Journal of Engineering and Computer Sciences
Qassim University, Vol. 8, No. 1, pp. 63-77 (January 2015/Rabi' I 1436H)

Uncertainty Analysis of Fault-Tree Models for Power System Protection

Saleh M. Bamasak and Ali Muhammad Ali Rushdi*

Department of Electrical and Computer Engineering,

Faculty of Engineering, King Abdulaziz University,

P. O. Box 80204, Jeddah, 21589, Saudi Arabia

* *arushdi@kau.edu.sa*

(Received 14/7/2015; Accepted for publication 1/9/2015)

ABSTRACT. This paper presents an algorithm that computes the uncertainty in the availability of power system protection using fault-tree modeling. The probability of a fault-tree top event such as "Protection Fails to Clear the Fault" is evaluated in terms of the nominal value and uncertainty of each of the basic-event probabilities. The proposed algorithm starts by obtaining the fault-tree top-event expression in the switching domain (Boolean-domain) and then converting it to an availability expression in the probability domain. The algorithm then utilizes the multiaffine nature of this reliability expression in the exact assessment of its uncertainty. An example of a typical power system protection scheme is presented wherein exact numerical estimates are obtained for both the nominal value and variance of the top-event probability.

Keywords: Availability, Uncertainty, Fault trees, Power system protection, Multiaffine behavior.

1. Introduction

One of the most important design considerations in power system protection is the requirement of *protection reliability*, which can be categorized to have the two distinct aspects: protection dependability and protection security [1]. These two aspects pertain to two different types of erroneous behavior. *Protection dependability* is defined as the degree of certainty that a relay system will operate correctly when there is a fault on the system. *Protection security* relates to the degree of certainty that a relay or relay system will not operate incorrectly when there is no fault on the system [2].

Fault-Tree Analysis (FTA) is a powerful diagnosis technique and is widely used for demonstrating the root causes of undesired events in system failure [3]. FTA has been employed in power system protection reliability analysis by many researchers [4]-[11]. The analysis was focused on construction of a fault-tree for certain protection schemes, computation of unavailability or failure rate values, and calculation of top-event probability. The parameters in these models are obtained from field data, data from systems with similar functionality and even by expert guessing, and hence are bound to vary widely and suffer from considerable uncertainty.

The study of uncertainty propagation in fault-tree analysis is a classical problem in reliability engineering. This problem deals with the evaluation of uncertainty in top-event probability arising from uncertainties in basic-event probabilities [12]. This problem of uncertainty analysis has been handled in reliability engineering by either (a) following a *stochastic-fuzzy* approach in which the pertinent probabilities are treated as fuzzy variables [13], [14], or (b) using a *doubly-stochastic* approach in which the pertinent probabilities are handled as random variables [15], [16].

In this paper, the doubly-stochastic approach to estimate the uncertainty in the top event probability will be employed, taking into consideration the uncertainties in the basic event probabilities. Since the top-event probability is a *multiaffine* function of the basic event probabilities [17], it has a *finite* multivariable Taylor expansion. Therefore an *exact* formula relating the variance of the top event probability to the variances of the basic event probabilities can be obtained [15]. Numerical results are then obtained for the variances of the top-event probabilities in typical power system protection schemes.

The remainder of this paper is organized as follows. In section **II** we illustrate the utility of fault trees in the study of power system protection by citing two illustrative examples. A brief survey of the fundamental families of algorithms used in the analysis of fault trees is presented in section **III**. The uncertainty analysis of fault-tree outputs is reviewed in section **IV**, which presents analytic formulas for the mean and variance of the top-event probability when the basic-event probabilities are statistically independent. Section **V** combines the ideas and concepts of the previous sections in a unified numerical example in which a specific protection situation is fault-tree modelled, and computations are made for the top-event probability and its variance. Section **VI** concludes the paper.

The notation used in the paper is given in Table (1) below:

Table (1). List of notation.

