1982

A framework for automatic security maintenance procedures

Talukdar
Carnegie Mellon University

Navin Tyle

Ravi Mehrotra

A FRAMEWORK FOR AUTOMATIC SECURITY MAINTENANCE PROCEDURES

by

3.N. Talukdar, R. Mahrotra 4 N. Tyla

Deceoiber, *1^12*

DRC-13-53-32

A FRAMEWORK FOR AUTOMATIC SECURITY MAINTENANCE PROCEDURES

Sarosh N. Talufcdar Ravi Mehrotra Navin Tyle

Power Engineering Program
Department of Electrical Engineering
Carnegie-Mellon University
Pittsburgh. Pennsylvania 15213

Abstract * This paper deals with security from the dispatcher's point of view and over operating horizons shorter than those used for unit committment. In this environment, the basic engine for automatic decision asking is the Optimum Power Flow (OFF). We seek to extend OPF procedures so that they can maintain security at or above preselected levels. To do this we first define an improved metric with which to measure security. The metric is continuous. Includes contingency probabilities and can be adjusted to reflect some contingency impacts. Next, we devise two ways of translating security as measured by the metric into constraints that can be added to an OP*". The first way uses currently available data. The second way is more powerful but requires data not now available. Both ways add large numbers of constraints for each contingency considered and so, result in rather large optimization problems. Algorithms for solving these problems have not yet been devised but some promising, parallel processing directions are becoming evident and are described in the last part of the paper.

I. THE PROBLEM

This paper is concerned with the centralized control of power systems for normal operations over short horizons - from a few minutes to a few hours into the future. More specifically, the problem of concern is how to schedule the power flows, voltages and other essentially continuous operating variables in order to minimize some cost function while maintaining an adequate level of security and meeting any other applicable constraints such *as* caps on the rates at which various emissions may be produced. The rest of this section will be devoted to better describing this problem and its importance.

I.I Operating States

Among the concerns in operating a power system are two sets of criteria that DyLlacco [3] called Load and Operating Constraints. The former requires all the loads be met in full; the latter Imposes limits on the values of system variables. DyLlacco went on to divide operations Into three "states'*: normal, restorative and emergency, defined as follows: The system is normal when the load and operating constraints are met. The system is in an emergency state when there are major violations of the operating constraints. The system is in a restorative state when only the load constraints are violated.

Ve note that the operating constraints are time dependent. For instance, the half-hour-rating of a line is greater than its 24 hour rating. Therefore, to remain normal the dispatcher may have to shift the system's operating point even though the loads and other exogenously specified quantities remain constant.

1.2 The Single Contingency Assumption

Ve will use the term "contingency" to mean a random disturbance that either causes, or can be modelled by, a change in the configuration of the system. Let C • {cif*»Cg) be the set of K separate contingencies that could occur over the current operating horizon.

Theoretically, two or more contingencies could occur simultaneously or within a short Interval. However, the likelihood of this eventuality Is usually low and the effort required to deal with it, high. Therefore, it is usual to assume that contingencies need only to be considered singly and that there will be enough time for a system to recover before the next contingency occurs. Ve will adopt this assumption in all succeeding developments.

1.3 T-Stablllty [21

Every time a power system changes its configuration a flurry of transient activity is produced that could trip relays and thereby, cause another configurational change. To distinguish cases where this will not happen, we will say that a configuration is T-stable when it outlasts the transients produced at its inception (Note that the more familiar notion of asymptotic stability does not imply T-Stabillty. The former allows transient excursions to be arbitrarily large as long *mm* they remain finite; the latter requires the excursions to remain small enough to keep from tripping relays.)

1.4 Configuration Chains [21

Let:

N be the set of components - generators, lines, etc - that make up the power system. Ve will attach subscripts to H to denote subsets that contain only on-line components. Since the topological arrangement of the system is fixed except that each of its components may be either on-line or off, these subscripted symbols can also be used to denote configurations.

Ho b* the existing (Incumbent) configuration "lk»*2k»*°*»**k ^e tne ch**-11 °£ configurations precipitated by the occurrence of c_k (see Fig. 1). The chain terminates when the system returns to normal operations. The terminal configuration, N^*_k, must of course, be T-Stable. Each configuration after N_{1k} comes into being either because its Immediate predecessor is not T-Stable or because of intervention by the dispatcher — the removal

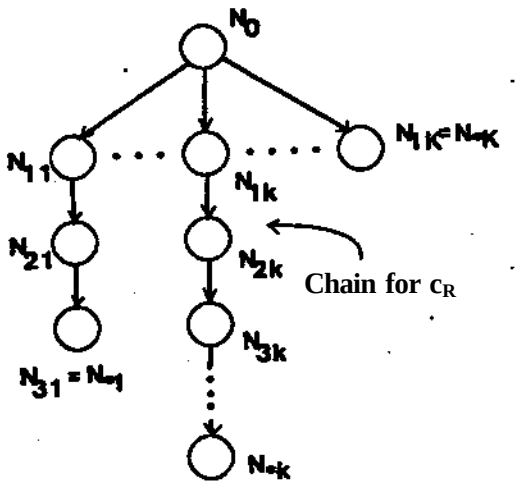

Fig. 1: Configuration Chains. Usually, the longer the chain the more serious the contingency. If N^*_k is empty, c_k will produce a system-wide-blackout. If N^*_k - N_o, the system returns to its original configuration and c_k has no lasting effect.

of a line to more favorably redistribute power flows, for instance.

