Consequence driven decomposition of large-scale power system security analysis

Florence Fonteneau-Belmudes*, Damien Ernst*, Christophe Druet†, Patrick Panciatici‡ and Louis Wehenkel*
*University of Liège, Belgium
†ELIA, Belgian Transmission System Operator ‡RTE, French Transmission System Operator

***Abstract*—This paper presents an approach for assessing, in operation planning studies, the security of a large-scale power system by decomposing it into elementary subproblems, each one corresponding to a structural weak-point of the system. We suppose that the structural weak-points are known a priori by the system operators, and are each one described by a set of constraints that are localized in some relatively small area of the system. The security analysis with respect to a given weak-point thus reduces to the identification of the combinations of power system configurations and disturbances that could lead to the violation of some of its constraints. We propose an iterative rare-event simulation approach for identifying such combinations among the very large set of possible ones. The procedure is illustrated on a simplified version of this problem applied to the Belgian transmission system.**

***Index Terms*—large-scale system, operation planning, decomposition, security analysis**

I. Introduction

Power system security assessment[1] aims at identifying so-called contingencies that could lead to unacceptable operating conditions if no preventive action was taken.

In real-time operation, when the operating point and topology are known and the objective is to assess the security over a relatively short time horizon (e.g. over the next 30 minutes), this problem may be approximated by screening a finite set of contingencies whose size grows in a linear fashion with the size of the power system itself (e.g. the classical $N-1$ criterion) and by verifying for each of them that the corresponding corrective control problem is feasible.

In operation planning, a few hours or days ahead of time, the problem becomes however much more complex, mainly because of increasing uncertainties about the future power injection patterns and system topologies. In this context, contingencies become combinations of power injection variations, topology changes and disturbances, which are so numerous that their screening is not feasible anymore. As a matter of fact, the "size" of the uncertainty set modeled by contingencies essentially grows exponentially with the length of the time-horizon over which one wants to analyze power system security.

[1]In this paper, for the sake of simplicity but without loss of generality, we will formulate our ideas in the context of so-called static security assessment. Also, in the main part of the paper we restrict our discussion to the analysis aspect of the problem, leaving the discussion of the corresponding preventive control problem to the concluding sections.

When the contingency-wise decomposition of security assessment is not tractable (as in the context of operation planning of large-scale power systems), one has to seek for other ways to decompose the problem into a reasonable number of independent and manageable subproblems.

In large-scale power systems, it turns out that security of operation is generally constrained by the operational limits of only some specific "weak" subparts of the system in relatively small number compared to the overall system size, as for instance long transmission corridors, or cross-border lines, or older system elements that were not dimensioned for today's requirements. The operation limits induced by such weak-points may generically be described by a number of constraints related to elements that are located in the corresponding weak area. In practice these weak areas are geographically localized and hence the set of constraints that must be satisfied for each one of them is typically a very small subset of all the operational constraints of the whole system.

The violation of some of the constraints related to a specific weak-point may initiate cascades that might quickly propagate to the rest of the system and could be extremely difficult to control. The weak-points can thus be considered as critical for the system security and it is rational, and as a matter of fact common engineering practice, to decompose power system security analysis into elementary subproblems each one focusing on a single weak-point at the time. From the analysis point of view, these subproblems may indeed be studied independently of each other and in parallel, and since their number is typically much smaller than the overall system size, it is sufficient to provide a general method for studying a single such subproblem to ensure that the overall security assessment problem has also a scalable solution. This decomposition is also appealing in the context of a large-scale interconnection operated by multiple Transmission System Operators (TSOs), because it supports in a natural way the fact that the security analysis effort is shared by the different operators, each one focusing on the weak-points involving constraints in his area of responsibility.

Focusing on the security analysis problem of large-scale power systems in this paper, we will work under the above discussed assumptions. Specifically, we assume that the weak-points are known beforehand, which should be the case in reality because they correspond to the structural properties of the considered power system, that the overall number of weak-points is typically much smaller than the total number of system elements, since otherwise the system would not

978-1-4244-7465-3/10/$26.00 ©2010 IEEE

at all be viable, and that each weak-point is geographically circumscribed, because of the laws of physics.

With these considerations in mind, we have focused our work on the subproblem corresponding to the analysis of system security for a given weak-point of a large-scale power system. Our contribution is to provide a generic algorithmic approach for the weak-point specific identification of the most dangerous contingencies within a very large set of candidate contingencies. Our approach is based on the conjecture that when focusing on a single weak-point of relevance, the subset of really dangerous contingencies is very small (and can therefore be seen as a rare event), but relatively "regular" (i.e. rather "simple" to describe once it has been identified). We call the approach proposed in this paper "Rare Event Simulation Approach" (RESA). This work is a follow up of the work of [1].

The rest of this paper is organized as follows. Section II describes explicitly the considered elementary subproblems and justifies the use of RESA to solve them. Section III describes the methodological background for identifying rare events in combinatorial search spaces with iterative sampling methods and presents a detailed algorithmic approach of RESA applied to the identification of dangerous contingencies for a given weak-point. This approach is then illustrated on a simplified version of the problem on the Belgian transmission system in Section IV, in which some simulation results are reported. Section V discusses our algorithm with respect to existing work. Conclusions and directions for further work are given in Section VI.