n	number of system components relevant to fault tree.
$X_i, \bar{X}_i$	indicator variables for successful and unsuccessful operation of component *i* at time t. These are switching (Boolean) random variables; $X_i = 1$ and $\bar{X}_i = 0$ if *i* is good, and $X_i = 0$ and $\bar{X}_i = 1$ if i is failed. For statistically-noncoherent systems, each fault-tree event i is not necessarily indicated by X_i; some events may be indicated by the $\bar{X}_i$'s.
$\overline{S}$	indicator variable for the existence of the top event at time t.
T	implies the transpose of vector.
q_i	unavailability of component *i* = probability that component *i* is unsuccessful at time t; $q_i = E\{\bar{X}_i\} = \Pr\{\bar{X}_i = 1\}$.
Q	Top-event probability, also called system unavailability = probability that the system is unsuccessful at time t; $Q = E\{\bar{S}\} = \Pr\{\bar{S} = 1\}$.
$\boldsymbol{q}$	n-dimensional vector of basic-event probabilities: $\boldsymbol{q} = [q_1\ q_2 .... q_n]^T$
$\mathbf{v}_1$	Mean value of $\boldsymbol{q}$; $\mathbf{v}_1 = [\nu_{11}, \nu_{21}, ..., \nu_{n1}]^T$
ν_{ij}	central moment j of q_i; $\nu_{ij} = E\{(q_i - \nu_{i1})^j\}$, j = 2, 3, 4, …
μ_1	mean value of Q
μ_j	central moment j of Q; $\mu_j = E\{(Q - \mu_1)^j\}$, j = 2, 3, 4, …
m	median (50th percentile) of a log-normally distributed variable.
F	error factor (range factor) of a log-normally distributed variable.
λ, ξ	mean and standard deviation of the natural logarithm of a log-normally distributed variable: $\lambda = \ln m$; $\xi = \ln F/1.645$.
ν_1, ν_2	mean and standard deviation of the log-normally distributed variable: $\nu_1 = m * \exp(\xi^2/2)$; $\nu_2 = \nu_1^2 * (\exp(\xi^2) - 1)$;

2. Construction of Fault Trees

Fault-tree analysis is a top-down deductive analysis structured in terms of events (or indicator variables of events) rather than components. The perspective is on faults or failures rather than successes, since a failure is usually easier to define than a non-failure, and there may be far fewer ways in which a failure can occur than the numerous ways in which non-failure can occur [18]. The focus is usually on a significant failure or a catastrophic or undesirable event, which is referred to as the top event since it appears at the top of the fault tree. In the construction of a fault tree, logic gates are used to relate the input or basic events and the intermediate events to the top event. It should be noted that a logic gate gives a qualitative description of the causal relationship between its inputs and its output. For example, the output event of an AND gate occurs if and only if all its input events occur, while the output of an OR gate occurs if at least one of its inputs occurs. Therefore the indicator variable for the output of an AND (OR) gate is obtained simply by ANDing (ORing) the indicator variables for its inputs. Detailed studies of the construction or synthesis of fault trees are available [19], [20]. Some examples demonstrating the construction of fault trees in the power system protection area are now presented.

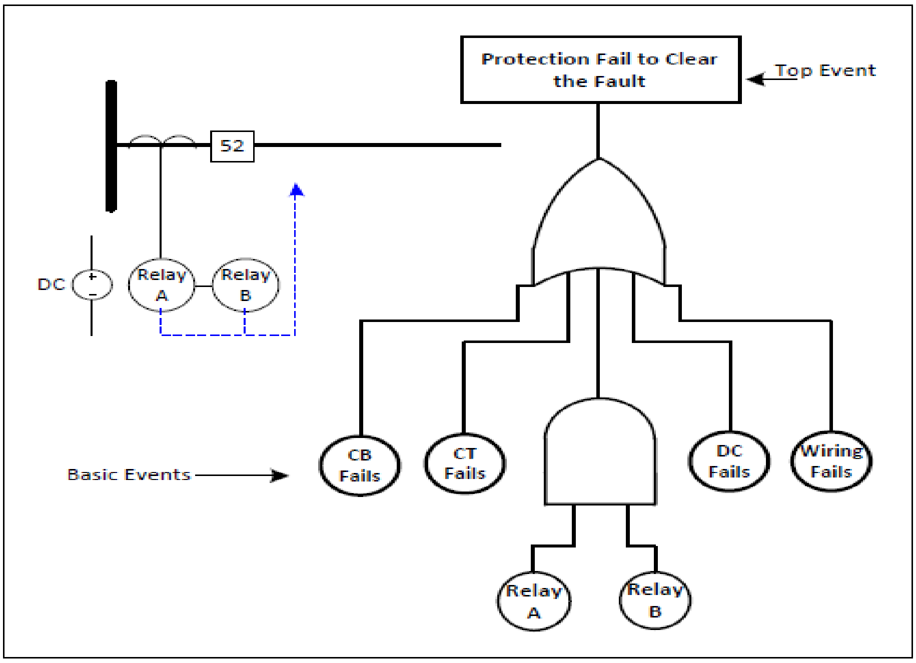

Fig. (1). Relay one-line diagram with corresponding fault-tree diagram.

The fault tree in Fig. (1) has been taken from [8] and will be analyzed further in section **V**. It describes the failure of a simple protection scheme that consists of a main relay and a backup relay (acting logically as a parallel system), a DC system, a circuit breaker, a current transformer and a wiring. The top event "Protection Fails to Clear the Fault" will occur if both relays fail at the same time or if any of the other components fail. The indicator variable for the top event and for the basic events are as follows:

$\overline{S_1}$ = Protection fails to clear the fault,

$\overline{X_1}$ = Circuit breaker fails,

$\overline{X_2}$ = Current-Transformer (CT) fails,

$\overline{X_3}$ = Battery (DC system) fails,

$\overline{X_4}$ = Wiring fails,

$\overline{X_5}$ = Relay-A fails,

$\overline{X_6}$ = Relay-B fails.

