Searching for Plausible N-k Contingencies Endangering Voltage Stability

Tilman Weckesser
Dept. Electrical Engineering & Computer Science
University of Liège, Belgium
E-mail: j.weckesser@ulg.ac.be

Thierry Van Cutsem
Fund for Scientific Research (FNRS)
University of Liège, Belgium
E-mail: t.vancutsem@ulg.ac.be

***Abstract*—This paper presents a novel search algorithm using time-domain simulations to identify plausible $\mathbf{N-k}$ contingencies endangering voltage stability. Starting from an initial list of disturbances, progressively more severe contingencies are investigated. After simulation of a $\mathbf{N-k}$ contingency, the simulation results are assessed. If the system response is unstable, a plausible harmful contingency sequence has been found. Otherwise, components affected by the contingencies are considered as candidate next event leading to $\mathbf{N-(k+1)}$ contingencies. This implicitly takes into account hidden failures of component protections. The performance of the proposed search algorithm is compared to a brute-force algorithm and demonstrated on the IEEE Nordic test system.**

***Index Terms*—N-k contingencies, cascading outages, protection hidden failures, voltage instability, time-domain simulation.**

I. Introduction

Today's power systems are increasing in size and complexity. Due to forces such as the globalization of electricity market, where an increasing share of power is traded across national and regional borders, individual (e.g. national) power systems have stronger interactions with their neighboring systems. Moreover, the increasing demand, the integration of distributed generation from fluctuating energy sources and delays in the reinforcement of the grid due to public objection result in more frequent operation of the power system closer to its limits. This may trigger cascading events, due to e.g. component overloading.

In order to ensure uninterrupted power delivery, system protection designers need to develop effective, automatic emergency control schemes (also referred to as System Integrity Protection Schemes - SIPS) against those rare but much impacting events. For that purpose, identification of plausible $N-k$ contingencies is crucial.

Since brute-force approaches for determining harmful $N-k$ contingencies are infeasible, due to the bare number of possible contingencies and their combinations, there is a need for efficient tools and methods to identify plausible harmful contingencies. In 2008 the IEEE PES CAMS Task Force on "Understanding, Prediction, Mitigation and Restoration of Cascading Failures" published an initial review of methods for cascading failure analysis [1]. In this paper, the Task Force concludes that the currently available methods for understanding and mitigating are not yet well developed.

The methodology presented in [2], [3], [4] consists of identifying plausible cascading events following an initial disturbance. First a fault is simulated in the system and, subsequently, a cascading outage event tree is constructed. In this tree, different cases are investigated. The first fault may be cleared normally or a clearance failure may take place. Cascading events can on the one hand be hidden failures, such as outdated protection settings or equipment failure, and on the other hand tripping of overloaded equipment. Probabilities are assigned to the individual events applying the rare event approximation technique. In [4], a branch of the event tree is explored using quasi-steady-state time simulation until the probability of the event sequence drops below a threshold or unacceptable system conditions were identified.

An approach applying the fault chain theory from security sciences to assess the power system's vulnerability was proposed in [5]. A degree of vulnerability is determined for transmission lines and sections in a power system based on a new vulnerability index.

The authors of [6] developed a "Random Chemistry" algorithm to identify minimal $N-k$ contingencies, which trigger large cascading failures. Their approach is based on the observation that a relatively small number of components contribute disproportionately to system vulnerability. The general idea is to randomly pick a large set of contingencies S_0, which causes cascading failures, and find the smallest subset S_m, which still causes cascading failures. For that purpose, random subsets of S_0 are simulated. If the subset still causes system failure, then S_0 is replaced by it. This process is continued until a subset with desired size k_{max} is found. Following, a pruning approach is applied, which removes individual contingencies from the subset and checks if a system failure still occurs.

In [7], the authors present a method, which utilizes data from many cascading failure simulations to determine an influence graph. This graph provides information on how cascades evolve in a particular system. The authors showed that outages propagate non-locally and that their method allows to quickly identify modifications that will reduce cascade propagation.

