TF 38.03.12

(15)

POWER SYSTEM SECURITY ASSESSMENT: A POSITION PAPER

Task Force 38.03.12

TABLE OF CONTENTS

Conveners : R.J. MARCEAU, J. ENDRENYI

Members: R. Allan, F. L. Alvarado, G. A. Bloemhof, T. Carlsen, G. Couto, E. N. Dialynas, N. Hatziargyriou, D. Holmberg, A. Invernizzi, J. Lumbreras, T. Manning, L. Messing, R. Naggar, Y.N. Rudenko (deceased), L. Salvaderi, J. R. Stewart, W. Wellssow, L. Wehenkel

KEYWORDS

Probabilistic security; deterministic security; utility risk evaluation

Abstract

Deterministic security assessment tends to provide a conservative security region for protecting the system against severe contingencies. In practice, this means that planners propose strong systems and operators operate with large security margins. Though investment and operational costs are relatively high, this has resulted in a high degree of reliability in most power systems. However, there is now pressure to operate power systems with lower security margins, partly due to economic imperatives but also due to practical difficulties such as obtaining authorizations from regulatory bodies to build power plants and transmission lines. In order to be able to operate the power system closer to the traditional (deterministic) security limits — and perhaps beyond — while offering comparable reliability, more refined methods for power system security assessment are needed which take into account the probabilistic nature of many variables in the decision-making environment. Probability methods permit the combined effect of such variables to be weighed under uncertainty, opening the door to quantified risk assessment in all of the facets of running a utility. The goal of the present report is to provide a framework for developing probabilistic utility security assessment methods and to outline the challenges which remain in order to attain this goal.

1. INTRODUCTION

1.1. BACKGROUND

During the early development of electric power systems, the functions of planning and operating a power system were often considered quite distinct. The questions planners and operators had to answer were different, and so were the tools employed to reach the answers. However, overlaps gradually developed in several areas. One example is the area of operations planning which inevitably intrudes into the system planner's domain, and another is the many aspects of evalu-

listes d'évaluation de la sécurité et de souligner les défis à relever afin d'atteindre cet objectif.

1. INTRODUCTION

1.1. LES ÉLÉMENTS DE BASE

Durant les premiers temps du développement des réseaux, les fonctions de planification et de conduite d'un réseau étaient souvent considérées comme étant tout à fait distinctes. Les questions auxquelles les planificateurs et les agents de conduite avaient à répondre étaient différentes et les outils employés pour avoir les réponses l'étaient également. Des recouvrements apparurent cependant graduellement dans plusieurs domaines. Un exemple est le domaine de la gestion prévisionnelle qui empiète sur le domaine du planificateur de réseaux et un autre exemple est constitué par les nombreux aspects de l'évaluation et de l'assurance de la fiabilité d'un réseau. En considérant ce dernier point, il n'est pas surprenant que les planificateurs et les agents de conduite travaillant dans des cultures différentes, aient développé pour les utiliser dans les évaluations de la sécurité, des concepts et des approches différents et qu'ils aient une manière différente de comprendre le rôle de la sécurité dans le domaine de la fiabilité.

Ce problème a été reconnu par la CIGRE parmi d'autres depuis pas mal de temps. Pour cette raison, le Groupe de Travail 38.03 a été créé à l'époque afin de passer en revue les différentes manières suivant lesquelles la fiabilité des réseaux était prise en considération et évaluée ainsi que les techniques d'évaluation employées. Cela s'est traduit par un document CIGRE « Power System Reliability Analysis Application Guide » [McGillis et al., 1987]. Le champ de ces considérations originelles était limité uniquement au domaine de l' « adéquation » de réseaux uniques (non interconnectés). Depuis lors, le plus récent Groupe Conseil 38.03 a estimé qu'il serait extrêmement avantageux d'étendre ce champ limité dans deux directions : une première afin de traiter des réseaux interconnectés du point de vue de l'adéquation (Groupe d'Action 38.03.11) et une seconde afin de ne considérer que les aspects liés à la sécurité de réseaux uniques (Groupe d'Action 38.03.12). La fonction première du présent rapport est, par conséquent, de passer en revue les résultats des recherches de ce dernier groupe d'action dont l'un des objectifs était de combler le fossé entre les manières de penser des planificateurs de réseaux et celles des agents de conduite.

1.2. LES PROBLÈMES

La plupart des auteurs attribuent à Dy Liacco l'établissement des bases théoriques relatives à la sécurité des réseaux dans une série de documents et de rapports publiés vers la fin des années soixante et soixante-dix [Dy Liacco 1967, 1968, 1974, 1978]. Il a défini, à l'origine, la sécurité sous la forme de la satisfaction d'un ensemble de contraintes d'inégalité sur un sous-ensemble de perturbations éventuelles dénommé « ensemble des aléas prochains ». Comme l'a fait remarquer [Tinguely 1992], depuis ce travail initial, plusieurs définitions ont été proposées, mais aucune d'entre elles n'a été trouvée entièrement satisfaisante. Par exemple, le North American Electric Reliability Council (NERC) qui fournit des directives relatives à la fiabilité et à la sécurité à toutes les entreprises d'électricité d'Amérique du Nord, définit la sécurité comme étant la « prévention d'indisponibilités en cascade lorsque l'alimentation par le réseau de grand transport est soumise à des perturbations sévères » [Balu et al. 1992], tandis qu'en Europe, un groupe de travail de la CIGRE a proposé récemment que « la sécurité d'un réseau est l'aptitude de celui-ci à faire face à des incidents sans que l'agent de conduite soit contraint de subir une perte non maîtrisée de la charge » [Haubrich & Nick 1993]. Une autre définition formule simplement que la sécurité des réseaux est « l'art et la science d'assurer la survie des réseaux » [Marceau 1993].

Cette dernière définition donne une signification générale à ce que les planificateurs et les agents de conduite peuvent entendre de manière intuitive lorsqu'ils utilisent le terme sécurité : de façon familière cela englobe tout ce qu'il faut faire pour la survie et l'exploitation saine d'un réseau. Mais lorsque l'on en vient à leurs tâches journalières, les planificateurs et les agents de conduite ont des objectifs très différents qui influencent nécessairement la manière dont ces concepts sont mis en œuvre en pratique. Les planificateurs déterminent les modifications qu'il faut apporter à un réseau afin de répondre à l'accroissement attendu de la charge et de tenir compte de variations dans la disponibilité des unités de production. Par contraste, les planificateurs de l'exploitation déterminent les limites de sécurité qui, à leur tour, permettront aux agents de conduite de surveiller et d'agir sur l'état de sécurité d'un réseau [Meyer et al. 1997].

La question du remplacement des méthodes déterministes traditionnelles par des technique probabilistes est de plus en plus d'actualité. Les limites de sécurité déterministes, par exemple, tendent à être tout à fait restrictives afin de se trouver du côté sûr. Il s'exerce toutefois de fortes pressions en vue d'exploiter les réseaux avec des marges de sécurité plus faibles, en partie du fait d'impératifs économiques (qui trouvent leurs racines dans une concurrence accrue et une tendance à la déréglementation, mais aussi du fait des difficultés pratiques pour obtenir des organismes réglementaires des autorisations de construire des centrales et des lignes de transport nouvelles (à cause des contraintes environnementales). Afin d'être capable d'exploiter un réseau plus près de ses limites de sécurité (déterministes) traditionnelles — et peut-être même au-delà — tout en offrant une fiabilité comparable, on a besoin, pour l'évaluation de la sécurité d'un réseau, de méthodes plus affinées qui prennent en compte, dans l'environnement de la prise de décision, la nature probabiliste de beaucoup d'aspects de l'environnement des compagnies d'électricité, y compris le facteur erreur humaine ainsi que les tendances à court et à long termes. Le contexte de l'exploitation a donc besoin, pour l'évaluation de la sécurité, d'outils d'analyse probabiliste qui sont comparables en complexité à ceux qui se trouvent présentement à la disposition du planificateur de réseaux dans le domaine de l'évaluation de la fiabilité.

TF 38.03.12

ating and ensuring system reliability. Considering the latter, it comes as no surprise that planners and operators, working in different cultures, have developed different concepts and approaches to use in reliability assessments, and have a different understanding of the role of security in the field of reliability.

This problem has been recognized by CIGRE amongst others for some considerable time. For this reason, the then Working Group 38.03 was created in order to review the various alternative ways that power system reliability was being considered and assessed, and evaluation techniques applied. This resulted in the CIGRE "Power System Reliability Analysis Application Guide" [McGillis et al. 1987]. However, the scope of those original considerations were limited only to the area of "adequacy" of single (non-interconneted) systems. Since then, the more recent Advisory Group 38.03 deemed that it would be extremely beneficial to extend this previously limited scope in two ways; one to deal with interconnected systems from an adequacy viewpoint (Task Force 38.03.11) and one to consider the security aspects albeit of single systems (Task Force 38.03.12). The primary function of this report is therefore to review the findings of the latter Task Force with one of its goals being to close the gap between the thought processes of system planners and of operators.

1.2. THE ISSUES

Most authors credit Dy Liacco for laying down the theoretical foundations of power system security in a series of reports and papers published in the late 1960s and 1970s [Dy Liacco 1967, 1968, 1974, 1978]. He originally defined security in terms of satisfying a set of inequality constraints over a subset of the possible disturbances called the "next contingency set". As pointed out by [Tinguely 1992], since this initial work, several definitions have been proposed, none of which has been found entirely satisfactory. For example, the North American Electric Reliability Council (NERC) which provides reliability and security guidelines to all the utilities in North America defines security as "prevention of cascading outages when the bulk power supply is subjected to severe disturbances" [Balu et al. 1992] whereas in Europe, a CIGRE working group has recently proposed that "power system security is the ability of the system to cope with incidents without the operator being compelled to suffer uncontrolled loss of load" [Haubrich & Nick 1993]. Yet another states simply that power system security is "the art and science of ensuring the survival of power systems" [Marceau 1993].

This last definition gives a general sense of what system planners and operators might intuitively understand when they use the term security: in a colloquial manner, it embraces all that it takes for the survival and healthy operation of a power system. But when it comes to their daily tasks, planners and operators have very different objectives which necessarily influences the way these concepts are implemented in practice. System planners determine the changes which must be brought to the system in order to meet expected load growth and account for variations in generation availability. In contrast, operations planners determine security limits which in turn permit operators to monitor and act upon the security status of the system [Meyer et al. 1997].

The question of replacing the traditional deterministic approaches by probabilistic techniques is increasingly timely. Deterministic security limits, for example, tend to be quite restrictive, to be on the safe side. However, there is pressure to operate power systems with lower security margins, in part due to economic imperatives (which find their roots in increased competition and a trend towards deregulation) but also due to the practical difficulties of obtaining authorizations from regulatory bodies to build new power plants and transmission lines (due to environmental constraints). In order to be able to operate the power system closer to — and perhaps beyond — traditional (deterministic) security limits while offering comparable reliability, more refined methods for power system security assessment are needed which take into account the statistical nature of many aspects of the utility environment, including the human error factor, and short- and long-term trends. The operations context is therefore in need of probabilistic analysis tools for security assessment which are comparable in complexity to those presently available to the system planner in the area of reliability assessment.

Probabilistic approaches have been slow in becoming part of the accepted methodology used for power system reliability studies. Several factors account for this, from the complexity of such methods to the credibility gap which always develops when models are sophisticated yet still contain, out of necessity, approximations. A further factor resulting in slow acceptance is the lack of probabilistic reliability standards in many areas. System planners have been using probability methods for generating reserve capacity evaluations for some time, but are reluctant to use the available probabilistic approaches for bulk power system evaluations, largely for the above reasons. Probabilistic methods for the evaluation of system security have received some attention by system operators [Billinton & Kuruganty 1980, Anderson & Bose 1983, Wu, Tsai & Yu 1988]; however, in present practice stability assessments are almost always performed by deterministic methods, even if they are combined with probabilistic planning tools. Finally, there is a lack of proper linkage between probabilistic adequacy and security methodology, although reports on efforts to provide an integrated framework for these studies have been published [Dodu & Merlin 1986, Leite da Silva, Endrenyi & Wang 1993].

1.3. THE GOALS OF THIS REPORT

In order to address these issues, the goal of the present report is therefore to attempt to answer the following questions:

- What is the technical meaning of the term security in the different contexts of power system applications?
- How does the concept of security relate to other concepts in the field of power system reliability, which are used concurrently or in a contrasting sense?
- What are the advantages and disadvantages of a probabilistic approach to computing security indices, and what guidelines can be offered for further development?

Les approches probabilistes ont mis longtemps à devenir partie intégrante de la méthodologie acceptée et utilisée pour les études de fiabilité des réseaux. Plusieurs facteurs expliquent cela, depuis la complexité de telles méthodes jusqu'au manque de crédibilité qui persiste toujours lorsque des modèles, aussi sophistiqués qu'ils soient aujourd'hui, contiennent encore, par nécessité, des approximations. Un autre facteur se traduisant par une lenteur dans leur acceptation, est le manque de normes réalistes de fiabilité dans beaucoup de domaines. Les planificateurs de réseaux ont utilisé depuis un certain temps des méthodes faisant appel aux probabilités pour des évaluations de capacités de production se trouvant en réserve, mais répugnent à employer les méthodes probabilistes disponibles pour des évaluations de réseaux de grand transport, en grande partie pour les raisons mentionnées ci-dessus. Des agents de conduite de réseaux ont accordé quelque attention à des méthodes probabilistes pour l'évaluation de la sécurité d'un réseau [Billinton & Kuruganty 1980, Anderson & Bose 1983, Wu, Tsai & Yu 1988] ; dans la pratique actuelle les évaluations de stabilité sont presque toujours effectuées à l'aide de méthodes déterministes, même si elles se trouvent combinées à des outils de planification probabilistes. Enfin, il manque un lien approprié entre l'adéquation probabiliste et la méthodologie de la sécurité, bien que des rapports relatifs à des efforts destinés à fournir un cadre intégré pour ces études aient été publiés [Dodu & Merlin 1986, Leite da Silva, Endrenyi & Wang 1993].

1.3. LES OBJECTIFS DU PRÉSENT RAPPORT

Afin de traiter ces problèmes, les objectifs du présent rapport sont de tenter de répondre aux questions suivantes :

- Quel est le sens technique du mot sécurité dans les différents contextes des applications réseaux ?
- Comment le concept de sécurité se trouve-t-il lié, dans le domaine de la fiabilité des réseaux, aux autres concepts qui sont utilisés concurremment ou dans un sens opposé ?
- Quels sont les avantages et les inconvénients d'une approche probabiliste pour le calcul d'indices de sécurité et quelles directives peut-on donner pour les développements futurs ?

Le chapitre suivant définit les concepts de base relatifs à la fiabilité des réseaux. Le chapitre 3 examine de façon plus précise l'adéquation et la sécurité et souligne leur relation avec les techniques existantes d'évaluation de la fiabilité utilisées dans la planification des réseaux. Le chapitre 4 offre une description conceptuelle de la manière dont les méthodes probabilistes peuvent être mises en œuvre dans les entreprises d'électricité pour l'évaluation de la sécurité et propose les domaines de recherche requis pour que de telles méthodes parviennent à maturité. Le chapitre 5 fournit des conclusions et des recommandations en vue d'études ultérieures.

2. CONCEPTS DE BASE

2.1. APPROCHE À LONG TERME DE LA FIABILITÉ DES RÉSEAUX

L'exploitation d'un réseau électrique est un processus complexe comportant de fréquents changements dans son état de fonctionnement. Chaque défaillance d'un composant, chaque réparation, chaque indisponibilité programmée ou non, chaque modification des conditions de charge introduira un nouvel état de fonctionnement. Il est usuel d'illustrer ce processus grâce au schéma de la figure 2.1 qui décrit l'historique du fonctionnement à l'aide d'un petit nombre d'états génériques du réseau. Chacun de ces états peut représenter une grande diversité de situations.

Pour autant qu'un commentaire soit nécessaire sur ce diagramme, le passage le plus fréquent à partir d'un état normal de fonctionnement se fait vers un état d'alerte qui est un état pleinement opérationnel du réseau mais quelques autres aléas peuvent créer un problème qui pourrait amener le réseau dans l'un des états d'urgence. Parfois pourrait survenir une situation d'urgence temporaire dans laquelle l'action de l'agent de conduite peut remédier à des contraintes sur des lignes ou à des tensions sur des jeux de barres inacceptables et ramener le réseau à un état d'alerte ou même à un état normal. Dans bien des cas cependant, une telle action corrective n'est possible que s'il y a délestage, transférant ainsi le réseau dans un état d'urgence contrôlée. A d'autres moments, les aléas survenant dans un état d'alerte pourrait amener, par force, le réseau dans une situation d'urgence extrême dans laquelle la stabilité et l'intégrité du réseau (c'est-à-dire le fait de continuer à fonctionner en réseau interconnecté) sont menacées.

Bien qu'un état d'urgence soit habituellement atteint à partir d'un état normal en passant par un état d'alerte, il peut être atteint directement si des aléas exceptionnellement sévères surviennent. Ces événements tels que des incidents multiples ou en cascade sont habituellement considérés comme des aléas extrêmes. Leurs effets sont souvent étudiés en vue de concevoir des mesures génériques qui peuvent fournir à un réseau une seconde ligne de défense l'aidant ainsi à éviter une panne complète.

Le diagramme de la figure 2.1 remonte à la fin des années soixante-dix [Fink & Carlsen 1978, EPRI 1981] alors que le problème principal des études de fiabilité des réseaux était l'évaluation des effets à long terme des défaillances des composants ; de ce fait les besoins des planificateurs de réseaux primaient. Ceci était satisfaisant pour les premières applications des méthodes d'évaluation de la fiabilité des réseaux. Au cours des dix dernières années, on s'est graduellement rendu compte qu'une évaluation complète de la fiabilité devait comprendre à la fois les effets à long terme (statiques) et les effets à court terme (dynamiques). En d'autres termes, il faut accorder une importance égale au fait de savoir à quel état le réseau aboutit après, disons, la perte d'un composant et comment il y arrive, si de toute façon il peut y arriver. Ceci a rendu nécessaire une refonte complète de la méthodologie de la fiabilité, une activité qui est toujours en cours.

2.2. EQUILIBRER LES BESOINS DE LA PLANIFICATION ET CEUX DE L'EXPLOITATION

Dans une bonne partie de la littérature technique récente, deux attributs décri-

The next chapter defines the basic concepts in power system reliability. Chapter 3 takes a closer look at adequacy and security, and outlines their relationship with existing reliability evaluation techniques used in system planning. Chapter 4 gives a conceptual description of how probabilistic methods can be implemented within utilities for power system security assessment and proposes those areas of research required for such methods to come to maturity. Chapter 5 provides conclusions and recommendations for further studies.

