Un système expert pour la gestion en temps réel des alarmes dans un réseau électrique

Pierre Girouard

B. Eng., McGill University, 1986

Department of Electrical Engineering

McGill University, Montréal

A thesis submitted to the Faculty of Graduate Studies and Research

in partial fulfillment of the requirements for the degree of

Master's Degree in Electrical Engineering

November 1987

Système expert pour la gestion des alarmes dans un réseau électrique

Résumé

Cette thèse présente un système expert pour le traitement en temps réel des messages d'alarme reçus dans les centres de contrôle de réseaux électriques. Ce logiciel, appelé GESTAL, génère des diagnostics concis qui identifient les causes de perturbations dans le réseau ainsi que les systèmes d'alarme et de protection ayant opérés. Ce système expert est composé d'un modèle des systèmes d'alarme et de protection du réseau, ainsi que de plusieurs groupes de règles de priorité différente. Bref, en utilisant le modèle du réseau, certaines règles construisent progressivement des graphes représentant diverses relations entre les alarmes reçues. Ces graphes sont ensuite analysés par d'autres règles afin d'établir des diagnostics sur les perturbations encourues. Enfin, il faut noter que le système expert a été développé dans un environnement *Symbolics* avec les langages *Lisp* et *ART 3.0* [Inference, 1987].

Les chapitres un, deux, et trois présentent divers concepts rattachés aux systèmes experts, aux réseaux électriques, et aux logiciels de traitement d'alarmes respectivement, tandis que le chapitre quatre décrit les fonctions et l'architecture du système expert GESTAL.

Abstract

This thesis presents a Model-Based Expert System for the processing of alarm messages in power networks' control centers. This Alarm Processor, called GESTAL, generates concise diagnoses identifying the cause(s) of network disturbances and describing the operation of the protection and alarm systems which operate to isolate faulty components. Essentially, the Alarm Processor is an agenda driven Expert System which is composed of a model of the power network's alarm and protection systems as well as several groups of rules. In brief, based on the Network Model, some given rules dynamically build graph structures which represent various types of relations between alarms as they are received. These graph structures are then analysed by other rules in order to diagnose the disturbance(s). The Alarm Processor has been developed using the *ART 3.0* [Inference, 1987] programming language in a *Symbolics* Lisp-Machine environment.

Chapters 1, 2, and 3 present background material on expert systems, electric power networks, and alarm processing software respectively, whereas chapter 4 describes GESTAL's functional characteristics and design.

Remerciements

Je veux remercier mes superviseurs, professeur Vincent Hayward et professeur Renato De Mori, pour leurs conseils judicieux et leur appui moral au cours des deux dernières années. Je suis également très reconnaissant au personnel du G.R.A.T. et du C.E.R. Maisonneuve d'Hydro-Québec pour sa collaboration dans l'élaboration de ce projet, plus particulièrement, je veux remercier messieurs Réal Galipeau, Paul Chicoine, Rénald Fréchette, Robert Antaya, Rénald Dubé, et Roch Hébert pour leur dévotion. Monsieur Lee Iverson m'a aussi aidé à utiliser plus efficacement les ordinateurs *Symbolics*, je tiens à l'en remercier. Les discussions techniques avec mon collègue et ami Jean-Michel Arès m'ont grandement servi dans la conception du système présenté dans cette thèse. Enfin, la firme *CAE Electronics Ltd* et les fonds de recherche *FCAR* m'ont permis, par leur support financier, de faire ces deux années de recherche en intelligence artificielle.

Table des matières

Liste des figures

Introduction

Un réseau électrique de grande taille est normalement subdivisé en plusieurs sous-réseaux qui sont gérés par des centres de contrôle indépendants. Les opérateurs de chacun de ces centres de contrôle surveillent l'état des postes et des lignes de transport afin d'assurer que les contraintes de charge soient respectées et que le réseau opère de façon sûre et économique. Dans le but de seconder les opérateurs dans cette tâche, un système d'ordinateurs acquiert des mesures et produit des messages d'alarme qui avisent les opérateurs du changement d'état de certains équipements ou du dépassement de seuils critiques pour des paramètres donnés. Lors de perturbations importantes, ce système d'acquisition de données tend à générer un nombre d'alarmes considérable. Dans de telles situations, les opérateurs ne sont pas toujours en mesure d'assimiler l'information pertinente à une analyse correcte de la panne, et donc, d'effectuer les manœuvres nécessaires pour remettre le réseau dans un état satisfaisant, et ainsi éviter des perturbations additionnelles. Étant donné les conséquences graves qui peuvent découler de ce genre d'incident, plusieurs groupes de chercheurs tentent présentement de développer des prototypes de "logiciels intelligents" pouvant générer des diagnostics de perturbations en temps réel, afin d'appuyer les opérateurs dans leur tâche d'analyse.

Le système expert de gestion d'alarmes présenté dans cette thèse génère automatiquement et en temps réel des diagnostics de pannes concis qui permettent aux

opérateurs de focaliser rapidement sur l'information importante lors de perturbations dans le réseau. Pour ce faire, ce système expert utilise un modèle des systèmes d'alarme et de protection du réseau ainsi qu'une base de règles hybride. En utilisant ce modèle du réseau, certaines règles construisent progressivement des graphes représentant diverses relations entre les alarmes reçues. Ces graphes sont ensuite analysées par d'autres règles afin de générer des diagnostics. Cette technique de gestion des alarmes, par analyse de modèle, comporte de nombreux avantages par rapport à d'autres architectures de système expert pour le traitement d'alarmes, notamment au niveau de l'acquisition des connaissances, du temps de réponse, de la validation, et enfin, de la capacité d'expansion du système.

Chapitre 1 Les systèmes experts

1.1 Introduction aux systèmes experts

Les *systèmes experts* sont des programmes d'ordinateur conçus pour résoudre des problèmes dans un domaine bien spécifique. La somme des connaissances d'un ou de plusieurs experts dans le domaine en question constitue la base du système expert. L'individu chargé d'extraire l'expertise du ou des spécialistes et de la transférer dans le programme se dénomme l'*ingénieur cogniticien*. L'ensemble des techniques utilisées pour essayer de réaliser ces systèmes à la capacité de raisonnement proche de celle de l'expert font partie du vaste domaine qu'est l'*intelligence artificielle* (ia).

L'utilité majeure des systèmes experts est de disséminer et de préserver une expertise humaine quelquefois rarissime et dispendieuse. Selon la nature et la complexité du domaine d'expertise, le système expert peut être fondé sur le savoir d'un seul spécialiste ou sur les connaissances de plusieurs experts. À ce jour, les domaines d'application typiques à ce genre de logiciel se limitent généralement au diagnostic, à l'interprétation, à la conception, et à la planification. Cette section décrit brièvement les diverses propriétés et les composants des systèmes experts en les comparant à des programmes conventionnels et en illustrant leur utilisation possible dans le domaine de l'ingénierie.

1.1.1 Composants de base

Un système expert comporte deux types de savoir, des *connaissances déclaratives* et des *connaissances procédurales*. Les connaissances déclaratives comprennent les descriptions et relations décrivant l'état du problème en main ainsi que les connaissances factuelles de l'expert face à ce genre de problème. Les connaissances procédurales, elles, se composent des différentes règles et procédures représentant les stratégies utilisées par l'expert pour résoudre un problème dans son domaine. Les connaissances déclaratives et procédurales sont représentées par des symboles dans la *base de connaissances* du système expert. Un système expert traite l'information de sa base de connaissances par l'entremise d'un *moteur d'inférence*. Le moteur d'inférence est un mécanisme virtuel qui applique les connaissances procédurales aux connaissances déclaratives afin de produire de nouveaux faits, rudiments de la solution recherchée. La communication entre l'usager et le système expert se fait au moyen d'un *interface à l'utilisateur*, tandis que l'*interface de développement* permet à l'ingénieur cogniticien d'examiner et de modifier la base de connaissances. Il peut arriver que le moteur d'inférence et le logiciel de développement utilisent des programmes externes; dans de tels cas, un *interface à d'autres logiciels* est nécessaire. En somme, un système expert consiste normalement en cinq éléments importants, soit une base de connaissances, un moteur d'inférence, un interface à l'utilisateur, un interface de développement, et un interface à d'autres logiciels. Les diverses interactions entre ces composants de base sont illustrées dans la figure 1.1.

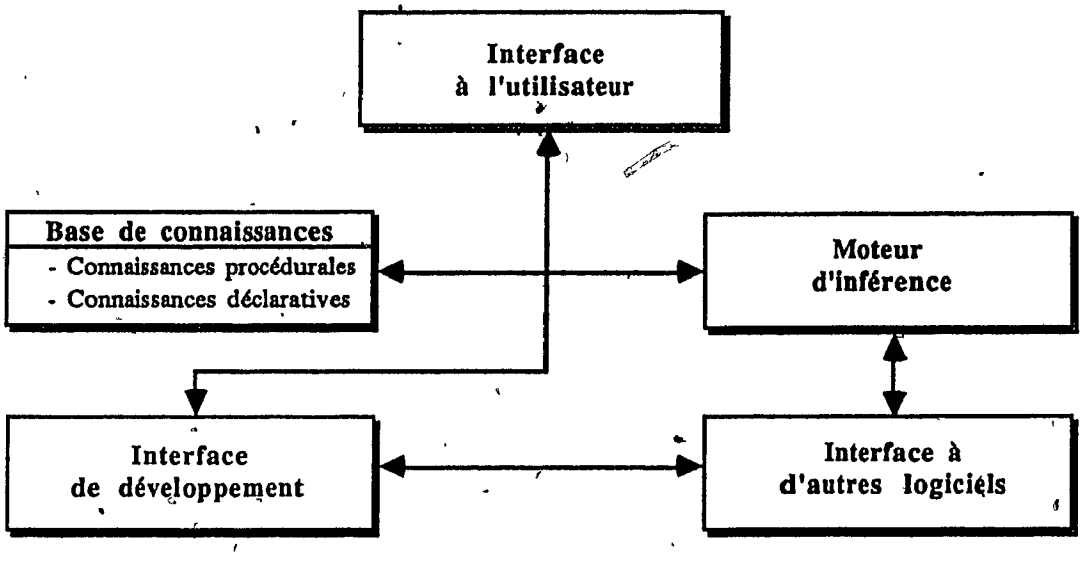


Figure 1.1 Composants de base d'un système expert

1.1.2 Systèmes experts et programmes conventionnels

Les techniques de programmation d'un système expert diffèrent grandement de celles normalement utilisées pour la programmation traditionnelle. Les distinctions les plus notoires se situent au niveau de la représentation des données et des connaissances, du contrôle des programmes, ainsi que des procédés de conception et d'implantation.

Le traitement de données conventionnel utilise normalement des algorithmes bien définis afin de compléter les tâches voulues. Ceci implique que les calculs ainsi que l'enchaînement des actions nécessaires à l'accomplissement des tâches en question sont préétablis. Bref, le problème a déjà été solutionné et le programme, qui consiste en *structures de données* et en *procédures*, n'est en fait qu'une version "codée" de l'algorithme. De plus,

puisque l'algorithme est encodé selon les conventions du langage de programmation et la dextérité du programmeur, ces programmes sont parfois difficiles à interpréter par d'autres personnes que le programmeur. Comme dernier point, il faut noter que le déroulement de ce type de programme s'effectue de façon séquentielle.

Les systèmes experts, eux, utilisent des méthodes *heuristiques* pour atteindre une solution; ils peuvent donc s'attaquer à des problèmes pour lesquels la définition d'un algorithme explicite est inconnue ou simplement inadéquate. La base de connaissances du système expert décrit, de façon symbolique, le domaine du problème sous forme de *descriptions*, *relations*, *règles*, et stratégies heuristiques. Puisque les connaissances sur le problème sont spécifiées explicitement, ces dernières peuvent donc être modifiées et assimilées par d'autres individus que l'ingénieur cogniticien. Aussi, l'ordre dans lequel le moteur d'inférence applique les règles à la base de connaissances déclaratives dépend entièrement du contenu de cette dernière, le déroulement du procédé ne suit donc aucune séquence préétablie. Puisque le système expert raisonne de façon similaire à un être humain, il lui est également possible de fournir des explications afin de justifier les conclusions atteintes, ceci représente un bénéfice majeur lors de l'analyse des solutions proposées par le système.

Étant donné la nature algorithmique des programmes conventionnels, leur conception se fait généralement de manière hiérarchique et la définition des structures de données et des algorithmes est clairement établie au début de leur implantation. Par contre, pendant le développement d'un système expert, les représentations choisies pour la base de connaissances peuvent changer à plusieurs reprises, soit tant que l'ingénieur cogniticien peut trouver de meilleures façons d'intégrer les connaissances des experts dans le domaine. Le développement d'un système expert nécessite donc plusieurs itérations des phases de conception, programmation, et raffinement.

1.1.3 Applications en ingénierie

De nos jours, on retrouve de plus en plus de systèmes experts dans les divers domaines de l'ingénierie. Par exemple, plusieurs des ces logiciels sont déjà utilisés pour des applications de *simulation*, de *diagnostic*, de *configuration*, et de *contrôle*. La rareté, le coût élevé, et enfin le caractère éphémère de l'expertise humaine expliquent l'affluence de systèmes experts dans ces domaines spécialisés. Les systèmes experts, en préservant et en accumulant l'expertise humaine dans une matière bien précise, permettent d'améliorer la productivité et les performances des experts aussi bien que des novices dans le domaine. La figure 1.2 illustre les principales fonctions dont un système expert peut s'acquitter avec succès.

Conception:	Guider l'usager vers la conception d'un système suivant des contraintes établies.
Contrôle:	Interpréter des signaux afin d'assurer le bon fonctionnement d'une opération.
Correction:	Rectifier les défaillances d'un système par des actions appropriées.
Diagnostic:	Déduire la cause d'une défaillance par l'analyse de données.
Interprétation:	Déterminer la signification de certaines mesures.
Organisation:	Ordonner des tâches dans le temps suivant des contraintes explicites.
Planification:	Générer un plan d'action afin d'atteindre un but préétabli.
Prédiction:	Déduire les conséquences possibles d'une situation donnée.

Figure 1.2 Utilisations des systèmes experts

Les systèmes experts constituent une nouvelle et puissante approche pour le développement de logiciels orientés vers la simulation et le diagnostic. Les techniques d'intelligence artificielle concernant la représentation des connaissances et les méthodes d'inférence permettent de modéliser un système donné et d'y intégrer les connaissances d'un

spécialiste afin de créer un logiciel qui puisse simuler ou analyser le comportement du système en question. Puisque les problèmes typiques d'ingénierie font souvent appel à un modèle, l'application de systèmes experts dans le domaine est très prometteuse. En fait, il existe déjà, avec la technologie actuelle, plusieurs applications de ce genre de système sur le marché. Un exemple est le système expert COMPASS [Goyal, 1985] pour l'entretien des multi-contacts dans les centrales téléphoniques. Ce système, développé par GTE, analyse les rapports d'entretien des multi-contacts et suggère les actions à prendre pour corriger les défauts.

La conception est une activité qui nécessite généralement des connaissances approfondies dans plusieurs domaines. Actuellement, les systèmes experts s'appliquent bien à des problèmes où les connaissances impliquées sont limitées et bien définies. Pour cela, l'utilisation de systèmes experts en conception est couramment restreinte à des sous-tâches où les connaissances requises sont claires et limitées. Par exemple, le système expert XCON est couramment utilisé pour configurer des systèmes d'ordinateur VAX-11/780. Ce n'est qu'après plusieurs essais infructueux en utilisant des méthodes de programmation conventionnelles que la firme DEC a finalement décidé de développer un système expert pour configurer ses systèmes 780. Ici, l'approche traditionnelle fut inefficace parce que les paramètres du problème changent rapidement, ce qui implique la nécessité d'effectuer des modifications majeures au progamme de configuration à chacun de ces changements. Par contre, le système expert programmé en OPS-5, langage de programmation basé sur des règles, est tout désigné pour ce genre de traitement.

Les techniques d'intelligence artificielle peuvent aussi se prêter à une multitude de problèmes du secteur industriel [Moore, 1984]. Dans ce secteur, les programmes conventionnels sont utilisés pour traiter des phénomènes à caractère continu tandis que les systèmes experts peuvent être utilisés pour gérer des changements discontinus tels que des

défaillances de système. Parmi les principales applications de systèmes experts en contrôle industriel, on retrouve entre autres l'interprétation de données provenant de sondes, le rétablissement de défaillances, et enfin l'optimisation des procédés de transformation suivant des contraintes économiques. Bien que les systèmes experts se comportent convenablement dans ce genre d'environnement, ils ne sont pas souvent laissés seuls pour gérer la production. En général, on les utilise conjointement avec un opérateur humain; dans un tel cas, le système expert simplifie grandement la tâche de l'opérateur en traitant rapidement les problèmes routiniers tandis que l'opérateur veille toujours pour résoudre les problèmes de nature exceptionnelle.

1.2 Concepts de base

Le développement d'un système expert est une tâche complexe qui ne se limite pas qu'à la définition de faits et de règles. L'ingénieur cogniticien, celui en charge du développement du système, doit sélectionner les techniques les plus appropriées pour représenter les connaissances déclaratives et procédurales. De bon choix peuvent souvent faire la différence entre un système médiocre et un logiciel de qualité commerciale. Cette section présente les principales stratégies qui s'offrent à l'ingénieur cogniticien pour représenter les connaissances d'un domaine d'expertise ainsi que les divers processus d'inférence disponibles.

1.2.1 Représentation des connaissances déclaratives

L'un des ojectifs fondamentaux de la conception d'un système expert est de construire la base de connaissances de façon à ce que le moteur d'inférence puisse la traiter efficacement et en plus, qu'elle soit facilement compréhensible pour ceux qui auront à la

consulter. Il n'existe pas de *paradigme* unique qui puisse représenter adéquatement n'importe quel genre de connaissance déclarative. Certains types connaissances déclaratives s'expriment plus facilement et plus efficacement suivant un paradigme donné tandis que d'autres pourraient être mieux représentés suivant une autre méthode. Les systèmes experts plus sophistiqués font donc souvent appel à plus d'un paradigme pour décrire leur base de connaissances déclaratives adéquatement, on parle alors de *représentation hybride* des connaissances. Les paragraphes qui suivent donnent un aperçu global des différentes techniques utilisées pour exprimer des connaissances déclaratives de façon factuelle.

Le *calcul prédicatif* [Manna, 1985] est un langage mathématique utilisé pour exprimer et manipuler des formules logiques. Par exemple, l'énoncé prédicatif "couleur (bloc-1 rouge)" signifie que l'élément appelé bloc-1 est de couleur rouge; ici, "couleur" est le *prédicat* tandis que "bloc-1" et "rouge" sont des *attributs*. Ce type de formule prédicative, où tous les termes sont des constantes, exemplifie la *logique propositionnelle*. Par contre, si seulement le prédicat est constant et que les attributs peuvent varier, on parle alors de *logique de premier ordre*. Finalement, en *logique modale*, tous les termes de l'énoncé peuvent être des variables. Puisque ce genre de formule permet d'exprimer diverses relations entre plusieurs entités, il est possible, en utilisant cette notation, de remanier une phrase de la langue française et de la représenter de façon formelle pour l'ordinateur. Parmi les limitations de ce type de représentation, on note qu'il est assez difficile de représenter des structures complexes comme des *taxinomies*; en plus, plusieurs opérations du calcul prédicatif se limitent à la logique de premier ordre et ne s'appliquent donc pas à la logique modale.

Un *réseau sémantique* [Quillian, 1968] peut être conceptualisé comme un graphe directionnel où chaque nœud correspond à un concept, un objet, ou un évènement et où chaque flèche exprime une relation. Bien que la même information puisse être représentée en utilisant

des techniques de calcul prédicatif, l'aspect visuel des réseaux sémantiques permet souvent aux utilisateurs de mieux interpréter les relations et interactions entre les différents éléments de la base de connaissances déclaratives. La figure 1.3 illustre comment une phrase peut être représentée de façon formelle pour un ordinateur en utilisant un réseau sémantique.

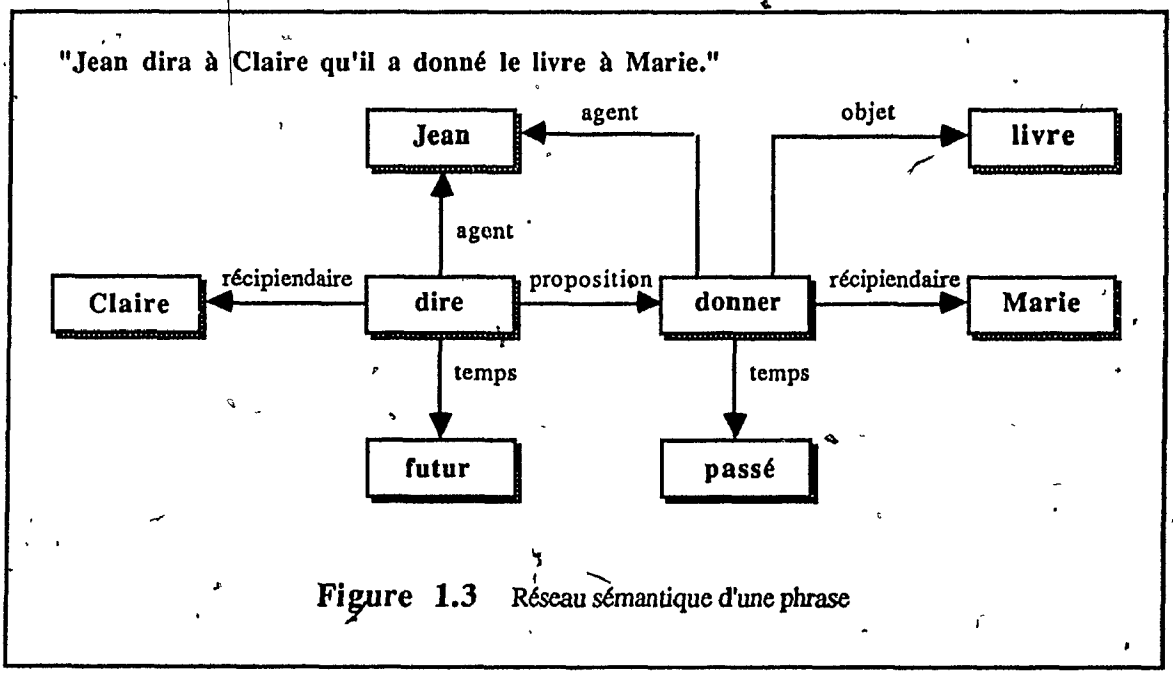


Figure 1.3 Réseau sémantique d'une phrase

La *représentation par schémas*, mieux connue sous les appellations anglaises "object-oriented representation" ou "frame-based representation" [Minsky, 1975], ressemble beaucoup aux réseaux sémantiques décrits auparavant. Cependant, dans la représentation par schémas, chaque nœud contient un ensemble d'attributs dans lesquels on peut inscrire des valeurs numériques, des symboles, ou encore des *attachements procéduraux*. Un attachement procédural ("demon" en anglais) est une fonction qui est appelée chaque fois que l'*inscription* ("slot" en anglais) est lue ou modifiée. Une autre caractéristique propre à la représentation par schémas est qu'on peut y définir des relations qui permettent à certains schémas d'hériter la valeur d'attributs de classes plus générales; en conséquence, ce type de représentation convient bien à la description de taxinomies complexes. La figure 1.4 donne un exemple de

représentation par schémas et illustre différents types de relations. Comme dernier point, il faut mentionner que ce genre de description convient moins bien à la représentation de faits disjoints, et de quantificateurs universels ou existentiels.

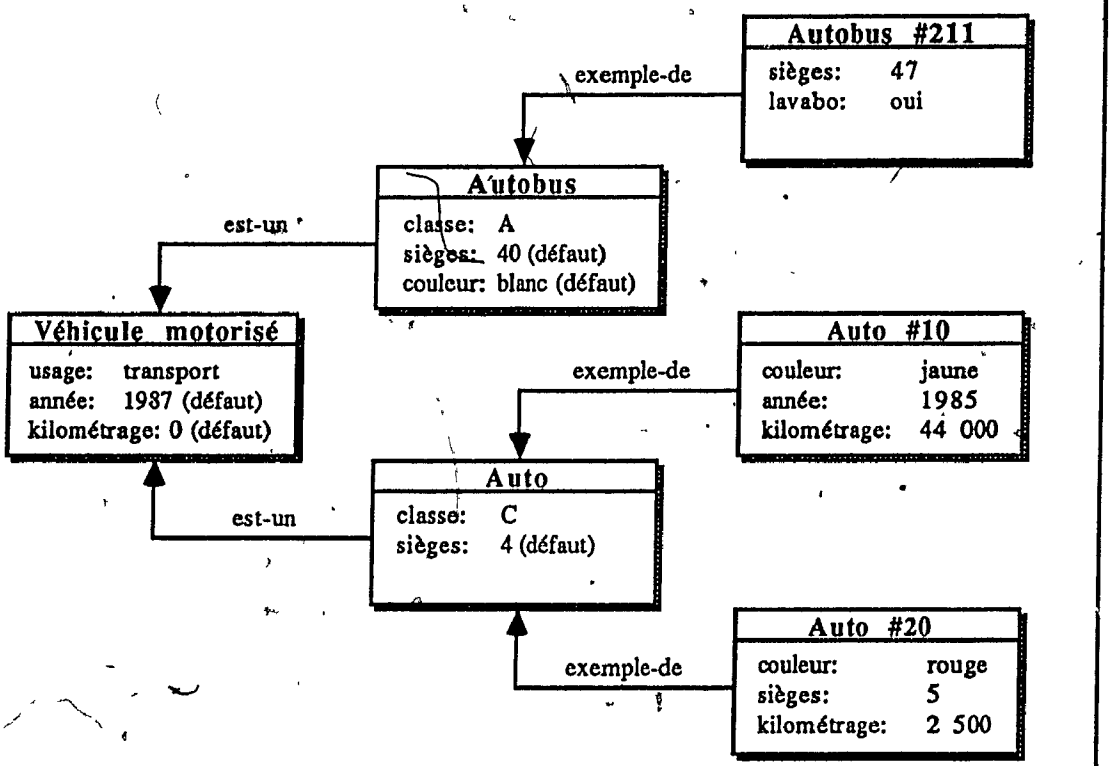


Figure 1.4 Représentation par schémas

1.2.2 Stratégies logiques

En plus de devoir spécifier quel type de représentation sera utilisé pour décrire les connaissances déclaratives, l'ingénieur cogniticien doit également déterminer avec quelle précision et par quelle stratégie logique ces connaissances seront traitées.

