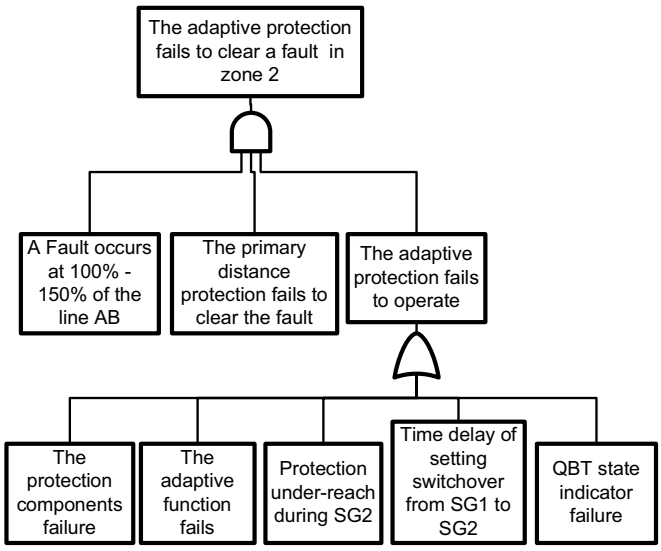

Figure 3: Fault tree illustration for zone 2 operation failures

The Bayesian Network's DAG of the fault tree in Figure 3 is shown in figure 4. The probability calculation of the DAG was carried out using the GeNIe software from the University of Pittsburgh [16].

The protection components' failure probabilities are based on statistical data or generic data from [17-21]. The components include: CT, CVT, numerical distance relay, circuit breaker, dc source, wiring and telecommunication.

The factor influencing the probability of the protection under-reach due the time delay during the setting switchover from SG1 to SG2 is shown in Figure 5. The Probability is determined by the length of time required for the switchover operation, type of fault occurring in the protected line and the QBT state during switchover. Table 2 shows probability of switchover taking place, which is prior data to the 'settings switchover' node. The state 'switchover' represents the probability of the adaptive protection in transition of switchover from SG1 to SG2. The probability is obtained from total number of switchover multiplied by a switchover duration, then divided by the total operation times of the adaptive protection. Tables 3 and 4 show prior probability of node 'type of fault' and 'QBT states' respectively. Data of the QBT node and settings switchover node are estimated under assumed the QBT operational scenario.

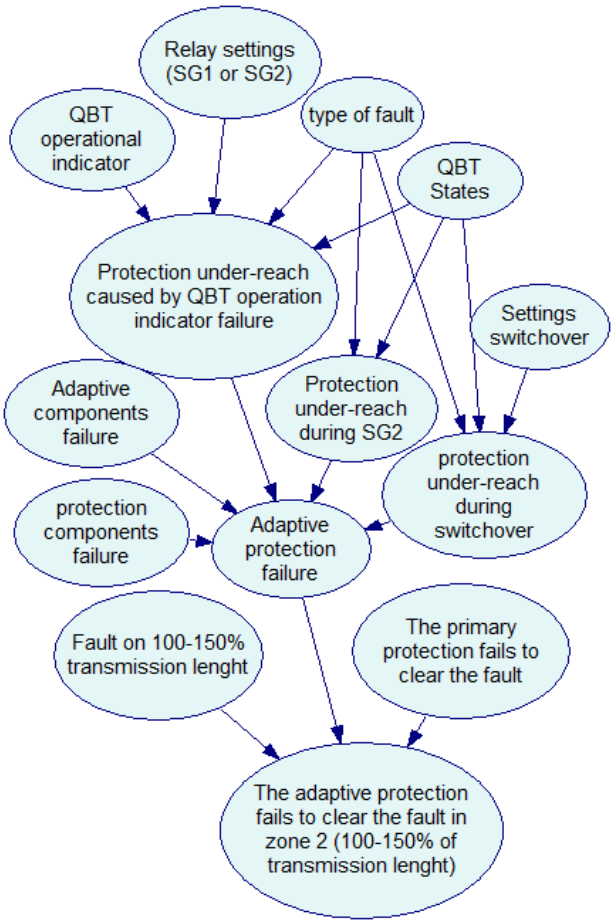

Figure 4: Bayesian Network model for the adaptive distance protection

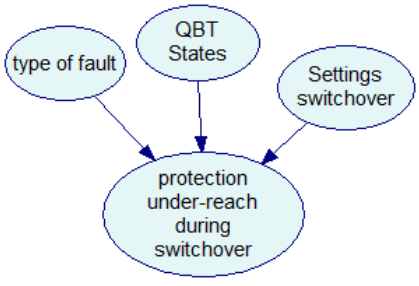

Figure 5. DAG for protection under-reach during switchover

switchover	0.0002261767
Not switchover	0.9997738233

Table 2: Prior probability of 'Settings switchover' node

L-G	L-L	L-L-L-G
0.78	0.15	0.07

Table 3: Prior probability of 'type of fault' node

Bypass	0.2
Boost Tap 1 – Tap 20, probability for each tap	0.3
Buck Tap 1 – Tap 20, probability for each tap	0.1

Table 4: Prior probability of 'QBT states' node

The 'protection under-reach during switchover' node contains a conditional probability table (CPT) as shown in Table 5. This table only shows some parts of the CPT due to space limitations. The CPT contains all combinations of states from the 'QBT states', 'type of fault' and 'settings switchover' nodes. The data is obtained from the RTDS simulation.