A method for identifying high risk $N-k$ contingencies based on network topology was presented in [8]. The authors propose to reduce the complexity and size of the system by converting it into a graph, where the nodes are functional groups and the edges are interfacing components. Here, a func-

tional group is made up of components which operate and fail together due to the connection structure and protection scheme. Interfacing components are breakers and open switches. Then high-risk $N-k$ contingencies are identified based on rare event approximation and event trees. The authors claim that the method captures most $N-k$ contingencies that are related to protection malfunctioning.

In [9], the authors propose an algorithm to online identify an event sequence, which may lead to a catastrophic failure. For that purpose, probable contingency sequences are investigated offline using power flow computations. The results are stored and used online to identify a collapse sequence relying on pattern recognition and fuzzy estimation.

The recent publication [10] reviews a number of existing methods and evaluates them with respect to their suitability for real-time applications.

In this paper, a new method is proposed, which aims at identifying plausible and harmful $N-k$ contingency sequences using time-domain simulations. The method tends to provide sequences with a small value of k, such that the system experiences instability. Individual contingencies added to a given sequence of disturbances involve equipment impacted by that sequence, which implicitly takes into account hidden failures of component protections.

The rest of the paper is structured as follows. In Section II-A, the search algorithm and its implementation into a parallel processing environment are presented. Results obtained from simulations of the IEEE Nordic Test System are shown in Section III. Finally, Section IV offers some concluding remarks.

II. Identification of plausible and harmful N-k contingencies

A. Detailed procedure

A block diagram of the proposed search algorithm is shown in Fig. 1. The input is a time-domain model of the power system and an initial selection of contingencies.

In the following, the proposed algorithm is described in more detail for the identification of harmful $N-k$ contingencies causing long-term voltage instability. However, it should be noted that the algorithm can easily be adapted to deal with other instability mechanisms. L is a list of $N-k$ contingencies, which is initialized with the aforementioned selection of initial contingencies. As long as this list is not empty, the method extracts the next entry C_i and performs a time-domain simulation beginning from the initial system operating point and applying the individual disturbances $c_m \in C_i$ consecutively, with a short-delay Δt in between them. During the time-domain simulation, the system state is monitored and the simulation is terminated if an instability is identified. Depending on the instability mechanism, different system states are monitored, e.g. for long-term voltage instability the bus voltages are monitored and compared to a threshold. Moreover, the model may include protective relays, which monitor certain system quantities and disconnect components to avoid e.g. under- or over-speed of synchronous machines etc. Thus, the response of

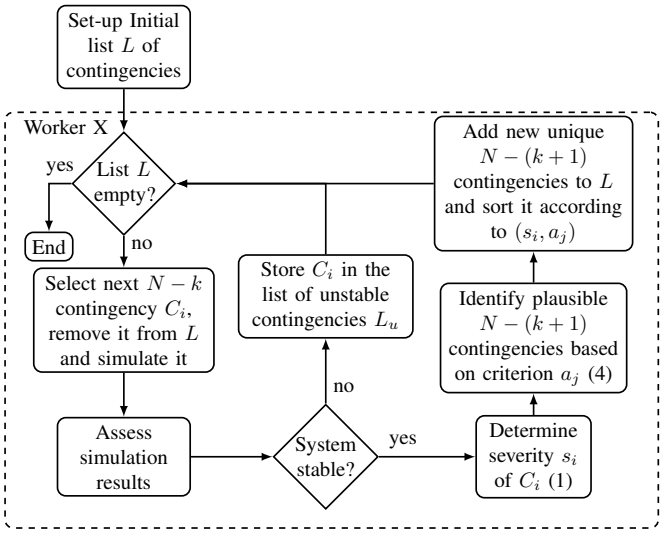


Fig. 1. Block diagram of the proposed search algorithm

protective relays can result in cascading tripping of additional components. At the end of the simulation, the obtained results are assessed to determine if it terminated normally and a new stable operating point was reached or if an instability was detected. If the contingency sequence C_i led to an instability, C_i is stored in the list of unstable contingencies L_u. However, if the system remained stable after C_i was applied and the number of individual contingencies k_i in C_i is smaller than a pre-defined maximum number k_{max}, then the severity s_i of C_i is computed and candidate k_i+1 contingencies are identified. How the severity of a contingency sequence is analyzed, depends on the instability mechanism with respect to which the system's vulnerability has to be assessed. In case of long-term voltage stability, it makes sense to consider the depression of the bus voltage magnitudes. Hence, the following severity index is proposed in this paper.

