Back to Table of Contents

EVALUATION OF METHODS FOR BREAKER-FLASHOVER PROTECTION

Ramón Sandoval
Comisión Federal de Electricidad
Sinaloa, México

Jean León Eternod
Schweitzer Engineering Laboratories, S.A de C.V.
México, D.F

ABSTRACT

Some electric utilities have reported an increase in the number of breaker-flashover failures. Dedicated protection is required to prevent or reduce damage resulting from breaker flashover. Protection schemes for lines, transformers and generators or standard breaker-failure protection, either fail to detect breaker-flashover conditions or operate too late to prevent extensive damage. As a result, breakers can explode, damaging neighboring equipment or placing substation personnel at risk. Frequently, only one phase of the breaker flashes over during synchronizing procedures. In this case the power system suffers an undesirable out-of-step and single-phase synchronization, which can produce extensive damage to generators and step-up transformers. Electric utilities apply different breaker-flashover protection schemes, that may use different input signals, such as phase current, residual current, voltages from one or both sides of the breaker, breaker position, or close signal information. This paper evaluates different breaker-flashover protection schemes, with particular emphasis on reliability and on the equipment required. We use the fault-tree analysis method to make numerical reliability calculations for comparison purposes. We develop and use an alternative transient program (ATP) simulation model to get a better understanding of this kind of failure. We also present fault records of real breaker-flashover events to analyze the behavior of different protection schemes for these events, validate the simulation model and suggested settings, and show the consequences of not having adequate protection in place.

INTRODUCTION

Some electric utilities have reported an increase in the number of breaker failures caused by internal or external flashover while the breaker is open. In this paper, we refer to these as breaker-flashover failures. Breakers must be designed and tested under several standards, such as IEEE C84.1, IEEE C37.06, IEEE C37.013, IEEE C37.09 [1] [2] [3] [4]. These standards dictate maximum voltage levels that breakers must withstand between their open terminals and the associated testing methods. Levels should be high enough to tolerate normal operating overvoltages such as those present during synchronization, when the breaker terminal voltages could be out of phase.

Some gas decomposition products caused by arcing for normal operations can adhere to the internal surfaces of SF6 breakers after several operations. Without regular maintenance this could lead to an internal flashover. Several other conditions can cause breakers to lose their dielectric strength and allow arcing between their open contacts. These conditions include:

- Internal or external contamination
- Low dielectric pressure
- Humidity

The risk of breaker flashover also increases if overload on transmission networks makes taking equipment out of service for maintenance very difficult. Low-cost breakers with reduced security margins are more prone to flashover.

Flashover can occur on any breaker in the network where an overvoltage condition is present, but the probability is higher on breakers used to synchronize two isolated power systems or on generator breakers. During the synchronization process, the out-of-phase angle between breaker contacts changes from 0 to 360 degrees continuously. Voltage between breaker contacts reaches its maximum instantaneous value when the angle difference between the voltages is 180 degrees, with a magnitude equal to double the nominal phase-to-ground peak voltage (Figure 1). One example is a breaker that synchronizes a generator on a 500kV system: the voltage changes continuously between 0 and 577.3 kV rms or 0 and 816 kV peak instantaneous voltages.

$$\Delta V_{rms} = \frac{500}{\sqrt{3}} \angle 0° - \frac{500}{\sqrt{3}} \angle 180^{\circ} = 577.3\ \text{kV}$$
$$\Delta V_{peak} = 816\ \text{kV} \tag{1}$$

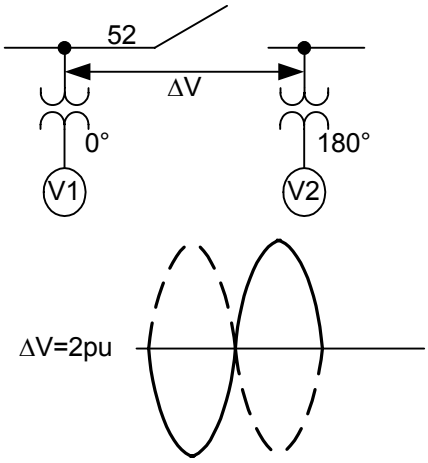

Figure 1 Voltage Waves on Both Sides of an Open Breaker When the Angle Is 180 Degrees.

Another possible cause of flashover can occur when a long high-voltage line, without line reactors, is energized. When the local breaker is closed the capacitive effect of the line will cause an overvoltage at the remote end. This overvoltage could cause the remote end breaker to experience a flashover.

If the dielectric strength on any of the breaker phases is lower than normal, a flashover can occur when the voltage across the open breaker contacts increase. The highest probability that this will happen is when the voltage angle is near 180 degrees. Besides damaging the breaker, this out-of-phase and unbalanced condition affects system stability and can lead to abnormally high stresses on electric equipment near the breaker, such as a generator or transformer.

From the power system point of view, a flashover is a series fault. A flashover is not a ground or a phase-to-phase fault, but a condition that resembles one phase of a breaker closed, with a residual current much lower than a phase-to-ground fault. A flashover can lead to a power oscillation. Line, transformer, and generator protection are not effective in this situation because they either do not detect flashover failure or do not detect it quickly enough. Neither is traditional or standard breaker-failure protection effective at detecting flashover failure, because these require an external trip signal from another protection device to initiate the breaker failure.

Relying on an external trip prolongs the failure until line, generator, or transformer protection trips.

REAL CASE ANALYSIS

System Data

Our case study is of a system where a real flashover happened during the synchronization process in a generator-transformer group connected to a 400 kV power system. The group included the following:

- A generator rated at 350 MVA, with a nominal voltage of 20kV and rated current of 10.104 kA.
- A generator-transformer rated at 375 MVA nominal, with a 20 kV delta to 400 kV grounded-wye

The substation arrangement is breaker and a half; the flashover occurred in the main breaker. The half breaker was open. There were no oscillographic records for the 400 kV breaker where the flashover occurred, but there were oscillographic records for the generator and adjacent 400kV line.

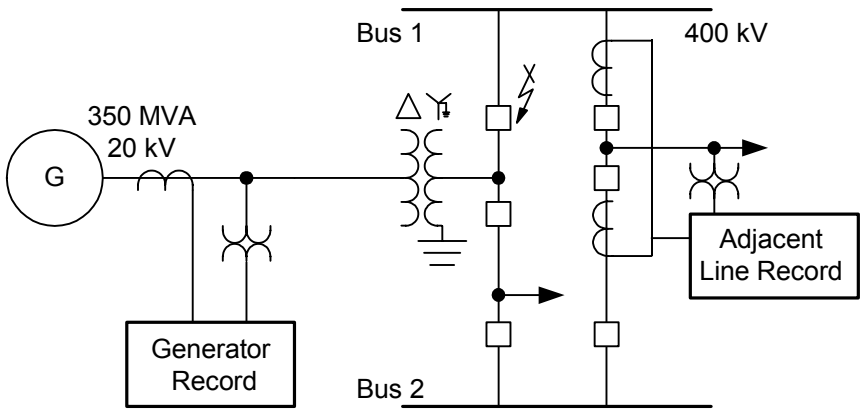

Figure 2 Case Study Data and Oscillographic Recorder Location

Analysis of Oscillographic Records

During the fault a key record was obtained at the 20 kV generator terminals. This record is shown in Figure 3, where we can see voltage and currents at the generator and calculate the same variables at the 400 kV level where the breaker flashed. Voltages on the adjacent 400 kV line where recorded at line-capacitive voltage transformers, Figure 4. The sequence of events was:

1. The 400 kV breaker A phase flashed over during synchronization. Currents at the generator suddenly appeared on A and B phases, and the terminal voltages on A and B phase experienced a phase shift.
2. After approximately one second (58 cycles) the power plant protection tripped as a result of the abnormal condition and sent a trip signal to the breaker and initiated the standard breaker failure scheme.
3. After 9 cycles, the breaker-failure scheme sent a trip signal to the breaker failure auxiliary relay (86BF) and cleared the bus, 67 cycles after the flashover occurred.

4. The 86BF auxiliary also tripped the 86G relay that trips the generator field breaker and turbine stop valves. The voltage at the generator terminals decreased very slowly. It took several seconds for the voltage to decrease to zero.
5. Four cycles after the 86BF tripped, currents in A and B phases reappeared because of a winding failure in the unit transformer 400kV A phase winding, from the high electromechanical stresses caused by the flashover. After the 86BF trip, these failed windings were still fed by the generator for several seconds, causing major transformer damage.

Table 1 shows the values of voltage and current at the generator and the 400 kV system bus during flashover; these values are in per unit (p.u.) with reference to nominal generator and transformer values.

Table 1 Voltages and Currents at Generator and Transformer During Flashover

Event	Generator Current (IA and IB, 20 kV level)	Breaker Current (IA 400 kV level)	Generator Voltage (VB, 20 kV level)	Adjacent Line Voltage (400 kV level)
First cycle of breaker flashover	5.1 p.u.	8.3 p.u.	0.31 p.u.	0.8 p.u.
Next 56 cycles of breaker flashover	Oscillation between 5.1 p.u. and zero Second oscillation 4.2 p.u.	Oscillation between 8.3 p.u. and zero Second oscillation 6.8 p.u.	Oscillation between 0.14 p.u. and 1.16 p.u.	Oscillation between 0.8 p.u. and 1.02 p.u.