II. Subproblem solution strategy

In this section we consider the basic problem that needs to be solved according to the proposed decomposition strategy. We focus on a weak area whose viability can be described by a small number of constraints on currents or voltages (in the static setting) in a small number of transmission system elements that are close to each other.

In this paper a *contingency* is defined as a combination of a configuration of the network (which includes the generation and load patterns, the topology and control structure) and of a hazardous event (corresponding to the tripping of one or several devices as lines or generators). In the sequel, a contingency is denoted by $\{C, E\}$, where C stands for "initial Configuration" and E for "hazardous Event". Such a combination implicitly defines the steady-state configuration that will be reached by the system starting from the initial configuration and after the occurrence of the considered hazardous event. The term "final configuration" is used to qualify this configuration. Notice that for cascading contingencies, the final configuration of the system is the result of a sequence of several steady-state configurations reached by the system starting from the occurrence of the triggering event.

Deciding whether a contingency is dangerous or not requires to evaluate the final configuration that follows its occurrence. As mentioned earlier, a contingency is considered as being dangerous if (at least) one of the constraints defining the considered weak-point of the system is violated in this final configuration. Hence, the acceptability of a final configuration is determined by defining thresholds on some state variables of the considered critical equipments (such as the ampacity of a transmission line, i.e. a threshold on the value of its current), above which the equipment is no longer safe and is likely to trip or to fail in some other way.

The security analysis procedure that we propose aims at setting up a list of the most dangerous contingencies in terms of such constraint violations associated to the final configuration and restricted to a specific weak-point. Let us explain how this approach differs from the usual procedure for performing power system static security analyses.

Usually, TSOs assess system security by performing what they commonly call "$N-k$" security analyses. Such a study consists in screening all the hazardous events corresponding to the loss of k transmission equipments for one specific initial configuration of the system or a set of a few different configurations, and in analyzing the consequences of each one of these contingencies in terms of all possible constraint violations in a system wide perspective. The standard operational rule is $k = 1$, however, when the likelihood of an incident with $k > 1$ is large enough, some $k = 2$ or $k = 3$ contingencies may also be considered. For each considered contingency, the output of such a study is composed of a global diagnosis on the stability of the system, in the form of a list of system elements that would trip, or be overloaded.

Instead, in this work we focus on a small subset of system elements that were a priori identified as critical for the considered weak-point. Our problem is therefore not a full screening of all the possible contingencies but a dedicated search for those that would have specific consequences, namely which would lead to the violation of at least one of the a priori identified constraints defining the weak-point. For each weak-point, the output of our procedure is a list of contingencies that would lead to its constraint violations. This is why we name our approach "consequence driven".

In the next subsections we describe from a technical point of view and validate our proposal of a rare-event simulation approach to identify the subset of contingencies dangerous for a given weak-point of a large-scale power system.

III. Rare-event simulation approach (RESA) for security assessment with respect to a weak-point

When considering the structure of the security analysis problem in the context of a specific weak-point of a large-scale power system, the dangerous $\{C, E\}$ combinations for a given weak-point are typically very rare with respect to the non-dangerous ones. Moreover, the subset of combinations that would appear as dangerous for a specific weak-point of the system will in most cases only involve a small set of features (i.e. a small set of dimensions used to describe the complete set of possible contingencies), e.g. those related to an area constrained by geographical or electrical distances around the considered weak-point. This suggests to develop specific methods for identifying rapidly among the set of possible contingencies those that are dangerous for a given weak-point, rather than to try to screen exhaustively the potentially

very large set of possible $\{C, E\}$ combinations in a system wide perspective. In addition, it will be useful to identify the subset of features that are sufficient to characterize the set of dangerous contingencies for a given weak-point.

In this section we provide a methodological framework which aims at these objectives. It is based on a combination of ideas from Monte-Carlo simulation and automatic learning.

A. RESA in combinatorial search spaces

In the literature many iterative sampling methods have been proposed for searching solutions to combinatorial or non-convex optimization problems, such as genetic algorithms, distribution estimation methods, Markov-Chain Monte Carlo methods, and also the so-called cross-entropy method (see [2], [3], [4] and [5]).

A common feature of these methods, from an algorithmic point of view, is to combine random sampling with an iterative process allowing one to "learn" the best sampling scheme for the problem under consideration. Generically, these algorithms work in the following way:

- define some initial sampling distribution over the considered search space and an objective function allowing to compare (or to rank) elements of the search space;
- at each iteration:
  - generate a subset of potential solutions over the search space by using the current sampling distribution;
  - evaluate the objective function for each configuration in the current sample;
  - use the pairs (configuration, objective function) in the current sample so as to determine a new sampling distribution better targeting the interesting solutions of the problem;
- halt the iterative process when the computational resources have been exhausted, or when the current sample is sufficiently pure in terms of objective function distribution, or when the variation of some sample statistics has not changed significantly since a certain number of iterations.

