

Génération de plans de reprise de service pour les réseaux de distribution d'EDF

Sylvie Thiébaux, Marie-Odile Cordier, Olivier Jehl, Jean-Paul Krivine

► **To cite this version:**

Sylvie Thiébaux, Marie-Odile Cordier, Olivier Jehl, Jean-Paul Krivine. Génération de plans de reprise de service pour les réseaux de distribution d'EDF. [Rapport de recherche] RR-3006, INRIA. 1996. inria-00073689

HAL Id: inria-00073689

<https://hal.inria.fr/inria-00073689>

Submitted on 24 May 2006

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

***Génération de plans de reprise de service pour les réseaux
de distribution d'EDF***

Sylvie Thiébaux, Marie-Odile Cordier,
Olivier Jehl et Jean-Paul Krivine

N° 3006

Octobre 96

_____ THÈME 3 _____



***rapport
de recherche***

Génération de plans de reprise de service pour les réseaux de distribution d'EDF*

Sylvie Thiébaux,[†] Marie-Odile Cordier,[†]
Olivier Jehl[‡] et Jean-Paul Krivine[‡]

Thème 3 — Interaction homme-machine,
images, données, connaissances
Projet Repco

Rapport de recherche n° 3006 — Octobre 96 — 82 pages

Résumé : Ce document est le rapport final d'un Contrat d'Etude Recherche et Développement conclu entre l'IRISA et EDF sur la génération de plans de reprise de service pour les réseaux de distribution d'électricité. L'objet du CERD est d'étudier l'apport de travaux récents en planification sous incertitude (notamment ceux effectués à l'IRISA) et dans une moindre mesure en intégration des réparations au diagnostic basé sur les modèles. Le rapport présente, de façon synthétique puis détaillée, le contexte et les objectifs des recherches, les travaux étudiés en planification sous incertitude et en diagnostic et réparations, les expérimentations effectuées avec le planificateur PASCALÉ développé à l'IRISA, les apports du prototype construit dans le cadre du CERD, et les directions qui devraient être poursuivies par une étude complémentaire visant à améliorer le prototype de façon substantielle.

Mots-clé : réseaux de distribution d'électricité, reprise de service, planification d'actions, diagnostic et réparations basés sur les modèles, actions stochastiques, observabilité partielle.

(Abstract: pto)

* Ce rapport est aussi paru en note interne EDF no HR37/96010.

[†] IRISA, e-mail: Prenom.Nom@irisa.fr

[‡] EDF DER MOS, 1 av. du Général de Gaulle, 92141 Clamart cedex, e-mail: Prenom.Nom@der.edf.gdf.fr

Generating Restoration Plans for EDF Power Distribution Systems

Abstract: This is the final report of a contract between IRISA and EDF on generating restoration plans for power distribution systems. The purpose of this contract is to study the adequation of recent works on planning under uncertainty (particularly work done at IRISA) and to a smaller extent on integrating model-based diagnosis and repair. This report presents, both synthetically and in detail, the context and objectives of the study, the works on planning under uncertainty and on diagnosis and repair considered, the experiments carried out with the PASCAL planner developed at IRISA, the prototype built in the framework of the contract, and the directions which should be followed in order to substantially improve the performances and functionalities of the prototype.

Key-words: power distribution systems, power restoration, action planning, model-based diagnosis and repair, stochastic actions, partial observability.

Table des matières

1 Bilan du CERD	7
1.1 Contexte et objectifs de l'étude	7
1.2 Travaux étudiés	8
1.3 Expérimentations réalisées avec PASCALE	9
1.4 Le prototype construit	10
1.5 Perspectives	11
A Contexte et objectifs de l'étude	13
A.1 Le problème de la reprise de service	13
A.1.1 Réseaux, incidents, et réalimentation	13
A.1.2 Localisation des portions fautives	14
A.1.3 Réalimentation des portions non-fautives	15
A.2 Principales difficultés du problème	15
A.3 L'existant : la maquette AUSTRAL	17
A.4 Objectifs de l'étude	18
B Travaux étudiés	19
B.1 Planification sous incertitude	19
B.1.1 Environnements stochastiques partiellement observables	19
B.1.2 Environnements stochastiques totalement observables	20
B.2 Diagnostic et réparation basés sur les modèles	21
B.2.1 Plans entrelaçant observations et réparations	21
B.2.2 IRS	22
B.3 Choix effectués suite à cette étude	23
C Expérimentations réalisées avec PASCALE	25
C.1 PASCALE	25
C.1.1 Un planificateur à portée générale pour ESTO	25
C.1.2 Modélisation de l'environnement et des actions	26
C.1.3 Modélisation des plans	29
C.1.4 Génération des plans	31
C.1.5 Mise en œuvre de PASCALE	35
C.2 Sur le choix de PASCALE pour les expérimentations	35
C.3 Modélisation du problème dans PASCALE	37
C.3.1 Contraintes d'intégrité	37
C.3.2 Situations	40
C.3.3 Contraintes probabilistes	41
C.3.4 Actions	43
C.3.5 Objectifs	44

C.4	Exemple de plan généré	45
C.5	L'estimateur d'état	45
C.6	Résultats des expérimentations et conclusions	49
D	Le prototype construit	51
D.1	L'estimateur d'état	52
D.1.1	Calcul de la distribution de probabilité initiale	52
D.1.2	Mise à jour et révision de la distribution	53
D.1.3	Quand change-t-on le plan?	55
D.2	Le planificateur	55
D.3	Exemple de session	57
D.4	Résultats obtenus et conclusions	59
E	Manuel utilisateur du prototype	61
E.1	Installation et chargement du prototype	61
E.1.1	Contenu de la distribution	61
E.1.2	Chargement du prototype	61
E.1.3	Installation à partir des fichiers sources	62
E.2	Schéma nominal d'un réseau	62
E.2.1	Chargement d'un schéma	62
E.2.2	Description des organes	62
E.2.3	Description des multipoles	63
E.2.4	Donnée du schéma nominal	64
E.3	Modifications possibles du schéma nominal	64
E.3.1	Modes de fonctionnements	64
E.3.2	Positions	64
E.3.3	Puissances maximales des disjoncteurs	65
E.3.4	Défauts	65
E.3.5	Puissances sur les multipoles	65
E.3.6	Clients sensibles	65
E.3.7	Requêtes sur l'état du réseau	66
E.4	Reprise	66
E.4.1	Modes manuel et télécommandé	66
E.4.2	Mode anomalies	67
E.5	Changement de paramètres pour la reprise	68
E.5.1	Combinaison des critères d'évaluation	68
E.5.2	Probabilités	69
F	Sessions tests	71
F.1	Trois reprises successives	71
F.1.1	Deux défauts sur un même départ	71