Current at the high-voltage side of the transformer was 8.3 p.u. for the first cycle, but during the oscillation it dropped to zero. Transformer ground protection (51NT) is coordinated for permanent phase-to-ground faults; because the flashover current decreases faster than the time needed by a time-overcurrent relay to trip, the time-overcurrent relay does not detect this fault condition. The current magnitude at the 400 kV bus oscillates from a value greater than the normal phase-to-ground fault current to zero during the 56-cycle period, as shown in Table 1. Digital relays with instantaneous reset cannot trip for this condition. Electromechanical or digital relays with electromechanical-type reset may trip, but will take a very long time. The generator terminal voltage drops to 0.31 p.u., but the 400 kV system voltage only drops to 0.8 p.u.

Analysis of the current and voltage phase angles shows that at the beginning of flashover both voltages are in phase; as the generator begins to deliver active power to the system, the phase angle between the voltages changes and voltage and current begin to oscillate. For the first 18 cycles after the flashover began, the generator exported active power to the system. For the next 28 cycles the generator imported active power, thereafter the generator exported active power again. The breaker failure relay (86BF) finally cleared the fault after 67 cycles. The maximum active power imported by the generator was greater than 1 p.u., but lasted less than 0.5 seconds. The reverse power relay (32) had a magnitude pickup value of 0.03 p.u. but had a time delay setting of 2 seconds, therefore this relay did not trip the generator field breaker.

Negative-sequence current was present throughout the event with a maximum of 3.35 p.u. The negative-sequence relay was set to protect the generator with a factor of $I_2^2t=k$. The normal value for k is approximately 10. With a setting of k = 5, the trip time for a constant negative-sequence current magnitude of 3.35 p.u. would be 0.446 seconds. Because the magnitude of the negative-sequence current oscillates between 3.35 p.u. and zero, the negative-sequence overcurrent relay

did not trip. The simulation studies conducted after the flashover determined that the maximum value of k should have been approximately 4. This shows that the normal values used for negative-sequence protection are too high to trip for flashover failure.

Failure Consequences

The consequences of this failure were:

- The high electromechanical stresses during the out-of-phase, unbalanced energization caused severe transformer damage. The failure to isolate the generator from feeding the damaged high voltage transformer windings for several seconds resulted in high transformer repair costs.
- Cumulative damage and loss of life of neighboring equipment.
- Base generation out of dispatch for some days until a replacement transformer was installed and tested. High cost of replacing lost energy with more expensive remote sources.
- Power system oscillations occurred; however there were no additional problems because the system was operated with good security margins at the moment of the event.

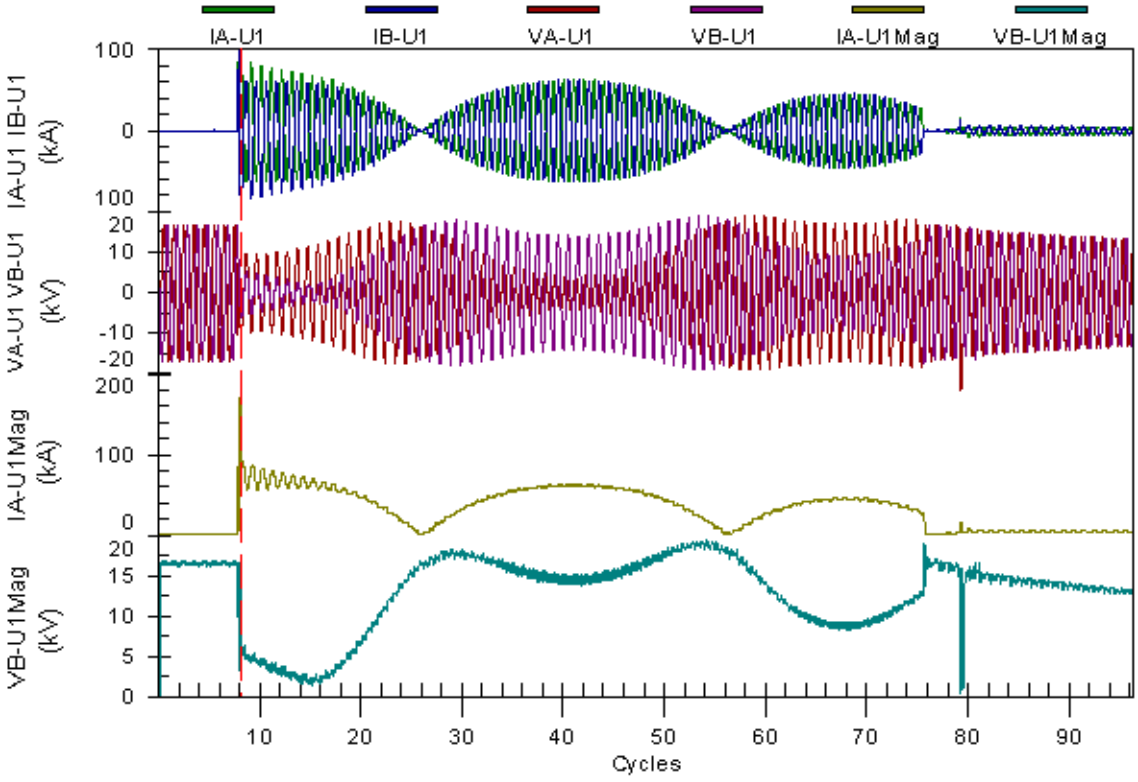

Figure 3 Real Generator Currents and Voltages During Breaker Flashover

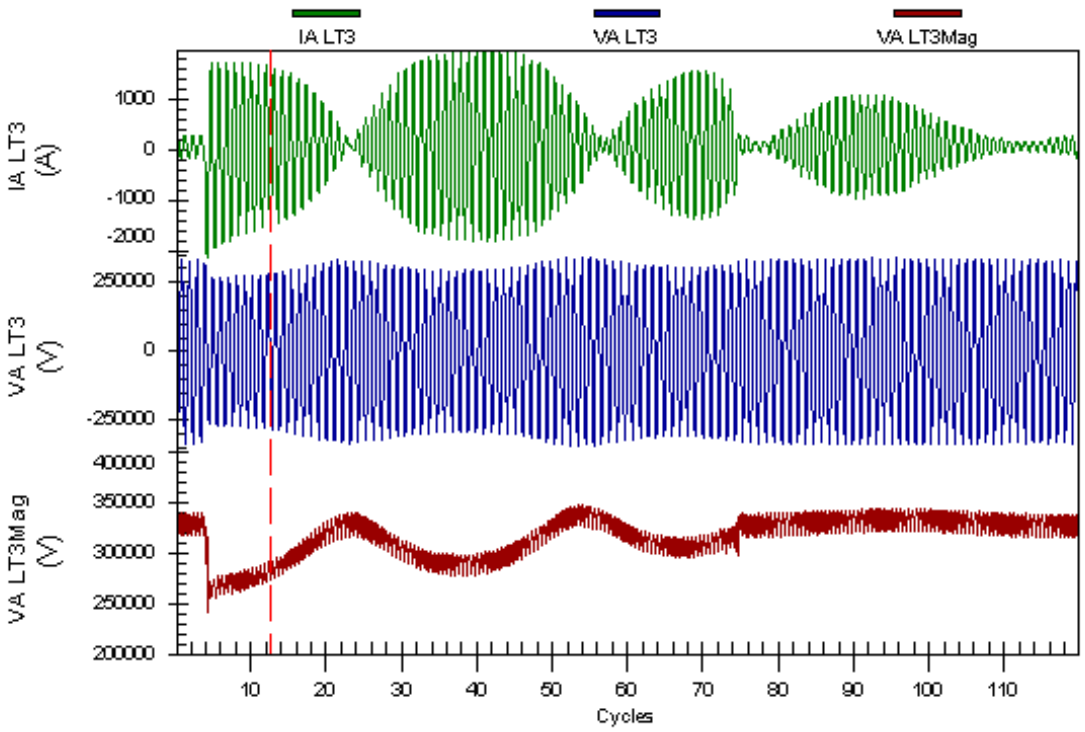

Figure 4 Adjacent Line Record of Current and Voltage at 400 kV During Generator Breaker Flashover

Even when the probability of a breaker flashover is low, the high costs of a failure justify using dedicated flashover protection that isolates the failed breaker as soon as possible, thereby avoiding damage to primary equipment. Implementation costs depend on the protection methods selected, but with present digital multifunction relays this can be done without additional equipment costs.

SIMULATION OF DIFFERENT FLASHOVER CONDITIONS

To obtain a better understanding for different flashover conditions, a model of the actual power system was created in ATP (EMTP). Comparing the simulation results, from the modeled power system, to the actual recorded results validated the power system model.

From Figure 5 it can be seen that the actual and simulated results match closely which confirms the accuracy of the simulation model. This model will now be used to investigate different conditions that can lead to flashover failure. In the simulated model flashover occurs when the voltage magnitude difference between the breaker contacts is approximately 2 p.u. At this point the angular difference between the voltages is 180°. Note that the simulated model ignores the effect of arc resistance.