In this paper, we want to exploit such iterative sampling based methods for rare combinatorial event simulations, i.e. in order to identify elements of a very small subset of "interesting" contingencies among a very large number of candidate ones located in an originally unstructured mixed continuous/discrete search space.

To do so, we first define an objective function over the original search space which is maximal only for the sought interesting solutions. Then we embed the original search space in a compact metric space where the objective function varies in a progressive way and on which we may apply naturally linear operators such as averaging and interpolation, and we use the iterative sampling based optimization approach together with averaging/interpolation operators over the embedding space so as to generate a sequence of sampling distributions defined over this space which progressively target subsets corresponding to dangerous contingencies with respect to the original problem.

One main ingredient of this approach, needed to allow the computation of the objective function over the embedding space, consists of a reverse mapping (pre-image computation) of the embedding so as to associate to each point of the embedding space an element of the original mixed discrete/continuous space over which the objective function is intrinsically defined.

B. The cross-entropy method (in general)

In our simulations reported below, we use as iterative sampling method the cross-entropy method [5]. This method proceeds as follows:

- define a hypothesis space of candidate sampling densities p_λ defined over $\mathbb{R}^n$ and indexed by a parameter vector λ. This space of distributions may be chosen in a problem specific way, for example by taking into account properties such as linearity, gaussianity or the possibility of multiple modes;
- set λ to its initial value λ_0 (typically λ_0 will be chosen so as to let the distribution p_{λ_0} cover the complete space $\mathbb{R}^n$);
- at each iteration i, draw a sample S_i of size s of configurations according to the current distribution defined by the current value λ_i (s is a parameter of the algorithm) and evaluate the value of the objective function $O(\cdot)$ for each one of these configurations;
- keep the subset S'_i of S_i corresponding to the $m < s$ best solutions (m is another parameter of the algorithm);
- use the sample S'_i to determine a new value λ_{i+1}. In the cross-entropy method, one typically uses at this step the maximum likelihood principle, i.e. one chooses the value λ_{i+1} such that the likelihood of the sample S'_{i+1} is maximal with respect to the selected space of distributions.

In the following sections, we describe the precise setting that we have used in order to apply this approach to the identification of dangerous contingencies for a given weak-point of a power system, in the form of a critical line constrained by its current flow.

Our settings comprise the choice of an objective function measuring the weak-point specific *severity* of a contingency, the embedding of the contingency set in suitable metric space and its pre-image computations, as well as the choices associated to the application of the cross-entropy method per se (space of sampling distributions, and choice of the parameters s and m).

In our validation section, we will focus on simple contingencies described by the loss of a single transmission system element.

C. The objective function

From now on, we denote a contingency by $x \in \mathscr{X}$, where $\mathscr{X}$ is the contingency space, i.e. the space gathering all possible $\{C, E\}$ combinations. The objective function $O(\cdot)$ is a real-valued function defined over $\mathscr{X}$ which takes its maximum values when x is a dangerous contingency for the considered weak-point.

The function $O(\cdot)$ is used at every iteration of the RESA algorithm for selecting among the several contingencies drawn from the current sampling density, those which correspond to the largest values of $O(x)$.

Subsequently, these latter are used to define, based on the maximum likelihood principle, the parameters defining the sampling density at the next iteration within the set of sampling densities used by the algorithm. As the iterations go on, the algorithm should generate sampling densities which give more weight to the dangerous contingencies.

In the classical cross-entropy framework, the function $O(\cdot)$ is given a priori. In our problem, one has the flexibility to choose among the set of real-valued functions defined on $\mathscr{X}$, one which leads to good performances. Pragmatically, we propose so as to define this function to associate to a contingency x a value that reflects its consequences on the operating conditions of the considered weak-point. When several weak equipments are considered, one can either consider an objective function related to one single weak equipment and repeat the procedure independently for all the weak equipments, or aggregate indices related to each of these equipments in order to have a unique value for the objective function $O(\cdot)$.

In our validations we chose to treat the case where the focus is on a single weak transmission line and we hence used for $O(x)$ the loading rate induced by the contingency x on the considered line. A contingency will thus be considered as dangerous if this value exceeds a threshold defined by the operator. This limit can for instance correspond to the ampacity of the considered line, as we did in our simulations.

In general, this choice of function $O(\cdot)$ should ensure that it takes its maximum value on the most dangerous contingencies with respect to the targeted weak-point. As $O(x)$ reflects the severity of the contingency x, the function $O(\cdot)$ will also be referred to as the severity function in the following.

D. Metrization of the contingency space

As explained in III-A, for iterative sampling methods to work well in our context, it is necessary to embed the contingency set in a metric space in such a way that the objective function will vary progressively over this metric space. This means that we need to define a projection operator on the discrete set of contingencies, calculating for each contingency a point in a metric space such that contingencies which are projected on nearby points have similar values of the security related objective function.

In the approach, probability densities will be learned that are defined over the metric space embedding contingencies; for each sample drawn in this space it will be necessary to compute a value of the severity function $O(\cdot)$, by associating to it an element of the original set of contingencies. The metrization process thus consists in choosing an adapted continuous space and defining a pre-image function that associates to each point of this space an element of the original contingency set.