F^ • Max {|N_{1k},N_{2k}|} where iN^jJis the number of of elements in the set N_{1k} \ will be called the minimally depleted configuration of c_k. If the topological effects of c_k are eliminated by a re- closure, 5^ - N2k* Otherwise S_k • Hj^.

1.5 Prediction Difficulties

The prediction of configurational transitions that result from a lack of T-Stabllity can be quite difficult. Transient stability and long-term-dynamic-simulation programs help by providing a means to simulate the response of the system to disturbances. But they are too computationally Intensive to use for real time control. And, though they provide good data on general trends and tendencies, for particular cases they yield far from Infallible results. The reasons are two fold. First, good dynamic models for many entities — loads and neighbouring systems, for instance — do not exist. Second, the programs do not adequately capture the stochastic nature of many phenomena — relay thresholds and redosure successes, for instance.

1.6 The Importance of Prior Positioning

Besides the difficulties they Inject Into prediction processes, there are other reasons for avoiding transitions that result from a lack of T-Stabillty. They have to do with the natural desire of dispatchers to keep their systems normal as much of the time as possible, even after a contingency has occurred.

There is good reason to belleve-see [4], for instance — that if the transmission network remains essentially intact for the first few swings caused by a contingency, and if there Is enough generation reserve, then there are strategies for keeping the system normal or at least, quickly returning it to normalcy.

To keep the network intact we must prevent transitions that result from T-Instabillty. But the time Interval spanning the first few swings is of the order of a second in length — too short for centralized agents (human or mechanical) to take action that would be effective in augmenting T-Stability, instead central agents must rely on positioning the system (i.e. selecting its operating point) prior to the occurrence of a contingency.

1.7 Security

The term security refers to a system's ability to remain normal despite the occurrence of contingencies. Intuitively, a system would be perfectly secure if all its possible terminal configurations were normal; it would be perfectly insecure if it were guaranteed to reach an abnormal terminal configuration during the operating horizon. It makes good engineering sense to allow for a continuum between these two extremes*and to arrange for an actual system to occupy a portion in the continuum depending on the likelyhood of its attaining an abnormal terminal configuration and the degree of abnormality that would result.

1.8 A Binary Security Metric [3] and its Disadvantages [1].

The only metric now available for measuring security is binary. It construes the system as being secure when the system is normal and none of the contingencies in C could cause a transition to an emergency state; otherwise the system is construed as being insecure. This metric has several major failings.

- It misses the fundamentally continuous nature . of security.
- It does not take into account the probabilities of contingencies. A contingency that is only moderately likely to occur is given as much importance as a contingency that is very likely.
- It does not take into account the degree of abnormality. A minor transgression of the load or operating constraints is given the same importance as a major transgression.
- It provides little prescriptive information. It merely indicates which contingencies would cause violations of the load and operating constraints.
- It is profoundly difficult to evaluate accurately — a consequence of the problems inherent In predicting terminal configurations (see 1.5)

These failings are not critical in the operating environment that now exists. The reason is that a scalar metric is not absolutely necessary. Dispatchers can and do use judgement to factor concerns like contingency probabilities and impacts into their security related decisions. However, if security maintenance is to automated, it will be best to start with precise, numerical representations for security levels. The difficulties Involved in Including fuzzy processes like judgement make the automation problem several times more complex. This means that new security metrics will be required; the failings of the binary metric render it unfit for use in automated processes.

1.9 The Need for Automatic Security Maintenance[1]

The basic functions of a centralized control facility are: data collection and display, analysis (limit checking, state estimation and contingency checking) and control for the normal, emergency and restorative states. Of these, the control function is least automated. There are no provisions for automatically scheduling voltages nor any for accommodating security except to the extent of meeting total load. Only the real power outputs of the generators are automatically scheduled and then, only -when the system is normal. All other decisions are left to the dispatcher.

The complexity of the decision making environment is increasing. Some of the reasons are Increasing interconnections, increasing amounts of energy shipped between and across systems and increasing numbers of decision variables. Dispatchers could use some help in handling decision making chores, particularly in the area of security where the amount of detail is large and the consequences of errors, serious.