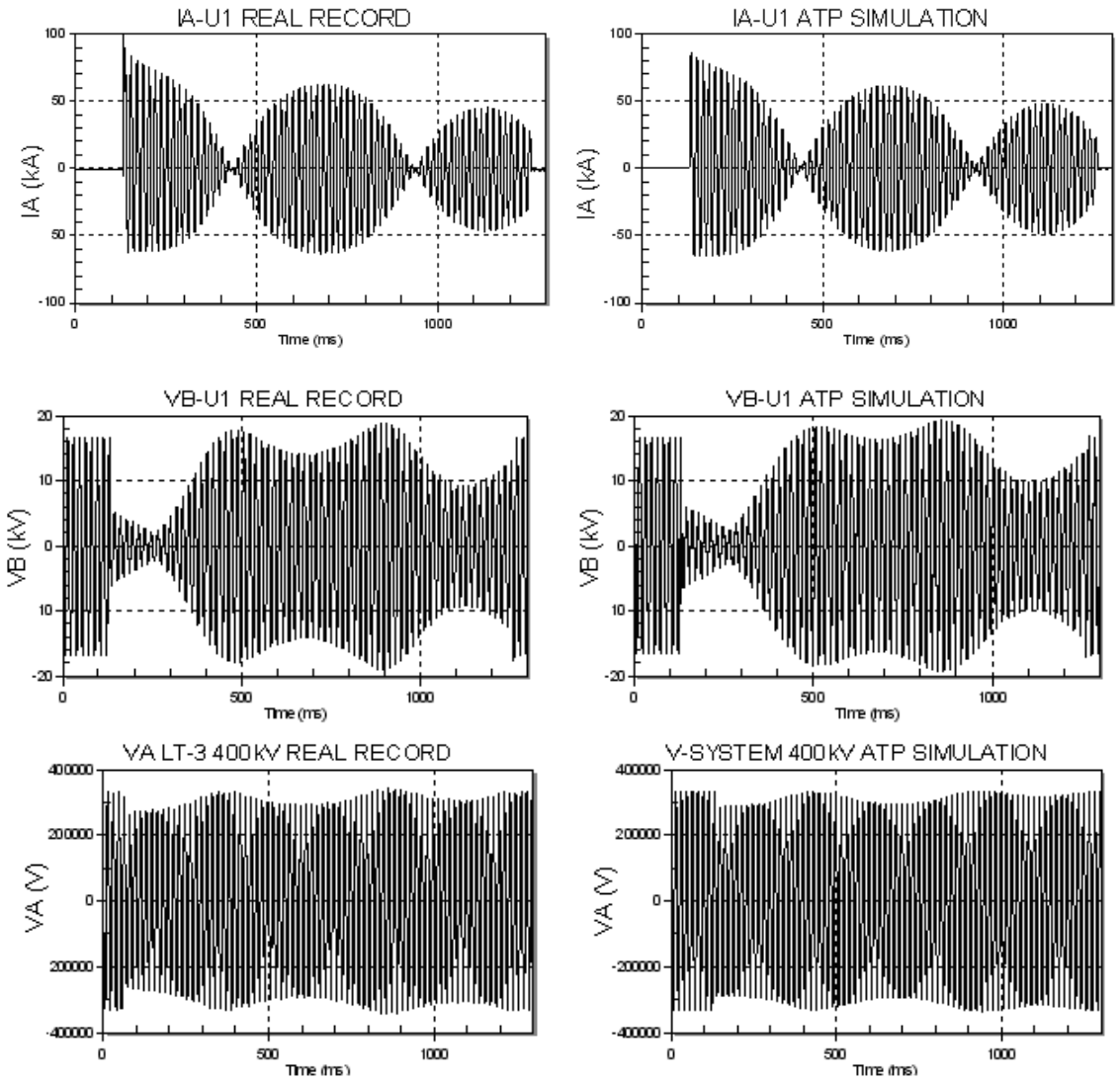

Figure 5 Comparison of Actual Records and ATP Simulation Results for Generator Voltage, Generator Current, and Adjacent Line Voltage

One main variable is the current at the failed breaker for which there are no actual records available. Simulation results in Figure 6 show that current magnitude oscillates from a value of 3.3 p.u. during the first cycle of flashover to zero approximately 18 cycles later. When setting the pickup current threshold and time-delay pickup of an overcurrent relay for flashover protection consideration should be given to the magnitude and duration of the current oscillation. A dc offset of 900A is also noticeable during the first few cycles after flashover; this effect can be ignored when setting a numerical digital protective relay.

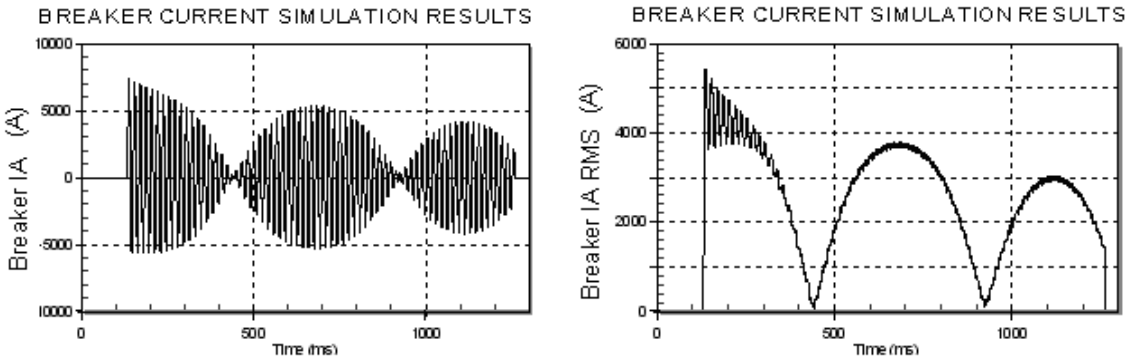

Figure 6 Failed Breaker Current From ATP Simulation Results

The effect of different flashover conditions can be evaluated using the simulated power system model; these different conditions are listed in Table 2.

Table 2 Current and Voltage Variations for Different Flashover Conditions

Case	Generator IA and IB	Breaker IA	Generator VB (phase-to-ground)	400 kV Bus VA (phase-to-ground)
Actual case	52.5–0 – 43 kA 5.1 – 0 – 4.2 p.u.	4.5 – 0 - 3.7 kA 8.3 – 0 – 6.8 p.u.	3.6 – 1.68 – 13.4 kV 0.31-0.14-1.16 p.u.	201 – 236 kV 0.87-1.02 p.u.
Flashover at 326 kV, 90°	53.3 – 0 – 43 kA 5.3 – 0 – 4.2 p.u.	4.9 – 0 - 3.7 kA 9 – 0 – 6.8k A	3.6 – 1.7 – 13.2 kV 0.31-0.15-1.14 p.u.	200 – 236 kV 0.86-1.02 p.u.
Without one of the parallel generators in the same bus	52.5 – 0 – 43 kA 5.2 – 0 – 4.2 p.u.	4.4 – 0 - 3.8 kA 8.1 – 0 – 7 p.u.	3.7 – 1.67 – 13.3 kV 0.32-0.14-1.15 p.u.	199 – 236 kV 0.86-1.02 p.u.
With weak system (Zthev •2)	49.2 – 0 – 40.7 kA 4.9 – 0 – 4 p.u.	4.0 – 0 - 3.6 kA 7.4 – 0 – 6.6 p.u.	3.8 – 2.3 – 13.4 kV 0.33-0.2-1.16 p.u.	177 – 239 kV 0.76-1.03 p.u.
Without one of the generators in the same bus and weak system	48.6 – 0 – 41.1 kA 4.8 – 0 – 4.1 p.u.	4.1 – 0 - 3.6 kA 7.6 – 0 – 6.6 p.u.	3.9 – 2.3 – 13.35 kV 0.34-0.2-1.16	170 – 239 kV 0.73-1.03 p.u.

From Table 2 and Figure **7** , we can observe changes in currents and voltages during different flashover conditions. Failure behavior does not change too much with these variations in system short circuit or angle between open breaker contacts at flashover initiation. Two issues to consider are:

- Very high dc current level if the flashover occurred at a 90º angle difference between the voltages of the open breaker contacts. The level is about 4 kA, 1.81 asymmetry.
- Lower voltage at the high voltage side (400kV) of the transformer (breaker bus voltage) if the system is weak, about 0.73 p.u.

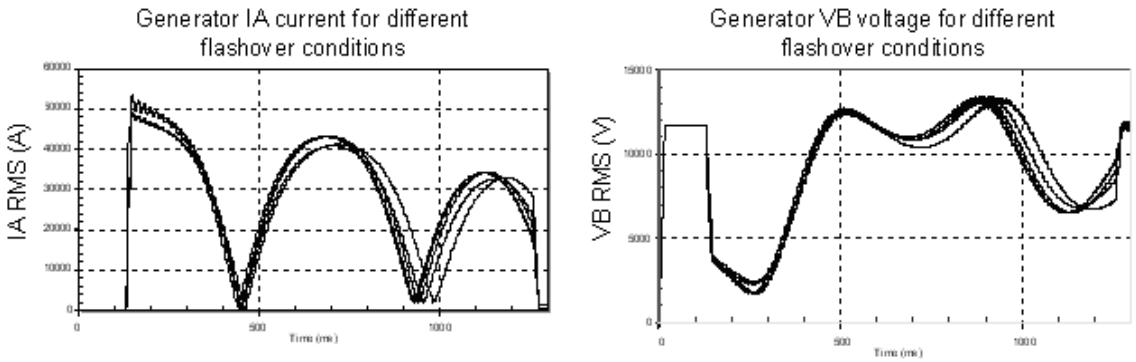

Figure 7 Generator Current and Voltage for Different Flashover Conditions

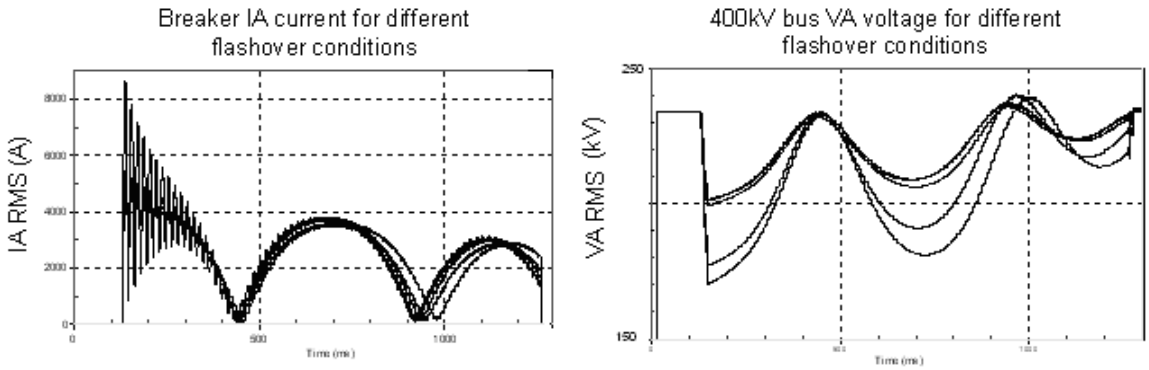

Figure 8 Breaker Current and Breaker/Bus Voltage for Different Flashover Conditions

Using this data, we can suggest and validate settings for breaker-flashover protection schemes.