We propose the following approach: we first represent the contingencies as points of a metric space by using physical quantities related to them that may be associated to coordinates (features) in a multidimensional setting, and then we associate to each point of this metric space the contingency from which it stands the closest according to the chosen metric.

Representing the contingencies as points of a multi-dimensional space requires to define coordinates for each contingency along with distances between the contingencies. A contingency can be seen as a large state vector, containing all the data on the configuration of the system and also information about the available and non-available equipments and the disturbances. Using the Euclidean distance or a kernel-based distance metric, it is possible to compute distances between each pair of contingencies. From this set of inter-contingency distances, dedicated methods such as multi-dimensional scaling algorithms (see [6]), that were already used in the context of power systems in [7], allow to compute coordinates for each contingency in the chosen number of dimensions.

To illustrate this metrization process, we give hereafter a detailed procedure for the specific case where the contingency set is limited to only one initial configuration C, while the event E varies among all possibilities for the loss of one or several transmission lines. The set of $\{C, E\}$ combinations considered here thus corresponds to the set of potential $N-k$ contingencies in the same base case. This procedure is the one used in the simulations reported subsequently.

In order to explain the strategy we have chosen to embed this specific contingency space in a metric space, we will first reason as if only $N-1$ contingencies corresponding to branch outages were considered. In such a case, one approach for metrization and pre-image computation could be to use the plane ($\mathbb{R}^2$) as metric space, to plot the geographical map of the power system on this plane and to associate to every point of the plane the branch which stands the closest to it (pre-image computation). In this case, the contingencies are represented according to their geographical distance and coordinates. The distance between a point in the plane and a branch could for example be defined as the distance between this point and the middle of the branch, which leads to a very easily interpretable representation.

The above embedding procedure may be extended in different ways in order to deal with $N-k$ contingencies with $k>1$, still corresponding to branch outages only. For example, we may consider $\mathbb{R}^{2k}$ as metric embedding space rather than $\mathbb{R}^2$, as it was the case with $N-1$ contingencies. A contingency is represented here by the k-tuple $(l_1, l_2, \ldots, l_k)$ where every l_i refers to a transmission line. The computation of the pre-image $(l_1, l_2, \ldots, l_k)$ of a point in the metric space $\mathbb{R}^{2k}$ might be done as follows. To identify the component l_1, we could take the first two components of the $2k$-dimensional vector in the metric space and exploit these two coordinates to identify a power system element as if we were dealing with an $N-1$ contingency. By taking the second two components of the $2k$-dimensional vector, we could identify l_2 using the same procedure, and then similarly $(l_3, \ldots, l_k)$. The rationale behind this approach lies on the assumption that if two contingencies $(l_1, l_2, \ldots, l_k)$ and $(l'_1, l'_2, \ldots, l'_k)$ are such that if for any i, l_i is close to l'_i, then these contingencies will have similar effects on the steady-state properties of the post-fault system.

However, nothing guarantees that the obtained k-tuple is

made of distinct branches or that the k-tuple does not correspond to a contingency which splits the network into several areas. To address this problem, we have slightly modified the pre-image computation procedure as follows. First, we consider that the elements of a k-tuple are identified sequentially. At every step j, we check after having identified l_j whether there exists in $\mathscr{X}$ a k-tuple whose first j elements are $(l_1, l_2, \ldots, l_j)$. If it is not the case, we choose as l_j the second closest branch to the considered point of the metric space. There is again a similar checking on this new l_j and the procedure repeats if necessary.

In the following, we denote by $PreImage : \mathbb{R}^{2\times k} \rightarrow \mathscr{X}$ the function that computes the pre-image of an element of the metric embedding space.

E. A fully specified algorithm

Figure 1 gives the tabular version of an iterative sampling based algorithm for identifying rare dangerous contingencies. This algorithm uses n-dimensional Gaussian laws as sampling distributions (referred to by $Gauss_{\mathbb{R}^n}(\cdot, \lambda_i)$ in the algorithm) and is a particular instance of the cross-entropy based approach for identifying rare events described in Section III-A.

The algorithm takes as input a pre-image function, an objective function $O(\cdot)$ and a threshold $\gamma \in \mathbb{R}$ defining the dangerous contingencies (a contingency x is dangerous if $O(x) > \gamma$). It outputs a set of contingencies which maximize this function and whose severity is greater than γ.

The parameters $\lambda_0 = [\mu_0, \sigma_0]^n$ of the initial sampling distribution (μ and σ refer to the mean and the standard deviation of the distribution, respectively) are usually chosen such that the initial sampling distribution covers well the entire contingency space. In our simulations, these will be chosen such that (i) μ_0 corresponds to the geometrical center of the subspace of the metric embedding space in which all the buses and lines of the electric system are located (ii) the ith component of σ_0 is equal to half the size of this subspace alongside its ith dimension.