Setting switchover	Switchover					
Type of fault	LL					
QBT States	Boost19	Boost20	Buck1	Buck2	Buck3	Buck4
Relay sees the fault	0.5	0.48	0.78	0.76	0.74	0.7
Relay cannot see the fault	0.5	0.52	0.22	0.24	0.26	0.3

Table 5: Conditional Probability Table of 'protection under-reach during switchover' node

QBT operational state information is obtained from the bypass switches. If the switch indications fail to provide its state, then the adaptive protection may select an incorrect setting group. The Bayesian Network model for this issue is shown in Figure 4 (protection under-reach caused by QBT operational indicator failure node). The variables input for this under-reach node are: the QBT operation indicator failure probability, relay settings (SG1 or SG2) probability, fault types probability and the QBT states probability. The failure probability of the QBT operational indicator is based on switch indicator failure data from [18, 21], while the SG1 and SG2 probability is estimated under assumed the QBT operational scenario.

In order to provide the security of protection, zone 2 of SG2 has to compromise its dependability. Therefore, there are small parts of the line faults which cannot be seen by the relay zone 2 comparator. The probability of this protection under-reach with SG2 applied is calculated using Bayesian networks as shown in Figure 4 (protection under-reach during SG2 node). This effect is influenced by the type of fault and the state of QBT during the fault. The probability values of the protection under-reach during phase-to-phase fault according to QBT state are shown in Table 6. The results are based on the RTDS simulation of the fault and protection response.

Table 6 only shows the QBT states having a non-zero probability of protection under-reach. Other states having zero probability have been omitted. The quantities in the table are calculated based on data in Table 1 using (1):

$$\text{Under-reach probability} = \frac{L_{fault}}{L_{total}} \quad (1)$$

where:

L_{fault} = length of line where undetected faults take place

L_{total} = total length of zone 2 reach in line BC

Unwanted operation failure mode is caused by the protection component spurious tripping when no fault occurs. The DAG for this failure mode is not shown here because of space limitation, but the calculation result is given in section 5.4.

QB State	Protection see faults	Protection Blinding
Boost20	0.96	0.04
Buck 11	0.96	0.04
Buck 12	0.94	0.06
Buck 13	0.9	0.1
Buck 14	0.86	0.14
Buck 15	0.8	0.2
Buck 16	0.72	0.28
Buck 17	0.68	0.32
Buck 18	0.6	0.4
Buck 19	0.52	0.48
Buck 20	0.44	0.56

Table 6: Probability of protection not being able to see a phase-to-phase fault at different QBT states.

5.4 Results

The probability calculation result of the adaptive distance protection is shown in Table 7. For comparison purposes, the reliability calculation for a conventional distance protection in transmission lines without a QBT is also shown in this table. The adaptive protection has a slightly higher probability of zone operation failure compared to conventional schemes. The probability of unwanted operation is very similar.

Distance Protection	Protection fails to clear a fault in in Z2	Unwanted operation
Adaptive	9.00972E-08	5.07951E-06
Conventional	8.90569E-08	5.07951E-06

Table 7: Probability of distance protection failure modes

According these results, the adaptive distance protection performance is as good as conventional distance performance in terms of security and dependability. The result is based on the assumed QBT operational scenario. Other operational scenarios may produce slightly different results.

6. Conclusion

A generic methodology for assessing the reliability of adaptive protection was proposed. The methodology involves collecting information of the protection system and the protected primary system then identifying all the failure

modes and their initiating events. Each failure mode and initiating event needs to be quantified using probability calculation tools. Bayesian Networks which provide flexibility in modelling and simplicity in input data requirements has been successfully applied and demonstrated in an example case study of an adaptive distance protection. The results reveal that when the adaptive protection is applied, the probability of failure to operate is only marginally higher compared to that of a conventional scheme. Moreover there is no significant difference in terms of the probability of unwanted operation.

Since detailed statistical parameters of protective equipment are rarely available, the proposed methodology is based on a simplified reliability model.

In future work, the assessment method will be refined, by including additional factors such as CT and CVT precision, transmission line parameter errors and human error. It is believed that the risk assessment using Bayesian network approach can provide valuable input to the protection scheme design process in the future.