Un système expert peut "raisonner" suivant une *logique monotone* ou *non-monotone*. Dans un système monotone, la logique mathématique s'assure qu'aucune déduction ne contredise les *axiomes* de la base de faits. En d'autres termes, l'ajout de nouveaux faits à la base de connaissances déclaratives ne nécessite jamais la modification ou la rétraction d'axiomes afin de maintenir la cohérence logique de cette dernière. Par contre, dans un contexte non-monotone, des faits acceptables à un certain stade du raisonnement peuvent être invalidés lors d'une étape ultérieure. Bien qu'étant moins stricte au plan de la logique mathématique, ce genre de raisonnement offre cependant une flexibilité et une généralité accrues. Dans un système non-monotone, il est aussi souvent nécessaire d'utiliser un mécanisme quelconque pour maintenir la base de connaissances dans un état cohérent, ce processus de maintien de la vérité est mieux connu sous l'appellation anglaise de "Truth Maintenance System (T.M.S.)" [Doyle, 1979]. Lorsqu'un *système de maintien de la vérité* est utilisé, chaque déduction est habituellement associée à une *justification*, liste des règles et des leurs antécédents qui légitimisent la déduction en question. Si à un moment donné, une déduction en vient à ne plus être justifiée par au moins une règle, celle-là, ainsi que tous les faits qu'elle justifie, seront alors retirés de la base de connaissances dans le but d'assurer une cohérence logique.

L'ingénieur cogniticien doit également tenir compte du degré de précision avec lequel le modèle sera développé. Il peut utiliser trois types de modèles: soit *exact*, *probabiliste*, ou *flou*. Dans un univers exact, chaque fait déduit d'une règle est une assertion, une certitude. Dans un monde probabiliste, le degré de vraissemblance d'un fait est évalué selon un modèle de Bayes entre les antécedents et les conséquents de la règle qui justifie ce fait. Parce qu'il est souvent très difficile d'établir un modèle probabiliste de façon purement théorique, la plupart des systèmes experts de ce type doivent être calibrés empiriquement, ce qui rend le développement fastidieux et les résultats souvent incohérents. Enfin, une théorie complète sur

les modèles flous [Negoita,1985] existe, et permet d'exprimer qualitativement des concepts tels que des couleurs, des dimensions, etc. En résumé, les modèles exacts sont utilisés pour traiter des problèmes où les connaissances sont précises, tandis que les modèles probabilistes et flous offrent des techniques pour traiter des connaissances de nature imprécise.

1.2.3 Paradigmes de raisonnement

Ce sont des paradigmes de raisonnement basés sur des techniques de recherche heuristiques [Winston, 1984] qui permettent aux systèmes experts de résoudre des problèmes pour lesquels aucune solution explicite n'existe. Essentiellement, les connaissances déclaratives décrivrent le *domaine de recherche* tandis que les connaissances procédurales dirigent la recherche. Cette section décrit les paradigmes de raisonnement, ou techniques de recherche heuristiques, les plus utilisés dans la conception de systèmes experts. Il faut noter que plusieurs de ces méthodes peuvent être déployées dans un même système expert.

Les deux techniques d'inférence les plus fondamentales sont respectivement l'*enchaînement avant* et l'*enchaînement arrière*. En enchaînement avant, les règles sont appliquées à la base de connaissances déclaratives afin de produire de nouveaux faits, ces derniers peuvent à leur tour causer le *déclenchement* d'autres règles qui généreront de nouveaux faits, et ainsi de suite, jusqu'à ce que plus aucune règle ne s'*amorce*. À cause du grand nombre de faits que peut produire ce genre de technique, les systèmes qui l'utilisent sont aussi appelés *systèmes de production*. Lorsques plusieurs règles s'amorcent simultanément, le moteur d'inférence détermine l'ordre dans lequel elles seront appliquées grâce à un algorithme de *résolution de conflits*, ou en anglais, "conflict resolution". Plusieurs méthodes de résolution de conflits existent, l'assignation d'un grade, ou d'une *salience*, à chacune des règles en est une, tandis que l'utilisation de méta-règles pour résoudre les conflits en est une autre. Par

opposition à l'enchaînement avant qui consiste à générer des faits de façon à progresser vers la solution, en enchaînement arrière, la solution est considérée comme le but primordial et la recherche se fait à partir de ce but. En enchaînement arrière donc, les règles sont amorcées par des buts et génèrent des sous-buts qui à leur tour amorcent d'autres règles, et ainsi de suite, jusqu'à ce que tous les sous-buts puissent être directement déduits de la base de faits. Les deux techniques d'inférence décrites ci-dessus sont des processus de déduction diamétralement opposés, elles ont donc chacune des utilités bien différentes. L'enchaînement avant est très efficace pour des problèmes d'assemblage ou pour tout problème ayant un grand nombre de résultats possibles. Par contre, les systèmes de diagnostic utilisent souvent l'enchaînement arrière, étant donné le nombre plus limité de conclusions connues, ou de diagnostics, possibles. Vu leur nature complémentaire, il peut être parfois très avantageux d'utiliser ces deux méthodes d'enchaînement dans un même système expert.

La méthode de *solution-par-essais*, connue sous l'appellation anglaise "generate-and-test", constitue un moyen efficace pour résoudre des problème où le domaine de recherche est très grand. Cette configuration de système expert comprend deux composants majeurs: un *générateur* qui suggère des solutions possibles au problème, ainsi qu'un *vérificateur*, chargé de rejeter ou d'approuver les solutions suggérées selon les contraintes du problème en question. Afin de limiter le nombre de solutions proposées, il est important de munir le générateur d'un algorithme d'émondage ("pruning" en anglais). Cet algorithme a pour fonction d'*émonder* l'arbre des solutions générées de façon à ne considérer que les *branches* prometteuses, assurant ainsi de meilleures performances de la part du système expert.

Le raisonnement par *points de vue multiples*, ou "multiple viewpoints" en anglais, constitue un autre paradigme de raisonnement disponible dans le développement d'un système expert. Un point de vue se définit comme étant un ensemble de faits assumés

véridiques dans un contexte donné. Cette stratégie permet donc de développer parallèlement un nombre quelconque de solutions hypothétiques à un problème donné, elle peut d'ailleurs être utilisée à des fins de solution-par-essais. De plus, parce qu'il est possible de lier des points de vue un à la suite de l'autre, on se sert souvent de points de vue pour traiter des problème de raisonnement temporel, chaque point de vue représente alors une série de faits vraissemblables à un moment donné.

Enfin, la *programmation par objets*, ou "object-oriented programming", correspond au dernier paradigme de raisonnement présenté dans cette section. En programmation par objets, les entités de base du programme, les objets, communiquent entre elles en s'envoyant des messages. Les objets ne nécessitent aucune stratégie stricte de contrôle; cependant, il est souvent avantageux d'opter pour une représentation hiérarchique des objets, tel que la représentation par schémas. Dans un tel cas, les schémas permettent de représenter les propriétés descriptives, structurelles, taxinomiques, et comportementales de chaque objet de façon claire et explicite. En somme, le modèle est constitué d'un ensemble d'objets qui exécutent leurs propriétés comportementales et qui dialoguent entres eux par l'envoi de messages. Ces messages dictent quelles opérations doivent être effectuées sans pour autant spécifier comment. Lorsqu'un objet reçoit un message, il consulte ses faits ainsi que la base de règles afin de déterminer les actions à prendre. Les actions typiques consistent à envoyer des messages à l'utilistateur et/ou à d'autres objets. Compte tenu de la grande modularité de cette technique de programmation, ce genre de modèle est entre autres très utile pour simuler des procédés impliquant plusieurs traitements distincts et simultanés.

1.3 Développement d'un système expert

L'ingénieur cogniticien extrait les connaissances des experts du domaine et implante ce savoir dans la base de connaissances du système expert en faisant une sélection judicieuse des techniques décrites précédemment. Quatre étapes de développement interdépendantes et se chevauchant sont généralement impliquées dans l'intégration d'un système expert, et constituent donc les principales tâches de l'ingénieur cogniticien.

1. Sélection et spécification du problème
2. Acquisition et conceptualisation des connaissances
3. Implantation
4. Vérification et évaluation

Comparativement, les modèles traditionnels de génie du logiciel [Ramamoorthy, 1984] subdivisent normalement le développement d'un programme conventionnel en étapes distinctes et ordonnées. Les principales phases sont l'analyse des besoins, les spécifications, la conception, l'implantation, ainsi que la vérification et mise au point du logiciel. Cette section donne un aperçu des quatre étapes fondamentales dans le développement d'un système expert et les compare à la méthodologie normalement impliquée dans l'intégration de logiciels conventionnels.

1.3.1 Sélection et spécification du problème

Avant de procéder au développement d'un système expert, l'ingénieur doit s'assurer que le problème est de nature à être résolu efficacement par ce type de logiciel. Si le problème se prête bien à une approche de programmation par règles, il s'agit alors de définir clairement et minutieusement les caractéristiques fonctionnelles du système expert projeté. En génie du logiciel traditionnel, les phases d'analyse des besoins et de spécifications du logiciel

correspondent assez bien à cette étape de *sélection et spécification du problème* pour le développement d'un système expert.

La sélection d'un problème adéquat pour la technologie actuelle n'est pas une tâche aussi triviale qu'on peut l'imaginer; en fait, une mauvaise sélection de la part de l'ingénieur cogniticien entraîne normalement des problèmes insurmontables lors de la conception du système expert. Cette étape se veut donc une phase critique où l'ingénieur cogniticien doit se servir de son expérience et de son jugement afin de déterminer la faisabilité du projet. Quelques-unes des considérations typiques qui porteront normalement l'ingénieur à l'acceptation d'un projet, compte tenu de la technologie actuelle, sont énumérées ci-dessous.

- Le problème est soit trop complexe ou trop abstrait pour qu'une solution algorithmique soit considérée, et/ou le problème évolue avec son environnement.

- Le solution au problème ne nécessite des connaissances que dans un domaine d'expertise bien défini, et un spécialiste est en mesure de résoudre le problème en question.

- La tâche est bien définie et peut être remplie en n'utilisant que des connaissances techniques et très peu de "bon sens".

- Il existe au moins un expert en mesure de décrire la démarche à suivre afin de résoudre les problèmes du domaine.

Ces guides de sélection sont utiles pour évaluer rapidement la faisabilité d'un projet, mais ne tiennent cependant pas compte des contraintes particulières qui peuvent régir le domaine du problème. Par conséquent, le critère de sélection ultime pour des projets de grande envergure devrait toujours être la démonstration réussie d'un *prototype* du système expert solutionnant les aspects critiques du problème.

1.3.2 Acquisition et conceptualisation des connaissances

L'acquisition et la conceptualisation des connaissances sont deux tâches qui se chevauchent et qui constituent une étape majeure dans le développement d'un système expert.

L'acquisition des connaissances [Jonhson, 1983] est généralement reconnue comme étant le talon d'Achille du développement d'un système expert. En effet, plusieurs facteurs incontrôlables régissent le succès de cette étape, soit, entre autres, le talent de l'ingénieur cogniticien pour extraire l'information pertinente au domaine du problème, l'abilité de l'expert pour communiquer ses connaissances de façon intelligible, ainsi que leur disponibilité pour des interviews. Il est cependant quelquefois possible d'éviter ces problèmes en extrayant les connaissances de sources d'expertise autres qu'humaines, telles que de schémas synoptiques, de dissertations, de bases de données, et/ou de livres.

La conceptualisation des connaissances commence lorsque l'ingénieur cogniticien devient plus familier avec le domaine du problème. Ce dernier peut alors faire une esquisse de la base de connaissances et choisir les paradigmes de raisonnement qui satisfont le mieux au domaine du problème. La conception de la base de connaissances consiste premièrement à déterminer avec quel niveau de détail les connaissances doivent être représentées, et ensuite à spécifier les relations, descriptions, et taxinomies requises. De même, une version préliminaire de l'architecture du système expert [Hayes-Roth, 1983] peut être précisée en étudiant le type des connaissances impliquées, la complexité du domaine de recherche, ainsi que les techniques de recherche applicables. On utilise alors cette esquisse du système expert afin de choisir l'environnement de développement qui sera utilisé. Par exemple, certains problèmes se prêtent bien à l'utilisation de langages n'offrant qu'un seul paradigme de raisonnement. Tel est le cas pour les langages *OPS/83*, *Prolog*, et *Smalltalk* qui sont fondés sur des stratégies de

raisonnement uniques, soit sur de l'enchaînement avant, de l'enchaînement arrière, et de la programmation par objets respectivement. Par contre, d'autres problèmes plus complexes nécessitent quelquefois l'utilisation de *langages hybrides* tels que *ART*, *KEE*, ou *Knowledge Craft*. Ces langages hybrides offrent une combinaison des diverses techniques de représentation des connaissances et de recherche de solution, afin de fournir à l'ingénieur cogniticien un environnement de développement beaucoup plus flexible. Enfin, une fois l'environnement de développement choisi, les connaissances déclaratives et procédurales peuvent y être implantées suivant les contraintes de ce dernier.

Cette étape de développement correspond quelque peu à la phase de conception en génie du logiciel conventionnel. Cependant, en assumant que le domaine du problème soit bien établi au départ, les algorithmes et structures de données spécifiés lors de la conception de logiciels traditionnels sont rarement appelés à être modifiés ultérieurement; tandis qu'en ingénierie des connaissances, les modèles développés durant cette étape devront sûrement être raffinés, sinon redéfinis complètement lors d'étapes subséquentes.

1.3.3 Implantation

La phase d'implantation consiste à intégrer et à mettre au point un prototype du système expert. Le temps requis pour compléter cette étape dépend grandement de la complexité du problème ainsi que de l'environnement de développement utilisé.

Une approche de développement, où l'intégration et la mise au point du prototype se font de façon incrémentale, accélère considérablement le processus d'implantation. En termes plus pratiques, l'ingénieur cogniticien a avantage à classifier les règles selon leur fonctionnement et selon l'information qu'elles doivent accéder. Il est alors possible de tester le

comportement de chaque classe de règles et de corriger toute disparité entre la base de connaissances procédurales et la base de connaissances déclaratives. À ce stade, l'ingénieur cogniticien est en mesure de découvrir et de noter certaines inefficacités au niveau de la représentation et du traitement des connaissances. Une fois que les performances du système sont acceptables sur le plan fonctionnel, on peut alors corriger ces inefficacités afin de permettre des "raisonnements" plus rapide de la part du système expert. L'implantation d'un système expert est donc un processus itératif nécessitant plusieurs phases de conceptualisation, de programmation, de mise au point, et de raffinement des bases de connaissances et des stratégies de contrôle. Par conséquent, l'implantation d'un système expert diffère grandement de celle d'un logiciel conventionnel, où l'intégration des algorithmes et des structures de données est un procédé non-répétitif.

L'environnement de développement peut faciliter considérablement la tâche de l'ingénieur cogniticien en lui offrant des outils de mise au point, un éditeur de la base de connaissances, et des mécanismes de compilation partielle. Les outils de mise au point permettent généralement d'entrer dans un *mode pas-à-pas* ou dans un *mode de dépistage*, il est alors possible d'examiner l'*agenda*, file d'attente des règles amorcées et prêtes à être appliquées, et la base de connaissances pendant le déroulement d'une session. En général, un éditeur de base de connaissances permet d'examiner, de modifier, et de rétracter des faits à volonté; souvent, il est aussi possible de représenter graphiquement les différentes relations qui existent entre les différents éléments de la base de connaissances déclaratives. La majorité des langages hybrides présents sur le marché offrent des environnements de développement très sophistiqués.

1.3.4 Vérification et évaluation

L'étape de vérification et d'évaluation [Hayes-Roth, 1983] implique une analyse de la robustesse et de la précision du système expert en le soumettant à une variété de problèmes typiques. L'évaluation d'un système expert diffère considérablement de celle d'un programme déterministe. Par exemple, la technique de "branch-and-path-coverage" est utilisée pour tester les structures "if-then" dans un programme déterministe. Toutefois, puisque le comportement non-déterministe des systèmes experts varie selon le contenu de la base de connaissances, la quantité invraisemblable de scénarios possibles, en ce qui a trait au déclenchement des règles, rend tout type de vérification exhaustive quelque peu utopique. Par conséquent, la vérification d'un système expert se fait à partir d'une études de cas typiques. L'ingénieur cogniticien et l'expert ne vérifient pas que les conclusions du système face à ces cas, ils analysent aussi comment il y arrive. Ce procédé permet donc de déceler les erreurs de logique, les éléments manquants, les mauvais concepts, les exceptions, ainsi que les mécanismes de contrôle inadéquats. Grâce à ces informations, l'ingénieur cogniticien est en mesure de spécifier les changements requis en vue d'améliorer le comportement du système expert. Ce raffinement nécessite plusieurs itérations des processus de conceptualisation, d'implantation, et de vérification afin d'obtenir un prototype acceptable.

Une fois qu'il a obtenu un prototype satisfaisant, l'ingénieur cogniticien peut estimer avec précision les ressources impliquées dans le développement d'un système complet. Par exemple, il est en mesure d'évaluer le nombre de règles, la dimension de la base de connaissances, les performances, ainsi que le temps de développement du produit fini. À ce moment, la version finale du système expert, basée sur la base de connaissances et l'architecture du prototype, peut enfin être développée.

1.4 Sommaire

Au cours des âges, l'expertise humaine, par sa rareté, son coût, et sa volatilité a toujours été une ressource des plus convoitées. Malgré leur développement souvent laborieux, les systèmes experts offrent désormais la possibilité de disséminer et de préserver des connaissances accumulées dans des champs d'expertise spécifiques. Notamment, l'utilisation de ces nouvelles techniques de programmation heuristique dans les divers domaines de l'ingénierie présente un avenir très prometteur.

L'ingénieur cogniticien est chargé de sélectionner les techniques de représentation, les stratégies logiques, ainsi que les paradigmes de raisonnement les plus appropriés pour traiter les connaissances procédurales et déclaratives reliées au domaine du problème. Enfin, le développement d'un système expert de grande envergure ne devrait jamais débuter avant l'obtention d'un prototype solutionnant adéquatement les parties critiques du problème, processus qui nécessite normalement plusieurs phases de conceptualisation, d'intégration, et de vérification.

Chapitre 2 Les réseaux électriques

Le logiciel de gestion des alarmes présenté dans cette thèse ainsi que le simulateur des systèmes de protection introduit par Arès [Arès, 1987] sont tous deux basés sur les systèmes de protection du réseau électrique d'Hydro-Québec. Afin de bien présenter le domaine du problème et de pouvoir en traiter certains aspects plus en détail, ce chapitre comporte une introduction aux réseaux électriques, un sommaire des applications de systèmes experts qui y sont possibles, ainsi qu'une description des systèmes de protection implantés dans le réseau actuel d'Hydro-Québec.

2.1 Introduction aux réseaux électriques

Cette section se veut une introduction à la structure ainsi qu'à la gestion de réseaux électriques de manière à donner une meilleure perspective quant à l'intégration de systèmes experts dans des *systèmes de gestion de réseau.*

2.1.1 Structure des opérations

L'objet d'un système de gestion de réseau est de coordonner la production et le transport d'énergie de façon à répondre aux besoins de la clientèle tout en minimisant les coûts

d'opération. L'énergie provient d'un *méga-système électrique* qui consiste généralement en la combinaison de plusieurs sources de production telles que des centrales thermiques, hydro-électriques, et nucléaires avec de l'électricité achetée de réseaux avoisinants. L'énergie chemine via des lignes de transport jusqu'à des postes, où la tension est abaissée, puis distribuée à de multiples points de demande. Le contrôle de la production et du transport de l'énergie est habituellement centralisé en un centre de gestion. Les opérateurs de ce centre reçoivent des télémesures de points stratégiques du réseau, cette information leur permet de contrôler le réseau et de le maintenir dans un état de fonctionnement optimal.

Dans de grands réseaux électriques comme ceux d'Hydro-Québec ou d'Ontario-Hydro, la gestion du méga-système électrique est implantée selon une structure hiérarchique à trois niveaux, soit un *centre de conduite du réseau* (*C.C.R.*), des *centres d'exploitaion régionaux* (*C.E.R.*), et des *centres d'exploitation de distribution* (*C.E.D.*). Le centre de conduite du réseau est un centre de décision et non d'exécution; il voit à l'optimisation des ressources énergétiques et surveille les mouvements d'énergie et le comportement du réseau. Les seules fonctions d'exécution qui y sont effectuées consistent au réglage fréquence-puissance ainsi qu'au délestage de charges lors de situations d'urgence. Le centre de conduite du réseau effectue donc la conduite du réseau de transport (735 kv - 550 kv), ensemble des installations servant à relier entre eux les centres de productions et les postes mixtes ou de transport. Toutes les autres manœuvres sur le réseau sont déléguées aux régions. Les centres d'exploitation régionaux ont donc comme fonctions d'exécuter les instructions provenant du centre de conduite du réseau et de collaborer avec celui-ci pour résoudre les différents problèmes de gestion; de plus, chaque centre d'exploitation régional doit surveiller et contrôler les différentes installations qui composent sa région. C'est là que s'effectue la conduite du réseau de transport délégué (315 kv - 120 kv) et du réseau de répartition, ensemble des installations servant à relier les postes de transport aux réseaux de distribution.

Finalement, les centres d'exploitation de distribution voient à effectuer la conduite du réseau de distribution d'une région ou d'un secteur, le réseau de distribution étant défini comme l'ensemble des installations nécessaires pour livrer l'énergie aux clients à partir des postes de distribution.

En somme, on peut caractériser la structure des opérations d'un réseau électrique par un flux descendant de commandes et un flux ascendant d'informations. Cette structure hiérarchique fournit aux opérateurs de tous les niveaux assez d'informations pour qu'ils puissent gérer efficacement leur part du réseau.

2.1.2 Systèmes de gestion de réseau

Le centre de conduite du réseau et les centres d'exploitation sont équipés de systèmes de gestion de réseau. Ces systèmes d'ordinateurs distribués permettent aux opérateurs de surveiller, d'analyser, et de contrôler la production et le transport d'électricité dans le réseau. Une esquisse de la configuration et du fonctionnement de ces systèmes est présentée dans cette section.

De façon conceptuelle, un système de gestion de réseau est composé de quatre composants fondamentaux [Evans, 1987], soit d'une base de données, d'un système *S.C.A.D.A.* ("Supervisory Control And Data Acquisition"), d'un *système de contrôle de production*, et d'un *système d'analyse de réseau.* Ce modèle conceptuel d'un système de gestion de réseau est illustré par la figure 2.1.

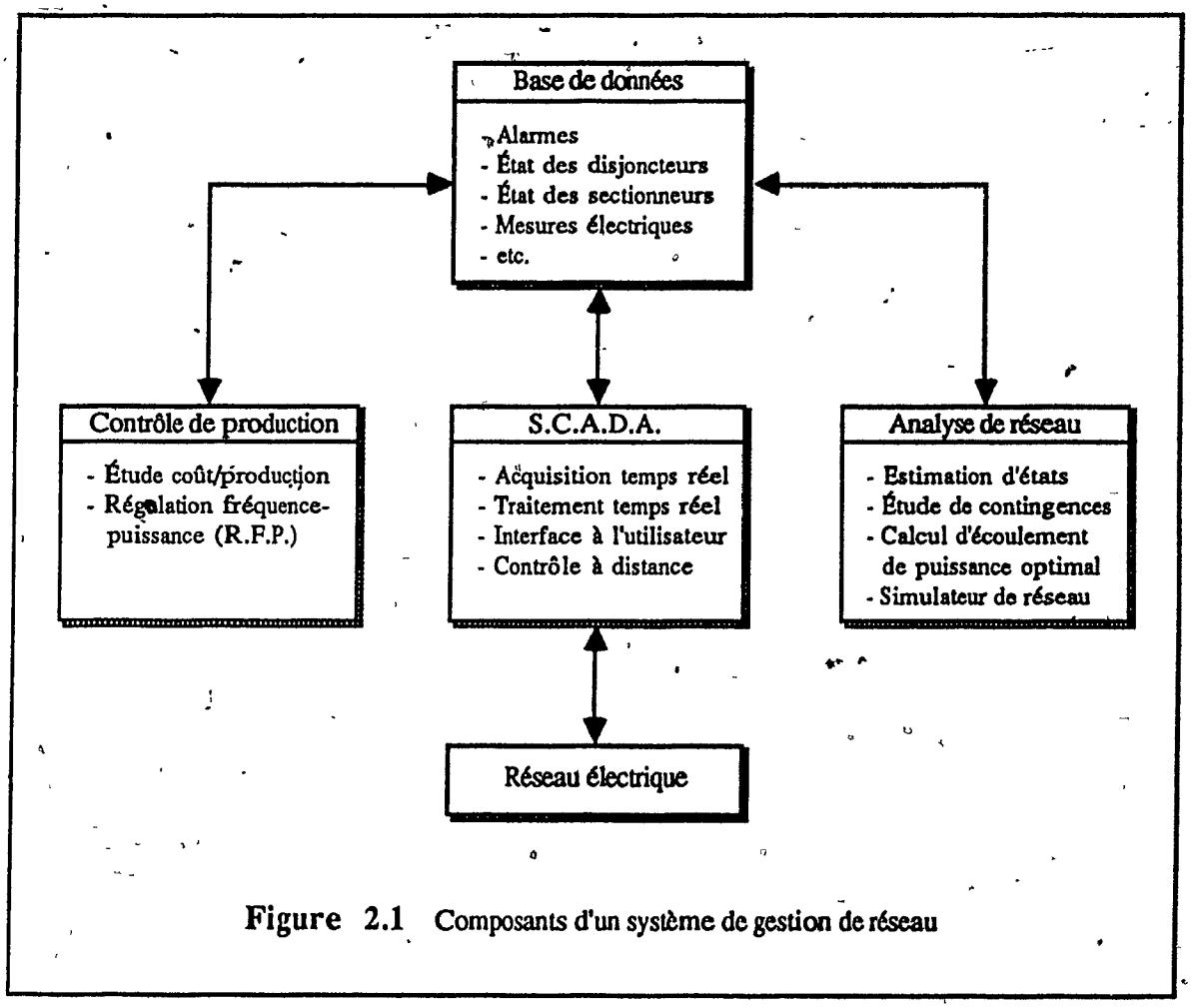


Figure 2.1 Composants d'un système de gestion de réseau

La base de données contient de l'information sur les alarmes des postes, l'état des disjoncteurs et sectionneurs, la position des prises des transformateurs, une variété de mesures électriques à travers le réseau, etc. La quantité considérable de données emmagasinées doit être accédée en temps réel par plusieurs programmes spécialisés. Les systèmes de gestion de réseau actuels doivent donc utiliser des *systèmes de gestion de bases de données* (S.G.B.D.) [Mooney,1987] très sophistiqués afin de satisfaire les contraintes encourues par l'utilisation de plusieurs programmes d'application avec une seule base de données.