2. BASIC CONCEPTS

2.1. LONG-TERM APPROACH TO SYSTEM RELIABILITY

The operation of an electric power system is a complex process with frequent changes in the operating state of the system. Every component failure, repair, planned or unplanned outage, or change in the loading conditions will introduce a new operating state. It has been customary to illustrate this process by the scheme in Fig. 2.1 where operating history is described with the help of a few generic system states. Each of these states can represent a wide variety of conditions.

Commenting on the diagram as necessary, the most frequent transition out of a *normal* operating state is to an *alert* state which is a fully operational system state but some further contingencies can cause a system problem which would send the system to one of the *emergency* states. Occasionally, a *temporary emergency* condition would set in where operator action can relieve unacceptable line stress or bus voltages and often return the system to an alert or even a normal state. In many cases, however, such remedial action is possible only if load is shed, transferring the system to a *controlled emergency* state. At other times, contingencies in an alert state could force the system into an *extreme emergency* condition, where the stability and integrity (i.e the continuation of interconnected operation) of the system are threatened.

Although an emergency state is usually reached from a normal state via an alert state, it can be reached directly if exceptionally severe contingencies occur. These events, such as multiple or cascading incidents, are usually referred to as extreme contingencies. Their effects are often studied in order to design generic measures which may provide a second line of defence to the power system in helping to avoid complete system shutdown.

The diagram of Fig. 2.1 dates back to the late 1970s [Fink & Carlsen 1978, EPRI 1981] when the main concern in power system reliability studies was the evaluation of the long-term effects of component failures; hence the needs of system planners were of primary interest. This was satisfactory for the first applications of power system reliability methods. In the last 10 years, however, it has been gradually realised that a complete reliability assessment must include both the long-term (static) and the short-term (dynamic) effects. In other words, equal consideration must be given to *what* state the system ends up in after, say, the loss of a component, and *how* it gets there, if it can get there at all. This necessitated a complete rethinking of the reliability methodology, an activity still in progress.

2.2. BALANCING PLANNING AND OPERATING NEEDS

In much of the newer literature, power system reliability is described through two attributes, *adequacy* and *security*. In several IEEE and CIGRE documents, these are defined as follows [IEEE Working Group 1978, McGillis et al. 1987]:

Adequacy is the ability of the system to supply the aggregate electric power and energy requirements of the customers within component ratings and voltage limits, taking into account planned and unplanned component outages.

Security is the ability of the system to withstand specific sudden disturbances such as the unanticipated loss of system components.

While adequacy and security are not numerical quantities, each can be measured through appropriate indices (such as the frequencies and mean durations of violations and the associated amounts of energy not supplied). In addition to the concepts of *system* adequacy and security, a new section of the International Electrotechnical Vocabulary (IEV) provides definitions for a series of system operating *states* (Chapter 191, Part 3). It may be instructive to review these in light of the above system reliability attributes.

A classification of system operating states is shown in Fig. 2.2. A state is *adequate* if all loads are served, system components are not stressed beyond their ratings and the bus voltages and system frequency remain within tolerances. A state is *normal* if no credible contingency occurring in that state can lead to inadequacy or initiate cascading sequences. Such a state is both adequate and secure, and

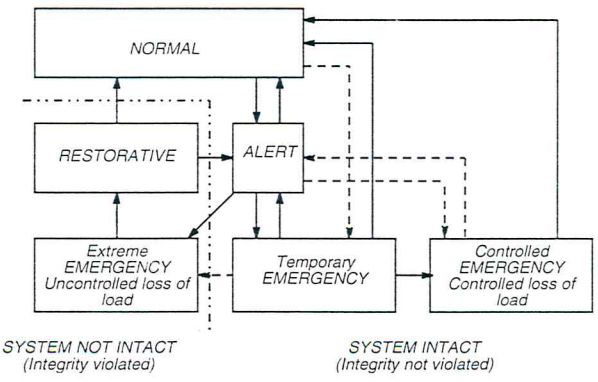

Figure 2.1. Processus mis en œuvre dans l'exploitation d'un réseau.

Figure 2.1. The process of power system operation.

vent la fiabilité des réseaux, l'adéquation et la sécurité. Dans plusieurs documents de l'IEEE et de la CIGRE, celles-ci sont définies comme suit [Groupe de Travail IEEE 1978, McGillis et al. 1987] :

• L'adéquation est l'aptitude d'un réseau à fournir la puissance électrique totale et les demandes en énergie des clients dans les limites des puissances nominales des composants et des tensions en tenant compte des indisponibilités programmées et non programmées de ces composants.

• La sécurité est l'aptitude d'un réseau à résister à des perturbations spécifiques subites telles que la perte imprévue de composants de ce réseau.

Alors que l'adéquation et la sécurité ne sont pas des grandeurs numériques, chacune d'elles peut être mesurée par des indices appropriés (tels que les fréquences et les durées moyennes des infractions et les quantités associées d'énergie non fournie). En plus de ces concepts d'adéquation et de sécurité d'un réseau, une nouvelle section du Vocabulaire Electrotechnique International (International Electrotechnical Vocabulary, IEV) donne des définitions pour une série d'états de fonctionnement d'un réseau (chapitre 191, partie 3). Il peut être instructif de les réexaminer en tenant compte des attributs de fiabilité ci-dessus.

La figure 2.2 montre une classification des états de fonctionnement d'un réseau. Un état est dit adéquat si toutes les charges sont desservies, que les composants du réseau ne subissent pas de contraintes allant au-delà de leurs puissances nominales et que les tensions des jeux de barres et la fréquence du réseau restent à l'intérieur des tolérances. Un état est normal si aucun aléa plausible survenant dans cet état ne peut conduire à l'inadéquation ou initialiser des séquences de défaillances en cascade. Un tel état est à la fois adéquat et sûr, et dans cet état, les conditions d'adéquation d'un réseau sont remplies. La plupart des réseaux se trouvent dans un état normal pour plus de 99 % du temps et la plupart des passages à partir d'un état normal se font vers un autre état normal.

La définition de l'aléa plausible peut être différente pour chaque entreprise

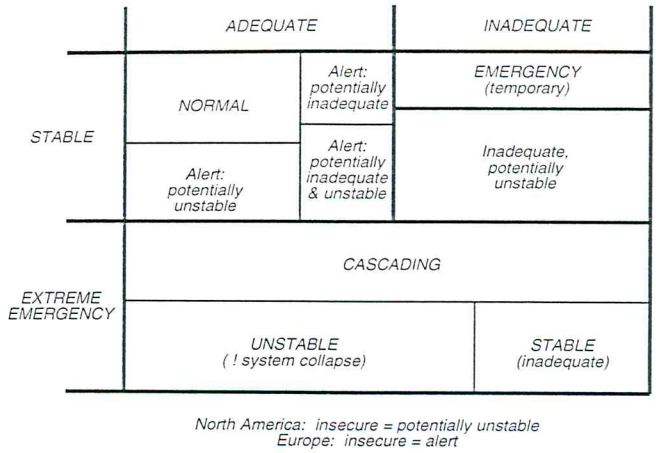

Figure 2.2. Classification des états de fonctionnement d'un réseau.

Figure 2.2. Classification of system operating states.

d'électricité. Selon la section 191-21 du Vocabulaire Electrotechnique International, c'est un événement « qui est reconnu comme suffisamment probable pour que le réseau électrique soit conçu et exploité pour y résister ».

Si après l'occurrence d'un aléa quelconque, la condition d'un état normal n'est plus satisfaite, le réseau entre dans un état d'alerte (dénommé non sûr suivant les usages européens). Dans un état d'alerte, au moins un autre aléa plausible peut se traduire par l'inadéquation ou initialiser des défaillances en cascade. Les états d'alerte peuvent être de deux types :

a) L'état peut être potentiellement inadéquat, c'est-à-dire qu'il peut survenir des aléas qui amènent le réseau dans des états inadéquats avec des surcharges de lignes et/ou des tensions de jeux de barres hors tolérances et/ou des pertes de consommation. Bien qu'encore stables, des états inadéquats sont considérés comme étant des états d'urgence, en ce sens qu'une action urgente de l'agent de conduite est nécessaire pour remédier aux symptômes d'inadéquation.

b) L'état peut être potentiellement instable, c'est-à-dire qu'il peut survenir des aléas qui déclenchent une séquence d'événements en cascade conduisant dans certains cas à l'instabilité. Cet état d'alerte est dénommé non sûr dans la littérature technique nord-américaine où ce terme est seulement employé pour ce type d'état d'alerte.

Un état d'alerte peut, bien entendu, être à la fois potentiellement inadéquat et potentiellement instable. Il faut cependant bien réaliser que cet état d'alerte lui-même est parfaitement adéquat et stable ; il est défini par des événements provoquant l'instabilité ou l'inadéquation qui peuvent survenir à la longue dans cet état mais ne sont pas encore survenus.

Alors que l'instabilité et les séquences de défaillance en cascade sont étroitement liées, toutes les séquences de cette sorte ne conduisent pas à l'ultime conséquence de l'instabilité : l'effondrement du réseau. En pratique, la stabilité peut être retrouvée après des défaillances en cascade, soit par un amortissement propre au processus, soit par l'action rapide des protections du réseau. Il est toutefois probable que l'état stable résultant ne sera pas adéquat.

Lorsque l'on utilise le terme adéquation, il faut bien prendre soin de s'assurer qu'il se rapporte ou bien au réseau ou bien à un état de fonctionnement. La définition de l'état adéquat a été donnée auparavant. L'adéquation du réseau est déterminée par des essais dits N-1 (ou similaires) dans lesquels on examine un ensemble d'aléas plausibles et, si les états après ces aléas sont toujours adéquats, le réseau est considéré comme étant adéquat. Ces états après aléas peu-

in this state, the conditions of system adequacy are fulfilled. Most power systems reside in a normal state for over 99% of the time, and most transitions out of a normal state are made to another normal state.

The definition of credible contingency can be different for each utility. According to section 191-21 of the International Electrotechnical Vocabulary (IEV), it is an event "which is recognized as sufficiently likely for the electric power system to be designed and operated to withstand it".

If after the occurrence of some contingency the condition of a normal state is no longer satisfied, the system enters an *alert* state (called *insecure* in European usage). In an alert state, at least one further credible contingency can result in inadequacy or initiate cascading. Alert states may be of two types:

a) The state may be *potentially inadequate*; that is, contingencies can occur in it which transfer the system into inadequate states with line overloads and/or bus voltages outside tolerances and/or losses of load. While still stable, inadequate states are considered *emergency states* in the sense that urgent operator action is needed to relieve the symptoms of inadequacy.

b) The state may be *potentially unstable*; that is, contingencies can occur which trigger a cascading sequence of events leading, in certain cases, to instability. This alert state is called *insecure* state in the North American literature where the term is applied only to this type of alert state.

An alert state may, of course, be both potentially inadequate and unstable. It must be realised, however, that the alert state itself is perfectly adequate and stable; it is defined through events causing instability or inadequacy that may eventually occur while in the state but have not yet occurred.

While instability and cascading sequences are closely related, not every such sequence leads to the ultimate consequence of instability: system collapse. In practice, stability may be regained after cascading, either through a damping inherent in the process, or through fast system protection action. It is likely, however, that the resulting stable state will not be adequate.

When using the term adequacy, care must be taken to make sure whether it refers to the system or to an operating state. Definition of the adequate state was given before. System adequacy is determined by so-called N-1 (or similar) tests where a selected set of credible contingencies is examined and, if the states after the contingencies are still adequate, the system is considered adequate. These post-contingency states may be normal or alert states.

In order to keep it simple, the diagram in Figure 2.2 is constructed to illustrate only the likely consequences of failures (movements to the right and downwards); consequences of operator actions are omitted. Thus, the controlled emergency condition (also called *partially adequate* state), which is mostly reached from the inadequate domain through operator intervention, is not shown.

2.3. DETERMINISTIC *VS* PROBABILISTIC APPROACHES

In the traditional deterministic culture, both adequacy and security are tested by a series of systematic experiments. In the case of adequacy, the so-called N-1 test is applied: key components are removed one-by-one and **the system must be so designed that no adequacy violations** (i.e. the load, voltages, var requirements, etc.) **occur in the resulting system configurations**. The line loadings and bus voltages are computed through load flow analysis, and their maximum permissible values are determined respectively by the lines' thermal limits and a utility's accepted operating criteria.

For security, stability studies are carried out for pre-selected contingencies and *stability limits* (based on transient, long-term or dynamic stability criteria) are established for the line loadings which are generally more constraining than the thermal limits. **Security limits are determined such that the system is stable, loses no load due to such contingencies and system quantities remain within emergency operating values regardless of system topology**.

The weakness of the deterministic approach lies primarily in the arbitrariness of selecting contingencies for the N-1 tests and of choosing the cases for stability studies (which hides the underlying probabilistic nature of many variables). The deterministic approach may also lead to omitting important cases and including unlikely ones, possibly resulting in overdesign without an indication that risks are reduced to acceptable levels. Probabilistic approaches reduce these weaknesses, but their usefulness is compromised in two areas where the methodology is not yet fully mature. One is the accuracy of the probabilistic models employed and the precision of the solution methods. These problems are also present in the deterministic approach, but due to the greater simplicity and transparency of this method the simplifications and approximations applied are often perceived to be justified. As a consequence, the deterministic approach can enjoy, often unfairly, higher credibility. The other area is the unavailability of (most) standards for what constitutes acceptable risks. Both areas are being further explored.

3. ADEQUACY AND SECURITY: A CLOSER LOOK

3.1. THE DISTINCTION BETWEEN ADEQUACY AND SECURITY

A considerable number of papers relating to power system reliability assessment have considered these two apparently distinct aspects of system reliability. The implication behind this subdivision is that the two are different in concept and in evaluation which can lead to misunderstanding of the reasoning behind this subdivision. There is no intention to indicate that two distinct processes are involved; instead, the intention is to ensure that reliability indices are calculated in a simply structured and logical fashion. Part of the reason for the subdivision is that adequacy, as defined, is far easier to calculate and therefore worthwhile to evaluate and apply, leaving the problem of "security" for further development and research.

GA 38 03 12

vent être des états normaux ou des états d'alerte.

Afin qu'il reste simple, le diagramme de la figure 2.2 est réalisé pour seulement illustrer les conséquences probables de défaillances (mouvements vers la droite et vers le bas) ; on a omis les conséquences des actions de l'agent de conduite. Ainsi la situation d'urgence contrôlée (encore appelée état partiellement adéquat) qui est le plus souvent atteinte à partir du domaine inadéquat par une intervention de l'agent de conduite, n'est pas représentée.

2.3. L'APPROCHE DÉTERMINISTE COMPARÉE À L'APPROCHE PROBABILISTE

Dans la culture déterministe traditionnelle, l'adéquation et la sécurité sont testées toutes deux à l'aide d'une série d'expérimentations méthodiques. Dans le cas de l'adéquation, on applique le critère dénommé N-1 : on enlève les composants clés un par un et **le réseau doit être conçu de telle façon qu'il ne survienne aucune violation de l'adéquation** (c'est-à-dire des exigences relatives à la charge, aux tensions, aux besoins en var, etc.) **dans les configurations résultantes du réseau.** On calcule les charges des lignes et les tensions aux jeux de barres à l'aide d'une analyse de la répartition des flux de puissance et les valeurs maximales admissibles correspondantes sont respectivement déterminées par les limites thermiques des lignes et par les critères de fonctionnement acceptés par la compagnie d'électricité.

Dans le cas de la sécurité, les études de stabilité sont effectuées pour des aléas présélectionnés et les limites de stabilité (fondées sur des critères de stabilité transitoire, à long terme ou dynamique) sont établies pour des charges des lignes qui sont généralement plus contraignantes que les limites thermiques.

Les limites de sécurité sont déterminées de telle manière que le réseau soit stable, ne perde aucune charge du fait de tels aléas et que les grandeurs de ce réseau restent à l'intérieur de valeurs de fonctionnement en urgence quelle que soit la topologie de ce réseau.

La faiblesse de l'approche déterministe réside principalement dans le caractère arbitraire de la sélection des aléas pour les tests N-1 et dans le choix des cas pour les études de stabilité (ce qui cache la nature probabiliste sous-jacente de beaucoup de variables). L'approche déterministe peut aussi conduire à omettre des cas importants et à inclure des cas improbables, ceci se traduisant éventuellement par un surdimensionnement sans indication que les risques soient réduits à des niveaux acceptables. Les approches probabilistes réduisent cette faiblesse, mais leur utilité est compromise dans deux domaines où la méthodologie n'est pas encore arrivée à pleine maturité. L'un de ces domaines est l'exactitude des modèles probabilistes employés et la précision des méthodes de résolution. Ces problèmes sont également présents dans l'approche déterministe, mais du fait de la plus grande simplicité et de la transparence de cette méthode, les simplifications et les approximations faites sont souvent perçues comme étant justifiées. En conséquence, la méthode déterministe peut jouir, souvent à tort, d'une crédibilité plus grande. L'autre domaine est le silence (de la plupart) des normes sur ce qui constitue des risques acceptables. Ces deux domaines continuent à être étudiés sous tous leurs aspects.

3. ADÉQUATION ET SÉCURITÉ : UN EXAMEN PLUS POUSSÉ

3.1. DISTINCTION À FAIRE ENTRE ADÉQUATION ET SÉCURITÉ

Un nombre considérable de rapports concernant l'évaluation de la fiabilité des réseaux ont pris en compte ces deux aspects apparemment distincts de la fiabilité d'un réseau. Ce qui est impliqué derrière cette subdivision, c'est que ces deux notions sont différentes au niveau du concept et de l'évaluation, ce qui peut conduire à mal comprendre le raisonnement impliqué. Loin de nous l'intention d'indiquer que deux processus soient impliqués ; au lieu de cela, notre intention est de nous assurer que les indices de fiabilité sont calculés d'une manière structurée simplement et logique. Une partie de la raison de cette subdivision est que l'adéquation, telle qu'elle est définie, est beaucoup plus facile à calculer et, par conséquent, intéressante à évaluer et à appliquer, laissant ainsi le problème de la « sécurité » faire l'objet de développements et de recherches supplémentaires.