Appendix

Transmission Line Section Length: L = 50km
Line Positive Sequence Impedance: $Z_{L1} = 13.93<86.5°\Omega$
Line Zero Sequence Impedance: $Z_{L0} = 39.3<82.7°\Omega$
QB Rating = 2000MVA
QB Tap Range ≈ ±20% of QB rating/±11° phase shift
Adaptive distance protection settings groups:
SG1: Zone1 = 80%, Zone 2 = 150%
SG2: Zone 1 = 80%, Zone2 = 180%
Relay characteristic angle: RCA = transmission line angle

References

[1] S. K. Salman and I. M. Rida, "Investigating the Impact of Embedded Generation on Relay Settings of Utilities' Electrical Feeders," *IEEE Transaction on Power Delivery,* vol. 16, pp. 246-251, 2001.

[2] F. Coffele*, et al.*, "Detailed Analysis of The Impact of Distributed Generation and Active Network Management on Network Protection System," in *CIRED 21st International Conference on Electricity Distribution*, Frankfurt, 2011.

[3] I. F. Abdulhadi*, et al.*, "The evaluation of distance protection performance in the presence of Quadrature Booster in support of a coordinated control strategy," presented at the 10th IET International Conference on Developments in Power System Protection (DPSP 2010) 2010.

[4] M. Khederzadeh and T. S. Sidhu, "Impact of TCSC on the protection of tranmission lines," *IEEE Transaction on Power Delivery,* vol. 21, pp. 80-87, 2006.

[5] P. Mahat*, et al.*, "A Simple Adaptive Overcurrent Protection of Distribution Systems With Distributed Generation," *IEEE Transactions on Smart Grid,* vol. 2, pp. 428-437, 2011.

[6] A. G. Jongepier and L. v. d. Sluis, "Adaptive Distance Protection of Double-Circuit Lines Using Artificial Neural Networks " *IEEE Transaction on Power Delivery,* vol. 12, 1997.

[7] A. A. Girgis*, et al.*, "An Adaptive Protection Scheme for Advanced Series Compensated (ASC) Transmission Lines," *IEEE Transaction on Power Delivery,* vol. 13, April 1998 1998.

[8] J. D. Andrews and T. R. Moss, *Reliability and Risk Assessment*, second ed. London: Professional Engineering Publishing, 2002.

[9] IEEE, "IEEE Guide for Protective Relay Applications to Transmission Lines," vol. IEEE Std C37.113-1999, ed. New York: IEEE, 1999, p. 107.

[10] I. Abdulhadi*, et al.*, "Adaptive Protection Architecture for Smart Grid," presented at the Innovative Smart Grid Technologies Conference Europe (ISGT Europe), Manchester, 2011.

[11] J. D. Musa, "Introduction to Software Reliability Engineering and Testing," presented at the International Symposium on Software Reliability Engineering (case Study), New Mexico, 1997.

[12] H. Kumamoto and E. J. Henley, *Probabilistic Risk Assessment for Engineers and Scientists*, second ed. New York: IEEE Press, 1996.

[13] L. Portinale and A. Bobbio, "Bayesian Networks for Dependability Analysis: an Application to Digital Control Reliability," presented at the 15th Conference on Uncertainty in Artificial Intelligence, Stockholm, 1999.

[14] M. Bouissou*, et al.*, "Assessment of a safety-critical system including software: a Bayesian belief network for evidence sources," ed. Washington: IEEE, 1999.

[15] RTDS Technologies, "RTDS Manual Set," ed, 2009.

[16] Decision System Laboratory University of Pittsburgh. (2010, 27 July). *GeNIe 2.0*. Available: http://genie.sis.pitt.edu/

[17] V. Gurevich, "Reliability of Microprocessor-Based Protective Devices Revisited," *Journalof Electrical Engineering,* vol. 60, pp. 1-6, 2009.

[18] C. R. Heising*, et al.*, "Summary of Cigre 13.06 Working Group World Wide Reliability Data and Maintenance Cost on High Voltage Circuit Breaker above 63 KV," presented at the IEEE Industrial Applications Society Annual Meeting, Denver, 1994.

[19] IEEE, "IEEE Recomended Practical for Design of Reliable Industrial and Commercial Power Systems," ed. New York: IEEE, 1997.

[20] E. O. Schweitzer*, et al.*, "Reliability Analysis of Transmission Protection Using Fault Tree Methods," presented at the Western Protective Relay Conference, 1997.

[21] G. D. Camps, "The Development of a Methodology to Determine the Maintenance Strategy for High Voltage Circuit Breakers," PhD, Electronic and Electrical Engineering, University of Strathclyde, Glasgow, 2010.