At each iteration i, a sample of s elements is drawn according to $Gauss_{\mathbb{R}^n}(\cdot, \lambda_i)$. Usually, in cross-entropy algorithms, the value of s is chosen an order of magnitude larger than the number of elements parametrizing the sampling distributions. In our simulations, n is equal to 4 and s is chosen equal to 50. The pre-image function is first applied to every element of the sample to identify to which contingencies they correspond. Afterwards, the different values that the objective function takes over these contingencies are computed. The contingencies which lead to the m best values of the objective function are then used to compute the next sampling distribution. The parameter m is usually chosen 10 to 20 times smaller than s. In our simulations, m is equal to 5.

Different stopping conditions can be thought of for this algorithm (see Section III-A). In our simulations, we will mostly for illustrative purposes stop the algorithm when a specific number of iterations has been reached.

IV. Illustration on the Belgian transmission system

This section presents the performances of the proposed approach. We consider here the Belgian transmission system, and more specifically its equipments operated at a voltage level of 150 kV and above (including about 600 buses and 635 transmission lines).

The specific problem illustrated here is the following. For simplicity reasons, we chose (as done in Section III-D) to limit the size of the contingency space and to keep the same initial configuration C during the whole study. As events E, we consider the tripping of one single transmission line at a time. The so-defined contingency space is embedded in $\mathbb{R}^2$, as explained in Section III-D, by associating to each point of the two-dimensional map of the Belgian transmission system the contingency corresponding to the tripping of the closest transmission line.

For the same simplicity reasons, we decided to target in this analysis one single equipment, a non-border 380 kV transmission line (between Bruegel and Courcelles). We define the objective function on the metric embedding space as being the loading rate of this target transmission line when the contingency $\{C, E\}$ occurs. Figure 2 presents the profile of this objective function on the chosen embedding space and locates the considered target transmission line. The color scale goes from dark blue for the less dangerous contingencies to dark red for the most dangerous ones. As explained in Section III-D, the plane is divided into surfaces corresponding to the tripping of the different transmission lines. This profile has been built by simulating all the $N-1$ contingencies implying a transmission line and by evaluating their influence on the target line in terms of overload. Note that the profile of the objective function is reported here for information but is not an input of the problem.

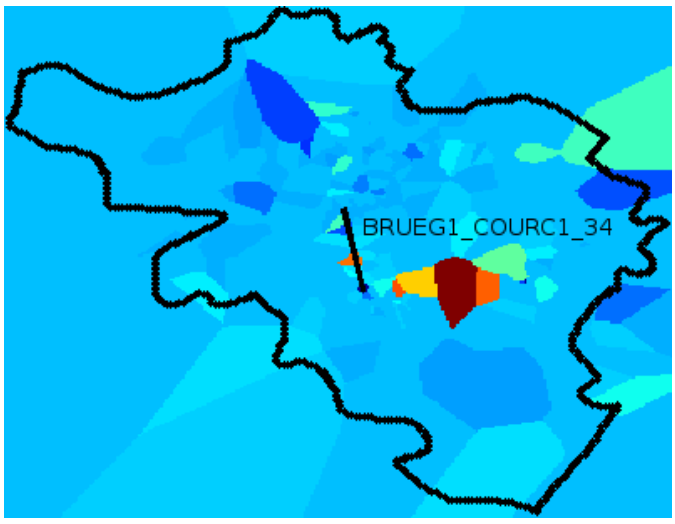

Fig. 2. Profile of the severity function over the metric embedding space.

A typical run of the developed iterative sampling algorithm applied to the considered problem leads to the results presented on Figure 3. The black points on these maps represent the set

Problem definition: A pre-image function $PreImage : \mathbb{R}^n \to \mathscr{X}$, an objective function $O : \mathscr{X} \to \mathbb{R}$ and a threshold $\gamma \in \mathbb{R}$.
Algorithm parameters: The parameters $\lambda_0 = [\mu_0, \sigma_0]^n$ of the initial n-dimensional Gaussian sampling distribution, the size s of the sample drawn at each iteration, the number m of best solutions chosen at each iteration.
Output: A set $\mathscr{X}_{dang}$ of elements of $\mathscr{X}$ such that $O(x) > \gamma$.
Algorithm:

Step 1. Set i equal to 0.

Step 2. Set S_i, T_i, S'_i and $\mathscr{X}_{dang}$ to empty sets.

Step 3. Draw independently s elements according to the pdf $Gauss_{\mathbb{R}^n}(\cdot, \lambda_i)$ and store them in S_i.

Step 4. For every element $y \in S_i$, compute $x = PreImage(y)$, compute $o = O(x)$, add the triplet (y, x, o) to T_i.

Step 5. Identify in T_i the m triplets with the highest values of o and set their y values in S'_i.

Step 6. Identify in T_i the triplets for which $o > \gamma$ and set their x values in $\mathscr{X}_{dang}$.

Step 7. Set $\mu_{i+1}[j] = \dfrac{\sum_{y \in S'_i} y[j]}{m}$ and $\sigma_{i+1}[j] = \sqrt{\dfrac{\sum_{y \in S'_i} (y[j] - \mu_{i+1}[j])^2}{m}}$ for $j = 1, \ldots, n$ and set $\lambda_{i+1} = [\mu_{i+1}, \sigma_{i+1}]$.