Bien que la distinction entre adéquation et sécurité au sens de la fiabilité soit généralement bien comprise par ceux qui développent les techniques analytiques, cette distinction est devenue moins évidente pour ceux qui sont impliqués dans les applications pratiques de l'évaluation de la fiabilité aux réseaux réels.

3.2. ADÉQUATION

Pour décrire ces deux concepts d'adéquation et de sécurité, il est avant tout nécessaire d'expliquer comment la majorité des réseaux sont planifiés et exploités. Un réseau peut se trouver dans un très grand nombre d'états possibles. Chaque alternateur peut être disponible ou non ; les lignes de transport peuvent également être disponibles ou non et la demande peut être extrêmement variable ; les alternateurs et les lignes peuvent aussi être déclassés. On pourrait imaginer ces états sous la forme d'un espace multidimensionnel englobant production, demande et transferts de puissance, mais pour la commodité de la présentation, nous considérerons simplement deux dimensions. La figure 3.1 montre une représentation conceptuelle des régions de fonctionnement qu'un réseau comportant deux injections de puissance pourrait adopter. Les formes des limites représentées sur cette figure relèvent de pures hypothèses.

Le domaine entouré par la limite de faisabilité représente toutes les combinaisons de répartition de la production pour lesquelles il existe un état d'équilibre (c'est-à-dire une solution des équations de répartition des flux de puissance) indépendamment d'autres contraintes : c'est la région de faisabilité. D'autre part, le domaine entouré par la limite d'adéquation est appelé région d'adéquation. Bien que la définition formelle de l'adéquation d'un réseau la définisse clairement en fonction des conditions de ce réseau dans

Although the distinction between adequacy and security in a reliability sense is generally understood by those developing the analytical techniques, the distinction has become less obvious to those involved in the practical applications of reliability assessment to real systems.

3.2. ADEQUACY

To demonstrate the twin concepts of adequacy and security, it is necessary first of all to explain how most power systems are planned and operated. The power system can reside in a very large number of possible states. Each generator can be available or unavailable; transmission lines can also be available or unavailable and the demand can be highly variable; generators and power lines can also be downrated. These states could be imagined to be a multi-dimensional space including generation, demand, and power transfers, but for presentational purposes we will simply consider two dimensions. Fig. 3.1 shows a conceptual representation of the operating regions that a two-injection power system could adopt. The shape of the boundaries illustrated in this figure are purely hypothetical.

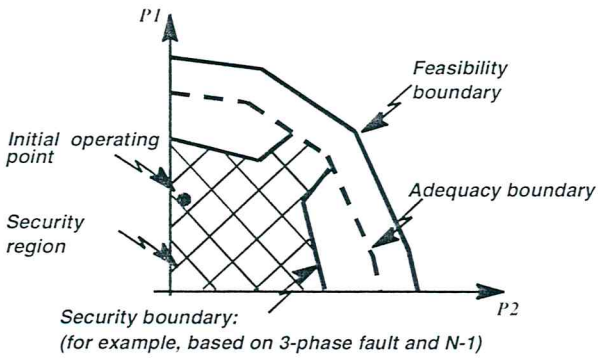

Figure 3.1. Régions de faisabilité, d'adéquation et de sécurité dans un réseau imaginaire comportant deux injections de puissance.

Figure 3.1. Hypothetical feasibility, adequacy and security regions in a two-injection power system.

The area circumscribed by the feasibility boundary represents all combinations of generation dispatching for which an equilibrium state (i.e. a load flow solution) exists, irrespective of other constraints: this is the feasibility region. On the other hand, that circumscribed by the adequacy boundary is called the adequacy region. Though the formal definition of system adequacy clearly defines it in terms of N-1 system conditions (i.e. "... taking into account planned and unplanned component outages"), most practicioners employ the IEV definition of state adequacy which simply requires that a given equilibrium state satisfy all system requirements including the load, voltages and var requirements, i.e. no power system constraint is violated. The adequacy concept is therefore seen by many to be a purely static one.

In adequacy analysis (irrespective of one's preferred definition of adequacy), the adequate and inadequate states are the only ones that are considered to determine system reliability: one focuses on the probability of being (or not being) in the adequate region. However, consideration of steady-state conditions alone leads to an oversimplified view of reliability. It may provide useful insights but is far from providing a complete picture: it does not identify any form of instability. It is clearly undesirable to operate a power system in an alert state for any considerable period of time, or in a state where the system's operation would be significantly disrupted if perturbed. Therefore, reliability analysis must be extended into the security area.

3.3. SECURITY

3.3.1. What is Security?

The proposed extension of reliability analysis to cover the possibility of instability has been called security analysis, an unfortunate term which has led to much misunderstanding because it is used in different senses by different people. Though the previous sections present definitions generally used in planning and operation, the term security is used in a number of different ways even in the electric power industry. In the area of power system protection, for example, engineers frequently refer to security as the ability of a protective device not to cause inadvertent trips. Power system reliability engineers, however, tend to relate security to the dynamic process that occurs when the system transits from one state to another.

Consider a power system which moves from one state to another as a result of, say, a fault on a transmission circuit resulting in the loss of a line. Both of these states may themselves be adequate if the system is able to satisfy all demands and constraints in the steady state. However, if the dynamic and transient behaviour of the system is also taken into account, it can turn out that the transfer may not be possible without violating stability criteria. In this case, the originating state would be deemed adequate but insecure (potentially unstable).

Further consideration of this example illustrates the difference between European and North American terminologies. Referring to Fig. 2.2, it may happen that the state from which the above transition occurs may be inadequate but secure if no transition out of it can lead to instability. This reflects North American usage of terms where insecure states are defined as the subset of the alert states from which credible contingencies can lead to instability. This definition allows for the existence of secure but inadequate states in which case the security region can reach beyond the adequacy boundary in Figure 3.1. The European usage prefers to call all alert states insecure, and by implication all inadequate states as well. In this case, the security region is fully inside the adequacy region, and Figure 3.1 is correct as shown. Part 3 of Chapter 191 of the IEV favours the former terminology, many operators prefer the latter.

l'état N-1 (c'est-à-dire en tenant compte des indisponibilités programmées et non programmées des composants), la majorité des praticiens emploient la définition du VEI de l'adéquation d'un état qui exige simplement qu'un état d'équilibre donné satisfasse à toutes les exigences du réseau y compris les exigences concernant la charge, les tension et les besoins en var, c'est-à-dire qu'aucune contrainte du réseau immédiat n'est enfreinte. Le concept d'adéquation est donc considéré par beaucoup comme étant un concept purement statique.

Dans l'analyse de l'adéquation (indépendamment de la définition préférée de chacun de l'adéquation), les états adéquats et inadéquats sont les seuls considérés pour déterminer la fiabilité du réseau : on se concentre sur la probabilité d'être ou de ne pas être dans la région adéquate. La prise en considération des seules conditions relatives à un régime permanent conduit à une vue trop simplifiée de la fiabilité. Cela peut fournir des aperçus utiles mais est loin de donner une image complète : on n'identifie aucune forme d'instabilité. Il n'est clairement pas souhaitable d'exploiter un réseau dans un état d'alerte pour un intervalle considérable quelconque de temps ou dans un état où l'exploitation de ce réseau serait interrompue de manière significative si elle se trouvait perturbée. C'est pourquoi l'analyse de la fiabilité doit être étendue au domaine de la sécurité.

3.3. SÉCURITÉ

3.3.1. Qu'est-ce que la sécurité ?

L'extension proposée de l'analyse de fiabilité afin de couvrir l'éventualité d'une instabilité a été appelée analyse de sécurité, un terme malheureux qui a conduit à bien des incompréhensions parce qu'il est utilisé avec des sens différents par des personnes différentes. Bien que les sections précédentes présentent les définitions généralement employées pour la planification et l'exploitation, le terme de sécurité est utilisé dans un bon nombre de sens différents, même dans le seul secteur électrique. Dans le domaine de la protection des réseaux par exemple, les ingénieurs parlent de la sécurité comme étant l'aptitude d'un dispositif protecteur à ne pas provoquer de déclenchements intempestifs. Les ingénieurs spécialistes de la fiabilité des réseaux tendent par contre à lier la sécurité au processus dynamique intervenant lorsque le réseau passe d'un état à un autre.

Considérons un réseau qui passe d'un état à un autre à la suite, disons, d'un défaut sur un circuit de transport se traduisant par la perte d'une ligne. Ces deux états peuvent chacun être adéquats si le réseau est apte à satisfaire toutes les demandes et toutes les contraintes en régime permanent. Cependant, si le comportement dynamique et transitoire de ce réseau est également pris en compte, il peut s'avérer que ce passage ne puisse être possible sans enfreindre les critères de stabilité. Dans ce cas, l'état d'origine sera réputé adéquat mais non sûr (potentiellement instable).

Une réflexion supplémentaire sur cet exemple illustre la différence existant entre les terminologies européenne et nord-américaine. En se référant à la figure 2.2, il peut arriver que l'état, à partir duquel s'effectue la transition, puisse être inadéquat mais sûr si aucune transition à partir de là ne peut conduire à l'instabilité. Ceci reflète l'usage nord-américain des termes où les états non sûrs sont définis comme étant le sous-ensemble des états d'alerte à partir desquels des aléas plausibles peuvent conduire à l'instabilité. Cette définition tient compte de l'existence d'états sûrs mais inadéquats et dans ce cas la région de sécurité peut s'étendre au-delà de la limite d'adéquation de la figure 3.1. L'usage européen préfère appeler non sûrs tous les états d'alerte et par implication, également tous les états inadéquats. Dans ce cas, la région de sécurité est entièrement située à l'intérieur de la région d'adéquation. et la figure 3.1 est correcte telle qu'elle est représentée. La partie 3 du chapitre 191 du VEI est en faveur de cette première terminologie alors que beaucoup d'agents de conduite préfèrent la seconde.

3.3.2. Identification des états sûrs

Afin de séparer les états sûrs et non sûrs, la pratique normale pour une entreprise d'électricité est de sélectionner une gamme d'aléas plausibles (fondée sur son propre historique d'exploitation et sa propre expérience) souvent désignés comme étant des aléas normaux. Ceux-ci ont été définis en section 2 ; en pratique, ils sont habituellement définis comme étant la perte de tout élément simple d'un réseau (c'est-à-dire ligne, transformateur, groupe générateur, ligne à deux ternes), soit perte soudaine, soit perte précédée d'un défaut monophasé ou triphasé [Galiana, McGillis & Marin 1992]. C'est ce que l'on appelle usuellement le critère N-1. L'entreprise d'électricité planifie et exploite son réseau de telle façon que, si un tel aléa plausible survient :

i) le réseau se rétablira rapidement grâce à l'intervention des systèmes usuels de protection et des dispositifs automatiques de conduite et continuera à fournir toute la charge à l'intérieur de valeurs caractéristiques d'urgence (tension et fréquence) et,

ii) retournera à un état stable, tout au plus au moyen de réajustements mineurs de ce réseau, y compris des manœuvres manuelles.

Le domaine dans lequel ces critères sont satisfaits est hachuré sur la figure 3.1 et est appelé « région sûre ». Dans cette région, la stabilité du réseau (c'est-à-dire la stabilité dynamique, transitoire ou à long terme) ne doit pas dépendre de plans de défense en profondeur [SPS, Special Protection Systems] tels que délestage ou déclenchement à la production ou intervention humaine directe. Comme cela a été mentionné plus haut, la sécurité exige que, exception faite pour les situations d'urgence (figure 2.2), l'on respecte à la fois l'adéquation en régime permanent et la stabilité en régime perturbé. Les limites de sécurité constituent par conséquent la première ligne de défense d'un réseau suivant une stratégie essentiellement « passive » ou « a priori » contre les nombreux événements qui peuvent perturber ou menacer son exploitation.

Comme mentionné ci-dessus, les mesures prises lors de la conception pour atténuer les effets d'aléas extrêmes fournissent à un réseau une seconde ligne de défense. Les stratégies qui entrent dans cette catégorie englobent un délestage local ou global contrôlé par la fréquence ou un déclenchement à la production.

TF 96.03.12

3.3.2. Identification of Secure States

In order to separate the secure and insecure states, normal practice for a utility is to select a range of credible contingencies (based on its own operating history and experience), often referred to as normal contingencies. These were defined in Section 2; in practice they are usually defined as the loss of any single element in a power system (i.e. line, transformer, generating unit, double-circuit line) either spontaneously or preceded by a single- or three-phase fault [Galiana, McGillis & Marin 1992]. This is usually referred to as the N-1 criterion. The utility plans and operates the power system such that, if any one of these credible contingencies occurs:

i) it will rapidly recover through the use of regular protection systems and automatic control devices, and continue to supply all the load within emergency (voltage and frequency) ratings, and,

ii) re-enter an adequate state at most by means of minor system readjustments, including manual switching.

The area where these criteria are satisfied is shown hatched in Fig. 3.1 and is called the "secure" region. In this region, system stability (i.e. either dynamic, transient or long-term voltage stability) must not depend on Special Protection Systems (SPS), such as load shedding or generation rejection, or direct human intervention. As stated above, security requires that, apart from temporary emergency conditions (Fig. 2.2), both steady-state adequacy and stability performance criteria be respected. Security limits therefore constitute the first line of defense of a power system in an essentially "passive" or "a priori" strategy against the many unforeseen events which can perturb or threaten its operation.

As mentioned before, design measures to mitigate the effect of extreme contingencies provide a second line of defence to the power system. Strategies which fall under this category include local or global frequency-controlled load shedding or generation rejection.

3.3.3. Security Criteria

This approach to dealing with power system security is fully deterministic. Deterministic criteria based on the N-1 rule tend to provide large margins in protecting the system against severe contingencies. In practice, this means that planners propose strong systems and operators operate with large security margins. Though investment and operational costs are relatively high, this has resulted in a high degree of reliability in most power systems.

The choice of deterministic criteria can have far-reaching effects on the geometry (i.e. size and shape) of the security region. For example, on a given system, if security limits determined on the basis of a criterion such as a single-line-to-ground fault are higher than those employing three-phase faults of equal duration, this will result in a larger region. However, the former criterion may result in a network reliability index of, say, 3 system shutdowns in ten years whereas the latter may provide a more reliable network by a factor of ten. In other words, increased system reliability is a direct consequence of establishing transmission capacity on the basis of more stringent criteria: the network is "capable of coping with a much wider range of adverse events" [McGillis et al. 1992]. Expressed in different terms, the short-term economic gain of operating at higher transmission capacities can be offset by a long-term drop in reliability. As it has been pointed out [Naggar 1986], probabilistic approaches based on appropriate criteria would undoubtedly help in finding an optimal bound between operating limits and system reliability.

3.4. SECURITY IN UTILITY OPERATIONS

3.4.1. The On-line Environment

The primary objective of operations planners (and of course operators) is security. Reliability indices are a means of quantifying the utility's performance (i.e. including criteria, strategies, investment choices and personnel administration) in its efforts to be secure.

In practice, system operators optimise the system such that, while operating within the security region, the total cost is minimised. This usually involves producing the most economic dispatch of generating plants within the operational constraints imposed: it is not necessarily the unconstrained optimum. When a contingency occurs, the effect can be to i) move the operating point shown in Fig. 3.1 and ii) change the geometry of the security region. Following this, the system will generally be reoptimised by the operators. If the point has moved outside the new security region, then the operators will take steps to bring the point back inside this secure domain (e.g. by reswitching or redispatch); if the point remains within the secure domain, then a redispatch may also be appropriate in order to reoptimise the system, in particular from an economics point of view.

3.4.2. Operations Planning

The power system frequently changes topology and, as we have seen, this can adversely impact the security region, especially in the case of the loss of some important element, such as a generator, a transmission line, a generator transformer, etc. Operators must therefore monitor power transfers and voltages to ensure that the system remains within the security region and, if necessary, take appropriate control measures (e.g. generation dispatch, reactive power switching). Operations planners determine this region, depending on the system structure, either by i) finding the security limits of each individual transmission corridor or ii) finding the secure dispatching limit of individual power plants for a set of pre-determined criteria. Such studies are usually performed off-line, particularly if security limits are based on transient- or voltage-stability criteria and require the use of correspondingly complex simulation software. As each change in topology modifies to some extent the limits of a power system, the problem of finding limits in this way is essentially of a combinatorial nature. Operations planners pare the problem down to a reasonable scale by analysing only a selected set of topologies (i.e. states), though this leads to conservative security limits [Marceau 1993]. Because of this inevitable underutilization of the system, system planners may be forced to prematurely upgrade the system when increased (secure) transmission capacity is desired.

3.3.3. Critères de sécurité

Cette approche pour traiter de la sécurité des réseaux est entièrement déterministe. Les critères déterministes fondés sur la règle N-1 tendent à fournir de grandes marges en protégeant un réseau contre des aléas sévères. En pratique cela signifie que les planificateurs proposent des réseaux robustes et que les agents de conduite les exploitent avec de grandes marges de sécurité. Quoique les investissements et les coûts opérationnels soient relativement élevés, ceci s'est traduit dans la plupart des réseaux par un degré élevé de fiabilité.

Le choix de critères déterministes peut avoir des effets d'une portée considérable sur la géométrie (c'est-à-dire la taille et la forme) de la région de sécurité. Par exemple, sur un réseau donné, si les limites de sécurité déterminées sur la base d'un critère de défaut monophasé à la terre sont plus élevées que celles mettant en jeu des défauts triphasés de durée égale, cela se traduira par une région plus grande. Le premier critère peut toutefois se traduire par un indice de fiabilité du réseau, disons, de 3 pannes de réseau sur dix ans, tandis que le second peut fournir un réseau dix fois plus fiable. En d'autres termes, une fiabilité accrue du réseau est une conséquence directe de la fixation de la capacité de transport sur la base de critères plus contraignants : le réseau est « capable de faire face à une gamme beaucoup plus large d'événements défavorables » [McGillis et al. 1992]. Ou en l'exprimant en des termes différents, le gain économique réalisé sur le court terme en exploitant avec des capacités de transport plus élevées peut être compensé par une chute sur le long terme de la fiabilité. Comme cela a été signalé [Naggar 1986], les approches probabilistes fondées sur des critères appropriés aideraient sans aucun doute à trouver un lien optimal entre les limites de fonctionnement et la fiabilité d'un réseau.

3.4. SÉCURITÉ DANS L'EXPLOITATION DES COMPAGNIES D'ÉLECTRICITÉ

3.4.1. L'environnement en ligne

L'objectif premier des planificateurs de l'exploitation (et bien entendu des agents de conduite) est la sécurité. Les indices de fiabilité constituent un moyen de quantifier le fonctionnement d'une entreprise d'électricité (c'est-à-dire couvrant les critères, les stratégies, les choix concernant les investissements et l'administration du personnel) dans ses efforts pour qu'il soit sûr.