1.10 Operating Variables and Constraints.

The variables of interest to dispatchers can be divided Into two categories — discrete and continuous. The former, consisting largely of generator commitments and breaker positions, can be used to make configurational changes. The latter can be divided into four vectors:

U c R*, a vector of variables whose values are controlled by regulators. U consists largely of generator-voltage-magnitudes, generator-real-power-outputs, transformer tap positions and loads that can be continuously managed, m is typically of order 100.

E e R^q, a vector of exogenously specified variables. E consists largely of unmanaged loads.

X e R^n, a set of state variables consisting largely of generator-reactive-powers, generator-voltage-angles and the magnitude and angles of the voltages at non-generator-buses, n is typically of order 1000. In a steady state, X is related to E and U by the power flow equations that can be put in the form [1]:

$$H(TJ, X, E) - 0 \qquad (1)$$

where H: $R^{* n * q} \to R^n$. The Load Constrains mentioned in I.I are a subset of (1).

B c R^p, a set of critical variables such as the power flows through major lines. Elements of B are either monitored by the dispatcher or cause relays to trip when they cross preassigned thresholds. In a steady state, B is related to X, E and U by a set of strongly nonlinear algebraic equations that can be put in the form [1]:

$$B - G(U, X, E) \qquad (2)$$

where G; $R^{m * n + q} \to R^2$. The Operating Constraints mentioned In I.I consist of limits on B of the form:

$$B \geq \underline{B} \qquad (3)$$

1.11 Rescheduling Windows

As far as the continuous variables are concerned, the dispatcher's means of control are limited to adjusting the set of points of the regulators that act on U. Some of the regulators are fast acting and the associated elements of U, like transformer tap positions, can be changed very quickly. Others, like generator power outputs, are rate limited. As a result the amount by which D can be changed in time t Is limited to a window about the initial operating point, U_Q. The larger t, the larger the window. The constraints that delineate this rescheduling window can be put in the forms:

$$U_O \text{ " } \wedge (U_O \text{»} t) \; 1^u \pounds^{u_o} \cdot 5 (V_O \;, t) \qquad (4)$$

or

$$U \text{ e } W(U_o, t) \qquad (5)$$

where D, 5: $\mathbf{I}^{m+1} - R^{-}$

1.12 A Wotatlonal Convention

In subsequent developments we will attach the subscript k to the symbols defined in I.10 and I.11 to associate them with the minimally depleted configuration. Thus, $\backslash_9 X_k$, E_k, etc. are the values of U, X, E etc. in 5^.

1.13 Optimum Power Flows (OPFs)

An OPF is a scheme for scheduling the continuous variables in a power system. It does this by minimizing a cost function while maintaining a set of algebraic constraints that constitute a static model of the system. The economic dispatch is the simplest forn of an OPF. It contains only one constraint - that total generation be equal to total load plus an approximation to total losses. More elaborate forns can include thousands of constraints [1], [15].

We focus on OPFs because as far as the continuous variables are concerned, they are , and will in all probability continue to be, the basic engines for automatic decision making.

The alternatives are formulations that use dynamic models and artiflcal intelligence techniques like Expert Systems [14]. The dynamic models involve a great deal of complexity and do not necessarily provide wore reliable' results than good static models augmented by judiciously chosen safety margins (see III.l) The artificial intelligence techniques have more promise for discrete variable decisions, and, in any case, require much more research to be serious contenders [16]. For further details on OPFS see [1], [15], [17].

1.14 Goals

We seek a scheme for automatically scheduling all the continuous variables by solving an OPF of the form:

(0P1): $\underset{U_o}{\text{Min}} \; <KU_o, Xp, Eo)$

St.: $S \geq a \qquad (6)$

$V \geq 0 \qquad (7)$

where:

•is a cost function selected by the dispatcher

U_otXo,Eo are the values of U, X and E for the existing configuration.

S is the security of the existing configuration

a is the minimum acceptable level of security

(7) is a set of any other constraints the dispatcher would like to impose, for instance, caps on the rates of production of various emissions.

To develop and implement this scheduling scheme five major tasks must be completed:

- define a metric for measuring security that is continuous, reflects contingency probabilities and by and large, better agrees with the notion of security (1.7) than the binary metric described in 1.8
- express (7) in terms of schedulable variables
- develop an algorithm for solving (0P1)
- develop the hardware for running the algorithm
- translate the algorithm into software.

The literature on security, eg [5] - [9], has been concerned more with analysis than prescription and hence, has not addressed these tasks in great detail.

In the rest of this paper we will focus on the first three of the.flv* tasks..