Le système S.C.A.D.A. se compose de matériels et de logiciels qui font, en temps réel, l'acquisition et le traitement de données telles que des mesures ou états d'équipements. Les données extraites sont normalement acquises par des micro-ordinateurs appelés R.T.U. ("Remote Terminal Units") et acheminées jusqu'au système de gestion de réseau par l'entremise de modems. Le système S.C.A.D.A. permet aussi de télécontrôler des appareils éloignés. Finalement, ce système comprend un interface à l'utilisateur composé de plusieurs consoles, ces dernières affichent de l'information continuellement mise à jour, de façon à présenter l'état du réseau avec précision.

Le système de contrôle de production se charge des études coût/production et comprend aussi le système de *régulation fréquence-puissance* (*R.F.P.*). Les études coût/production déterminent la combinaison optimale de la quantité d'électricité produite versus la charge suivant des considérations économiques. Le système de régulation fréquence-puissance veille à la qualité de l'énergie produite, ce processus s'assure entre autres que la fréquence du réseau respecte les normes contractuelles établies et que les écoulements de ligne à des réseaux voisins se fassent tels que stipulés.

Enfin, le système d'analyse de réseau se compose d'un ensemble de programmes qui utilisent les paramètres d'opération du réseau à des fins d'*estimation d'état*, d'*études de contingences*, de *calcul d'écoulement de puissance optimal*, et de *simulation de réseau* pour entraîner les opérateurs. L'estimateur d'état permet aux opérateurs d'éviter des pannes coûteuses et de prévoir certains problèmes de transport d'électricité en lui fournissant des estimés de valeurs qui ne sont pas fournies par le système d'acquisition de données. Le logiciel d'étude de contingences est utilisé pour évaluer, par simulations, la robustesse du réseau face à certaines situations anormales, ces simulations permettent donc de déceler des faiblesses dans le réseau, et à long terme, d'assurer une plus grande stabilité de ce dernier. Les

calculs d'écoulement de puissance optimal visent à déterminer le *facteur de puissance* qui permet de minimiser les pertes de puissance réelle, tout en respectant les contraintes d'opération et de sécurité du réseau. En dernier lieu, le simulateur de réseau est un outil qui reproduit la majorité des caractériques des systèmes S.C.A.D.A., de contrôle de production, et d'analyse du réseau afin d'entraîner les opérateurs et de simuler des évènements hypothétiques.

2.1.3 États d'opération d'un réseau électrique

Le fonctionnement d'un réseau électrique est normalement régi par des *contraintes de charge* et des *contraintes d'opération*. Les contraintes de charge spécifient la demande en puissance du réseau tandis que les contraintes d'opération dictent les limitations physiques des appareils de façon à maintenir un certain facteur de sécurité dans le réseau. En fonction des contraintes respectées, le réseau électrique peut être considéré comme étant dans un *état normal*, un *état d'urgence*, ou un *état de restauration*. Lorsque les contraintes de charge et d'opération sont toutes deux respectées, le réseau est dans un état normal. Toutefois, une violation des contraintes d'opération, puisqu'elle peut engendrer des bris d'équipement et déstabiliser une partie du réseau, invoque un état d'urgence. Enfin, quand les contraintes de charge ne sont plus respectées, on parle généralement d'état de restauration.

2.1.4 Rôle des opérateurs

Les opérateurs du système de gestion de réseau doivent contrôler le réseau en considérant des facteurs de sécurité et de rentabilité. Leur responsabilité principale consiste à maintenir le réseau électrique dans un état normal. L'utilisation de certaines fonctions du système de gestion de réseau, telles que le système S.C.A.D.A. ainsi que les logiciels d'analyse de contingences et d'estimation d'état, devrait normalement leur fournir l'aide

nécessaire afin de respecter les contraintes de charge et d'opération en tout temps. En plus, les opérateurs doivent voir à l'optimisation de la production et du transport de l'électricité de façon à limiter les coûts d'opération, ceci est rendu possible par l'utilisation du logiciel d'étude de coût/production ainsi que du système de régulation fréquence-puissance inclus dans le système de gestion de réseau décrit précédemment. Finalement, les opérateurs sont aussi responsables d'assigner les tâches aux *opérateurs mobiles* afin que les manœuvres locales nécessaires soient effectuées promptement.

2.2 Applications de systèmes experts

Présentement, les opérateurs des systèmes de gestion de réseau électrique doivent estimer l'état d'appareillage à partir de très grandes quantités de données. Les manœuvres qu'ils effectuent sont basées sur l'analyse et l'interprétation de celles-ci. Cependant, vu la complexité et l'ampleur des réseaux actuels, l'opérateur peut facilement être englouti sous une avalanche de données. Dans ce contexte, l'utilisation de systèmes experts peut sans doute solutionner le problème de la surabondance d'informations présentées à l'opérateur en lui offrant des outils de diagnostic, d'analyse, et de planification de haut niveau. La référence [EPRI, 1986] présente une évaluation de la faisabilité et des bénéfices de diverses applications d'intelligence artificielle en gestion de réseaux électriques. De plus, quelques exemples de systèmes experts traitant des problèmes de gestion de données sont brièvement décrits ci-dessous.

1. **Traitement d'alarmes** [Wollenberg, 1985]: Une des fonctions des systèmes de télécommande d'un système de gestion de réseau est de présenter à l'opérateur des messages d'alarme indiquant des changements d'état ou des défauts

d'équipements. Or, lors de pannes non-triviales, l'opérateur peut recevoir un nombre considérable de messages, rendant l'analyse et l'interprétation correcte de ces dernières presqu'impossibles en temps réel. Un système expert de traitement d'alarmes permet de réduire le nombre de messages d'alarme affichés et de présenter des messages plus compréhensibles à l'opérateur.

2. **Diagnostic de fautes** [Talukdar, 1987]: Un système expert pour le diagnostic de fautes identifie clairement la ou les causes à l'origine d'une perturbation dans le réseau à partir des messages de changement d'état et d'alarme reçus à la console de l'opérateur.

3. **Sélection de contingences** [Sobajic, 1987]: L'analyse de contingences est un processus important dans le développement d'un réseau robuste. Le nombre de contingences possibles est cependant très grand et la durée de chacune de ces analyses est longue. Le système expert de sélection de contingences détermine les contingences critiques, réduisant ainsi le nombre d'analyses à effectuer.

4. **Système de restauration** [Sakaguchi, 1983]: Suite à une perte de charge, lorsque le réseau est en état de restauration, le système expert détermine rapidement les manœuvres à effectuer afin de ramener le réseau dans son état normal.

5. **Planification d'écoulement de puissance** [Fujiwara, 1986]: Du point de vue de la sécurité, de la stabilité, et de la rentabilité, il est important de bien planifier les écoulements de puissance dans un réseau électrique. Un plan d'écoulement de puissance acceptable s'obtient après plusieurs essais successifs

de plans différents. Ce procédé est laborieux puisque chaque essai comporte la confection et la vérification d'un nouveau plan.. Le système expert simplifie la planification en automatisant ce processus itératif.

6. **Contrôle de tension/puissance réelle** [Liu, 1985]: Le contrôle des composantes réelles et imaginaires de la tension et de la puissance s'effectue à l'aide d'échangeurs de prises sur les tranformateurs, de charges inductives, de bancs de condensateurs, etc. Ce contrôle est important puisqu'il assure que les seuils critiques d'équipement ne soient pas franchis. Ici, le système expert conseille l'opérateur dans ses décisions touchant le contrôle des différentes composantes de la puissance et de la tension.

2.3 Systèmes de protection dans un réseau électrique

Les systèmes de protection ont comme objectif de limiter ou d'éviter les bris d'équipement ou les pertes de charge résultant de défauts électriques tels que des court-circuits, des surcharges, des déphasages, etc. La philosophie de protection consiste à isoler le défaut le plus rapidement possible, et dans certains cas, à essayer par la suite de rétablir la charge. L'isolement des fautes se fait généralement par le déclenchement des disjoncteurs et/ou des sectionneurs adjacents à l'élément en panne. Cette section donne un aperçu des fonctions fondamentales d'un système de protection pour réseau électrique. La description présentée est sommaire, le lecteur est donc invité à consulter des ouvrages de référence spécialisés [Hydro-Québec, 1973] pour plus de détails.

2.3.1 Défauts, alarmes, et composants du réseau

Le transfert de l'énergie des centrales de production jusqu'aux multiples points de demande est un processus distributif mettant en cause plusieurs types de lignes et de postes. La figure 2.2 illustre l'appareillage normalement présent dans un poste.

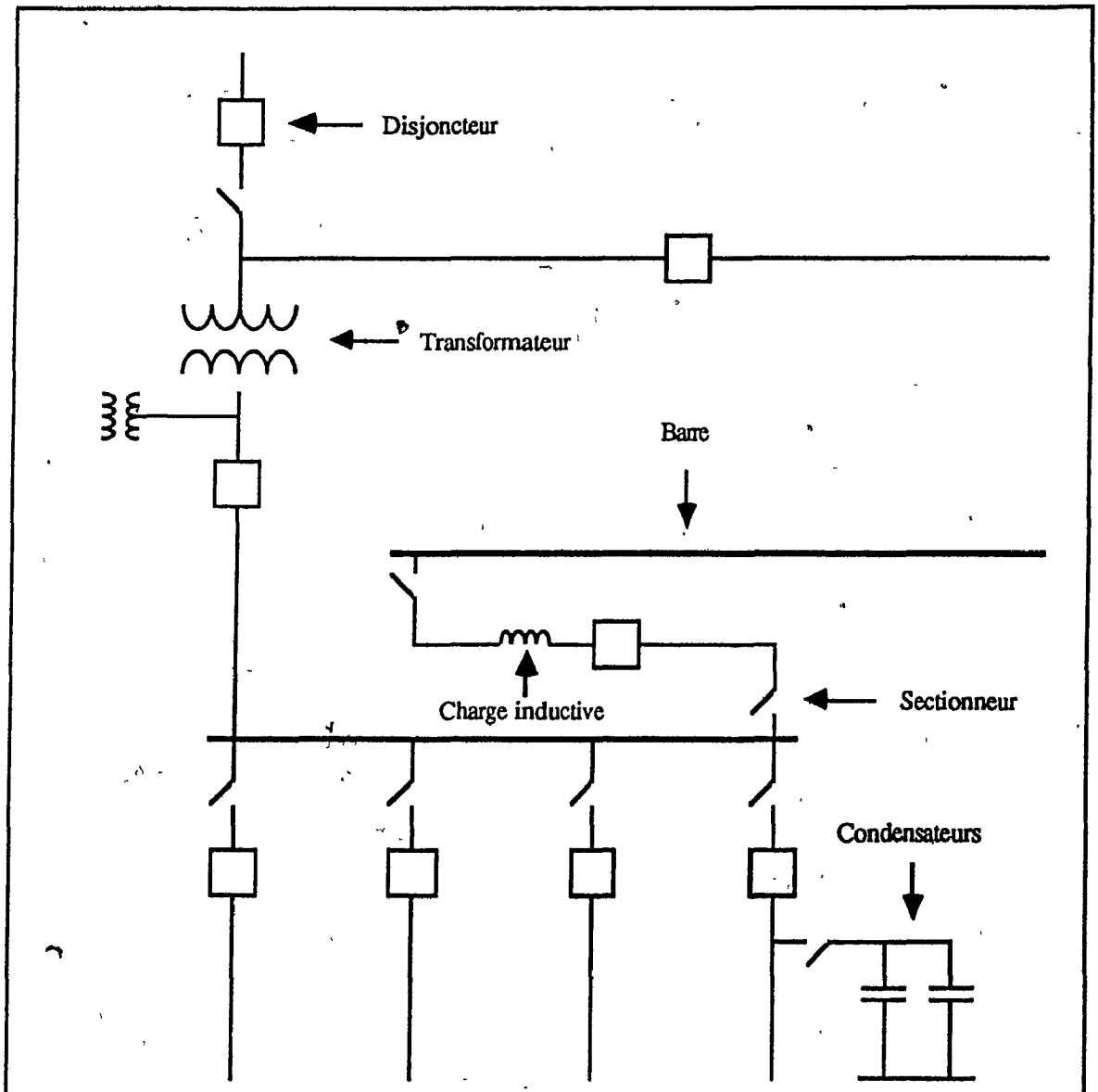


Figure 2.2 Composants de base d'un poste

Des changements d'état ou des conditions anormales sur des équipements de postes ou des lignes produisent des messages d'alarme qui sont immédiatement relayés aux postes impliqués ainsi qu'au centre d'exploitation régional. Ces messages d'alarme, tels que reçus au centre d'exploitation régional, informent l'opérateur sur la nature, la temporalité, et la provenance des défauts ou des changements d'état décelés dans le réseau. Les pannes typiques consistent en des défauts de gaz, d'échauffement, ou de différentiel sur un transformateur, en des problèmes de basse pression d'air ou de gaz sur un disjoncteur, et en des fautes de surtension ou de déphasage sur une ligne. Quant aux changements d'état, ils indiquent entre autres l'ouverture ou la fermeture de disjoncteurs et de sectionneurs, ainsi que des pertes de tension sur des lignes. Bref, l'opérateur d'un centre d'exploitation régional reçoit des sequences d'alarmes provenant de différents postes et pouvant indiquer soit la présence d'appareils défectueux ou ayant dépassés certains seuils d'opération, soit l'activation de systèmes de protection.

2.3.2 Protection principale et protection de secours

Les systèmes de protection dans le réseau sont conçus pour déceler la présence de défauts et isoler automatiquement les équipements menacés en ouvrant les disjoncteurs appropriés. La protection de l'appareillage est rendue possible grâce à l'utilisation de divers relais connectés suivant une logique bien précise. Lorsqu'un défaut important apparaît dans un poste, les relais en cause déclenchent et entraînent l'ouverture de disjoncteurs de façon à promptement isoler l'appareillage en faute.

De façon à limiter la portion du réseau qui doit être isolée lors de fautes, le réseau est subdivisé en zones de protection bornées par des disjoncteurs. Suite à un défaut, la zone affectée est isolée immediatement laissant le reste du réseau opérer normalement. Comme

l'illustre la figure 2.3, les zones de protection sont centrées autour des éléments fondamentaux du réseau, soit les centrales, les lignes, les transformateurs, et les barres. De plus, des zones adjacentes ont généralement un disjoncteur en commun.

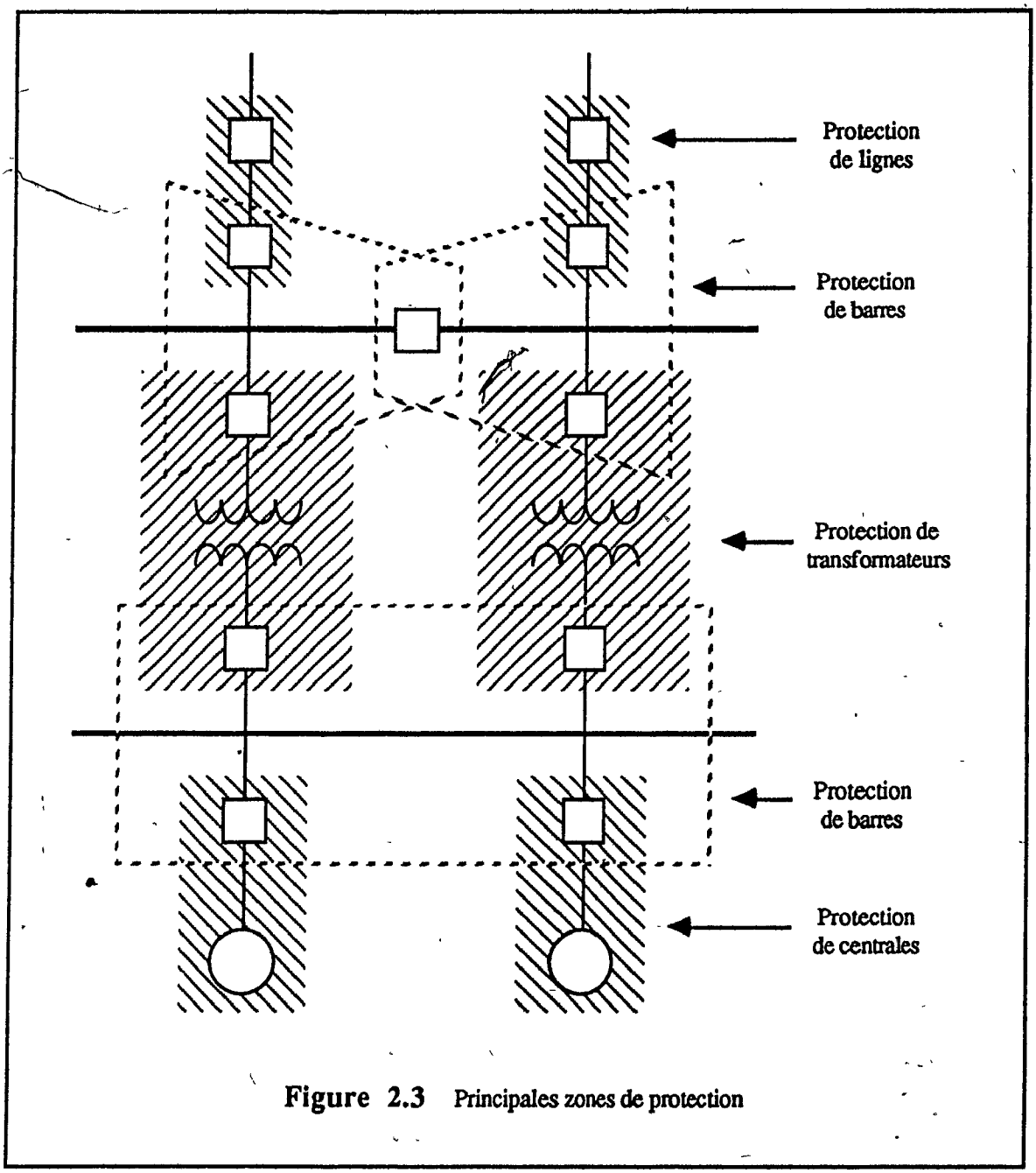
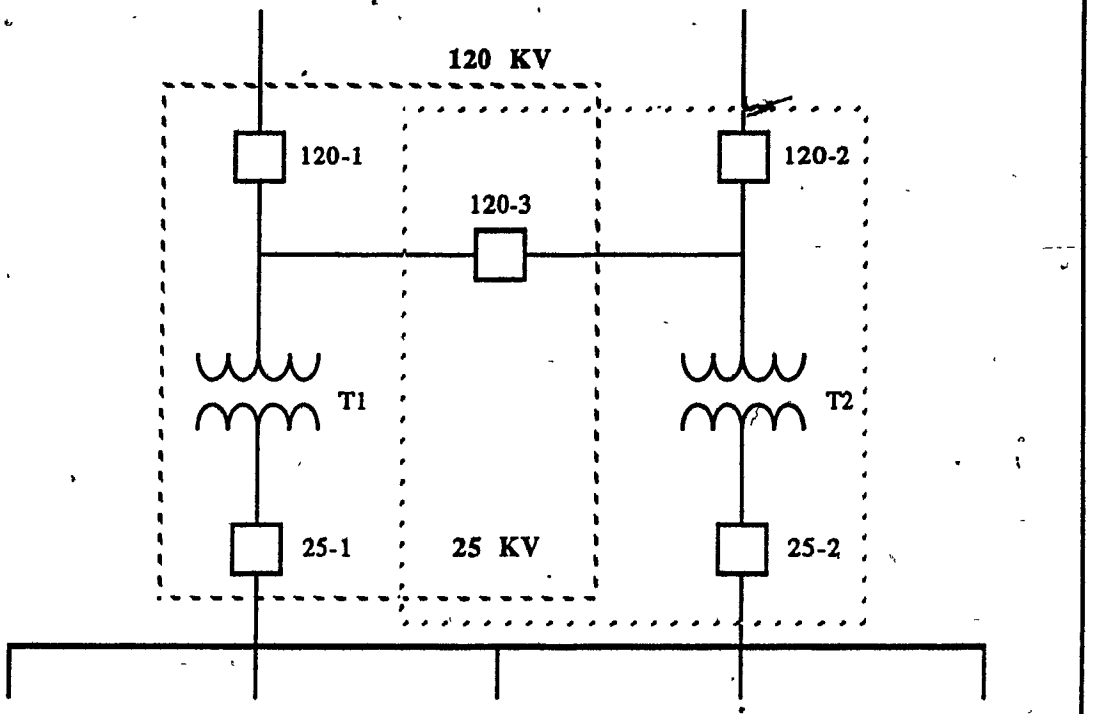


Figure 2.3 Principales zones de protection

La *protection principale* provoque le déclenchement de tous les disjoncteurs d'une zone lors de la détection d'une faute sérieuse à l'intérieur de cette région. Toutefois si, pour une raison ou une autre, il arrive qu'un ou plusieurs disjoncteurs ne puissent opérer correctement, laissant ainsi la faute sous tension, la *protection de secours* s'amorcera alors automatiquement. La protection de secours a pour but d'activer la protection principale de certaines des zones adjacentes à la zone en faute, soit les régions connectées à cette dernière via des disjoncteurs qui n'ont pas opéré normalement. Cette stratégie assure normalement l'isolement d'une faute dans des délais de l'ordre de douze à trente cycles d'un soixantième de seconde, soit un laps de temps inférieur à une demie seconde.

La figure 2.4 exemplifie ces mécanismes de protection à l'aide d'un poste fictif, et décrit la séquence typique des alarmes qui seraient reçues au centre d'exploitation régional dans une telle éventualité. Dans cet exemple, un défaut important sur l'élément T1 active la protection principale de ce dernier. Les disjoncteurs 120-1, 25-1, et 120-3 devraient alors s'ouvrir automatiquement, cependant, le disjoncteur 120-3 n'opère pas tel que prescrit et demeure fermé, laissant la faute sur le transformateur T1 sous tension. La protection de secours de l'appareil T1 active alors la protection principale de la zone adjacente, celle du tansformateur T2. Il en résulte le déclenchement des disjoncteurs 120-2 et 25-2, isolant ainsi les zones de T1 et de T2, et donc la faute originelle.



Liste d'alarmes	
T1 .... 94-1*	(Protection principale de T1)
D120-001TC	Ouverture non-autorisée
D025-001TC	Ouverture non-autorisée
T1 .... 94R*	(Protection de secours de T1)
T2 .... 94-1*	(Protection principale de T2)
D120-002TC	Ouverture non-autorisée
D025-002TC	Ouverture non-autorisée

Figure 2.4 Opération des protections principale et de secours

2.3.3 Protection de ligne

Les lignes de transport sont des éléments à haute tension qui relient différentes parties du réseau sur des distances quelquefois considérables. Lorsqu'un défaut survient sur

une ligne de transport, il doit être isolé le plus rapidement possible de sorte à éviter des dommages à l'appareillage ou une perte de stabilité dans le réseau. Pour ces raisons, la protection des lignes de transport comporte normalement un système de *téléprotection*, mécanisme qui assure un transmission instantanée d'informations d'une extrémité à l'autre de la ligne par l'entremise de ligne téléphonique, de faisceau hertzien, ou d'ondes porteuses sur la ligne même. Cette stratégie permet donc un déclenchement instantané des disjoncteurs à chacune des extrémités de la ligne même si le défaut n'est initialement perçu qu'à une seule de ces extrémités. La raison pour laquelle une faute peut être détectée à un bout avant l'autre réside dans la conception même des systèmes de protection. La détection de faute sur une ligne se fait à l'aide de relais d'impédance. Un de ces relais est placé à chaque extrémité de la ligne, et le temps de détection de la faute par chacun des relais dépend de la distance entre le défaut et chacun d'eux. Typiquement, trois temps de détection discrets sont possibles, selon si la faute se trouve dans le premier, le deuxième, ou le troisième *gradin* de protection.

