IEEE Transactions on Power Systems, Vol. 10, No. 2, May 1995

CONCEPTUAL FRAMEWORK FOR EVALUATION AND INTERPRETATION OF THE RELIABILITY OF THE COMPOSITE POWER SYSTEM

B. PORRETTA E.G. NEUDORF
Toronto, Canada

ABSTRACT

This paper presents a conceptual framework for reliability evaluation which is based on the principles which underlie the procedures used in practice to achieve reliability of operation. Based on this framework, the paper discusses: the interpretation of the meaning of **Security** and **Adequacy**; the observability of **Security** and **Adequacy** interruptions; the different nature of interruptions due to **Security** and **Adequacy** and their impacts on the customer interruption costs; the interdependence of **Security**, **Adequacy** and operating costs; the nature of forced outages of generation and transmission elements and how they impact **Security** and **Adequacy**; and a practical procedure for the calculation of **Adequacy** and **Security**.

1.0 INTRODUCTION

For the purpose of reliability evaluation, the Composite Power System (COPS) is defined to consist of the generating units and of the transmission elements whose flows can be changed by generation rescheduling. The definition excludes the networks which supply load radially. The reason for this exclusion is that the modelling requirements for the COPS are different and more complex than the modelling requirements for radial networks. In summary, in the case of the COPS, modelling of generation failures, generation rescheduling, economic dispatch and operating reserves are essential as will be discussed later. However, these factors are not relevant to the reliability evaluation of radial networks for which the models must emphasize continuity and, therefore, transmission and switching equipment failures. From the point of view of developing practical computer programs, the significance of this is that modelling simplifications which are acceptable for the COPS are not acceptable for radial networks and vice versa.

A considerable amount of work has been done [5] and is being done on the development of computer programs for the evaluation of the reliability of the COPS. To date, several programs are available for this evaluation such as SYREL [12], RECS [10], GATOR [13], COMREL [14], CREAM [2], PROCOSE [8] and TRELSS [1].

However, utilization of these programs in practice is far from being widespread. This is due to three main interrelated aspects, namely:

a. Insufficient clarity and consensus as to the meaning of the quantities computed in terms of what can be done to achieve reliability of design and operation.

b. Insufficient credibility in the quantities computed likely due to insufficient validation of these quantities by comparison with experience.

c. The excessive amount of computer time needed for practical studies which require analysis for several months and several years.

This paper presents a conceptual framework based on the principles which underlie the procedures used to achieve reliability of operation. Based on this framework, the paper draws a number of conclusions regarding the meaning of **Adequacy** and **Security**, their interdependence and observability, the factors affecting them, and the modelling simplifications which are possible in their calculation. Based on the discussion provided, a practical procedure to compute **Adequacy and Security** is outlined.

In Section 2.0 the principles underlying the procedures used in practice to achieve reliable operation of the COPS are reviewed. These principles are then used as a basis for the conceptual framework developed in the subsequent Sections.

2.0 OPERATION OF THE COMPOSITE POWER SYSTEM

The essential objective of system operation is to provide a reliable supply of power at minimum cost. The reliable operation of the power system depends on the ability of the operators to deploy for on-line operation the generation/transmission resources as and when required to meet the load. Since these resources require a "start-up time" before they can be put on-line, their need for on-line operation must be predicted. This prediction is prone to errors due to:

a. Error in the forecast of the load that will have to be served at different times in the future.

b. Changes to the operability status of generation and transmission resources.

c. Error in the forecast of the weather since this can affect the load, the equipment capabilities, and may require adoption of different operating postures.

In practice, the on-line deployment for operation of the needed resources is based on an On-Line Operating Plan. Henceforth this will be referred to as the Plan. This Plan is continually updated so that it always covers about 24 hours into the future and reflects the changes in the forecasts of load, weather, and equipment availability. This Plan, in essence, consists of:

d. The load forecast for each of the future 24 hours.

e. The transmission and generation resources committed for operation for each hour.

f. A list of the equipment to be outaged for maintenance and the times at which the outages are to take place.

g. Remedial action plans for the times when difficulties are predicted. These remedial actions would consist of things such as cancellation of scheduled outages, recalling equipment from maintenance, arrangements for interconnection assistance, departures from economic dispatch and load cuts.

The reliability of the system operated consistent with the above Plan depends critically on how effectively the Plan

94 SM 498-6 PWRS A paper recommended and approved by the IEEE Power System Engineering Committee of the IEEE Power Engineering Society for presentation at the IEEE/PES 1994 Summer Meeting, San Francisco, CA, July 24-28, 1994. Manuscript submitted January 4, 1994; made available for printing June 10, 1994.

makes allowances for errors in the forecasts. These errors result from two main processes, namely:

i. Sudden changes, such as equipment failures or quick load changes, which immediately impact system conditions. For these changes there is little or no time to develop remedial actions and to "start-up" off-line equipment.

ii. Long term changes which impact system operation at a time in the future sufficiently ahead to permit planned remedial actions and "start-up" of the additional equipment required to cope with the changes.

The errors in the forecasts due to (ii) above can be dealt with "after the fact" through the normal updating of the Plan and thus require no special allowances. The changes from (i) above, however, cannot be dealt with "after the fact" in a planned manner, as there is insufficient time available. There are several aspects of system operation which are aimed at guarding against sudden changes or contingencies. The resultant capability of the system to cope with these contingencies is referred to as *Security*. (The word *Security* is used here with the meaning it has in the everyday operation of composite power systems [17]). Later on, parallels will be drawn between this term and the term **Security** formally defined as one of the components of the reliability of the COPS.) It is impractical to guard against all sudden contingencies since this would result in unacceptable design and operation costs [9]. In practice, the system is designed and operated to be able to withstand a set of contingencies which, based on experience, ensure acceptable *Security* at acceptable costs. This set of contingencies will be referred to as the Design Contingency Set (DCS) [4]. The system is usually designed and operated so that it can withstand each of the DCS contingencies. In some cases, generation rejection and load rejection schemes are used to achieve this. There are four aspects to *Security*, namely:

1. The ability of the system to transit from a pre-disturbance to a post-disturbance state in a stable manner.
2. The ability of the system to be manoeuvred out of rating violations in the first few minutes following the disturbance.
3. The ability of the system to be brought back within a predefined time into a posture such that any next DCS contingency can be withstood.
4. The ability of the system to restore quickly (i.e. within a time which is much shorter than the start-up time of off-line equipment) supply to load that has been interrupted to maintain the system secure.