II. AH IMPROVED SECURITY METRIC

11.1 Contingency Types

In terns of their severity, contingencies can be divided into three categories:

- minor - if the system is properly positioned before the contingency the minimally depleted configuration will be T-Stable and normal. The dispatcher need take no further action. A small minority of all contingencies belong to this category.
- moderate - proper positioning can make the minimally depleted configuration T-Stable and normal but only if short term ratings and resources are used. The dispatcher has to make conflgurational changes before the short term capabilities run out. Most contingencies belong to this category.
- major - there is no position for the pre disturbance system that will cause the minimally depleted configuration to be T-Stable and normal. A loss of normalcy is inevitable. Should such a contingency occur the dispatcher's objective is to restore normalcy with a minimum of trauma. A small minority of contingencies belong to this category.

11.2 Concerns

II.1 indicates that the principal concern in making a system secure is to position it, prior to the occurrence of any contingency, so that the minimally depleted configurations resulting from the occurrence of the minor and moderate contingencies, will be T-Stable and normal.

Auxiliary concerns are:

- for moderate contingencies to have enough rescheduling room to move the system to a long-term-normal-operating-point before the short term capabilities run out.
- To minimize the adverse impacts of major contingencies (i.e. to develop emergency and restorative strategies).

In the subsequent material we will focus on the principal concern and write expressions in terns of the two configurations involved with this concern, namely, the incumbent configuration, N_o, and the minimally depleted configuration, 5^. However, the OPF formulations we develop can be applied to rescheduling and restorative problems by replacing N_o and $\bar{N}_k$ by the configurations relevant to these problems.

11.3 The Probability of Normalcy

We will now define a continuous security metric that Includes contingency probabilities.

To make a system perfectly secure we would have to insure that the minimally depleted configuration for every possible contingency would be T-Stable and normal. For high but not perfect security, we need the chances of 8^ being T-Stable and normal to be high, especially if the associated contingency, c^, is likely. This idea can be captured in a metric in the following way. Let:

L be the length of the horizon considered

N_Q be the incumbent configuration (that exists at the beginning of the horizon), N_Q must be T-Stable and normal. Otherwise the system is either in an emergency or a restorative state and security considerations are irrelevant.

QQ be the probability that no contingency occurs In L, i.e., the probability that N_o persists uninterrupted over L.

Ok be the probability that cfc will be the first contingency to occur In L.

P_k be the probability that $\bar{N}_k$ is T-Stable

P£ be the probability that $\bar{N}_k$ is normal or can be made normal in time t_k. (The value of r_k is to be selected by the dispatcher. More will be said about this in II.4(a)).

S c [0,1] be the value of security. S-l means that N_o is perfectly secure. S*0 means that the system is guaranteed to become abnormal in the operating horizon.

We define S as follows:

$$S - Q_o + \sum_{k=1}^{K} Q_k P_k P'_k \qquad (8)$$

In words, S is the probability that either no contingency occurs over the entire horizon or, if a contingency occurs, the system will remain normal.

II.4 Remarks

(a) The definition of the metric makes no explicit mention of contingency impacts - the degree of abnormality, if any, produced by contingencies. In other words, a contingency with a small impact, like a small violation of the operating constraints, has not been explicitly distinguished for a contingency with a large Impact. We might arrange for an Implicit distinction through the values of the probabilities P_k. However, we prefer a more direct approach. We allow the dispatcher to choose a time, t_k, for each contingency. If the minimally depleted configuration of the contingency is initially abnormal but the abnormality is small enough to be eliminated by rescheduling in t_k, then the configuration will be treated as if it were uninterruptedly normal.

(b) We note in passing that the security metric is akin to the probability-of-loss-of-load-metric used in expansion planning.

III. SECDRITY ENHANCEMENT

Contingencies and their occurrence probabilities are outside the dispatcher's control. Therefore, the only way for a central agent (human or mechanical) to change the value of S is by changing P_k and P£, k«l, ...,K.

III.l Using Safety Margins to Increase Pv

Let RQ be the region in the space of U that is feasible in terms of the load and operating constraints embodied in (1) - (3) for the incumbent configuration, N_o. In other words

$$Ro - \{U \mid H_o(U,X,E_o) - 0, G_o(U,X,E_o) - ^ \geq 0\} \qquad (9)$$

Actually, all of RQ is not used for operations. Instead it is reduced by the addition of safety margins (sometimes called stability margins) to the operating constraints. Let these margins be denoted by M and the reduced region they produce, by RQCM). Then

$$^(M) - \{U|H_o(U,X,E_o) - 0,\ C_o(U,X,E_o) - ^ \geq M\} \qquad (10)$$

RQ and R_o are illustrated in Fig. 2.

The purpose of the margins is to enhance the chances of the minimally depleted configurations of the minor and moderate contingencies being T-Stable. The greater the value of M the greater the values of P_k for these contingencies.