Dans la pratique, les agents de conduite optimisent le réseau de telle manière qu'en fonctionnant à l'intérieur de la région de sécurité, le coût total soit minimisé. Ceci implique habituellement de réaliser la répartition la plus économique des centrales de production à l'intérieur des contraintes opérationnelles imposées ; ce n'est pas nécessairement l'optimum sans contraintes. Lorsqu'un aléa survient, l'effet peut être i) de déplacer le point de fonctionnement indiqué sur la figure 3.1 et ii) de modifier la géométrie de la région de sécurité. A la suite de cet aléa, le réseau sera généralement réoptimisé par les agents de conduite. Si ce point s'est déplacé à l'extérieur de la nouvelle région de sécurité, les agents de conduite entreprendront des actions afin de ramener ce point à l'intérieur du domaine sûr (par exemple, en réalisant de nouvelles manœuvres ou une nouvelle répartition) ; si ce point reste à l'intérieur du domaine sûr, une nouvelle répartition peut aussi être appropriée afin de réoptimiser le réseau, en particulier du point de vue économique.

3.4.2. Planification de l'exploitation

Un réseau change fréquemment de topologie et, comme nous l'avons vu, ceci peut avoir un impact négatif sur la région de sécurité, particulièrement dans le cas de perte d'un élément important tel qu'un alternateur, une ligne de transport, un transformateur d'alternateur, etc. Les agents de conduite doivent par conséquent surveiller les transferts de puissance et les tensions afin de garantir que le réseau reste à l'intérieur de la région de sécurité et prendre, si nécessaire, les mesures de conduite appropriées (répartition de la production, soutien en puissance réactive). Les planificateurs de l'exploitation déterminent cette région en fonction de la structure du réseau soit i) en trouvant les limites de sécurité pour chaque couloir individuel de transport, soit ii) en trouvant la limite sûre de répartition des centrales individuelles pour un ensemble de critères prédéterminés. On effectue généralement de telles études en mode déconnecté (ou si l'on préfère en « temps différé »), particulièrement si les limites de sécurité sont fondées sur des critères de stabilité transitoire ou de stabilité de la tension et exigent l'emploi de logiciels complexes en conséquence. Comme chaque changement dans la topologie modifie dans une certaine mesure les limites d'un réseau, le problème de trouver des limites de cette manière est essentiellement de nature combinatoire. Les planificateurs ramènent ce problème à une échelle raisonnable en analysant seulement un ensemble sélectionné de topologies (c'est-à-dire d'états) quoique ceci conduise à des limites conservatrices de sécurité [Marceau 1993]. A cause de cette sous-utilisation inévitable du réseau, les planificateurs pourraient être contraints de moderniser prématurément ce réseau dès qu'une capacité accrue de transport est souhaitée.

3.4.3. Evaluation en ligne de la sécurité

Ces observations constituent la base des efforts considérables actuellement entrepris pour amener l'analyse de la sécurité dans l'environnement en ligne. La logique est simple : si les limites de sécurité déterministes sont déterminées de manière précise pour la topologie du réseau en exploitation à tout instant donné, ceci élimine le besoin de limites conservatrices basées sur des choix et des hypothèses nombreux et représente une forme d'optimisation. Les techniques d'avant-garde des systèmes de gestion de l'énergie (Energy Management Systems, EMS) réalisent vraiment une évaluation en ligne de la sécurité en régime permanent, bien que ceci ne soit utile que pour des réseaux dans lesquels la sécurité en régime permanent constitue un problème. Dans des réseaux plus complexes, la détermination de limites de sécurité en ligne requiert l'emploi de logiciels extrêmement rapides pour des simulations relatives à la stabilité transitoire et à la stabilité de la tension ou des systèmes intelligents d'estimation qui peuvent déterminer de telles limites dans un laps de temps compatible avec le besoin de telles informations exprimé

IF 63.03.12

3.4.3. On-line Security Assessment

These observations form the basis of considerable efforts presently engaged in bringing security analysis to the on-line environment. The logic is simple: if deterministic security limits are determined precisely for the system topology in operation at any given time, this eliminates the need for conservative limits based on numerous choices and assumptions, and represents a form of optimisation. State-of-the-art Energy Management System (EMS) technology does indeed perform on-line steady-state security assessment, though this is useful only in systems where steady-state security is an issue. In more complex systems, on-line security limit determination requires the use of extremely rapid transient- or voltage-stability simulation software, or intelligent limit estimation systems which can determine such limits in a time-frame compatible with the operator's need of such information. The main focus of present research in dynamic security assessment is to develop the hardware and software technologies which will make this a reality [Meyer et al. 1997].

3.4.4. The Effect of the Time it Takes to Complete Remedial Action

If a power system state is inadequate, this implies that one or more system constraints are violated or maybe that system demand is not being satisfied. Remedial action is therefore required. This may take the form of redispatch, shedding load, or various alternative ways of controlling system parameters. However, all of these remedies require time to be accomplished. The necessary timescales for remedial action vary with the problem. If the inadequacy is a thermal overload then the operators may have many minutes or even hours to seek a solution. If the problem is one of voltage (i.e. either overvoltage or voltage collapse), then the timescale is several seconds to a few minutes. If it is transient instability, the timescale is seconds at most.

If the dynamic process of the power system causes departure from this state before the remedial action can be accomplished, then the system may transfer to a state with a higher degree of inadequacy or to an unstable state. If, on the other hand, the remedial action can be accomplished in a shorter time than that taken by the dynamic process, the system may revert to an adequate state or become partially inadequate where some loads are not supplied but the voltage and line constraints are not violated. This leads to the conclusion that the time to perform remedial action is a fundamental parameter in determining whether a state is adequate, partially adequate, inadequate or insecure.

Any state which can be defined as either inadequate or insecure can be considered a system failure state and, therefore, contributes to system unreliability. Reliability evaluation techniques which recognize as failure states only those in which inadequacy has been determined therefore ignore or neglect adequate states in which insecurity exists (potentially unstable states). However, these may lead to cascading or instability and, thus, to system failures not recognized in adequacy studies.

3.4.5. Failure States

We can now see that there are three cases which could lead, in principle, to a loss of supply. These are:

1) Cases where a combination of demand and generation is such that it is **not possible to operate within the secure region** (corresponding to stability criteria and N-1). In this case, it is necessary to either pre-fault disconnect demand, or (more likely) operate within the potentially insecure type of alert state.

2) Cases where it is **not possible to operate within the adequate or even the potentially inadequate state**. The commonest instance of this is a global insufficiency of generation. In this case, load shedding has to occur.

3) Where the power system is being operated within the secure area, but a fault or combination of faults, or two faults in rapid succession occur which take the operating point outside the adequate area. This is shown in Fig. 3.2 and corresponds to **the case of an extreme contingency** against which the so-called security region is not immune.

The above logic demonstrates that if the concept of security is ignored, some insecure states are declared adequate (as they should) and are not correctly accounted for as states which contribute to system unreliability. Nevertheless, probabilistic adequacy assessment coupled with deterministic (and therefore crude) security limits is traditionally the only practical alternative open to planners because of the enormous technical challenge of extending probabilistic methods into the area of security.

3.4.6. Instability

There is some controversy considering the position of instability in reliability analysis. Some authors consider the unstable state to be equivalent to the insecure state, but this practice is not followed in this document. Here, an insecure state is defined as one that is *potentially* unstable (see section 2.2). Instability may lead to system collapse or, if the remedial action is accomplished in a sufficiently short time, to a stable state which is likely to be both inadequate and insecure (potentially unstable). This is illustrated in Fig. 2.2.

3.5. SUMMARY

In this chapter, we have seen that the concept of security and its relationship to reliability is highly dependent on context. In system operations, the achievement of security is the principal objective: from the operator's point of view, if the system is secure at all times, reliability is achieved. In system planning, due to the practical difficulties associated with identifying secure and insecure states, reliability assessment has historically been based on the concept of adequacy.

These observations account for many of the difficulties which arise in attempting to arrive at universal definitions of both adequacy and security: the operations and system planning contexts have developed two related but different paradigms which are useful and meaningful in their respective contexts. This also accounts for the fact that probabilistic methods developed for reliability analysis in the system planning context fall short of the needs of the operations context: if probabilistic methods are to be applied with any success in operations, they must specifically target security assessment.

It would be possible in principle to operate the system probabilistically,

par l'agent de conduite. L'objet principal des recherches présentes concernant l'évaluation de la sécurité dynamique est de développer les technologies des matériels et des logiciels qui en feront une réalité [Meyer et al. 1997].

3.4.4. L'effet du temps mis à achever une action corrective

Si un état du réseau est inadéquat, ceci implique qu'une ou plusieurs contraintes de ce réseau soient enfreintes ou peut-être que la demande du réseau ne soit pas satisfaite. Une action corrective est donc nécessaire. Ceci peut prendre la forme d'une nouvelle répartition, d'un délestage ou de diverses autres manières d'agir sur les paramètres de ce réseau. Toutes ces actions réclament cependant un certain temps pour être accomplies. Les échelles de temps nécessaires pour ces actions varient avec le problème à résoudre. Si l'inadéquation consiste en une surcharge thermique, les agents de conduite peuvent disposer de plusieurs minutes ou même de plusieurs heures, pour chercher une solution. Si le problème concerne la tension, là l'échelle des temps va de plusieurs secondes à quelques minutes. S'il s'agit d'une instabilité transitoire, l'échelle des temps correspond à quelques secondes tout au plus.

Si le processus dynamique du réseau provoque une sortie de cet état avant que l'action corrective puisse être accomplie, le réseau peut aller vers un état comportant un degré plus élevé d'inadéquation ou vers un état instable. Si, d'autre part, l'action corrective peut être accomplie en un temps plus court que celui mis par le processus dynamique, le réseau peut retourner à un état adéquat ou devenir partiellement inadéquat lorsque certaines charges ne sont pas alimentées, mais que les contraintes relatives à la tension et aux lignes ne sont pas enfreintes. Ceci conduit à la conclusion que le temps pour effectuer une action corrective est un paramètre fondamental en vue de déterminer si un état est adéquat, partiellement adéquat, inadéquat ou non sûr.

Tout état que l'on peut définir comme étant soit inadéquat, soit non sûr, peut être considéré comme un état de défaillance du réseau et contribue, par conséquent, à la non fiabilité du réseau. Les techniques d'évaluation de la fiabilité qui reconnaissent comme états de défaillance seulement ceux dans lesquels l'inadéquation a été déterminée, ignorent par conséquent ou négligent les états adéquats dans lesquels l'insécurité existe (états potentiellement instables). Ceux-ci peuvent toutefois conduire à des défaillances en cascade ou à l'instabilité et ainsi à des pannes du réseau qui ne sont pas reconnues dans les études d'adéquation.

3.4.5. Etats de défaillance

Nous pouvons maintenant voir qu'il existe trois cas qui peuvent conduire, en principe, à une perte d'alimentation. Ce sont :

1) Les cas où une combinaison de la demande et de la production est telle qu'il n'est **pas possible de fonctionner à l'intérieur de la région sûre** (correspondant aux critères de stabilité et N-1). Dans ce cas, il est nécessaire, soit de déconnecter la demande avant défaut, soit (plus probablement) de fonctionner dans un type potentiellement non sûr d'état d'alerte.

2) Les cas où il n'est **pas possible de fonctionner dans un état adéquat ou même potentiellement inadéquat.** L'exemple le plus commun de ce cas est une insuffisance globale de la production. Dans ce cas, il faut procéder à des délestages.

3) Lorsque le réseau est bien exploité à l'intérieur du domaine sûr mais que surviennent un défaut ou une combinaison de défauts, ou encore deux défaut se suivant rapidement, déplaçant alors le point de fonctionnement à l'extérieur du domaine adéquat. Ceci est représenté sur la figure 3.2 et correspond **au cas d'un aléa extrême** contre lequel la région dite de sécurité n'est pas immunisée.

La logique ci-dessus démontre que si le concept de sécurité est ignoré, certains états non sûrs sont déclarés adéquats (comme cela se doit) et ne sont pas correctement pris en compte comme états contribuant à l'insécurité du réseau. L'évaluation probabiliste de l'adéquation associée à des limites de sécurité déterministes (et par conséquent grossières) est traditionnellement la seule variante pratique ouverte aux planificateurs à cause de l'énorme défi technique que représente l'extension des méthodes probabilistes au domaine de la sécurité.

3.4.6. Instabilité

Il existe une certaine controverse sur la prise en considération de l'instabilité dans l'analyse de la fiabilité. Certains auteurs considèrent que l'état instable est équivalent à un état non sûr, mais cette façon de voir n'est pas retenue dans le présent document. Ici, un état non sûr est défini comme un état qui est potentiellement instable (voir section 2.2). L'instabilité peut conduire à l'effondrement du réseau ou, si l'action corrective est réalisée en un temps suffisamment court, à un état stable dont il est probable qu'il soit à la fois inadéquat et non sûr (potentiellement instable). C'est ce qu'illustre la figure 2.2.

3.5. RÉSUMÉ

Dans ce chapitre, nous avons vu que le concept de sécurité et sa relation avec la fiabilité sont extrêmement fonction du contexte. Dans l'exploitation des réseaux, l'obtention de la sécurité est le principal objectif : du point de vue de l'agent de conduite, si le réseau est sûr à tout instant, la fiabilité est assurée. Dans la planification des réseaux, du fait des difficultés pratiques liées à l'identification des états sûrs et non sûrs, l'évaluation de la fiabilité a été fondée historiquement sur le concept d'adéquation.

Ces observations expliquent un bon nombre des difficultés qui apparaissent lorsque l'on tente d'arriver à des définitions universelles à la fois pour l'adéquation et la sécurité : les contextes de l'exploitation et de la planification des réseaux ont développé deux paradigmes liés mais différents qui sont utiles et expressifs dans leurs contextes respectifs. Ceci explique également le fait que les méthodes probabilistes développées pour l'analyse de la fiabilité dans le contexte de la planification des réseaux ne répondent pas aux besoins du contexte de l'exploitation : si ces méthodes probabilistes doivent s'appliquer avec quelque succès à l'exploitation, il faut qu'elles aient spécifiquement pour objectif l'évaluation de la sécurité.

Il serait en principe possible d'exploiter un réseau de manière probabiliste en utilisant l'analyse coûts-avantages. On

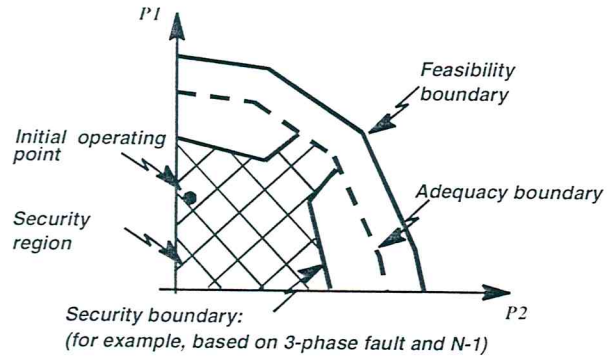

Figure 3.2. Passage d'un état sûr à un état inadéquat.
Figure 3.2. Transition from secure to inadequate state.

using cost-benefit analysis. However, it is presently felt within utilities that using probabilistic procedure operationally may increase the risk of a large catastrophe because of the comparatively low degree of maturity of these methods to date. Nevertheless, there is still merit in calculating the actual operational risk (a probabilistic value) even if this is not optimized on a cost-benefit basis. In the new environment of open energy markets and competing power generation, risk determination is fast becoming a necessity and this will, without doubt, further encourage the development of appropriate probabilistic methods.

4. PROBABILISTIC SECURITY ASSESSMENT

4.1. INTRODUCTION

The probabilistic nature of power system security (both dynamic and static) has been well recognized since the early days of modern power system operation and control [Dy Liacco 1967, Fink & Carlsen 1978, Schweppe 1978]. However, probabilistic security assessment has not been much developed. Even if some practical methods have been elaborated, none has been able to impose itself and, as we have seen, in today's everyday practice the problem is still essentially approached deterministically.

Since the probabilistic approach aims at making better use of the information available for decision-making, it should in principle lead to better decisions, which explains the real interest in this approach in many utilities. Because present-day conditions force systems to operate closer to their limits, the need for objective decisions based on a quantitative evaluation of incipient risks is more stringently felt.

This chapter proposes some thoughts and orientations on the introduction of probabilistic methods in the field of power system security assessment. It aims at identifying the interest and the field of application of the probabilistic analysis, at stating orientations which are in continuity with deterministic analysis, by taking into account the different contexts which exist in a utility, and at basing probabilistic analysis on well-known and proven methods. It is structured as follows:

- Description of a theoretical framework for probabilistic security assessment
- Discussion and illustration of the approach and expectations of using the probabilistic approach in different contexts
- Discussion on the strategy to be adopted in order to introduce the probabilistic approach smoothly in working methods
- Summary

4.2. PROBABILISTIC *VS* DETERMINISTIC SECURITY ASSESSMENT

4.2.1. A Framework For Probabilistic Security Assessment

As highlighted in the preceding chapters, security assessment aims at taking decisions so as to reach an appropriate compromise between operating (and investment) costs and robustness with respect to possible disturbances.

The aim of the probabilistic approach is essentially to make systematic use of the information available in any decision-making context. Indeed, much of the information available to the decision-maker is of a probabilistic nature, such as future load patterns, next contingencies, neighbouring system states, long-term economic and social contexts to quote only the most straightforward ones. Furthermore, among the aspects usually considered as deterministic, most suffer from various sources of uncertainty, resulting for instance from limitations in modeling and measurement systems, and hence are better modeled by (subjective) probability distributions than deterministic default values.

The probabilistic approach may be described as a sequence of steps leading to the evaluation of alternative decisions in terms of their impact on the operating (and investment) costs and economic losses generated by disturbances. Notice that the trade-off between normal operating (and investment) costs and security will be a consequence of the choice of a severity function, which is discussed below.

An important outcome of this formulation is that the impact of a disturbance on decision-making is now weighed by its probability of occurrence and its impact in terms of economic consequences, measured by the severity function. The probability of occurrence may vary with equipment type, location and configuration as well as with meteorological conditions. The economic consequences may be small (e.g. loss of a small plant without important variations in frequency and voltages) or large (e.g. a partial blackout).