Step 8. If stopping conditions are reached, output $\mathscr{X}_{dang}$ and stop. Otherwise, $i \leftarrow i + 1$ and go to **Step 2.**

Fig. 1. An algorithm for identifying the elements such that a function $O : \mathscr{X} \to \mathbb{R}$ exceeds a threshold γ by iterative sampling when $\mathbb{R}^n$ is chosen as metric space.

of points drawn from the search space during, respectively, iterations 1, 2, 3 and 4 (50 points are drawn at each iteration).

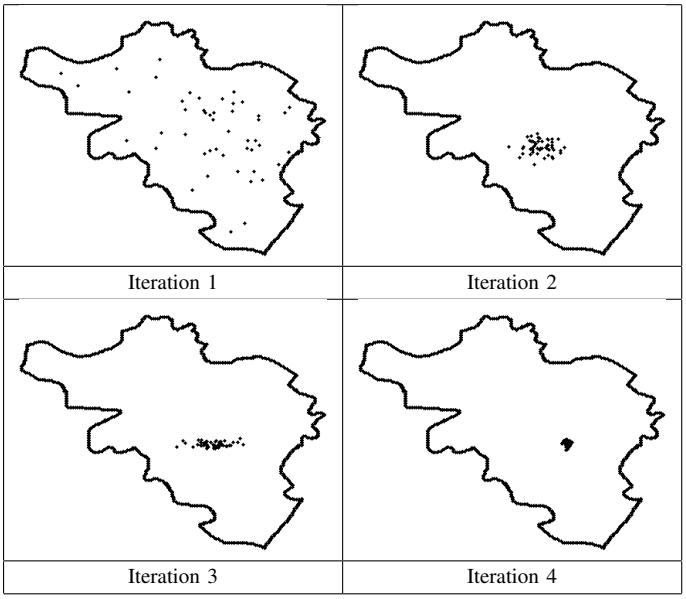

Fig. 3. Illustration of the successive samples of 50 points drawn from the contingency space over the iterations of by the iterative sampling algorithm.

These results show that the successive sampling distributions built at each iteration of the algorithm rapidly concentrate to an area corresponding to the most dangerous $N-1$ contingency with respect to the loading of the critical transmission line. Moreover, some other dangerous contingencies have been identified during the execution of the algorithm.

The dangerous contingencies in this problem are presented on Table I, in which they are sorted by decreasing severity. Note that we chose to define a contingency as dangerous if, after the occurrence of this contingency, the loading rate of target line becomes greater than twice its value in the base case (which is equal to 11.2%). Concretely, a contingency is considered as dangerous if the subsequent loading rate of the target transmission line is greater than 22.4%. This criterion defines six dangerous contingencies, numbered from 1 to 6 in Table I for easier referral.

Table II presents the probabilities of identification of the six dangerous contingencies. These probabilities have been computed over 100 runs of the iterative sampling algorithm by counting in how many runs each of these contingencies were identified. The performances of the proposed procedure are compared in this table to those of a classical Monte Carlo sampling of the contingency space. For this latter method, we took 100 random sets of 124 $N-1$ contingencies (which was the average number of different contingencies analyzed during one run of the iterative sampling algorithm) from the 634 potential ones, and counted how many times each of the six dangerous contingencies appeared in these sets. The results collected in Table II correspond to the conversion of these numbers into probabilities.

To complement these results, Table III shows the probabilities that the two, three, four, five and six most dangerous contingencies are identified during one run of the iterative sampling algorithm and the Monte Carlo method. These probabilities are still computed over 100 runs for each method.

We observe that our iterative sampling framework allows to identify the most dangerous $N-1$ contingency with a very satisfying probability (0.91), two others of the six dangerous contingencies with a probability greater than 0.7, and the three last ones with a probability of 0.36 to 0.51. Even these last figures are still higher than the performances of the Monte Carlo method, with which all the contingencies are identified with a probability 0.20 in expectation. These results are all the more interesting as they have been obtained by studying on average (over the 100 runs executed) 124 contingencies, whereas an exhaustive screening of the contingency space

TABLE I

LIST OF THE DANGEROUS CONTINGENCIES WRT TRANSMISSION LINE BRUEG1_COURC1_34, SORTED BY DECREASING SEVERITY, WHERE THE SEVERITY OF A CONTINGENCY IS THE LOADING RATE IT INDUCES ON THE TARGET TRANSMISSION LINE.

Contingency number	Disconnected transmission line	Severity (loading rate of line BRUEG1_COURC1_34)
1	GRAMM1_STAM+1_31	32.2%
2	STAM+1_TERGN1_31	26.1%
3	CHAMP1_GRAMM1_32	25.9%
4	COURC1_MEKI+1_33	25.4%
5	COURC1_GOUY 1_58	25.1%
6	CHAMP1_COURC1_56	22.6%

TABLE II

PROBABILITIES OF IDENTIFICATION OF THE SIX DANGEROUS CONTINGENCIES (WRT TRANSMISSION LINE BRUEG1_COURC1_34) DURING ONE RUN.