$$s_i = \frac{1}{k_i} \sum_{b \in B} [\max(0, V_b(t_0) - V_b(t_e))]^2 \qquad (1)$$

where B are all buses in the system, t_0 the time at the beginning of the simulation and t_e the time at the end of the simulation. It is assumed that a larger value of s_i corresponds to a more severe contingency. The square of the deviation is used to increase the weight of large deviations. In order to favor a small number of contingencies and a breadth-first search like behavior, the sum of squared voltage deviations is divided by the number of contingencies k_i.

Afterwards, new candidate $N-(k_i+1)$ contingencies are determined. The aim is to identify component outages, which are plausible as subsequent contingencies. For that purpose, it is investigated, which power system components were dominantly affected by C_i. These are good candidates for the (k_i+1)-th contingency, since hidden failures of their protections might lead to inadvertently disconnecting them, in response to the contingency C_i. Appropriate indices for identification of affected components are again dependent on the instability mechanism that is investigated. In the case of

long-term voltage stability, the change of apparent power flows in lines ΔS_j as well as the change in reactive power injection of generators ΔQ_j are relevant. They are computed as follows:

$$\Delta Q_j = Q_j(t_e) - Q_j(t_0) \tag{2}$$

$$\Delta S_j = S_j(t_e) - S_j(t_0) \tag{3}$$

The proposed index a_j, which expresses how much a component j is affected by a contingency, is defined as follows:

$$a_j = \begin{cases} \alpha \cdot \Delta Q_j, & \forall j \in \text{ generators} \\ \Delta S_j, & \forall j \in \text{ transmission lines.} \end{cases} \tag{4}$$

In response to a contingency the reactive power changes will be shared among several generators and, consequently, the individual changes may be small in comparison to apparent power changes in transmission lines in the surroundings of the contingency. In order to allow a higher weighting of the generator reactive power changes, the α factor is introduced. A component j is considered to be affected if a_j is greater than a pre-defined threshold a_{th}. Based on this, candidate $N-(k_i+1)$ contingencies are derived, which are characterized by the severity of the underlying $N-k_i$ contingency C_i and the index a_j of the added (k_i+1)-th single contingency. Subsequently, it is assessed:

- if the candidate $N-(k_i+1)$ contingency contains exactly the same individual contingencies as an already assessed $N-k_n$ contingency;
- if a subset of individual contingencies of the candidate $N-(k_i+1)$ contingency was already found to result in an instability.

If for a candidate $N-(k_i+1)$ contingency none of the above conditions holds true, it is considered to be unique and it is added to L. L is then sorted descending primarily with respect to s_i and secondarily with respect to a_i. After the update of L, the algorithm extracts the next most severe contingency from the list and continues the assessment. This process is terminated, when all contingencies in the dynamic list L are investigated and the list is empty.

B. Illustrative example

An illustration of the proposed approach is offered in Fig. 2. It is shown how an increasing number of applied contingencies progressively deteriorates the displayed bus voltage. Initially, a $N-1$ contingency is simulated. The resulting stable system response is shown with solid line. Various controls respond to the disturbance as indicated in the figure. When the final steady-state A is reached, the severity of the $N-1$ contingency is determined with (1) and the affected components are identified with (4). Subsequently, one of them is considered in the $N-2$ contingency. In the enlarged detail shown in Fig. 2, the occurrence of the two outages (c_1 and c_2) can be observed. A new final steady-state B is reached, where the severity of the contingency as well as the affected components are determined. One of them is selected as third contingency. The dotted curve shows the voltage evolution after the $N-3$ contingency was applied. This causes severe deterioration of

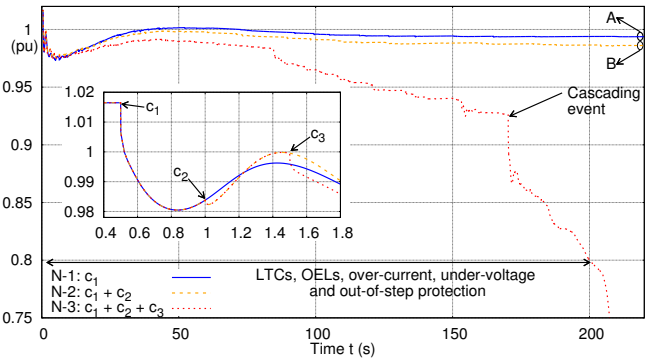


Fig. 2. Illustration of $N-k$ search approach - Voltage evolution after applying $N-1$, $N-2$ and $N-3$ contingencies.

