A MODEL FOR THE SECURITY ANALYSIS OF A BULK POWER SYSTEM

JULIO C.S. SOUZA
DEE
CP 38 063 Gavea Rio de Janeiro Brazil

LEONTINA M.V.G. PINTO
PUC/RJ
CP 22452

Abstract - This paper presents a novel approach to the static security analysis of a bulk composite generation/transmission system. The algorithm is based on a relaxation technique that allows the inclusion of security constraints in a standard optimal operation model without a significant increase in computational effort. The model is able to evaluate system security indices not only in terms of the probability of a desired operating state (such as the probability of an extreme emergency) but also in terms of the severity of such states (measured, for instance, as the expected loss of load caused by extreme emergencies). It is also possible to evaluate the expected increase in operation cost necessary to ensure post-disturbance feasibility. Finally, it is possible to calculate sensitivity indices that indicate the best reinforcements to be made in order to accomplish a safer operation. The proposed algorithm is flexible and compatible with different system state selection criteria (enumeration, Monte-Carlo, etc.). Case studies with different realistic systems illustrate the application of the proposed methodology.

Keywords - Power Application Software, static security analysis, reliability, probabilistic methods

INTRODUCTION

A major aim of the reliability analysis is to assess the adequacy of an electrical network considering the associated uncertainties, such as load variations, equipment failures, etc. The network adequacy is usually expressed by indices related to the expectance of load curtailment necessary to bring the system to a feasible operating point, such as the Loss of Load Probability (LOLP) and the Expected Power not Supplied (EPNS). The adequacy assessment problem has been extensively studied and several models [1] and computational tools [2] have been proposed for its solution.

However, planners and operators look far beyond adequacy. It is well known that an adequate state may be unsafe: despite base-case feasibility, the occurrence of a disturbance may lead to violation on operation constraints and/or corrective load shedding. Although recognized as a major concern [3] and despite the earlier approaches proposed to solve it [4,5], the security analysis is still a challenge [6]. Recent IEEE meetings continue to address the problem (the security assessment was a preferred topic for the 1992 Summer Meeting) and new models, such as the described in [7], continue to be investigated.

The difficulty of this task lies basically on the number of system analysis to be performed. While the adequacy assessment requires, in principle, a base-case analysis for each of the set of possible network configurations, the security analysis needs the additional analysis of each post-contingency scenario per configuration. The increase in computational requirements may be dramatic: if the planner wishes to take into account, for example, a set of twenty contingencies (which is not too much for a real network, with hundreds or thousands of circuits), the computational requirements increase at least by a factor of 21 (twenty contingencies plus the base-case). Any model and corresponding computational tool for the security assessment must therefore handle this complexity carefully so as to compute accurate indices within a reasonable computational cost.

This paper presents a novel approach to the security analysis of a bulk composite generation/transmission system. The model is based on a relaxation technique that allows the network analysis to handle pre- and post-contingency operation constraints without loss of efficiency. The algorithm is able to assess:

- security indices such as the probability and severity of different system operating states (adequate, alert, emergency, extreme emergency)
- economic indices such as the expected increase in operation cost or expected preventive load curtailment necessary to ensure post-disturbance feasibility
- sensitivity indices which detect the best reinforcements that lead to a better security level or how to relax the security criteria in order to achieve a lower operation cost.

The model is general and can be used to extend most existing reliability programs. As an illustration, the proposed methodology is applied to the CREAM program [8], based on Monte-Carlo sampling and DC power flow. Case studies with realistic systems are presented and the obtained results discussed.

BASIC CONCEPTS

Identification of a system state

The objective of the security-constrained dispatch is to find an operating point that ensures system feasibility even in the case of a major disturbance. As it is not possible to protect the system from every possible contingency (as, for instance, the loss of many lines), the security analysis requires the specification of a set of contingencies - the critical contingency set - that should reflect the operation aims and strategies. For a given set, a system operating state can be classified as [9]:

- Normal: the system is able to supply the predicted load with no violation in its operating constraints and will remain feasible if one of the critical disturbances (contingencies) occurs.
- Alert: the system is able to supply the predicted load with no violation in the pre-contingency (base-case) constraints. However, system feasibility will not be sustained if one or more critical contingencies occur.
- Emergency: the operating point violates base-case operation constraints; the operator should perform the required control actions (as, for instance, generation rescheduling) to eliminate violations without load curtailment.
- Extreme emergency: the operating point violates base-case electrical constraints and it is necessary to curtail load to eliminate system problems. The total amount of load curtailment depends on the operation strategies implemented to bring the system to an acceptable state.
Adequacy x security assessment