The fundamental device for enabling the system to cope with sudden contingencies is to include in the Plan amounts of generation/transmission resources in excess of those strictly needed to meet the forecasted load. In general, in practice the excess resources related to generation are referred to as "Operating Reserves" and the excess resources related to transmission are referred to as "*Security* Limits". In this paper the term "Operating Reserves" is used to cover both generation and transmission excess resources.

The *Security* aspect in (1) above is dealt with by a combination of special automatic control schemes and preventive on-line deployment at all times of Operating Reserves of sufficient amount, response, and distribution. These on-line reserves will be referred to as "Spinning Reserves". These take the form of unloaded MW generation under AGC and governor control, unloaded MX generation, unloaded capacity on transmission lines, and spare tap positions on on-load tap changing transformers.

The *Security* aspect in (2) above is dealt with by the unused "Spinning Reserves" and with off-line reserves which can be brought on-line quickly (about five minutes). This additional off-line reserve will be referred to as "Ready Reserves".

The *Security* aspect in (3) above is dealt with by additional off-line reserves which can be brought on-line within a predefined time T which is about 10 to 30 minutes. These reserves will be referred to as "T-Reserves". These reserves can be supplemented by loads which by contractual agreement can be interrupted to preserve system reliability.

The *Security* aspect in (4) above is dealt with by relying first on the Operating Reserves and, as time progresses, by using the full off-line installed and not failed capacity including equipment which can be recalled from maintenance. The time required for this off-line equipment to be brought on-line (Tss), will vary depending on their off-line status and could extend to about 15 hours, and in some cases even longer, for cold thermal units.

The discussion below will be based on a Tss of 15 hours. It must be remembered, however, that this time can vary depending on the equipment involved. Such variation, however, does not change the applicability of the concepts presented.

Based on the above, the time over which *Security* is measured will vary from fault inception up to about 15 hours later. The reliability performance of the system during this time depends on:

A. The suitability of the choice of DCS contingencies and the correctness of the determination of the amount, response, and distribution of the various classes of Operating Reserves required to ensure that these contingencies can be withstood.

B. The suitability of the special controls installed to contain the DCS contingencies selected for containment.

It is important to notice that the system *Security* is evaluated on the basis of the DCS contingencies only. The contingencies outside of this set are not considered in a quantitative way for practical decision making.

In practice, the system operators ensure that the required Operating Reserves are maintained by operating the system to be within operating rules which will be referred to collectively as *Security* Limits. These limits identify the amount and location of spare generation/transmission capacity which must be maintained on-line and the amount and location of generation/transmission capacity which must remain deployable within various prespecified times. These *Security* Limits are expressed in terms of quantities such as MW capacity, MW flows, and voltages. As already noted, the term "*Security* Limits" in practice is used to refer to only transmission excess resources. In this paper the term is used to refer to all of the operating rules related to both the generation and transmission excess resources.

2.1 Characteristics Of The On-line Operating Plan

The driving operating objective in the formulation of the Plan is to ensure that the resources are operated in the most economic manner within reliability constraints.

The development of the Plan is supported by a predictive off-line process which starts months in advance. This process provides to the on-line environment a 24 hour predictive Plan every 24 hours. For each hour of the Plan the generation and transmission resources planned for operation minimize operating costs within the sole constraints of the total installed capacity not failed or not on scheduled maintenance, of the *Security* Limits and of equipment ratings. As soon as the plan enters the on-line operating environment, it starts being updated to take into account changes which invalidate the forecasts on which the Plan was based. As discussed above, these changes can be classified as sudden or long term changes.

The sudden changes will cause immediate changes in the actual operating conditions. Thus immediate control actions are, in general, required to bring the system back into a secure posture. Therefore, sudden changes require "improvisation" of modifications to the Plan. These modifications, in general, require immediate utilization of the Operating Reserves, short notice commitment of new Operating Reserves to replace the used ones, and short notice commitment of off-line generation/transmission resources that may take several hours to bring on-line. The successful implementation of these modifications to the Plan are time dependent because they depend on the status of the Operation Reserves and other system resources at the time of the disturbance (initial conditions) and on the speed with which control actions can be implemented. As an example, if a sudden change causes a line to overload to its 15 minute limited time rating, it is crucial that fast response spare generation be available for rescheduling within 15 minutes. For a given disturbance, the time into the future (Tss) at which the Plan ceases to be time dependent depends on the equipment, committed to cope with the disturbance, which has the longest "start-up" time. This time, as already noted, is about fifteen hours for cold thermal units. During Tss the reliability of the system operated consistent with the Plan depends on:

i. The amount, response, and distribution of the Operating Reserves.

ii. How long thermal overloads can be tolerated.

iii. How fast load can be shed.

iv. How fast required off-line equipment can be brought to operating status.

v. The initial condition status of the Operating Reserves and other system resources.

From the above, it can be concluded that the reliability impacts of a change event during the period Tss does not depend on the total installed capacity [7]. The reason for this is that the resources not committed as Operating Reserves will require at least Tss to be made available for operation. It is important to notice that within the time Tss, the emphasis is on preservation of load supply rather than most economic operation. Operation during this period is characterized by control actions aimed at avoiding or minimizing load cuts, steering the system back into a secure posture, and, ultimately, bringing it back into economic operation. Therefore, during Tss, as the operation is not optimized, the answers from simulation can have many values depending on the course of actions postulated. This greatly complicates modelling for reliability evaluation during this period.