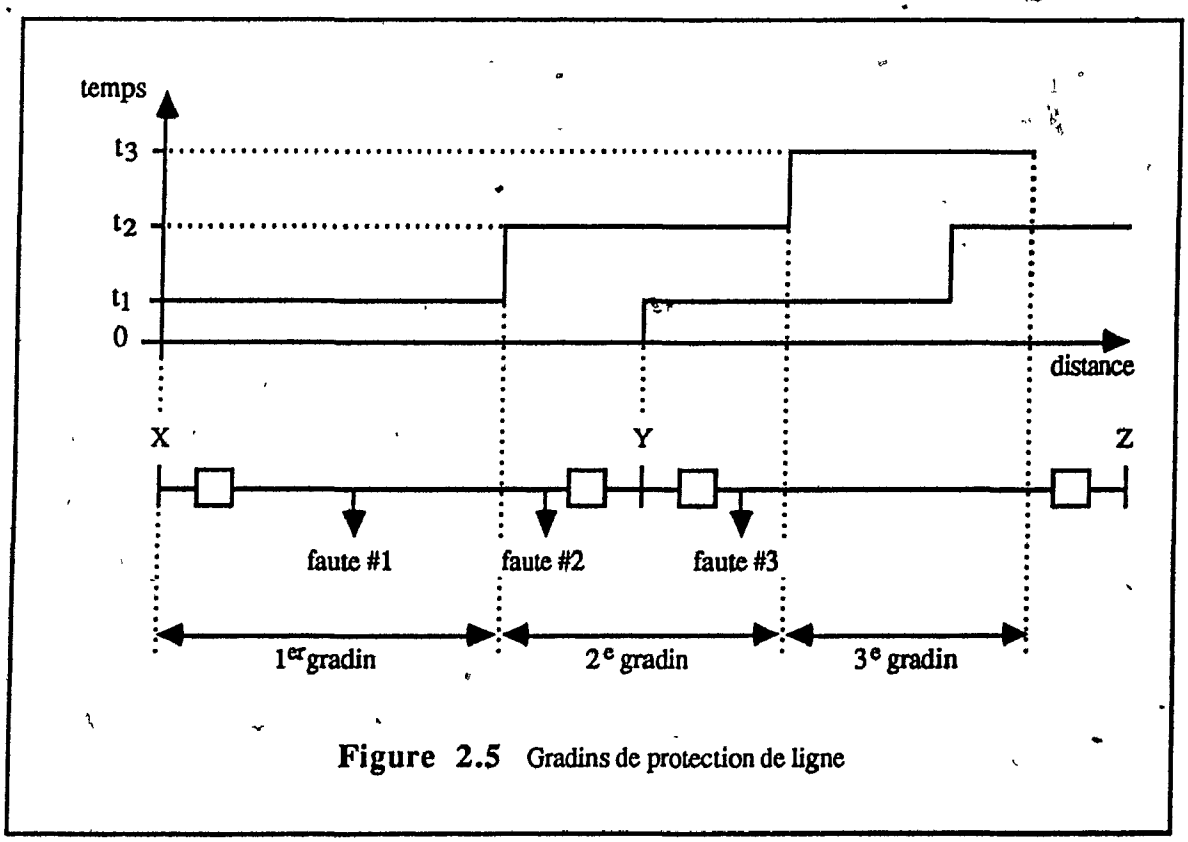


Figure 2.5 Gradins de protection de ligne

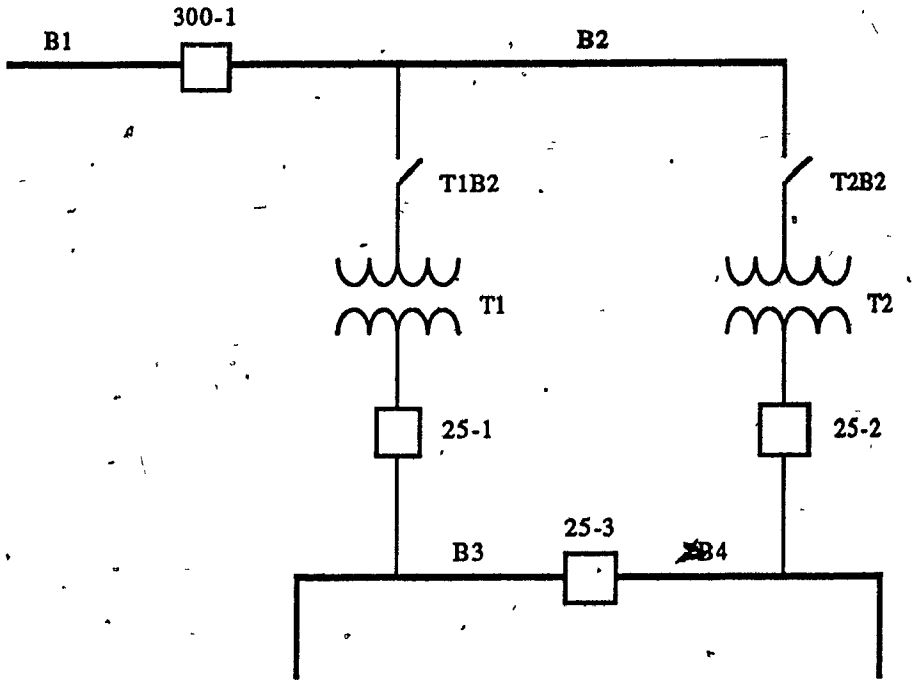
La figure 2.5 tente de clarifier le concept de gradin à l'aide d'un exemple simplifié de protection de ligne. Les points X, Y, et Z représentent des postes reliés entre eux par les lignes XY et YZ. Contrairement à la réalité, où des relais d'impédance sont placés à chaque extrémité d'une ligne, dans cet exemple simplifié, un seul relais d'impédance contrôle chacune des lignes. Un de ces relais est situé à la sortie du poste X et un autre à la sortie du poste Y. Tel qu'illustré, le premier gradin du relais d'impédance X couvre environ 80% de la ligne XY, le deuxième entre 80% et 120%, et le troisième jusqu'à 150% approximativement. La ligne YZ est surveillée de façon similaire par le relais à la sortie du poste Y. Le temps de détection pour chacun des trois gradins est indiqué par t_1,t_2,et t_3 respectivement. Par conséquent, suite aux fautes #1 ou #2 illustrées sur le diagramme, la ligne XY serait isolée en un temps t_1 ou t_2 respectivement. Cependant, la faute #3 peut être décelée ou par le deuxième gradin de la protection de ligne XY, ou par le premier gradin de la protection de ligne YZ; puisque le premier gradin opère plus rapidement qu'un deuxième gradin, la faute sera donc detectée en un temps t_1 par la protection de YZ. Il est important de noter que suite à la détection d'un défaut sur un ligne, les mécanismes de *télédéclenchement* assurent l'ouverture des disjoncteurs à chaque extrémité de cette ligne.

2.3.4 Rétablisseur de service

Afin d'augmenter la stabilité du réseau et de réduire les interruptions au service à la clientèle, plusieurs postes sont munis de *rétablisseurs de service*. Essentiellement, le rôle d'un rétablisseur de service consiste à ré-alimenter des zones importantes du réseau qui ont dû être isolées momentanément afin de déconnecter des appareils ayant subis un défaut.

Le transformateur constitue l'équipement fondamental des postes de distribution. Lorsqu'un transformateur doit être isolé à cause d'une faute quelconque sur celui-ci, il est important de pouvoir approvisionner quand même les appareils en aval. C'est pourquoi la majorité des installations utilisent des transformateurs jumelés en pair, de façon à pouvoir fournir un approvisionnement même lorsqu'un des deux est déconnecté. Dans bien des cas cependant, ces deux transformateurs, connectés en paralèlle sur une même barre, définissent une seule et unique zone de protection. Ainsi, lors d'une faute sur un des tranformateurs, la protection principale, qui a pour fonction d'isoler la zone, se trouve à isoler les deux transformateurs à l'aide de disjoncteurs. Le rétablisseur de service a pour but de déconnecter le transformateur en panne et de ré-alimenter la charge en aval par l'autre transformateur.

La figure 2.6 exemplifie le fonctionnement d'un rétablisseur de service en présentant la séquence typique des alarmes qui seraient générées suite à un défaut de gaz sur un transformateur T1 équipé de ce système. En premier lieu, la protection principale isole la zone en ouvrant automatiquement les disjoncteurs 300-1, 25-1, et 25-2. Ensuite, le rétablisseur de service fait ouvrir le sectionneur T1B2 qui n'est plus sous charge à ce moment-là. Enfin, les disjoncteurs 300-1 et 25-2 se referment afin de ré-alimenter les barres B3 et B4 via le transformateur T2 exclusivement. Par la suite, le rétablisseur de service est verrouillé afin de ne pas risquer de remettre sous tension le transformateur défectueux (T1) lors d'évènements futurs. Il faut noter que toute défaillance d'équipement encourue lors de manœuvres effectuées par le rétablisseur de service a comme conséquences immédiates d'annuler toute manœuvre ultérieure et de verrouiller le rétablisseur de service.



Liste d'alarmes	
T1 ..... '63	(Défaut de gaz sur T1)
T1@.. 94-1*	(Protection principale de T1 et T2)
D300-001TC	Ouverture non-autorisée
D025-001TC	Ouverture non-autorisée
D025-002TC	Ouverture non-autorisée
T2B2 .... TC	Ouverture non-autorisée
D300-001TC	Fermeture non-autorisée
D025-001TC	Fermeture non-autorisée
T1@.. RS..3	(Rétablisseur de service verrouillé)

Figure 2.6 Opération d'un rétablisseur de service

2.4 Sommaire

La structure des opérations d'un réseau électrique se caractérise par un flux descendant de commandes et un flux ascendant d'informations. Cette structure hiérarchique, constituée d'un centre de conduite du réseau, de centres d'exploitation régionaux, et de centres d'exploitation de distribution, fournit aux opérateurs de tous les niveaux assez d'informations pour qu'ils puissent gérer leur part du réseau. Le système de gestion de réseau, composé d'une base de données, d'un système S.C.A.D.A., d'un système de contrôle de production, et d'un système d'analyse de réseau, peut parfois engloutir les opérateurs sous une avalanche de messages d'alarme, les rendant inaptes à interpréter correctement les informations reçues.

L'utilisation de systèmes experts peut sans doute solutionner le problème de la surabondance d'informations présentées à l'opérateur en lui offrant des outils de diagnostic, d'analyse, et de planification de haut niveau. Plusieurs prototypes de systèmes experts visant à résoudre ce problème ont déjà été développés.

Enfin, dans un réseau électrique, les systèmes de protection ont comme objectif de limiter ou d'éviter les bris d'équipement ou les pertes de charge. La philosophie de protection consiste à isoler le défaut le plus rapidement possible, et dans certains cas, à essayer par la suite de rétablir la charge.

Chapitre 3 Le traitement des alarmes

3.1 Description du problème

Lors de perturbations dans un réseau électrique, les opérateurs au centre de contrôle doivent analyser rapidement des séquences d'alarmes et de changements d'état en vue d'identifier les causes de la panne. Grâce à ces diagnostics, les opérateurs sont en mesure d'effectuer les manœuvres nécessaires pour remettre le réseau dans un état satisfaisant et ainsi éviter la propagation de fautes dans le réseau. Toutefois, au cours de pannes importantes, le système d'acquisition de données (S.C.A.D.A.) peut afficher plusieurs dizaines ou même des centaines de messages d'alarme aux consoles de l'opérateur du centre de contrôle. Par conséquent, ce dernier risque d'être tout simplement débordé et donc dans l'incapacité de gérer le réseau de manière optimale.

En général, seulement quelques-unes des alarmes d'une séquence sont d'importance majeure. Celles-ci, connues sous le nom d'*alarmes principales*, identifient la cause de la perturbation ainsi que les systèmes de protection qui ont isolé cette dernière. Les autres alarmes reçues ne sont pas essentielles puisqu'elles ne font qu'identifier les conséquences normales de l'opération des systèmes de protection. Ainsi, lors de perturbations, le problème majeur des opérateurs consiste à analyser une séquence d'alarmes afin d'en extraire les alarmes principales.

Dans le cas où le nombre de messages reçus est considérable, le problème d'analyse devient très complexe puisque les alarmes principales sont souvent éparpillées dans la séquence et que l'importance d'une alarme dépend généralement de la présence d'autres alarmes dans la séquence. Les délais encourus pendant que les opérateurs complètent une telle analyse peuvent être coûteux en termes de qualité de service puisque les pertes de charge ne sont pas remédiées immédiatement et que les perturbations risquent de se propager si certaines manœuvres ne sont pas effectuées dans les plus brefs délais. Les opérateurs ne peuvent cependant se permettre d'effectuer des manœuvres basées que sur une analyse superficielle des évènements puisque des manœuvres incorrectes risquent d'engendrer des bris d'équipement ou la propagation des perturbations dans le réseau. En somme, considérant la configuration actuelle des centres de contrôle de réseaux électriques et le nombre toujours grandissant de points d'alarme qui y sont raccordés, les opérateurs courent de plus en plus le risque de faire face à un surplus d'informations lors de perturbations de réseau.

3.1.1 Classification des alarmes

Les centres de contrôle de réseaux électriques comportent un système d'acquisition de données qui présente des messages d'alarme aux opérateurs lors de fautes. Les anomalies signalées peuvent indiquer soit des défauts affectant l'appareillage surveillé ou soit des problèmes dans le système de surveillance même. Plus spécifiquement, les alarmes sont classifiées en quatre catégories [Hébert, 1986]:

1. **Alarmes d'annonciateur et de dépassement de seuils:** Ces messages représentent les points d'acquisition dont la valeur consiste en un état normal ou anormal. Par exemple, une température trop élevée dans un transformateur ou une basse pression d'air dans un disjoncteur sont des anomalies qui produisent

des alarmes de cette catégorie. Ce sont les annonciateurs locaux et les fonctions de surveillance de seuils implantées dans la console de l'opérateur qui ont la responsabilité générer ces états.

2. **Alarmes de changement d'état non-autorisé:** Elles identifient des appareils qui changent d'état sans être en mode de télécommande. Par exemple, l'ouverture ou la fermeture d'un disjoncteur par le système de protection ainsi qu'une perte de tension sur une ligne sont des changements d'état qui génèrent des alarmes de cette catégorie. En général, de tels changements d'état peuvent être causés par un déclenchement d'appareil, une manœuvre locale, ou une manœuvre par automatisme local.

3. **Alarmes de refus de manœuvre:** Ces alarmes identifient des appareils télécommandés qui refusent d'opérer sur l'ordre de télécommandes.

4. **Alarmes de systèmes:** Ces messages sont générés par le système d'ordinateurs du centre de contrôle, ses périphériques, et les consoles, lors de défauts dans des systèmes qui ne correspondent pas à des points d'alarme spécifiques. Par exemple, un défaut de console, un défaut de lien de communication, et une permutation d'appareil sont tous des anomalies qui génèrent des alarmes de systèmes.

3.2 Systèmes de gestion des alarmes

Divers types de systèmes ont été développés pour aider à résoudre le problème de gestion des alarmes dans les centres de contrôle de réseaux électriques. ¸La complexité des solutions varie entre de simples algorithmes de classification d'alarmes jusqu'à des prototypes de "systèmes intelligents" qui analysent les évènements reçus afin de générer de l'information de haut niveau.

3.2.1 Hiérarchisation des alarmes

En général, les consoles des opérateurs sont gérées par un logiciel qui affiche les alarmes sur un écran cathodique de façon à clairement identifier leur importance. Par exemple, un code de couleurs est souvent utilisé afin de mieux percevoir les divers niveaux de priorité des alarmes. De plus, les alarmes peuvent être regroupées de façon à celles de "haute priorité" soient affichées d'abord sur l'écran cathodique, et que les autres, de priorité moindre, ne soient présentées à l'écran que si l'espace le permet. Ces logiciels classifient les alarmes reçues en utilisant une hiérarchie préétablie. Une lacune fondamentale de ces systèmes de classification est qu'ils ne tiennent pas compte du fait que l'importance d'une alarme dépend généralement du contexte dans lequel elle est reçue.

3.2.2 Suppression des alarmes

La suppression d'alarmes [EPRI, 1987] lors de conditions prédéterminées constitue une autre technique de gestion des alarmes. Par exemple, un logiciel peut être configuré de façon à supprimer les alarmes qui sont attendues suite à la réception de certaines combinaisons d'alarmes identifiant des perturbations spécifiques dans le réseau. D'autre part,

des alarmes spécifiques ou même des classes entières d'alarmes peuvent être supprimées temporairement lors de conditions spécifiques dans le réseau. Par exemple, lors d'orages électriques, certaines alarmes peuvent être inhibées automatiquement puisqu'elles ne signalent pas des anomalies véritables étant données les conditions environnementales observées.

3.2.3 Gestion par analyse

Cette approche au problème de gestion des alarmes consiste à utiliser un système expert pour analyser en temps réel les séquences d'alarmes reçues au centre de contrôle de réseau. Un tel système expert utilise des règles heuristiques représentant les connaissances d'experts en comportement de réseau afin d'établir des diagnostics suite à des perturbations et ainsi limiter la quantité d'informations présentées aux opérateurs.

La principale fonction d'un système de gestion d'alarmes par analyse consiste à générer des diagnostics concis expliquant la signification de séquences d'alarmes. Par exemple, lorsqu'une faute de barre se produit et que tous les disjoncteurs associés à cette barre déclenchent correctement, plusieurs alarmes sont reçues au centre de contrôle. Dans un tel cas, l'objectif d'un logiciel de gestion par analyse est de générer un message de la forme *"barre X isolée"*. Bref, des diagnostics de ce genre permettent aux opérateurs de localiser rapidement les appareils ou systèmes défectueux lors de perturbations dans le réseau.

La réduction du nombre de fausses alarmes est un autre problème fondamental qui peut être résolu à l'aide de systèmes de gestion par analyse. Pour ce faire, la base de connaissances du système expert doit inclure une représentation de "l'expertise" permettant aux opérateurs d'identifier de fausses alarmes. Puisque les opérateurs identifient de fausses alarmes en notant l'absence de certaines alarmes ou conditions reliées, cette expertise peut être

représentée en termes d'un modèle qui spécifie les relations causales entre les divers types d'évènements. Ainsi, un système expert peut aider à réduire le nombre de fausses alarmes dans un centre de contrôle.

En résumé, l'approche de gestion par analyse permettra éventuellement une gestion des alarmes beaucoup plus efficace. Toutefois, cette nouvelle technologie devra d'abord être éprouvée en développant des prototypes de systèmes qui pourront ensuite être déployés à l'échelle de réseaux entiers.

3.3 Intelligence artificielle et gestion des alarmes

Tel que décrit dans la section précédente, les techniques actuelles dans le domaine de l'intelligence artificielle permettent de développer des systèmes de gestion d'alarmes qui fournissent à l'opérateur une analyse continuelle de l'état du réseau. Ainsi, plutôt que de simplement réorganiser l'affichage des messages d'alarme aux consoles, ces systèmes extraient l'information critique de ces messages et la combinent à l'information contenue dans les bases de données du centre de contrôle afin de générer des diagnostics de haut-niveau semblables à ceux établis par les opérateurs mêmes.

Divers prototypes de systèmes experts ont été développés pour interpréter des séquences d'alarmes reçues aux centres de contrôle de réseau. Cette section décrit brièvement quatre de ces systèmes experts. Bien que le type d'information générée diffère pour chacun de ces systèmes, l'objectif de chacun d'entre eux est le même, soit d'aider l'opérateur à établir rapidement et avec précision des diagnostics de pannes à partir de séquences d'alarmes et/ou de changements d'état.

3.3.1 Diagnostic par reconnaissance

Ce genre de système expert [EPRI, 1986] compare les séquences d'alarmes reçues à des séquences d'alarmes pré-compilées afin de détermininer la ou les causes de la perturbation. Les séquences pré-compilées sont obtenues à partir de simulations, d'arbres logiques ou d'autres techniques d'analyse de perturbations, et par conséquent, chacune de ces séquences correspond à une faute ou à une combinaison de fautes dans le réseau. Les règles heuristiques évaluent en temps réel le degré de chevauchement entre la séquence reçue et les séquences pré-compilées afin d'établir la cause probable de la perturbation.

Il est important de noter que la précision et la qualité des diagnostics générés par ce genre de technique dépend fortement de la plénitude des séquences d'alarmes pré-compilées dans la base de connaissances. Par conséquent, ce genre de logiciel est généralement utilisé pour l'analyse de séquences d'alarmes produites par des systèmes pour lesquels il est possible de pré-compiler un nombre limité de séquences d'alarmes correspondant aux contingences majeures. Ainsi, dans le cas d'un réseau électrique contenant plusieurs dizaines de milliers de points d'alarme, vu le très grand nombre de séquences différentes pouvant être générées, l'implantation de tels systèmes constitue une tâche très complexe et par conséquent, une solution peu pratique au problème de la gestion des alarmes.

3.3.2 Diagnostic par hypothèses

Un système expert qui établit des diagnostics de fautes à partir d'hypothèses est présenté dans [Talukdar, 1987]. Lors de la réception d'une séquence d'évènements, ce système conçoit des hypothèses qui pourraient expliquer la ou les causes de cette séquence. Pour chacune de ces hypothèses, le système utilise un programme de simulation afin de

calculer la séquence d'alarmes résultante et celle-ci est comparée à la séquence reçue. Lorsque la séquence reçue correspond à une séquence générée à partir d'une hypothèse, le système est en mesure d'établir un diagnostic décrivant la cause de la perturbation. Ainsi, le noyau de ce système de diagnostic consiste en une méthode pour générer toutes les hypothèses plausibles pouvant expliquer une séquence d'alarmes spécifique. Par exemple, considérons le circuit simplifié de la figure 3.1 pour lequel une alarme indiquant le déclenchement du disjoncteur D1 a été reçue au centre de contrôle.

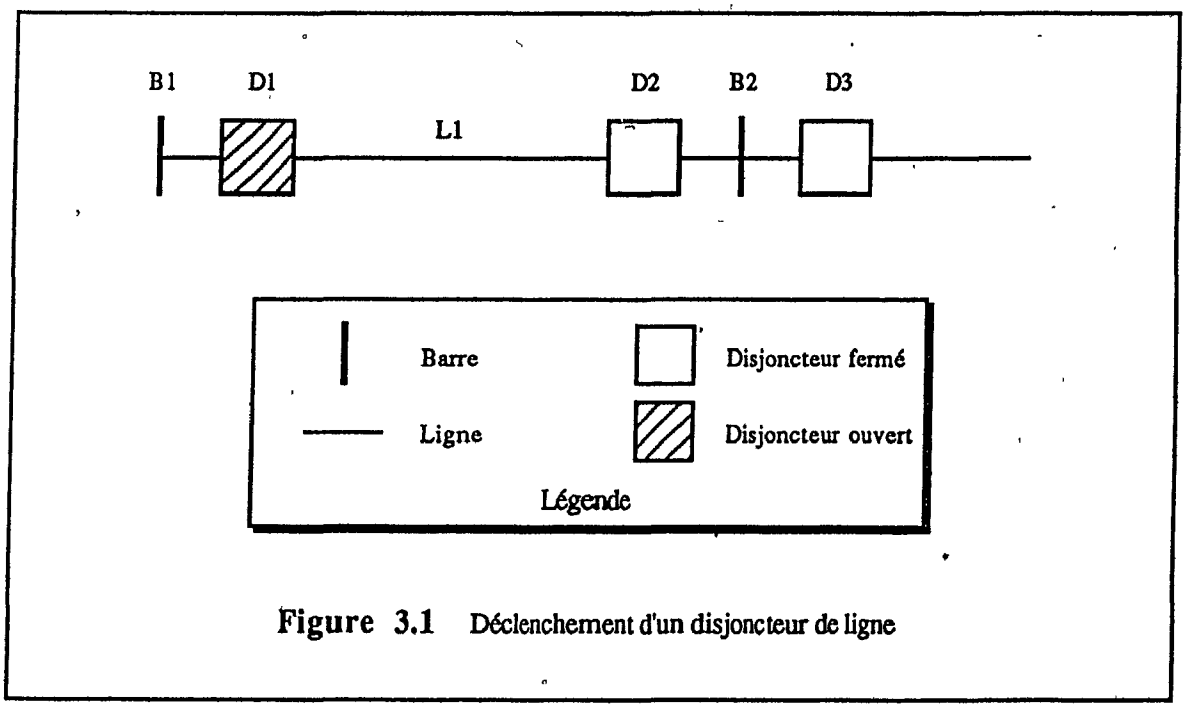


Figure 3.1 Déclenchement d'un disjoncteur de ligne

Plusieurs hypothèses peuvent expliquer l'alarme indiquant ce changement d'état. Trois d'entres elles sont énumérées ci-dessous.

1. Cette alarme est fausse.
2. Il y a une faute permanente sur la ligne L1; les disjoncteurs D1 et D2 ont tous deux déclenchés normalement mais l'alarme pour D2 a été "perdue".

3. Il y a une faute permanente sur la ligne L1; le disjoncteur D1 s'est ouvert; D2 ne s'est pas ouvert; D3 s'est ouvert comme protection de secours mais l'alarme de D3 a été "perdue".

En général, des hypothèses sont définies pour trois types d'évènements, soit les fautes d'équipement, l'opération correcte des systèmes de protection, et les erreurs dans l'opération de divers systèmes (fausses alarmes, mauvaise opération de systèmes de protection, etc.). De façon plus formelle, le principe de fonctionnement du logiciel [Talukdar, 1987] peut être exprimé de la manière suivante:

Déterminer tous les H_i tel que:

$$\| H_i \| \leq k \qquad (1)$$

$$F(H_i) = A \qquad (2)$$

où:

- $H_1, H_2, \ldots$ sont des hypothèses.
- $H_i \supseteq E$, $i = 1, 2, 3, \ldots$

  E est l'ensemble de tous les évènements possible qui peuvent générer des alarmes: fautes, opération de divers systèmes, erreurs dans l'opération de systèmes, etc.
- $\| H_i \|$ est le nombre d'évènements dans H_i.
- k est un nombre entier représentant le plus grand nombre possible d'évènements dans une hypothèse.
- $F(H_i)$ est la séquence d'alarmes qui serait causée par les évènements dans H_i.
- A est la séquence d'alarmes reçues.