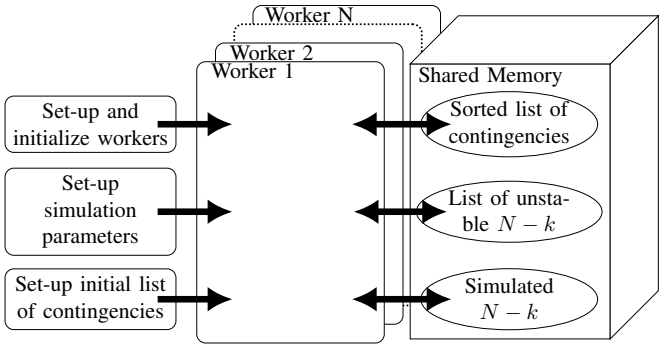


Fig. 3. Implementation into parallel computating environment

the voltage and triggers a cascading event. Eventually, the voltage collapses.

C. Implementation into a parallel computing environment

In order to speed up the assessment and due to the fact that every C_i in L can be simulated and assessed individually, a parallel processing approach has been used. A visualization is shown in Fig. 3. In this approach, a pool of workers is set-up and initialized, where the number of workers is dependent on the available hardware. The parameters for the simulations are read as well as an initial list of contingencies. Some of the data such as the lists L, L_u and a list of already simulated contingencies need to be accessible for all workers. Hence, these are stored in shared memory to which all workers, one at a time, have access. After initialization, each worker runs the part of the algorithm discussed in Section II-A, which is inside the dashed box labeled "Worker X" in Fig. 1.

III. Results

A. IEEE Nordic Test System

In order to demonstrate the performance of the proposed $N-k$ search algorithm, the Nordic test system set up by the IEEE Task Force on "Test Systems for Voltage Stability and Security Assessment" is utilized. The detailed data as well as the operating points can be found in [11]. A one-line diagram is shown in Fig. 4.

All MV loads are served through distribution transformers equipped with LTC. Contrary to [11] the LTCs do not have

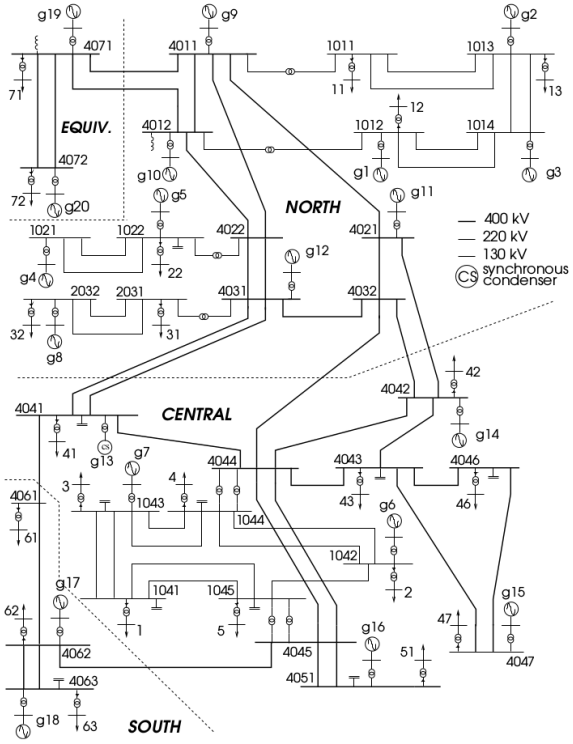


Fig. 4. One-line diagram of the IEEE Nordic test system [11]

constant tapping delays, but variable delays with an inverse time characteristic.