For the long term changes there is sufficient time to permit operator response to be "fully planned". This means that the Plan modifications meet the operating objectives in an optimum manner. Therefore, any new equipment committed for operation can be readied so that it can be put on-line immediately when required. Based on the above discussion, for the impact of sudden changes over the period beyond Tss and for all other changes which are anticipated ahead of time by at least Tss, the operators will have a "fully planned" Plan to respond to these changes. Therefore at any one time, beyond some Tss the system operated consistent with the Plan is characterized by the following:

1. The reliability is not dependent on the initial conditions of the available resources at the time the changes were identified.
2. The reliability is not time dependent since the preparatory off-line work which was possible make the equipment called for by the Plan loadable when required without delay.
3. The reliability of the system is solely dependent on the total installed generation/transmission capacity not failed or which is not on unrecallable scheduled maintenance, and on the amount of resources which have to be set aside as Operating Reserves.
4. The system resources are deployed to meet operating objectives optimally, namely, optimal dispatch within the constraints of total available capacity, *Security* Limits, and equipment ratings.

Because of the continual changes discussed above, the Plan can be divided in two operating periods: a first period, starting from real time to Tss, over which implementation of the Plan is time dependent, that is, it depends on the initial conditions and how fast control actions can be implemented; the remaining period over which implementation of the Plan is not time dependent since off-line preparations are going on to ensure that equipment will be ready for on-line operation immediately as required.

3.0 INTERPRETATION OF THE DEFINITIONS OF SECURITY AND ADEQUACY

The reliability of the bulk power system can be divided into two components, namely, **Security** and **Adequacy**. Several definitions of these concepts are available in the literature [6,11]. CIGRE [6] defines them as follows:

<u>Adequacy</u> **A measure of the ability of a bulk power system to supply the aggregate electrical power and energy requirements of the customers within component ratings and voltage limits, taking into account scheduled and unscheduled outages of system components and the operating (Security) constraints imposed by operations.**

<u>Security</u> **A measure of the ability of the bulk power system to withstand specified sudden disturbances such as electric short circuits or unanticipated loss of system components.**

The use of these definitions as a basis for modelling for quantitative reliability evaluation, requires that they be interpreted in terms of actual system operation so that a concrete basis for modelling requirements can be established. Also, this type of interpretation would make the results of the analysis more useful for design or operating decisions.

3.1 Interpretation of **Adequacy** In Terms of System Operation

The interpretation of **Adequacy** is embodied in the established calculation methods such as LOLP [16], F&D [16], CREAM [2] and TRELSS [1]. These **Adequacy** calculation methods are characterized by the following:

a. State analysis is done without consideration of how and when the state was entered. That is, initial conditions and failure mechanisms are not considered.

b. All generation/transmission capacity not failed and not on maintenance is considered immediately available to meet the load and for remedial actions. No consideration is given to the time required to develop the remedial actions and bring the necessary equipment into operation and loading it to the required level.

c. The **Adequacy** of the system analyzed depends only on the capacity (continuous ratings) of installed generation/transmission which is not failed or which is not on unrecallable scheduled maintenance.

Comparison of items a, b, and c above with items 1, 2, and 3 in Section 2.1 indicates that the established **Adequacy** calculation methods simulate the power system under "fully planned" conditions, namely, consistent with the Plan beyond the time Tss. Therefore a fundamental characteristic of **Adequacy** is that it is a steady state (i.e. time independent) quantity. The only aspect that is not covered by the established **Adequacy** calculation techniques is item 4 in Section 2.1, namely, the requirement for economic dispatch within the constraints of installed capacity and *Security* Limits. Here, there are two separate aspects to be addressed, namely: requirement for economic dispatch; requirement to be within *Security* Limits. The latter requirement is covered explicitly in the CIGRE definition while the former is not. Let's address first the need to model *Security* Limits. As discussed above, these limits ensure maintenance on the system of the required Operating Reserves which are dictated by the DCS contingencies which the system must be able to withstand. Recognition of these limits would require a successful state to have:

1. Sufficient available capacity to meet the load plus spare capacity to meet the Operating Reserves requirements.
2. The spare capacity required to meet the Operating Reserve must meet the requirements of "response" (such as under governor control) and "distribution" (i.e. must be at the required locations). For example, a state with a load of 10,000 MW and only nuclear generation available for an amount of 15,000 MW is not a reliable state (i.e. it is a failure state) because the spare nuclear generation does not meet the "response" requirements of the generation Operating Reserves (unless the nuclear units are equipped with special controls for load following).

Another aspect related to the modelling of *Security* Limits is that it makes the **Adequacy** of a system dependent on how the system is operated to ensure acceptable *Security*. If the severity of the DCS contingencies is increased, the Operating Reserves requirements are higher and the *Security* of the system is higher. However, the **Adequacy** of the system is lower because the capacity of the Operating Reserves (both generation and transmission) must be subtracted from the capacity available in the state to obtain the amount useable to meet the load. In addition the cost of the operation is higher since the increased Operating Reserves (resulting in more limiting *Security* Limits) constrain the economic dispatch of the generation and also more resources must be maintained on-line. Thus, the **Adequacy** of a predefined system is not only dependent on its design, the installed capacity and the failure performance of the equipment, but is also dependent on how it is "planned for operation" in the steady state to meet *Security* requirements [9].

The above discussion implies that preventive measures are always taken to ensure compliance with the *Security* Limits. These preventive measures include things such as less economic dispatch, switching, arranging for interconnection assistance, and load cutting. *Security* Limits are enforced to ensure *Security* of the system "in case" any of the DCS contingencies were to occur. Thus, *Security* Limits represent the "premium" paid for insurance against "dreaded events". In practice, the fact that the *Security* Limit violations would result in actual load loss only if certain contingencies were to occur, permits the exercise of operator judgement as to when, and which, preventive measures should be implemented. In general, with the exception of load cutting, all other preventive measures are normally implemented. Whether preventive load cuttings is actually implemented, however, depends on the contingencies involved. In general, the DCS contingencies can be separated in two classes, namely:

Class I:
These are contingencies for which **there is not sufficient time** for after-the-fact remedial actions by manual or automatic means and which, without these remedial actions, would result in totally unacceptable events such as the blacking out of major population centres.