F.1.2	Problème pour lequel la maquette AUSTRAL fait mieux	71
F.1.3	Un défaut sur deux départs adjacents	73
F.2	Défaut unique alimenté par plusieurs disjoncteurs	73
F.3	Deux défauts sur deux départs adjacents	77
F.4	Un contre-exemple	77

1 Bilan du CERD

Ce document est le rapport final d'un Contrat d'Etude Recherche et Developpement conclu entre l'IRISA et EDF sur la génération de plans de reprise de service pour les réseaux de distribution d'électricité. L'objectif du CERD est d'étudier l'apport de travaux récents en planification sous incertitude (notamment ceux effectués à l'IRISA) et dans une moindre mesure en intégration des réparations au diagnostic basé sur les modèles. Le rapport présente tout d'abord un bref bilan de l'étude, qui résume successivement son contexte et ses objectifs, les travaux étudiés en planification sous incertitude et en diagnostic et réparations, les expérimentations effectuées avec le planificateur PASCALÉ développé à l'IRISA, les apports du prototype construit dans le cadre du CERD, et les directions qui devraient être poursuivies par une étude complémentaire visant à améliorer le prototype de façon substantielle.

Ce bilan est complété par des annexes techniques en partie basées sur les rapports précédents du CERD, qui reprennent en détail chacun des éléments du bilan et qui permettront au lecteur d'approfondir les points de son choix.

1.1 Contexte et objectifs de l'étude

Le contexte de cette étude (voir le premier rapport du CERD [Jehl et al.94] et l'annexe A de ce rapport) est la reprise de service suite à un incident entraînant la perte d'un ou plusieurs départs HTA sur les réseaux de distribution d'EDF. Il s'agit de localiser les portions fautives grâce aux télésignalisations de défaut (TSD) situées sur les organes de coupures du réseau, et d'élaborer un plan de reprise constitué d'ordres de fermeture et d'ouverture d'organes, qui isole les portions fautives et redirige le courant produit par les départs adjacents vers les portions non-fautives. Les plans produits doivent être admissibles, i.e., ne pas dépasser les intensités maximales des disjoncteurs alimentant les départs, ni celles pouvant circuler sur les lignes. De plus, certains paramètres doivent idéalement être optimisés, comme le nombre de clients réalimentés (en donnant priorités aux clients sensibles), le nombre de manœuvres (de manière à ne pas trop s'éloigner du schéma normal d'exploitation), et l'équilibrage des marges des départs en prévision de la prochaine heure de pointe.

Deux facteurs compliquent la reprise et son automatisation. Le premier est l'indéterminisme des manœuvres d'organes. En effet, l'organe ou sa télécommande (TC) peuvent tomber en panne et la manœuvre n'est alors pas exécutée. Le second est l'observabilité partielle de l'état du réseau en cours de reprise. En effet, la localisation des portions fautives est incertaine, car les TSD peuvent ne pas transmettre d'indication, et même transmettre une indication contraire à la réalité. De plus, les positions des organes manœuvrés ne sont pas connues avec certitude car (1) la TC de l'organe peut acquiescer positivement un ordre alors que celui-ci n'a pas été exécuté, et (2) l'incertitude quant au bon fonctionnement de la manœuvre ne peut pas toujours être levée car la télésignalisation de position (TSP) de l'organe peut ne pas transmettre d'information.

Ces deux facteurs ont les conséquences suivantes. Premièrement, l'espace des hypothèses possibles sur l'état du réseau est gigantesque, et donc difficile à gérer de façon systématique et exhaustive. Deuxièmement, un plan de reprise peut échouer en raison d'une mauvaise localisation du défaut ou de l'échec d'une manœuvre. Par échec, nous entendons que l'exécution du plan ne se déroule pas comme prévue. Les conséquences d'un tel échec peuvent être multiples (manœuvres inutiles, perte momentanée de départs supplémentaires ...) et entraînent un certain coût (ou risque). L'évaluation d'un plan devrait donc idéalement prendre en compte tous

ces risques (c'est à dire le coût entraîné par tous les échecs possibles), et au minimum, le plan en cours d'exécution devrait être révisé dès qu'un échec est détecté.

Ces conséquences rendent difficile la conception d'un système de reprise s'appuyant sur un modèle des réseaux de distribution. EDF a construit la maquette AUSTRAL, un système mixte, intégrant un modèle des réseaux (pour la localisation du défaut, et la vérification de l'admissibilité des plans) et un système expert (pour la sélection/évaluation d'un plan, et la gestion des hypothèses sur l'état du réseau en cours de reprise) [Bredillet et al.94]. Le raisonnement hypothétique du système expert n'était pas systématique, puisqu'un échec du plan courant se soldait par la simple révision de l'hypothèse de localisation du défaut, ou encore par un pur abandon de la reprise (les ordres effectués étaient défaits de manière à se ramener à la configuration avant incident). D'autre part, la maquette était limitée à une faute unique, et l'évaluation des plans ne prenait pas en compte les risques d'échec.

L'objectif du CERD était donc d'étudier les développements récents dans les domaines de la planification sous incertitude, et dans une moindre mesure de l'intégration des réparations au diagnostic basé sur les modèles, qui pourraient permettre de remédier à certaines des limites de la maquette AUSTRAL.

1.2 Travaux étudiés

Nous avons principalement étudié trois types de travaux (voir l'annexe B de ce rapport). Dans le domaine de la planification sous incertitude, notre intérêt s'est tout d'abord porté sur la planification pour environnements stochastiques partiellement observables. Ces environnements sont caractérisés par (1) des actions stochastiques (i.e., dont les effets sont probabilistes) qui amènent de l'information tout en modifiant l'état de l'environnement, et (2) une connaissance incertaine de l'état de l'environnement à tout moment, matérialisée par une distribution de probabilité sur les états. Le but de la planification est de construire une fonction (un plan) associant l'information-capteur à la prochaine action à exécuter. Cette fonction maximise certains critères représentés par une fonction d'utilité, en tenant compte des risques. Il est clair que la reprise de service est typiquement un problème de planification pour environnements stochastiques partiellement observables.