System adequacy is generally assessed by reliability algorithms and measured in terms of the probability and severity of a system problem (emergency) or loss of load (extreme emergency). Emergency and extreme emergency scenarios can be detected by a simple base-case analysis, usually corresponding to an OPF. The difference between a normal and an alert state, however, can only be detected by a model able to assess system security: besides the base case, it is necessary to check feasibility of all critical disturbance scenarios.

Safe system x safe operating point

From the operator point of view, it may be important to check the security level associated to a specified operating point. If, for instance, a desired schedule fails to meet any post-contingency constraint, the system will be considered in an alert state even if there was an adequate generation reschedule able to bring the system to a normal state. The results of this analysis will therefore depend on the given operating point, regardless of the existence of a better (safer) schedule.

Reference [7] presents a model for the security analysis of an operating point based on a base-case OPF and post-contingency pure power flows. The proposed model is able to detect post-disturbance infeasibilities - and therefore to calculate probability indices; no severity indices are proposed.

On the other hand, most of the planning studies are related to the security level associated to a system. In this case, it can be assumed that the operator is able to find the best preventive operating point (using, if necessary, the models described in [10,11]). Under this assumption, a system state would be considered normal if there is any operating point able to meet all pre- and post-contingency constraints.

This analysis seems more realistic for planning purposes since it does not depend on an initial - and maybe inadequate - operating point. It is however more complex: instead of simply checking the feasibility of a given operating point, it is now necessary to perform a security-constrained dispatch and check the existence of a safe operating point. Next section formulates the security-constrained dispatch problem and discusses the available algorithms for its solution.

THE SECURITY-CONSTRAINED DISPATCH PROBLEM

The security-constrained dispatch requires that the operating point \( x \) remains feasible even if one of a list of \( n \) disturbances occurs and can be written as:

\[
\begin{align*}
\text{Min} & \quad c(x) \\
\text{s.t.} & \quad A_0(x) = b_0 \\
& \quad A_i(x) = b_i \quad i = 1, \ldots, n
\end{align*}
\]

where \( x \) is the operating point

\( A_0(x) = b_0 \) is the set of operation constraints

\( A_i(x) = b_i \) are the operation constraints associated to the \( i \)-th disturbance.

\( c(x) \) represents the cost associated to the preventive operating point - including, if desired, the minimum preventive load curtailment necessary to ensure that all post-contingency operation constraints will be met.

The number of constraints in problem (1) may be explosive. For each \( i \)-th configuration, the optimal operation of a system with hundreds of buses and lines corresponds to a problem subject to thousands of constraints. A critical set with only ten or twenty contingencies may easily lead to tens or hundreds of thousands of constraints and therefore to a problem which is extremely difficult - probably impossible - to solve by standard optimization techniques.

References [10,11] present a model for the security-constrained optimal dispatch illustrated in Figure 1. The algorithm uses mathematical decomposition techniques that allow the iterative solution of a base-case economic dispatch and several contingency analysis. Post-contingency infeasibilities are "translated" into constraints to be added to the base-case optimal dispatch problem, in order to achieve post-disturbance feasibility with the minimum possible cost.

THE DECOMPOSITION APPROACH

The key feature of this algorithm is the decomposition of an impossible-to-solve large scale problem into several manageable problems (one base-case and several contingencies) which can be solved by specialized optimal load flow models. It should nevertheless be noted that the computational burden necessary to perform a security-constrained dispatch is far from negligible.

Considering, for instance, a critical set of twenty contingencies and a small number of iterations to achieve convergence (three, for example) one security-constrained dispatch (which means the classification of one system state) would require 63 optimal load flows. The analysis of 10 000 states, typical in a reliability study, would require more than half a million optimal power flows and would therefore be infeasible within a reasonable computational burden. It was therefore necessary to develop a new approach, able to handle a high number of analysis, described in the next section.