Figure 4.1 describes a theoretical framework for probabilistic security assessment. Various security scenarios are defined by the conjunction of three components: a pre-contingency equilibrium state (denoted by "state"), a modeling hypothesis (denoted by "model") defining structure and parameters of static and dynamic models, and a sequence of external disturbances (denoted by "disturbances") which are supposed to initiate the dynamics. Given the precise definition

pense cependant généralement dans le cercle des compagnies d'électricité que l'utilisation d'une procédure probabiliste à des fins opérationnelles peut accroître le risque d'une grande catastrophe par suite du degré de maturité comparativement faible à ce jour de ces méthodes. Néanmoins, il existe toujours un mérite à calculer le risque opérationnel réel (une valeur probabiliste) même si celui-ci n'est pas optimisé sur une base coûts-avantages. Dans le nouvel environnement des marchés ouverts de l'énergie et de la concurrence au niveau de la production, la détermination du risque devient rapidement une nécessité et ceci encouragera sans nul doute le développement de méthodes probabilistes appropriées.

4. EVALUATION PROBABILISTE DE LA SÉCURITÉ

4.1. INTRODUCTION

La nature probabiliste de la sécurité (dynamique et statique à la fois) des réseaux a bien été reconnue dès les premiers jours de l'exploitation et de la conduite modernes de ces réseaux [DyLiacco 1967, Fink & Carlsen 1978, Schweppe 1978]. L'évaluation de la sécurité n'a toutefois pas été beaucoup développée. Même si un certain nombre de méthodes pratiques ont été élaborées, aucune d'entre elles n'a été capable de s'imposer et, comme nous l'avons vu dans la pratique de tous les jours, l'approche de ce problème reste toujours essentiellement déterministe.

Comme l'approche probabiliste a pour objectif de faire un meilleur usage des informations disponibles en vue de la prise de décision, cette approche devrait en principe conduire à de meilleures décisions, ce qui explique le réel intérêt porté à cette approche par beaucoup de compagnies d'électricité. Parce que les conditions actuelles contraignent les réseaux à fonctionner plus près de leurs limites, le besoin de décisions objectives fondées sur une évaluation quantitative des risques encourus est ressenti de façon plus impérieuse.

Le présent chapitre propose quelques idées et quelques orientations concernant l'introduction de méthodes probabilistes dans le domaine de l'évaluation de la sécurité des réseaux. Il vise à identifier l'intérêt et le domaine d'application de l'analyse probabiliste, à fixer des orientations qui se trouvent dans le prolongement de l'analyse déterministe en prenant en compte les différents contextes qui existent dans une entreprise d'électricité et en fondant l'analyse probabiliste sur des méthodes bien connues et éprouvées. La structure de ce chapitre est la suivante :

- Description d'un cadre théorique pour l'évaluation probabiliste de la sécurité
- Examen et illustration de la méthode et des espoirs mis dans l'emploi de l'approche probabiliste dans différents contextes
- Examen de la stratégie à adopter afin d'introduire en douceur l'approche probabiliste dans les méthodes de travail
- Résumé

4.2. COMPARAISON ENTRE ÉVALUATION PROBABILISTE ET ÉVALUATION DÉTERMINISTE DE LA SÉCURITÉ

4.2.1. Un cadre pour l'évaluation probabiliste de la sécurité

Comme cela a été mis en évidence dans les chapitres précédents, l'évaluation de la sécurité a pour but de prendre des décisions de manière à arriver à un compromis approprié entre les coûts de fonctionnement (et les investissements) et la robustesse relativement aux perturbations éventuelles.

Le but de l'approche probabiliste est essentiellement de faire un usage systématique des informations disponibles dans tout contexte de prise de décision. En effet, une bonne part des informations à la disposition des décideurs sont de nature probabiliste, tels que les profils des consommations futures, les aléas prochains, les états dans lesquels se trouvent les réseaux avoisinants, les contextes économiques et sociaux à long terme pour ne citer que les plus simples. De plus, parmi les aspects considérés habituellement comme déterministes, la plupart souffrent de diverses sources d'incertitude résultant par exemple de limitations dans la modélisation et dans les systèmes de mesure et sont mieux modélisés par des dispositions probabilistes (subjectives) que par des valeurs déterministes par défaut.

L'approche probabiliste peut se décrire comme étant une séquence d'étapes conduisant à l'évaluation de décisions portant sur des variantes en termes d'impact correspondant sur les coûts de fonctionnement (et les investissements) et de pertes économiques engendrées par les perturbations. A noter que le compromis entre les coûts normaux de fonctionnement (et les investissements) et la sécurité sera une conséquence du choix de la fonction de sévérité qui est étudiée ci-dessous.

Une conséquence importante de cette formulation est que l'impact d'une perturbation sur la prise de décision est maintenant pondéré par sa probabilité d'occurrence et son impact en termes de conséquences économiques mesuré par la fonction de sévérité. La probabilité d'occurrence peut varier avec le type d'équipement, de l'emplacement et de la configuration, ainsi qu'avec les conditions météorologiques. Les conséquences économiques peuvent être faibles (par exemple la perte d'une petite centrale sans variations importantes de la fréquence et des tensions) ou importantes (par exemple, panne générale sur la quasi-totalité du réseau).

La figure 4.1 décrit un cadre théorique pour l'évaluation probabiliste de la sécurité. On définit divers scénarios par la conjonction de trois composantes : un état d'équilibre avant aléa (désigné par « état »), une hypothèse de modélisation (désignée par module) définissant la structure et les paramètres des modèles statiques et dynamiques et une séquence de perturbations externes (désignée par « perturbations ») qui sont supposées initialiser les phénomènes dynamiques. Etant donné la définition précise d'un scénario, on peut en principe déterminer sa sévérité (ou risque conditionnel) qui évalue les conséquences techniques et/ou économiques de ce scénario. Comme dans tous les environnements pratiques de prise de décision, certaines de ces trois composantes au moins sont

TF 36.03.12

1. Assumption of a prior probability distribution of static and dynamic models of the power system and its possible pre-contingency states, depending on the decision-making context (ctxt) and the information (info) available therein:

$$p\,(\text{model, state} \mid \text{ctxt, info})$$

2. Assumption of a conditional probability distribution of all possible disturbances according to the context and the information at hand (this could model faults as well as random load variations):

$$p\,(\text{disturbances} \mid \text{ctxt, info, model, state})$$

3. Definition of a severity function, which evaluates the severity of a particular scenario (i.e. model, state and disturbances) in terms of its consequences (e.g. expected economical consequences taking into account the various costs of load-shedding, voltage and frequency degradations, brownouts):

$$\textit{severity}\,(\text{ctxt, info, model, state, disturbances})$$

4. Evaluation of the overall risk as the expectation of severity:

$$\overline{\text{Risk}}\,(\text{ctxt, info}) \equiv$$

$$\int_{\text{state, model}} \left[\int_{\text{dist}} \textit{severity}\,(\text{ctxt, info, model, state, disturbances}) \times p\,(\text{disturbances} \mid \text{ctxt, info, model, state}) \right]$$

$$\times\, p\,(\text{model, state} \mid \text{ctxt, info})$$

5. Evaluation of a decision by summing its corresponding operating (and investment) costs, on the one hand, and overall risk, on the other hand (Note that in practice these costs are also of probabilistic nature and the values used are actually expected values.

Figure 4.1. The main steps of the probabilistic security assessment framework.

of a scenario, one can in principle determine its severity (or conditional risk), which evaluates technical and/or economic consequences of the scenario. Since in all practical decision-making environments at least some of the three scenario components are uncertain, decisions should be based on the *expected* severity (i.e. the risk) by taking into account (at least in theory) all possible scenarios and weighing their severity by their probability of occurrence.

Notice that the probability distributions of power system states, models and disturbances depend on two conditions, which we have distinguished on purpose: context (ctxt), to distinguish between planning, operation or management environments; and information (info) to account for the dependence of decisions on the quality of prior knowledge about models, forecasts and disturbances. Therefore, the severity itself also depends on the decision-making context and the available information. For the sake of simplicity, this has so far been assumed to be a deterministic quantity. However, in practical situations, outage costs will depend on many uncertain factors, like for example the time taken for load restoration as well as extraneous factors influencing the customer perception of service interruptions. Probability distributions and severity functions, hence the risk, depend of course on the decision alternative which is considered. Examples of these various aspects are provided in Section 4.4.

Thus the probabilistic approach allows — in fact obliges — the user to model his degree of ignorance on the various aspects. In particular, not only the distribution of system states and dynamic models of one's own power system can in principle be taken into account, but also the level of accuracy of knowledge about states and the behaviour of the overall environment (neighbouring utilities, customers, etc.). Finally, a very appealing characteristic of the probabilistic approach is that it is completely general and may in principle be used in an integrated fashion at various steps of the decision-making. From long-term system planning to real-time decision-making, the same methodology can be used; only the shape of probability distributions and possibly the definition of severity functions need be changed.

4.2.2. The Decision-Making Contexts

The different decision-making contexts are: operations (including operations planning), system planning, and management. As we have seen in the previous chapter, security is the primary focus of the operations context. However, for strategic feedback to flow between the different contexts, uniform information protocols and methods of analysis must exist for the different contexts.

As the context moves from planning towards operation, approaching "real time", probability distributions become in principle sharper since additional information becomes available and the range of conditions and disturbances which will be influenced by the decisions becomes narrower. However, perfect knowledge is never available: even in the emergency state, when the contingency has already occurred, there remains (often significant) uncertainty about the subsequent trajectory of the system. Thus, the risk associated with the system varies according to the context:

- When the system is in operation, the considered risk depends on the state of the system during a time period of some seconds to some hours. It is the "instantaneous" risk.
- When a system is being designed, the risk depends on all the possible events that may affect the system during several years. It is the eventual risk.
- When the performance of the system is assessed, the calculated risk integrates the different instantaneous risks of the period being examined. It is the incurred risk.

4.2.3. Modeling the Available Information

In the probabilistic approach, the modeling steps 1 and 2 in Fig. 4.1 explicitly

1. Distribution de probabilité présumée des modèles statiques et dynamiques du réseau et de ses états possibles avant aléas en fonction du contexte de prise de décision (ctxt) et des informations disponibles (info) :

$$p\ (\text{modèle, état} \mid \text{ctxt, info})$$

2. Distribution de probabilité conditionnelle présumée de toutes les perturbations possibles selon le contexte et les informations dont on dispose (ceci peut modéliser des défauts aussi bien que des variations aléatoires de charge) :

$$p\ (\text{perturbations} \mid \text{ctxt, info, modèle, état})$$

3. Définition d'une fonction de sévérité qui évalue la sévérité d'un scénario particulier (c'est-à-dire modèle, état et perturbations) sur le plan de ses conséquences (conséquences économiques attendues tenant compte des divers coûts dus aux délestages, aux dégradations de la tension et de la fréquence, aux pannes générales) :

$$\textit{sévérité}\ (\text{ctxt, info, modèle, état, perturbations})$$

4. Evaluation du risque global en tant qu'espérance de sévérité :

$$\overline{\text{Risque}}\ (\text{ctxt, info}) \equiv$$

$$\int_{\text{état, modèle}} \left[\int_{\text{dist}} \textit{sévérité}\ (\text{ctxt, info, modèle, état, perturbations}) \times p\ (\text{perturbations} \mid \text{ctxt, info, modèle, état}) \right]$$

$$\times p\ (\text{modèle, état} \mid \text{ctxt, info})$$

5. Evaluation d'une décision par sommation des coûts correspondants de fonctionnement (et d'investissement) d'une part et du risque global d'autre part. (Noter que dans la pratique ces coûts sont aussi de nature probabiliste et que les valeurs utilisées sont des valeurs réellement attendues.)

Figure 4.1. Les étapes principales dans le cadre de l'évaluation probabiliste de la sécurité.

incertaines, les décisions devraient être fondées sur la sévérité attendue (c'est-à-dire le risque) en prenant en compte, (au moins en théorie), tous les scénarios possibles et en pondérant leur sévérité par leur probabilité d'occurrence.

Il faut noter que les distributions de probabilité pour les états du réseau, les modèles et les perturbations dépendent de deux conditions que nous avons distinguées à dessein : contexte (ctxt) pour faire la distinction entre les environnements de planification, d'exploitation ou de gestion, et informations (info) pour prendre en compte la dépendance des décisions sur la qualité des connaissances antérieures concernant les modèles, les prévisions et les perturbations. C'est pourquoi la sévérité elle-même dépend aussi du contexte de prise de décision et des informations disponibles. Pour des raisons de simplicité, on a admis jusqu'à maintenant qu'il s'agissait d'une valeur déterministe. Dans des situations pratiques les coûts des indisponibilités dépendront toutefois de beaucoup de facteurs incertains tels que le temps mis par exemple à rétablir la consommation de même que des facteurs étrangers influençant la perception par le consommateur de l'interruption du service. Les distributions de probabilité et les fonctions de sévérité, donc le risque, dépendent bien sûr de la variante de décision qui est prise en considération. La section 4.4 fournit des exemples de ces divers aspects.

L'approche probabiliste permet ainsi — et en fait oblige — l'utilisateur à modéliser son degré d'ignorance concernant ces divers aspects. En particulier, non seulement la distribution des états du réseau et les modèles dynamiques du réseau de chacun peuvent en principe être pris en compte, mais également le niveau de précision des connaissances relatives aux états et au comportement de l'environnement global (compagnies d'électricité avoisinantes, clients, etc.). Enfin, une caractéristique très attrayante de la méthode probabiliste est qu'elle est complètement générale et peut en principe être utilisée de manière intégrée à diverses étapes de la prise de décision. Depuis la planification des réseaux sur le long terme jusqu'à la prise de décision, on peut utiliser la même méthodologie ; la forme seulement des distributions de probabilité et éventuellement la définition des fonctions de sévérité ont besoin d'être modifiées.

4.2.2. Les contextes de la prise de décision

Les différents contextes de la prise de décision sont : l'exploitation (y compris la gestion prévisionnelle), la planification des réseaux et la gestion d'ensemble. Comme nous l'avons vu dans le chapitre précédent, la sécurité est le souci premier dans le contexte de l'exploitation. Toutefois, pour que des informations stratégiques en retour circulent entre ces différents contextes, il faut qu'il existe pour ces différents contextes des protocoles d'information et des méthodes d'analyse uniformes.

Au fur et à mesure que le contexte passe de la planification à l'exploitation, en se rapprochant du « temps réel », les distributions de probabilité deviennent en principe plus resserrées du fait que des informations supplémentaires deviennent disponibles et que la plage des situations et des perturbations qui sera influencée par les décisions devient plus étroite. Des connaissances parfaites ne sont toutefois jamais à disposition : même en état d'urgence, lorsque l'aléa est déjà survenu, il reste une incertitude (souvent importante) pour ce qui concerne l'évolution ultérieure du réseau. Ainsi, le risque associé au réseau varie selon le contexte :

- Lorsque le réseau est en exploitation, le risque considéré dépend de l'état de ce réseau durant un intervalle de temps allant de quelques secondes à quelques heures. C'est le risque « instantané ».
- Lorsqu'un réseau est en train d'être conçu, le risque dépend de tous les événements possibles qui peuvent affecter ce réseau pendant plusieurs années. C'est le risque éventuel.
- Lorsque le fonctionnement du réseau est évalué, le risque calculé

take into account information accuracy. In particular, the information which is not perfectly known in a given context may be randomized appropriately (e.g. unobservable parts such as neighbouring utilities or badly defined modeling aspects such as load behaviour etc. should be represented by "uninformative" probability distributions), in order to yield robust decisions.

On the other hand, using sharper probability distributions corresponding to more precise data makes it possible to assess the value (in terms of impact on the decisions) of better information, and thereby allows one to justify economically the gathering of new data, for example by improving measurement systems, by exchanging information with other utilities, or by refining models and improving model parameter estimates. Thus, the amount of information available about the system clearly influences the expected risk. It is therefore important to be able to study the influence of the quality of the information available in a given context on the quality of the decisions which will be taken therein.

Notice that the usual practice in deterministic security assessment consists of replacing unavailable information by default values: either conservative values and hypotheses for those parameters that are expected to have a significant influence, or expected values otherwise. In the probabilistic approach, it is possible instead to use a properly chosen probability distribution, thereby avoiding biased evaluations: when new data becomes available, the probability distribution need only to be updated. For example, in on-line security assessment, if the operator becomes aware of the fact that a lightning storm is crossing an important transmission corridor, he will significantly update his estimate of disturbance probabilities. Such knowledge allows him to economically justify certain decisions in order to reduce the system's risk with respect to contingencies in this corridor.

Similarly, in a power system with a large amount of independent producers and dispersed generation, it is well known that the lack of information available about these system components may lead to difficulties and increased costs since robust decisions must be taken with respect to the unknown behaviour of the uncontrollable part of the system. Again, the probabilistic approach enables one to assess the economic impact of various alternatives. Also, the effect of exchanging (or hiding) system data between different companies can also be modeled in this way.

4.3. APPLICATION OF THE PROBABILISTIC METHOD IN DIFFERENT CONTEXTS

4.3.1. Applications in Operations

In the operations context, the probabilistic method would consist in:

- Evaluating, in real time, the instantaneous risk associated with the state of the system.
- Comparing this risk to an alert threshold.
- Identifying the possible actions which would reduce the instantaneous risk.
- Evaluating the cost associated with each possible operation and the gain expected on the risk level. The net gain is the gain minus the cost.
- Choosing the operation with the greatest net gain. If the gain is never positive, do not change the state of the system.

The use of the probabilistic method makes it possible to make decisions justified economically on the basis of an evaluation of the impact of these choices on the risk of insecurity of the system. An evident benefit of this approach is that it is able to justify operations that would, *a priori,* appear to be very costly (i.e. for the customers) if their profitability is confirmed by a quantitative evaluation of the risk. It also makes it possible to avoid operations that the transfer limits would have imposed if risk analysis determines that they are not profitable to the utility in economic terms. Furthermore, time-varying disturbance probabilities may be taken into account, e.g. according to weather forecasts and anticipated lightning storms. Finally, the probabilistic approach permits one to arbitrate objectively between preventive control and post-disturbance emergency actions. **All these possibilities result in an optimization of transfer capability and a more economic system.**

4.3.2. Applications in Planning

In the system planning context, the probabilistic method would consist in:

- Evaluating the eventual risk associated with each of the system design scenarios analyzed.
- Comparing this risk to some threshold value of maximum acceptable eventual risk.
- Discarding scenarios that do not respect this threshold.
- Choosing, from the remaining scenarios, an optimal scenario by performing a technical and economical analysis integrating all aspects of the problem. This analysis may include an economical evaluation of the eventual risk.