Il existe deux types de travaux sur ces environnements. Le premier est basé sur les techniques de la recherche opérationnelle pour la résolution de processus de décision Markoviens partiellement observables (PDMPO) [Cassandra et al.94]. Nos conclusions sont que le modèle des PDMPO est complètement adéquat pour encoder le problème de la reprise, mais que les algorithmes de résolution sont encore beaucoup trop complexes pour être de quelque utilité. En effet, ils sont limités à des problèmes d'une centaine d'états, donc à des réseaux comportant entre 1 et 2 organes! Le deuxième type de travaux est basé sur une extension des algorithmes de planification classiques aux actions stochastiques amenant de l'information [Draper et al.94]. Nos conclusions sont que ce cadre n'est pas assez expressif pour les besoins de la reprise de service. D'une part, il nécessiterait des descriptions d'actions de taille exponentielle en le nombre d'organes, et d'autre part, que l'on se limite à évaluer les plans en terme de leur probabilité de satisfaction d'un objectif décrit par une formule logique (dont nous ne disposons évidemment pas, à moins de savoir à l'avance quelles lignes peuvent être réalimentées).

Etant données ces difficultés, notre attention s'est alors portée sur les travaux en planification pour des environnements stochastiques totalement observables, notamment ceux effectués l'IRISA [Thiébaux95]. Contrairement à l'état d'un environnement partiellement observable, ce-

lui d'un environnement totalement observable n'est inconnu que lors de la planification, mais à l'exécution du plan, on suppose que l'on peut tout observer. Ainsi, les actions sont toujours stochastiques mais n'amènent pas d'information (celle-ci étant supposée disponible à l'exécution), et le planificateur produit une fonction (un plan) associant l'état de l'environnement à la prochaine action à exécuter. Donc, les plans produits ne cherchent pas à gagner de l'information sur l'état du système, et les risques ne sont vraiment pris en compte dans l'évaluation des plans que dans la mesure où l'on est capable d'observer un échec lorsqu'il se produit.

Il est clair que l'utilisation sur un domaine partiellement observable d'un planificateur conçu pour des environnements totalement observables ne constitue qu'une solution partielle. Mais, par rapport à la complexité du traitement idéal de l'observabilité partielle, on peut espérer ici obtenir une solution viable pour des réseaux de taille réelle. C'est donc principalement sur ces travaux que nous avons orienté la suite du CERD, en évaluant tout d'abord l'adéquation au problème du planificateur pour environnements stochastiques totalement observables PASCALE développé à l'IRISA (voir le second rapport du CERD [Jehl et al.95], la section suivante, et l'annexe C de ce rapport), puis en nous basant sur les conclusions des expérimentations effectuées pour construire un prototype dédié au problème (voir la section 1.4, et l'annexe D de ce rapport).

Les autres travaux que nous avons étudiés sont ceux intégrant les réparations aux diagnostics basé sur les modèles, puisqu'il est clair que la reprise de service peut aussi être vue comme un problème de diagnostic (localisation des portions fautives) et de réparation (réalimentation des parties non-fautives). Les deux approches existantes [Friedrich et al.92, Sun et al.92] sont similaires. Plutôt que de se baser sur une architecture à un seul niveau (le planificateur) comme tel était le cas pour la planification dans des environnements partiellement observables, elles utilisent une architecture à deux niveaux comportant un module de diagnostic et un planificateur classique. Le module de diagnostic maintient une distribution de probabilités sur les diagnostics possibles, et choisit, à chaque étape, s'il est préférable d'acquérir une information sur l'état du système afin de discriminer entre plusieurs diagnostics, ou de réparer certaines fonctionnalités. Le planificateur est utilisé pour produire une séquence d'actions qui permet d'obtenir l'information choisie ou d'effectuer la réparation choisie.

Nos conclusions sont que ces approches ont été conçues pour résoudre un problème substantiellement plus simple que celui posé par la reprise : en supposant qu'observations et actions sont fiables, que l'on peut tout observer si on le souhaite, et que les plans de réparations pour les différents diagnostics sont compatibles, trouver un entrelacement entre observations et actions induisant un bon compromis entre coûts des pannes, des observations et des réparations. Nous pensons cependant que l'approche de [Sun et al.92] pourrait être étendue de façon à passer outre ces limites, et les expérimentations que nous avons menées avec PASCALE, ainsi que le prototype que nous avons construit, constituent une première étape dans cette direction.

1.3 Expérimentations réalisées avec PASCALE

Les premières expérimentations menées (voir l'annexe C de ce rapport et le second rapport du CERD [Jehl et al.95]) avaient trois objectifs principaux. Premièrement, il s'agissait d'évaluer l'adéquation au problème d'un planificateur à portée générale pour des environnements stochastiques totalement observables, comme PASCALE. Ensuite, les planificateurs pour environnements totalement observables n'apportant qu'une réponse partielle au problème de la reprise de service, le deuxième objectif était d'obtenir une borne supérieure sur la taille des

problèmes qu'une approche plus élaborée (comme la planification pour environnements partiellement observables) pourrait être à même de traiter. Enfin, puisque faire l'hypothèse d'une observabilité totale ne rend pas pour autant le problème réel totalement observable, le planificateur ne pouvait pas être le seul composant de l'architecture. Nos expérimentations ont donc été basées sur une architecture à deux niveaux, comportant un estimateur d'état en plus du planificateur. Cet estimateur est chargé de gérer une distribution de probabilité sur les états du réseau, et de déterminer, en fonction de l'histoire des observations obtenues et des actions exécutées, l'état le plus probable à chaque instant. La prochaine action exécutée est alors celle que le plan prescrit pour cet état le plus probable. Le troisième objectif était donc d'évaluer l'intérêt d'une architecture à deux niveaux similaire à celle préconisée dans les travaux intégrant diagnostic et réparation.

Nos conclusions sur ces expérimentations sont les suivantes. PASCALE a permis une description extrêmement simple et concise des aspects logiques de la reprise de service (mais pas des aspects numériques, comme les intensités maximales), ainsi que l'évaluation des risques pour les échecs détectables instantanément (principalement les échecs de manœuvres acquittés comme tels par les TC). Par rapport à la maquette AUSTRAL, l'association entre le planificateur et l'estimateur d'état a rendu possible une gestion systématique des hypothèses, et le traitement de fautes multiples sur plusieurs départs.