Another fault tree can be constructed by considering a total redundancy protection system in which the Relay-B in Fig.(1) is fed by a different CT and a different DC source; however, both relays trip the same circuit breaker. This fault tree is shown in Fig. (2).

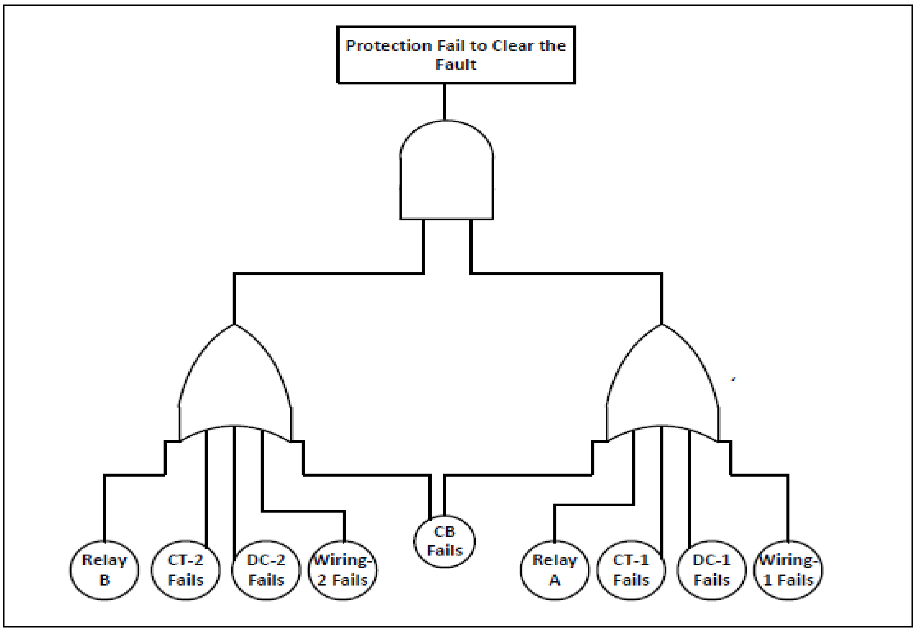

Fig. (2). Fault-tree diagram for a redundant system.

The indicator variables for the top event and for the basic events are as follows:

$\overline{S_2}$ = Protection fails to clear the fault,

$\overline{X_1}$ = Circuit breaker fails,

$\overline{X_2}$ = Current Transformer-1 fails,

$\overline{X_3}$ = Battery-1 Fails,

$\overline{X_4}$ = Wiring-1 fails,

$\overline{X_5}$ = Relay-A fails,

$\overline{X_6}$ = Current Transformer-2 fails,

$\overline{X_7}$ = Battery-2 Fails,

$\overline{X_8}$ = Wiring-2 fails,

$\overline{X_9}$ = Relay-B fails.

In passing, we stress that the fault trees considered might only represent an initial or first-cut approach to the problem. Other power-protection experts might argue that there are other sources of concern that warrant inclusion in the fault tree, or might wish to pursue the analysis further by expressing some events in terms of more basic causes.

3. Analysis of Fault Trees

A fault tree is a logical formulation which can be used to express the top event as a logical function of basic events. Noting that the algebra of events (set algebra) is isomorphic to the bivalent or two-valued Boolean algebra (switching algebra), we may choose to employ this latter type of algebra by considering the inputs and output of a fault tree as indicator variables of the respective events. Hence the fault tree produces a switching or Boolean function for the indicator variable of the top event in terms of the indicator variables of the basic events. It is now necessary to move from the Boolean domain to the probability domain so as to obtain the top-event probability as a function of basic-event probabilities. Based on these ideas, many algorithms have emerged for converting the switching (Boolean) expression for the indicator variable of the top event into a probability-ready expression (PRE), i.e. into an expression that is directly convertible, on a one-to-one basis, to a probability expression. It should be noted that, in a PRE, all ORed terms/(products) are disjoint, and all ANDed terms (sums) are statistically independent. The conversion from a PRE to a probability expression is trivially achieved by replacing Boolean variables by their expectations, AND operations by multiplications and OR operations by additions [21], [22]. In the following, we give a brief classification of the available algorithms for converting a general switching expression into a PRE .