The use of the probabilistic method makes it possible to make more accurate economic decisions based on an evaluation of the impact of these choices on the risk of insecurity to the system. **An evident benefit is that it shows the value of reducing the risk through actions impacting on the frequency of events, while the deterministic method applies only to the reduction of their consequences.**

4.3.3. Applications in Management

In the management context, the probabilistic method consists in monitoring the incurred risk associated to each customer within a certain time frame and comparing this risk to each one's supply-reliability statistics: this permits one to assess the extent to which the planning and operating strategies used by a company have met its objectives and its contractual obligations.

In the context of the unbundling of electrical companies and the introduction of customer-supplier relationships between generation, transmission and distribution, the availability of probabilistic performance indicators evaluating the incurred risk for a customer during a given period of time makes it possible to define a clear contractual relationship. By comparing the incurred risk with the actual reliability performance of the system, the supplier has in hand strategic information which allows him to justify his price or to adjust his performance in accordance to the needs of his customer. Additionally, **the follow-up of incurred risk *versus* appropriate**

CA 33.04.12

intègre les différents risques de la période en cours d'examen. C'est le risque encouru.

4.2.3. Modélisation des informations disponibles

Dans l'approche probabiliste, les étapes de modélisation 1 et 2 de la figure 4.1 tiennent explicitement compte de la précision des informations. En particulier, les informations qui ne sont pas parfaitement connues dans un contexte donné peuvent être rendues aléatoires de manière appropriée (par exemple des parties non observables telles que les compagnies d'électricité voisines ou des aspects de modélisation mal définis tels que le comportement de la charge, etc., devraient être représentées par des lois de probabilité « non informatives »), afin d'obtenir des décisions énergiques.

D'autre part, l'utilisation de distributions de probabilité plus resserrées correspondant à des données plus précises rend possible l'estimation de la valeur (en termes d'impact sur les décisions) de meilleures informations et permet par là à chacun de justifier économiquement la collecte de nouvelles données, par exemple en améliorant les systèmes de mesure, en échangeant des informations avec d'autres compagnies d'électricité ou en affinant les modèles et en peaufinant les valeurs estimées des paramètres des modèles. Ainsi, le volume des informations disponibles concernant le réseau influence clairement le risque prévu. C'est pourquoi il est important d'être capable d'étudier l'influence de la qualité des informations disponibles dans un contexte donné sur la qualité des décisions qui seront ainsi prises.

A noter que, dans l'évaluation déterministe de la sécurité, la pratique usuelle consiste à remplacer des informations non disponibles par des valeurs par défaut ; soit des valeurs et des hypothèses conservatrices pour ceux des paramètres qui sont supposés avoir une influence significative, soit autrement par des valeurs attendues. Dans l'approche probabiliste, il est possible d'utiliser, en lieu et place, une loi de probabilité choisie de façon convenable en évitant de ce fait des évaluations faussées : lorsque de nouvelles données deviennent disponibles, cette distribution de probabilité a seulement besoin d'une mise à jour. Par exemple, lors d'une évaluation en ligne, si l'agent de conduite s'aperçoit du fait qu'un orage est en train de croiser un couloir important de transport, il reverra significativement à la hausse son estimation des probabilités de perturbations. Une telle connaissance lui permet de justifier économiquement certaines décisions prises en vue de réduire le risque du réseau quant aux aléas dans ce couloir.

De façon similaire, dans un réseau comportant une grande quantité de producteurs indépendants et des unités de production disséminées, il est bien connu que le manque d'informations disponible sur ces composants du réseau peut conduire à des difficultés et à des coûts accrus du fait qu'il faut prendre des décisions énergiques relativement au comportement inconnu de la partie non maîtrisable de ce réseau. De nouveau, l'approche probabiliste permet à chacun d'évaluer l'impact économique de diverses alternatives. L'effet d'échanger (ou de cacher) des données intéressant le réseau entre différentes compagnies d'électricité peut être également modélisé de cette manière.

4.3. APPLICATION DE LA MÉTHODE PROBABILISTE DANS DIFFÉRENTS CONTEXTES

4.3.1. Applications dans la gestion prévisionnelle

Dans le contexte de la gestion prévisionnelle, la méthode probabiliste consisterait à :

- Evaluer en temps réel le risque instantané associé à l'état du réseau.
- Comparer ce risque à un seuil d'alerte.
- Identifier les actions possibles qui pourraient réduire ce risque instantané.
- Evaluer le coût lié à chaque exploitation possible et le gain attendu sur le niveau du risque. Le gain net est ce gain moins le coût.
- Choisir l'exploitation présentant le gain net le plus élevé. Si le gain n'est jamais positif, ne pas changer l'état du réseau.

L'utilisation de la méthode probabiliste rend possible la prise de décisions justifiées économiquement sur la base d'une évaluation de l'impact de ces choix sur le risque d'insécurité du réseau. Un avantage évident de cette approche est qu'elle est capable de justifier des exploitations qui apparaîtraient a priori être très onéreuses (par exemple pour les clients), si leur rentabilité est confirmée par une évaluation quantitative du risque. Cela rend aussi possible d'éviter des exploitations que les limites de transfert auraient imposé si l'analyse du risque détermine qu'elles ne sont pas rentables pour la compagnie d'électricité en termes économiques. De plus, des probabilités de perturbations variant dans le temps peuvent être prises en compte, par exemple selon les prévisions météorologiques et les orages attendus. Enfin, l'approche probabiliste permet à chacun d'arbitrer de manière objective entre actions de régulation préventive et actions d'urgence après perturbations. **Toutes ces possibilités se traduisent par une optimisation de la capacité de transfert et un réseau plus économique.**

4.3.2. Applications à la planification

Dans le contexte de la planification des réseaux, la méthode probabiliste consisterait à :

- Evaluer le risque éventuel associé à chacun des scénarios de conception de réseau analysé.
- Comparer ce risque à une certaine valeur de seuil du risque éventuel maximal acceptable.
- Rejeter les scénarios qui ne respectent pas ce seuil.
- Choisir parmi les scénarios restants, un scénario optimal en réalisant une analyse technique et économique intégrant tous les aspects du problème. Cette analyse peut englober une évaluation économique du risque éventuel.

L'emploi d'une telle méthode probabiliste permet de prendre des décisions économiques plus exactes fondées sur une évaluation de l'impact de ces choix sur le risque d'insécurité d'un réseau. **Un avantage évident est que cela montre la valeur de la réduction du risque par des actions ayant un impact sur la fréquence des événements, alors que la méthode déterministe s'attache seulement à la réduction de leurs conséquences.**

TF 38.03.12

reliability indices makes it possible to measure the effectiveness of the system's security strategies and more easily justifies projects aimed at strengthening the system.

4.4. EXAMPLE

4.4.1. The Power System

In this section, a simple, hypothetical but realistic power system model is used to illustrate the concepts introduced above, though no numerical results are provided. Even so, it is hoped that the discussion will clarify the concepts of the present chapter and underline their value.

Fig. 4.1 depicts the single-line diagram of a small hypothetical power system. It is composed of two large power plants (a hydro plant composed of five 500 MW units and a coal fired thermal plant of three 600 MW units), a longitudinal 400 kV transmission system (composed of three corridors) and two load areas (a main 3000 MW load area and a secondary one of 1500 MW peak). There is an old synchronous compensator of 300 Mvar installed close to a big steel plant (300 MW peak), approximately in the middle of one corridor. Inside the main load area, there is an independent producer operating a brand new 500 MW combined-cycle gas power plant. Additionally, there are remote-controlled capacitor banks in each load area.

The system is interconnected with two larger neighbouring systems *via* a 1000 MW DC link (to neighbour A, 10 000 MW peak load) and a double circuit AC link of about 150 km (to neighbour B, 30 000 MW peak load). The two neighbours are also interconnected *via* a double circuit AC link of 75 km.

The system has structural weaknesses: risk of transient instability (mostly due to the long distance between the hydro plant and the other plants) and risk of voltage instability (due to the lack of reactive support in the secondary load area). Small signal instabilities may also appear in the form of undamped oscillations between the hydro plant and some remote machines of neighbour A. Upon loss of generation, frequency stability is mainly conditioned by the spinning reserve of neighbours A and B and the capacity of the double circuit AC interconnection. Thus, various automatic emergency and special stability control systems have been added to the system: generation shedding in the hydro plant; under-voltage load shedding in the secondary load area; under-frequency load shedding in both main and secondary load areas; automatic tripping of the interconnecting lines to neighbour B upon out-of-step detection.

It is supposed that the utility which originally owned the transmission system and the two large power plants has been split into an independent generating company operating the plants, and a separate transmission company responsible for planning and operating the 400 kV transmission system and its interconnections, together with the various reactive support devices and special stability control systems.

4.4.2. Decision-Making in Operations and Operations Planning

A short-term operations planning task is now considered: we are in a normal weekday at the end of August; it is 1 p.m. and the operator has to determine strategies for the peak load condition of tonight, which is expected according to yesterday's forecast to be reached at 6 p.m. with the following conditions: 1000 ± 2% MW in the secondary load area and 1800 ± 1.5% MW in the main load area. The steel plant is scheduled to remain in operation until 6:30 p.m. There is plenty of water in the reservoirs, but some generating sets are under maintenance: one in the hydro plant and one in the coal fired plant. Temperature is rather high, and line overload protections are using summer settings. All lines and interconnections are in operation. Before starting his work, the operator looks at the most recent weather fore-

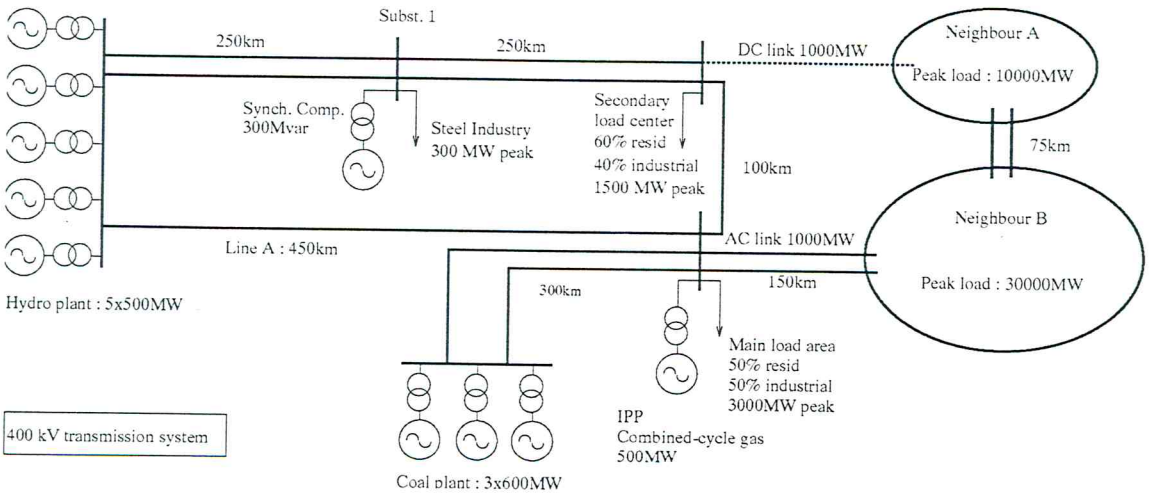

Figure 4.2. Réseau imaginaire.
Figure 4.2. Hypothetical power system.

4.3.3. Applications à la gestion globale

Dans le contexte de la gestion globale de l'entreprise, la méthode probabiliste consiste à surveiller durant un certain intervalle de temps le risque encouru associé à chaque client et à comparer ce risque aux statistiques relatives à la fiabilité d'alimentation de chacun ; ceci permet à chacun d'évaluer la mesure dans laquelle les stratégies de planification et d'exploitation utilisées par une compagnie donnée ont atteint leurs objectifs et rempli leurs obligations contractuelles.

Dans le contexte de la déconcentration des compagnies d'électricité et de l'introduction de relations clients-fournisseurs entre les entités assurant la production, le transport et la distribution de l'énergie électrique, la disponibilité d'indicateurs probabilistes de fonctionnement évaluant le risque encouru par un client sur un intervalle de temps déterminé permet de définir une relation contractuelle claire. En comparant le risque encouru aux performances réelles au niveau de la fiabilité du réseau, le fournisseur a en main des informations stratégiques qui lui permettent de justifier son prix ou d'ajuster ses performances selon les besoins de son client. De plus, **le suivi du risque encouru par rapport à des indices appropriés de fiabilité rend possible la mesure de l'efficacité des stratégies de sécurité d'un réseau et justifie plus facilement les projets ayant pour but de renforcer le réseau.**

4.4. EXEMPLE

4.4.1. Réseau imaginaire étudié

Dans cette section, nous utiliserons un modèle de réseau, simple, imaginaire mais réaliste afin d'illustrer les concepts introduits ci-dessus et bien qu'aucun résultat numérique ne soit fourni. Même ainsi, nous espérons que cette étude clarifiera les concepts et soulignera leur valeur.

La figure 4.2 représente le schéma unifilaire d'un réseau imaginaire de petite taille. Ce réseau se compose de deux centrales de grande puissance (une usine hydroélectrique comprenant cinq groupes de 500 MW et une centrale thermique brûlant du charbon comportant trois tranches de 600 MW chacune), un réseau de transport à grande distance (comprenant trois couloirs) et de deux zones de consommation (une zone principale avec une consommation de 3 000 MW et une zone secondaire avec une consommation de 1 500 MW en pointe). Il existe un compensateur synchrone de 300 Mvar, de type ancien, qui est installé à proximité d'une grande aciérie (300 MW en pointe), approximativement au milieu d'un des couloirs. A l'intérieur de la zone principale de consommation, il y a un producteur indépendant d'énergie électrique qui exploite une centrale flambant neuve de 500 MW, à cycle combiné, brûlant du gaz naturel. Il existe de plus, dans chaque zone de consommation, des batteries de condensateurs commandées à distance.

Ce réseau est interconnecté avec deux grands réseaux avoisinants à l'aide d'une liaison CC de 1 000 MW (vers le réseau voisin A, 10 000 MW en charge de pointe) et une liaison CA à deux lignes d'env. 150 km de long (vers le réseau B, 30 000 MW en charge de pointe). Ces deux réseaux voisins sont eux-mêmes interconnectés à travers une liaison CA à deux lignes de 75 km de long.

Ce réseau présente une faiblesse structurelle : risque d'instabilité transitoire (dû principalement à la grande distance séparant l'usine hydroélectrique et les autres centrales) et risque d'instabilité en tension (dû au manque de soutien en puissance réactive dans la zone secondaire de consommation). Des instabilités peuvent aussi apparaître sous la forme d'oscillations non amorties entre l'usine hydroélectrique et certaines machines éloignées du réseau A. En cas de perte d'une partie de la production, la stabilité de la fréquence est essentiellement conditionnée par les réserves tournantes des réseaux voisins A et B ainsi que la capacité de transport de l'interconnexion CA à deux lignes. On a ajouté pour cette raison au réseau divers systèmes fonctionnant automatiquement en cas d'urgence et des systèmes spéciaux de régulation de la stabilité : déclenchement de la production à l'usine hydroélectrique, délestage à minimum de tension dans la zone secondaire de consommation, délestage à minimum de fréquence à la fois dans les zones principale et secondaire de consommation, déclenchement automatique des lignes d'interconnexion vers le réseau voisin B dès détection d'une rupture de synchronisme.

On a supposé que la compagnie d'électricité qui était à l'origine propriétaire du réseau de transport et des deux grandes centrales, a été séparée en une compagnie de production d'énergie électrique exploitant les centrales et une compagnie distincte responsable de la planification et de l'exploitation du réseau à 400 kV et de ses interconnexions en même temps que des divers dispositifs de soutien en puissance réactive et des systèmes de régulation de la stabilité.

4.4.2. Prise de décision en exploitation et en gestion prévisionnelle

On considère maintenant une tâche de gestion prévisionnelle à court terme : nous sommes un jour normal de la semaine à la fin du mois d'août. Il est 1 heure de l'après-midi et l'agent de conduite a à déterminer les stratégies pour passer la pointe de consommation en soirée qui, selon la prévision de la veille, devrait être atteinte à 18 h dans les conditions suivantes : 1 000 MW ± 2 % dans la zone secondaire de consommation et 1800 MW ± 1,5 % dans la zone principale de consommation. Il est prévu que l'aciérie reste en activité jusqu'à 18 h 30. Il y a beaucoup d'eau dans les réservoirs des barrages, mais quelques groupes générateurs sont en cours de maintenance : un à l'usine hydroélectrique et un à la centrale thermique. La température est plutôt élevée et les protections des lignes contre les surcharges affichent les réglages d'été. Toutes les lignes et toutes les interconnexions sont en service. Avant de commencer son travail, l'agent de conduite consulte les informations météorologiques les plus récentes (reçues à midi) ; on s'attend à ce que le temps soit clair sur la zone principale de consommation, mais il sera nuageux avec du vent près de la zone secondaire de consommation avec une forte probabilité d'orages.

Les stratégies de fonctionnement doivent être publiées à 15 h afin de permettre aux différentes compagnies assurant la production de finaliser les transactions avec leurs clients. En vue de constituer une provision pour des coûts potentiels d'indisponibilité, nous

cast information (received at noon): the weather is expected to be clear in the main load area, but it will be cloudy and windy near the secondary load area with a high probability of thunderstorms.

The operating strategies must be published by 3 p.m. in order to enable the different generating companies to finalize transactions with customers. In order to make a provision for potential outage costs, we assume that the grid code specifies that each generating company must pay a connection fee to the transmission company in proportion to the generated MWs times the effect of their injection on the overall risk. This of course assumes that the transmission company is solely responsible for customer outage costs in the event that the service is interrupted. The operating strategies must therefore be provided in the form of connection fee tables at each generating company injection node(s), reflecting the sensitivity of the risk for various generation dispatch levels.

Thus the basic subproblem which the operator needs to solve in order to determine the strategies will be to assess the expected risk on a per hour basis under various assumed generation schedules meeting the expected demand. Let us discuss various assumptions he could make in order to figure out the probabilistic model needed for this.