La contrainte (1) assure que les hypothèses sont plausibles tandis que la contrainte (2) spécifie que chaque hypothèse doit expliquer la séquence d'alarmes reçues. Des algorithmes bien définis existent pour calculer $F(H_i)$. Cependant, la fonction inverse n'existe pas et c'est pourquoi ce système expert génère d'abord des hypothèses pour ensuite vérifier leur validité. Le dévelopement du logiciel de diagnostic décrit ci-haut requiert une combinaison de techniques de programmation heuristiques et algorithmiques. Par conséquent, ce logiciel est composé d'un système expert écrit en OPS-5 et de programmes algorithmiques écrits en Lisp et en C. L'architecture du logiciel nécessite quatre modules qui opèrent en parallèle et qui communiquent ensemble par l'entremise d'une base de connaissances commune.

1. **Module de gestion** (OPS-5):
   - contrôle l'exécution des autres modules.
   - extrait les alarmes principales de la séquence reçue.

2. **Générateur de conjectures** (OPS-5):
   - suggère des évènements pour développer les hypothèses incomplètes d'après les alarmes principales extraites par le module de gestion.

3. **Module de construction** (OPS-5 / C):
   - génère les alarmes qui correspondent aux évènements suggérés par le générateur de conjonctures.

4. **Module de vérification** (LISP):
   - évalue les hypothèses développées par le module de construction et élimine celles qui sont inconsistantes avec la séquence d'alarmes reçues.

La configuration de ce système expert permet d'ajouter des programmes additionnels à chacun des modules afin de raffiner leurs fonctions respectives et d'adapter le logiciel à divers réseaux électriques.

3.3.3 Diagnostic par analyse de modèle

Lors de perturbations complexes dans un réseau électrique, l'opération des systèmes de protection résulte en un grand nombre d'alarmes transmises au centre de contrôle. Afin d'aider les opérateurs à analyser de telles perturbations, un système expert [Fukui, 1986] a été développé pour identifier la cause des perturbations ainsi que les divers systèmes de protection impliqués dans l'isolation des appareils affectés. Ce logiciel utilise les messages de changements d'état reçus au centre de contrôle ainsi que des modèles de la topologie et des systèmes de protection du réseau pour générer des diagnostics. Tel qu'illustré dans la figure 3.2, ce système expert est composé d'un moteur d'inférence et de trois bases de connaissances.

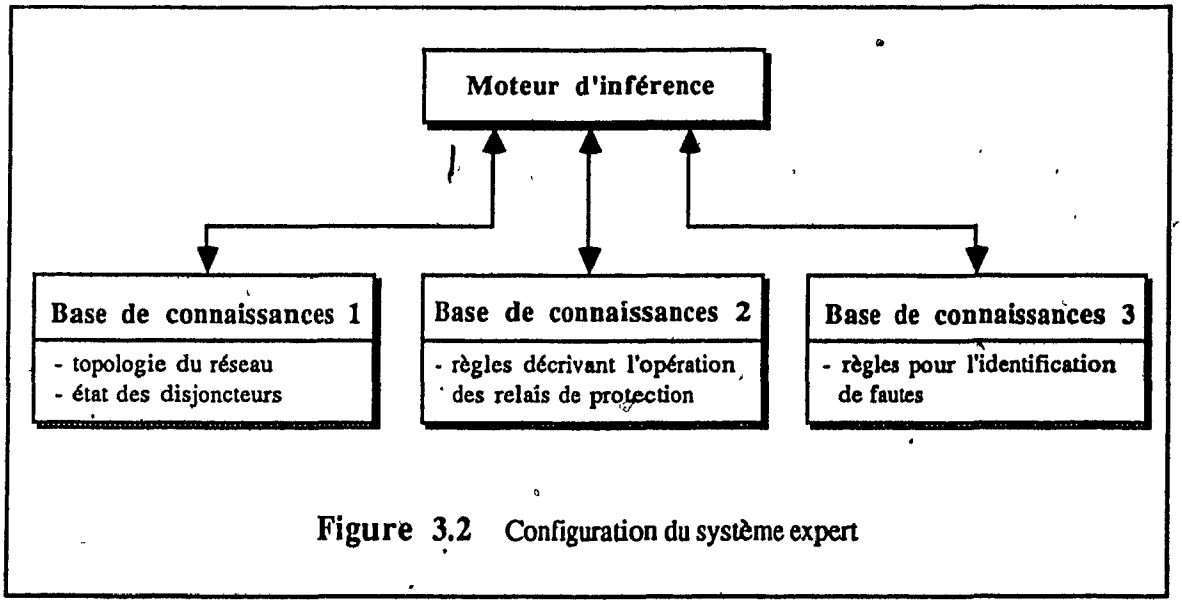
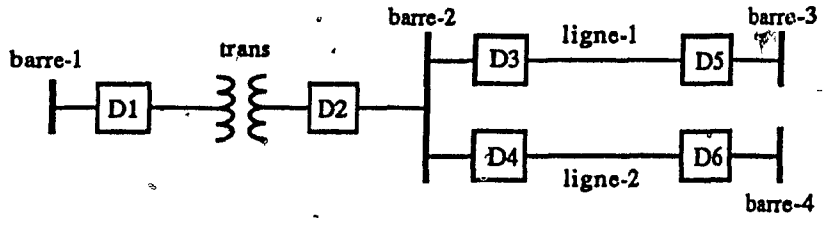
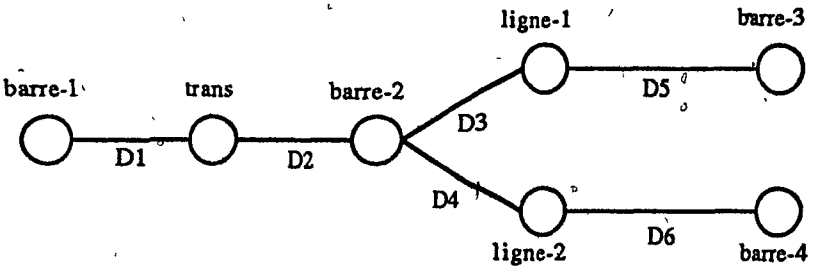


Figure 3.2 Configuration du système expert

La première base de connaissances contient des prédicats décrivant la topologie du réseau ainsi que l'état des disjoncteurs. La seconde base de connaissances se compose de règles décrivant l'opération des relais de protection et finalement, la troisième base de connaissances consiste en des règles heuristiques représentant les connaissances utilisées par les opérateurs pour identifier les composants affectés par des fautes.



a) Schéma original du réseau électrique



b) Représentation sous forme de graphe

réseau (barre-1, D1, trans, fermé)
réseau (trans, D2, barre-2, fermé)
réseau (barre-2, D3, ligne-1, fermé)
réseau (barre-2, D4, ligne-2, fermé)
réseau (ligne-1, D5, barre-3, fermé)
réseau (ligne-2, D6, barre-4, fermé)

c) Représentation sous forme de prédicats (Prolog)

Figure 3.3 Représentation par prédicats de la topologie du réseau

Base de connaissances 1 - *Topologie du réseau*: Cette base de connaissances décrit sous forme de prédicats les connections entre les disjoncteurs et les autres équipements du réseau. Cette description peut être élaborée à partir d'un graphe représentant la topologie du réseau. Chaque élément est représenté par un nœud du graphe tandis que chaque disjoncteur est représenté par une branche. La

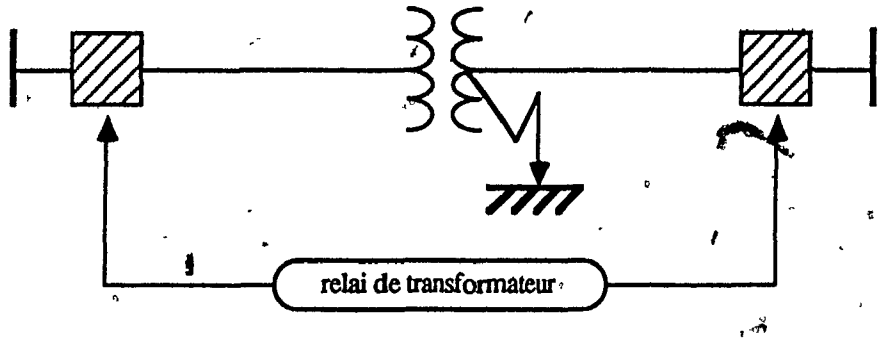
figure 3.3 illustre les étapes à suivre pour traduire un schéma électrique sous forme de prédicats décrivant la topologie du réseau.

Base de connaissances 2 - *Opération des relais de protection*: Bien qu'en réalité, la combinaison de plusieurs types de relais constitue les systèmes de protection du réseau, il est suffisant, pour les fins d'analyse du système expert, de décrire l'opération de ces systèmes de façon simplifiée en termes de seulement quelques types de "relais regroupés". Par exemple, dans le cas d'un système de protection à distance composé de relais d'admittance et de relais de réactance, il est suffisant de décrire les caractéristiques fonctionnelles d'un relai de protection à distance. Ainsi, la seconde base de connaissances contient des règles de Prolog décrivant l'opération des systèmes de protection en termes de relais regroupés. Voici la règle fondamentale pour l'opération des relais, ainsi que deux exemples de règles de relais simplifiés tels qu'illustrés dans la figure 3.4. Il est à noter que plusieurs nouveaux types de relais regroupés peuvent facilement être ajoutés à ce genre de modèle.

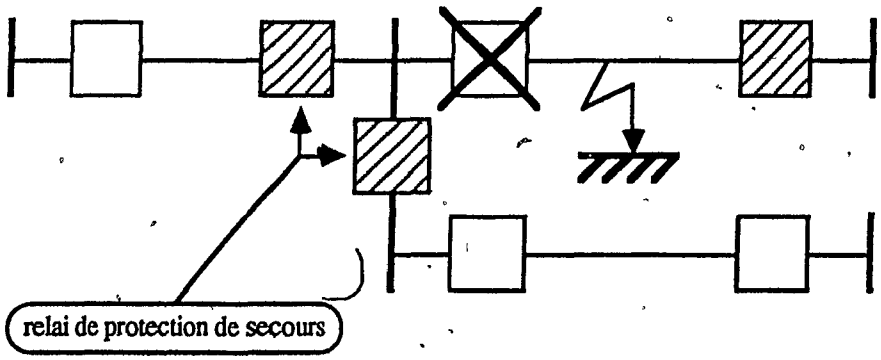
(a) Règle fondamentale:

```
active (Relai, Faute):-
    protection (Relai, Faute).
```

Explication: Premièrement, il est bon de rappeler que les termes commençant par des lettres majuscules représentent des variables. Le mécanisme de cette règle est assez général: si une "Faute" existe dans une région de protection d'un "Relai", alors le "Relai" est activé.



a) Relai simplifié de la protection principale d'un transformateur



b) Relai simplifié de la protection de secours d'une zone

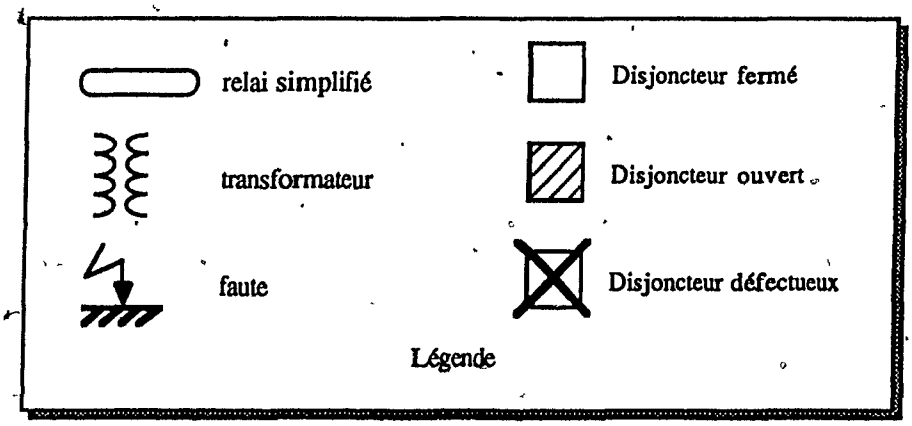


Figure 3.4 Exemples de relais simplifiés

(b) Règle de relai pour la protection principale d'un transformateur:

```
protection (Relai, Faute):-
    relai (Relai, relai_de_tranformateur, Disjoncteurs, Zones, [], []),
    membre (Faute, Zones).
```

Explication: Si une "Faute" est décelée dans une des "Zones" qui correspond à un des nœuds surveillés par un "Relai" de type "relai_de_tranformateur", alors la "Faute" existe dans la zone de protection du "relai_de_transformateur" "Relai".

(c) Règle de relai pour la protection de secours d'une zone:

```
protection (Relai, Faute):-
    relai (Relai, relai_de_secours, Disjoncteurs, [], Relai_principal, []),
    est_activé (Relai_principal),
    relai (Relai_principal, Type, Disjoncteurs_du_Relai_principal,
                    Zones, [], []),
    membre (Disjoncteur, Disjoncteurs_du_Relai_principal),
    non (declenché (Disjoncteur)),
    membre (Faute, Zones).
```

Explication: Si une "Faute" existe dans une des "Zones" de protection d'un "Relai_principal" qui a été activé, et qu'un "Disjoncteur" de ce "Relai_principal" n'a pas déclenché, alors la "Faute" affecte aussi le "Relai" de type "relai_de_secours" qui agit comme protection de secours pour le "Relai_principal".

Base de connaissances 3 - *Règles pour identifier les composants affectés par des fautes*: Cette base de connaissances contient les règles utilisées pour l'analyse de perturbations basées sur les *messages de changements d'état* reçus au centre de contrôle. Tel qu'illustré dans la figure 3.5, ces règles sont subdivisées en une

hiérarchie à trois niveaux, soit de règles pour l'analyse de fautes simples, de règles pour l'analyse de fautes multiples, et de règles pour le traitement de manques d'information et pour l'analyse d'interactions entre fautes.

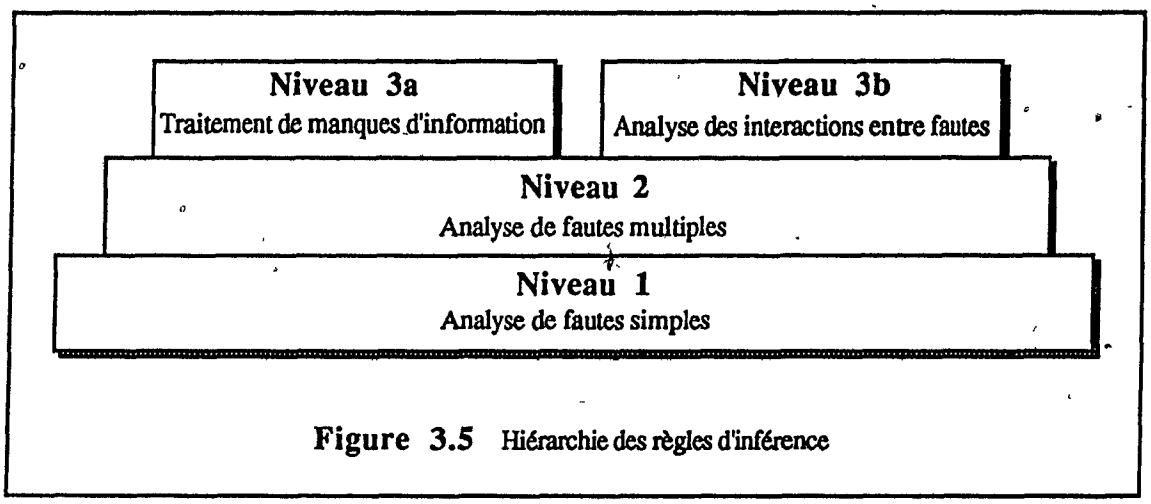


Figure 3.5 Hiérarchie des règles d'inférence

Les fautes simples sont identifiées en utilisant le mécanisme d'enchaînement arrière de Prolog afin de localiser le nœud du modèle qui justifie l'opération de tous les relais ayant opérés. Lors de fautes multiples ou de défauts dans les relais ou disjoncteurs, les règles d'analyse pour fautes simples ne peuvent identifier les nœuds affectés. Dans de telles situations, les règles de niveau plus élevé dans la hiérarchie sont utilisées. Les règles d'analyse de fautes multiples subdivisent les relais ayant opérés en des groupes correspondant à des fautes simples. Par la suite, les règles d'analyse de fautes simples sont appliquées à chacun de ces groupes afin de déterminer le nœud affecté par chacune des fautes. Lorsqu'un relai n'opère pas normalement, son message de changement d'état n'est pas transmis au centre de contrôle et par conséquent, il en résulte un manque d'information. Dans de tels cas, le système expert détecte une inconsistance de données et, par conséquent, invoque des règles pouvant identifier des défauts

dans les relais et disjoncteurs. Par exemple, une règle typique exprime le fait que si un relai a été stimulé et qu'un de ses disjoncteurs associés n'a pas déclenché, alors ce disjoncteur peut être considéré comme étant défectueux. En utilisant de telles règles, le système expert génère l'information nécessaire pour compléter l'analyse d'une séquence incomplète. Lors de fautes multiples causant l'isolation de plusieurs zones de protection, le système expert utilise un groupe de règles pour déduire les relations entre ces fautes. Par exemple, en analysant deux zones de protection adjacentes qui ont été isolées, le système expert établit une ou plusieurs hypothèse(s) décrivant le genre de faute ayant pu générer cette configuration. Par conséquent, lors de l'analyse de fautes multiples, le système expert peut générer plus d'un diagnostic décrivant la cause de la perturbation. Enfin, lorsque le système expert a identifié les composants isolés et la cause probable d'une faute, la séquence d'opération des divers systèmes de protection peut être simulée en utilisant les règles décrivant le fonctionnement des relais. De cette façon, le système expert peut expliquer comment une faute a causé une configuration de réseau spécifique.

3.3.4 Analyse par règles heuristiques

Un système expert a été développé pour supprimer les messages redondants contenus dans les séquences d'évènements reçus aux centres de contrôle de réseaux. Ce système expert [Wollenberg, 1986] utilise des règles d'enchaînement avant afin d'extraire les alarmes principales d'une séquence donnée. Essentiellement, ces règles heuristiques peuvent être subdivisées en quatre catégories.

1. **Analyse de l'élément en cause:** Les règles de cette catégorie sont utilisées pour identifier le type d'élément (ligne, barre, transformateur, etc.) affecté par la condition d'alarme. De plus, ces règles vérifient si d'autres alarmes reliées à ce même élément ont été reçues au préalable afin de déterminer si la condition d'alarme de cet élément se déteriore. Si tel est le cas, une condition est spécifiée de façon à ce que les règles de présentation des alarmes reconnaissent cet état et qu'elles affichent les alarmes principales qui y correspondent.

2. **Déduction de pertes de production:** Ces règles analysent les alarmes de changements d'état non-autorisés et les alarmes de systèmes afin de déterminer s'il y a eu ou non perte de production. Ces règles permettent donc au système expert de déduire une perte de production même sans avoir reçu une alarme indiquant cette condition spécifique.

3. **Suppression d'alarmes redondantes:** Ces règles analysent les alarmes reçues afin de spécifier quelles alarmes sont redondantes ou inutiles. Deux règles typiques de cette catégorie sont décrites ci-dessous.

   (a) Supprimer une alarme de retour à la normale si aucune alarme n'a été reçue au préalable pour l'élément en cause.

   (b) Supprimer les alarmes de déclenchement et de réenclenchement de disjoncteurs si elles changent l'état (sous-tension, hors-tension, sous-charge, hors-charge) d'une ligne ou d'un transformateur.

4. Présentation des alarmes: Ces règles déterminent quelles sont les alarmes qui doivent être affichées à la console de l'opérateur. Pour se faire, elles utilisent l'information générée par les règles des trois niveaux précédents. Deux règles typiques de cette catégorie sont décrites ci-dessous.

(a) Présenter une alarme de perte de tension lorsque les disjoncteurs ont déclenché aux deux extrémités d'une ligne ou d'un transformateur.

(b) Afficher toutes les alarmes indiquant une condition qui se déteriore. De telles conditions sont identifiées par les règles d'analyse de l'élément en cause.

En résumé, ce système expert utilise une hiérarchie de règles d'enchaînement avant à quatre niveaux pour analyser les séquences d'évènements en temps réel afin de supprimer les messages redondants ou inutiles.

3.4 Sommaire

Lors de perturbations dans un réseau électrique, le système d'acquisition de données (S.C.A.D.A.) présente de longues séquences d'alarmes et de changements d'état aux opérateurs du centre de contrôle. Afin d'aider ces derniers à extraire l'information pertinente de ces séquences, des logiciels sont intégrés aux bases de données du centre de contrôle pour indiquer la priorité des alarmes reçues ainsi que pour supprimer certaines alarmes redondantes lors de conditions préétablies. Bien que de tels logiciels simplifient la tâche des opérateurs, le problème de gestion des alarmes n'en est pas pour autant résolu puisque dans bien des cas, l'opérateur est tout de même submergé par les informations qui lui sont présentées. En guise de solution à ce problème, des prototypes de systèmes experts ont été développés pour analyser, en temps réel, des séquences d'évènements reçus au centre de contrôle, ceci afin d'établir des diagnostics de perturbations et de limiter le nombre de fausses alarmes présentées aux opérateurs. Ce chapitre a décrit quatre architectures distinctes de tels systèmes experts. Ces architectures seront comparées à celle du système expert présenté dans cette thèse.

Chapitre 4 Un système expert pour la gestion des alarmes

Ce chapitre décrit un système expert pour la gestion en temps réel des alarmes reçues aux centres de contrôle d'un réseau électrique. Pour des raisons pratiques, le nom de GESTAL sera dorénavant utilisé pour identifier ce système de gestion des alarmes "intelligent". La première section de ce chapitre traite, de façon générale, des divers aspects fonctionnels de GESTAL. Une vue plus détaillée de son architecture interne, ainsi qu'une évaluation de ses performances sont également présentées dans les sections subséquentes.

4.1 Vue d'ensemble du système

4.1.1 Objectifs fonctionnels

Tel que décrit dans le chapitre précédent, au cours de pannes importantes, le système d'acquisition de données du centre de contrôle d'un réseau électrique peut afficher plusieurs centaines de messages d'alarme aux consoles de l'opérateur. Par conséquent, ce dernier risque alors d'éprouver des difficultés à gérer le réseau de manière optimale. Dans ces cas, l'utilisation d'un système expert peut grandement simplifier la tâche de l'opérateur en réduisant la quantité et en augmentant la qualité de l'information lui étant présentée. Les

diverses fonctions incluses dans GESTAL pour arriver à ces fins sont exposées et expliquées dans les paragraphes qui suivent.

Lors de perturbations de réseau, les opérateurs doivent analyser les informations leur étant présentées, et ce, le plus rapidement possible, afin d'effectuer les manœuvres nécessaires pour maintenir ou remettre le réseau dans un état normal. Par conséquent, il est primordial que le temps de réponse d'un système de gestion d'alarmes soit assez court pour permettre à l'opérateur de réagir en un temps acceptable. De plus, puisque le but d'un tel système est d'alléger la tâche des opérateurs, il est primordial que son utilisation ne nécessite pas d'interventions supplémentaires de la part de ces derniers. En somme, le fonctionnement *automatique* et le traitement des messages *en temps réel* constituent deux caractéristiques fondamentales pour tout système de gestion d'alarmes, GESTAL a donc été conçu selon ces critères.

La nature du traitement des alarmes varie considérablement d'un système à l'autre. L'objetif de certains est de réduire le nombre d'alarmes présentées à l'opérateur, tandis que d'autres ont comme but d'interpréter les messages d'alarme reçus. Ceux-ci sont plus intéressants puisqu'ils évitent aux opérateurs de devoir interpréter et analyser les alarmes eux-mêmes. D'ailleurs, une analyse de plusieurs mois auprès des opérateurs d'Hydro-Québec a révélé qu'un système capable d'interpréter les messages d'alarme et d'établir des diagnostics concis constitue le point de mire pour les développements futurs dans ce domaine. Conçu suivant cette ligne de pensée, le système expert GESTAL peut interpréter de façon claire et précise les alarmes reçues suite à l'opération des divers systèmes d'alarme et de protection. Par exemple, lorsqu'un défaut de gaz est décelé dans un transformateur et que tous les systèmes de protection fonctionnent correctement, plusieurs messages d'alarme sont affichés aux consoles de l'opérateur. On y retrouve entre autres un message indiquant la faute de gaz sur le

transformateur, un autre annonçant une alarme de déclenchement, et enfin toute une série de changements d'état correspondant au déclenchement de chacun des disjoncteurs de la zone de protection.