A. Orthogonalization (disjointness)

These algorithms start with a sum-of-products (SOP) expression for a switching function and orthogonalize it by making all its terms mutually disjoint. The basic internal step for such algorithms is to consider a sum ($T_i \vee T_j$) of the two terms T_i and T_j that are non-disjoint and are such that neither of them subsumes the other. The term T_j is disjointed with (made orthogonal to) the term T_i by the relation:

$$T_i \vee T_j = T_i \vee T_j(\overline{y_1 y_2 \dots y_e})$$
$$= T_i \vee T_j(\overline{y_1} \vee y_1\overline{y_2} \vee y_1 y_2 \overline{y_3} \vee \dots \vee y_1 y_2 y_3 \dots y_{e-1}\overline{y_e}), \quad (1)$$

where $Y = \{y_1, y_2, y_3, \dots y_e\}$ is the set of literals that appear in T_i and do not appear in T_j. Note that T_j is replaced by e terms that are disjoint among themselves as well as being disjoint with T_j. In the limiting case of e = 0 (Y = φ), T_j subsumes T_i and is absorbed by it, i.e.,

$$T_i \vee T_j = T_i \vee T_j(0) = T_i. \quad (2)$$

The seminal work on orthogonalization (disjointness) is due to Abraham [23] and to Dotson and Gobien [24].Visual insight into the process of disjointness can be obtained through the use of logic aids such as the Karnaugh map [25].

B. Algorithms based primarily on statistical independence

Orthogonalization algorithms make a natural utilization of the statistical independence of basic events, when such independence can be assumed. There are other algorithms [22] which try to make a more direct use of statistical independence, not only through preserving it when it exists, but also by deliberately making it more manifestable through appropriate operations. For example, it is always possible to handle the complement of an expression instead of the expression itself if one uses the De

Morgan identity

$$\overline{(\vee_{i=1}^{n} X_i)} = \wedge_{i=1}^{n} \bar{X}_i, \quad (3)$$

then statistical independence can be utilized in the ANDed form that appears on the right-hand side of equation (3).

C. Expansion or Factoring Algorithm

The most powerful class of algorithms producing PREs are based on repeated use of the Boole-Shannon expansion [25]-[31] in which a switching expression is expanded about one of its variables in the form

$$\bar{S}(\bar{\boldsymbol{X}}) = \left(\bar{X}_i \wedge \bar{S}(\bar{\boldsymbol{X}}|\bar{X}_i = 1)\right) \vee \left(X_i \wedge \bar{S}(\bar{\boldsymbol{X}}|\bar{X}_i = 0)\right). \quad (4)$$

It should be noted that equation (4) represents a substantial step towards creating a PRE; the two terms on the right-hand side are disjoint, and each of them is an ANDing of statistically independent entities (under the assumption that ***X*** consists of statistically independent components).

$$Q(\mathbf{q}) = q_i Q(\mathbf{q}|1_i) + (1 - q_i) Q(\mathbf{q}|0_i). \quad (5)$$

where Q($\boldsymbol{q}$ | j_i), j = 0,1, is the function Q($\mathbf{q}$) with q_i set equal to j while the rest of the elements of $\boldsymbol{q}$ are left intact. Once a symbolic expression of the top-event probability as a function of basic-event probabilities is obtained, it can be used to derive important measures for the various basic events.

The indicator variable $\bar{S}_1$ of the top event for the fault tree in Fig. (1) can be expressed in terms of basic events as:

$$\bar{S}_1 = \bar{X}_1 \vee \bar{X}_2 \vee \bar{X}_3 \vee \bar{X}_4 \vee \bar{X}_5 \bar{X}_6. \quad (6)$$

Henceforth, the basic events are assumed to be statistically independent. Equation 6 can be rewritten in the disjoint SOP form as:

$$\bar{S}_1 = \bar{X}_1 \vee X_1 \bar{X}_2 \vee X_1 X_2 \bar{X}_3 \vee X_1 X_2 X_3 \bar{X}_4 \vee X_1 X_2 X_3 X_4 \bar{X}_5 \bar{X}_6 \quad (7)$$

which corresponds to the following expression for the top-event probability Q_1

$$Q_1 = q_1 + q_2(1 - q_1) + q_3(1 - q_1)(1 - q_2) + q_4 (1 - q_1)(1 - q_2)(1 - q_3) + q_5 q_6 (1 - q_1)(1 - q_2)(1 - q_3)(1 - q_4). \quad (8)$$

Alternatively, by using the complement of Eq. 6, the top-event probability can be expressed equivalently as:

$$Q_1 = 1 - (1 - q_1)(1 - q_2)(1 - q_3)(1 - q_4)(1 - q_5 q_6). \quad (9)$$

In the same manner, for the fault tree shown in Fig. (2), the expressions of $\overline{S_2}$ and Q_2 can be obtained as

$$\bar{S}_2 = \bar{X}_1 \vee (\bar{X}_2 \vee \bar{X}_3 \vee \bar{X}_4 \vee \bar{X}_5 \bar{X}_6)(\bar{X}_7 \vee \bar{X}_8 \vee \bar{X}_9 \vee \bar{X}_{10} \bar{X}_{11}). \quad (10)$$

$$Q_2 = q_1 + p_1\{q_2 + p_2[q_3 + p_3(q_4 + p_4 q_5 q_6)]\}\{q_7 + p_7[q_8 + p_8(q_9 + p_9 q_{10} q_{11})]\}, \quad (11)$$

where, $p_i = (1 - q_i)$.

