Application of the FMEA and FTA for Analyzing Dependability of Generator Phase Fault Protection System

M.Karakache[1] ,B.Nadji[2] ,I. Ouahdi

(1,2,3) Laboratoire de Recherche sur L'Electrification des Entreprises Industrielles
(FHC)University of Boumerdes, Algeria

ABSTRACT

Generator protective systems are sometimes very complex incorporating many different equipment groups. The inherent dependability parameters such as reliability, availability, maintainability and security of such complex systems are a concern of the protection engineer and present a significant analytical problem. This paper describes the use f the failure modes analysis and their effects (FMEA) for analyzing the dependability of the protection systems and the fault tree method for analyzing the dependability parameters of generator stator phase fault protection system and showing the advantages of backup protection system.

Keywords: dependability, protection, FMEA, circuit breaker, fault tree, differential, Backup, protection, failure, availability.

INTRODUCTION

Generator faults are always considered to be serious since they can cause severe and costly damage to insulation, winding, and the core; they also produce severe mechanical torsional shock to shafts and coupling. As a consequence, for faults in or near generator that produce high magnitudes of short circuit- currents, differential protection systems with good characteristics are chosen, these characteristics are; fastness, sensitivity, reliability and selectivity. To achieve desirable reliability, redundant systems are usually used and they are called backup protection systems.

Analyzing the dependability parameters of industrial systems such protection systems can be done with different methods. Two famous methods has been used ;the failure modes analysis and their effects (FMEA) analysis (FTA).

The FMEA is an inductive technique, it adds to identify the failure modes of an item, the causes of each mode and the effects on the function of the item. The results of FMEA are generally represented into a table.

The fault tree which is a deductive technique. It permit to identify the causes of an undesirable event of a system I is also a qualitative method; it can be used to estimate the dependability parameters values using the probability measures of the causes appearance.

A protection for an electric power system comprises the following parts:

A measurement device with current- and/or voltage transformers and their sensors measuring the relevant quantities.

A relay, which when certain conditions are fulfilled sends signals to a circuit breaker or another switching device. This relay was earlier a separate unit, but can in modern protections be a part of a larger unit for protection, supervision and control.

Circuit breaker, which executes the given instruction(s) from the relay.

A telecommunication system mainly used at distance (line) protections to get a faster and more reliable performance.

Power supply system, which shall secure the power supply to the protection system, even with faults in the system. [4]

GENERATOR PHASE FAULT ROTECTION SYSTEMS

Primary Protection System

Phase fault protection of generator stator windings uses some form of high speed differential relaying; this one will detect three-phase faults, phase-to-phase faults, double phase-to-ground faults and some single phase – to- ground faults. To achieve such protection, two

current transformers are used for each phase; one connected at the generator neutral end and the other is on the terminal. The secondaries of these two transformers are connected to the relay. When the relay detects a fault (proportional to the difference between the currents of the secondaries), it sends a signal to the circuit breaker to trip generator. In our case, we study a unit-connected generator (the case of a power station), so we have a turbo generator with its excitation system, prime mover, a step up transformer and the auxiliaries' transformer. When the relay detects a fault, it sends a signals to trip the generator circuit breaker, the excitation system circuit breaker and a signal to trip also the prime mover. These relays are supplied by a power system supply (we consider all the relays supplied by one power supply system).

So primary protection system for generator stator phase fault can contain; six current transformers, generator circuit breaker, field circuit breaker, power system supply and three differential relays. These elements are interconnected by what we call wiring connections. So we can say that the primary protection system contains five subsystems, the CT's, the breakers, the relays, the power supply and the wiring connections subsystem. [2][3][4]

Backup Protection system

The type and sophistication of backup protection provided is dependent to some degree upon the size of the generator and the method of connecting the generator to the system. When a generator is connected to the system in the unit generator-transformer configuration, high-speed phase fault backup protection can be obtained by extending the protective zone of the unit transformer differential relay scheme to include the generator and sometimes the unit auxiliaries' transformer. In our case we consider it to be extended only for Generator.

