IDENTIFYING PLAUSIBLE CASCADING EVENTS IN SYSTEM STABILITY ASSESSMENT

Bogdan OTOMEGA[1*], Thierry VAN CUTSEM[2]

An implementation of the event tree approach is proposed to determine possible sequences of cascading failures with severe impact on a given power system. The algorithm takes into account protection systems hidden failures and transmission system equipments overload. At each level of the event tree development, the sequence probability order is computed and a filtering tool is used to identify possible harmful sequence. These are furthermore analysed with a time domain simulation tool in order to assess their impact on the power system. This paper contains the description of the event tree algorithm as well as examples of its practical application on the Nordic32 test system.

Keywords: cascading failure, hidden failure, event tree.

1. Introduction

Power system are designed and planned to withstand predetermined disturbances. However, the impact of an initial disturbance may be aggravated by other sources of vulnerability such as human errors, system topology changes, protection/control system failures, power flow changes due to electricity market, missing or erroneous system information when taking important decisions, or communication network failures when sending critical control signals. Thus, under these conditions the power system may become vulnerable, and cascading events could develop which may lead to separation of the power system into islands and results in the loss of a substantial amount of load.

Due to their low occurrence probability, cascading failure events are not taken into account when designing the control and protection systems. Thus, these systems are unable to maintain or restore system stability in this unanticipated and complex situations.

However, cascading failures in large-scale electric power systems are an important cause of the latest blackouts experienced all over the world [1-3]. In recent years this type of incidents seem to increase in frequency and severity,

[1] PhD student, Department of Electrical Engineering and Computer Science (Montefiore Institute), University of Liege, Belgium (*Corresponding author)
[2] Research Director – Fund for Scientific Research (FNRS), Department of Electrical Engineering and Computer Science, (Montefiore Institute), University of Liege, Belgium

possibly due to the complex environment brought about by the electric industry deregulation. In the same time, the economic penalties associated with such events are increasing as the society is heavily dependent on the availability of high-quality power supply. The fact that the consequences of these cascading events could be very severe and that the simple equipments failure combination produces a combinatorial explosion, were the motivations to build an algorithm meant to identify plausible severe cascading events that could be used for security assessment.

2. Protection systems and hidden failures

Protection systems are designed to initiate switching actions to rapidly and reliably isolate faults. Standard designs ensure the reliability of a fault isolation at the expense of some small likelihood of false trips. This approach minimizes component system damage and is appropriate when the system is in a normal operating state.

The main drawback is that, in general, these relays take actions to protect a localized region of the network without considering the impact on the whole network [4]. For example, under power system stress conditions, due to outages or excessive loading, additional switching to isolate faults will cause additional stress that may contribute to widespread system failures. Moreover, if the switching is due to an incorrect relay operation, the protection system contribute to power system weakening.

The failures of generating units, transmission lines, transformers and other power system components can be grouped into the following categories [5]:

- ***Independent outages***, when the outage of each equipment is caused by an independent fault. Independent outages of two or more elements are referred to as overlapping or simultaneous independent outages. The probability of such an outage is calculated as the product of individual equipments failure probability.
- ***Dependent outages***, when the outage is the result of the occurrence of one or more other outages. Dependent outages are the protection systems response to the changing system parameters due to what previously happened in the power system. An example is the incorrect operations of 3rd zone relay observing high currents and low voltages under stress conditions. The probability of such an outage can be approximated, due to their low probability, with the product of the failure probabilities of each equipment as if there were independent.
- ***Common-cause outages*** are outages having an external cause with multiple failure effects, where the effects are not consequences of each other. An example is the primary protection failure followed by the back-up protection clearing, which disconnects more equipments. The effect of common-cause outages on reliability indices can be significant and comparable with the effect of

N-2 or higher-order outages. The probability of a common-cause outage is larger than the probability of independent outages resulting in a similar event.

- ***Station originated outages*** can occur due to a ground fault on the breaker, a stuck breaker, bus faults or a combination of these outages. This can produce the outage of two or more transmission elements and/or generating units, which are not necessarily on the same right-of-way. The bus-bar fault is one of the well-known station originated outages, all transmission or generation components connected to that specific bus-bar being tripped.

Among the incorrect relay operations, a common scenario exists: the relay has an undetected defect that remains dormant until abnormal operating conditions are reached. This is often referred as ***hidden failure*** [6].