4. Uncertainty Analysis

In reliability analysis of power system protection, models such as reliability block diagrams and fault trees are used to predict the reliability of the system [7], [8]. The parameters in these models are usually obtained from field data, data from systems with similar functionality and even by expert guessing, and hence are bound to suffer from considerable uncertainty [32]. The uncertainty problem pertaining to fault-tree outputs has an analytic doubly stochastic treatment via the method of moments. This method utilizes the multiaffine nature [17] of the top-event probability as a function of the basic event probabilities.

Since the components of **q** are statistically independent, the following expressions for the mean value (expectation) μ_1 of Q and its variance μ_2 can be drawn [15].

$$\mu_1 = Q(\boldsymbol{\nu}_1), \tag{12}$$

$$\mu_2 = \sum_{1\le i\le n} C_i^2 \nu_{i2} + \sum\sum_{1\le i<j\le n} C_{ij}^2 \nu_{i2}\nu_{j2} + \sum\sum\sum_{1\le i<j<k\le n} C_{ijk}^2 \nu_{i2}\nu_{j2}\nu_{k2} + \cdots + C_{12\ldots n}^2\, \nu_{12}\nu_{22}\ldots\nu_{n2}\,, \tag{13}$$

where

$$C_i = \left(\frac{\partial Q}{\partial q_i}\right)_{\boldsymbol{q}=\boldsymbol{\nu}_1} \tag{14}$$

$$C_{ij} = \left(\frac{\partial^2 Q}{\partial^2 q_i \partial q_j}\right)_{\boldsymbol{q}=\boldsymbol{\nu}_1} \tag{15}$$

$$C_{ijk} = \left(\frac{\partial^3 Q}{\partial q_i \partial q_j \partial q_k}\right)_{\boldsymbol{q}=\boldsymbol{\nu}_1} \tag{16}$$

5. Case Study

Consider the fault-tree top event $\overline{S_1}$ in Fig.(1) and the unavailability nominal values for the basic event taken from [9] and shown in Table (2). The top-event probability or unavailability Q_1 = 0.00044403426, which can be easily calculated by substituting the basic events unavailability's $q_i \ldots q_6$ from Table (2) into Eq. (8) or Eq. (9). This nominal value of Q_1 would not be obtained exactly in [9] (or in many references on power systems), because therein Q_1 would be simply given approximately by

$$Q_1 = q_1 + q_2 + q_3 + q_4 + q_5 q_6. \tag{8a}$$

For *typical small q values* as those in Table (2), Eq. (8a) serves as a *practical overestimation* of Eq. (8), though it results from an *invalid* one-to-one transformation of Eq. (6). Here, it yields the numerical value Q_1 = 0.0004440841, an overestimation by a *trivial* 0.011%. It seems an approximation could be *tolerated* in this case. However, there are cases in which an approximation might lead to considerable or unacceptable error. Anyhow, approximation should be avoided when one is concerned about uncertainty.

Table (2). Unavailabilities of Protection System Components.

Components	Unavailability
Circuit Breaker	$q_1 = 300*10^{-6}$
Current Transformer	$q_2 = 30*10^{-6}$
DC power System	$q_3 = 50*10^{-6}$
Wiring (per connection)	$q_4 = 64*10^{-6}$
Protective Relay Misapplications	$q_5 = q_6 = 290*10^{-6}$

Here, we generalize the situation in [9] by treating the basic-event reliabilities as log-normally distributed variables with medians equal to the deterministic values in Table (2), and with appropriate error factors. Note that a log-normally distributed variable with unity error factor has a zero variance and a mean equal to its median, and hence reduces to a non-random variable of a deterministic value equal to the original mean.