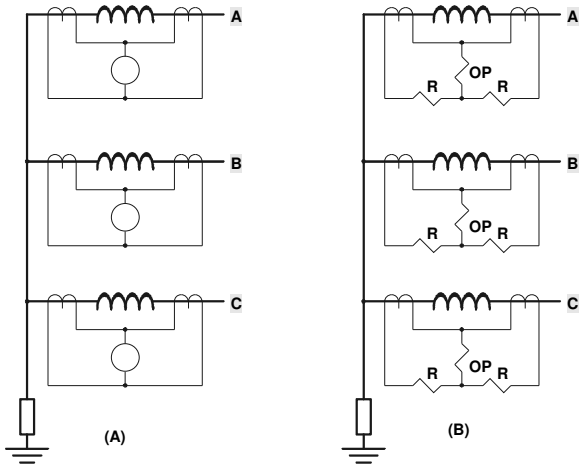

Figure 1 Stator windings of a generator protected by differential relays. (A) Basic differential over current relay, (B) percentage differential relay

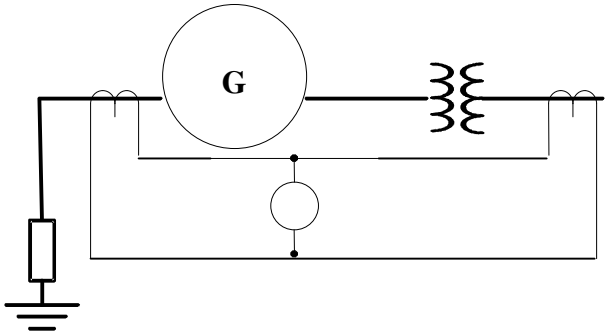

Figure 2 Unit connected overall differential protection

This backup is often referred to as the overall differential scheme and is illustrated in figure 2.
In this case, for each phase a relay is connected to the secondaries of two current transformers, one on the neutral end of the generator, the other on the secondary of step-up transformer. This relay and when it detects a fault, it send signals to trip the generator, the filed, the prime mover and also the circuit breaker of the step-up transformer. So backup protection system contains three differential relays supplied by a power system supply, three current transformers, a step-up transformer circuit breaker, generator circuit breaker, field circuit breaker and the wiring connections.

FAILURE MODES AND EFFECTS ANALYSIS

Failure modes and effects analysis (FMEA). A procedure by which each potential failure mode in a system is analyzed to determine the results or effects thereof on the system and to classify each potential failure mode according to its severity. It has been used firstly on 1960 in aeronautic for analyzing air plans security.[5].
First and in order to make the rest of the paper clear, we take these definitions:

failure: Termination of the ability of an item to perform its required functions.

failure cause: The circumstances during design, manufacture, or use which have led to failure; *syn:* root cause.
failure mode: The manner in which failure occurs; generally categorized as electrical, mechanical, thermal, and contamination.

The table 1 contains the analysis of failure modes and effects analysis applied to protection system elements using the results published in [6], for the circuit breaker, in [7], for transformer, in [8] for relays.

FAULT TREE ANALYSIS METHOD

The fault tree analysis is a tool used for dependability studies, it is a method of combining component failures rates, a concept first proposed by H.A.Watson of Bell Telephone Laboratories to analyze the Minuteman Launch Control System. This method, used and refined over the ensuing years, is attractive because is does not require extensive theorical work and is a practical tool that any engineer can learn to use. While computer programs are available to assist in developing and analyzing complex fault trees, this paper shows that small fault trees, which are easily analyzed manually, are also very useful. [1][5]

Fault tree construction (qualitative analysis)
A fault tree is tailored to a particular failure of interest and models only that part of the system, which influences the probability of that particular failure. The failure of interest is called the Top Event. A given system may have more than one top event, which merits investigation. For a protection system, the top event may be (the protection system fails to clear a fault in the prescribed time).

The top event is a box containing the description of the failure event of interest. The fault tree breaks down the top event into lower-level events. Logic gates show the relationship between lower-level events and the top event. The OR gate expresses the idea that any of several failures can cause the protection system to fail. The AND gate expresses the idea that both subsystems must fail for the top event occur. [1][5]

Application on the primary protection system
First and in order to make easy the work, we devise our system into subsystems, the current transformers represent a first subsystem, the relays represent a second subsystem, the circuits breakers a third one, the fourth subsystem includes the wiring connections and the fifth one is the power system supply. The top event in our case is (the primary protection fails to clear a fault in the prescribed time). The top event occurs if one of the five subsystems fails to operate. Each subsystem fails if one of the elements it contains fails to operate, for example the first subsystem fails if one of the CT's fails to measure current. So, for the primary system we need to use only the OR gates. The fault tree can be constructed as shown in figure3. The top event is represented in a rectangle; the circles are used to represent the basic events.