In order to simulate the dynamic system response in more detail, certain component protections were included in the model. All generators are protected with a simple out-of-step protection and an under-voltage protection. The out-of-step protection trips the respective generator instantaneously, if its rotor speed exceeds ± 0.08 % of nominal speed. The under-voltage protection considers two thresholds. The generator is tripped with a delay of 30 s, if the terminal voltage drops below 0.9 pu, but stays above 0.8 pu. It is instantaneously disconnected, if the voltage falls below 0.8 pu.

B. Operating points

The proposed method is tested on different operating points, which are described in detail in [11].

- **Operating point B:** Operating Point (OP) B is an $N-1$ secure operating point.
- **Operating points B plus $50-400$ MW:** Additional six OPs are considered, where the loading of the Central region (see Fig. 4) has been uniformly increased by a total of 50, 100, 250, 300, 350 and 400 MW, respectively. This leads to an increased power flow from the North to the Central region and increases the stress of the system.

Due to the size of the test system, only up to three contingencies ($k_{max} = 3$) are considered. Moreover, the loss of generator $g20$ was not considered, since it represents the connection to a large external grid aggregated into an equivalent generator. The time delay between two subsequent contingencies Δt was chosen to be 0.5 s and the weighting factor α was set equal to 2.5.

A case is considered to be unstable, when the voltage at one bus drops below 0.6 pu and remains below this threshold for at least 500 ms. When an instability is detected the simulation is terminated.

TABLE I
COMPARISON OF NUMBER OF INVESTIGATED CASES IN THE BRUTE-FORCE (BF) APPROACH AND IN THE PROPOSED APPROACH ($N-k$ SEARCH) WITH a_{th} BETWEEN $0.25-1.00$ PU ON 100 MVA BASE.

Approach	a_{th}	Number of sim.	$N-1$	$N-2$	$N-3$
BF	–	55 736	74	24 514	31 147
$N-k$ search	0.25	7 980	74	812	7 093
	0.50	4 364	74	586	3 698
	1.00	1 935	74	370	1 490

TABLE II
COMPARISON OF NUMBER OF IDENTIFIED UNSTABLE CASES IN THE BRUTE-FORCE (BF) APPROACH AND IN THE PROPOSED APPROACH ($N-k$ SEARCH) WITH a_{th} BETWEEN $0.25-1.00$ PU ON 100 MVA BASE.

Approach	a_{th}	Number instable cases	$N-1$	$N-2$	$N-3$
BF	–	2 292	0	226	2 065
$N-k$ search	0.25	1 595	0	222	1 372
	0.50	1 196	0	207	988
	1.00	790	0	176	604

C. Performance of the proposed approach

In this section the proposed approach is compared to a Brute-Force (BF) approach. In the latter, all possible combinations of up to three component (generator and/or transmission line) outages are considered. For that purpose, first, all $N-1$ contingencies are simulated, then all $N-2$ contingencies, while omitting those that include an $N-1$ contingency resulting in instability. Finally, all $N-3$ contingencies are investigated omitting combinations, including an unstable $N-1$ or $N-2$ contingency. It should be noted that, in order to keep the number of cases limited, permutations of contingencies in a sequence were not considered. The total number of cases to be investigated, as well as a split into $N-1$, $N-2$ and $N-3$ cases is shown in Table I. In order to investigate the sensitivity of the proposed algorithm with respect to variation of the threshold a_{th}, results for respectively $a_{th} = 0.25$, 0.50 and 1.00 pu (on 100 MVA base) are presented and discussed. Table I also shows the resulting total number of investigated cases as well as $N-1$, $N-2$ and $N-3$ cases with the proposed method. It can be observed that in all three variants the number of cases is only a fraction ($3.4-14.3$ %) of the number of cases simulated in the BF approach. The results show that halving a_{th} results in an increase by a factor of 1.8 and 2.3, respectively. This is dominated by a rise of the number of investigated $N-3$ contingencies.