Le point négatif majeur est la complexité beaucoup trop importante, PASCALE n'ayant pu traiter que des réseaux de taille élémentaire (6 organes). Deux facteurs y contribuent. Le facteur prépondérant est la généralité des traitements effectués par un planificateur à portée générale comme PASCALE, qui n'exploite aucune des spécificités du problème. Ceci n'est pas lié à PASCALE : nous pensons qu'aucun des planificateurs à portée générale existant n'y remédiera. Le second est l'évaluation des risques d'échecs que nous avons mentionnés, qui est d'autant plus coûteuse que fine. L'étape suivante du CERD (voir la section suivante et l'annexe D de ce rapport) a donc consisté à construire un prototype dédié à la reprise de service, donc annihilant le premier facteur, et à la fois suffisamment simple pour traiter des réseaux de taille réelle, et suffisamment élaboré pour donner une idée de l'étendue de la seconde source de complexité.

1.4 Le prototype construit

Les choix concernant le prototype construit ont été dictés par la nécessité de traiter des réseaux de taille réelle en un temps raisonnable. Gérer les hypothèses de façon systématique pour finir par rétablir le courant et traiter des fautes multiples sur plusieurs départs a donc été privilégié sur tout autre préoccupation. Ainsi, le prototype n'évalue pas les risques, car nous voulions tout d'abord nous assurer qu'un traitement ne remédiant qu'à certaines des limites de la maquette AUSTRAL ne serait déjà pas trop complexe pour des réseaux réels. Cependant, nous voulions aussi estimer l'étendue des problèmes posés par l'évaluation des risques en comparant les mécanismes mis en jeu dans le prototype avec ceux mis en jeu dans PASCALE.

L'architecture à deux niveaux s'étant avérée satisfaisante lors de nos expérimentations avec PASCALE, le prototype est basé sur cette même architecture. Les différences principales sont les suivantes. Le prototype est dédié au réseaux de distribution est donc basé sur un modèle spécifique à ces réseaux, similaire à celui utilisé dans la maquette AUSTRAL. Ce modèle peut être vu comme un simulateur de réseaux retournant l'état du réseau résultant de l'exécution d'une manœuvre d'organe, l'information-capteur disponible, et une alarme en cas de dépassement d'une puissance maximale.

La génération des plans de reprise est maintenant réactive, c'est à dire entrelacée avec l'exécution, comme dans les approches intégrant diagnostic et réparation. Comme pour notre expérimentation avec PASCALÉ, l'estimateur d'état prend en compte l'histoire des observations et des actions. Il calcule une distribution de probabilité initiale sur les états en accord avec les informations transmises par les TSD, invoque le planificateur qui fournit un plan pour l'état le plus probable, débute l'exécution de ce plan – en utilisant le modèle des réseaux pour mettre à jour et réviser la distribution suite à l'exécution d'une action et l'obtention de nouvelles observations – et demande un nouveau plan au planificateur dès que l'ancien échoue (i.e., est inadéquat pour l'état le plus probable de la nouvelle distribution).

Le planificateur se base sur le modèle des réseaux pour générer un plan (une séquence d'actions) admissible pour l'état donné par l'estimateur. Il explore l'espace entier des plans de niveau 1 (plans ne faisant qu'étendre les départs adjacents) par une méthode permettant de traiter simultanément des fautes multiples sur plusieurs départs. Les plans sont ensuite évalués, et le meilleur est retourné à l'estimateur. Les risques n'étant pas pris en compte dans l'évaluation, ce plan n'est optimal que si l'état donné par l'estimateur était correct et si les manœuvres n'échouent pas.

Le prototype a été testé sur le réseau semi-rural sur lequel la maquette AUSTRAL a été expérimentée. Un bon nombre d'exemples impliquant des fautes multiples sur plusieurs départs ont été examinés (voir l'annexe F de ce rapport), et ont donné entière satisfaction (le prototype arrivait à réalimenter les portions non-fautives). Le temps de résolution est du même ordre que celui de la maquette AUSTRAL, alors que l'étendue des problèmes traités est beaucoup plus large. Le contraste de ces résultats et de ceux obtenus avec PASCALÉ suggère que la source des difficultés de ce dernier était bel et bien sa trop grande généralité, beaucoup plus que l'évaluation des risques. En effet, lorsque le prototype explore tous les plans de niveau 1 pour un état du réseau donné, il effectue un travail de complexité quasi-équivalente à celle mise en jeu dans l'évaluation effectuée par PASCALÉ. Puisque les temps de calculs actuels sont tout à fait raisonnables et que les performances de l'implémentation actuelle (en Standard ML [Paulson91]) peuvent être largement améliorées, il est encore possible de tenir compte des risques et ainsi d'accroître de façon significative la qualité des plans produits par le prototype, tout en restant à la portée de réseaux de taille réelle.

1.5 Perspectives

Par rapport à la maquette AUSTRAL, les principaux apports du prototype sont une gestion systématique des hypothèses annihilant les échecs globaux de la reprise, et la prise en compte d'un nombre arbitraire de fautes sur un nombre arbitraire de départs. Par contre, le problème de l'évaluation des risques qui n'était pas abordé par la maquette AUSTRAL ne l'est pas non plus par le prototype. C'est donc dans cette direction que des travaux futurs devraient se porter.

Idéalement, on voudrait pouvoir générer des plans tenant compte des risques de façon optimale (i.e., tenant compte de du coût entraîné par *tous* les échecs possibles) pour le choix de la prochaine action, cette action pouvant viser à gagner de l'information sur l'état du réseau, à réapprovisionner certaines portions non-fautives, ou les deux. Il est clair, au vu de la complexité du problème de la planification optimale pour environnement stochastiques partiellement observables, qu'il sera impossible d'atteindre l'optimalité pour des réseaux réels. Par contre, il est tout à fait envisageable de tenter de s'en approcher, et de déterminer dans quelle mesure cela est possible.

Une stratégie possible est la suivante. On remarque tout d'abord qu'aucun des plans de niveau 1 générés par le prototype n'est réutilisé lorsqu'une manœuvre d'organe échoue, alors qu'il suffirait de regarder dans la liste de ces plans pour en trouver un approprié. Il est donc possible d'exploiter ces plans existants pour évaluer les risques vis à vis de dysfonctionnement d'organes. D'autre part, on remarque que l'architecture à deux niveaux fournit un cadre simple et naturel pour entrelacer l'exécution, le calcul de plans, et la projection de ces plans et de leur conséquences sur un horizon donné et sur les hypothèses les plus probables. En effet, on peut très bien envisager de remplacer l'estimateur d'état par un composant plus élaboré effectuant cette projection, comme cela est suggéré par les travaux que nous avons mentionnés dans le domaine du diagnostic. Cette projection permettra d'évaluer les risques provenant d'une mauvaise localisation des portions fautives. En faisant varier l'étendue (largeur, profondeur) de la projection, il sera possible de déterminer un bon compromis entre temps de calcul et qualité des plans de reprise.