METHODS FOR FLASHOVER-PROTECTION

Electric utilities use several different schemes for breaker-flashover protection. These methods can use information from any of the following: phase currents, residual current, voltages from one or both sides of the breaker, breaker position auxiliary contacts (52a or 52b), close-signal monitoring or timers, depending on individual company philosophies. Circuit breaker flashover protection may be realized in a separate protection relay or in a multifunctional breaker, line, transformer, or generator relay. Separate flashover protection relays are available, but their functionality can be replicated in multifunctional programmable protective relays.

Once the flashover is detected, all the breakers in the bus must be tripped, as in a conventional breaker-failure scheme. Security considerations are very important to avoid misoperations.

There is very little literature available about breaker flashover protection. The IEEE standard C37.102-1987 [5] describes a simple method to detect flashover in generator breakers that has both low security and low dependability. In addition, this method cannot be directly applied in double-breaker substation arrangements (ring bus, double breaker, or breaker and a half) or in single-pole trip-and-reclose breakers for transmission lines. It also fails to detect three-phase flashovers. Engineers have had to look for other methods to resolve these problems. This paper tries to serve as a guide in selecting and comparing those different methods, from the point of

view of equipment needed and reliability. Most examples are based on generator breakers, but may be used for any breaker.

Method A. Residual Overcurrent and Breaker Auxiliary Contact

This is the simplest and easiest method. It is described in the IEEE C37.102 [5] standard and is based on breaker residual-current measurement and a breaker auxiliary contact (52a or 52b). Flashover is detected and the bus cleared if there is residual current and the breaker is open. This condition could also occur for a short period during normal close operations where phases do not close simultaneously and there is a delay in contact change. These cases require a timer to confirm that there is a flashover. The logic diagram for this scheme is shown in Figure 9.

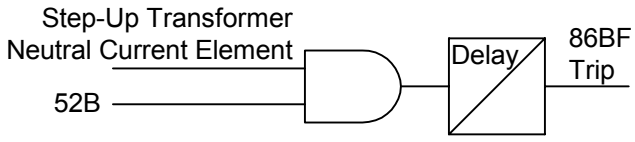

Figure 9 Logic Diagram of Breaker Flashover, Method A, Residual Current and Breaker Auxiliary Contact.

The residual current element should be set at a low level to detect small residual currents, thereby covering cases where flashover is not an out-of-phase condition and residual current is proportional to load. This element should also be set to cover cases where current decreases very rapidly to a value close to zero during an oscillation. The suggested value is above the normal residual current during load. For a step-up transformer this should be less than 5 or 10 percent of nominal current. For our case study, nominal current is 541A; the current transformer has a ratio of 1000/5, so a 0.3 A to 0.5 A setting is correct. The timer should be set longer than normal closing time, plus a security margin. We suggest a setting of 100 to 125 ms. IEEE C37.102 suggests using the same timer that is used for standard breaker-failure schemes, but that is not necessary if there are enough timers available in the multifunction relay. Standard breaker-failure schemes must be coordinated with backup protection, whereas breaker-flashover protection need only be coordinated with closing time.

Residual current could be obtained directly from the breaker current transformer (CT), neutral connection, but is usually obtained from the neutral CT of a step-up transformer because any residual current at the breaker will pass through this point, as Figure 10 shows. Figure 10 represents a typical connection to a multifunction generator relay with breaker-flashover protection included.

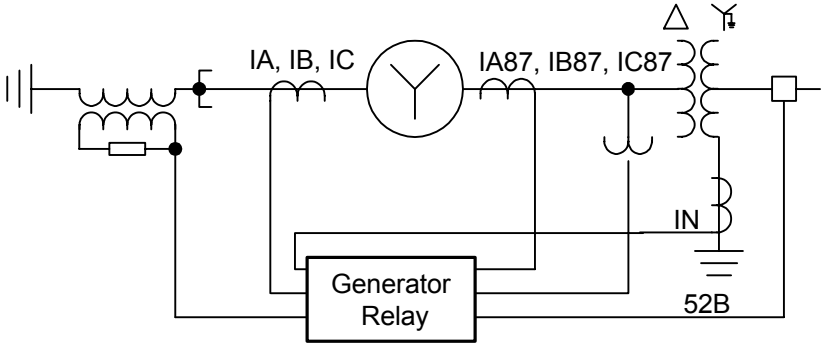

Figure 10 Flashover Protection Scheme With Multifunction Generator Relay

Step-up neutral transformer current is applicable where there is only one generator breaker. It should not be used where there are bus arrangements, such as breaker and a half, ring bus, or double bus-double breaker, because it can detect flashover but cannot determine which breaker flashed over. For these cases, you need one breaker-flashover scheme per breaker that can be implemented in a multifunction relay at the substation (breaker-failure relay or line relay) or at the power plant protection panel in a multiwinding transformer relay, as Figure 11 shows.

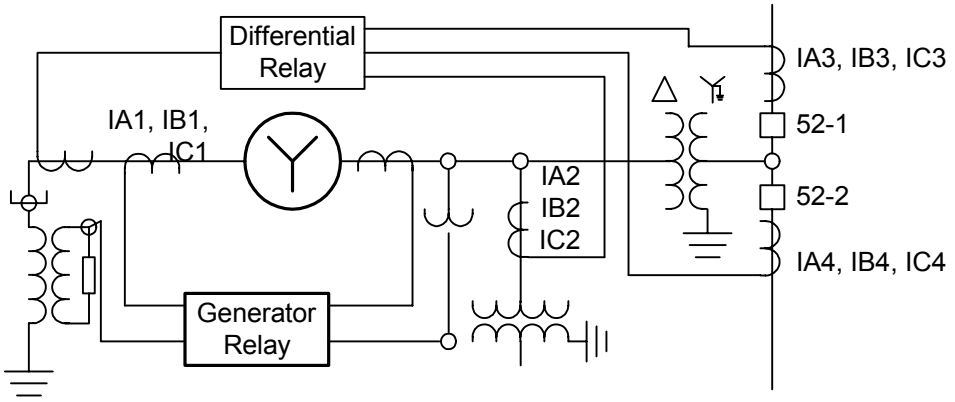

Figure 11 Flashover Protection Scheme With a Four-Winding, Multifunction Differential Relay.

Another approach would be to use step-up transformer neutral protection and the logic in Figure 9 to detect flashover, and another relay with residual overcurrent elements for each breaker to trip the right bus. We do not recommend this method because it adds points of failure without any advantage over using a separate scheme for each breaker.

The main disadvantage of Method A is lack of security and dependability. If the breaker auxiliary (52b) signal is not received, it will not trip for a flashover condition. If we use 52a instead of 52b, then it leads to a very insecure state where any external phase-to-ground failure with transformer-fed residual current will trip the bus. The breaker auxiliary signal could fail because the breaker mechanism fails, or the auxiliary relay fails, or the control circuit connections between breaker and relay fail.

It is possible to use a normally closed (52b) or normally open (52a) auxiliary contact. Some people believe that using the 52b contact improves security by decreasing the chance of incorrect breaker-open indication. However, if we accept this conclusion, we must also accept that the chance of incorrect breaker-closed indication increases, which reduces dependability.

A further problem with these methods emerges at breaker-and-a-half arrangements where a generator and a line share the half breaker, or when the flashover scheme is for a line breaker. If the line has single-pole trip and reclose, residual current and one pole open is a normal condition. This method can be applied in single-pole operation breakers if we use 52b auxiliary contacts for phases A, B, and C in series, so that the scheme does not trip until there is an indication of the three phases of the breaker open. Here, too, dependability will drop because the probability that an open breaker will not be detected is multiplied by a factor of three.

This method also does not work for three-phase flashover, but the probability of this kind of failure is very low. Other methods are available that avoid an insecure condition without losing dependability.

Method B. Current and Breaker Auxiliary Contact Per Phase

One possible variation of Method A is the use of current and breaker contact per phase, which has the advantages of directly targeting relay operation per phase and of applying to single-pole-operating breakers.

This method, which we call Method B, is not applied in practice because its security would be very low. During a normal close condition, if the breaker contact does not change, Method B would trip the bus incorrectly if the overcurrent element were set as low as we recommend, so that the overcurrent element remains asserted during current oscillations.

Method C. Time Limits and Close-Signal Monitoring to Detect Flashover

One way to increase the security of methods A and B is to limit the time period when the schemes can start. The logic diagram in Figure 12 only allows scheme operation if latch conditions occur in the first five cycles after current flows in the breaker. With this timer and logic combination, we solve the case where a breaker auxiliary signal is lost in the scheme during normal operation with the breaker closed and residual or phase currents present. Methods A and B would trip for this condition, Method A with an external fault and Method B only with load.