Class II:
These are contingencies for which **there is sufficient time** for after-the-fact remedial actions by available automatic controls or manual means.

In practice, the operator is given no choice but to cut load to stay within the limits intended to guard against Class I contingencies. However, violation for limits intended to guard against Class II contingencies are tolerated, based on operator judgement, and for these load cutting would, in general, occur only after the fact.

This discussion related to when load is actually cut in practice underscores the importance of differentiating between what is done to "plan" system operation to be consistent with predefined operating objectives, and what is actually done at "real-time" to keep steering the system to be consistent with the Plan in the face of unexpected events and to minimize load interruptions. The Plan is developed as if the DCS contingencies will occur for sure, while in real-time, the planned cuts are actually taken only for Class I contingencies while the cuts from Class II contingencies take place only if the contingencies would occur. According to this discussion, **Adequacy** calculations, which apply to planned operation, provide a measure of whether the system generation/transmission capacity is sufficient to meet the operating objectives but provide a prediction of load interruption which represent the upper bound of what would actually be interrupted at real-time. However, since the objective of system planning is to design a system which can withstand all of the DCS contingencies, the load interruption prediction provided by the **Adequacy** calculation is a relevant prediction for design decisions and operation planning.

Economic dispatch is a fundamental consideration in the operation of the system, but it is not mentioned in any of the definitions in the literature. If one interprets **Adequacy** in the narrow sense of predicting load interruptions, then economic dispatch may not be important if it can be established that the calculation techniques for determining the load cuts always converge to the same results regardless of the starting conditions in the base case load flow. Furthermore, load interruption indices are not sufficient to provide the design engineer a sufficiently informed basis to guide and justify design modifications. The modelling of economic dispatch, therefore, is considered important since besides removing doubts about the correctness of the computed load cuts, it will permit quantitative evaluation of other factors such as:

1. Trade-offs between reliability and operating costs. As already noted, reliability can be increased by accepting less economic operation.
2. Probability of bottling cheap generation. This is indicative of poor integration of the transmission, generation and load.
3. More meaningful comparison of alternatives. Different alternatives can have the same load interruptions but significantly different fuel costs.
4. A number of indices which depend on the correct prediction of the probability distribution of line power flows such as: transmission losses and their dollar value; probability of interface flows exceeding predefined limits. Without economic dispatch loss calculation and flow distributions are meaningless since these distributions are strongly influenced by economic dispatch.

Based on the above, **Adequacy** would be interpreted as follows:

Adequacy is a measure of the sufficiency of the capacity (rating) of the installed Generation/Transmission equipment to permit planning the economic operation of the power system to meet the power and energy requirements of the customers and the Operating Reserves requirements to achieve Security of operation.

3.2 Interpretation of **Security** in Terms of Actual System Operation

There are only a few papers in the literature that address the calculation of **Security** [4,9,15]. None of the methods presented has received general acceptance. Therefore, the interpretation of the definition of **Security** will be done largely on the basis of the discussion provided in this paper.

From the discussion in Section 2.0, it is evident that **Security**, as defined above, quantifies the capability of the system to withstand the DCS contingencies. That is, **Security** quantifies *Security*. Drawing from the discussion in Section 2.0, it can be stated that **Security**:

1. Quantifies the sufficiency of the Operating Reserves (which are derived from the DCS contingencies) to give the system the capability (for the DCS contingencies) to: transit from a pre-contingency to a post-contingency state in a stable manner; be manoeuvred out of violation conditions within limited-time ratings; be brought back within a predefined time (about 30 minutes) into a posture capable to withstand any next DCS contingency; restore supply quickly to load interrupted as a result of the DCS contingency.
2. Evaluates the reliability of the system operated consistent with Plan over the time Tss. This is the time during which the Operating Reserves constrain remedial actions.
3. Is a transient quantity. Therefore it depends on the initial conditions, how fast actions can be taken, how fast system conditions change, and how fast violations can be tolerated.
4. Depends on the Operating Reserves, namely, on the reserve generation/transmission resources which are on line or which can be put on line on short notice. The reserve resources which are available only after a long time do not affect **Security** and, therefore, **Security** does not depend on the total installed resources.
5. Is ensured by keeping the systems within *Security* Limits at all times.
6. Can be improved at the expense of poorer **Adequacy** and increased operating costs.

An important aspect of **Security** is that it is determined on the basis of predefined contingencies, namely, the DCS contingencies. Thus, comparisons and evaluation of alternatives are done on the basis of the DCS contingencies. Other contingencies, in practice, are not relevant because they do not impact design decisions in a quantitative way.

Based on the above, **Security** can be interpreted as follows:

Security is a measure of the sufficiency of the Operating Reserves to enable the power system to: be operated within modes that remain stable for prespecified sudden disturbances; provide the operator with sufficient manoeuvrability to remedy out of limit conditions in the immediate disturbance aftermath; provide the operator with sufficient reserves to reposture the system to be able to again cope with a next DCS contingency; provide the operator with sufficient resources to minimize the reliability impact of prespecified sudden disturbances.

4.0 THE NATURE OF FORCED OUTAGES AND THEIR IMPACTS ON ADEQUACY AND SECURITY

From the point of view of reliability impacts, forced equipment outages are of two types, namely:

1. Automatically initiated outages. These are outages which are initiated by relay action and occur suddenly without warning.
2. Manually initiated outages. These are outages which are initiated by operator action to avoid damage to equipment due to failure mechanisms that evolve slowly. Depending on the problem, manual outages are initiated from minutes to several days from the time the impending failure is identified.