THE PROPOSED APPROACH

The relaxation technique

The proposed methodology takes advantage of an important characteristic of electrical systems: a realistic network is never supposed to operate with too many violated constraints. As a consequence, most operation constraints could simply be dropped from the problem formulation with no loss of precision. Moreover, in realistic bulk systems, a contingency in a regional utility seldom has a significant impact on the whole system; it may therefore be possible to consider only the constraints in the affected area and neglect the rest of the system. The security-constrained problem can thus be simplified by taking into account not all but only the "important" operation constraints, identified by their impact on the desired significant indices.
This characteristic has been extensively exploited by different models: the linearized optimal operation algorithm described in [12] is based on the relaxation of most non-critical flow limits; convergence of decomposition methods used for system planning/operation [13] is usually fast because there are few system "bottlenecks" that really impact on the optimal solution; variance reduction techniques reported in [13-15] achieve a good representation of system problems with a few constraints.

The proposed algorithm

The algorithm can be summarized in the following steps:

• Construct the set of critical constraints
  \[ A_c(x) = b_c \]  
  (2)
  As the critical set is formed by all relevant pre- and post-disturbance operation constraints, the security-constrained problem (1) can be written as:
  \[ \text{Min } c(x) \] 
  \[ \text{s/to } A_c(x) = b_c \]  
  (3)
  where \( c(x) \) is a minimum load curtailment function

• Proceed to the security assessment:
  1. Select system configurations (scenario) using any desired method (Enumeration, Monte-Carlo, etc.)
  2. Test each scenario security: solve the security-constrained problem (3) using the following relaxation technique:

2.a First, drop all constraints that represent post-disturbance scenarios. The remaining critical constraints are used to form a relaxed (yet accurate) version of the base-case dispatch problem:
  \[ \text{Min } \lambda_1 = c(x) \] 
  \[ \text{s/to } A^0_c(x) = b^0_c \]  
  (4)
  where \( A^0_c(x) = b^0_c \) is the subset of critical constraints associated to the base-case

If an initial operating point is available, check feasibility of critical base-case subset. If this point fails to meet any constraint, the system is, in principle, operating in an emergency situation.

2.b Solve problem (4) and calculate the minimum base-case operation cost \( \lambda_1^* \).

2.c Continue the optimization process, now enforcing all post-disturbance critical constraints. The final problem is a relaxed (but accurate) version of the security-constrained dispatch:
  \[ \text{Min } \lambda_2 = c(x) \] 
  \[ \text{s/to } A_c(x) = b_c \]  
  (5)
  Solve problem (5), obtaining the solution \( \lambda_2^* \)

Remark: As the aim of security analysis is to check pre- and post-disturbance feasibility, the operation cost functions \( \lambda_1^* \) and \( \lambda_2^* \) represent respectively the minimum load curtailment to achieve base-case and post-disturbance feasibility. Should an economic security assessment be performed, other cost functions could be used to reflect the desired objectives.

2.d Use the minimum values \( \lambda_1^* \) and \( \lambda_2^* \) to classify the operating state:

• A normal state is characterized by null base-case and preventive load curtailment values:
  \[ \lambda_1^* = 0 \]  
  (6-a)
  \[ \lambda_2^* = 0 \]  
  (6-b)

• An alert state corresponds to a null base-case and a positive preventive load curtailments:
  \[ \lambda_1^* = 0 \]  
  (7-a)
  \[ \lambda_2^* > 0 \]  
  (7-b)

• Emergency states are, if desired, detected at the beginning of the process. An extreme emergency state is detected if it is necessary to curtail load in the base-case and consequently also in post-contingency scenarios:
  \[ \lambda_1^* > 0 \]  
  (8-a)
  \[ \lambda_2^* > 0 \]  
  (8-b)

Store operating state classification and optimal values \( \lambda_1^* \) and \( \lambda_2^* \) for final security indices evaluation.

3. Calculate security indices:

• Probability of each system state

• Severity of each system state

The standard adequacy analysis generally takes the expected base-case load curtailment \( E(\lambda_1) \) as a severity index for an extreme emergency severity. This idea can be extended to use the expected preventive load curtailment as a measure of the severity of an alert state. As in the adequacy assessment, the practical interpretation of this index depends on operation strategies: it seems reasonable to curtail load to prevent, for instance, a blackout; no one would agree, however, to shed load to alleviate a small overload.