Nous pensons donc qu'une étude plus approfondie des travaux dans le domaine de l'intégration des réparations au diagnostic [Sun et al.92], et l'exploitation de certaines des caractéristiques du prototype actuel, constituent une voie prometteuse vers le traitement des risques dûs aux échecs de manœuvres et à l'observabilité partielle.

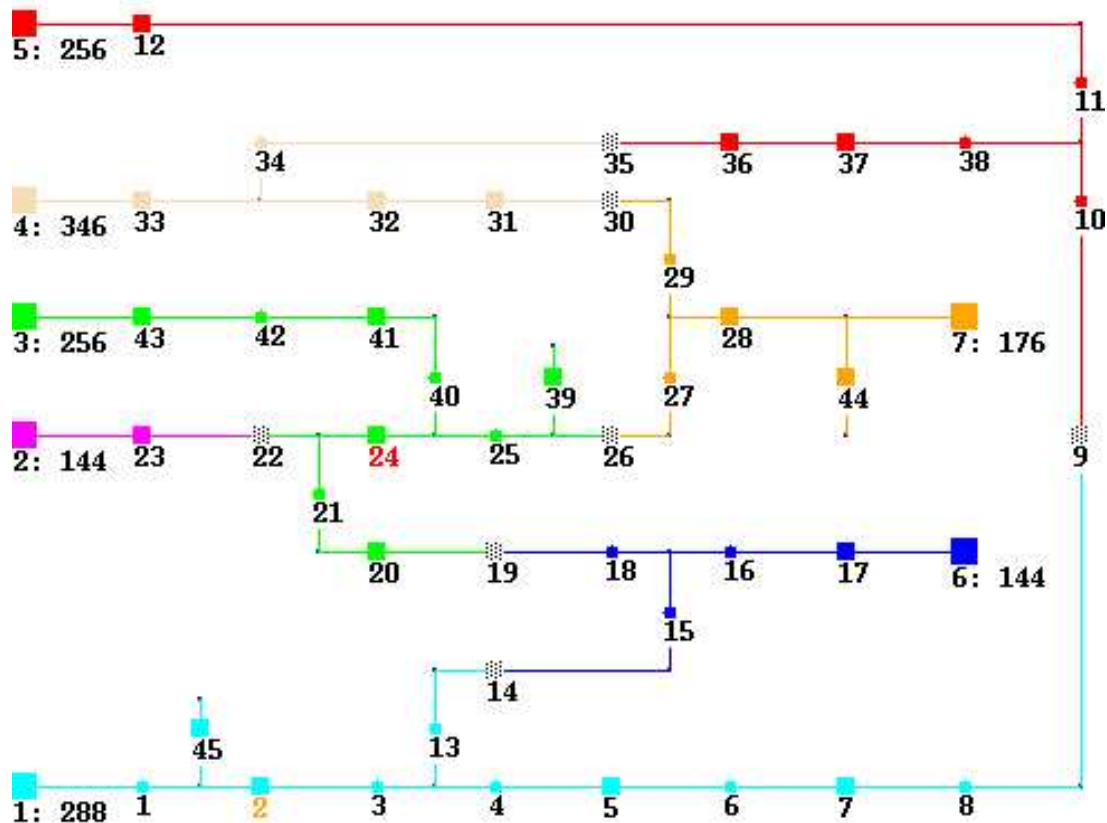


FIG. 1 – Réseau semi-rural

A Contexte et objectifs de l'étude

Cette annexe, qui reprend en partie des deux premiers rapports du CERD [Jehl et al.94, Jehl et al.95], décrit le problème de la reprise de service tel qu'on se propose de le résoudre, et spécifie les objectifs de l'étude.

A.1 Le problème de la reprise de service

A.1.1 Réseaux, incidents, et réalimentation

Au niveau d'abstraction qui nous intéresse, un réseau de distribution d'électricité peut être vu comme un ensemble de lignes électriques connectées entre elles par des organes de coupure (OC) et alimentées par des disjoncteurs (DR) télécommandés. DR et OC ont deux positions possibles : ouverts ou fermés. Un DR fournit du courant ssi il est fermé, et un OC stoppe la propagation du courant ssi il est ouvert. Le réseau est maillable, mais en général, il est exploité de façon arborescente : les positions des OC sont choisies de manière à ce que les chemins parcourus par le courant forment des arbres, appelé départs. La racine d'un départ est un DR, ses feuilles sont des OC ouverts (ou la terre), et chaque ligne appartient à un seul départ, i.e, chaque ligne n'est alimenté que via un seul chemin électrique. Des clients peuvent être situés sur n'importe quelle ligne, et ne sont approvisionnés que si cette ligne l'est.

La figure 1 représente un tel réseau utilisé en milieu semi-rural.¹ Les DR sont représentés par des gros carrés, les OC télécommandés (e.g., l’OC 20) par des carrés de taille moyenne, et les OC manuels (e.g., l’OC 10) par des petits carrés. Les organes grisés (OC 9, 14, 19, 22, 26, 30, et 35) sont ouverts, et les autres sont fermés. Les départs ont des couleurs différentes.

En cas de défaut (court-circuit) permanent sur une ou plusieurs lignes, les DR alimentant ces lignes disjonctent de manière à protéger le reste de leur départ d’une surtension. Il s’agit alors de localiser les portions² fautives, de les isoler en ouvrant les OC télécommandés qui les entourent, et de réalimenter les portions non-fautives en ouvrant et fermant des organes télécommandés de manière à rediriger le courant vers ces portions. Il s’agit donc d’un problème de diagnostic, couplé à un problème de recherche d’un plan de reprise constitué d’ordres d’ouverture et de fermeture. Pour le résoudre, on dispose d’une durée de l’ordre de quelques minutes.

Actuellement, un opérateur se charge de cette tâche, dont les étapes sont détaillées dans les paragraphes suivants. Pour ceci, il se base sur son expertise ainsi que sur des plans de reprise pré-établis. Tous deux sont spécifiques à un schéma nominal du réseau, i.e., sa configuration normale d’exploitation. EDF étudie l’automatisation de la reprise, en vue d’améliorer sa rapidité, la qualité des plans, et le traitement d’incidents de grande ampleur (e.g., défauts multiples) qui obligent à s’éloigner du schéma nominal.