The automatically initiated outages have the following reliability impacts:

a. Since they are sudden, the capability of the system to withstand them transiently depends on the preposturing of the system and thus depends on the amount, response, and distribution of the "Spinning Reserves".

b. Load loss occurs for only those DCS contingencies contained through load rejection schemes or for which the operator will cut load after-the-fact.

c. The ability of the system to recover from these contingencies over the time Tss depends on the Operating Reserves and on the initial conditions of the other system resources.

Therefore, automatically initiated outages impact **Security**. If their duration is longer than Tss, they impact the planned operation of the system, and therefore, they also impact **Adequacy**.

The manually initiated outages have the following reliability impacts:

i. Being manually initiated, these outages are expected and, in general, will not result in sudden load loss.

ii. If an outage has to be initiated within Tss, it will impact economic operation over the period from outage initiation to expiry of Tss.

iii. If the outage is long enough, it will impact planned operation.

Therefore, manually initiated outages impact economic operation and impact **Adequacy** if long enough.

Statistical analysis of failure data on generating units and transmission lines using Ontario Hydro failure data from 1980 to 1991 shows consistently the following pattern, which is considered to be typical of this equipment.

For generation:

1. About 90% of forced outages are manually initiated.
2. About 95% of forced outages last more than seven hours, and 93% last more than fifteen hours.

For transmission:

3. About 95% of forced outages are automatically initiated.
4. About 95% of forced outages last less than seven hours, 90% last less than a half hour, and 99% last less than fifteen hours.

From the above and within the context of the foregoing discussion, it is concluded that:

I. **Adequacy** is impacted in a primary way by generation failures, and it is not impacted significantly by transmission failures. Thus, for **Adequacy** calculations, transmission failures can be neglected.

II. **Security** is impacted in a primary way by transmission failures, and it is not impacted significantly by generation failures. Thus, for **Security** calculations, generation failures can be neglected.

From this it is concluded that it is very important that reliability evaluation of the COPS address both **Security** and **Adequacy**. Note that these conclusions are valid only for the COPS which was defined to exclude radial networks.

5.0 NATURE OF SECURITY AND ADEQUACY INTERRUPTIONS

Security interruptions are due to sudden unexpected events and have no warning. Thus the amount, frequency, duration, and location of the load interrupted is totally unpredictable. Therefore, the model to quantify **Security** must be capable of computing all of the above parameters. Also, as there is no warning, the customer costs for **Security** interruptions are higher.

Adequacy addresses planned operation. Therefore, **Adequacy** interruptions have warning and can be planned in terms of who, when and how often. Thus, a model to quantify **Adequacy** requires to be able to compute only the magnitude and location of the total interruption. Once this is known, the size, frequency, and duration of the interruptions to the individual customers are determined by the load cutting plan. Because of the warning, the **Adequacy** interruption costs are smaller.

6.0 A PRACTICAL PROCEDURE FOR ADEQUACY AND SECURITY EVALUATION

It is evident from above discussions that **Adequacy** and **Security** models based on explicit contingency simulations are very complicated and computational requirements are very large. However, it is possible to obtain practical estimates of **Security** and **Adequacy** by taking advantage of the concepts presented above.

As already discussed, it is evident that if at any one time T_0 the operator is planning the operation of the system at a point in time at which all installed (and not yet failed) equipment can be considered for operation, the equipment that he must consider out of service are those which are failed at To and which have a remaining repair time longer than Tss. If all transmission failures last less than Tss, which as discussed above is a good approximation, than at no one time there will be a failed line which will still be out of service Tss later. However, since most of the generation failures last longer than Tss, at any one point in time the state of the system Tss later is characterized by all transmission in-service and some of the generating units out-of-service. Thus, the probabilistic state space of the system representative of what could be present Tss later from any real time, can be enumerated on the basis of the failure of generating units only. This state space addresses the system in the "Steady State" and, as discussed before, it forms the basis for **Adequacy** calculations, and through the use of *Security* Limits, it can also be used to calculate **Security** as described in the following procedure.

1. Separate the DCS contingencies into a Class I set (C_1) and a Class II set (C_2). The definitions for these classes was provided in Section 3.1 above.
2. Develop two sets of *Security* Limits: one set (SL_{12}) to guard against both the C_1 and C_2 contingency sets; and one set (SL_1) to guard against the C_1 contingency set only.
3. Assume that the transmission elements have infinite ratings, and generate a state space of load flows such that in each state the available generation is dispatched optimally. The generation deficiency, if any, is balanced by load cuts allocated to load buses consistent with a predefined load curtailment plan. In this step, as the transmission is never limiting, the total load cuts are exactly the same as the generation deficiency (no generation bottling) and the load curtailment plan is adhered to without exception. Let this load cut be LG.
4. Re-analyze each of the states in 3. above imposing the continuous thermal ratings of the transmission elements. In some of the states it would be found that transmission is limiting and, in these cases, any or all of the following could occur: the generation is redispatched to eliminate or minimize the violations resulting in a less economic dispatch; some generation may be found bottled; some load may be cut at some buses to eliminate the violations; the allocation of load cuts due to generation (calculated in 3.0 above) may have to be modified to minimize additional load cuts and thus the load curtailment plan would not be followed. In this step, the following measures attributable to transmission thermal limits would be computed: generation bottling; fuel cost penalties; restrictions on the implementation of load curtailment policies; additional load cuts. Focusing on the calculation of load cuts, denote these additional cuts due to transmission ratings as LT_0.
5. Re-analyze each of the states in 3.0 above recognizing the thermal ratings of the transmission elements and the SL_1 set of *Security* Limits defined in 2. above. This will result in a worse performance for each of the measures identified in 4. above. Again, focusing on load cuts, denote the additional cuts, as compared to 4. above, as LT_1.
6. Re-analyze each of the states in 3.0 above imposing the SL_{12} limits in additional to all the limits already imposed in 5. above. The change in performance from 5. above is attributable to the C_2 contingencies. Denote the additional load cuts, as compared to 5. above, as LT_2.