Figure (3) handles the case where a single basic-event probability q_1 is random, while all other basic-event probabilities are deterministic. The horizontal axis of Fig. (3) represents a change in the error factor F_1 of q_1 from 0 to 20. Note that an excessive value of the error factor should be avoided since (a) it is unwarranted for practical modelling, and (b) it might violate the assumption that the area under the infinite tail (1.0, ∞) of the log-normal pdf is negligible compared to unity. The vertical axis of Fig. (3) represents the variance (second-order central moment) μ_2 of top-event probability Q. The various plots in Fig. (3) correspond to various percentages of the tabulated median value of q_1 ($300 * 10^{-6}$) given in Table (2). For example, the label 20% in Fig. (3) means that q_1 has a median of $60* 10^{-6}$. Figure (4) is similar to Fig. (3) but it considers the case where all basic-event probabilities are random, independent and identically distributed. The change in the variance μ_2 of the top-event probability Q in Fig. (4) is substantially greater than the corresponding one in Fig. (3).

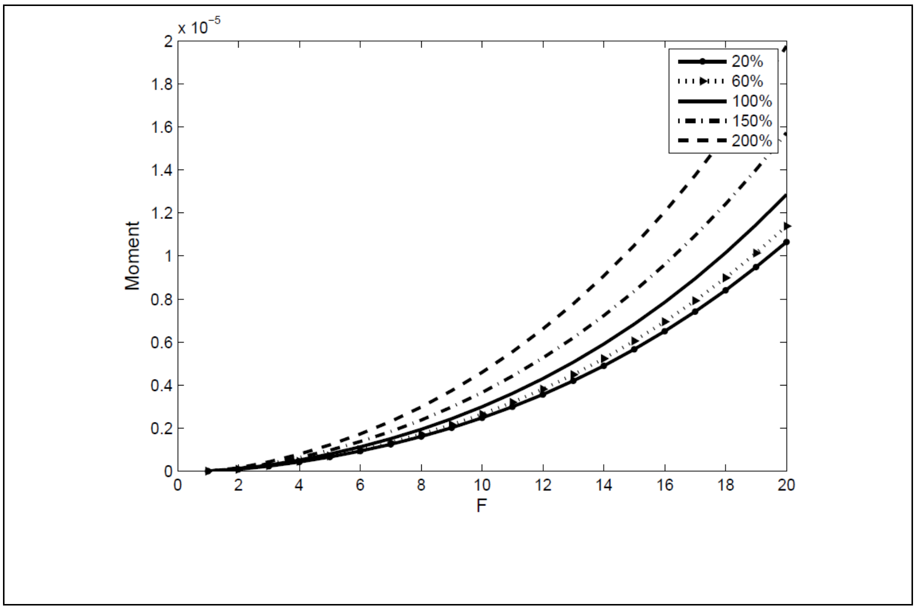

Fig. (3). Change in the variance (second-order central moment) μ_2 of the top-event probability Q due to variation in *q_1* error factor alone.

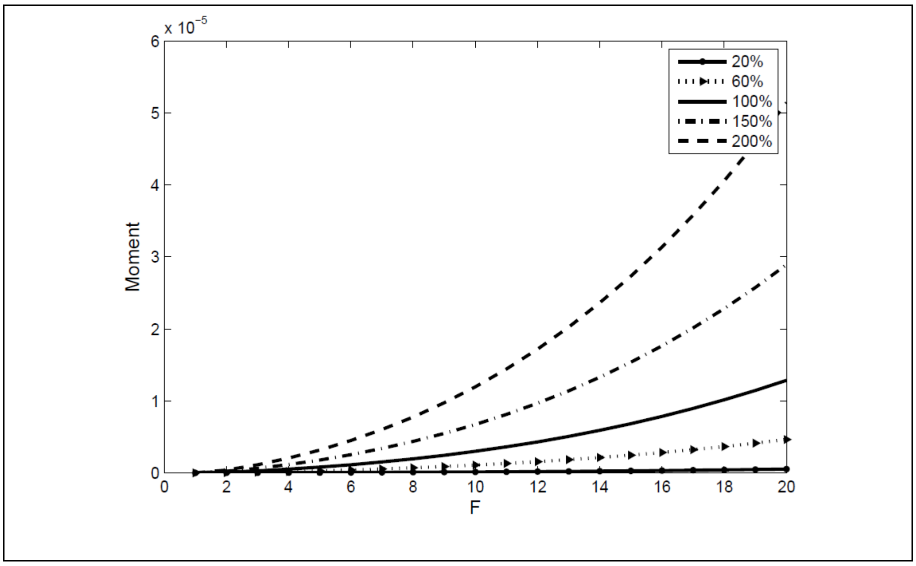

Fig.(4). Change in the variance (second-order central moment) μ_2 of the top-event probability Q due to identical variations in error factors of all *q's*.

6. Conclusions

In this paper, we illustrated the utility of fault trees in the study of power system protection by citing two illustrative examples. A brief survey of the fundamental families of algorithms used in the analysis of fault trees is presented, and the uncertainty analysis of fault-tree outputs via the method of moments is reviewed. Analytic formulas are presented for the mean and variance of the top-event probability when the basic-event probabilities are statistically independent. The concepts introduced are demonstrated via an illustrative numerical example.