Table II shows the number of identified unstable cases with the BF approach as well as the proposed approach for varying a_{th}. As expected, the results show that the test system in OP B is $N-1$ secure and no instability occurs for any

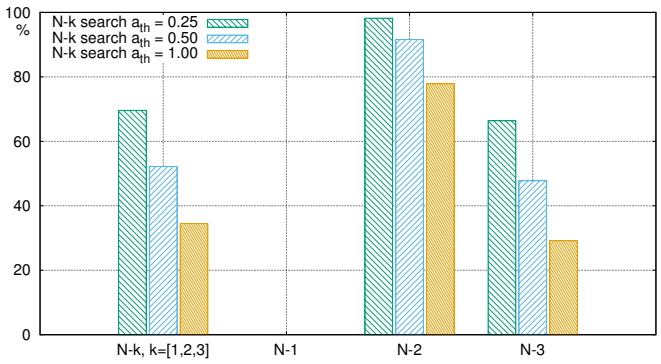


Fig. 5. OP B: Comparison of ratio of identified unstable contingencies with the proposed $N-k$ search approach.

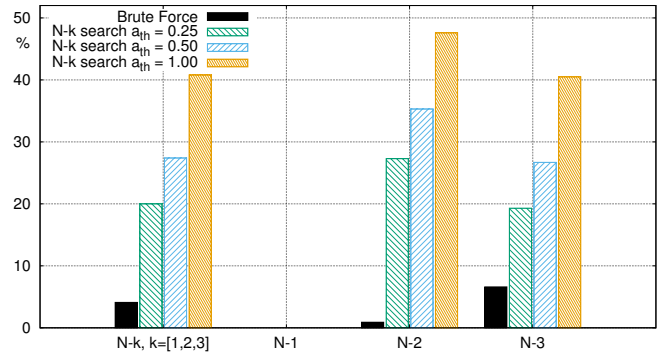


Fig. 6. OP B: Comparison of the BF with the $N-k$ search approach with respect to probabilities of identifying an unstable contingency when simulating a $N-k$ case, $k=1,2,3$.

$N-1$ contingency. The BF algorithm identified 2 292 unstable contingencies. Of those only 9.8 % are $N-2$ contingencies and the remaining are $N-3$ contingencies. While performing only a fraction of the number of simulations, the proposed approach identified between $34.5-69.6$ % of all unstable cases depending on the chosen a_{th}. The individual ratios are shown in Fig. 5. In addition, let us recall that the proposed method does not aim at identifying all unstable $N-k$ contingencies, but a subset of plausible ones.

When comparing the results of the BF approach presented in Table I and Table II, it is striking that the number of cases investigated is very large with respect to the number of identified unstable cases. For example, to identify the 226 unstable $N-2$ contingencies, 24 514 $N-2$ cases needed to be simulated. This can also be expressed as a probability. The probability of identifying an unstable case when simulating a $N-2$ contingency is only 0.9 % in the BF approach. In Fig. 6 the probabilities for identifying an unstable case with the BF approach and the proposed ($N-k$ search) approach are compared. It can be observed that the probabilities of identifying an unstable case are significantly higher with the proposed approach than with the BF approach, where the probabilities are between $0.9-6.6$ %. An increase of the probabilities with an increase of a_{th} can be noticed. However, it should be recalled that the number of identified unstable contingencies declines simultaneously. For this reason, a_{th} should be chosen carefully taking into account the desired identification ratio and the available computational resources.

In the remaining of the paper, a threshold $a_{th}=0.50$ was assumed, since it allows identifying 91.6 % of the unstable $N-2$ contingencies, while only performing 4 364 simulations, which corresponds to 7.8 % of the simulations carried out in the BF approach.

The considerable higher probabilities of identifying unstable cases and the lower number of required simulations demonstrate the benefit of the proposed approach.

D. Earliness of identification of harmful contingencies

The search algorithm is aiming at "fast" identification of harmful contingencies, which lead to instability. In order to assess this feature, the number of identified unstable $N-2$ and $N-3$ contingencies is shown in Fig. 7 as a function of the number of performed simulations. Figure 7a shows the results of the unstable $N-2$ contingencies. It can be observed that during the first 1 100 simulations the number of identified unstable $N-2$ contingencies rises quickly and 80 % of the unstable $N-2$ cases identified by the proposed method are found within this period. On the contrary, the number of identified $N-3$ contingencies grows almost linearly with the number of simulations (see Fig. 7b) and 80 % of the unstable $N-3$ contingencies are identified after approximately 2 850 simulations (65 % of the total number of simulations).