KEY FEATURES OF THE PROPOSED APPROACH

Compatibility

The relaxation algorithm is general and can be used to extend most standard AC or DC OPF tools to handle security constraints. Dynamic restrictions written as the sum of generations and line flows correspond to standard constraints and can be trivially handled by the security-constrained problem. Moreover, the model does not depend on the technique used to select system states and can be used both with Enumeration or Monte-Carlo based approaches.

Severity indices

As in the traditional adequacy assessment based on optimization algorithms [8], it is possible to evaluate - with no additional computation effort - bus security indices, such as the expected base-case or preventive load curtailment.
Sensitivity analysis

It is possible to obtain, as a by-product of the optimization process, the sensitivity of preventive load curtailment with respect to generation and transmission reinforcements. As reported in [8], these sensitivities can be derived directly from the dual multipliers associated to the generation limit constraints.

Security price

Despite the use of the minimum load curtailment function to represent operation costs, the model is general and can accommodate other cost functions. For example, an economic cost function would be more suitable for an analysis of the economic impact of the security requirements.

Reference [16] discusses an important issue concerning the security analysis: the "security price". It is shown that the security problem is more constrained than the economic dispatch and therefore:

\[ \lambda_2^* \geq \lambda_1^* \]

As a higher security level is usually associated to a higher cost, an important question is the cost increase that the operator/planner would accept to pay in order to accomplish a safer operation. For instance, the relaxation of a tight security requirement (such as remaining feasible for an unlikely severe disturbance) may lead to a significant economy in terms of operation cost.

As proposed in [16], the dual multipliers associated to post-disturbance constraints can provide useful information for the price/security trade-off. These multipliers can be seen as the sensitivities of the objective function (i.e., operation cost) with respect to variations in each constraint limit and can be used to calculate the improvement in the operation cost associated to a disturbance relaxation.

The Optimal Power Flow

The objective of the OPF is to minimize system operation costs, subject to operation constraints such as network equations, limits on circuit flows and bounds on generation. The linearized OPF corresponds to a linear programming (LP) problem:

\[
\begin{align*}
\text{Min} & \quad C P \\
\text{s.t.} & \quad P = B \theta \\
& \quad F = A P \\
& \quad P \leq P \leq P \\
& \quad E \leq F \leq F
\end{align*}
\]

where

- \( P \) is the vector of net active power injections (generation-load)
- \( C \) is the vector of power injection costs
- \( \theta \) is the vector of node voltage angles
- \( B \) is a matrix given by
  \[
  B = S \gamma S
  \]
  is the node-branch incidence matrix
  \( \gamma \) is the diagonal matrix of circuit susceptances
- \( F \) is the vector of active line flows
- \( A \) is the matrix of the sensitivities of flows with respect to node injections given by
  \[
  A_{ij} = e_i B^{-1} e_j
  \]
  is the vector of sensitivities of the active flow in line \( ij \)
  \( e_i \) is an auxiliary vector whose elements are null except for element \( i \) (equal to \( \gamma_i \) and \( j \) (equal to \( \gamma_{ij} \))
- \( P \) and \( P \) are the vectors of active power injection limits
- \( E \) and \( F \) are the vectors of active flow limits

One of the most widely used algorithms to solve the linearized DC OPF is described in [12]. This model can be extended to represent load curtailment as dummy generators [8], thus allowing the representation of the minimum load curtailment linear function. Non-linear cost curves (representing, for instance, fuel costs) are piecewise linearized. It is also possible to include additional linear constraints to accommodate, for instance, utilities interchange or dynamic constraints.

The overall approach is based on a dual relaxation technique that can be summarized as:

1. Relax all flow constraints. Perform a merit order dispatch, i.e., determine the optimal generation schedule regarding only generation limits.
2. Check for circuit overloads (note that all generation limits are met). If there is no overload, the optimal solution was found.
3. Take the most violated circuit. Perform an optimal generation rescheduling (including, if desired, load shedding) to eliminate the overload. Go back to step 2.

The optimal generation scheduling mentioned in step 3 corresponds to adjusting (at a minimum cost) the generations in order to bring the violated flow to its limit. Reference [12] shows that the final values of bus generations are given by a linear system composed by the set of active power injection/flow constraints met at their limits \( L_g \) and \( L_r \):

\[
\begin{bmatrix}
A_{ij} \\
0
\end{bmatrix}
\begin{bmatrix}
P
\end{bmatrix}
= \begin{bmatrix}
L_t \\
0
\end{bmatrix}
\]

514
It may be seen that, while the submatrix $A_t$, corresponding to active flow constraints, is "dense", the injection constraints are simply represented by an identity. This special structure is extensively exploited by the customized LP algorithm. Injection limit constraints are trivial and it is not difficult to handle a large number of controllable generators. On the other hand, the algorithm is extremely sensitive to the number of flow equations met at their limits (corresponding to the size of submatrix $A_t$).