In [7] the protection system hidden failure is defined as a permanent defect that will cause an individual relay or a relay system to incorrectly and inappropriately remove system components as a direct consequence of another switching event. In order a relay failure to be considered as hidden failure, one must be able to monitor the defect which led to relay misoperation with an appropriate supervision system. A failure that results in an immediate trip without any prior event is not considered a hidden failure, because the power system is designed to withstand the loss of any component (N-1 criterion).

In general hidden failures are of two kinds [8]:

- ***software failures***: the protection system settings are inappropriate or outdated for the prevailing system conditions. Consequently, although the relay functions correctly, in effect it has a hidden failure because of the inappropriate setting. This category may include human errors or negligence [9];
- ***hardware failures***: actual failure in the relay.

In sequel are presented the normal functioning and the possible failure modes of the directional comparison blocking scheme, which is one of the most popular protection schemes for protecting HV and EHV transmission lines. The one-line diagram and the schematic control logic are presented in Fig. 1.

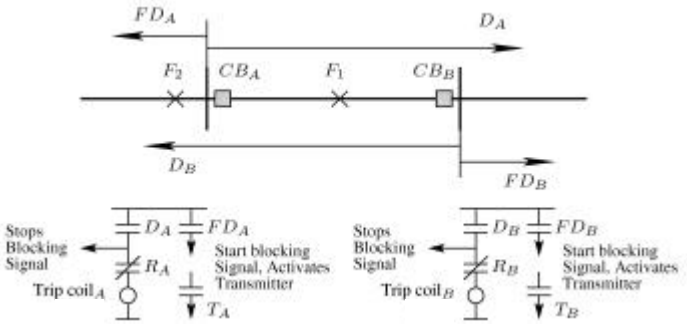

Fig. 1. One line diagram and schematic logic of the directional comparison blocking scheme

The usual sequence of actions for a fault in the protected area, e.g. F_1, is the following: the directional relays D_A and D_B are picking up the fault and close their normally open contacts. The fault detectors FD_A and FD_B do not see the fault, thus their respective transmitter T_A and T_B do not send the action blocking signal, the receiver relays R_A and R_B remain closed. Consequently, the line is instantaneously cleared from both ends by opening the respective circuit breakers CB_A and CB_B.

For a fault situated outside the protected line, e.g. F_2, the fault detector FD_A picks up the fault and gives the permission to transmitter T_A to start sending the action blocking signal. The receiver relay R_B opens his normally closed contacts and avoids the opening of the circuit breaker CB_B.

Table 1. presents the possible hidden failures of the directional comparison blocking scheme leading to incorrect trip.

Table 1

Failure modes of the directional comparison blocking scheme

Hidden failure	Effect	Consequence
The FD cannot be activated	No action blocking signal	Line trip from one end
T blocked	No action blocking signal	Line trip from one end
D continuously activated	Override action blocking signal	Line trip from one end
R cannot receive signal	Receiver relay remains closed	Line trip from one end
R continuously activated	Receiver relay always open	Line does not trip from both ends
CB contacts stuck	CB could not open	Line does not trip from both ends

3. Using event trees to model cascading outages

Event trees are structures which starting from an "undesired initiator" can describe a chronological sequence of events. Each new event depends on what previously happened and for each new possible event considered, a new branch and a node are added in the tree, with the associated probability.

The functioning of the protection systems as well as the development of a cascading outage can be described by a sequence of dependent events. If in the first case the sequence is governed by the time delays used to initiate/inhibit protection actions, in the second case the disconnection of power system equipments sequence is uncontrolled and depends on previous events and their impact on the power system and the time delays of different protection systems. In both cases the event tree is a suitable structure to model the sequence of events.

Such an event tree structures were used in order to model the protection failure scenarios, including stuck breaker events [10] or hidden failures [11]. Also, the algorithm presented in [12] can be seen as an event tree for power system equipment overloads.

The first two steps in Fig. 2. diagram represent the reduced form of a protection system event tree, where the upper branch represents the sequence of events leading to the normal clearing (NC) of the fault and the lower branch

includes all possible sequences corresponding to hidden failures (see Table 1.) resulting in protection system clearing failure (CF).