Future work might include an extended study of power-protection schemes from the perspective of fault trees, with more detailed quantification of the first four moments of the top-event probability [15], [16], with the basic-event probabilities allowed to be statistically correlated [33].

7. References

1. **Blackburn, J. L., and Domin, T. J.,** *Protective Relaying: Principles and Applications,* CRC Press, New York, NY, USA, (2014).
2. **Udren, E., Zipp, J., Michel, G., Mustaphi, K., Nilsson, S., Phadke, A., Ramaswami, R., Rockefeller, G., Sachdev, M., Strang, W., *et al.*,** "Proposed statistical performance measures for microprocessor-based transmission-line protective relays. ii. collection and uses of data," *IEEE Transactions on Power Delivery,* Vol. 12, No. 1, (1997), pp. 144-156.
3. **Lee, W., Grosh, D., Tillman, F., and Lie, C.,** "Fault tree analysis, methods, and applications : A review," *IEEE Transactions on Reliability,* Vol. 34, No. 3, (1985), pp. 194-203.
4. **Beresh, R., Ciufo, J., and Anders, G.,** "Basic fault tree analysis for use in protection reliability," *International Journal of Reliability and Safety,* Vol. 2, No. 1, (2008), pp. 64-78.
5. **Hong, Y., Lee, L., and Cheng, H.,** "Reliability assessment of protection system for switchyard using fault-tree analysis," *Proceedings of the International IEEE Conference on Power System Technology, (PowerCon 2006)*, (2006), pp. 1-8.
6. **McCalley, J., and Fu, W.,** "Reliability of special protection systems," *IEEE Transactions on Power Systems,,* Vol. 14, No. 4, (1999), pp. 1400-1406.
7. **Zhang, J., Ding, M., and Qi, X.,** "Research on modeling methods of relay protection system," *Proceedings of the IEEE Asia-Pacific Power and Energy Engineering Conference (APPEEC 2011),* (2011), pp. 1-4.
8. **Schweitzer III, E., Fleming, B., Lee, T., and Anderson, P.,** "Reliability analysis of transmission protection using fault tree methods," *Proceedings of the 24th Annual Western Protective Relay Conference,* (1997), pp. 1-17.

9. **Morris, B., Moxley, R., and Kusch, C.,** "Then versus now: A comparison of total scheme complexity," *Proceedings of the IEEE 62nd Annual Conference for Protective Relay Engineers,* (2009), pp. 304-311.

10. **Khorashadi, H., Li, Z., and Madani, V.,** "Adaptive dependable and secure protection systems for electric power systems," *Proceedings of the Transmission and Distribution Conference and Exposition, 2008 (T&D IEEE/PES),* (2008), pp. 1-6.

11. **Schweitzer, E., Whitehead, D., Ferrer, H., Tziouvaras, D., Costello, D., and Escobedo, D.,** "Line protection: Redundancy, reliability, and affordability," *Proceedings of the IEEE 64th Annual Conference for Protective Relay Engineers,* (2011), pp. 1-24.

12. **Nuclear Regulatory Commission,** "Reactor safety study: an assessment of accident risks in US commercial nuclear power plants, App. II," WASH-1400 (NUREG-75/014), *Available from NTIS; Springfield, Virginia, 22151,USA,* (1975).

13. **Tanaka, H., Fan, L., Lai, F., and Toguchi, K.,** "Fault-tree analysis by fuzzy probability," *IEEE Transactions on Reliability,* Vol. 32, No. 5, (1983), pp. 453-457.

14. **Weber, D.,** "Fuzzy fault tree analysis," *Proceedings of the Third IEEE Conference on Fuzzy Systems (IEEE World Congress on Computational Intelligence),* (1994), pp. 1899-1904.

15. **Rushdi, A. M.,** "Uncertainty analysis of fault-tree outputs," *IEEE Transactions on Reliability,* Vol. 34, No. 5, (1985), pp. 458-462.

16. **Rushdi, A. M., and Kafrawy, K.,** "Uncertainty propagation in fault-tree analyses using an exact method of moments," *Microelectronics and Reliability,* Vol. 28, No. 6, (1988), pp. 945-965.

17. **Rushdi, A. M.,** "How to hand-check a symbolic reliability expression," *IEEE Transactions on Reliability,* Vol. 32, No. 5, (1983), pp. 402-408.

18. **Ebeling, C.,** *An Introduction to Reliability and Maintainability Engineering,* McGraw-Hill, New York, NY, USA, (2004).

19. **Henley, E., and Kumamoto, H.,** *Probabilistic Risk Assessment: Reliability Engineering Design, and Analysis.* IEEE Press, New York, NY, USA, (1981).