Based on the above analysis, the prediction of the expected load actually interrupted (ELAI) would be given by

$$ELAI = P \times LG + P_0 \times LT_0 + P_1 \times LT_1 + P_2 \times LT_2 \quad (1)$$

Where: $LG + LT_0 + LT_1$ = **Adequacy**
$P_2 \times LT_2$ = **Security**

P, P_0, P_1 = Probabilities of not being able to find alternative sources of power supply to remedy generation shortages, or to enable rescheduling to eliminate thermal limits violations, or to enable rescheduling to eliminate violation of the SL_1 limits respectively.

P_2 = Probability of occurrence of any of the contingencies in the C_2 set.

Reference [4] is an example where the concepts underlying the above procedure were used.

From the above, it is evident that the development of *Security* Limits is very important. Clearly, these limits are an input to the reliability evaluation problem as the essence of reliability analysis is the separation of states into success and failure states, and the *Security* Limits, as well as equipment rating limits, form the fundamental criteria for such separation. In practice, the need for *Security* Limits is being dealt with daily in the operation of all major utilities. Several research efforts aimed at advancing the state of the art in this important area are currently underway.

7.0 OBSERVABILITY OF ADEQUACY AND SECURITY

The usefulness of simulation for engineering design depends on how well the simulated system predicts the behaviour of the real system. The power system simulation techniques for reliability calculations have so far not yet been successfully compared to experience. Credibility of these calculations requires that this comparison be done successfully. Before comparison of the computed reliability with the observed reliability can be done, it is necessary to interpret what is being computed in terms of the real system.

As discussed above, **Adequacy** relates to planned operation. Therefore, it cannot be measured by real time observation of load interruptions. **Adequacy** can be measured by looking at a point on the Plan Tss or longer in the future from real time. Note that if P, P_o, and P_1 in Equation (1) are reduced to zero, no **Adequacy** interruptions actually occur. Since **Adequacy** interruptions are predicted by the Plan, this provides time to the operators to develop remedial actions which tend to reduce P, P_o, and P_1 to zero. Therefore, load interruptions due to **Adequacy** are rarely observed completely at real time.

Security relates to sudden real time disturbances. Therefore, it can be measured by real time observation. Since, as just discussed, some of the **Adequacy** interruptions can also be observed at real time, it is important to separate those out to get the **Security** interruptions.

Based on the discussion in Section 4.0, **Security** is impacted mostly by transmission failures while **Adequacy** is impacted mostly by generation failures. Accordingly, statistics of load interruptions experienced should show that the observed interruptions are due mostly to transmission. Analysis of actual statistics will show that this is in fact the case.

8.0 CONCLUSIONS

This paper has presented a conceptual framework and a way of thinking which leads in a logical way to the modelling requirements and the possible simplification for **Security** and **Adequacy** calculations. Also, the paper develops a practical interpretation for **Security** and **Adequacy**, provides a discussion on their observability on the actual system, and outlines a procedure for practical calculations.

BIOGRAPHIES

Berardino Porretta received a B.A.Sc. in Electrical Engineering in 1966 and a M.Eng. in Computer Science in 1970 from the University of Toronto, Ontario, Canada. He joined Ontario Hydro in 1966. He worked with Ontario Hydro for 28 years. In the period 1965-1975 he worked in the Power Systems Operation Division where he headed a group responsible for the development of computer programs for operation planning (such as power flow, transient stability, economic generation dispatch, and security limits determination) and for on-line use (such as state estimation, security monitoring, contingency simulation, breaker position analysis, and predictive security assessment). In the period 1976-1993 he worked in the Power Systems Plannings Division where he headed a group responsible for development and maintenance of computer programs for solution of planning problems (such as composite reliability analysis (PROCOSE), sparse network reduction for power flow and stability calculations, power flow analysis, voltage stability analysis, and production costing). Currently he heads his own company offering a number of services including application programs for power systems analyses. He is a Professional Engineer in the Province of Ontario and a member of IEEE.

Ernie G. Neudorf graduated in Electrical Engineering from the University of British Columbia (B.A.Sc, 1961) and University of Toronto (M.Eng. 1970). He worked in Ontario Hydro's Power System Planning Division for 32 years. He is a Senior Member of the IEEE and a Registered Professional Engineer in the Province of Ontario.