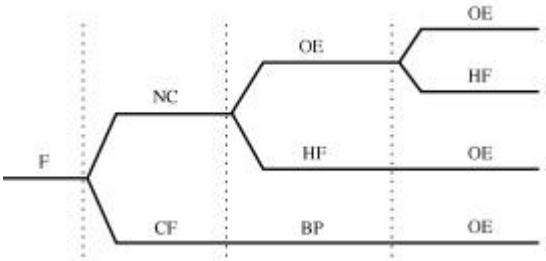

Fig. 2. Cascading outage event tree

As illustrated in Fig. 2., starting from the action of the primary protection, the model of a cascading outage event tree can be developed. The events taken into account when expanding the event tree could be classified into:

- ***overloaded equipments trip*** (OE). This category includes the tripping action of transmission lines due to high current and of reactive power limited generators due to low voltage. The associated probability to this event is $p_1=1$;
- protection system ***hidden failures*** (HF), which includes both software and hardware failures. For example we consider inadvertent trip of transmission lines approaching limits or limited generators, due to inappropriate settings, and, respectively, relay malfunction (e.g. 2^{nd} and 3^{rd} zone relay). Depending of the hidden failure type, the associated probability, p_2, can be determined using linear or exponential functions or approximated with the standard component unavailability;
- ***back-up protection action*** (BP), which may disconnect more than one equipment. For example, in the stuck breaker case the back-up protection may disconnect all equipments connected to the same bus-bar as the faulted one. The probability of this event, p_3 (which can be approximated as the product between the probability of the initial fault and the hidden failure probability), is greater than the probability of independent outages resulting in a similar event.

Taking into account the probabilities associated to each branch of the event tree, results that, we can compute the probability of each sequence. To this purpose the rare event probability approximation is usually made [13]. The main idea of this approximation is that probabilities of the independent events considered in the sequence have very small values and almost same magnitude order. Therefore, the high order terms in the probability polynomial expression can be omitted. It results that, a probability order can be associated to each sequence. The smaller the probability order the greater the occurrence probability.

Referring to Fig. 2., the probability of the 3^{rd} sequence from the top can be written as $p_f p_2 p_1$, where p_f is the probability of the initial fault. Appling the rare

event probability approximation, $p_f=p_2=P$, the sequence probability can be computed as P^2, since $p_1=1$. Thus, the probability order of the sequence is 2.

4. Cascading outage determination algorithm

Considering the cascading outage event tree model, Fig. 2, an algorithm to identify plausible cascading events can be developed including the following steps:

1. Apply the initial disturbance to the initial state of the power system and draw up the list of next possible disturbances, including both software and hardware hidden failures related to the initial disturbance. During the event tree expansion this list will be updated in order to include overloaded system components and the possible software hidden failures of components approaching their limits.

2. Apply a disturbance from the list determined at previous step. Priority is given to equipments exceeding limits (overloaded lines, reactive limited generators), if any, as their probability is equal to 1. More than one disturbance will be applied at once only if they have a common cause, see the back-up protection action. Even if methods as the ones presented in [6,7] consider the possibility of more than one hidden failure per sequence, due to their very low probability, we consider only one per sequence, as in [14]. Furthermore, we consider hardware hidden failures revealed only by the initial fault. If a specific sequence includes already a hidden failure and the list of possible disturbances does not contain an overloaded equipment the sequence expansion is stopped.

3. Classify the sequences into harmless or potentially harmful. To this purpose we use a procedure based on voltage drop estimates computed with linear approximation methods, detailed in [15]. The sequences are flagged as potentially harmful if the post-contingency voltage drops are larger than a specified threshold value.

4. Compute the probability order of the sequences using the rare event probability approximation. For the sequences flagged as harmless, if the probability order is smaller than a predefined threshold, then the algorithm proceeds with Step 2, else the sequence development is stopped.

5. Analyze the potentially harmful sequences with Quasi Steady-State (QSS) time simulation [18] in order to assess the sequence severity. If the system behavior is unstable the development of that specific sequence is stopped. If the system is stable and if the sequence probability order is smaller than the threshold, then go to Step 2, otherwise stop the sequence development. During the time simulation, overloaded lines and reactive limited generators are added to the list of possible disturbances (with probability *1* of occurrence), as well as the transmission lines or the generators approaching or reaching limits (with

probability p_1). Afterwards, when a sequence involving such tripping is analyzed with QSS simulation, the equipment is tripped only after it gets overloaded or limited, with or without a temporization.