Contingency number	Probability of identification	
	Iterative sampling	Monte Carlo
1	0.91	0.22
2	0.41	0.14
3	0.74	0.21
4	0.36	0.22
5	0.51	0.29
6	0.83	0.26

would have required to analyze 634 contingencies by running a security analysis for each one of them (but would have identified all the dangerous contingencies with a probability 1). Note that, even if 200 points are drawn from the metric embedding space during one run of the iterative sampling algorithm, several points correspond to a same contingency, and therefore less than 200 different contingencies need to be analyzed in one run of the algorithm. As for the probabilities or identifying several dangerous contingencies during one single run of the importance sampling algorithm, they are rather low (below 0.40), and significantly decrease when considering more dangerous contingencies, whereas these joint probability are almost equal to zero, even for only two different contingencies, with the Monte Carlo method. We can add to these results that the average number of dangerous contingencies identified during one run of the iterative sampling method is equal to 3.4, which shows a large improvement versus 1.1 for the Monte Carlo method.

The obtained results highlight the efficiency of our importance sampling approach, which is able to identify the contingencies that are dangerous for a target transmission line with a rather high probability and efficiently, by screening only a small part of the contingency space. The significant improvement brought by the iterative sampling method with respect to the classical Monte Carlo method is due to the fact that our approach exploits, at each iteration $i > 1$, the information contained in the previously drawn sample. As explained in Section III-A, the new sampling distribution thus computed gives more weight to the points leading to high values of the severity function.

TABLE III

JOINT PROBABILITIES OF IDENTIFICATION OF THE TWO, THREE, FOR, FIVE AND SIX MOST DANGEROUS CONTINGENCIES (WRT TRANSMISSION LINE BRUEG1_COURC1_34) DURING ONE RUN.

Contingencies	Probability of identification	
	Iterative sampling	Monte Carlo
1 and 2	0.39	0.03
1, 2 and 3	0.34	0.01
1, 2, 3 and 4	0.16	0
1, 2, 3, 4 and 5	0.11	0
1, 2, 3, 4, 5 and 6	0.10	0

V. RELATED WORK

The rare-event simulation approach proposed in this paper for efficiently identifying rare dangerous contingencies was first used within the context of power system security analysis in [8]. In this latter paper, the space of contingencies was made of load patterns and the cross-entropy algorithm was applied without any metrization of the contingency space. This approach was then applied to $N-k$ security analyses in large-scale power systems in [7].

As regards the identification of dangerous contingencies, it has long been recognized by power system engineers that crude Monte Carlo simulations may be computationally inefficient. Numerous techniques were proposed to address this problem. For example, References [9], [10] propose to combine, in the context of distribution systems, Monte Carlo simulations with some analytical approaches. Reference [11] proposes to exploit artificial neural networks based on the learning vector quantization algorithm to make Monte Carlo techniques more computationally efficient for loss of load probability calculations. Importance sampling as well as other variance reduction techniques have also been recurrently proposed in the power system literature as an enhancement of Monte Carlo methods (see, e.g., [10], [12], [13], [14]).

In order to identify probability distributions targeting dangerous contingencies, the method proposed in this paper only requires to run a security analysis for a relatively small set of contingencies. Viewed in this light, it can be parented to the significant body of work related to contingency filtering and contingency screening in power systems (see, e.g., [15], [16], [17]). Most of the approaches for contingency filtering however rely on deterministic algorithms while the one proposed in this paper is a stochastic one. The importance sampling distributions computed over the course of the cross-entropy algorithm could possibly also be used as classifiers for dangerous and non-dangerous contingencies: indeed, they should ideally associate a low probability to non-dangerous contingencies and a high probability to dangerous ones. To this extent, the proposed approach has some similarities with the many works where classifiers for assessing the degree of severity of power system scenarios are built (see, e.g., [17], [18], [19]).

VI. CONCLUSION

We have proposed in this paper to decompose large-scale power system security analysis along a set of priorly known

weak-points of the considered system.

By exploiting the fact that the contingencies leading these weak-points to unacceptable operating conditions are rare, we developed an iterative sampling framework to efficiently identify the dangerous contingencies in this context. Even if still preliminary, the efficiency of the proposed importance sampling approach, illustrated by our simulations on the Belgian network, suggests that this method could identify in a computationally efficient way the dangerous contingencies with respect to a weak-point in very large contingency spaces.

While our proposed framework is very general, the particular instance of this framework for which we proposed a fully specified algorithm only applies to contingency spaces related to one single initial configuration of the system and to the loss of transmission elements. We believe that working on the development of the underlying algorithms to make it possible to handle more general contingency spaces is a promising research direction. In particular, it could be very interesting to extend the contingency space to the wide variety of potential generation patterns that it is now possible to observe, due to the increasing penetration of renewable energies. In this prospect, our approach could be used to identify among these patterns those that could be potentially dangerous for the weak-points of the system.