Over the years a great deal of thought, judgment, analysis and experience have gone into the determination of a value for M that makes Pk *l*°st unity for the minor and moderate contingencies. We will denote this value of M by M^*. Some representative examples of the elements of M^* are: 20% reserve margin

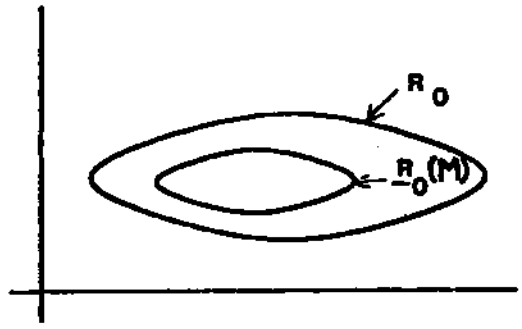

Fig. 2: R_Q, the normal region for N_o and ^(M), the region obtained by the addition of M, the vector of safety margins.

on generation and at most 20° of angle spread across key transmission lines.

Ill.2 Making Py • 1

Let R^ be the region in the space of U that is feasible in terms of the load and operating constraints for configuration N^. That is*

$$R_k = \{U | R_k(U, X.Efc) - 0,\ G^U.X.Efc) - ^ \geq 0\} \quad (11)$$

To ensure that N. can be normal in the time, t^, allotted for rescheduling by the dispatcher, we need to ensure that R^ is reachable from U_Q, the operating point of the Incumbent configuration, that is:

$$W_k(U_o, t_k) > 0 \quad (12)$$

When (12) is met P_k - 1. A pictorial view of satisfying (12) is given in Fig. 3.

IV. SECURITY CONSTRAINED OPTIMUM POWER FLOWS

We are now In a position to express (6) In terms of schedulable variables and thus, to rewrite (0P1) in forms necessary for the development of solution algorithms. We will describe two ways of rewriting (0P1). In both cases, our approach will not be to determine the actual value of S, but rather, to ensure only that S ≥ o. As a result we will not have to explicitly consider all the possiblle contingencies but only some subset of them. For instance, if $Q_{o<}$ a then we must find a subset of contingencies, K Q C K, such that by protecting against the occurrence of the contingencies in t^ we obtain the desired level of security. Thus, we seek a KQ so that

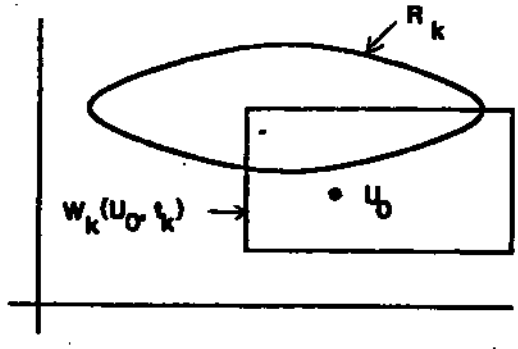

Fig. 3: 1^ can be made normal in time t_k if W_{fc}, the rescheduling window, and B^, the normal region for ±£, have a non-empty intersection.

$$\sum_{k \in K_a} Q_k P_k P'_k \geq \alpha - Q_o \quad (13)$$

We will call K,- a protected set. Before proceeding further, we reemphaslze that if ^ Is propertly selected (i.e. (13) is satisfied),then we need do nothing about the contingencies outside KQ. AS one might suspect, KQ is not unique and finding a solution of (13) is not trivial but can be done by techniques to be discussed in V.

In both the following reformulations of (0P1) we will make P^*_i - 1 by the technique described in III.2. The reformulations differ only in the manner in which they handle P_k.

IV. 1 Contingency Constrained Optimum Power Flows

This first and simpler formulation uses the contingency constrained scheme suggested by Stott, et.al. [15]. The assumption is that the safety margins M* guarantee the T-Stability of all configurations of interest, that is P^ - 1. With this assumption (0P1) can be rewritten in the form:

(COPF): $\min_{U_o} \phi(U_o, X_o, E_o)$

st: $U_o \in R_o(M^*)$ (14)

$R_k \cap W_k(U_o, t) > 0,\ k \in K_a$ (15)

$\sum_{k \in K_a} Q_k \geq \alpha - Q_o$ (16)

$V \geq 0$ (17)

(14), (15) ensure that N_k, $k \in K_a$ will be T-Stable and normal and the protected~set large enough to make security at least equal to a.

(COPF) Is a very large nonlinear programming problem. To emphasize this we note that (14) is equivalent to:

$$VW \quad \text{II } 0 \quad (18)$$

$$C_o(U_o, X_o, E_o) - \beta_o \geq M^* \quad (19)$$

and (15) is equivalent to:

$$\left.\begin{aligned} R_k(U_k, X_k, E_k) &= 0 \quad (20)\\ C_k(U_k, X_k, E_k) - \beta_k &\geq 0 \quad (21)\end{aligned}\right\} k \in K_a$$

(18) and (20) contain about twice as many nonlinear algebraic equations as there are nodes in the network.