A.1.2 Localisation des portions fautives

La tâche de détection des portions fautives du réseau est facilitée par la présence de capteurs, appelés télésignalisations de défaut (TSD), placés sur les OC télécommandés. Ces capteurs indiquent s’ils ont ”vu passer un défaut” ou non, i.e., si un défaut se trouve plus en aval sur leur départ. Par exemple, si la ligne reliant les OC 5 et 6 est fautive, le DR 1 disjoncte et les TSD des OC 2 et 5 devraient indiquer que la panne est en aval, alors que celles des OC 7 et 45 devraient indiquer qu’elle n’y est pas.

Malheureusement, les TSD ne sont pas toujours fiables : elles peuvent être en panne (elles ne donnent pas d’indication), et même mentir (elles donnent une indication erronée). Il en découle plusieurs hypothèses de localisation du défaut, qui correspondent à plusieurs hypothèses sur le mode de fonctionnement des TSD. Par exemple, si le DR 1 disjoncte, si seule la TSD de l’OC 5 indique un défaut en aval, et si l’on suppose un défaut unique, alors il y a cinq hypothèses possibles. Soit celui-ci est en amont des OC 2 et 45, auquel cas 5 ment, soit il est en aval de 45, et 45 et 5 mentent, soit il est entre 2 et 5, et 2 et 5 mentent, soit il est entre 5 et 7, et 2 ment, soit enfin il est en aval de 7, et 2 et 7 mentent. Il existe des préférences entre ces hypothèses : la probabilité d’un défaut multiple est faible devant celle d’une TSD menteuse, et cette dernière est plus importante si la TSD n’indique aucun défaut en aval que si elle en indique un, car les TSD ne détectent pas tous les types de défauts. Seule la phase de réalimentation peut permettre de discriminer entre les hypothèses, surtout lorsqu’elle se passe mal.

1. On ne représente ici que l’ossature principale du réseau. En particulier, on s’abstrait des antennes dépourvues d’OC connectant les clients au réseau.

2. Par portion, nous entendons un ensemble de lignes situées entre des organes télécommandés. Ces portions constituent la plus fine granularité possible du diagnostic à distance.

A.1.3 Réalimentation des portions non-fautives

Les portions fautives ayant été localisées, la première étape est de les isoler en ouvrant les OC télécommandés qui les entourent. Puis les portions non-fautives sont réalimentées en manœuvrant des organes télécommandés de façon à rediriger le courant vers ces portions. Par exemple, si nous suspectons la portion entre les OC 5 et 7, l'isolation consiste à ouvrir ces organes, et la réalimentation à par exemple refermer le DR 1 pour réapprovisionner les lignes en amont de l'OC 5, et, par exemple, et fermer l'OC 9 pour réapprovisionner les lignes en aval de l'OC 7 via le DR 5.

Certaines contraintes se posent, qui déterminent quels sont les plans de reprise *admissibles* : chaque DR, resp. chaque ligne, ne peut fournir, resp. ne peut supporter, qu'une certaine puissance maximale. On risque donc de ne pas pouvoir acheminer le courant via certains chemins, ni réussir à réalimenter toutes les portions non-fautives à moins de décharger un DR d'une partie de sa charge après l'incident et de la faire reprendre par d'autre. Idéalement, la reprise s'efforce aussi d'optimiser certains paramètres, comme réapprovisionner le maximum de consommateurs possibles en privilégiant certains clients prioritaires comme les hôpitaux, minimiser le nombre de manœuvres afin de rester proche du schéma nominal, et équilibrer les marges de puissance des DR en prévision de la prochaine heure de pointe.

Même si le défaut a été correctement localisé, la reprise est rendue difficile par le manque de fiabilité des télécommandes (TC) des organes télécommandés. Une TC peut être en panne (elle ne transmet pas l'ordre qui n'est donc pas exécuté et le signale en retournant un acquit négatif), et même mentir (elle transmet l'ordre et retourne un acquit positif alors que la manœuvre n'est pas exécutée car l'organe est en panne). Dans la plupart des cas d'acquit positif, il est tout de même possible de savoir si l'ordre a vraiment été exécuté en consultant la télésignalisation de position (TSP) de l'organe, qui indique si ce dernier est ouvert ou fermé. Parfois cependant, l'incertitude ne peut pas être levée car la TSP est en panne (ne retourne pas d'information). Lorsqu'un DR disjoncte au cours de la reprise, il est alors difficile de savoir si ceci est dû à une mauvaise localisation du défaut, à un deuxième défaut qui n'avait pas pu être détecté, ou à la mauvaise exécution d'une manœuvre acquittée positivement.

Notons qu'il est raisonnable de faire l'hypothèse qu'une TSD ne change pas de mode de fonctionnement pendant la reprise. En revanche, le mode d'une TSP peut évoluer de correct à en panne et vice-versa à tout moment. Celui d'une TC peut évoluer à tout moment de correct à en panne ou menteur avec une certaine probabilité, ces deux derniers modes étant permanents. Puisque nous ne nous intéressons qu'au mode des TC des organes manœuvrés au cours de la reprise, ceci revient à considérer chaque manœuvre comme une action stochastique [Thiebaut et al.93, Kushmeric et al.94, Draper et al.94] pouvant éventuellement modifier, outre la position de l'organe, le mode de fonctionnement de sa TC.

A.2 Principales difficultés du problème

Les caractéristiques de ce problème sont assez différentes de celles du problème de la reprise de service sur les réseaux de *transport* d'électricité, problème qui a déjà été étudié dans la littérature. En effet, pour les réseaux de transport, il est raisonnable de ne considérer que très peu de sources d'incertitude [Mondon et al.91], voire aucune [Friedrich et al.92]. En revanche, la reprise sur les réseaux de distribution comporte de nombreuses sources d'incertitude dues aux actions stochastiques et à l'observabilité partielle, i.e., à l'incomplétude et au manque de

fiabilité de l'information sur l'état du réseau tout au long de la reprise. La conséquence de cette incertitude est une combinatoire accrue³ rendant difficile le choix d'un plan de reprise optimal, et même de garantir que l'on finira par réapprovisionner les portions non-fautives.