Reference [12] reports that this number is not very high. The elimination of an overload may eliminate other overloads. In other words, bringing the most violated constraint to its limit (that is, including the constraint in submatrix $A_t$) may turn it unnecessary to consider other violated constraints. Thus, $A_t$ does not correspond, in principle, to all constraints that were overloaded at the beginning of the optimization process, but to all "important constraints" - known as active constraints - met at their limit at the end of the process. These results have been confirmed in practice: this algorithm has been used for many different systems and purposes, such as operation [10], planning [17] and reliability analysis [8]; the number of constraints being simultaneously held in submatrix $A_t$ is seldom higher than ten, even for bulk systems.

The inclusion of additional constraints in submatrix $A_t$, such as limits on area interchanges or sum of active generations/flows in a given region (for dynamic security representation), is straightforward. It is however important to stress that a high number of active additional constraints may imply in an undesirable increase in the size of submatrix $A_t$ and therefore in loss of efficiency.

**The critical constraint set construction**

As generation limit bounds can be trivially handled by the LP algorithm, the critical set construction will be focused on the determination of the "important" flow constraints - and corresponding critical circuits (lines, transformers) that have a significant impact on the system security.

Each contingency corresponds to a different network configuration. As a consequence, a critical circuit may be associated to several critical constraints - one for each different pre- and post- disturbance scenarios. The detection of the critical constraints should, in principle, require the analysis of a higher number of post-contingency configurations than the identification of the critical circuits. For this reason, the first step will correspond to the construction of the smaller critical circuit set. A further post-contingency analysis will compute the corresponding critical constraint set.

If all pre- and post-disturbance scenarios could be enumerated, the set of critical circuits could be constructed by the following algorithm:

1. Select a system scenario
2. Check for flow constraint violations. If there is no violation, there is no critical circuit for this configuration; go back to 1.
3. Else, perform an OPF. Include all circuits corresponding to the active constraints held by submatrix $A_t$ at the optimal solution in the critical circuit set. Go back to step 1.

As the number of possible scenarios can not usually be enumerated for bulk systems, it becomes necessary to establish a selection criterion, which should be closely related to the critical post-disturbance set.

Considering a critical contingency set determined by the following rule:

The system must be feasible for each circuit contingency; uncertainties associated to generation faults must also be considered according to corresponding probability.

three methods for the scenario selection criterion may be attractive:

1. Enumerate all single line faults. Assume no generation outages.
2. Enumerate all single line faults. For each line contingency, sort generation outages according to failure probabilities.
3. Use Monte-Carlo method to sort a number of possible disturbances (say, 1000): (one line fault plus generation outages).

The critical circuit sets obtained with each method were checked for 10 000 possible disturbances (one circuit outage + sampled generation outages) sampled by the Monte-Carlo method. Each scenario was analyzed by two optimization models that calculated the minimum load shedding necessary to eliminate violations in:

- all circuit constraints
- only the constraints associated to the critical circuit set.

The error associated to the critical set representation can be measured by the difference between the load curtailment calculated by both models. An accurate critical circuit set should naturally reflect system problems and therefore lead to close results in both models.

The obtained results are summarized in Table 1, where the errors associated to each method are given as the percentage of the exact expected preventive load curtailment. It may be seen that method 1 was not able to provide a good critical set, probably due to the generation outages influence. On the other hand, methods 2 and 3 showed a good performance: both came out with the same critical circuit set - which represented exactly the system problems.