E. Assessment of N-k contingencies at various loading levels

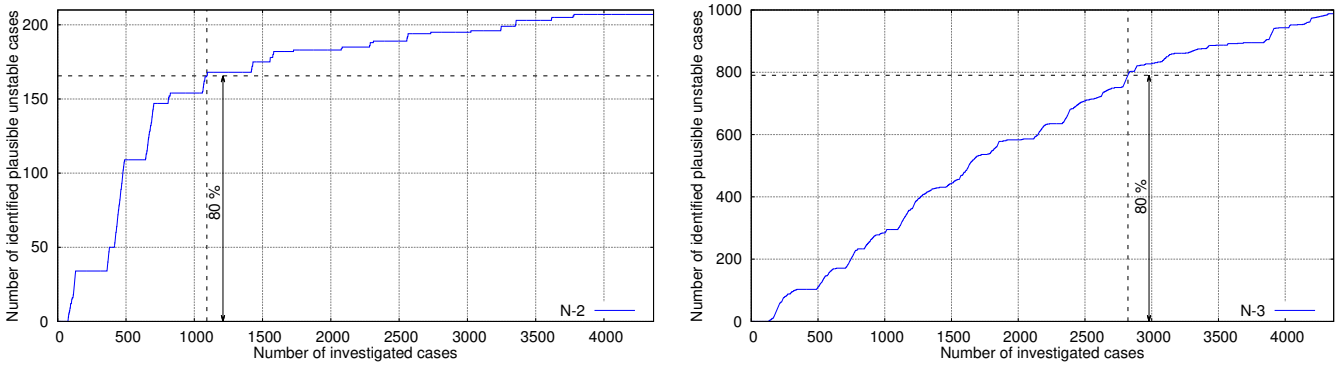
In this section, the effect of a demand increase as described in Section III-B on the number of identified $N-k$ contingencies is discussed. Figure 8 shows the results in a bar graph. It can observed that the absolute number of harmful $N-k$ contingencies decreases with an increase of the loading level, which seems counterintuitive at first glance. While the number of $N-1$ contingency increases to 13, the number of $N-2$ contingencies drops from 202 to 83 and the number of $N-3$ contingencies from 988 to 277.

This observed decrease may be explained by the simultaneous increase of $N-1$ contingencies. While the original OP B is $N-1$ secure, the number of unstable $N-1$ contingencies increases steadily up to 13 in OP B plus 400 MW. Each identified unstable $N-1$ contingency results in the elimination of all unstable $N-2$ and $N-3$ contingencies, which contain the $N-1$ contingency of concern. Similarly, each new unstable $N-2$ contingency eliminates all unstable $N-3$ contingency combinations containing that $N-2$ contingency.

This also explains the temporary increase of the $N-2$ contingencies when the additional loading increases from 50 MW to 100 MW. At both OPs, there are three $N-1$ contingencies and, therefore, the increased stress on the system translates into a larger number of $N-2$ contingencies.

IV. Conclusion

In this paper, a search algorithm for identification of harmful $N-k$ contingencies was presented. The method does not attempt to identify all harmful $N-k$ contingencies, but



(a) $N-2$ contingencies (b) $N-3$ contingencies

Fig. 7. OP B: Number of identified unstable cases over number of simulations

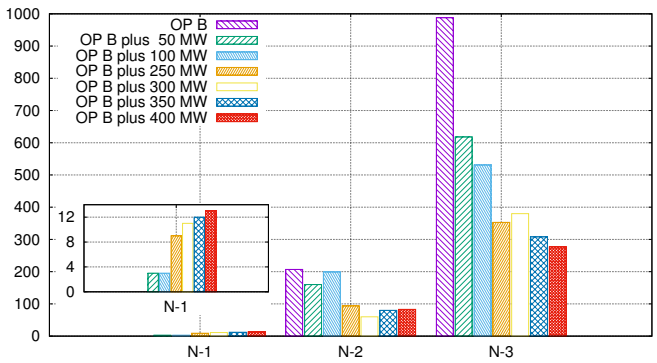


Fig. 8. Comparison number of unstable $N-k$ contingencies in varied loading levels with magnified detail of number of $N-1$ contingencies.