Examinons tout d'abord la difficulté du choix d'un plan optimal. Notons qu'il est impossible de formuler un objectif de reprise correspondant à une propriété logique à satisfaire (e.g, que telles ou telles lignes soient alimentées). En effet, cela nécessiterait la connaissance préalable des portions qui peuvent être réalimentées, et donc de connaître avec certitude quelles sont les portions fautives, et quels sont les modes de fonctionnement des TC. Le mieux que l'on puisse faire est donc évaluer l'utilité d'un plan en accord avec les préférences mentionnées dans la section précédente, et sélectionner le plan dont l'utilité est maximale. Idéalement, cette évaluation doit tenir compte des risques en cas d'échec, les coûts de panne étant potentiellement élevés. Pour notre exemple, supposons qu'une mauvaise localisation de la faute entraîne l'ouverture du DR 5 lorsque nous fermons l'OC 9. Si l'hypothèse de localisation de la faute entre les OC 5 et 7 n'avait pas une très grande probabilité, il était peut-être préférable de chercher à s'assurer de cette hypothèse (par exemple en gardant l'OC 5 fermé et en regardant si ceci fait redisjoncter le DR 1), plutôt que de chercher à réalimenter tout de suite les lignes en aval de l'OC 7. L'incertitude entraînant un nombre gigantesque d'hypothèses et de plans possibles à considérer, cette évaluation est prohibitive, et l'on doit donc renoncer à la génération d'un plan optimal.

Un objectif qui semble plus facile à atteindre, est de n'évaluer les risques que partiellement, mais de tout de même finir par réapprovisionner les portions non-fautives. On acquiert donc certaines des informations manquantes et on identifie certaines des informations erronées, en commençant à exécuter un plan de reprise approprié pour les hypothèses les plus probables et en confrontant les observations résultantes aux prédictions. Puisque différentes portions fautives et différents modes de fonctionnement des TC requièrent des plans de reprise substantiellement différents, le plan courant doit alors être révisé dès qu'il s'avère inadéquat. Cette révision n'est toujours pas gratuite, car l'espace des hypothèses doit être géré dans son intégralité et de façon systématique, si l'on veut garantir de finir par exécuter le plan de reprise adéquat.

A ces difficultés d'ordre combinatoire liées à l'incertitude, s'ajoutent les difficultés suivantes qui se manifestent lorsque l'on utilise un planificateur à portée générale pour générer les plans de reprise. Premièrement, les manœuvres d'organes sont des actions assez complexes possédant de nombreuses ramifications (effets secondaires) qui dépendent du contexte d'exécution. Par exemple, la fermeture d'un OC peut causer l'approvisionnement de certaines lignes et même l'ouverture d'un DR si une ligne fautive est nouvellement approvisionnée. Il n'est pas possible d'explicitement tous ces effets sans rendre la taille de la description des actions exponentielles en le nombre d'organes. Or, les modélisations d'actions classiquement utilisées en planification sont peu expressives : elles supposent que tous les effets des actions sont explicitement décrits et sont connus avec certitude. Certains planificateurs permettent de déduire automatiquement les ramifications grâce à des contraintes d'intégrité (contraintes logiques définissant quels sont les états possibles de l'environnement), mais cette déduction est coûteuse. Deuxièmement, la reprise possède certaines spécificités, comme la localité des effets des manœuvres d'organes, et

3. Si l'on omet les aspects numériques, le nombre d'états possibles d'un réseau est $36^t \times 12^d \times 2^{m+l}$ états, t étant le nombre d'OC télécommandables, d le nombre de DR, m le nombre d'OC manuels, et l le nombre de lignes. En effet, un OC télécommandable a $3 \times 2 \times 3 \times 2 = 36$ états possibles correspondant aux modes de fonctionnement de sa TSD (3 modes), à celui de sa TSP (2 modes), à celui de sa TC (3 modes), et à sa position (2 positions). Un DR ne comporte pas de TSD, de sorte qu'il n'a que 12 états. Un organe à commande manuelle n'a que deux états possibles correspondant à sa position. Une ligne n'a que deux états possibles : soit elle est fautive, soit elle ne l'est pas. Par exemple, le réseau en figure 1 comporte environ 2.10^{67} états.

le peu d'importance de l'ordre dans lequel les manœuvres sont exécutées. Les planificateurs à portée générale nous donnent rarement les moyens d'exploiter de telles spécificités, d'où une complexité plus importante qu'elle ne devrait l'être.

A.3 L'existant : la maquette AUSTRAL

Le projet AUSTRAL est un projet pluriannuel de recherche et de développement en cours à EDF au département MOS [Pprd94]. Son objet est, entre autres, la réalisation de fonctions évoluées pour l'aide à la conduite des réseaux de distribution et à leur intégration dans des systèmes existants ou en cours de développement. La reprise automatique de service est l'une de ces fonctions. Préalablement, une maquette dédiée à la reprise de service [Jehl et al.93, Bredillet et al.94] a été réalisée en Lelisp et en LISA [Delouis93]. La maquette AUSTRAL est un système mixte, alliant un raisonnement basé sur un modèle (pour la localisation du défaut, et la vérification de l'admissibilité des plans) à un raisonnement de type système expert (pour la sélection/évaluation d'un plan, et la gestion des hypothèses sur l'état du réseau en cours de reprise). Elle est largement autonome, mais fait parfois appel à l'opérateur lorsque la combinatoire à gérer est trop importante.

Pour pallier le faible pouvoir d'expression des modélisations d'actions classiques, la maquette AUSTRAL se base sur un modèle dédié aux réseaux de distribution d'électricité. Ce modèle peut être vu comme un simulateur de réseaux permettant de déterminer l'état résultant du lancement d'un ordre, d'effectuer la répartition des charges, et de vérifier que l'on obtient un état admissible.

Pour pallier la combinatoire liée à l'incertitude et au nombre de plans de reprise possibles, la maquette AUSTRAL fait plusieurs hypothèses simplificatrices, décrites ci-dessous. Ces hypothèses font que la maquette peut ne pas réussir à réalimenter les portions non-fautives, notamment en cas d'incident de grande ampleur.

Premièrement, la maquette est limitée à un départ fautif, et à un seul défaut sur ce départ. Ceci à l'avantage de simplifier le processus de diagnostic : il suffit de considérer toutes les portions sur le départ fautif, et de préférer les localisations induisant un nombre minimal de TSD menteuses au vu des informations qu'elles fournissent. Ceci à aussi l'avantage de simplifier le processus de génération des plans de reprise. En effet, on peut alors décomposer la reprise en 4 phases distinctes : isolation de l'amont du défaut pour laquelle il suffit d'ouvrir l'organe en amont de la portion fautive, reprise des portions non-fautives en amont, pour laquelle il suffit de réenclancher le DR ayant disjoncté, isolation aval qui est symétrique à l'isolation amont, puis reprise aval.