Also, in our specific case study we did not explicitly take into account the effect of post-contingency controls. In practice, however, power system engineers want to detect situations (contingencies) in which corrective controls are not able to manage the viability of the system. This viewpoint can be integrated into our framework by simply adapting in a suitable way the module assessing the effects of a specific contingency on the system so that it also models corrective control efforts.

ACKNOWLEDGEMENTS

Florence Fonteneau-Belmudes thanks FRIA (Belgian Fund for Research in Industry and Agriculture) for allowing her to carry out this research. Damien Ernst acknowledges the financial support of the Belgian National Fund of Scientific Research (FNRS) of which he is a Research Associate. This work has been supported by the Belgian Network DYSCO (Dynamical Systems, Control, and Optimization), funded by the Interuniversity Attraction Poles Programme, initiated by the Belgian State, Science Policy Office. The scientific responsibility rests with the authors.

REFERENCES

[1] F. Fonteneau-Belmudes, D. Ernst, and L. Wehenkel. A rare event approach to build security analysis tools when $N-k$ ($k>1$) analyses are needed (as they are in large scale power systems). In *Proceedings of the 2009 IEEE Bucharest PowerTech Conference*, Bucharest, Romania, 2009. 8 pages.

[2] D.E. Goldberg. *Genetic Algorithms in Search, Optimization and Machine Learning*. Addison-Wesley, 1989.

[3] H. Muehlenbein, T. Mahnig, and A. Ochoa Rodriguez. Schemata, distributions and graphical models in evolutionary optimization. *Journal of Heuristics*, 5:215–247, 1999.

[4] C. Andrieu, N. de Freitas, A. Doucet, and M.I. Jordan. An introduction to MCMC for machine learning. *Machine Learning*, 50:5–43, 2003.

[5] R.Y. Rubinstein and D.P. Kroese. *The Cross-Entropy Method. A Unified Approach to Combinatorial Optimization, Monte-Carlo Simulation, and Machine Learning*. Information Science and Statistics. Springer, 2004.

[6] I. Borg and P. Groenen. *Modern Mutlidimensional Scaling: Theory and Applications*. Springer New York, 2005.

[7] F. Belmudes, D. Ernst, and L. Wehenkel. Pseudo-geographical representations of power system buses by multidimensional scaling. In *Proceedings of the 15th International Conference on Intelligent System Applications to Power Systems (ISAP 2009)*, Curitiba, Brazil, 2009. 6 pages.

[8] F. Belmudes, D. Ernst, and L. Wehenkel. Cross-entropy based rare-event simulation for the identification of dangerous events in power systems. In *Proceedings of the 10th International Conference on Probabilistic Methods Applied to Power Systems (PMAPS-08)*, Rincon, Puerto Rico, 2008. 8 pages.

[9] R.N. Allan and M.G. Da Silva. Evaluation of reliability indices and outage costs in distribution systems. *IEEE Transactions on Power Systems*, 10(1):413–419, 1995.

[10] M.V.F. Pereira, M.E.P. Maceira, G.C. Oliveira, and L.M.V.G. Pinto. Combining analytical models and Monte-Carlo techniques in probabilistic power system analysis. *IEEE Transactions on Power Systems*, 7:265–272, 1992.

[11] X. Luo, C. Singh, and A.D. Patton. Power system reliability evaluation using learning vector quantization and Monte-Carlo simulations. *Electrical Power Systems Research*, 66(2), 2003.

[12] K. Bae and J.S. Thorp. An importance sampling application: 179 bus WSCC system under voltage based hidden failures and misoperations. In *Proceedings of the Thirsty-First Annual Hawaii International Conference on System Sciences*, page 39. IEEE Computer Society, 1998.

[13] J.H. Pickels and I.H. Russel. Importance sampling for power system security assessment. In *Proceedings of the Third International PMAPS Conference*, pages 47–52, 1991.

[14] Q. Chen. *The Probability, Identification and Prevention of Rare-Events in Power Systems*. PhD thesis, Iowa State University, 2004.

[15] D. Ernst, D. Ruiz-Vega, M. Pavella, P. Hirsch, and D. Sobajic. A unified approach to transient stability contingency filtering, ranking and assessment. *IEEE Transactions on Power Systems*, 16(3):435–444, 2001.

[16] F. Capitanescu, M. Glavic, D. Ernst, and L. Wehenkel. Contingency filtering techniques for preventive security constrained optimal power flow. *IEEE Transactions on Power Systems*, 22(4):1690–1697, 2007.

[17] K.W. Chan, R.W. Dunn, A.R. Daniels, J.A. Padget, A.O. Ekwue, P.H. Buxton, and M.J. Rawlins. On-line dynamic-security contingency screening and ranking. *IEE Proceedings- Generation, Transmission and Distribution*, 144(2):132–138, 1997.

[18] L. Wehenkel, T. Van Cutsem, and M. Ribbens-Pavella. An artificial intelligence framework for on-line transient stability assessment of power systems. *IEEE Transactions on Power Systems*, PWRS-4:789–800, 1989.

[19] L. Wehenkel, C. Lebrevelec, M. Trotignon, and J. Batut. Probabilistic design of power-system special stability controls. *Control Engineering Practice*, 7(2):183–194, 1999.