REFERENCES

1. M.P. Bhavaraju, N.J. Balu, M.G. Lauby: "Transmission System Reliability Evaluation of Large Scale Systems" CIGRÉ Symposium, Montreal, 1991, Paper No. 1A-11.
2. M.V.F. Pereira, L.M.V.G. Pinto, "A New Computational Tool for Composite Reliability Evaluation" IEEE/PES 1991 Summer meeting, San Diego, California, July 28 - Aug 1, 1991.
3. "Adequacy and Security of Power Systems at the Planning Stage: Main Concepts and Issues". CIGRE, Symposium, Montreal, 1991, Working Group 37.08, Paper No. 1A-05.
4. B. Porretta, D.L. Kiguel, G.A. Hamoud, E.G. Neudorf, "A Comprehensive Approach for Adequacy and Security Evaluation of Bulk Power Systems" IEEE Transactions on Power Systems, Vol. 6, No. 2, May 1991.
5. M. Th. Schilling, R. Billinton, A.M. Leite Da Silva, M.A. El-Kady: "Bibliography on Composite System Reliability" IEEE Trans. on Power Systems, Vol. 4, No. 3, pp. 1122-1132, 1989.
6. "Power System Reliability Analysis. Application Guide" prepared by CIGRÉ Working Group 38-03, Edited by Leslie Kelley-Réguier, 1987.
7. B. Porretta, "Modelling Requirements for Bulk Power System Reliability Evaluation", Proceedings of the 1st International Symposium on Probabilistic Methods Applied to Electric Power Systems, Edited by S. Krishnasamy, Pergamon Press, Oxford, 1987, pp. 267-280.
8. B. Porretta, D.L. Kiguel, "Bulk Power System Reliability Evaluation, Part I: PROCOSE - A Computer Program for Probalistic Composite System Evaluation", Proceedings of the 14th International Reliability Availability Maintainability (Inter-RAM) Conference for the Electric Power Industry, Toronto, May 1987, pp. 440-447.
9. J.C. Dodu, A. Merlin, "New Probabilistic Approach Taking into Account Reliability and Operation Security in EHV Power System Planning at EDF", IEEE Transactions, PWRS-1, No. 3, August 1986, pp. 175-181.
10. A.P. Meliopoulos, A.G. Bakirtizis, R.R. Kovacs, R.J. Beck, "Bulk Power System Reliability Assessment Experience With the RECS Program", IEEE Transactions, PWRS-1, No. 3, August 1986, pp. 235-243.
11. "Reliability Concepts in Bulk Electric Systems" by Reliability Criteria Subcommittee, North American Electric Reliability Council, Feb. 1985.
12. EPRI Report RP1530-1, July 1982.
13. G.E. Marks, P.M. O'Neil, "GATOR - An Approach to Bulk Power and Sub-transmission Reliability Assessment", 8th Annual Reliability Engineering Conference for the Electric Power Industry, Portland, OR, 1981, pp. 223-230.
14. R. Billinton, T.K.P. Medicherla, "Overall Approach to the Reliability Evaluation of Composite Generation and Transmission Systems", IEEE Proceedings, Vol. 127, pt. c, March 1980.
15. A.M. Leite Da Silva, J. Endrenyi, L. Wang, "Integrated Treatment of Adequacy and Security in Bulk Power System Reliability Evaluations", IEEE Transactions on Power Systems, Vol. 8, No. 1, pp. 275-285, Feb. 1993
16. J. Endrenyi, "Reliability Modelling in Electric Power Systems" Book, John Wiley & Sons, 1978, Chapter 7.
17. W.K. Pence, "New Michigan Pool Center Stresses System Security", Electrical World, October 21, 1968.

DISCUSSION

D. L. Kiguel and G. A. Hamoud (Ontario Hydro, Toronto, Canada) The authors are to be commended for a timely and thought provoking paper. The paper addresses the problem of evaluating the reliability of the composite power system and proposes a practical method for computing its two components, system adequacy and system security. The paper concentrates on the practical aspects of the composite system but little is mentioned about the modelling requirements to obtain meaningful results.

We have the following comments and questions on the paper:

1. Most power systems are designed with some redundancy in the transmission network, so that loads can continue to be supplied after the occurrence of certain transmission contingencies. In the operation of such systems, guarding against those contingencies takes the form of observing operating limits on transmission lines and/or groups of lines (interfaces). These operating limits are, in general, dependent on the system conditions and can vary from one system state to another. In addition, limits based on stability and voltage considerations are observed at all times to prevent blackouts, while thermal limits may not. These factors can significantly affect the adequacy and the security of the power system. The procedure proposed in the paper did not address these issues. Would the authors elaborate on the problems involved in determining the operating limits and how to include state dependent limits in the reliability evaluation?
2. An important conclusion in the paper is that adequacy of the composite power system is impacted primarily by generation failures; therefore for adequacy calculations, transmission failures can be neglected. We believe that in the proposed approach the impact of some transmission failures is included in the calculation by observing transmission limits based on anticipation of certain contingencies, that is, by operating the system in a pre-postured mode. However, the pre-postured mode of operation will result in over estimating load cuts. If these limits are imposed, load cuts may be required even before a contingency actually occurs and the authors' method would compute a higher than necessary interruption. We believe that if a transmission contingency permits "after the fact" remedial actions, its contribution to the expected load cut should be weighed with the probability of the contingency. In practice, some transmission failures result in system conditions that can be tolerated for limited periods of time and load is cut only after implementing available remedial actions.
3. The various terms in the definition of the ELAI index given by equation (1) cannot be added directly to obtain the total load interrupted due to adequacy and security. Adding the terms, as suggested in the paper, will result in double counting of the probabilities of some system states. In addition, the LT_2 term in the equation should also represent an adequacy component and the probability P_2 changed to reflect the operating policy for the system. We believe that each term in the equation reflects the impact of a certain operating policy on system adequacy and there will be no security component if all the contingencies have been taken into account in the adequacy assessment.
4. The authors used Ontario Hydro's failure data of transmission lines to draw some conclusions regarding the impact of transmission failures on the reliability of the composite system. Can such conclusions be generalized without more detailed reliability studies of other systems? Was the proposed methodology compared with other available methods for composite system reliability evaluation?

The authors comments on the above points and remarks are appreciated.

Manuscript received August 10, 1994.

J. Endrenyi and L. Wang (Ontario Hydro, Toronto, Canada) The authors are to be congratulated on an article with a refreshingly independent view on bulk power system reliability concepts and approaches. In particular, they re-examine the meaning and usefulness of the adequacy and security measures and hint at how related indices could be calculated without undue effort.

In reading the paper, however, a number of points ask for clarification. The concept of security limits play a central role in the arguments; it is defined, in Section 2, in terms of "excess resources", and later in the same section, in terms of operating (loading) limits presumably derived from transient stability studies. For sure the two are related but are they necessarily the same? Besides, do these limits not depend on the action and speed of the protection system, of which there is no mention at all in the paper?

The main finding of the article appears to be the one in Section 4 where it is suggested that for adequacy calculations transmission failures, and for security calculations generating failures, ought to be neglected. This seems to be an overly sweeping recommendation: there is no guarantee that it can be applied to all systems. It may be more valid in the study of "strong" systems and less so when considering weaker ones.

It is noted in the paper that interruptions violating adequacy only are hardly ever observed. This is so only because generation planning (adaquacy-based, as it should be) was done with sufficient margin. Otherwise, these interruptions could be just as observable as are those related to security violations.

It is regrettable that the role and advantages of a fully probabilistic methodology are not mentioned. True, one can live by a hybrid deterministic (for security limits)/probabilistic (for adequacy) approach, but more insight and more information could be gained from a probabilistic model covering the entire area. Indeed, efforts are being made to develop such a technique. In Equation 1, a probabilistic index is suggested; however, the meaning of the index ELAI is unclear, and no hint is given on how the individual terms in the equation could be computed.