Close-signal monitoring provides another security improvement to Method C. The logic shown in Figure 12, blocks the start of the scheme if there is a close signal present and for six cycles afterward. With this we solve the case of a normal close with load, where the breaker contact does not change its state. Method B would trip in this situation.

Then, in order to trip, Method C requires:

- Phase current greater than the setting value, without no current five cycles before the start of the scheme
- Breaker auxiliary contact open (for 52a)
- No closing signals to breaker at least six cycles before the start

Once the scheme starts, it seals in and uses a timer to confirm the flashover condition. The timer could stop if current drops below the setting (near to zero), if 52a changes to indicate a closed breaker, or if there is a close signal.

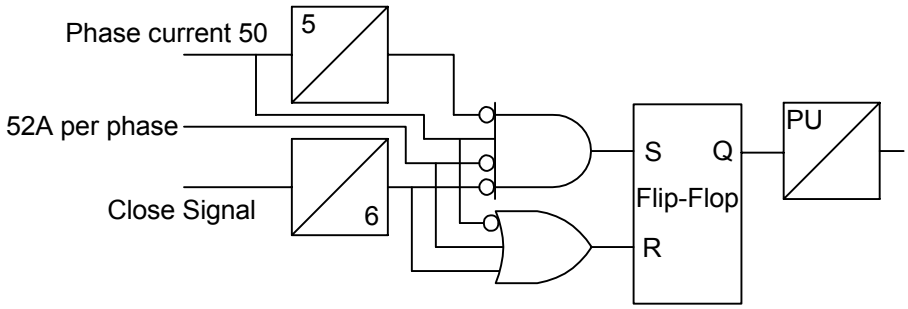

Figure 12 Method C: Improvements With Close-Signal Monitoring and Time Limits to Start

Method C could be applied to three-phase or single-phase breakers and improve security without loss of dependability.

Method C works well for three-phase flashover if used as shown in Figure 12.

Method C could be modified to include residual or step-up transformer neutral current instead of phase current for generator breakers where there is no single-pole tripping, but then it would no longer work for three-phase flashovers. In this case, the 52a signal must be formed with A-, B- and C-phase 52a auxiliary contacts in parallel or with 52b auxiliary contacts in series.

Method D. Live-Bus Voltage Supervision

Some flashover schemes use live-bus voltage relay supervision to initiate the scheme. The theory is that voltage should be at normal levels or higher before or during the flashover. But in many cases, such as the one in our case study, voltage is only normal before flashover, then drops to 0.8 p.u. at the beginning of the failure because of the out-of-phase synchronization. In this case voltage drops to 0.8 p.u. because the bus has a very high short-circuit level (strong network). For buses in weak systems voltage could drop to lower levels. Our simulation results indicated 0.73 p.u. for a weak system.

For this and other examples, voltage supervision should be set to 0.6 p.u. or lower to ensure that the scheme starts. There is no increase in security because a voltage element set to 0.6 p.u. will be active all the time with load or for some external faults. Dependability is affected because two dependability related failures are now possible:

- Loss of secondary potentials from PTs
- One more setting, so more chance of human error

We do not recommend the use of live-bus voltage supervision.

Method E. Voltage at Both Sides of the Breaker

Two characteristics of flashover events are:

- There is no current before the flashover and there is high voltage between open breaker terminals.
- During flashover, current flows and voltage drops to near zero.

It is possible to detect flashover with a scheme that uses these conditions. These conditions also happen during a normal close of the breaker, so the scheme must be supervised by close-signal monitoring, similar to Method C. Logic for this scheme is shown in Figure 13. Suggested setting for high voltage across open terminals before operation is 0.8 p.u. phase-to-ground voltage, to ensure operation when the breaker flashes with high voltage on one side and the other side dead. For our case study, with a PT ratio of 3500/1, 400 kV nominal and 230 kV phase-to-ground, the recommended setting is 53 V secondary. To set the low-voltage detector for conditions after flashover we need to consider possible voltage drop across the arc resistance. Based on our simulation results, we assume arc resistance was very low. We simulated zero ohms resistance and all the results matched oscillographic records. For our case study, which does not have pre-insertion resistors, 10 percent of nominal phase-to-ground voltage could be used, about 6.8 V secondary. For breakers with pre-insertion resistors the low-voltage detector should be set below voltage drop, with resistors inserted to increase security during close operations. Time limits need to be applied to ensure that voltage drop and current flow coincide.

This method has the following advantages:

- Good dependability and security with supervision of voltage across the breaker
- Record of voltage that causes flashover, enabling users of digital relays with recording features to evaluate breaker performance

Although it has these advantages, Method E has the following problems to solve:

- It requires three-phase PTs on both sides of the breaker, which are not available in most substations
- It cannot be used with PTs on the generator side and PTs on line side where there is a step-up transformer because:
  - the voltage drop in the transformer that is proportional to current
  - the step-up transformer also introduces a phase-angle shift
  - A scheme to compensate for these issues could be used, but would be very complex and lack dependability
- Security decrease compared to methods A and C for two reasons:
  - loss of secondary potential failure
  - two more settings increase risk of human error

This method is not common in many electric companies; field engineers are not familiar with it. Training and information would be very important to applying it.

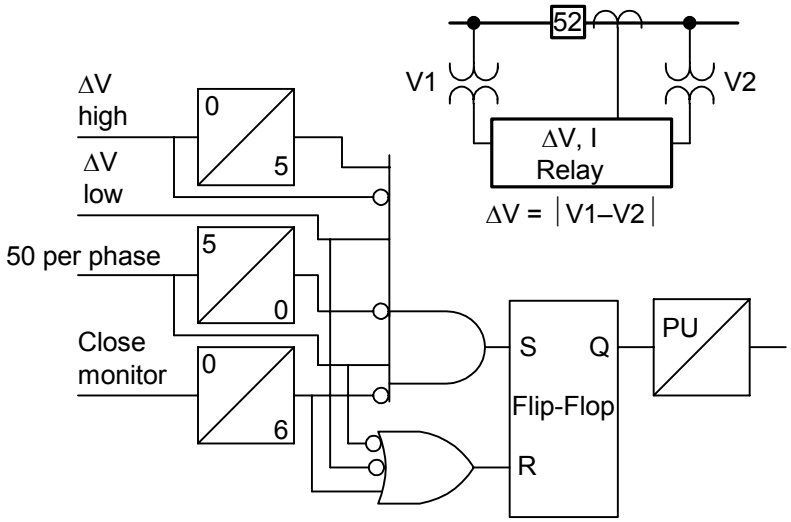

Figure 13 Flashover Protection Using Voltage at Both Sides of the Breaker and Close Monitor.

BREAKER STATES AND FAILURE MODES

We have described one of the possible failure modes for breakers, the flashover failure or failure while the breaker is open. Some utilities use standard, traditional breaker failure protection that covers the case of failure to trip when there is line, transformer, or generator failure, and primary protection trips. Breaker-flashover protection is more common everyday, but is not standard and there are several questions about its application. We try to answer some of them.

There are other modes of breaker failure, for example: failure to trip with load current or without current, failure to close, or breaker failure while the breaker is closed, with pre-insertion resistors. Figure 14 describes all the possible states and failure modes in a breaker. A comprehensive breaker-protection scheme should cover all these modes of failure and can be achieved in modern multifunction relays.

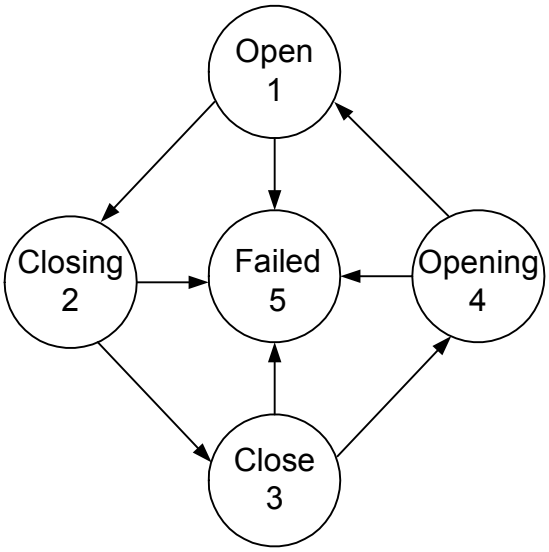

Figure 14 Breaker States and Failure Modes.

MONITORING AND PREDICTIVE MAINTENANCE OF BREAKERS

Comprehensive breaker protection is needed in every breaker and flashover-protection logic is a must in breakers used to synchronize generators or systems, or in long high-voltage lines. An important question is whether we can decrease the number of breaker failures or detect some problems before they cause a major failure. Present technology permits the same intelligent electronic device (IED) that is used as a multifunction protective relay to be used as a real-time monitoring and maintenance tool.

As a performance monitor, this device could alarm for several abnormal conditions that can give us an early indication that there is a problem in the breaker or in the protection-associated scheme signals. Some of these important alarms are:

- Slow electrical trip or close alarm, per phase, measuring the time between the close or trip control signals and current interruption. This slow operation could mean mechanical or internal isolation problems.
- Slow mechanical trip or close alarm, per phase, measuring the time between the close or trip control signals and 52a or 52b breaker contacts. This slow operation could mean mechanical or control circuit problems.
- Current that contradicts breaker contact 52a indication (52a open and current flow). This particular alarm increases the security of flashover methods A and C. It also increases the security of standard breaker-failure schemes that use 52a instead of current, which is normal in generation applications.
- Voltage difference between the terminals of a closed breaker. This alarm increases the security and dependability of flashover Method E with six PTs, because it can indicate problems such as loss of secondary potential, as well as problems with the 52a signal for scheme A or C.
- Pole scatter during close or trip operations, alarming if the time between the 52a change in the first pole and the 52a in the last pole is longer than a threshold.