20. **Henley, E., and Kumamoto, H.,** *Designing for Reliability and Safety Control*, Prentice-Hall, Inc., Englewood Cliffs, New Jersey, USA, (1985).

21. **Bennetts, R.,** "On the analysis of fault trees," *IEEE Transactions on Reliability,* Vol. 24, No. 3, (1975), pp. 175-185.

22. **Rushdi, A. M., and Abdulghani**, **A.,** "A comparison between reliability analyses based primarily on disjointness or statistical independence: the case of the generalized Indra network," *Microelectronics and Reliability,* Vol. 33, No. 7, (1993), pp. 965-978.

23. **Abraham, J.,** "An improved algorithm for network reliability," *IEEE Transactions on Reliability,* Vol. 28, No. 1, (1979), pp. 58-61.

24. **Dotson W., and Gobien, J.,** "A new analysis technique for probabilistic graphs," *IEEE Transactions on Circuits and Systems,* Vol. 26, No. 10, (1979), pp. 855-865.

25. **Rushdi, A. M.,** "Symbolic reliability analysis with the aid of variable-entered Karnaugh maps," *IEEE Transactions on Reliability,* Vol. 32, No. 2, (1983), pp. 134-139.

26. **Rushdi, A. M., and Goda, A. S.,** "Symbolic reliability analysis via Shannon's expansion and statistical independence," *Microelectronics and Reliability,* Vol. 25, No. 6, (1985), pp. 1041-1053.

27. **Rushdi, A. M., and Ba-Rukab O. M.,** "A doubly-stochastic fault-tree assessment of the probabilities of security breaches in computer systems," *Proceedings of the Second Saudi Science Conference, Part Four: Computer, Mathematics, and Statistics,* Jeddah, Saudi Arabia, (2005), pp. 1-17.

28. **Rushdi, A. M., and Ba-Rukab O. M.,** "Fault-tree modelling of computer system security," *International Journal of Computer Mathematics,* Vol. 82, No. 7, (2005), pp. 805-819.

29. **Rushdi, A. M. A.,** "Partially-redundant systems: Examples, reliability, and life expectancy," *International Magazine on Advances in Computer Science and Telecommunications,* Vol. 1, No. 1, (2010), pp. 1-13.

30. **Rushdi, A. M. A., and Hassan A. K.,** "Reliability of migration between habitat patches with heterogeneous ecological corridors," *Ecological Modelling,* Vol. 304, (2015), pp. 1-10.

31. **Rushdi, A. M. A., and Alturki, A. M.,** "Reliability of coherent threshold systems," *Journal of Applied Sciences*, Vol. 15, No. 3, (2015), pp. 431-443.

32. **Yin, L., Smith, M., and Trivedi, K.,** "Uncertainty analysis in reliability modeling," *Proceedings of the Annual IEEE Reliability and Maintainability Symposium,* (2001), pp. 229-234.

33. **Kafrawy, K. F., and Rushdi, A. M.**, "Uncertainty analysis of fault trees with statistically correlated failure data," *Microelectronics and Reliability*, Vol. 30, No. 1, (1990), pp. 157-175.

تحليل الريبة لنماذج أشجار الأخطاء الخاصة بحماية نظم القدرة

صالح م. بامسق و علي محمد علي رشدي*

قسم الهندسة الكهربائية وهندسة الحاسبات، كلية الهندسة،
ص. ب. ٨٠٢٠٤، جامعة الملك عبد العزيز، جدة، ٢١٥٨٩، المملكة العربية السعودية
arushdi@kau.edu.sa

(قدم للنشر في ٢٠١٥/٧/١٤ ، قبل للنشر في ٢٠١٥/٩/١)

مخلص البحث. تعرض ورقة البحث هذه خوارزمية تحسب الريبة في متاحية حماية نظام للقدرة باستخدام نمذجة شجرة الأخطاء. يتم تقدير احتمال الحدث الأوجي لشجرة الأخطاء مثل حدث فشل الحماية في إجلاء الأعطاب، وذلك بدلالة القيمة الاسمية والريبة لكل احتمال من احتمالات الأحداث الأساسية. تبدأ الخوارزمية المقترحة بالحصول على تعبير رياضي عن الحدث الأوجي لشجرة الأخطاء في ميدان التبديل (الميدان البولاني) ثم تحول هذا التعبير إلى تعبير عن المتاحية في ميدان الاحتمالات، وتعقب ذلك باستغلال السلوك عديد الخطية لتعبير المعولية الناتج في عمل تقدير دقيق للريبة الحادثة فيه. يتم شرح مثال توضيحي لخطة حماية نمطية لنظام قدرة، حيث يجري الحصول على تقديرات رقمية دقيقة لكل من القيمة الاسمية والتباين في قيمة احتمال الحدث الأوجي.