The resulting cascading events can be divided with respect to the power system behavior into stable and unstable sequences. In the former case we can compute the security margin, while in the latter case we can determine which are the corrective actions, e.g. amount of load shedding. These parameters can be used in order to rank the resulting cascading outages and also to identify weak areas.

5. Algorithm results

The proposed algorithm has been tested on the Nordic32 test system used by a CIGRE Task Force on Long-term Dynamics. The data can be found in [19] while the one-line diagram is shown in Fig. 3.

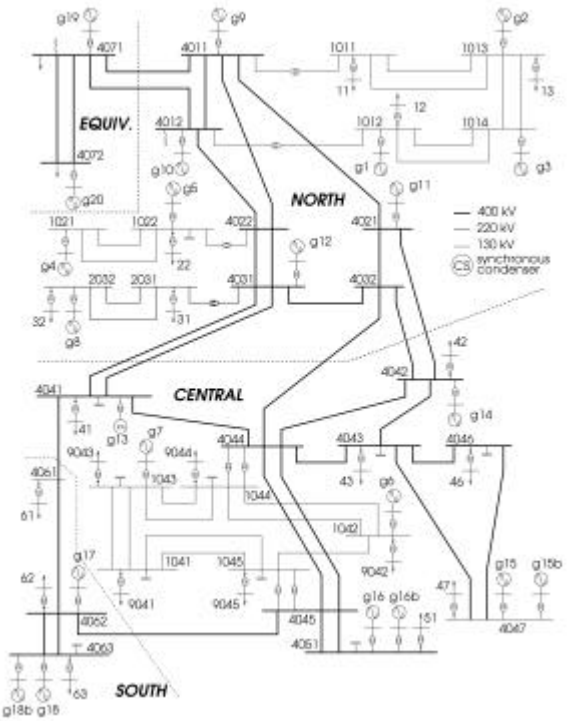

Fig. 3. Nordic32 test system

The model includes 55 buses, 23 generators and 22 voltage-sensitive loads. We have assumed for all buses a double bus-bar configuration, with the power flows balanced as much as possible on the two bus-bars. In the nodes were both load and generation are connected, we considered them connected to the

same bus-bar. Hence, when considering a stuck breaker situation less equipments are tripped by the back-up protection and the power imbalance is less severe.

Table 2. presents a summary of the results obtained starting from a list of 155 initial disturbances, including all branches and generators. The criterion to accept a system time evolution was that all transmission voltages remain above 0.85 pu.

Table 2

Summary of the algorithm results

	Total number	Prob. order 1	Prob. order 2	Prob. order 3
All scenarios	714	5	457	252
Unstable	571	5	314	252
Stable	143	-	143	-

As can be seen, a number of 714 sequences were retained, out of which 571 represent unstable scenarios, with different probability orders. The remaining are scenarios with stable voltage evolution but resulting in lost load. Note that, some scenarios include the same disturbances but the sequence is different. Thus, the above figures should be corrected in order to count them only once.

Furthermore, at the considered operating point the system is very stressed and cannot withstand the loss of generators g6, g14, g15, g15b and g16, which are correctly identified by the algorithm as probability order 1 sequences. A great part of the unstable scenarios include these generators, mostly g6 and g14 located close to the load area.

Figure 6. presents the voltage evolution at the most affected buses in a probability order 3 case. The initial disturbance, is the loss of line 4021-4042, followed by the false trip of 4043-4042. This causes the field current of generator g7 to get limited and after a temporization of 60 s (the value was chosen for figure legibility reasons) is tripped. After the loss of g7, two more generators get limited, namely g14 and g6.