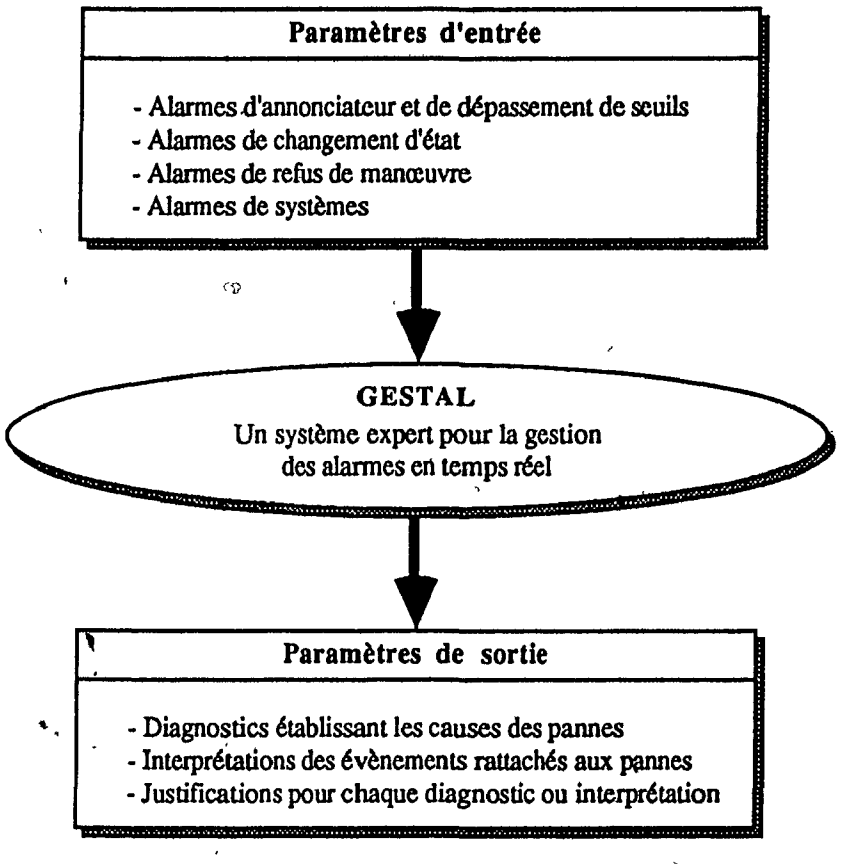


Figure 4.1 Aspect fonctionnel de GESTAL

Pourtant, la seule information que l'opérateur doit extraire de tous ces messages est que le transformateur a été isolé correctement suite à une faute de gaz. De plus, les alarmes principales sont généralement immergées dans une foule d'autres alarmes qui ne font qu'exprimer les conséquences normales de l'opération des systèmes d'alarme et de protection. Ces alarmes ne sont pas essentielles pour établir un diagnostic correct de la panne, et par

conséquent, elles rendent le processus d'analyse beaucoup plus complexe pour l'opérateur. Ainsi, suite à un diagnostic établi par GESTAL, afin de permettre à l'opérateur de comprendre les fondements de cette analyse, ce dernier a également accès à une justification expliquant, par des relations entre les diverses alarmes reçues, comment le diagnostic a été fait. La figure 4.1 illustre les principales caractéristiques fonctionnelles de GESTAL.

En somme, les diagnostics de GESTAL sont conçus pour identifier les causes des perturbations et décrire l'opération des systèmes d'alarme et de protection activés. De plus, chaque diagnostic est associé à une justification consistant en une liste des alarmes utilisées pour fonder l'analyse.

4.1.2 Contexte de développement

Le prototype de GESTAL a été développé en deux étapes. En premier lieu, un modèle de réseau et un simulateur [Arès, 1987] ont été conçus et mis au point. La mise au point de ces systèmes s'est faite en collaboration avec les experts en automatisme d'Hydro-Québec. Ceux-ci ont analysé les résultats des simulations pour différentes classes de fautes de façon à permettre un raffinement adéquat du modèle. La seconde phase a été le développement et la mise au point de la base de règles de GESTAL. Le raffinement de ce dernier s'est effectué à partir de séquences d'alarmes produites par le simulateur et de listes d'évènements déjà encourus dans le réseau même d'Hydro-Québec. Bref, le simulateur a servi à valider le modèle du réseau utilisé par GESTAL ainsi qu'à générer des messages d'alarme pour la mise au point de ses règles de diagnostic.

La configuration globale des systèmes experts impliqués dans le développement et la vérification de GESTAL est illustrée dans la figure 4.2. Le raisonnement des deux systèmes experts est basé sur un modèle du réseau ("model-based reasoning"). Tel qu'indiqué sur le schéma, le simulateur et GESTAL utilisent tous deux le même modèle du réseau; toutefois, ils peuvent fonctionner indépendamment l'un de l'autre.

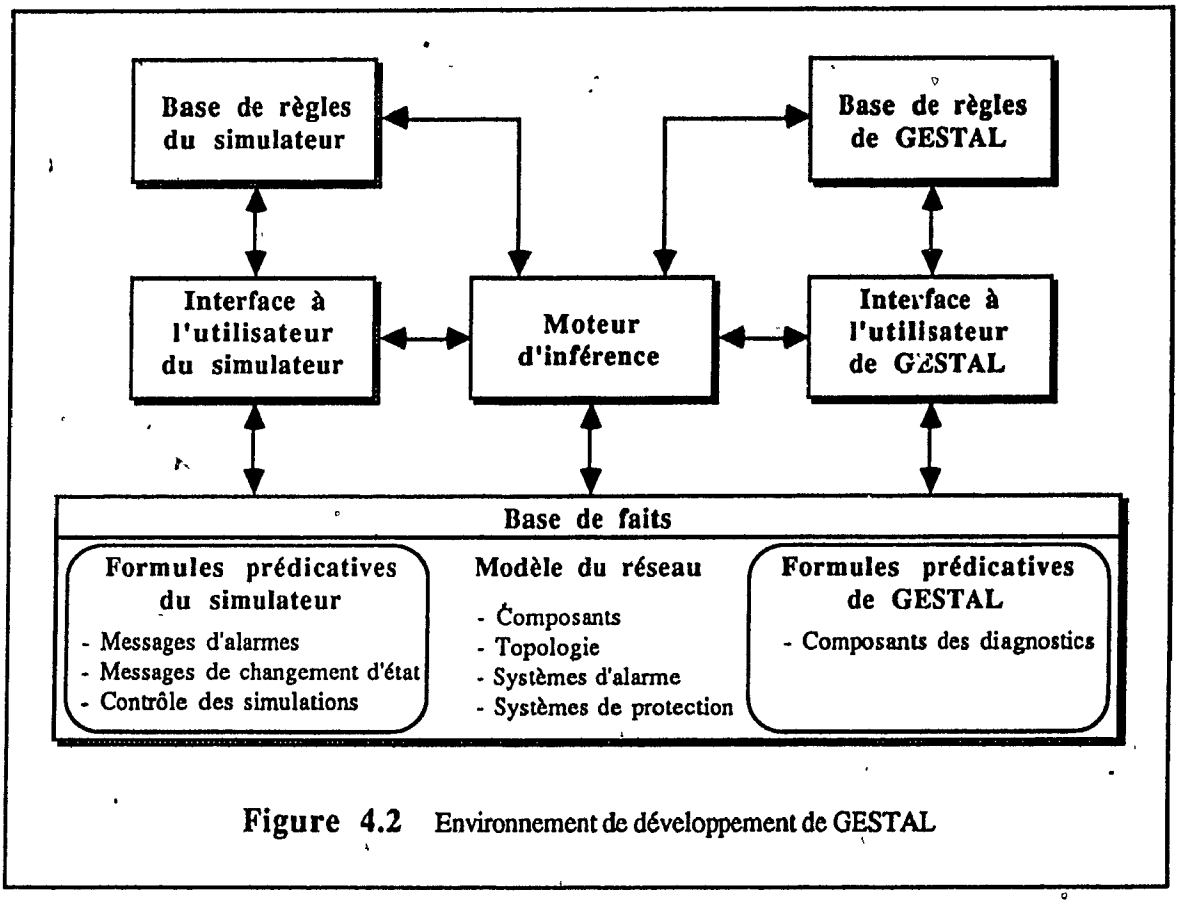


Figure 4.2 Environnement de développement de GESTAL

Le modèle consiste en une représentation par schémas qui exprime la topologie du réseau, l'état des appareils, ainsi que les mécanismes fonctionnels des systèmes d'alarme et de protection. Le simulateur se compose d'un modèle du réseau, d'une base de règles, et d'un interface à l'utilisateur. Suite à une perturbation fictive définie par des défaillances d'équipements spécifiques du réseau, le simulateur génère les messages d'alarme et la configuration du réseau qui devraient normalement résulter de l'opération des systèmes

d'alarme et de protection. Enfin, GESTAL consiste en un modèle du réseau, une base de règles, et un interface à l'utilisateur. Suite à l'analyse d'une séquence d'alarmes décrivant une perturbation donnée dans le réseau, il produit des diagnostics qui identifient l'élément et le type de défaut en cause, ainsi que les sytèmes d'alarme et de protection qui ont opérés.

Les deux systèmes experts ont été développés sur un super-mini-ordinateur *Symbolics 3640*. La plus grande partie des programmes a été écrite en utilisant l'environnement de développement pour systèmes experts *ART 3.0* [Inference, 1987]. Ce langage hybride permet des représentations par schémas et par formules prédicatives; de plus, plusieurs paradigmes de raisonnement sont offerts, soit l'enchaînement avant, l'enchaînement arrière, ainsi que le raisonnement par points de vue multiples. Le langage ART 3.0 et l'environnement de la machine-Lisp ont permis, grâce leurs fonctions de mise au point très sophistiquées, de développer rapidement des prototypes opérationnels du simulateur et de GESTAL. Enfin, il faut souligner qu'une portion des systèmes a été encodée en Lisp afin d'améliorer leur temps de réponse.

4.1.3 Description générale du mécanisme interne

Cette section décrit globalement, à l'aide d'un exemple, le mécanisme logique impliqué dans l'interprétation de séquences d'alarmes en temps réel. La figure 4.3 illustre le contenu de la base de faits de GESTAL à quatre moments successifs, lors d'une panne dans le réseau électrique. Ces quatre fenêtres temporelles permettent d'expliquer sommairement le processus de génération de diagnostics propre à GESTAL. Sur le schéma, les *branches* expriment des relations de *parenté* entre les *nœuds*, tandis que l'ensemble de ces branches et de ces nœuds constitue un *arbre à diagnostic*. GESTAL établit les causes de perturbations en analysant les propriétés des *racines* d'arbres à diagnostic complets.

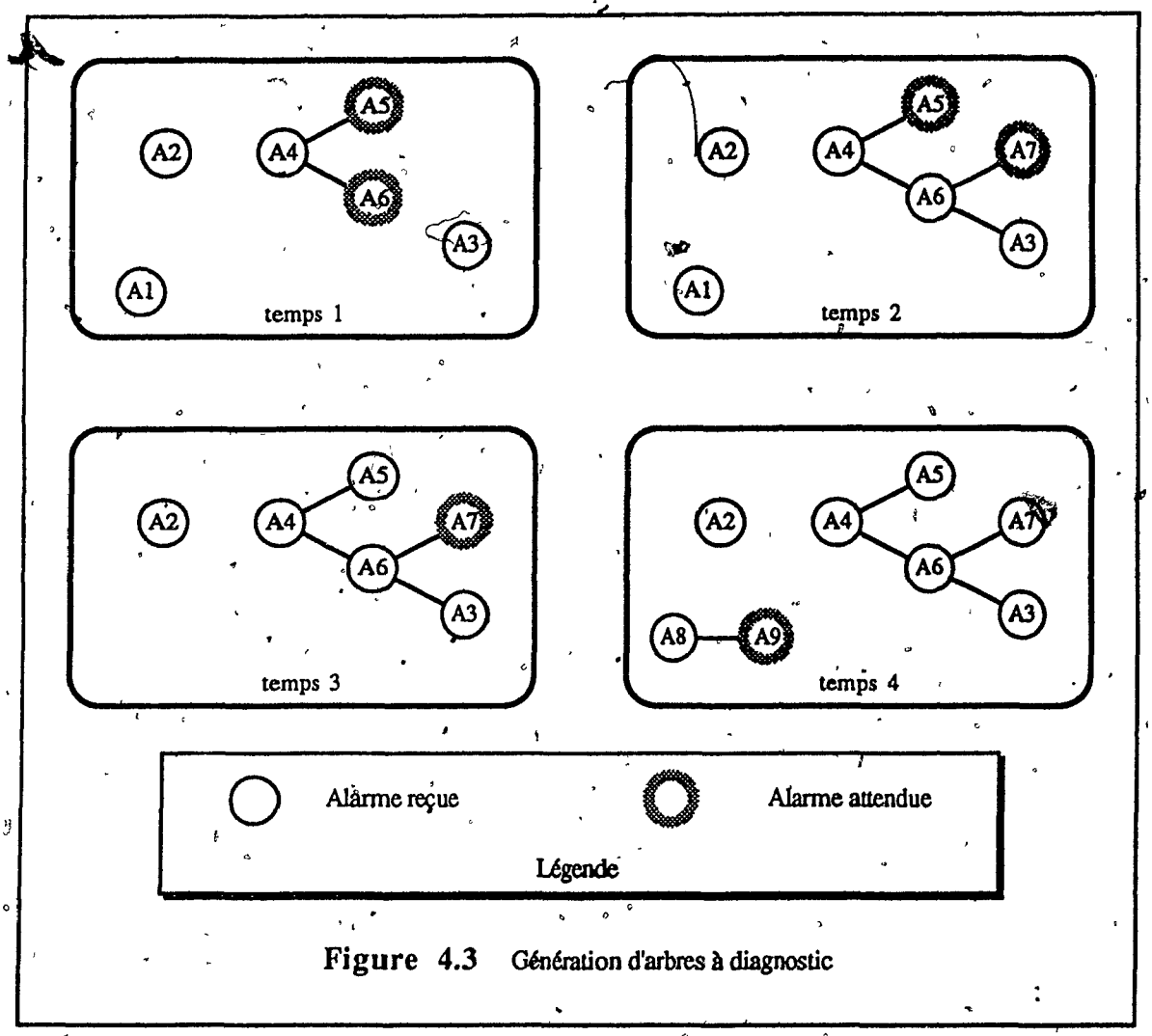


Figure 4.3 Génération d'arbres à diagnostic

Temps 1: GESTAL a déjà reçu les alarmes A1, A2, A3, et A4. En examinant son modèle du réseau dans la base de faits, le système conclut que suite à l'alarme A4, l'opération normale des systèmes d'alarme et de protection devrait causer les alarmes A5 et A6. Par conséquent, GESTAL crée un arbre à diagnostic incomplet, où les enfants sont les alarmes attendues A5 et A6, et la racine est A4.

Temps 2: L'alarme attendue A6 est enfin reçue. Toutefois, une analyse du modèle indique que les alarmes A7 et A3 sont des conséquences logiques de cette alarme. Le nœud A7 s'ajoute donc à l'arbre sous forme d'alarme attendue. Par contre,

puisque l'alarme A3 est déjà présente dans la base de faits, elle ne fait qu'être reliée à l'arbre par une nouvelle branche.

Temps 3: L'alarme attendue A5 est reçue et placée à l'endroit approprié dans l'arbre à diagnostic A4. Le nœud A1 est retiré de la base de faits parce qu'il est très peu probable qu'il ne soit jamais relié à un arbre, étant donné son "âge" déjà considérable.

Temps 4: L'alarme A8 est reçue, et devient la racine d'un nouvel arbre à diagnostic puisque l'alarme A9 est dorénavant attendue. De plus, l'arbre A4 se complète suite à la réception de l'alarme A5. GESTAL peut alors établir la cause de la perturbation, composée des alarmes A3, A4, A5, A6, et A7, en extrayant de son modèle du réseau le défaut normalement à l'origine d'une alarme du type A4.

En somme, GESTAL génère les diagnostics en deux étapes: premièrement, les arbres à diagnostic sont assemblés progressivement lors de l'arrivée de nouvelles alarmes dans la base de faits, et deuxièmement, les diagnostics mêmes sont produits à partir d'une analyse des propriétés de la structure d'arbres à diagnostic complets et des différents nœuds qui les composent.

4.2 Modèle du réseau électrique

4.2.1 Aménagement des connaissances

L'une des étapes capitales dans le développement d'un système expert est de déterminer quelles connaissances seront exprimées de manière déclarative, et lesquelles seront représentées de façon procédurale. Cette décision doit se faire en évaluant des critères propres au système expert projeté. Par exemple, pour le devéloppement de GESTAL, il était primordial de s'assurer que le système soit très robuste et facilement modifiable, de manière à permettre l'intégration rapide de nouveaux postes dans la base de connaissances sans pour autant menacer le bon fonctionnement du système déjà instauré.

Tel que mentionné ci-dessus, la robustesse et la capacité d'expansion sont les deux objectifs fondamentaux qui ont guidé la conception de l'architecture de GESTAL. À partir de ces critères de base, des contraintes spécifiques ont été définies pour le développement des bases de connaissances. La première de ces contraintes consiste à s'assurer que les exceptions dans la structure des systèmes d'alarme et de protection du réseau électrique puissent être intégrées au modèle de manière efficace et élégante. La seconde contrainte majeure exige que le temps de réponse de GESTAL soit le plus indépendant possible du nombre d'appareils contrôlés, ceci garantissant des diagnostics en temps réel même pour un réseau d'ampleur considérable. Enfin, la dernière contrainte notable se situe au niveau de l'acquisition de données: il est important de trouver une source d'expertise stable et durable de façon à permettre des revisions du système pendant plusieurs années. Une longue étude, fondée sur les critères énumérés ci-dessus, a permis de déterminer de manière concluante qu'une configuration basée sur un modèle déclaratif du réseau constituait l'architecture optimale pour GESTAL.

Ainsi, la base de connaissances procédurales contient des règles de diagnostic basées sur la philosophie générale du fonctionnement des systèmes d'alarme et de protection du réseau électrique, tandis que la base de connaissances déclaratives se compose d'information décrivant les mécanismes d'alarme et de protection propres à chaque appareil ainsi que l'état des divers équipements. Cette approche permet de modifier les connaissances se rapportant à la topologie du réseau, à la configuration des postes, et à l'opération des systèmes de protection, sans pour autant devoir ajuster la base de règles en réponse à ces changements. De plus, le processus d'acquisition des connaissances est grandement simplifié, puisque la plus grande partie de l'information requise par GESTAL provient de schémas synoptiques des systèmes d'alarme et de protection. En dernier lieu, il faut mentionner qu'une fois la base de connaissances procédurales bien définie, seule la base de connaissances déclaratives devra être modifiée pour la mise à jour périodique du système.

4.2.2 Paradigme de stimulus-réaction

Le modèle du réseau représente les mécanismes de génération d'alarmes et d'opération des systèmes de protection en utilisant un *paradigme de stimulus-réaction.* Tel qu'illustré sur la figure 4.4a), à la description de chaque appareil est associée une liste d'alarmes avec leurs stimuli et leurs réactions spécifiques. Les stimuli représentent les causes possibles ayant pu activer une alarme sur un élément, tandis que les réactions spécifient les répercussions normalement attendues suite à l'activation d'une alarme. Un code normalisé est défini pour les différents types de stimuli et de réactions afin de pouvoir représenter explicitement les connaissances associées aux mécanismes d'alarme et de protection. Un échantillon de ce code, illustrant le niveau de détail des connaissances utilisées dans le modèle du réseau, est décrit par la figure 4.4b).

```
[ appareil
        . . .
    [ alarme #1     [ stimulus #1 ... stimulus #m ]     [ réaction #1 ... réaction #n ] ]
        . . .
    [ alarme #k     [ stimulus #1 ... stimulus #i ]     [ réaction #1 ... réaction #j ] ]
        . . .   ]
```

a) Listes de stimulus-réaction pour les alarmes d'un appareil

Code	Signification
Stimuli:	
diff	Faute différentielle aux bornes de l'appareil
gaz	Présence de gaz critique dans l'appareil
temp	Température élevée dans l'appareil
htemp	Température critique dans l'appareil
Réactions:	
décl	Déclenchement des disjoncteurs de la zone de protection
sec	Activation de la protection de secours
rs	Activation du rétablisseur de service
tim	Délai associé à une réaction

b) Échantillon de la codification des stimuli et des réactions

```
[ appareil
        . . .
    [ alarme #i     [ stimulus #1 ... stimulus #j ]
                    [ réaction #1 ... [ tim t_m réaction #m ] ... réaction #n ] ]
        . . .   ]
```

c) Représentation d'une réaction à retardement

Figure 4.4 Représentation à l'aide du paradigme stimulus-réaction

Les caractéristiques des systèmes d'alarme et de protection sont extraites de schémas synoptiques, et puis encodées pour chaque élément sous forme de codes d'alarme, de stimuli, et de réactions. Par conséquent, le modèle de chaque élément du réseau comprend une liste des messages d'alarme qui peuvent l'affecter, et pour chacune de ces alarmes, une énumération des causes et des effets reliés à leur activation.

Le modèle du réseau permet également la définition de ***réactions à retardement.*** Les *réactions immédiates* se produisent dès la détection d'un de leurs stimuli correspondants, tandis que les réactions à retardement sont activées après un certain délai. Ainsi dans la figure 4.4c), la réaction #m sera activée t_m cycles après la détection d'un de ses stimuli associés. Le *cycle*, période de temps de 1/60 de seconde, est l'unité de temps généralement utilisée dans les réseaux électriques. Cet aspect temporel du modèle est essentiel puisque les systèmes d'alarme et de protection fonctionnent suivant une chronologie très spécifique.

Bref, le modèle de stimulus-réaction offre la flexibilité nécessaire pour représenter explicitement et exactement les causes possibles de l'activation d'une alarme. De plus, cette approche fournit une méthode normalisée et systématique pour modéliser les connaissances relatives aux systèmes d'alarme et de protection.

4.2.3 Taxinomie des éléments du réseau

Une représentation par schémas est utilisée pour représenter les divers équipements qui composent le réseau électrique. Les principaux appareils modélisés sont les transformateurs, les lignes, les barres, les disjoncteurs, et les condensateurs. Chaque élément est caractérisé par un ensemble d'attributs. Les attributs indiquent l'état des appareils, les relations avec d'autres équipements, ou encore, tel que mentionné précédemment, le

fonctionnement des systèmes d'alarme et de protection. Des attributs typiques sont énumérés dans la figure 4.5.

Attributs décrivant l'état d'un appareil	
[utilisable <v ou f>]:	Indique si un appareil est utilisable ou non.
[alimenté <v ou f>]:	Indique si un équipement est sous tension ou non.
[status <ouvert ou fermé>]:	Indique si un sectionneur ou un disjoncteur est ouvert ou fermé.
[connecté <v ou f>]:	Indique si un élément est toujours connecté au réseau.

Attributs exprimant des relations à d'autres éléments	
[disj <liste de disjoncteurs>]:	Spécifie les disjoncteurs qui constituent la zone de protection principale d'un appareil.
[élément_adj <liste d'éléments>]:	Spécifie les appareils qui constituent les centres des zones de protection adjacentes à un disjoncteur.
[aux <liste d'éléments>]:	Contient la liste des éléments qui partagent la même alarme que l'élément en question. Ceci est nécessaire quand l'activation d'une même alarme peut être due à une défaillance sur plus d'un appareil.

Attributs associés aux systèmes d'alarmes et de protection	
[alarme <code [<stimuli> <réactions>]>]:	Tel qu'énoncé dans la section 4.2.2, chaque élément peut contenir plusieurs de ces attributs qui décrivent le fonctionnement des systèmes d'alarmes et de protection associés celui-ci.

Figure 4.5 Principaux attributs utilisés par GESTAL

La représentation par schémas permet à certains schémas d'hériter la valeur d'attributs de classes plus générales. Le modèle du réseau utilise cette propriété dans la définition de sa taxinomie. En effet, une *structure d'héritage* à trois niveaux permet de définir rapidement le modèle de chaque appareil. Le niveau le plus général est appelé le *type*, ensuite vient la *classe*, et suivie au dernier niveau par le *composant*.

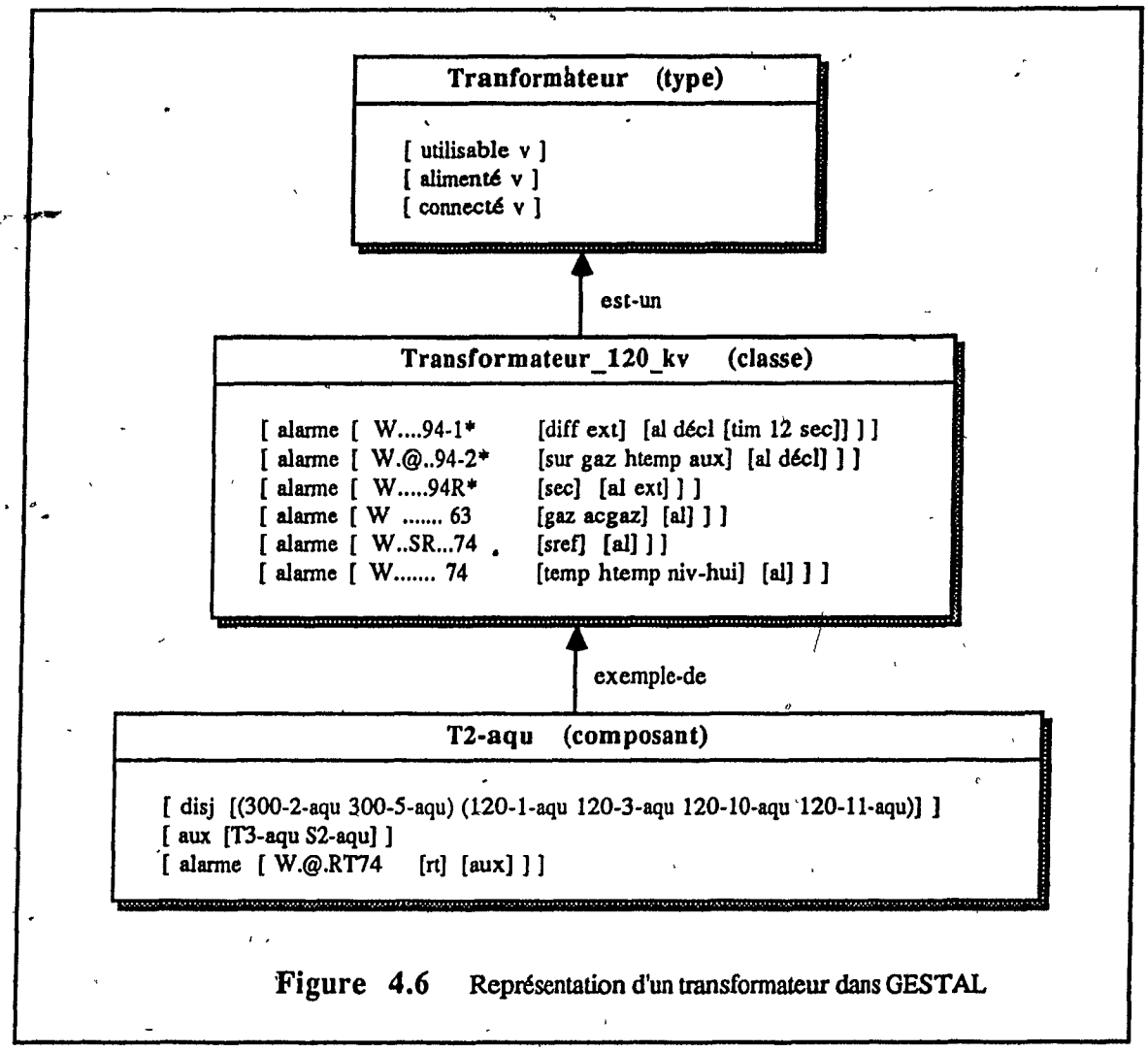


Figure 4.6 Représentation d'un transformateur dans GESTAL

La figure 4.6 exemplifie l'utilisation de structures d'héritage en décrivant les différents niveaux taxinomiques nécessaires à la définition du modèle d'un transformateur. Tel qu'illustré, le type "Transformateur" se compose d'attributs communs à toutes les classes de

transformateurs, soit de ceux qui expriment l'état d'un transformateur par défaut. La classe "Transformateur_120_kv" est constituée d'attributs généralement retrouvés chez tous les transformateurs de postes de transport de 120 kv, soit d'alarmes propres à cette classe d'appareils. Enfin, le composant "T2-aqu" comporte des attributs exprimant les connexions spécifiques de cet élément, ainsi qu'une alarme typique à ce transformateur particulier.