- Pole discrepancy, looking for conditions where 52a (or current) indicates one or two poles closed, with one or two poles open. IEEE 37.102 suggests pole discrepancy could protect against flashover because one phase has current and the other two do not. We do not recommend this approach because it requires a long delay and current thresholds would be difficult to set. Some utilities use pole discrepancy with a one-to-two second timer and only trip the failed breaker, but this does not work for flashover protection.

Contact wear information, important from the maintenance point of view, is not just the number of operations. To provide good contact wear information, an IED needs to measure both the number of operations and the current per pole. Precise information helps to program maintenance as needed for the breaker to optimize maintenance resources, improve power system reliability, and increase circuit-breaker life expectancy.

FAULT TREE RELIABILITY ANALYSIS OF FLASHOVER-PROTECTION METHODS

Fault Tree Methodology and Input Data

We use fault tree reliability analysis to numerically evaluate security and dependability, and quantitatively compare different flashover protection methods. This method is easy to apply, and its use for protection and automation reliability estimates has been previously documented [6] [7].

The scheme failure of concern is called the top event. The probability that the scheme fails for the top event is a combination of the failure probabilities of the components in the scheme. We use AND and OR gates to represent combinations of failure probabilities. For an OR gate, any inputs to that OR gate can contribute to scheme failure. Total failure probability is the sum of the failure probabilities of input events. For an AND gate, any inputs to that gate must fail together to cause scheme failure. The upper level probability for scheme failure from an AND gate is the product of input probabilities.

We can use the device failure rate to estimate the failure probability for each device in the scheme. One industry practice is to provide failure rates as Mean Time Between Failures (MTBF). MTBF could be based on field failure data or on assumptions about complexity and exposure of equipment. If we have 50 auxiliary relays and only one such relay fails per year, we can assume a failure rate of 1/50 failure per year or an MTBF of 50 years from field experience. If we have 1000 units, we can expect 1000•1/50 = 20 failures per year. Some communications equipment vendors, however, if they estimate failure rates based upon complexity, could publish an MTBF of 80 years.

Failure rates are useful for predicting maintenance cost or the probability of security failure, but they do not tell us whether a device will be available when called upon to clear a fault. For dependability estimation, we should use unavailability, that is, the fraction of time a device cannot work when needed.

Unavailability, as calculated in the following equation, provides us with this information.

$$q = \lambda T = T / MTBF$$

Where:

q is unavailability

λ is failure rate

T is average downtime per failure

MTBF is mean time between failures

Each failure causes downtime, T. Therefore the system is unavailable for time T out of total time MTBF, and q indicates the fraction of time the system is not available. It is unitless. If a multifunction IED has self-tests and a monitored failure alarm, we could easily detect a failure on this device. Detection could take some seconds, but for total T we may consider two days for detection, analysis of the failure, and repair or replacement before the device is again in service and useful. Unavailability with this example:

T = 2 days with self-test and alarm

MTBF = 100 years

q = 2 / (100 • 365) = 0.0000548 unavailability or 0.02 days/year

One weakness of several protection or control schemes is the dependency on breaker auxiliary relays. MTBF could work well for high-quality auxiliary relays, for example 200 years, but T is always large because of a lack of automatic supervision. Failure of an auxiliary relay could go unnoticed until the next maintenance period or until operation of that relay is required. If the maintenance or testing period is every two years, a failure could occur the day following a maintenance test or one day before the next period, an average time of one year. For this example:

T = 1 year without self-test and 2 years maintenance period

MTBF = 200 years

q = 365 / (200 • 365) = 0.005 unavailability or 1.825 days/year

The result is 91 times worse than the example with the multifunction IED, even considering the much better MTBF.

Unavailability gives direct information about the probability that a device on the scheme will fail and contribute to scheme failure to trip when needed (dependability failures). From references [4] and [5], we obtain unavailability or MTBF estimations for several devices used in flashover schemes and we make our own estimations for the rest of them. These numbers, although the approximations are subject to dispute, provide valuable information for checking the degree of magnitude improvements and the impact of automatic supervision and alarms, redundancy, or other changes on the scheme configuration. Some of them are based on field statistics and more precise models could be built using more field data. We would greatly appreciate any failure rate data that utilities could provide to us in order to refine these models.

Table 3 Unavailability and MTBF Indices for Devices Used in Flashover Schemes

Devices or Basic Events	MTBF	T	Unavailability • 10^6
Current transformers	500 years	2 days	11
Potential transformers with loss of secondary potentials supervision or PTs used for SCADA measuring[1]	125 years	2 days	44
52a breaker auxiliary relay false open	200 years	1 year	5000
52a breaker auxiliary relay false close	800 years	1 year	1250
52b breaker auxiliary relay false open	800 years	1 year	1250

52b breaker auxiliary relay false close	200 years	1 year	5000
Auxiliary relay with automatic supervision and alarm. (52a contradicts current or 52a and 52b coincidence or 52a contradicts voltage)	200 years	2 days	27
Control wiring connection point (like close signal or 52a). Tested at commission but without automatic supervision[2]	5,000 years	1 year	200
Monitored CD battery and charger	100 years	1 day	27
Multifunction relay (IED), dependability-related failures	175 years	2 days	31
Multifunction relay (IED), security-related failures	2000 years. Failure rate 0.0005 per relay per year		
Human error per setting, dependability-related failures		Indefinite	7.75
Human error per setting, security-related failures	4000 years. Failure rate 0.00025 per setting per year		

[1] Reference [4] uses the same MTBF and q for CTs and PTs. Our own experience shows that secondary circuit PT failures are more common than CT failures because of some factors. CT failure consequences to personnel and equipment security are greater and field personnel have much more care with them. PT secondary is protected by fuses or molded case circuit breakers that mean an extra point of failure. We use a factor of 4 to reflect this experience.

[2] Some panel factory statistics show that wiring points have 1 failure per about 500 connection points after the first point-to-point continuity check. After functional testing, this failure rate decreases 100 times. Then a 1/50,000 failure rate after testing when the scheme is new and tested is a good estimation. After years of service a control wiring could fail for some other reason; we increase by a 10 times factor to get 5000 MTBF per wiring point.

We use these numbers to analyze security and dependability for each breaker-flashover scheme described earlier. Our top event is "Protection Fails to Clear Breaker-Flashover Failure in Prescribed Time" for dependability analysis. We shorten this to "Failure to Trip During Flashover" in our fault trees and we use unavailability numbers.

Our top event is "Protection Trips 86BF and Bus Incorrectly" for security analysis and we use failure rate numbers. This is because unexpected operations or false trips typically occur at the instant a component fails or very soon afterwards.

For some data on multifunction relays, we separate failure rates and unavailability numbers for security-related failures and for dependability-related failures. CFE observed 57 damage relays over a population of about 10,000 units with similar technology, resulting in 175 years MTBF (1998 data). Of these 57 damaged relays, only five trip incorrectly; all other failures disable the relay and alarm. For dependability-related failures we use MTBF=175 years and 2 days downtime. For security-related failures, relay failure rate is 5/10000, or MTBF = 2000 years.

For dependability, human setting-error time to detect is indefinite. Our experience with multifunction programmable relays shows that unavailability is similar to IED hardware failures. We estimate that it is equal to relay hardware unavailability. If Method E has 4 settings and is the most complex one for breaker flashover, we can assign ¼ of this unavailability per setting ($7.75 \bullet 10^{-6}$), as a way to weight settings complexity for comparison purposes.

For security-related settings errors, the time to detect is much faster because load changes, close or trip operations, or external faults could cause incorrect trip and error detection very soon after relay commission. Our experience shows that the security-related settings-error failure rate is higher than security-related relay hardware failures. We estimate a failure rate twice the failure rate of relay hardware per the Method E scheme, ¼ per setting (0.00025 failure rate).

For breaker auxiliary relays we can also separate the failure rate for open incorrect indication and for close incorrect indication. If we assume that 52a has a greater probability of false open breaker indication than of false close indication, and that 52b is the opposite, we can account for security and dependability changes with 52a to 52b change. We assume a factor of 4 times between these two opposite conditions.

Fault Tree for Method A. Residual Current and 52b

Dependability

The fault tree shows components that may contribute to dependability failure of this method. For wiring unavailability, we only consider input signal 52b. We do not consider any trip circuit between the breaker flashover scheme and 86BF or between 86BF and breakers, because these will be common to all the schemes. Our failure to trip during flashover considers all the variables related to the scheme for comparison purposes, but does not consider 86BF or other breakers in the bus failing to clear the fault.