4.4.3. Model

Since the transmission system as well as the generating units in the two large power plants are well-known from past experience, the operator would probably assume a deterministic modeling for them. On the other hand, the combined-cycle gas turbine is very new, and he could suppose that it will be operated with rather conservative (but not precisely known) settings of under/over speed and under/over voltage protections. Concerning load models (*i.e.* steel plant, main and secondary load areas), he would probably randomize them (*i.e.* assign probabilities to selected load levels) according to statistical information collected during similar conditions in the past. Protection delays and thresholds could be randomized in the same fashion to take into account existing uncertainties. Furthermore, knowing that the model of the DC line used in his dynamic simulation program is not very reliable, he could assume a certain probability that the DC line will trip upon faults in the nearby AC system. On the other hand, the equivalent models used to represent the neighbouring utilities will need to be randomized significantly around their expected operating point, since their details and operating strategies are not known. In particular, the operator would assume a certain probability that the interconnection between the two neighbours is operated with only one single circuit in operation, and randomize the amount of spinning reserve and other equivalent machines' parameters.

4.4.4. Operating State

The first step is to define a probability distribution for the load level of the system in each area for the considered time period, *i.e.* at 6 p.m., taking into account yesterday's forecast and additional information obtained at 12 a.m. The operator would adjust the load forecast in the secondary load area to a higher value, say 1200 ± 4% MW, with a Gaussian distribution, to take into account the effect of the predicted weather conditions. In each scenario, the difference between the assumed generation dispatch schedule and the total amount of load plus losses is allocated arbitrarily (with randomized participation factors) among the generating units in operation and the interconnections. Given the final active generation schedule, voltage set-points and reactive power support devices are also adjusted according to usual operating strategies, so as to yield voltages near nominal values.

4.4.5. Disturbances

There are mainly three kinds of events that may initiate dynamics possibly leading to abnormal system conditions: the load trend (which will be growing, at various possible rates of change), internal device failures (with a very low probability) and failures of external origin, with a much higher probability in the secondary load area, since a storm is expected there. The internal device failures could probably be neglected in this study, since they are very unlikely; on the other hand, the external disturbances (load and faults) should be modeled as random processes, starting at time t = 6 p.m. and acting upon the system during one hour. Their probability distributions would be derived from operating statistics under normal and stormy conditions.

4.4.6. Severity

The severity of a scenario is measured by the outage costs for both buyers and generating companies which would be disconnected during the scenario. Such costs depend on the amount of energy not received (or not sold), and possibly a fixed price for critical consumers, e.g. like the steel plant. In order to model the time taken by load restoration, one could use statistical information derived from off-line simulations, relating it to the kind of generators lost and the amount of load to restore. Thus, we assume that given the description of the consequences of a scenario, it is possible to compute an equivalent global outage cost.

What remains to be done? Supposing that all the probability distributions mentioned above have been defined, the risk may in principle be determined by Monte-Carlo simulations. In the brute force approach, this would imply, for each assumed generation dispatch schedule, sampling several thousand or more scenarios, and simulating them numerically (*i.e.* for both short-term and mid-term dynamics) in order to determine the consequences and compute the expected severity. Clearly, at the present time this would not be feasible with existing software and hardware, even for as simple a system as that of Figure 4.1. However, it may be possible to improve the efficiency of the above procedure by using various filtering and/or variance reduction techniques. For example, among all the possible simulation scenarios, by means of fast screening tools, it may be possible to sort out a much smaller number that would actually lead to severe conditions, and simulate only the latter in detail.

Another more basic question concerns the sensitivity of the computed risk levels to the assumed input information. Clearly, before using the probabilistic approach, a utility would like to know how some more or less arbitrary choices (e.g. assumptions about outage costs or behaviour of neighbouring

supposons que le code du réseau spécifie que chaque compagnie doit payer à la compagnie assurant le transport un droit de raccordement proportionnels aux MW produits multipliés par l'effet de leur injection sur le risque global. Ceci suppose bien entendu que la compagnie de transport est seule responsable des coûts d'indisponibilité client au cas où le service est interrompu. Les stratégies de fonctionnement doivent donc être fournies sous la forme de tables de droits de raccordement au(x) nœud(s) d'injection pour chaque compagnie de production, reflétant la sensibilité du risque aux divers niveaux de répartition de la production.

Donc, le sous-problème que l'agent de conduite a à résoudre afin de déterminer les stratégies sera d'évaluer le risque attendu sur une base horaire pour divers programmes de production escomptés satisfaisant la demande attendue. Nous pouvons alors examiner les diverses hypothèses qu'il pourrait faire pour déterminer le modèle probabiliste dont il a besoin pour cela.

4.4.3. Modèle

Comme le réseau de transport de même que les groupes générateurs des deux grandes centrales sont bien connus en fonction de l'expérience passée, l'agent de conduite présumera probablement pour eux une modélisation déterministe. D'autre part, la turbine à gaz à cycle combiné est très neuve et il pourrait supposer qu'elle sera exploitée avec des réglages plutôt conservateurs (mais non connus de manière précise) pour les protections fonctionnant à minimum/maximum de vitesse et à minimum/maximum de tension. En ce qui concerne les modèles des charges (c.-à-d. l'aciérie, les zones principale et secondaire de consommation), il les randomisera probablement (c.-à-d. qu'il assignera des probabilités à des niveaux de charge choisis) selon les informations statistiques collectées durant des conditions similaires par le passé. Les temporisations et les seuils des protection pourraient être randomisés de la même manière afin de prendre en compte les incertitudes existantes. Par ailleurs, sachant que le modèle de la ligne CC utilisé dans son programme de simulation n'est pas très fiable, il pourrait présumer avec une certaine probabilité que la ligne CC déclenchera sur défaut dans le réseau CA avoisinant. D'autre part, les modèles équivalents utilisés pour représenter les compagnies d'électricité avoisinantes auront besoin d'être randomisés de façon importante autour de leur point de fonctionnement escompté du fait que les détails correspondants et leurs stratégies de fonctionnement ne sont pas connus. En particulier, l'agent de conduite supposera avec une certaine probabilité que l'interconnexion entre les deux réseaux n'est exploité qu'avec une seule ligne en service et randomisera la quantité de réserves tournantes et d'autres paramètres de machines équivalents.

4.4.4. Etat de fonctionnement

La première étape consiste à définir une distribution de probabilité pour le niveau de charge du réseau dans chaque zone pour la période considérée, c.-à-d. à 18 h en tenant compte des prévisions de la veille et des informations complémentaires recueillies à 12 h. L'agent de conduite ajustera la prévision de charge dans la zone secondaire de consommation à une valeur plus élevée, disons 1200 MW ± 4 % avec une distribution de Gauss afin de tenir compte des conditions météorologiques prévues. Dans chaque scénario, la différence entre le programme de répartition prévu et le volume total de la charge plus les pertes est allouée de manière arbitraire (avec des coefficients randomisés de participation) aux groupes générateurs en exploitation et aux interconnexions. Etant donné un programme final de production de puissance active, les points de consigne en tension et les dispositifs de soutien de la puissance réactive sont également ajustés selon les stratégies de fonctionnement habituelles, de façon à arriver à des tensions près de leurs valeurs nominales.

4.4.5. Perturbations

Il y a principalement trois sortes d'événements qui puissent initialiser des phénomènes dynamiques conduisant éventuellement à des conditions anormales pour le réseau : la tendance de la consommation (qui peut éventuellement croître suivant diverses vitesses de variation), les défaillances internes des dispositifs (avec une très faible probabilité) et les défaillances d'origine externe, avec une beaucoup plus grande probabilité dans la zone secondaire de consommation du fait qu'un orage y est attendu. Les défaillances internes des dispositifs pourraient probablement être négligées dans cette étude du fait qu'elles sont très improbables ; d'autre part, les perturbations externes (charge et défauts) devraient être modélisées en tant que processus aléatoires démarrant au temps t = 18 h et agissant sur le réseau pendant une heure. Leurs distributions de probabilité seraient dérivées de statistiques de fonctionnement dans des conditions normales et par temps d'orage.

4.4.6. Sévérité

La sévérité d'un scénario se mesure par les coûts d'indisponibilité à la fois pour les acheteurs et les compagnies d'électricité qui se trouveraient déconnectés durant le scénario. De tels coûts sont fonction de la quantité d'énergie non reçue (ou non vendue) et il s'agit éventuellement d'un prix fixé pour des consommateurs critiques, tels que l'aciérie par exemple. Afin de modéliser le temps pris pour le rétablissement de la consommation, on pourrait utiliser des informations statistiques déduites de simulations en mode déconnecté, en les liant au genre d'alternateurs perdus et à l'importance de la consommation à rétablir. Ainsi, nous supposons qu'étant donné la description des conséquences d'un scénario, il est possible de calculer un coût d'indisponibilité global équivalent.

Que reste-t-il à faire ? En supposant que toutes les distributions de probabilité mentionnées ci-dessus aient été définies, le risque peut en principe être déterminé par des simulations de Monte-Carlo. Dans une approche « en force », ceci impliquerait, pour chaque programme de répartition de production admis, d'échantillonner plusieurs milliers de scénarios ou davantage et de les simuler numériquement (c.-à-d. pour des caractéristiques dynamiques à la fois à court et à moyen terme) afin de déterminer leurs conséquences et de calculer la sévérité attendue. Evidemment, pour le moment, ceci ne serait pas faisable avec les matériels et les logiciels existants même pour un réseau aussi simple que celui de la figure 4.1. Il serait cependant possible

TF 38.08.12

utilities) will influence the resulting strategies. Thus, in the context of operations planning, engineers would make some sensitivity studies in order to determine the accuracy of results.

Other similar problems with a broader scope would also need to be solved for maintenance scheduling of the transmission lines and other equipment under the responsibility of the transmission company. The generating companies on the other hand would schedule their own maintenance periods according to their expectation of return, indirectly taking into account security *via* their expectation of the risks at their injection points. They would thus build up a data base of statistics of the latter in order to perform their own risk assessment.

4.4.7. Decision-Making in Planning

Let us suppose that during about the same period, the planning department launches a new study in order to assess various ways to improve system security. To be realistic, we suppose that present-day conditions exclude building new lines or calling for new generators. The decision alternatives considered could for example be: series compensation of lines from the hydro plant; thyristor controled series compensation; single-pole switching of lines; replacement of the synchronous compensator by a larger, more reliable static var compensator. The planning study could assume that the new equipment is commissioned within one year and evaluate the annual savings for a five-year period.

The planning study could also assume various system trajectories for the five years following commissioning. At each time step, they would simulate system operation according to the probabilistic strategy described above including the expected decision-making processes of generating companies in order to define plausible maintenance schedules. In order to consider the impact of weather conditions, they would use long-term statistics on storm occurrences and relate these to forced equipment outages due to unreliability; water reservoir inflows would also be taken into account.

4.4.8. Information Exchange

In the example above, we have supposed that information is missing about some parts of the system in each decision-making context, forcing the decision-maker to fill-in with more or less subjective probability distributions. For example, the operator didn't know some key information about the neighbouring utilities, and was forced to assume a random distribution in order to compute the expected risk. Similarly, operations planners cannot assume they have full information about the maintenance schedules of the different generators and, reciprocally, the generating companies have only a limited view on system security through the use of statistics about risks imputed to their injection points.

This lack of information leads of course to suboptimal use of system resources (*i.e.* from either under- or over-design). In other words, sharing more information leads to better planning and operation of the system, thus reducing costs for everybody. Hence, one possible use of the probabilistic framework, in the context of off-line studies, is to estimate the savings which would result from sharing information. These cost reductions could be estimated by each decision-maker on his own, thus providing an incentive for sharing information in a multilateral way.

For example, in off-line studies, the operations planning department could perform simulations of system operation under the assumption that the operator has obtained information from the neighbouring utilities concerning the status of their interconnecting lines, the amount of primary reserve, and more accurate model data. Feeding this information into the operations planning studies would both lead to tighter estimates of the risk, and allow better use of the system by adapting the strategies to actual system conditions. Comparing the corresponding costs and risks with those obtained with less information allows one to determine the economic value of the information.

4.5. APPLICATION OF THE PROBABILISTIC APPROACH INTO WORKING METHODS

The probabilistic approach to security assessment attempts to quantify the risk associated with decisions in order to maintain the same reliability as before but with a higher level of system capability. It aims to achieve this solely by enhancing the decision-making process. However, the introduction of this approach into working methods is difficult because of the strength of the deterministic tradition and because of the uncertainties related to the accuracy of the probabilistic results. Also, the objective is not to evaluate the risk in an absolute sense but to act in order to avoid an unacceptable risk. It is thus the quality of the decision that counts and not the quality of the hypotheses on which the decision is based: one performs decisions on a relative basis, *i.e.* by analysing alternatives and comparing them on an equal footing. Of course, the concept of quality has yet to be defined rigourously in the decision-making context.

One way to approach the problem consists in enhancing the deterministic method by adding probabilistic analysis results as an explanation. For example, a company might quantitatively assess the risk associated with decisions without changing proven working methods. This type of exercise could — over time — lead to enhanced deterministic criteria, but it perpetuates their use.

Another way to approach the problem consists in developing a strictly probabilistic decision-making method that would co-exist with the deterministic method. The confrontation of both methods should make it possible, on the one hand, to enhance and reinforce the probabilistic method in order to be sure of the quality of the decisions it leads to, and on the other hand, to readjust the deterministic decision criteria on the basis of the additional information contributed by the probabilistic method. In the long term, this could conceivably lead to the adoption of the probabilistic approach, though, in the short term, it could also contribute to discredit the method if results are not found convincing.

A further possibility would be to determine for successive classes of deterministic criteria (e.g. single-phase, three-phase, single line, double line, etc.) their associated risk level. Then, for a given decision found out by the probabilistic approach to be optimal, one could associate to it the deter-

d'améliorer l'efficacité de la procédure ci-dessus en utilisant diverses techniques de filtrage et de réduction de la variance. Par exemple, au moyen d'outils de sélection rapides, il pourrait être possible d'extraire, parmi les scénarios de simulation possibles, un nombre plus petit de scénarios qui conduiraient réellement à des conditions sévères et simuler seulement ces derniers en détail.

Une autre question plus fondamentale concerne la sensibilité des niveaux calculés de risque aux informations admises par hypothèse à l'entrée. Evidemment, avant d'employer une approche probabiliste, une compagnie aimerait savoir comment certains choix plus ou moins arbitraires (par exemple, des hypothèses faites quant aux coûts dus aux indisponibilités ou au comportement de compagnies d'électricité avoisinantes) influenceront les stratégies résultantes. Dans le contexte de la gestion prévisionnelle, les ingénieurs feront ainsi des études de sensibilité afin de déterminer l'exactitude des résultats.

Il sera aussi nécessaire de résoudre des problèmes similaires couvrant un champ plus large pour programmer la maintenance des lignes de transport et des autres équipements se trouvant sous la responsabilité de la compagnie de transport. D'autre part, les compagnies assurant la production programmeront leurs propres périodes de maintenance selon leur espérance mathématique de retour, tenant ainsi indirectement compte de la sécurité au travers de leur espérance de risque à leurs points d'injection. Elles établiront donc une base de données comportant des statistiques concernant cette dernière afin de réaliser leur propre évaluation des risques.

4.4.7. Prise de décision lors de la planification

Supposons qu'à peu près au même moment, le service chargé de la planification lance une nouvelle étude afin d'évaluer diverses façons d'améliorer la sécurité du réseau. Afin d'être réaliste, nous supposons que les conditions d'aujourd'hui excluent de construire de nouvelles lignes ou de faire appel à de nouveaux alternateurs. Les autres variantes à envisager pourraient être par exemple : compensation série des lignes partant de l'usine hydroélectrique, compensation série commandée par thyristors, réenclenchement monophasé des lignes, remplacement du compensateur synchrone par un compensateur statique de puissance réactive qui ait une puissance nominale plus grande et qui soit plus fiable. L'étude de planification pourrait admettre que le nouvel équipement soit mis en service dans un délai d'un an et évaluer les économies annuelles réalisées sur une période de cinq ans.

L'étude de planification pourrait aussi projeter diverses évolutions du réseau pour les cinq années suivant cette mise en service. A chacune de ces étapes, on pourrait simuler l'exploitation du réseau selon la stratégie probabiliste décrite ci-dessus y compris les processus prévus de prise de décision des compagnies assurant la production en vue de définir des programmes de maintenance plausibles. Pour prendre en considération l'impact des conditions météorologiques, on pourrait utiliser des statistiques à long terme relatives à l'apparition des orages et lier celles-ci aux indisponibilités forcées des équipements dues à la non fiabilité ; il faudrait également tenir compte des arrivées d'eau dans les barrages-réservoirs.

4.4.8. Echange d'informations

Dans l'exemple ci-dessus, nous avons supposé qu'il manquait des informations concernant certaines parties du réseau dans chaque contexte de prise de décision, forçant ainsi le décideur à compléter à l'aide de distributions de probabilité plus ou moins subjectives. Par exemple, l'agent de conduite n'avait pas connaissance de certaines informations clés concernant les compagnies d'électricité avoisinantes et se trouvait contraint de retenir une répartition aléatoire afin de calculer le risque attendu. De façon similaire, les planificateurs travaillant sur la gestion prévisionnelle ne peuvent pas présumer qu'ils disposent de toutes les informations relatives aux programmes de maintenance des différents alternateurs et, réciproquement, les compagnies assurant la production ont seulement une vue limitée de la sécurité du réseau par l'emploi de statistiques relatives aux risques imputés à leurs points d'injection.

Ce manque d'informations conduit bien entendu à une utilisation en dessous de l'optimum des ressources du réseau (ou par sous-dimensionnement, ou par surdimensionnement). En d'autres termes, partager davantage d'informations conduit à une meilleure planification et à une meilleure exploitation du réseau, réduisant ainsi les coûts pour tout le monde. Une utilisation possible du cadre probabiliste dans le contexte des études en mode déconnecté est d'estimer les économies qui résulteraient du partage des informations. Chaque décideur peut estimer pour sa part ces réductions de coût, créant ainsi une incitation à partager les informations d'une façon multilatérale.

Par exemple, dans les études en mode déconnecté, le service assurant la planification de la gestion prévisionnelle pourrait effectuer des simulations de l'exploitation du réseau en supposant que l'agent de conduite ait obtenu des compagnies d'électricité avoisinantes les informations concernant l'état de leurs lignes d'interconnexion, l'importance des puissances affectées en première réserve et des données caractéristiques plus précises pour les modèles. L'introduction de ces informations dans les études de planification conduirait à la fois à des estimations de risques plus serrées et permettrait une meilleure utilisation du réseau en adaptant les stratégies aux conditions réelles du réseau. La comparaison des coûts et des risques correspondants avec ceux obtenus avec moins d'informations permet à chacun de déterminer la valeur économique de ces informations.