In the constructed tree we have the notations:
A the primary protection system fails
A1 the CT's subsystem fails
A2 the relays subsystem fails
A3 the circuit breaker subsystem fails
A4 the power supply fails
A5 the wiring connections fail
A11 the CT1 fails,
A12 the CT2 fails
A13 the CT3 fails,
A14 the CT4 fails
A15 the CT5 fails,
A16 the CT6 fails
A21 the relay 1 fails
A22 the relay 2 fails
A23 the relay 3 fails
A31 the prime mover tripping fails
A32 the field circuit breaker fails
A33 the generator circuit breaker fails

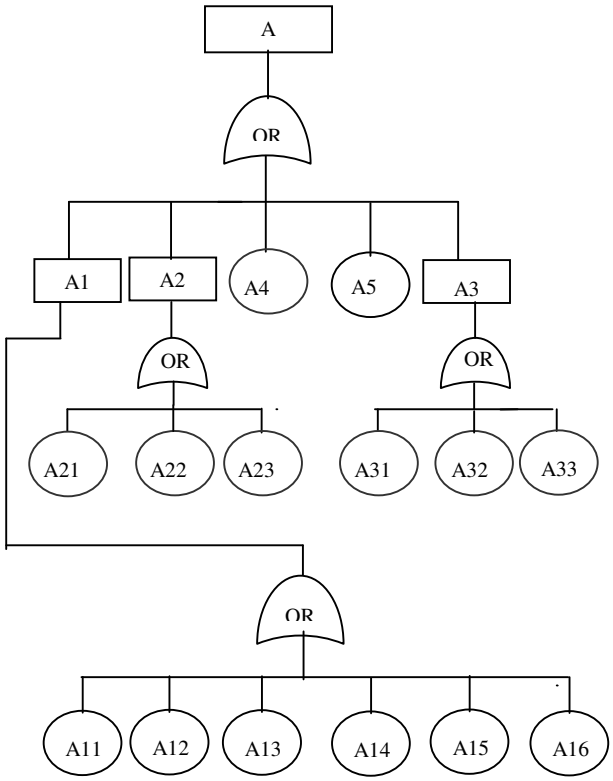

Figure 3 Fault tree construction for Primary protection system

Application on protection system containing primary and backup
In this case the top event occurs if both primary and backup protection fail to operate, that means we use the AND gate. Adding the backup protection is viewed as adding new subsystems; one subsystem contains three current transformers connected on the secondaries of the step-up transformer and the other contains three differential relays connected between the secondaries of these new current transformers and those of the current transformers already connected at the generator

neutral end. We assume that the power system supply is the same and given the following new notations:
C the subsystem that contains the current transformers connected on the generator neutral end;

B1 the subsystem containing the relays and CT's of the primary protection;
B2 the subsystem containing the relays and CT's of the backup protection.

Then, the fault tree in this case will be constructed as shown in figure4.
A17, A18, A19 new added CT's
A24, A25, A26 new added relays.

Quantitative analysis
By construction of the fault tree, we do qualitative analysis of the dependability of the protection system. That means we identify the causes of system's failure, but until this construction we don't have any information about the values of dependability parameters (reliability, availability, maintainability and security). With the fault tree analysis we can calculate some of these parameters, but we must have information about the components.

Device failure rates and unavailabilities
A device failure rate gives us the number of failures we can expect per unit time. During the useful lifetime of a device, we can frequently assume a constant failure rate. Failure rate can come from therorical calculations such as MIL-HDBK-217F parts-count procdures, or from field experience, for example, suppose there is in service population of 10000 devices, and we observe 10 failures in one year. The reciprocal gives us an estimated mean time between failures (MTBF) of 1000 years.

The strict definition of MTBF is the sum of Mean time to fail (MTTF) and the mean time to Repair (MTTR). MTTF is the reciprocal of failure rate. However MTTR is usually small and, in this paper we assume, MTBF is approximately equal to MTTF.