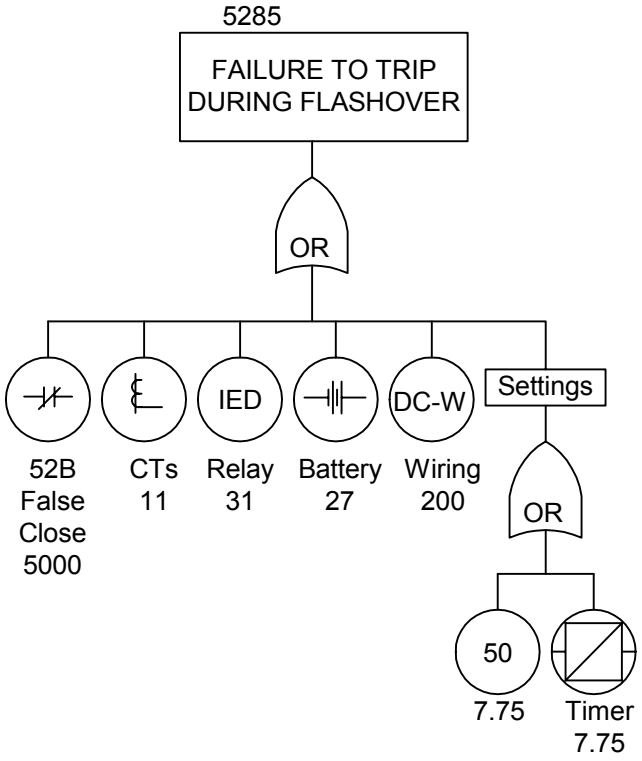

Figure 15 Unavailability •10^6 for Method A Without Automatic 52a Supervision

Security

For security we only consider failure rates of the breaker auxiliary relay, dc wiring, multifunction relay, and timer setting. We consider that the CTs, PTs, battery, and 50-element setting cannot

fail in a way that causes a false trip. An external ground failure must occur to cause scheme A to trip if 52b remains closed while the breaker is closed. If 52b does not have any kind of supervision, we assume that it could be closed enough time to coincide with ground failure. If we also assume a maintenance period of two years and downtime T=1 year, we can assume that it is almost certain that an external ground failure will occur and we can use directly the 52b failure rate.

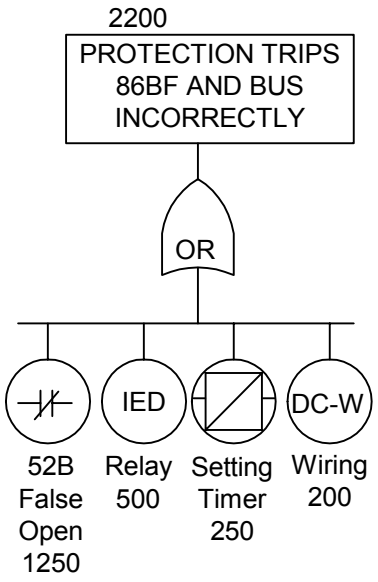

Figure 16 Security Failure Rate $\bullet 10^6$ for Method A Without Automatic 52a Supervision

Using Breaker Auxiliary 52b Instead of 52b in Method A

We evaluated changing to 52a instead of 52b for out Method A. As we expected, dependability improves and security decreases. Using Method A with 52a instead of 52b, dependability is $1{,}535 \bullet 10^{-6}$ and security is $5950 \bullet 10^{-6}$.

Adding Automatic Breaker Auxiliary Supervision to Method A

If we add any kind of automatic supervision to 52a or 52b and its dc wiring, for example, 52a contradicts 52b, or 52a contradicts current, a 52a failure will be quickly detected and fixed. If we assume downtime of two days, unavailability decreases from $1250 \bullet 10^{-6}$ to $27 \bullet 10^{-6}$. The probability of dependability failure decreases from $1535 \bullet 10^{-6}$ to $312 \bullet 10^{-6}$.

With this same assumption, we can estimate that the probability that an external ground fault will coincide with 52a false close indication is very low. If we use directly the 52a failure rate for the case without automatic supervision and with a one-year downtime, we can assume that with automatic supervision that probability is 2/365 times smaller. An external ground fault must occur in the two days following a 52a failure to cause a false trip. The improvement in security is outstanding; the probability of a false trip decreases from $5950 \bullet 10^{-6}$ to $778 \bullet 10^{-6}$.

Fault Tree for Method B, Phase Current and 52a Per Phase

Dependability

Dependability for this method will be exactly the same as that of Method A with three advantages:

- Directly targets the failed phase
- Covers the rare case of three-phase flashover
- Could be applied to single-pole-trip breakers

Security

This method is not applied in practice because security is very low. We need to take into consideration the same conditions we use for Method A, plus the probability of a 52a false open indication or a normal breaker close with load. Although we use automatic supervision for the breaker auxiliary, if 52a fails during the breaker close, it will cause a false trip. We use the 52a failure rate directly to estimate the probability of security failure with this scheme

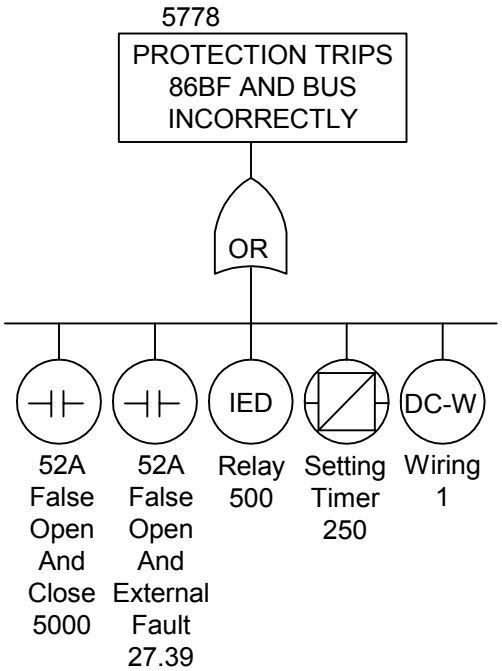

Figure 17 Security Failure Rate •10^6 for Method B With Automatic 52a Supervision

Fault Tree for Method C, Close Monitoring and Coincidence Timers

Dependability

Method C dependability is the same as that with Method A or B. We add close signal, coincidence timers, and some logic. Extra logic and timers (without more settings) do not increase unavailability because we are evaluating only multifunction digital relays and this extra component's unavailability is included in relay unavailability. Close signal could not fail in a way that causes a dependability failure. Our result is the same fault tree and 1535•10^6 unavailability without 52a automatic supervision or 312•10^{-6} unavailability with it.

Security

Method C can be applied to single-pole-trip breakers, covers three-phase flashover, and is secure, because it will not fail and trip the bus incorrectly unless both 52a and the close signal fail simultaneously during a close operation. It will not trip if 52a fails later because of coincidence timers. Automatic 52a supervision becomes less important because 52a failure is no longer the most probable cause of security failure.

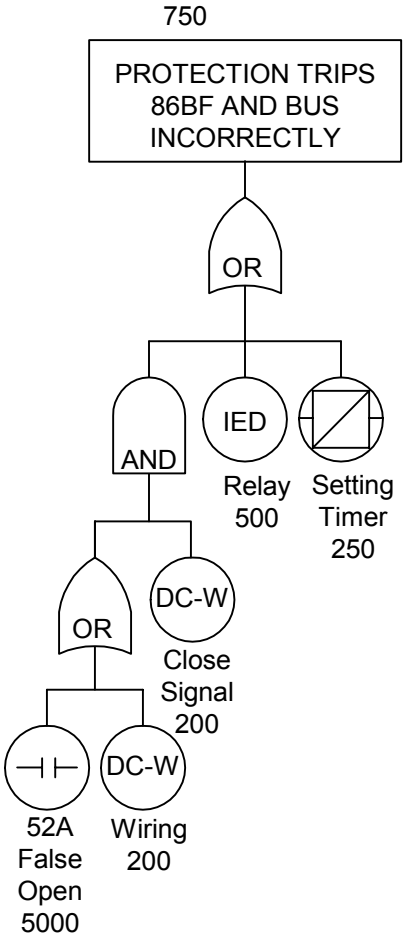

Figure 18 Security Failure Rate $\bullet 10^{6}$ for Method C Without Automatic 52a Supervision

Fault Tree for Method D, Close Monitoring, Coincidence Timers, and Live-Voltage Supervision

Dependability

Method D dependability is lower than other methods. The fault tree is similar to that for Method C, but we add two more unavailability components: PTs and one more setting. This results in $1587 \bullet 10^{6}$ unavailability without 52a automatic supervision or $364 \bullet 10^{-6}$ with it.

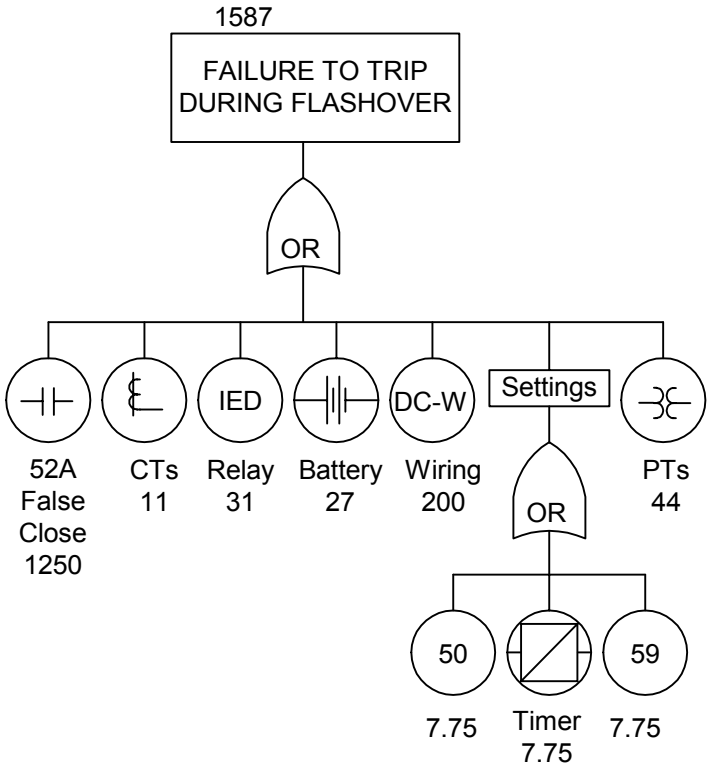

Figure 19 Unavailability •10^6 for Method D Without Automatic 52a Supervision

Security

The Method D security failure rate fault tree is the same as that of Method C. Live voltage supervision does not add any security because settings must be too low and it will be active almost all the time, with normal load and with several fault conditions. On the other hand, there are no security related failures caused by this element.