Manuscript received August 11, 1994.

B. Porretta and E.G. Neudorf. The authors thank the discussers for their valuable comments and questions allowing clarification of some points which, due to space limitation, could not be made in the paper.

Messrs D.L. Kiguel and A. Hamoud raise four points and these will be addressed below individually.

1. On state dependence of the Security Limits.

   As the discussers point out, Security Limits are state dependent. Therefore, for each state enumerated, one should verify that the Security Limits available apply and, if not, develop new ones. The current method for developing Security Limits is empirical and requires several power flow and stability calculations. With this method, it is not practical to check and or develop new limits for each state enumerated because it would require a very large amount of time. The fact remains, however, that the Security Limits are a fundamental part of the criteria required to decide whether a state is a success or a failure. Therefore, if these limits are not developed, composite reliability analysis cannot be done. Until faster and more automated techniques for development of Security Limits are developed, composite reliability analysis will have to rely on the assumption that few representative limits apply to a large number of states.

2. On system operation pre-postured to withstand contingencies by load cutting before these contingencies occur so as not to risk **Security** failures.

   The cutting of load before DCS contingencies whose occurrence would otherwise cause **Security** failures, is the **Adequacy** price paid to ensure **Security**, and this is why the two are interdependent. Better **Security** would require even more load cuts before contingencies occur and thus would result in worse **Adequacy** and vice versa. Therefore, the loads cut before DCS contingencies occur is not an "overestimating" of the cuts but rather the **Adequacy** "worsening" to ensure **Security** for the DCS contingencies.

3. On double counting in the ELAI expression.

   Let's summarize the meaning of the interruption terms in the ELAI expression.

   LG = interruptions due to generation failures only.

   LT_0 = additional (to LG) interruptions due to transmission thermal limits.

   LT_1 = additional (to LG + LT_0) interruptions due to the SL_1 limits, namely, the limits to withstand those contingencies for which there is no time to cut load after contingency occurrence.

   LT_2 = additional (to LG + LT_0 + LT_1) interruptions due to the SL_{12} limits which enable the system to withstand all DCS contingencies even those for which there is time to cut the load after contingency occurrence.

   The ELAI expression applies separately to each of the states enumerated. In each of the states some or all of the above load cuts can be non-zero. Since each of above load cuts are defined as "additional" there cannot be double counting. Also note that the probabilities in the ELAI expression are not related to the probability of the state for which the ELAI is being evaluated but rather related to the probability that the operator can diminish the failure severity of the state in the time between "planned operation" and "real time". Note also, that LT_2 is truly a **Security** interruption because the operator consciously accepted a failure of any C_2 contingencies. Of course such failure would be suffered only if any of the C_2 contingencies were to occur.

4. On the consequences of differences in the failure performance of components in the Ontario Hydro system with that of components in other systems.

   The authors agree with the discussers that the failure performance of components in other systems can be different. However, the concepts presented remain valid. And the essence of these concepts is:

   a. **Adequacy** is a steady state quantity and therefore must be evaluated at a point in time at which steady state conditions are guaranteed. This time is T_{ss} or longer ahead in the future of operating time. Therefore, if the duration of the failures of a component is shorter than T_{ss}, these failures should not be modelled in **Adequacy** calculations.

   b. **Security** is a transient quantity (i.e. initial conditions and time dependent). If some forced outages are manually initiated, and therefore planned, these outages should not be modelled in **Security** calculations since these outages will never results in **Security** failures.

This paper is really not proposing a different composite reliability evaluation method. The method always is in essence state enumeration followed by state analysis with respect to failure criteria. This paper has focussed on what failures should be considered for state enumeration (e.g. neglect transmission failures in enumerating state space for **Adequacy** calculations), and has focussed on the failure criteria to be used for state analysis. It also has focussed on how to measure experienced reliability (e.g. for **Adequacy**, measure planned operation) so that it has the same meaning as the reliability computed using current methods.

Messrs J. Endrenyi and L. Wang raise four points. Each of these is addressed below.

5. On the definition of Security Limits.

In a summary way, the paper has reviewed the following system planning and operating practices.

a. Design and operating requirements for **Security** are specified in terms of a predefined list of DCS contingencies which the system must be able to withstand.

b. The mechanism that allows design and operation so that the DCS contingencies can be withstood is the provisions of spare generation/transmissions resources.

c. In practice, to facilitate operation, the requirements for spare generation/transmission resources is translated in terms of Security Limits. These limits are developed manually based on numerous power flow and transient studies. The limits arrived at obviously do depend on the speed and type of controls and these are modelled in the transient stability studies. Obeyance of these limits ensures that the necessary spare resources are carried on the system at all times.

The main point that the paper is making is this context is that **Security** requires additional resource besides those strictly required to meet the load. Therefore, if a state has just enough generation/transmission resources to meet the load, then that state is a failure state (not **Adequate**) because it cannot meet the **Security** requirements.

6. On the modelling of transmission failures for **Adequacy** calculations.

This is addressed in 4. above.

7. On the real-time observability of **Adequacy** interruptions.

The authors do not agree with the discussers. The concept presented is not related to the planning margin used. The fact that **Adequacy** interruptions are not observed or are only partially observed at real-time is due to the fact that these interruptions are known to the operator at least T_{ss} before they would occur. Therefore, the operators have time to develop and implement remedial actions (such as public appeals) that diminish the necessary load cuts. This means that in the ELAI expression the probabilities P, P_0, and P_1 tend to zero.

8. On the use of a full probabilistic method.

There is nothing non-probabilistic suggested in the paper. The fact that Security Limits are based on deterministic criteria does not make the reliability analysis using these limits deterministic. As an example, the generation unit capacity used in the LOLP calculation are deterministic "capacity limits", but this does not make the LOLP calculations deterministic.

Manuscript received November 4, 1994.