Failure rates are very useful in predicting maintenance costs, but not tell the whole story about whether a device will be available when called upon to perform. Thus we need to consider unavailability is the fraction of time a device cannot perform. It is unit less.
By definition the availability of a device is the probability that this device be in such a state so as to perform the function for which it was designed under given conditions and at a given time t, under the assumption that external conditions needed are assured. We will use the symbol A (t). The unavailability is noted 1-A (t) or Ã. If we call, A availability, λ constant failure rate, T the average down time per failure, we have:

$$MTBF=1/\lambda \qquad (1)$$

$$1-\tilde{A}\approx T/MTBF \qquad (2)$$

Each failure causes down time T, therefore the system is unavailable for time T out of total time MTBF

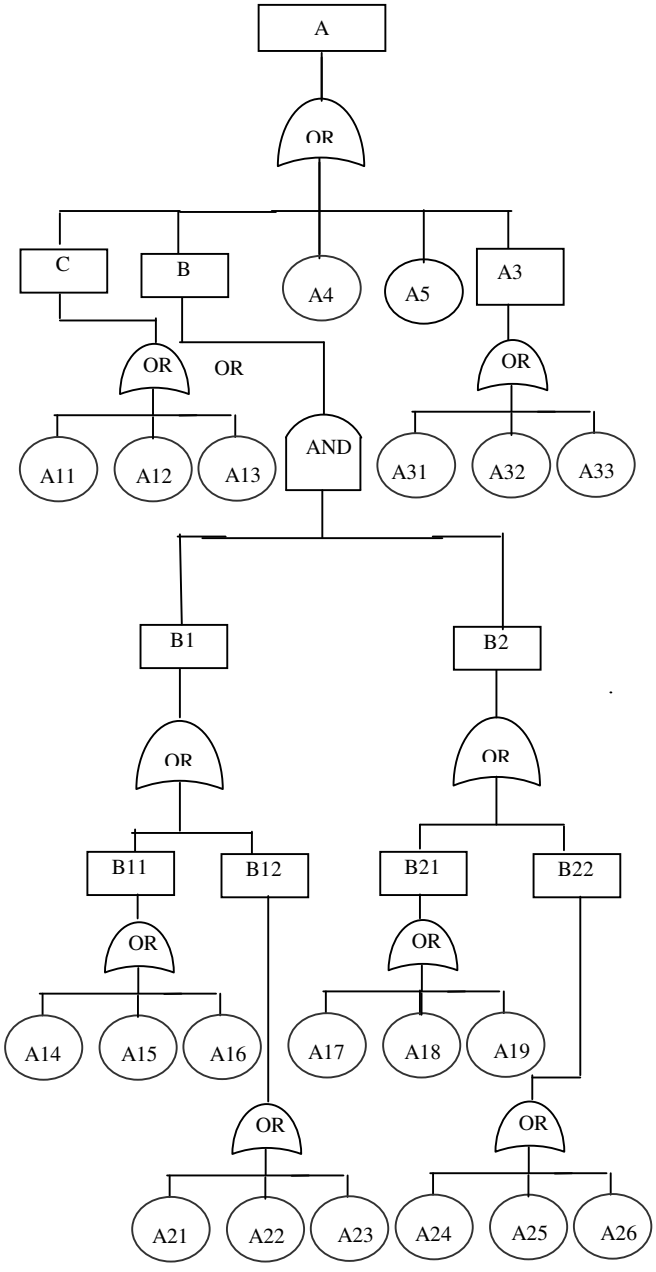

Figure 4 Fault tree construction for both primary and Backup protection System

.

For Protective Relay and Based on the field experience of industrial societies, an MTBF of 100 years is conservative for modern digital relays of quality design and construction, but electromechanical relays have an MTBF less. A Digital relay may have an unavailability of $\tilde{A}_R = 100.10^{-6}$.

The power system supply consists generally of a battery and charger and distribution circuits which are both inside and the outside the control house. If a loss of power system supply is monitored and responded to in less than a day, it's unavailability is assumed to be equal to $\tilde{A}_P = 50.10^{-6}$.

The unavailability of the Current transformer is assumed to be $\tilde{A}_T = 10.10^{-6}$.