rather plausible harmful $N-k$ contingencies assuming that computational resources are limited and a brute-force approach is infeasible. The approach uses time-domain simulations to identify combinations of k contingencies leading to an instability. A list of initial contingencies is provided. The first contingency on the list is simulated and the simulation results are assessed with respect to stability. If the system remains stable, the algorithm investigates which power system components were dominantly affected. These components in combination with the applied $N-k$ contingency are then considered in candidate $N-(k+1)$ contingencies, which are added to a list. The contingencies in the list are sorted according to severity to ensure that the most severe are investigated first.

The proposed method was tested on the IEEE Nordic Test System, which was assessed with respect to its vulnerability to voltage instability. The method's capability to identify harmful $N-k$ contingencies was evaluated through a comparison with the stability assessment results obtained with a brute-force approach. The results suggest that the method performs better in identifying harmful $N-k$ contingencies with smaller k, which was targeted when defining the severity index. Moreover, it was demonstrated that the method early identifies harmful $N-2$ contingencies. Finally, the number of identified harmful $N-k$ contingencies in an increasingly stressed operating point was investigated.

In the future, it is envisioned to test the proposed approach with respect to other instability mechanisms and on larger test systems. Moreover, the method will be extended to identify stable but non-viable operating conditions and to evaluate the severity of the identified unstable cases.

Acknowledgment

This research was supported by the Amprion GmbH, Germany. We thank Dr. Eckhard Grebe, Valeri Franz, Klaus Vennemann and Dr. Roland Becker for their expert comments.

References

[1] IEEE PES CAMS Task Force, "Initial review of methods for cascading failure analysis in electric power transmission systems," *2008 IEEE Power and Energy Society General Meeting - Conversion and Delivery of Electrical Energy in the 21st Century*, no. July, pp. 1–8, 2008.

[2] D. S. Kirschen and D. P. Nedic, "Consideration of hidden failures in security analysis," in *Power Systems Computation Conference*, 2002, pp. 24–28.

[3] D. P. Nedic, "Simulation of large system disturbances," Ph.D. dissertation, University of Manchester, 2003.

[4] B. Otomega, "Distributed and Centralized System Protection Schemes Against Voltage and Thermal Emergencies," Ph.D. dissertation, University of Liege, 2007.

[5] A. Wang, Y. Luo, G. Tu, and P. Liu, "Vulnerability assessment scheme for power system transmission networks based on the fault chain theory," *IEEE Transactions on Power Systems*, vol. 26, no. 1, pp. 442–450, 2011.

[6] M. J. Eppstein and P. D. H. Hines, "A "random chemistry" algorithm for identifying collections of multiple contingencies that initiate cascading failure," *IEEE Transactions on Power Systems*, vol. 27, no. 3, pp. 1698–1705, 2012.

[7] P. Hines, I. Dobson, and P. Rezaei, "Cascading Power Outages Propagate Locally in an Influence Graph that is not the Actual Grid Topology," *IEEE Transactions on Power Systems*, pp. 1–8, 2015. [Online]. Available: http://arxiv.org/abs/1508.01775

[8] Q. Chen and J. D. McCalley, "Identifying high risk N-k contingencies for online security assessment," *IEEE Transactions on Power Systems*, vol. 20, no. 2, pp. 823–834, 2005.

[9] J. Hazra and A. K. Sinha, "Identification of catastrophic failures in power system using pattern recognition and fuzzy estimation," *IEEE Transactions on Power Systems*, vol. 24, no. 1, pp. 378–387, 2009.

[10] P. F. Petersen, H. Johannsson, and A. H. Nielsen, "Investigation of suitability of cascading outage assessment methods for real-time assessment," *2015 IEEE Eindhoven PowerTech, PowerTech 2015*, pp. 13–17, 2015.

[11] T. Van Cutsem (Chair), "Test Systems for Voltage Stability Analysis and Security Assessment," IEEE PES Power System Dynamic Performance Committee, Tech. Rep. PES-TR19, 2015.