IV.2 A Chance Constrained Optimum Power Flow

The safety margins, M*, used In the preceeding formulation are fairly restrictive. Can they be relaxed to provide more operating room and therefore, lower operating costs, while still maintaining the desired security level? If this cannot be achieved with the (COPF) formulation, can the safety margins be specially adjusted to make it achievable? The answer to both questions is "yes" provided that more information is available. Specifically, we need to know $f_k(M)$, the probability distribution of the safety margin M. In explanation, we note that M is an uncertain vector - all the uncertainties in our abilities to predict the dynamic responses of a power system make it impossible to precisely determine the least margins M^, that would make N. T-Stable. However, if we know f_k such that

$$\text{Probability } \{M \geq M_k\} - f_k(M)$$

Then we can use an approach called Chance Constrained Programming [12], [13] to Insert P_k and M into the overall problem formulation thereby, allowing their values to be chosen by the solution algorithm rather

than being prescribed, a priori, as in (COPF). Specifically, to ensure that the probability of J^ being T-Stable is at least P_k, we need to satisfy:

$$f_k\,(\,;_o(U_o,X_o,E_o \quad - So))I \quad P_k \qquad (22)$$

Now, we can rewrite (QP1) in the form:

(CHPF): Min $\langle U_{ow} X_o, E_o)$
U_o

$$'' \quad V^R o \qquad (23)$$

$$f_k\,(WVV \quad -^{\wedge} \quad F_k \qquad (24)$$

$$R_k \cap W_k(U_o, t_k) > 0 \qquad k\epsilon K_\alpha \qquad (25)$$

$$0 \leq P_k \leq 1 \qquad (26)$$

$$\sum_{k\epsilon K_a} 0.P. > a - 0 \qquad (27)$$

$$V \wedge 0 \qquad (28)$$

V. A DECOMPOSITION FOR ASYNCHRONOUS PARALLEL PROCESSING

In this section we will develop algorithms for solving the security constrained optimum power flow. Since both the Contingency Constrained and Chance Constrained formulations have the same structure, we do not have to develop separate algorithms for both of them. Instead, we will focus on only the (COPF) version.

There are between 2 and 6 times as many load and operating constraints as there are nodes in a network. If we want to deal with full size systems (of the order of 1000 nodes) and reasonable numbers of contingencies (of the order of 10) then (COPF) grows to include tens of thousands of constraints and decision variables — altogether too much for solution in any reasonable amount of time on existing uniprocessors, array machines and pipeline machines. The only viable approach appears to be the use of MIMD (Multiple Instruction Multiple Data) machines and asynchronous algorithms. An MIMD machine contains a number of independently programmable processors that can cooperate by exchanging information. An asynchronous algorithm keeps the information exchange mechanisms from degrading performance as rapidly as happens in a synchronous algorithm. This is because synchronous procedures include synchronization points. The first processor to reach one of these points must wait for the slower processors to catch up. This introduces delays and communication overheads that can quickly overwhelm the benefits of deploying several processors on the problem. In an asynchronous algorithm, however, each processor is allowed to proceed down its job stream at its own pace, regardless of the progress made by the other processors. For further details on asynchronous process see [10].

V.I An Overview

• We begin by selecting for further consideration a set K_a of contingencies. Eventually, we will choose K_a, a subset of KQ, and arrange to protect against the ill effects of the contingencies in this subset. The size and entries in Kg will depend on the desired level of security. The higher the level, the bigger; K_Q. Nothing will, nor need be, done about the contingencies outside K_a,

The selection of KQ and the positioning to protect against the occurrence of Its members will be done by breaking (COPF) into ^ + 1 separate subproblams, each of which will be assigned to a separate processor. One of these subproblems is associated with the incumbent configuration and will be called the "Master Problem". The others *are* associated with the contingencies and will be called Slave Problems.

The Master Problem will be formulated in two versions. The first is used to select KQ and achieve the desired security level, This version is of the mixed integer linear programming cype. The second version is used to minimize cost without degrading security. It is of the nonlinear programming type as are all the Slave Problems.

V.2 A Heuristic

The decision variables in (COPF) are U_o and U_k, k«l, ••.,K. Suppose we elect to solve (COPF) iteratlvely. Let Uj be the estimate of U_o after the i-th Iteration.

Most of the decision variables and complexity of (COPF) arise from having to satisfy (15). This constraint requires non empty intersections between W_k>the rescheduling windows, and R_k, the normal regions ot the associated minimally depleted configurations. We can decompose this constraint for parallel processing by selecting a single point, u£, to represent each region, R_k. How should this point be chosen? An intuitively appealing way is to place it inside R^ and as close to U_o^* as possible. Thus, u£ is found by solving:

(SPk): Min $||u_k^i - U_o^i||$
U_k^i

st: $U_k^* e \wedge$

(SPk) is referred to as the k-th Slave Problem.