For the Circuit Breaker we Assume that 90% of failures are detected by the usual monitors in the breaker, and in some relays, another 5% are detected by visual inspection every two months, The remaining 5% are detected by maintenance every two years, thus its unavailability is assumed to be equal to
$\tilde{A}_B = 300.10^{-6.}$ [1][5]

Application

With fault tree we can do two kinds of dependability analysis, the qualitative one and the quantitative one.

With qualitative analysis, we determine how system can fail, that means the basic events that can make system failures.

These basic events are represented with circles in the tree.

With quantitative analysis, we calculate the values of dependability parameters. These parameters are: reliability, availability, security and maintainability. The data, which we can have, can indicate which parameter is being easy to calculate. In our case, we have as data, the failure rates of each component, in other words the unavailability of each component, so we are interested by calculation of the whole system unavailability. In the case of fault tree analysis. We have the OR gates and the AND gates.

The unavailabity of the whole system is the sum of the devices unavailabities when they are connected to OR gate, and the product when they are connected to an AND gate. With those two rules we can find that the unavailabity of the primary protection system $\tilde{A}_s$ without backup is calculated as shown in equation (3)

$$\tilde{A}_s = 6.\tilde{A}_T + 3.\tilde{A}_R + 3\tilde{A}_B + \tilde{A}_P + \tilde{A}_C \qquad (3)$$

which gives us $\tilde{A}_S = 1360.10^{-6}$

But with backup protection the unavailability is calculated as shown in equation (4)

$$\tilde{A}_S = 3.\tilde{A}_B + \tilde{A}_P + \tilde{A}_C + 3.\tilde{A}_T + 9(\tilde{A}_R + \tilde{A}_T)^2 \qquad (4)$$

Which gives us $\tilde{A}_S = 1030.10^{-6}$

CONCLUSION

Using the FMEA fro analyzing the dependability parameters is very important, it permit to find the critical points of the considered system. Future surveys based on the FMEA are recommended so that more knowledge about the protection system element will be acquired and the problems of protection will be more clear.

Fault tree analysis method is an attractive tool to study the dependability parameters of industrial systems such the protection system. It helps us to define the causes of system's failures and to estimate some dependability parameters values if we have data.

Adding redundant system (backup protection) improves unavailability.

REFERENCES

1. E. O. Schweitzer, III, Bill Fleming, Tony J. Lee, Pullman, WA USA Paul M "Reliability Analysis of Transmission Protection Using Fault Tree Methods". 1997 (SEL Papers)

2. ANSI/IEEE C37.102-1995IEEE, "IEEE Guide For AC Generator Protection'' (IEEE Standards), pp 20-32, 1995

3. IEEE Power Engineering Society Tutorial 95TP102, "IEEE Tutorial on the Protection of Synchronous Generator.", (PES tutorials), pp8-11, 1995

4. C, Russell Mason, "The Art & Science of Protective Relaying", (book), pp 1-12, 171-183, 1956.

5. A.Villemeur, '' Sûreté de fonctionnement des systèmes industriels.''(book) 1988.

6. IEEE Std 493-1997 (Revision of IEEE Std 493-1990) "IEEE Recommended Practice for the Design of Reliable Industrial and Commercial Power Systems (gold book)".

7.Baretly William " Analysis of Transformer failures" Proceedings of the sixty Ninth Annual International Conference on Doble Clients, April 2000.

8. MIL-HDBK-217E, October, 1988," Military Handbook, Reliability Prediction of Electronic Equipment".

9. IEEE Std C37.10-1995 "IEEE Guide for Diagnostics and Failure Investigation of Power Circuit Breakers"

Element	Failure modes	Failure causes	Failure effects on protection system	recommendation
Circuit breaker	- Failure in the closed position - Failure to close c) Failure to close properly -Failure to stay closed, i.e., unintended trip -Failure in the open position -Failure to open - Failure to open properly -Failure to stay open, i.e., unintended close	Operating mechanism failure (mechanical failure)	- fault not cleared - service interrupted	Operating mechanism lubrification. Tests indicated in [9] recommended
Instrument transformer (CT or VT)	– no output – incorrect output	– electrical (insulation breakdown) -Thermal - mechanical	– fault not cleared – other equipment damage (circuit breaker)	Test indicated in [10]
Relay	– no output – incorrect output	– software failure – hardware failure	- fault not cleared - equipment damage	- Use or redundant relay,

Table 1. Application of the FMEA to power protection system elements