Fault Tree for Method E, Voltage at Both Sides of the Breaker

Dependability

This method adds the probability of failure caused by PT unavailability and by more settings, but eliminates breaker auxiliary and dc wiring related unavailability. The total result is that this method shows the best dependability if we consider that both sets of three-phase PTs have some method of automatic supervision and a downtime of two days. This supervision could be in the form of alarms as 52a contradicts voltage difference, as current contradicts voltage difference, or from other methods based on changes of voltage or current-sequence components.

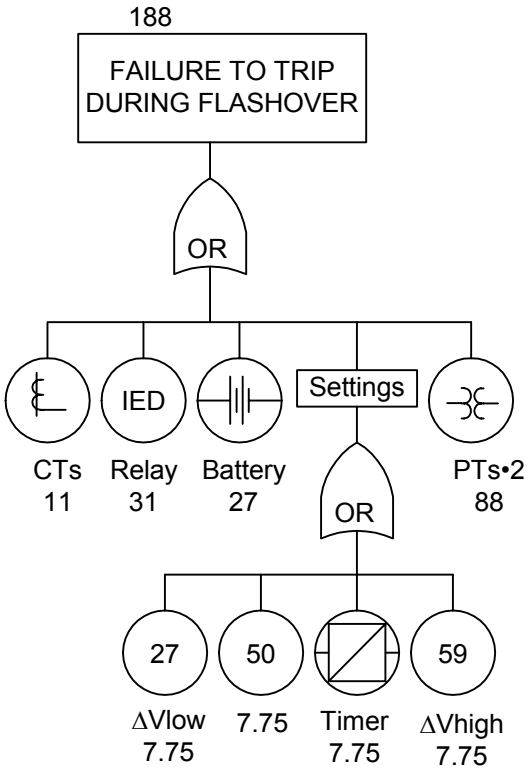

Figure 20 Unavailability •10^6 for Method E

Security

One source of failure rate in this method is a failure of the close signal. If this signal fails and there is a normal close, it will trip the bus incorrectly. Fortunately, this is a very simple component and we assume its failure rate to be equal to any other CD wiring point. This method also adds more settings.

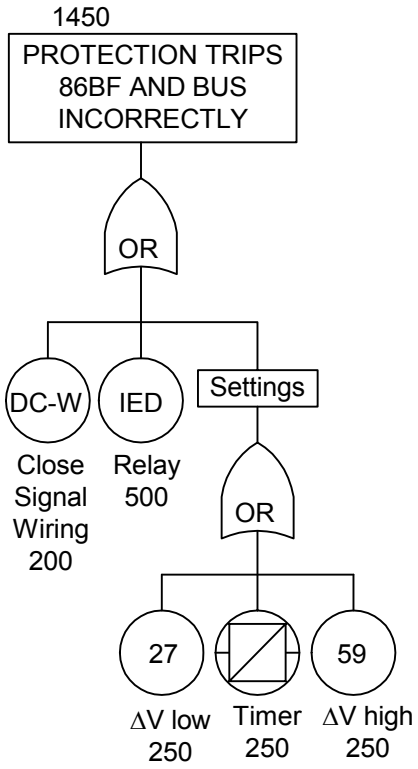

Figure 21 Security Failure Rate •10^6 for Method E

Table 4 Results of Comparison Between Breaker-Flashover Methods

Breaker-Flashover Protection Method	Unavailability •10^6 (Probability of Dependability Failure)	Security Failure Rate•10^6	Observations
A, Residual current and breaker auxiliary contact 52b	5285 (worst)	2200	Do not apply for 3 phase flashover or single pole trip and reclose breakers
A, Residual current and breaker auxiliary contact 52a	1535	5950 (worst)	Do not apply for 3 phase flashover or single pole trip and reclose breakers
A with automatic 52a supervision and alarm	312	778	Do not apply for 3 phase flashover or single pole trip and reclose breakers
B, Phase current and breaker auxiliary contact per phase	1535	5950 (worst)	
B with automatic 52a supervision and alarm	312	5778	
C, phase current, breaker auxiliary, close monitoring and coincidence timers	1535	750 (best)	
C with automatic 52a supervision and alarm	312	750 (best)	Security does not depend on downtime of 52a

D, same as C with live-voltage supervision	1587	750 (best)	
D, with automatic 52a supervision and alarm	364	750 (best)	
E, phase current, voltage difference, and close monitoring	188 (Best)	1450	Needs three-phase voltage on both sides of the breaker.

CONCLUSIONS

1. Breaker-flashover failures are not cleared quickly enough by generator, line, transformer, or conventional breaker-failure schemes to avoid equipment and system damage. They can cause severe damage and high failure costs.
2. A dedicated breaker-flashover scheme is a must for breakers used to synchronize systems or generators, or for those used to switch long high-voltage lines. It could also be used on any breaker.
3. There are several methods for implementing breaker-flashover protection. Decisions should be based on the equipment needed to implement and on reliability. It is possible to use existing multifunction digital generator or transmission substation relays to implement protection.
4. Method A, described in IEEE C37.102, uses residual current and breaker auxiliary position has lower dependability and security than other methods if applied without automatic breaker auxiliary supervision. It cannot be applied in single-pole operation breakers without decreasing dependability and does not cover three-phase faults. If it is modified to use phase current instead of residual current to cover single-pole trip-and-reclose breakers, security is worse.
5. Method C, based on phase currents, close monitoring, and coincidence timers has a very good dependability and security compromise and could be applied to any breaker. Security is the best and dependability is very close to the best if used with automatic auxiliary contact supervision.
6. Method D, using live-voltage supervision, has low dependability and does not improve security over Method C. We do not recommend its use.
7. Method E, using voltage at both sides of the breaker, has the best dependability. Security is lower than Method C, but still good in the same order of magnitude.
8. Methods based on breaker auxiliary contact, such as methods A and C, improve dramatically if some kind of automatic breaker auxiliary supervision is applied. This supervision could be the use of 52a and 52b contacts, current contradicts 52a alarm, or any other way to notice and quickly fix problems with this signal. Method A, recommended by IEEE C37.102, shows almost the best possible security and very good dependability applying a 52a alarm. For this particular method, a 52a alarm is vitally important.
9. Present technology allows us to use multifunction intelligent electronic devices to protect and monitor breakers in all their possible operation states, increasing both breaker and system reliability.

REFERENCES

[1] IEEE C84.1-1989: Voltage Ratings for Electric Power Systems and Equipment (60 Hz).

[2] IEEE C37.06-1987: AC High-Voltage Circuit Breakers Rated on a Symmetrical Current Basis—Preferred Ratings and Related Required Capabilities.

[3] IEEE C37.013-1993: IEEE Standard for AC High-Voltage Generator Circuit Breakers Rated on a Symmetrical Current.

[4] IEEE C37.09-1979: IEEE Standard Test Procedure for AC High-Voltage Circuit Breakers Rated on a Symmetrical Current Basis.

[5] IEEE C37.102-1987: IEEE Guide for AC Generator Protection.

[6] E.O. Schweitzer, III, B. Fleming, T.J. Lee, and P.M. Anderson, "Reliability Analysis of Transmission Protection Using Fault Tree Methods," Proceedings of the 24th Annual Western Protective Relay Conference, Spokane, Washington, October 21–23, 1997.

[7] G.W. Scheer, "Answering Substation Automation Questions Through Fault Tree Analysis," Proceedings of the 4th Annual Texas A&M Substation Automation Conference, College Station, Texas, April 8–9, 1998.

BIOGRAPHIES

Ramon Sandoval is a Protection Engineer for Comisión Federal de Electricidad at Topolobampo Thermal Power Station. He has worked for CFE since 1992 in electrical maintenance of power and industrial equipment such as induction motors, synchronous generators, breakers, AVRs, and step-up transformers. For the last five years he has been a power station protection engineer, installing, testing, and using different types of protective equipment commonly used in industrial plants and power systems. This includes a variety of electromechanical, static, and digital multifunction relays. He received training in power system modeling and simulation from LAPEM using ATP and has worked developing field procedures for protective relay testing using power system simulators and transient simulation software.

Jean Leon Eternod is a field application engineer for Schweitzer Engineering Laboratories at Mexico City. Prior to joining SEL in 1998, he worked for the Comisión Federal de Electricidad Power Systems Studies Office in protection and control corporate management. While with CFE from 1991 to 1998, he worked with wide-area network protection schemes, single-pole trip and reclose studies, and database validation for short circuit, load flow and dynamic simulation. He received his BSEE from the National Autonomous University of Mexico (UNAM), where he also completed postgraduate coursework in power systems. He received training in power system simulation from Power Technologies Inc. He has delivered technical papers for the summer meeting of the Mexican chapter of IEEE, Monterrey's Iberoamerican Protections Symposium, AMIME Rotating Machinery Conference, WPRC and Texas A&M protective relay conferences in the fields of power systems protection, simulation, and synchronized phasor measurement applications.

20040930
TP6183

Back to Table of Contents