<table>
<thead>
<tr>
<th>SYSTEM</th>
<th>METHOD 1</th>
<th>METHOD 2</th>
<th>METHOD 3</th>
</tr>
</thead>
<tbody>
<tr>
<td>MRITS</td>
<td>0%</td>
<td>0%</td>
<td>0%</td>
</tr>
<tr>
<td>SSE</td>
<td>23%</td>
<td>0%</td>
<td>0%</td>
</tr>
<tr>
<td>BPA</td>
<td>15%</td>
<td>0%</td>
<td>0%</td>
</tr>
</tbody>
</table>

Table 1 - State selection criterion performance

It is interesting to note that, although unable to estimate the expected preventive load curtailment, the critical set constructed by method 1 was able to detect all alert states and therefore to calculate exact probability indices. This result is not unexpected: if a disturbance leads to many overloads, only one of the violated circuits is enough to detect the alert state; however, the correct evaluation of the state severity would require all the active flow constraints.

A question concerning the Monte-Carlo based method 3 is the number of samples necessary to obtain the critical set. The same study was repeated for 2 000, 3 000 and 5 000 samples: no new critical circuit was detected. The 1 000 sample size required to construct the critical circuit set may be considered small: the enumeration method would require the analysis of almost 700 line outage scenarios for the BPA system.
It should also be noted that Monte-Carlo method is more robust than enumeration: while, in some cases, the enumeration method may "miss" important line/generator fault combinations, the Monte-Carlo based method can sample configurations until "convergence". (for instance, N samples without finding any new critical circuit.

This process may be illustrated with the BPA case study. Convergence criterion was set to five hundreds consecutive samples without a new critical circuit and was achieved in 1350 samples (850 for set construction plus 500 for convergence). Twenty-eight critical circuits were found in approximately two minutes.

Table 2 presents a key factor for the relaxation method performance: the number of critical circuits. It can be seen that the number of critical circuits can be considered small. Furthermore, it may be noted that it does not grow linearly with the size of the system.

<table>
<thead>
<tr>
<th>SYSTEM</th>
<th>NUMBER OF CRITICAL CIRCUITS</th>
<th>Number</th>
<th>% of total</th>
</tr>
</thead>
<tbody>
<tr>
<td>MRTS</td>
<td>12 circuits</td>
<td></td>
<td>30%</td>
</tr>
<tr>
<td>SSE</td>
<td>21 circuits</td>
<td></td>
<td>12%</td>
</tr>
<tr>
<td>BPA</td>
<td>28 circuits</td>
<td></td>
<td>4%</td>
</tr>
</tbody>
</table>

Table 2 - Critical circuits

Eliminating repeated constraints

Given the set of critical circuits, the critical constraint set may be now obtained: for each critical circuit and for each critical contingency, equation (12) is used to derive the corresponding constraint.

The number of critical constraints may still be very high. As each disturbance corresponds to a different network configuration, each circuit may lead to 2 \((n+1)\) upper and lower bounds) flow constraints. Taking the BPA system, for instance, the 28 critical circuits would correspond to 2 \times 28 \times 679 = 38,024 constraints. It is therefore necessary to improve the problem size reduction.

This may be done considering that most disturbances have a local or regional effect and do not impact the whole system. Consequently, flow constraints do not usually change for every different contingency. Therefore, the algorithm tests for redundancy before storing the constraints:

- For each critical circuit
  - for each critical constraint
    - use equation (12) to obtain flow limit constraint
    - compare the new constraint with the already stored and check for redundancy
    - Redundant? Discard
      - Not redundant? Include in the critical constraint set.

This algorithm was checked with the three systems. The maximum number of different (total, not active) constraints was not higher than 200 - a good result, since the number of constraints in a simple OPF can easily reach thousands.

As the triangular factors of matrix \(B^{-1}\) are available from the power flow analysis, the computational effort required to compute all constraints (even the redundant ones) is not very high. For instance, the BPA study reduced the critical set to 196 constraints in less than 20 seconds.

Some Numerical Results

This section describes in more detail the application of the proposed algorithm to a real-life system. The BPA system was chosen since it is the more complex. It must be stressed that this corresponds only to an illustration with a non-updated network and final data were not checked with BPA. Therefore, the presented results, though giving a good idea of the algorithm performance, do not reflect the system security level.

The critical constraint set obtained after redundancy elimination was used to perform the security assessment of the three systems. The first study pointed out an unexpected characteristic common to all three systems: none of them was able to resist to all single line faults - probably because of the lack of the subtransmission links, which may have a significant importance in disturbance situations. In order to illustrate the performance of the security analysis algorithm, two different sets of forty line contingencies, selected at random, were chosen to form the critical disturbance set.