Once u£ has been found for all k e^, we can proceed to reposition U_o to maximize security, if the desired level has not yet been reached, or to minimize cost, once it has been reached. The security maximization can be posed as a mixed integer programming problem of the form:

(MP1): Max $\sum_{k\epsilon K_\alpha} Q_k \beta_k$
U_o

$$\text{st:} \quad U_o + \bar{D}_k(U_o^i) - U_k^i \geq (1-\beta_k)\gamma \qquad (29)$$

$$U_k^i - U_o + \underline{D}_k(U_o^i) \geq (1-\beta_k)\gamma \qquad k\epsilon K_\alpha \qquad (30)$$

$$\beta_k - 0 \text{ or } 1 \qquad (31)$$

where *y* is a large negative number, say -100, and $\bar{D}_k$> $\underline{D}_k$ determine the rescheduling window, W_k (see (4) and (5)).

The net effect of (29) - (31) is to make 6_k-l when u_k^i e W_k(u£). Otherwise, þ^-0.

The solution to (MP1) is the new estimate, $Uj^{:+1}$, for the operating point of the incumbent configuration. If this estimate is outside ^(M*) we discard it and the associated values of u£. We continue solving (MP1) until the desired level of security, a, is reached. That is until

$$\sum_{k\epsilon K_\alpha} \beta_k Q_k \geq a - Q_o \qquad (32)$$

Then &.-1 «^ kEKg and we can turn our attention to minimizing cost while preserving security by solving the nonlinear programming problem

(MP2): Min $\cdot(U_o, X_{o\prime\prime}, E_\bullet)$
U_o

$$\text{st:} \quad U_o + \bar{D}_k(U_o^i) - u_k^i$$

$$u_k^i \sim \not{p}_O{}^+ S_k(U_o^i) = 0 \qquad kcK_\alpha$$

$$U_o \; C \; \underline{R}_o(M^*)$$

We will call (MP1) or MP2), which ever la being used, the Haater Problem.

V.3 An Asynchronous Procedure

A synchronous procedure for coordinating the Master and Slave Problems Is as follows:

Step 0: Guess u£. Set i - 0.

Step 1: Solve each of the Slave Problems to get U_k^i, $i \in K_\alpha$.

Step 2: Solve the Master Problem to get U_0^{i+1}

Step 3: Have the results converged sufficiently or Is there evidence that they are not going to converge? If so, stop; otherwise Increment 1 by 1 and return to Step 1.

As asynchronous extension of this procedure Is obtained by replaceIng "1" by "latest available" and allowing the processors assigned to the Master and Slave problems to proceed at their own rates.

V.4 Discussion

The decomposition and asynchronous procedure described In the prereedlng material are neither unique nor, as we shall see, without fallings. However, they have educational merit and considerable potential - we feel that modifications can be made to eliminate their fallings. The other decompositions we have ex* perlmented with have less potential. One of them is described in the companion paper [10] as an illustration of the way in which asynchronous procedures may be constructed. In a simulated multiprocessing environment it performed reasonably well with a 550 bus example and 2 contingencies. However, it cannot accomodate rescheduling.

The decomposition described In this paper is radical in the sense that it breaks the computations into intense, concurrent processes thst require only relatively sparse exchanges of information. Infact, the Master Process needs only to broadcast the current estimate of the vector U_0 to the Slave Processes. They in turn, need only to pass the current estimates of their solution vectors, U_k, back to the Master Processes. These relatively modest interprocess communications can readily be handled by existing technology. For Instance an architecture that could be used would contain Kg* 1 minicomputers like VAXs (one for the Master Process and one for each Important contingency) interconnected by a data highway like the Brown Boveri Partnerbus. However, before undertaking the assembly of hardware there are some Improvements that need to be made to the decomposition. These will be identified and explained below.

The second part of the Master Process, (MP2) and all the Slave Processes, (SPk), are of the standard OPF form. There are good reasons to believe that they can be effectively processed asynchronously. Among the reasons are that effective techniques, e.g. [11], are now available for solving OPF problems like (MP2) and (SPk). Also, it is difficult to envision the circumstances under which the asynchronous combination of (MP2) and(SPk) would fall to converge. Therefore, it seems reasonable to conclude that the procedures described earlier will be effective In minimizing cost while preventing degradations in an already established security level.

This leaves the issues addressed In the first part of the Master Process, (MP1), namely: the Improvement of security until a desired level, a, is achieved. The basic problem in making the Improvements is to find a subset of contingencies, Ka. against which to protect the system. Kg must be chosen to meet two criteria. First, it must include likely contingencies In numbers sufficient to meet the security level. Second, there must be at least one operating position for the Incumbent configuration from which the normal regions of the contingencies in $t^$ must be reachable without going outside the associated rescheduling windows.