4.5. APPLICATION DE L'APPROCHE PROBABILISTE DANS LES MÉTHODES DE TRAVAIL

L'approche probabiliste pour l'évaluation de la sécurité tente de quantifier le risque associé aux décisions afin de maintenir la même fiabilité qu'auparavant mais avec un niveau plus élevé de capacité de transport du réseau. Son objectif est d'y arriver uniquement en améliorant le processus de prise de décision. L'introduction de cette approche dans les méthodes de travail est cependant difficile à cause de la force de la tradition déterministe et à cause des incertitudes liées à l'exactitude des résultats probabilistes. Ainsi, le but n'est pas d'évaluer le risque dans l'absolu mais d'agir afin d'éviter

mininistic criterion which would lead to a similar risk and/or cost.

4.6. SUMMARY: THE CHALLENGES OF THE PROBABILISTIC APPROACH

In the last twenty years, much theoretical progress has been made, e.g. in exploiting probability theory for decision-making in intelligent systems. In terms of research, some pioneering work was done in the eighties by [Billinton & Kuruganty 1980, Anderson & Bose 1983, Wu, Tsai & Yu 1988] followed more recently by [Alvarado et al. 1991, Leite da Silva, Endrenyi & Wang 1993, Vieira Filho et al. 1994, Wehenkel 1996, Jacquemart et al. 1995, McCalley et al. 1995, Irizarry et al. 1995]. Probability methods have also been successfully applied to the load flow problem. However, the major challenges in implementing a probabilistic approach in power system security assessment are practical ones.

Indeed, the first challenge concerns the **data collection problem**, in other words, how to develop good enough probabilistic models of the power system? This question entails, on the one hand, the gathering and processing of statistical information about power system states, models and disturbances, and, on the other hand, the use of engineering judgement to fill in missing information. In this respect, the good news are that utilities are collecting large amounts of real-time data in a systematic fashion, which may be easily stored thanks to the low cost of modern storage devices. Further, automatic learning techniques are progressing and will hopefully allow one to extract the required probabilistic models from such very large data bases.

The second challenge lies in the definition of a **severity function**, which requires the economic evaluation of (short term and long term) consequences of a disturbance, in particular the customer's perception of service interruptions, and quality variations. This is certainly a non-trivial problem. Further, in order to correctly assess the risks of certain very large disturbances, it may become necessary to develop more detailed and more global dynamic simulation models than those used today in security assessment [Wehenkel et al. 1997].

The third is related to **computational aspects**, in other words, how to estimate the expected risk with sufficient accuracy? Whatever its precise definition, the risk is essentially a non-linear, highly complex function of the models, states and disturbances, and its computation *via* brute force would involve massive numbers of Monte-Carlo trials, each one consisting of one or several detailed numerical simulations. In order to do this, the challenge is to develop integrated software frameworks combining screening tools and detailed simulations, going beyond the simple determination of individual transfer limits described originally in [Marceau 1993]. Again, the good news comes from the hardware side: Monte-Carlo simulations are very easy to parallelize and, when compared to the possible economic earnings, computing power is extremely cheap.

Another related issue concerns the extraction of decision-making strategies from the Monte-Carlo simulations, in other words, how to identify decisions leading to a **better economic trade-off between risk and operating costs?** In this context again, automatic learning and stochastic optimization techniques may be valuable tools in order to extract and exploit useful information from the Monte-Carlo simulations.

5. CONCLUSION AND RECOMMENDATIONS

Though probabilistic methods have long evolved in the area of power system reliability assessment, they were used almost exclusively in adequacy evaluations by system planners. The basic focus in system operation is the other aspect of reliability, security, which at the present is almost always evaluated through methods employing deterministic criteria. Efforts at formalizing the concepts of probabilistic security and adequacy and their relation to reliability are not yet at a very advanced stage, and it is hoped that this report will contribute to the advancement of this complex topic. **Our first recommendation is that further work be done to define a consistent set of terms for probabilistic adequacy and security assessment, based on the discussion in the present report.**

Power systems tend to become larger and larger with more sophisticated emergency controls and defense plans mitigating the possible consequences of disturbances. These technological changes have led to more robust and more economic systems; at the same time, growing economic pressure have forced the systems to operate ever closer to the present deterministic limits. Hopefully, this report has demonstrated that a probabilistic approach to security analysis provides a promising framework for obtaining more flexible limits and for better assisting in planning and operating decisions. **Our second recommendation is that an integrated probabilistic security and adequacy methodology be developed, including appropriate indices and criteria.**

In the developing culture of free third-party access to transmission systems, and increased competition and deregulation in the industry, the number of decision-makers will grow very quickly. Information sharing (*i.e.* information trading) will become a major concern in future power system planning and operation. Here too, the probabilistic approach may be useful in allowing decision-makers to evaluate the economic impact of information about other utilities' systems and strategies, customers, policies, etc. and the price they should be ready to pay for it. Also, probabilistic methods are required to determine the risks involved with decison alternatives. **Our third recommendation is that the issues of information exchange and risk analysis be actively addressed by utilities, including the development of appropriate probabilistic models.**

In the opinion of the present Task Force, the probabilistic approach to power system security assessment will be, when fully developed, a sound, flexible and very general tool, superior to the present deterministic approaches. It will have widespread potential for applications and allow decision-makers to make better use of information and to assess the risks involved with the alternatives they can choose from.

un risque inacceptable. C'est alors la qualité de la décision qui compte et non la qualité des hypothèses sur lesquelles cette décision est fondée : on prend des décisions sur une base relative, c.-à-d. en analysant des variantes et en les comparant sur un pied d'égalité. Bien entendu, il faut maintenant définir de façon rigoureuse le concept de qualité dans le contexte de la prise de décision.

Une manière d'aborder le problème consiste à améliorer la méthode déterministe en y ajoutant les résultats de l'analyse probabiliste en tant qu'explication. Une compagnie peut, par exemple, évaluer de manière quantitative le risque associé aux décisions sans changer des méthodes de travail ayant fait leurs preuves. Ce type d'exercice pourrait — à la longue — aboutir à des critères déterministes améliorés, mais perpétue leur emploi.

Une autre manière d'aborder ce problème consiste à développer une méthode de prise de décision strictement probabiliste qui pourrait coexister avec la méthode déterministe. La confrontation de ces deux méthodes permettrait, d'une part, d'améliorer et de renforcer la méthode probabiliste afin d'être sûr de la qualité des décision auxquelles elle conduit et, d'autre part, de réajuster les critères déterministes de décision sur la base d'informations complémentaires apportées par la méthode probabiliste. Sur le long terme cela pourrait en théorie conduire à l'adoption de l'approche probabiliste, bien que sur le court terme, cela puisse aussi contribuer à discréditer la méthode si les résultats ne sont pas reconnus convaincants.

Une autre possibilité serait de déterminer pour des classes consécutives de critères déterministes (par exemple, monophasé, triphasé, ligne simple, ligne double, etc.) leur niveau de risque associé. Ainsi, pour une décision donnée indiquée comme étant optimale par l'approche probabiliste, on pourrait lui associer le critère déterministe qui aurait conduit à un risque et/ou à un coût similaire.

4.6. RÉSUMÉ : LES DÉFIS DE L'APPROCHE PROBABILISTE

Au cours des vingt dernières années, beaucoup de progrès théoriques ont été réalisés, par exemple en exploitant la théorie des probabilités pour la prise de décision dans des systèmes intelligents. Pour ce qui concerne la recherche, quelques travaux de pionniers ont été faits dans les années quatre-vingts [Billinton & Kuruganty 1980, Anderson & Bose 1983, Wu, Tsai & Yu 1988], suivis par [Alvarado et al. 1991, Leite da Silva, Endrenyi & Wang 1993, Vieira Filho et al. 1994, Wehenkel 1996. Jacquemart et al. 1995, Irizarry et al. 1995]. Les méthodes probabilistes ont également été appliquées avec succès au problème de la répartition des flux de puissance. Les défis majeurs pour la mise en œuvre d'une approche probabiliste pour l'évaluation de la sécurité des réseaux sont toutefois d'ordre pratique.

En effet, le premier défi concerne **le problème de la collecte des données,** soit en d'autres termes, comment développer des modèles probabilistes de réseaux suffisamment bons ? Cette question implique, d'une part, de rassembler et de traiter les informations statistiques relatives aux états, aux modèles et aux perturbations du réseau et, d'autre part, de faire appel à un jugement relevant de l'ingénierie pour remplacer les informations manquantes. A cet égard, il y a comme bonnes nouvelles que les compagnies d'électricité collectent de façon systématique de grandes quantités de données en temps réel qui peuvent être facilement mises en mémoire grâce au faible coût des dispositifs modernes de stockage. De plus, les techniques d'apprentissage automatique continuent de faire des progrès et permettront d'extraire de ces bases de données très importantes les modèles probabilistes demandés.

Le deuxième défi est dans la définition d'une **fonction de sévérité** qui exige l'évaluation économique des conséquences (à court terme et à long terme) d'une perturbation, en particulier la perception par le client des interruptions de service et des variations de la qualité. Ce n'est certes pas un problème sans importance. De plus, afin d'évaluer correctement les risques de certaines perturbations très importantes, il peut devenir nécessaire de développer des modèles pour simulations dynamiques plus détaillés et plus globaux que ceux utilisés aujourd'hui dans l'évaluation de la sécurité [Wehenkel et al. 1997].

Le troisième défi est en relation avec **les aspects liés aux calculs,** en d'autres termes, comment évaluer le risque attendu avec une précision suffisante ? Quelle que soit sa définition précise, le risque est essentiellement une fonction extrêmement complexe, non linéaire des modèles, des états et des perturbations et sa détermination par un calcul « en force » impliquerait un nombre énorme d'essais de Monte-Carlo, chacun consistant en une ou plusieurs simulations numériques détaillées. Pour réaliser cela, le défi consiste à développer des cadres logiciels intégrés combinant des outils de sélection et des simulations détaillées, allant bien au-delà de la simple détermination de limites de transfert individuelles décrites à l'origine par [Marceau 1993]. De nouveau, les bonnes nouvelles viennent du côté matériel : les simulations de Monte-Carlo sont très faciles à traiter en parallèle et lorsqu'on la compare aux gains économiques possibles, la capacité de calcul est extrêmement bon marché.

Un autre problème connexe concerne l'extraction de stratégies de prise de décision en partant des simulations de Monte-Carlo, en d'autres termes, comment identifier les décisions conduisant à **un meilleur compromis entre risque et coûts de fonctionnement** ? Dans ce contexte, les techniques d'apprentissage automatique et d'optimisation stochastique peuvent être de nouveau des outils précieux en vue d'extraire et d'exploiter des informations utiles à partir des simulations de Monte-Carlo.

5. CONCLUSION ET RECOMMANDATIONS

Bien que les méthodes probabilistes se soient longtemps développées dans le domaine de l'évaluation de la fiabilité des réseaux, elles étaient utilisées presqu'exclusivement dans les évaluations de l'adéquation par les planificateurs de réseaux. Le centre d'intérêt fondamental dans l'exploitation d'un réseau est l'autre aspect de la fiabilité, la sécurité, qui est à présent presque toujours évaluée au moyen de méthodes employant des critères

TF 38.03.12

REFERENCES

Anderson, P.M., and Bose, A., "A Probabilistic Approach to Power System Stability Analysis", *IEEE Trans. on Power Apparatus and Systems,* Vol. 102, No. 8, pp. 2430-2439, 1983.

Alvarado, F., Hu, Y., Ray, D., Stevenson, R., and Cashman, E. "Engineering Foundations for the Determination of Security Costs", *IEEE Trans. on Power Sys.,* Vol. 6, No. 3, pp. 1175-1182, 1991.

Balu, N., Bertram, T., Bose, A., Brandwajn, V., Cauley, G., Curtice, D., Fouad, A., Fink, L., Lauby, M.G., Wollenberg, B.F., Wrubel, J.N., "On-Line Power System Security Analysis", *Proceedings of the IEEE,* Vol 80, No. 2, February 1992, pp. 280.

Billinton, R., and Kuruganty, P.R.S., "A Probabilistic Index for Transient Stability", *IEEE Trans. on Power App. and Systems,* Vol. 99, No. 1, pp. 195-206, 1980.

Dodu, J.C., Merlin, A., "New Probabilistic Approach Taking Into Account Reliability and Operating Security in EHV Power System Planning at EDF", *IEEE Trans. on Power Systems,* Vol. 1, No. 3, pp. 175-181, 1986.

Dy Liacco, T.E., "The Adaptive Reliability Control System", *IEEE Trans. on Power App. and Systems,* Vol. PAS-86, No 5, pp. 517-531, May 1967.

Dy Liacco, T.E., *Control of Power Systems via the Multi-Level Concept,* Case Western Reserve University, Systems Research Center, Report SRC-68-19, June 1968.

Dy Liacco, T.E., "Real-Time Computer Control of Power Systems", *Proceedings of the IEEE,* Vol. 62, pp. 884-891, July 1974.

Dy Liacco, T.E., "System Security: The Computer's Role", *IEEE Spectrum,* Vol. 15, pp. 43-50, June 1978.

EPRI Report EL1773, *Reliability Indices for Power Systems,* March 1981.

Fink, L.H. and Carlsen, K., "Operating Under Stress and Strain", *IEEE Spectrum,* Vol. 15, pp. 48-53, Mar. 1978.

Fouad, A.A. (Chairman), "Dynamic Security Assessment Practices in North America", Report by IEEE Working Group on Dynamic Security Assessment, Power Systems Engineering Committee, *IEEE Trans. on Power Systems,* Vol. 3, No. 3, Aug. 1988, pp. 1310-1321.

Galiana, F.D., McGillis, D., Marin, M., "Expert Systems in Transmission Planning", *Proceedings of the IEEE,* Vol. 80, No. 5, May 1992.

Haubrich, H.-J., Nick, W.R., "Adequacy and Security of Power Systems at Planning Stage / *Adéquation et sécurité des réseaux électriques au stade de la planification* ", *Electra,* No. 149, August 1993.

Hatziargyriou, N.D., Karakatsanis, T.S., "Probabilistic Load Flow For Assessment of Voltage Stability", accepted for publication in *IEE Proc. on Generation, Transmission and Distribution.*

IEEE Working Group Report, "Reliability Indices for Use in Bulk Power System Supply Adequacy Evaluation", *IEEE Trans. on Power App. and Systems,* Vol. 97, No. 4, July-Aug. 1978, pp. 1097-1103.

Irizarry-Rivera, A.A., McCalley, J.D., and Vittal, V., "A Theoretical Foundation for Computing Probability of Instability in Electric Power Systems", submitted for publication, 1995.

Jacquemart, Y., Wehenkel, L., Van Cutsem, T., and Pruvot, P., "Statistical Approaches to Dynamic Security Assessment: The Data Base Generation Problem", *Proc. of SIPOWER'95, 2nd IFAC Symp. on Control of Power Plants and Power Systems,* pp. 243-246, Dec. 1995.

Laurin, D., Naggar, R., "Analyse de la sécurité du réseau de transport — Optimisation du choix de critère de comportement du réseau", Association canadienne de l'électricité, mars, 1985.

Leite da Silva, A.M., Endrenyi, J., Wang, L., "Integrated Treatment of Adequacy and Security in Bulk Power System Reliability Evaluations", *IEEE Trans. on Power Systems,* Vol. 8, No. 1, pp. 275-285, Feb. 1993.

McCalley, J.D., Fouad, A.A., Vittal, V., Irizarry-Rivera, A.A., Agrawal, B.L., and Farmer, R.G., "A Risk-Based Security Index for Determining Operating Limits in Stability Limited Electric Power Systems", submitted for publication, 1995.

Marceau, R.J., *Mechanizing Dynamic Security Analysis,* (Ph.D. thesis) Department of Electrical Engineering, McGill University, 1993.

McGillis, D., (Chairman) et al., *Power System Reliability Analysis Application Guide,* Report by CIGRE WG 03 of SC 38, Technical Brochure No 26, 1987, CIGRE, Paris.

McGillis, D., Galiana, F.D., Loud, L., Marceau, R.J., "The Influence of the Choice of Criteria on System Design", *9th Conference on the Electric Power Supply Industry (CEPSI),* Hong Kong, Nov. 23-27, 1992.

Meyer, B., (Chairman) et al., New Trends and Requirements for Dynamic Security Assessment / *Nouvelles tendances et nouveaux besoins en analyse de sécurité dynamique* — Report by CIGRE TF 02.13 of SC 38, 1997, Electra No 175, CIGRE, Paris.

Naggar, R., *Identification d'un critère de conception plus rentable que le critère actuel pour le réseau La Grande de l'an 2000,* rapport interne, Hydro-Québec, Planification des équipements. fév. 1986.

Naggar, R., Laurin, D., McGillis, D., "Transmission System Security Analysis for the Choice of Deterministic Design Criteria", Sixth Conf. on the Elec. Power Supply Ind. (CEPSI), Jakarta, 1986.

Schweppe, F.C., "Power systems '2000': Hierarchical Control Strategies", *IEEE Spectrum.* Vol. 15, No 7, pp. 42-47, 1978.

Tinguely, C., *Système-expert pour l'analyse de sécurité d'un réseau de transport d'énergie électrique,* (Ph.D. thesis, No. 1089), Ecole Polytechnique fédérale de Lausanne, 1992.

Vieira Filho, B.X., Pereira, M.V.F., Gomes, P., and Nery, E., "A Probabilistic Approach to Determine the Proximity of the Voltage Collapse Region / *Une approche probabiliste pour la détermination de l'effet de proximité d'une région d'effondrement de tension*", CIGRE, paper 38-201, 1994.

Wehenkel, L., "Contingency Severity Assessment for Voltage Security Using Non-Parametric Regression Techniques", *IEEE Trans. on Power Syst.,* Vol. PWRS-11, No. 1, pp. 101-111, Feb. 1996. Paper # 95 WM 162-8 PWRS, with discussions.

Wehenkel, L., Lebrevelec, C., Trotignon, M.,Batut J., "A probabilistic approach to the design of power systems protection schemes against blackouts" To appear in Proc. of IFAC/CIGRE Symp. on Control of Power Systems and Power Plants. Beijing, Aug. 1997.

Wu, F.F., Tsai, Y.K., and Yu, Y.X. "Probabilistic Steady State and Dynamic Security Assessment", *IEEE Trans. on Power Systems,* Vol. 3, No. 1, pp. 1-9, 1988.