Tables 3 and 4 show some results of the security analysis for the BPA system. Each sample corresponds to the analysis of the base case plus each critical contingency. The Alert State Probability (ASP) and the Expected Preventive Power Not Supplied (EPPNS) may be compared to the traditional LOLP and EPNS adequacy indices.

<table>
<thead>
<tr>
<th>Estimate</th>
<th>LOLP</th>
<th>EPNS</th>
<th>ASP</th>
<th>EPPNS</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.06</td>
<td>16.35</td>
<td>0.52</td>
<td>366.70</td>
<td></td>
</tr>
<tr>
<td># Samples</td>
<td>1000</td>
<td>567</td>
<td></td>
<td></td>
</tr>
<tr>
<td>CPU Time</td>
<td>18 min</td>
<td>6 min</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Each OPF</td>
<td>0.273 sec</td>
<td>0.576 sec</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Table 3: Results for critical disturbance set 1.

<table>
<thead>
<tr>
<th>Estimate</th>
<th>LOLP</th>
<th>EPNS</th>
<th>ASP</th>
<th>EPPNS</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.06</td>
<td>16.35</td>
<td>0.15</td>
<td>67.59</td>
<td></td>
</tr>
<tr>
<td># Samples</td>
<td>1000</td>
<td>3671</td>
<td></td>
<td></td>
</tr>
<tr>
<td>CPU Time</td>
<td>18 min</td>
<td>21 min</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Each OPF</td>
<td>0.273 sec</td>
<td>0.282 sec</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Table 4: Results for critical disturbance set 2.

It can be seen that:

- The results confirm typical Monte-Carlo characteristics: the worst case, corresponding to a very high expected preventive load curtailment, was "easier" to estimate than the low base-case EPNS; the higher EPPNS (table 3) also converges much faster.

- Although the number of samples is significantly smaller, the security assessment of each sample requires a higher computational effort than the pure adequacy assessment. However, this increase is acceptable: the total computation time required for both security and adequacy assessment is approximately the same. Considering that the size of the standard security problem is hundreds or thousands higher than the adequacy problem, doubling the computation time may be considered a good result.

- The "security price", in this case, is measured by the increase in the expected value of the preventive load shedding: approximately 350 MW for the first case and 50 MW for the second.
Sensitivity Analysis

It may be seen that the security requirements associated to the first critical disturbance set lead to a high operation cost. A sensitivity analysis was carried out to determine which critical disturbance to relax in order to achieve a lower operation cost. All disturbances were ranked by sensitivity order and the (most sensitive) one was discarded from the critical disturbance set. The new results showed a new EPPNS equal to 10% of the initial value - in other words, the relaxed critical disturbance was responsible for 90% of the expected preventive load curtailment.

CONCLUSIONS

This paper presents a novel model for the security assessment of bulk generation/transmission power systems. A relaxation technique was used to reduce the large scale security-constrained dispatch, with thousands or millions of constraints, to a medium-sized manageable problem. The main features of the proposed algorithm are:

- The compatibility with existing reliability methods
- The evaluation of security indices such as the probability of an alert or emergency state and the expected "security cost", represented as the increase in the operation cost necessary to meet security criteria.
- The sensitivity analysis, able to point out the best reinforcements in order to improve system security and the critical contingencies responsible for the highest increase in operation cost.

The proposed methodology was applied to an available reliability assessment program - CREAM. Case studies with different realistic systems illustrated the performance of the proposed algorithm: it was possible to calculate the desired security indices with no substantial increase in computational requirements.

FURTHER WORK

Two natural extensions of this work are now being investigated:

1. The complete AC implementation is now completed. This extension is straightforward and preliminary results show that the number of constraints necessary to represent voltage limits is much smaller than the number of constraints necessary to represent overloads. A complete report is now being prepared and will be published soon.

2. The extension to accommodate dynamic constraints is a much more difficult task. As discussed in this paper, a set of simulations of the system performance for different contingency scenarios starting from a given operating point is not, in our point of view, a correct way to analyze system security. As described, the security analysis will only be independent from the operation point if security constraints can be formulated as a function of generations and/or loads.

This target seems to be met by the work reported in [18,19] - a new model able to formulate dynamic constraints as a function of bus loads (and therefore generations). The inclusion of these constraints in the security analysis is now being investigated and may make it possible the joint static/dynamic analysis without a significant increase in computational requirements.

REFERENCES