(MP1) can be solved by commerlcally available mixed Integer linear programming packages such as [18]. Also it can be shown and our experience confirms that the asynchronous processing of (MP1) with (SPk) Is convergent. The difficulty is that (MP1) can have many local maxima with significantly different values. Therefore, (MP1) can home In on a local maximum that does not provide sufficient security while there are other maxima that do. Ways to remedy this falling is a matter of continuing research. One possibility is to run (MP1) concurrently on several processors with different starting points.But this could require an excessive number of processors.

VI. CONCLUSIONS

This paper has:

- defined a new security metric
- described two ways of Incorporating the security metric into OPF formulations.
- Outlined an asynchronous procedure that with further research and modification could yield a good way to solve the OPF formulations.

The security metric is continuous, includes contingency probabilities and can be made to reflect contingency Impacts. In these respects it represents a significant improvement over the existing binary metric.

The choice of OPFs to handle security issues stems from our belief that OPFs will continue to be the basic engines for automatic decision making over the horizons and variables important to security.

Of the two OPF formulations described, the first, called a Contingency Constrained Optimum Power Flow, requires no new information to assemble. The second, called a Chance Constrained Optimum Power Flow, allows more freedom of movement but needs Information not currently available. Specifically, it needs the probability distributions of the effectiveness of safety margins (stability margins) in maintaining the T-Stabillty of the configurations that would result from the occurrence of contingencies.

The computational procedures we have outlined are based on our belief that asynchronous multiprocessing is the only viable way to handle the enormous complexity of automatic-security-maintenance problems. The procedural outlines suggest promising directions to pursue but a great deal of work remains to be done in this area.

VII. ACPJOWLEDGEMEMT

The work reported here was supported in part by a grant from Brown Boveri Control Systems, Inc.

VIII. REJMJIENCES

[1] S.H. Talukdar, F.F. Vu, "Computer Aided Dispatch for Electric Power Systems", Invited paper, Proc. of the IEEE, Vol. 69, No. 10, Oct. 1981.

[2] S.H. Talukdar, ft. Mehrotra, V.K. Kalyan, N.Tyle," Optimum Power Formulations for Automatic Security Maintenance," Invited paper, Proceedings of the 1982 IEEE International Large Scale Systems Symposium.

[3] T.E. DyLiacco, "The adaptive reliability control system. "IEEE Trans. Power App. Syst. Vol. PAS-86, pp.517-531, May 1967.

[4] D.ft. Davidson, D.H. Bwart, L.K. Klrchmayer, "Long Term Dynamic Response of Power Systems: An Analysis of Major Disturbances" IEEE Trans, on PAS, Vol. PAS-94, May/June 1975.

[5] F.F. Wu, Sadatoshi Kurmagai, "Limits on Power Injections for Security-Constrained Power Flows", 1981 IEEE ISCAS, pp.755-58.
[6] R.J. Kay, and F.F. Wu, "Stability in the Prefaul State Space", 1981 ISCAS pp.936-942.
[7] F.D. Galina, M. Banakar, "Approximation Formulae for the dependent Load-Flow Variables," IEEE Trans. on PAS, March 1981, pp.1128-1137.
[8] F.D. Galiana, J. Jargis, "Security Regions in Power Networks", 1981, IEEE ISCAS, pp.750-754.
[9] G.L. Blankenship, L.H. Fink, "Statistical characterizations of Power System Stability & Security", Proc. Second Lawrence Symposium on Systems and Decision Sciences 1978, pp.62-70.
[10] S.N. Talukdar, S.S. Pyo," Asynchronous Algorithms for Parallel Processing," submitted to PICA-83.
[11] S.N. Talukdar, T.C. Giras, V.K. Kalyan, "Decompositions for Optimal Power Flows and other large Optimization Problems," submitted to IEEE Trans. on CAD.
[12] A. Charnes, W.W. Cooper, "Chance-Constrained Programming, "Management Science, Vol. 6,pp.73-80, 1959.
[13] I.M. Stancu-Minasian, M.J. Wets, "A Research Bibliography in Stochastic Programming, 1955-1975," Operations Research, Vol. 24, November/December 1976, pp. 1078-1119.
[14] "Expert Systems in the Microelectronic Age," edited by D. Michie, Univ. Edinburg Press, 1979.
[15] B. Stott, O.Alsac, J.L. Marinho," The Optimum Power Flow Problem," International Conference on Electric Power Problems, the Mathematical Challenge, Seattle, WA, 1980.
[16] S.N. Talukdar, N. Tyle, "Expert Systems for Power Problems", CMU Working Paper, 1982.
[17] S.N. Talukdar, T.C. Giras, V.K. Kalyan, "Decompositions for Optimal Power Flows" submitted to PICA-83.
[18] L. Schrage, "Introduction to LINDO," University of Chicago, Chicago, 1981.