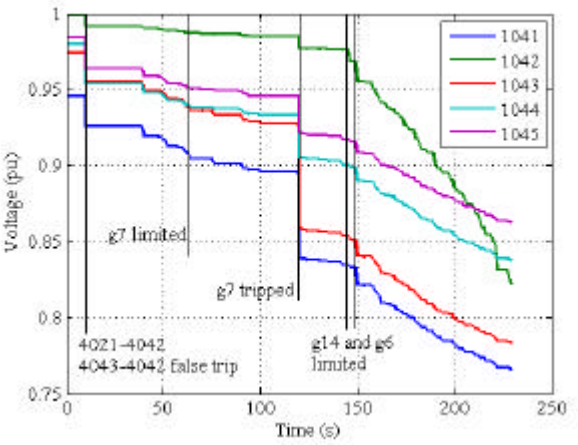

Fig. 6. Voltage evolution and cascade sequence

6. Conclusions

This paper outlines the implementation of an event tree based algorithm to identify plausible cascading events. The even tree development considers various events such as hidden failures and overloaded equipments trippings. The resulting cascading scenarios can be used in system stability assessment studies as well as to devise system protection schemes.

The proposed scheme has been successfully tested on the small Nordic32 test system. As of writing this paper, promising results have been obtained on the model of a real-life system.

REFERENCES

[1]. *U.S. - Canada Power System Outage Task Force*, Final Report on the August 14, 2003 Blackout in the United States and Canada: Causes and Recommendations, Apr. 2004, Available online: http://www.nerc.com.

[2]. *UCTE*, Final Report of the Investigation Committee on the 28 September 2003 Blackout in Italy, Apr. 2004, Available online: http://www.ucte.org.

[3]. *C. Vournas*, Technical Summary on the Athens and Southern Greece Blackout of July 12, 2004, Aug. 2004, Available online: http://www.pserc.org.

[4] *J.C. Tan, P.A. Crossley, P.G. McLaren, P.F. Gale, I. Hall and J. Farrell*, "Application of a wide area back-up protection expert system to prevent cascading outages", Proc. of IEEE Power Engineering Society Summer Meeting, vol. 2, pages 903-908, July 2001.

[5] *M.S. Grover and R. Billinton*, "A computerized approach to substation and switching station reliability evaluation", Proc. of IEEE Power Engineering Society Winter Meeting, Jan. 27 - Feb. 1, 1974.

[6] *S. Tamronglak, S.H. Horowitz, A.G. Phadke and J.S. Thorp*, "Anatomy of power system blackouts: preventive relaying strategies", IEEE Transaction on Power Delivery, vol. 11, issue 2, Apr. 1996.

[7] *A.G. Phadke and J.S. Thorp*, "Expose hidden failures to prevent cascading outages in power systems", IEEE Computer Applications in Power, vol. 9, issue 3, pages 20-23, July 1996.

[8] *A.G. Phadke*, "Hidden failures in protection systems, security and reliability in a changing environment", Proc. of Bulk Power Systems Dynamics and Control, Onomichi, Japan, Aug. 2001.

[9] *D.C. Elizondo, J. de la Ree, A.G. Phadke and S. Horowitz*, "Hidden failures in protection systems and their impact on wide-area disturbances", Proc. of Power Engineering Society Winter Meeting, 2001.

[10] *Q. Chen and J.D. McCalley*, "Indentifying high risk N-k contingencies for on-line security assessment", IEEE Transactions on Power Systems, vol. 20, issue 2, pages 823-834, May 2005.

[11] *D.P. Nedic*, Simulation of large system disturbances, PhD Thesis, University of Manchester Institute for Science and Technology, December 2003.

[12] *I. Dobson, B.A. Carreras and D.E. Newman*, "Probabilistic load-dependent cascading failure with limited component interaction", Proc. of IEEE International Symposium on Circuits and Systems,Vancouver, Canada, May 2004.

[13] *Q. Chen and J.D. McCalley*, "A cluster distribution as a model for estimating high-order event probabilities in power systems", Proceedings of the International Conference on Probabilistic Methods Applied to Power Systems, pages 622 – 628, 12-16 Sept. 2004.

[14] *D.S. Kirschen and D.P. Nedic*, "Consideration of hidden failures in security analysis", 14th Power Systems Computation Conference, Sevilla, 24-28 June 2002

[15] *B. Otomega and T. Van Cutsem*, "Fast contingency filtering based on linear voltage drop estimates", Proc. of the IEEE PowerTech conference, St. Petersburg, Russia, 2005.

[16] *T. Van Cutsem and C. Vournas*, Voltage Stability of Electric Power Systems, Boston, Kluwer Academic Publishers (now Springer), 1998.

[17] *CIGRE Task Force 38.02.08 (M. Stubbe, convenor)*, Long-term dynamics - Phase II, Final report, January 1995.