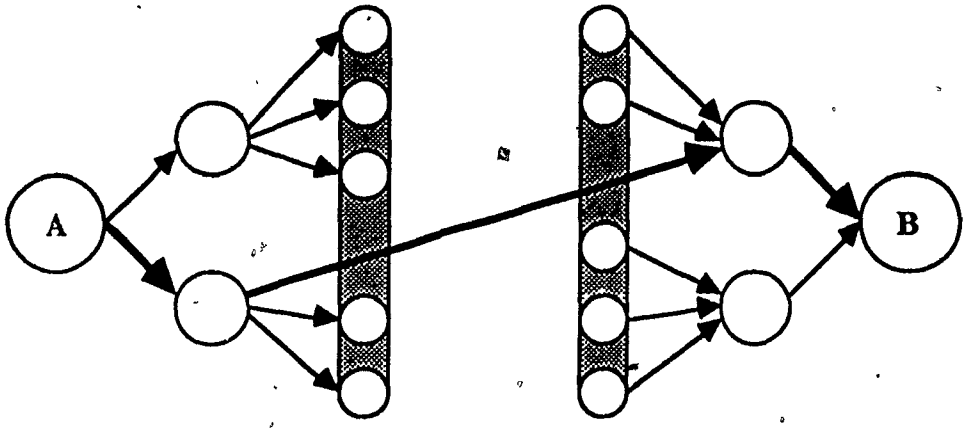
4.3 Stratégie de raisonnement

4.3.1 Nature de l'analyse

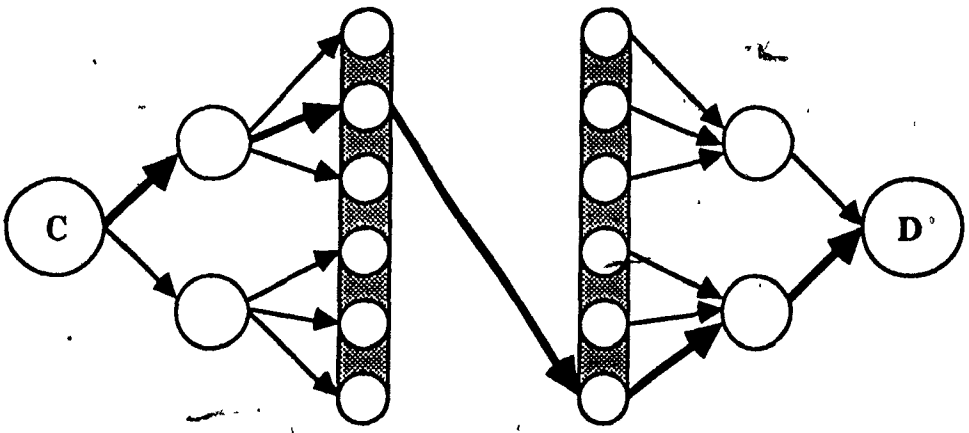
L'interprétation de messages d'alarme en temps réel est un procédé qui comporte plusieurs facettes. Ainsi, avant de concevoir un système expert de gestion d'alarmes, deux aspects fondamentaux de ce problème doivent être étudiés en détail. Premièrement, il faut déterminer le *niveau d'abstraction* auquel l'analyse des messages reçus peut se faire le plus efficacement possible. Deuxièmement, une stratégie d'analyse générale doit être conceptualisée pour tenir compte du caractère temporel du processus d'interprétation, aspect qui résulte du flux continuel d'évènements devant être analysés par le système expert. L'architecture de GESTAL combine des concepts tirés de recherches antérieures avec de nouvelles techniques d'analyse afin de résoudre les différentes portions du problème. La première partie de cette section présente le niveau d'abstraction auquel GESTAL traite les messages d'alarme qu'il reçoit, et la seconde partie introduit la technique utilisée pour résoudre le problème de la temporalité des évènements dans l'interprétation de messages d'alarme.

Afin de déterminer le niveau d'abstraction idéal auquel analyser les pannes dans le réseau, il est d'abord nécessaire d'étudier comment les perturbations s'y propagent, puisque les diagnostics sont généralement basés sur les relations existant entre les divers évènements encourus au cours d'une panne. Trois niveaux d'abstraction distincts sont impliqués dans le traitement des alarmes d'un réseau électrique, soit le *niveau physique*, le *niveau systémique*, et le *niveau informationnel*. Le niveau physique correspond au propriétés physiques et électriques de l'appareillage du réseau. Par exemple, la surtension d'une ligne de transport ou l'échauffement d'un transformateur sont des phénomènes du niveau physique. De plus, il faut noter que ces phénomènes sont tous de nature continue et ne peuvent donc pas être représentés avec exactitude par un modèle discret. Le niveau systémique comprend tous les mécanismes logiques propres aux systèmes d'alarme et de protection du réseau. Le processus de déclenchement de disjoncteurs suite à une faute dans une zone, ainsi que le procédé de génération de messages d'alarme pour ces évènements se situent au niveau systémique. La nature du niveau systémique est intrinsèquement discrète puisque ce niveau décrit des systèmes basés sur l'opération de relais et de logiciels. Enfin, le niveau informationnel est celui auquel l'opérateur interagit, il correspond aux messages d'alarme reçus et aux commandes exécutées.

Tel qu'illustré sur la figure 4.7, la propagation de perturbations peut se faire au niveau systémique ou au niveau physique. Sur cette figure, le niveau physique est indiqué par des régions ombragées pour souligner sa nature continue, par opposition au caractère discret des autres niveaux. La relation entre deux messages d'alarme peut provenir d'activités systémiques: l'ouverture non-autorisée d'un disjoncteur est effectivement relié de manière systémique à l'alarme de déclenchement de la zone en cause. La figure 4.7a) illustre ce concept et démontre que la relation existant entre un message "A" et un évènement "B" peut provenir exclusivement de la logique de contrôle du niveau systémique.



a) Propagation d'une perturbation au niveau systémique



b) Propagation d'une perturbation au niveau physique

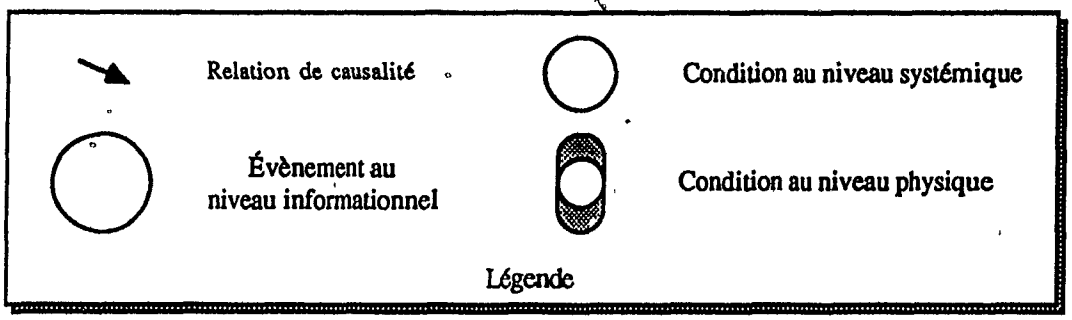
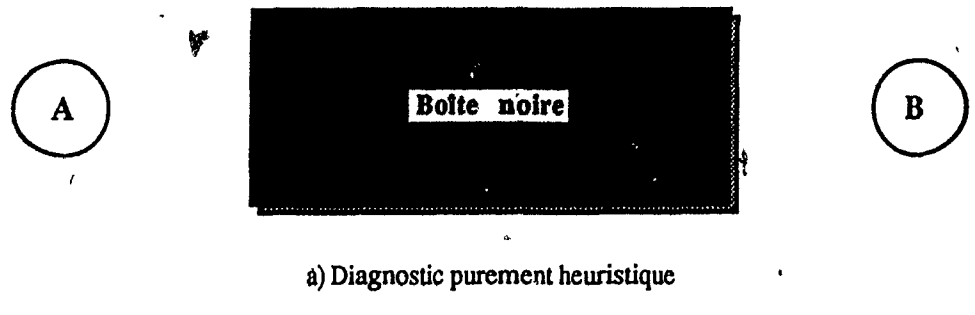


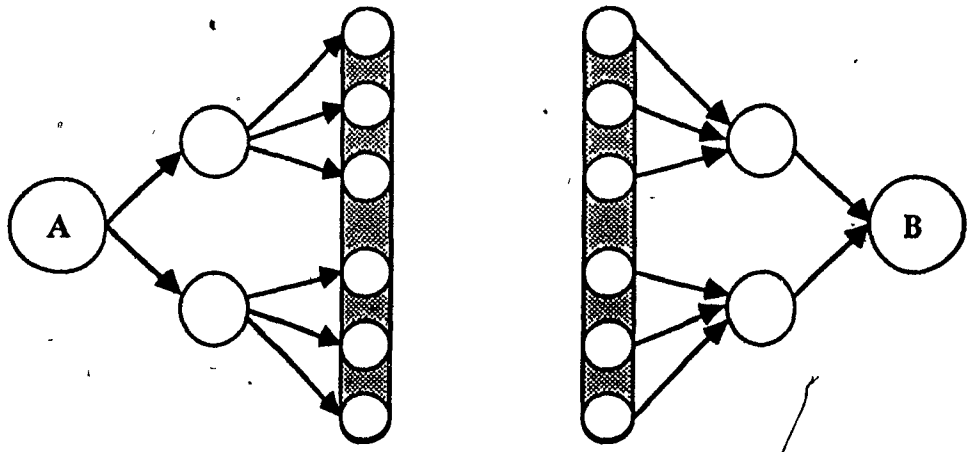
Figure 4.7 Diverses propagations de perturbations dans un réseau électrique

Par contre, l'échauffement d'un transformateur résultant d'une surcharge sur celui-ci exemplifie le caractère physique de certaines propagations, ce phénomène est décrit par la figure 4.7b). Dans cet exemple, la manœuvre "C" occasionne une surcharge qui, après un certain laps de temps, engendre un échauffement, signalé à l'opérateur par l'alarme "D". Bref, les propagations de perturbations dans le réseau électrique peuvent s'expliquer en analysant le fonctionnement des niveaux physique et systémique respectivement. Toutefois, l'analyse des phénomènes physiques est souvent très complexe vu leur nature continue.

Conceptuellement, le diagnostic de pannes peut se faire de deux manières complètement distinctes, soit basé entièrement sur un modèle ou de façon purement heuristique. Tel qu'illustré dans la figure 4.8a), un système expert qui utilise une approche entièrement heuristique n'a aucune notion sur le fonctionnement interne du réseau et de ses systèmes de protection: toute déduction faite quant aux relations possibles entre deux évènements "A" et "B" est basée totalement sur des règles heuristiques, aucune notion sur les niveaux physique et systémique n'est utilisée. À l'antipode, un système de diagnostic basé exclusivement sur un modèle doit être en mesure de modéliser tous les états possibles du réseau électrique. Ce genre de système utilise donc toutes les connaissances relatives à l'opération des niveaux physique et systémique. Idéalement, dans le contexte des réseaux électriques, cette dernière approche est nettement plus intéressante puisqu'elle permet de n'utiliser qu'un nombre limité de règles, peu importe l'ampleur du réseau. Toutefois, tel que mentionné précédemment, il est très difficile de modéliser le fonctionnement entier d'un réseau électrique, vu le caractère continue du niveau physique. Pour ces raisons, tel qu'illustré dans la figure 4.8c), GESTAL est conçu comme un système de diagnostic hybride. Ce système modélise le niveau systémique, à caractère discret, et se sert de techniques heuristiques pour expliquer le fonctionnement complexe du niveau physique.



a) Diagnostic purement heuristique



b) Diagnostic basé exclusivement sur un modèle

c) Diagnostic hybride combinant un modèle avec des techniques heuristiques

Figure 4.8 Approches possibles au diagnostic de pannes dans un réseau électrique

En somme, GESTAL utilise un système hybride pour produire ses diagnostics. Ce système modélise les niveaux systémique et informationnel, tandis qu'il considère le niveau

d'abstraction des phénomènes physiques comme une *boîte noire.* Les relations ayant trait au niveau physique sont produites par des règles heuristiques.

La temporalité des messages d'alarme est un aspect très important du problème de diagnostic des pannes, puisque la continuité du flux d'informations présentées à l'opérateur est intrinsèque au problème même de traitement des alarmes. Les systèmes conçus sans considération pour cette facette du problème sont en mesure d'établir des diagnostics à partir d'une séquence fixe d'évènements seulement. Mais puisque dans un environnement réaliste, l'acquisition de messages d'alarme est un processus continu, ces systèmes doivent alors définir, de façon heuristique et donc incertaine, des fenêtres temporelles fixes dans lesquelles ils peuvent y faire leur analyse. Ce procédé complique davatange la tâche déjà complexe d'interprétation des messages d'alarme. Dans cette optique, une approche différente, tenant compte du flux continu d'informations en jeu, a été prise dans la conception de l'architecture interne de GESTAL. La méthode utilisée consiste en la génération progressive de diagnostics au fur et à mesure que de nouveaux messages d'alarme sont reçus. Cette méthode est expliquée plus en détail dans la prochaine section.

4.3.2 Génération progressive d'arbres à diagnostic

Tel que décrit dans la section 4.2, chaque message d'alarme possible, ainsi que les stimuli et les réactions qui y sont associés, sont inclus dans la taxinomie de GESTAL. Par conséquent, les règles d'analyse du système expert peuvent utiliser le modèle du réseau afin de déduire les conditions de la logique de protection à l'origine de chacune de ces alarmes ainsi que les réactions attendues suite à la réception de ces dernières. C'est ainsi que les règles d'analyse de GESTAL se servent du modèle du réseau pour générer progressivement des *arbres à diagnostic* expliquant le fonctionnement des systèmes d'alarme et de protection lors

d'une perturbation quelconque dans le réseau. Enfin, il est intéressant de noter que les arbres à diagnostic se représentent par des graphes acycliques et directionnels.

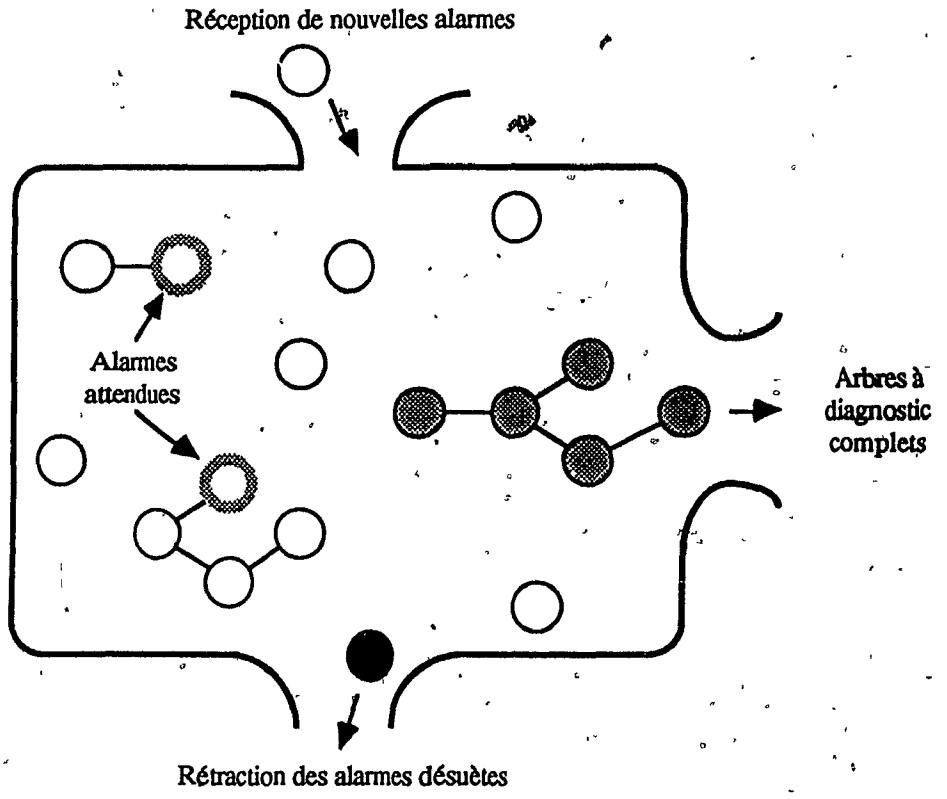


Figure 4.9 Génération progressive d'arbres à diagnostic dans la base de connaissances

Le processus de diagnostic comporte quatre étapes distinctes, soit la définition de *nœuds*, la spécification de relations inter-nodales, l'analyse d'arbres à diagnostic, et la rétraction de nœuds désuets. Chaque alarme reçue est ajoutée à la base de connaissances déclaratives sous la forme d'un nœud. Sommairement, un nœud contient le code de l'alarme, son type, le temps d'arrivée, le temps de traitement, ainsi que de l'information décrivant sa relation avec d'autres nœuds. Un nœud devient désuet après un certain laps de temps, il est alors retiré de la base de connaissances. La base de règles utilise le modèle du réseau afin

d'établir des liens possibles entre les divers nœuds présents dans la base de connaissances. Lors de la réception de certaines alarmes, le système établit des liens avec des nœuds qui n'existent pas encore, dans ces cas, des nœuds temporaires sont créés jusqu'à l'arrivée des alarmes attendues. Si les alarmes attendues ne sont pas reçues dans un intervalle de temps spécifié par le modèle, alors ces nœuds sont traités en conséquence par certaines règles. Lorsqu'un arbre de nœuds est complet, lorsqu'il ne contient plus de nœuds temporaires, cet arbre à diagnostic est retiré de la base de connaissances et traité afin de produire une interprétation de la séquence d'alarmes reçues. Il faut également souligner que plusieurs arbres peuvent être liés ensemble pour former un arbre de plus grande taille. La figure 4.9 illustre sommairement les mécanismes décrits ci-dessus.

4.3.3 Formules prédicatives des nœuds

Cette section décrit de manière plus détaillée la structure interne des nœuds représentant les alarmes dans la base de connaissances déclaratives de GESTAL. Le nœud est en quelque sorte un véhicule abstrait qui permet de représenter divers types de relations entre les alarmes analysées par le système expert. Une description de la formule prédicative typique d'un nœud est donnée dans la figure 4.10.

```
[ Nœud
      [ <alarme> [<type> <temps d'arrivée> <temps de traitement>
                  <liste des parents> <liste des frères> <liste des enfants>
                  <liste d'actions> <information supplémentaire>          ] ]
                ]
```

Figure 4.10 Formule prédicative représentant un nœud

<alarme>: Identifie avec unicité l'alarme en question.

<type>: La base de règles traite les nœuds d'après leur type. Plusieurs types de nœuds sont utilisés par GESTAL, on retrouve entre autres les suivants:

- alarme reçue
- alarme attendue
- changement d'état reçu
- changement d'état attendu
- alarme jamais reçue
- changement d'état jamais reçu

<temps d'arrivée>: Spécifie à quel moment le message a été reçu. Ceci est très important car les relations entre les différent nœuds tiennent compte de la temporalité. En effet, ces relations sont basées sur le modèle des systèmes d'alarme et de protection du réseau, et prennent ainsi en considération la chronologie des évènements dans l'opération de ces systèmes.

<temps de traitement>: Spécifie quand le nœud devra être traité par la base de règles. Cet attribut sert pour les *réactions à retardement* ainsi que pour la rétraction de nœuds qui ne sont plus utiles.

<liste de parents>: Exprime les relations entre le nœud et ceux dont il découle logiquement. Dans un arbre à diagnostic, la *racine* est le seul nœud qui n'a pas de parent.

<liste de frères>: Exprime les relations entre le nœud et d'autres qui ont un ou des stimuli en commun. Parfois, cette liste est également utilisée pour relier des racines de différents arbres de manière heuristique.

<liste des enfants>: Exprime les relations entre le nœud et ceux qui en résultent selon le modèle de la logique de protection.

<liste d'actions>: Décrit l'héritage des actions à retardement reçues des ancêtres du nœud à sa création. À cette liste peut quelquefois s'ajouter les actions à retardement du nœud même.

<information supplémentaire>: Contient soit les stimuli et les réactions dans le cas d'un nœud d'alarme, ou soit le changement d'état pour un nœud du même type.

En somme, chaque nœud, identifié avec unicité par un code d'alarme, contient deux types d'information, soit des *attributs de traitement* et des *attributs de relation.* Les attributs de traitement caractérisent le nœud et sont utilisées par les règles de GESTAL pour construire des arbres à diagnostic. Quant aux attributs de relation, ils spécifient les liens entre les différents nœuds de la base de faits. Ces relations définissent des arbres à diagnostic, graphes directionnels et acycliques qui représentent le noyau des diagnostics produits par GESTAL.

4.3.4 Hiérarchie des règles

Les règles d'analyse de GESTAL sont subdivisées en une hiérarchie à cinq niveaux. Ces règles sont conçues de façon à ce que le système expert puisse être déployé à plus grande échelle sans qu'elles nécessitent de modifications. Ainsi, afin de permettre à GESTAL d'analyser des séquences d'alarmes provenant de postes additionnels, seul le modèle du réseau doit être développé en conséquence. De plus, les règles d'analyse sont généralement assez flexibles pour s'accommoder aux variations possibles entre un réseau électrique et un

autre. Il existe cependant une classe de règles qui dépend du réseau spécifique en cause, ce sont les règles heuristiques utilisées pour traiter le niveau physique du réseau (voir la section 4.3.1). Ainsi, seulement ces règles heuristiques et le modèle du réseau devraient être adaptés pour intégrer GESTAL dans un réseau autre que celui d'Hydro-Québec. La figure 4.11 donne un aperçu de la hiérarchie existant entre les différentes classes de règles.

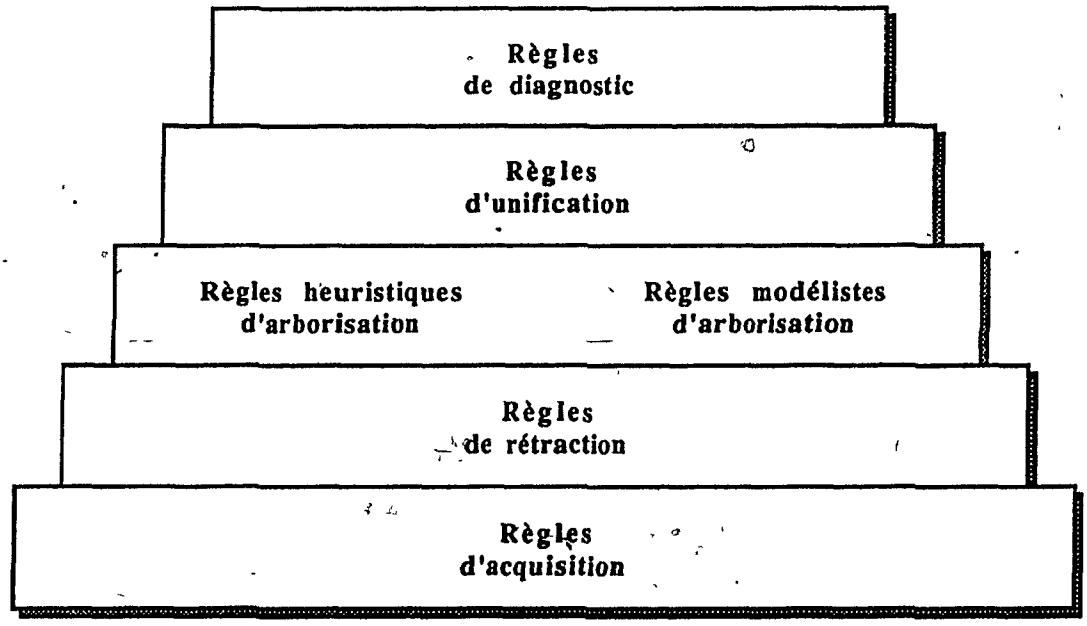


Figure 4.11 Hiérarchie des règles dans GESTAL

Au niveau le plus bas, on retrouve les règles d'acquisition. Ces règles ont comme fonction d'ajouter de nouveaux nœuds à la base de connaissances déclaratives. Donc, si aucune règle d'un niveau supérieur ne peut s'appliquer et si des messages d'alarme attendent dans la *file d'entrée*, une règle d'acquisition ajoute la prochaine alarme à la base de faits. Au niveau suivant, les règles de retraction assurent que les nœuds désuets soient retirés de la base de faits, de manière à garder un nombre limité d'alarmes en *mémoire vive*. Les règles

d'arborisation occupent la salience suivante. À l'aide du modèle ou d'heuristiques, ces règles créent les liens entre les nœuds présents dans la base de connaissances. Ces agrégats ordonnées de nœuds forment des arbres à diagnostic. Les règles d'unification, qui servent entre autres à unifier des alarmes avec leur signal de rappel, ont une priorité plus élevée afin de permettre une production de diagnostics plus rapide. Enfin, les règles de plus haute salience sont les règles de diagnostic; elles sont activées aussitôt qu'un arbre à diagnostic complet est décelé dans la base de faits, et ont comme objet de transformer ces arbres en diagnostics compréhensibles pour l'opérateur.

4.4 Évaluation

4.4.1 Validation du système

Vu la configuration hybride de GESTAL, la vérification du système comporte deux étapes bien distinctes. La première phase consiste en la validation du modèle de réseau et de toutes les règles d'analyse basées sur celui-ci. Tandis que la seconde étape, qui est l'approbation des règles heuristiques, doit se faire par une étude de cas typiques.

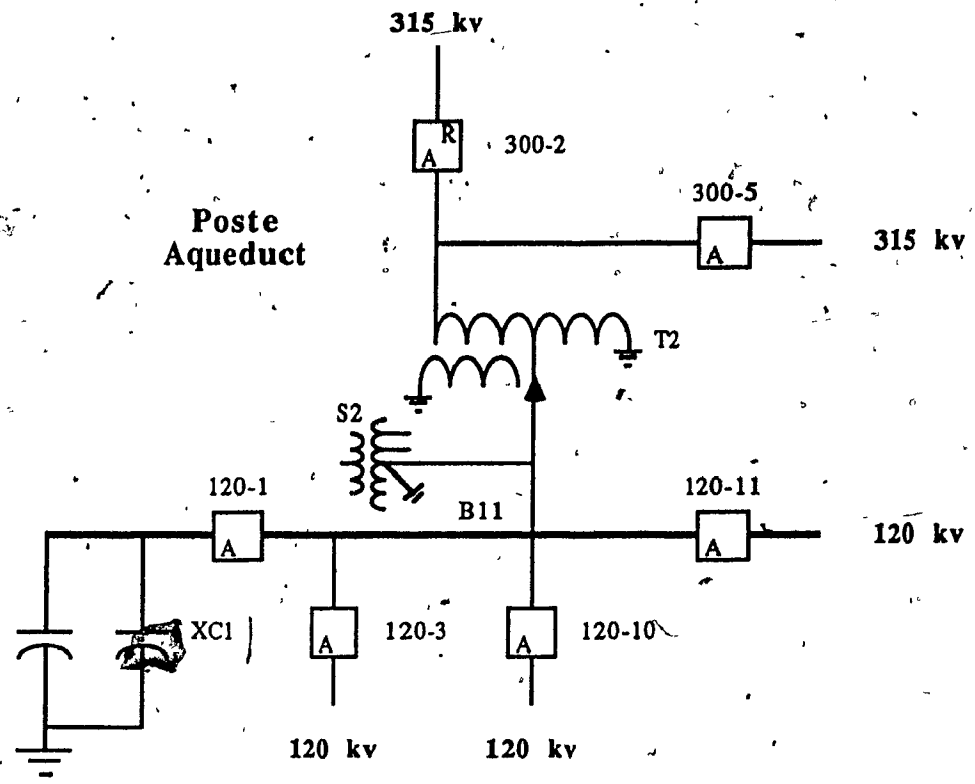
La plus grande partie des diagnostics produits par GESTAL dépend du modèle de réseau inclus dans la base de faits. Les règles qui régissent cette portion du procédé d'analyse sont facilement perfectibles, et ce, de façon permanente. Toutefois, le modèle du réseau nécessite une mise au point beaucoup plus extensive. En effet, les connexions entre les divers composants ainsi que les mécanismes de protection qui leur sont associés doivent être vérifiés de façon exhaustive afin d'assurer des diagnostics cohérents. Puisque le simulateur de réseau est basé sur le même modèle que GESTAL, ce processus de validation peut être grandement

simplifié en utilisant ce simulateur pour vérifier le modèle. Bref, si le simulateur fonctionne convenablement, alors la portion des diagnostics de GESTAL ayant trait au modèle du réseau est assurée d'opérer convenablement.

La base de règles heuristiques nécessite l'usage d'une technique de mise au point plus conventionnelle, soit une étude de cas typiques. GESTAL a donc été soumis à une variété d'essais, où des séquences d'alarmes lui étaient présentées dans le but de recevoir un diagnostic en temps réel. Les diagnostics et les justifications produits par GESTAL ont ensuite été vérifiés afin d'améliorer la capacité analytique de ce dernier. Il faut mentionner que plusieurs de ces listes d'alarmes correspondent à des perturbations déjà encourues dans le réseau d'Hydro-Québec.

4.4.2 Exemple de diagnostic

Cette section présente un exemple du processus de vérification utilisé pour la mise au point de GESTAL. La figure 4.12 illustre une portion du poste de transport Aqueduc ainsi qu'une liste des alarmes qui ont été reçues à la suite d'un défaut de gaz sur le transformateur T2-aqu. La figure 4.13a) affiche deux diagnostics établis par GESTAL lors de la réception de ces alarmes. La figure 4.13b) montre les justifications produites lors de l'analyse pour supporter le premier de ces diagnostics. Enfin, il est bon de rappeler que le modèle du transformateur T2-aqu a déjà été décrit dans la figure 4.6 de la section 4.2.3, traitant de la taxinomie des éléments du réseau.



Date	Heure	Poste	Code	Détails	
18/07/87	18:35:27	Aqueduct	D300-005TC	Non-autorisé Ouvert	
18/07/87	18:35:27	Aqueduct	D300-002TC	Non-autorisé Ouvert	
18/07/87	18:35:27	Aqueduct	D120-003TC	Non-autorisé Ouvert	
18/07/87	18:35:27	Aqueduct	D120-011TC	Non-autorisé Ouvert	
18/07/87	18:35:27	Aqueduct	D120-010TC	Non-autorisé Ouvert	
18/07/87	18:35:27	Aqueduct	T2.....63	Accuml gaz T-2	N
18/07/87	18:35:27	Aqueduct	T2@..94-2*	Décl surint gaz T-2 & gaz S-2	N
18/07/87	18:35:27	Aqueduct	S2@.....27	Pert tens S-2 & S-3	N
18/07/87	18:35:27	Aqueduct	T2@.RT..74	Cond anorm temp & niv huile S-3	N
18/07/87	18:35:27	Aqueduct	D300...../	Discord phase disj 300kv	N
18/07/87	18:35:27	Aqueduct	D300...../	Discord phase disj 300kv	R
18/07/87	18:35:27	Aqueduct	SA.....64	Mise à la terre serv aux.	N
18/07/87	18:35:27	Aqueduct	SA.....27	Bas tens serv aux.	N
18/07/87	18:35:27	Aqueduct	CH.....74	Cond anorm bas & haute tens char	N
18/07/87	18:35:27	Aqueduct	CP....HUM	Humid. pref. & sécheur CP1 & 2	N
18/07/87	18:35:27	Aqueduct	300-5....<	Bas pres air disj. 300-5	N
18/07/87	18:35:30	Aqueduct	T2@.RT..74	Cond anorm temp & niv huile S-3	R
18/07/87	18:35:30	Aqueduct	SA.....64	Mise à la terre serv aux.	R
18/07/87	18:35:30	Aqueduct	SA.....27	Bas tens serv aux.	R
18/07/87	18:35:30	Aqueduct	CH.....74	Cond anorm bas & haute tens char	R
18/07/87	18:35:30	Aqueduct	CP.....HUM	Humid. pref. & sécheur CP1 & 2	R
18/07/87	18:35:36	Aqueduct	T2@..94-2*	Décl surint gaz T-2 & gaz S-2	R
18/07/87	18:36:11	Aqueduct	300-5....<	Bas pres air disj. 300-5	R
18/07/87	18:36:25	Aqueduct	T2.....63	Accuml gaz T-2	R

Figure 4.12 Liste d'alarmes reçues à la suite d'un défaut de gaz sur T2-aqu

```
* Diagnostic * :  18 07 87   18:35:27        Element : T2-aqu

Faute: T2@..94-2* ===> Accumulation critique de gaz
   Faute associée: T2.....63 ===> Accumulation critique de gaz sur T2-aqu

Protection de T2-aqu opère avec complication(s).
   Complication: l'élément 120-1-aqu ne s'ouvre pas.
État résultant de T2-aqu: hors tension.
```

```
* Diagnostic * :  18 07 87   18:35:27        Element : T2-aqu

Faute: T2.....63 ===> Accumulation critique de gaz
   Faute associée: T2@..94-2* ===> Accumulation critique de gaz sur T2-aqu

État résultant de T2-aqu: hors tension.
```

a) Diagnostics d'une faute de gaz sur le transformateur T2-aqu

```
* Justification * :  18 07 87   18:35:27        Element : T2-aqu

                          Surintensité
                          Température critique
Faute: T2@..94-2* ===>    Accumulation critique de gaz
                          Gaz dans tranformateur auxiliaire

   Faute associée: T2.....63 ===> Accumulation critique de gaz
                                  Présence de gaz

18/07/87 18:35:27      T2@..94-2* reçu.
  18/07/87 18:35:27      D120-003TC reçu.
  18/07/87 18:35:27      D120-001TC n'a pas été reçu.
  18/07/87 18:35:27      D120-011TC reçu.
  18/07/87 18:35:27      D120-010TC reçu.
  18/07/87 18:35:27      D300-005TC reçu.
  18/07/87 18:35:27      D300-002TC reçu.

État résultant de T2-aqu: hors tension.
```

b) Justification du diagnostic T2@..94-2*

Figure 4.13 Exemples de diagnostics et de justifications

Les cinq premières alarmes de la séquence identifient le déclenchement de disjoncteurs. Parmi les alarmes subséquentes, celles dont le message se termine par un "N" représentent de nouvelles conditions d'alarme, tandis que celles finissant par un "R" expriment le retour à des conditions normales. Il faut noter qu'une grande partie des messages reçus sont le résultat du déclenchement des disjoncteurs, alors que seulement quelques-uns en identifient la cause. Lors de la réception d'une telle séquence d'alarmes, l'opérateur doit d'abord déterminer la cause de la perturbation et puis voir si le défaut est isolé correctement, c'est seulement alors qu'il est en mesure d'effectuer les manœuvres correctives nécessaires. Tel qu'illustré sur la figure 4.13a), GESTAL a produit deux diagnostics afin d'interpréter cette séquence d'alarmes. Le premier identifie l'alarme ("T2@..94-2*") et le défaut qui a causé le déclenchement des disjoncteurs de la zone de protection du transformateur. Ce diagnostic signale également que même si le disjoncteur 120-1 n'a pas déclenché tel que prévu, le transformateur en panne a toutefois été isolé. Dans ce cas-ci, GESTAL parvient à identifier avec exactitude la cause de la panne en associant cette perturbation à une autre alarme reçue pendant la panne, soit l'alarme "T2.....63" indiquant un défaut de gaz. La figure 4.13b) démontre plus clairement ce concept de fautes associées. Bref, cet exemple illustre comment GESTAL interprète les alarmes et fournit à l'opérateur l'information dont il a besoin pour effectuer les manœuvres appropriées en temps voulu.

4.4.3 Performances

Plusieurs essais similaires à celui présenté précédemment ont été faits sur GESTAL en labotatoire, et dans chaque cas, ce dernier a produit des diagnostics adéquats. La prochaine étape d'évaluation consisterait donc en l'implantation d'un prototype dans l'environnement de travail même des opérateurs, soit dans un centre de contrôle de réseau électrique. Ceci permettrait d'éprouver sérieusement la robustesse de l'architecture choisi. De

plus, les prédictions théoriques, relatives au temps de réponse de GESTAL versus l'ampleur du réseau électrique contrôlé, pourraient être vérifiées.

4.5 Sommaire

Le fonctionnement *automatique* et le traitement des messages en *temps réel* constituent deux caractéristiques fondamentales à tout système de gestion d'alarmes pour un réseau électrique. GESTAL est un système expert qui répond à ces objectifs en utilisant une base de connaissances déclaratives contenant un modèle des systèmes d'alarme et de protection, ainsi qu'une base de règles spécifiant une technique d'analyse par construction d'arbres à diagnostic. Il produit des diagnostics qui identifient les éléments et leur(s) défauts, ainsi que les systèmes d'alarme ou de protection ayant opérés.

Le modèle du réseau représente les mécanismes de génération d'alarmes et de fonctionnement des systèmes de protection en utilisant un *paradigme de stimulus-réaction.* Le modèle de chaque élément du réseau comprend une liste des messages d'alarme qui peuvent l'affecter, et pour chacune de ces alarmes, une énumération des causes et des effets reliés à son activation. Cette approche fournit une *méthode normalisée et systématique* pour modéliser les connaissances relatives aux systèmes d'alarme et de protection du réseau.

La base de connaissances procédurales contient des règles d'analyse basées sur la philosophie générale du fonctionnement des systèmes d'alarme et de protection du réseau électrique. Le caractère temporel du processus d'interprétation, qui résulte du flux continuel d'évènements présentés aux consoles de l'opérateur, est intégré sous forme d'*arbres à diagnostic*. GESTAL produit progressivement des arbres à diagnostic pour expliquer le

fonctionnement des systèmes d'alarme et de protection lors de la réception de messages d'alarme.

Enfin, l'évaluation de GESTAL en laboratoire a permis premièrement, de valider certains concepts nouveaux quant au traitement des alarmes dans un réseau électrique, et en second lieu, de démontrer la faisabilité d'intégrer un tel système expert dans un centre de contrôle de réseau.

Conclusion

Cette thèse a présenté GESTAL, un système expert pour la gestion en temps réel des messages d'alarme reçus dans un centre de contrôle de réseau électrique. Ce système expert a été conçu pour seconder les opérateurs dans l'analyse de séquences d'alarmes générées lors de perturbations dans le réseau. La base de connaissances de GESTAL a été configurée de façon à clairement séparer les connaissances requises sous la forme d'un modèle de réseau et de règles décrivant le processus d'analyse.

Une taxinomie des composants et un paradigme de stimulus-réaction ont permi d'élaborer un modèle de réseau représentant de façon explicite la structure des systèmes d'alarme et de protection. Une méthodologie a donc été développée pour extraire l'information pertinente des schémas synoptiques du réseau et la représenter dans la base de connaissances de GESTAL. Par conséquent, le modèle de réseau peut facilement être déployé à plus grande échelle, pour ainsi permettre l'analyse de messages d'alarme provenant de plusieurs postes. De plus, il n'est pas nécessaire de re-vérifier la base de règles lors de l'intégration du modèle de chacun de ces postes, seul leur modèle doit être validé, et cela peut se faire rapidement en utilisant le simulateur de réseau [Arès,1987].

La base de règles de GESTAL a été conçue de façon à combiner une technique d'analyse basée strictement sur les caractéristiques fonctionnelles des systèmes d'alarme et de

protection, avec une technique d'analyse fondée sur les règles heuristiques utilisées par les spécialistes en comportement de réseau. Cette approche a permis d'exploiter les avantages de ces deux techniques d'analyse afin d'établir des diagnostics fiables, et de justifier ces derniers par les alarmes principales qui leur correspondent. De plus, la technique d'analyse par arbres à diagnostic a résolu de façon élégante le problème fondamental de la génération de diagnostics à partir d'un flux continu d'alarmes. Plus particulièrement, la construction graduelle des arbres à diagnostic, lors de la réception d'alarmes, permet d'analyser des séquences d'alarmes sans devoir intégrer de mécanismes complexes pour sectionner le flot d'alarmes en sequences de dimensions fixes. Finalement, les règles ont été conçues de façon à ce que le modèle du réseau puisse être déployé à grande échelle sans pour autant affecter le temps de réponse de GESTAL.

En somme, l'architecture et les stratégies d'inférence de GESTAL offrent des avantages majeurs par rapport à d'autres systèmes de gestion d'alarmes, notamment en termes d'acquisition de connaissances, de vérification, de temps de réponse, et enfin d'expansion du système.

Travaux futurs

GESTAL, le logiciel de gestion d'alarmes décrit dans cette thèse ainsi que le simulateur présenté dans [Arès, 1987] sont tous deux des prototypes de systèmes experts qui pourraient éventuellement être déployés à l'échelle d'un réseau électrique entier. Le modèle de réseau présentement intégré se compose de deux postes avec leurs lignes de transport associées. La prochaine phase de développement possible pour ces systèmes serait de déployer le modèle de réseau à plus grande échelle et de raffiner les bases de règles du simulateur et de GESTAL.

Le modèle du réseau pourrait aussi être utilisé pour développer d'autres systèmes experts. Notamment, un *vérificateur de manœuvres* ainsi qu'un *planificateur de manœuvres* pourraient être développés basés sur ce modèle. Le vérificateur de manœuvres analyserait les manœuvres suggérées par les opérateurs du centre de contrôle afin de déterminer si elles respectent les contraintes d'opération ou de charge du réseau. D'autre part, le planificateur de manœuvres suggérerait des plans d'actions pour rétablir des conditions d'opération normales à la suite de pertes de charge dans le réseau.

Enfin, les techniques de diagnostic utilisées avec succès par GESTAL pourraient être employées pour solutionner des problèmes d'interprétation en temps réel dans d'autres domaines de l'ingénierie. En l'occurrence, le traitement d'alarmes dans les centrales nucléaires constitue une application très prometteuse pour le type de système présenté dans cette thèse.

Références

Amelink, H., Forte, A.M., Guberman, R.P. 1986, *Dispatcher Alarm and Message Processing*. IEEE Trans. on Power Systems, Bol. PWRS-1, No. 3, August, 1986, pp188-194.

Arès, J-M., *A Knowledge-based Model and Simulator for Alarm and Protection Systems of Power Networks*, Department of Electrical Engineering, McGill University, Montréal, Canada, 1987.

Clayton, B.D. 1986, *ART Programming Tutorial, Volumes one, two, and three.* Inference Corporation, Los Angeles, CA.

Daniel, H.A., Mayur, N. 1985, *More than Mainframes.* IEEE Spectrum, August, 1985, pp 54-61.

De Mori, R. 1986, *Expert Systems.* Course Notes, McGill University, School of Computer Science, Montréal, Canada.

Doyle, J. 1979, *A Truth Maintenance System.* Artificial Intelligence Journal, Vol. 12, No. 3, pp 231-272.

EPRI 1985, Power Plant Alarm Systems: *A Survey and Recommended Approach for Evaluating Improvements.* EPRI Research Project 2011, Palo Alto, CA.

EPRI 1986, *Artificial Intelligence Technologies for Power System Operations.* EPRI Research Project 1999-7, Palo Alto, CA.

Evans, J.W. 1987, *Survey of EMS Architectures.* Conference Proceedings: PICA 1987, pp 274-281.

Faught, W.S. 1986, *Applications of AI in Engineering.* IEEE Computer, July 1986, pp 53-60.

Fujiwara, R., et al. 1986, *An Intelligent Load Flow Engine for Power System Planning.* IEEE Software, March 1986, pp 26-37.

Fukui, C., Kawakami, J. 1986, *An Expert System for Fault Section Estimation Using Information from Protective Relays and Circuit Breakers.* IEEE Trans. on Power Delivery, Vol. PWRD-1, No. 4, October 1986, pp 83-90.

Gervarter, W.B. 1987, *The Nature and Evaluation of Commercial Expert System Building Tools.* IEEE Computers, May 1987, pp 24-41.

Goyal, S.K. et al. 1985, *COMPASS: An Expert System for Telephone Switch Maintenance.* Expert Systems, Vol 2, No. 3, July 1985, pp 112-126.

Harmon, P., King, D. 1985, *Artificial Intelligence in Business: Expert Sytems,* New York, NY: John Wiley & Sons.

Hayes-Roth, F., Waterman, D.A., Lenat, D.B. 1983, *Building Expert Systems*, Reading, Mass.: Addison-Wesley.

Hébert, R. 1986, *Fonction "traitement des alarmes" dans un C.E.R.*, Hydro-Québec, Division technique d'exploitation, Service G.R.A.T., Région Maisonneuve.

Horton, J.S. et al. 1985, *Advances in Energy Management Systems*. Conference Proceedings: PICA 1985, pp 70-78.

Hydro-Québec 1973, *Cours 501: Initiation à la Protection (Volumes 1 et 2).*

Hydro-Québec 1984, *Centre de conduite du réseau d'Hydro-Québec.*

IEEE Tutorial Course 1981, *Fundamental of Supervisory Control Sytstems*. IEEE Publications, Piscataway, NJ.

Inference Corporation 1987, *The ART Reference Manual*. Inference Corporation, Los Angeles CA.

Intellicorp 1984, *The Knowledge Engineering Environment.* Intellicorp: Knowledge Sytstems Division, Menlo Park, CA.

Johnson, P.E. 1983, *The expert mind: a new challenge for the information scientist.* Bemelman's Th. M.A. (Ed.) Beyond Productivity, North Holland Publishing Company, The Netherlands.

Laffey, T.J., Perkins, W.A., Nguyen, T.A. 1986, Reasoning About Fault Diagnosis with LES. IEEE Expert, Spring 1986, pp 13-20.

Liu, C.C., Tomsovic, K. 1985, An Expert System Assisting Decision-Making of Reactive Power/Voltage Control. IEEE Trans. on Power Systems, Vol. PWRS-1, No. 3, August 1986, pp195-201.

Manna, Z., Waldinger, R. 1985, *The Logic Basis for Computer Programming*. Reading, Mass.: Addison-Wesley.

Masiello, R.D. 1985, *Computers in Power: a Welcome Invader.* IEEE Spectrum, Febuary 1985, pp 51-57.

McDermott, J. 1982, *R1: A Rule-Based Configurer of Computer Systems.* Artificial Intelligence Journal, Vol. 19, pp 39-88.

Minsky, M. 1975, *A Framework for Representing Knowledge,* P.Winston (Ed.), The Psychology of Computer Vision, McGraw-Hill.

Mooney, H.P. 1987, *A Complete Relational DBMS for an EMS Product.* Conference Proceedings: PICA 1987, pp 289-293.

Moore, R.L. 1984, *A Real-Time Expert System for Process Control.* Proceedings: 1st Conference on Artificial Intelligence Applications, Denver, Colorado, pp 569-576.

Murphy, T.E. 1985, *Developing Expert Systems Applications for Process Control.* Proceedings: ISA International Conference, October 1985, Philadelphia, Pen., pp 533-541.

Negoita, C.V. 1985, *Expert Systems and Fuzzy Systems,* Menlo Park, CA: Benjamin/Cummings.

O'Connor, D.E. 1984, *The Learning Curve for Building Large Expert Systems.* Proceedings: CAM-I, 13th Annual Meeting and Technical Conference, Clearwater Beach, FL., pp 19-30.

Quillan, R. 1968, *Semantic Memory.* Semantic Information Processing, M. Minsky (Ed.), MIT Press, Cambridge Mass.

Ramamoorthy, C.V. et al. 1984, *Software Engineering: Problems and Perspectives.* IEEE Computers, October 1984, Vol. 17, No. 10, pp 191-209.

Ramamoorthy, C.V., Shekhar, S., Garg, V. 1987, *Software Development Support for AI Programs.* IEEE Computer, January 1987, pp30-40.

Rich, E. 1983, *Artificial Intelligence,* New York, NY: McGraw-Hill.

Sakaguchi, T., Matsumoto, K. 1983, *Development of a Knowledge-Based System for Power System Restoration.* IEEE Transactions on Power Apparatus and Systems, Vol. PAS-102, No. 2, Febuary 1983, pp 320-329.

Schor, M.I. 1986, *Declarative Knowledge Programming: Better than Procedural ?*. IEEE Expert, Spring 1986, pp 36-43.

Sobajic, D.J., Pao, V.H. 1987, *An Arfificial Intelligence System for Power System Contingency Screening*. Conference Proceedings: PICA 1987, pp 107-113.

Talukdar, S.N., Cardozo, E., Leào, L.V. 1986, *Toast: The Power System Operator's Assistant*. IEEE Computer, July 1986, pp 53-60.

Talukdar, S.N., Cardozo, E. 1987, *A Distributed Expert System for Fault Diagnosis*. Conference Proceedings: PICA 1987, pp 101-106.

Wallich, P. 1986, *Software "doctor" prescribes remedies*. IEEE Spectrum, October 1986, pp 43-48.

Waterman, D.A. 1985, *A Guide to Expert Systems*, Reading, Mass.: Addison-Wesley.

Williams, C. 1986, *Expert Systems, Knowledge Engineering, and AI Tools - An Overview*. IEEE Expert, Winter 1986, pp 66-70.

Winston, P.H. 1984, *Artificial Intelligence*, Reading, Mass.: Addison-Wesley.

Wollenberg, B.F., et al. 1986, *Artificial Intelligence Solutions to Power System Operating Problems*, IEEE 1986 Summer Meetin, Mexico City, Mexico, July 20-25, 1986.

Wollenberg, B.F. 1985, *Feasibility Study for an Energy Management System Intelligent Alarm Processor.* IEEE Trans. on Power Systems, Vol. PWRS-1, No. 2, May 1986, pp 241-247.

Zualkernan, I., Tsai, W.T., Volovik, D. 1986, *Expert Systems and Software Engineering: Ready for Marriage ?.* IEEE Expert, Winter 1986, pp 24-31.