La reprise aval est effectuée en estimant la charge à reprendre, puis en examinant toutes les combinaisons d'ordres de fermeture et d'ouverture d'organes permettant la réalimentation sans transfert de charge sur un troisième DR. Les plans résultants sont appelés plans de niveau 1. Si aucun plan de niveau 1 réalimentant toutes les portions non-fautives n'est admissible, la maquette AUSTRAL forme alors les plans de niveau 2 à partir d'un plan de niveau 1 sélectionné par l'opérateur et ne réalimentant qu'une partie des portions non-fautives. Ces plans de niveau 2 font appel à d'autres DR de secours pour délester une partie des charges des DR de secours du niveau 1. Ces plans nécessitant un protocole de communication complexe avec le centre de distribution, l'opérateur est sollicité pour choisir le plan à appliquer parmi ceux générés. Qu'elle serve de base à une sélection automatique ou une sélection par l'opérateur, l'évaluation

des plans prend en compte les critères mentionnés en sous-section A.1.3, mais pas les risques d'échec. C'est donc la deuxième simplification effectuée par la maquette AUSTRAL.

La troisième simplification dans la maquette AUSTRAL est le produit d'une gestion non-systématique des hypothèses en cours de reprise, par un raisonnement de type système expert. Cette gestion est la suivante. Lors de l'isolation amont (resp. aval), si les informations transmises par la TC ou la TSP de cet organe laissent supposer que l'ordre n'est pas passé, le processus est réitéré sur l'organe suivant en amont (resp. aval). Lors de la reprise amont, si le DR réenclanché redisjoncte, seule l'hypothèse de localisation du défaut est révisée plus en amont. En mode interactif, la maquette AUSTRAL demande à l'utilisateur s'il préfère privilégier l'hypothèse d'une mauvaise localisation du défaut ou bien l'hypothèse d'une mauvaise isolation. Si un DR disjoncte lors de la reprise aval, la maquette AUSTRAL abandonne la reprise, en défaisant au préalable les ordres passés de manière à retrouver la configuration du réseau avant la tentative de reprise.

A.4 Objectifs de l'étude

Pour faire face aux problèmes combinatoires liés à l'incertitude, le choix qui a été fait dans la maquette AUSTRAL est de faire certaines simplifications : un défaut unique sur un départ, pas d'évaluation des risques, en cas d'échec de la reprise amont, seul un retour arrière sur l'hypothèse d'une mauvaise localisation de la faute est effectué ce qui peut s'avérer erroné, et en cas d'échec de la reprise aval, aucun retour arrière n'est effectué. Ces simplifications peuvent mener la maquette AUSTRAL à ne pas pouvoir rétablir complètement le courant, notamment dans le cas d'incidents de grande ampleur.

L'objectif du CERD était donc d'étudier certains travaux récents en planification sous incertitude (planification en présence d'actions stochastiques, planification pour des environnements partiellement observables, planification réactive), et dans une moindre mesure en diagnostic et réparation, qui pourraient permettre de remédier à certaines des limites de la maquette. Le CERD s'est déroulé de la façon suivante : la littérature dans les domaines concernés a été étudiée, une première approche du problème a été évaluée par le biais d'expérimentations à partir du planificateur à portée générale PASCALE développé à l'IRISA, puis, au vu des conclusions de ces expérimentations, un prototype dédié au problème de la reprise a été construit. Ces étapes respectives sont l'objet des annexes qui suivent.

B Travaux étudiés

Cette annexe, qui reprend certaines parties d'un article relatant les résultats du CERD [Thiebaut et al.96], décrit les approches en planification sous incertitude et en diagnostic et réparation qui ont été envisagées pour remédier aux limites de la maquette AUSTRAL.

B.1 Planification sous incertitude

B.1.1 Environnements stochastiques partiellement observables

Une approche possible du problème de la reprise consiste à s'appuyer uniquement sur la technologie actuelle en planification : un planificateur à portée générale traitant les types d'incertitude présents est utilisé pour effectuer simultanément la localisation des portions fautives et la réalimentation des portions non-fautives. Les caractéristiques de la reprise font qu'il s'agit, dans la terminologie planification, d'un environnement stochastique partiellement observable. Ces environnements sont caractérisés par (1) des actions stochastiques qui amènent de l'information tout en modifiant l'état de l'environnement de façon probabiliste, et (2) une connaissance incertaine de l'état de l'environnement à tout moment, matérialisée par une distribution de probabilité sur les états. Le but de la planification est de construire une fonction (un plan) associant l'information-capteur à la prochaine action à exécuter. Cette fonction maximise certains critères représentés par une fonction d'utilité, en tenant compte des risques. Elle est optimale compte tenue de l'observabilité partielle et des actions stochastiques, et prescrit tour à tour des actions dans le but de gagner de l'information ou de faire évoluer l'environnement. Deux types de travaux existent pour traiter ces environnements, et aucun d'entre eux ne s'est avéré adéquat pour notre problème, dû à un manque d'expressivité ou à une trop grande complexité.

Le premier type de travaux s'est attaché à améliorer les techniques traditionnelles de la recherche opérationnelle pour résoudre des processus de décision Markoviens partiellement observables (PDMPO) [Cassandra et al.94]. L'intérêt de ces travaux est que le modèle des PDMPO est assez général pour encoder notre problème. Bien que les questions liées à la modélisation des actions et de l'environnement n'aient pas été abordées dans le cadre de ces approches (e.g., elles supposent donnée une fonction retournant les états pouvant résulter de l'exécution d'une action et leur probabilité), nous pouvons facilement imaginer des formalismes qui pourraient rendre cet encodage concis [Thiebaut et al.93]. Malheureusement, les algorithmes actuellement disponibles pour résoudre des PDMPO explorent potentiellement l'espace entier des distributions de probabilités sur les états, ce qui rend notre problème clairement hors de leur portée. En effet, ils sont limités à des problèmes d'une centaine d'états, ce qui correspond à des réseaux comportant 1 ou 2 organes!

Le second type de travaux étend les modélisations et algorithmes classiques en planification à des actions stochastiques procurant de l'information [Draper et al.94]. De notre point de vue, l'avantage principal par rapport aux travaux précédents est que l'espace des distributions de probabilités sur les états n'est exploré que très implicitement, et par des algorithmes de recherche plus flexibles. Néanmoins, l'application de ces travaux à la reprise de service pose deux difficultés majeures. Les algorithmes sont limités à une sous-classe des PDMPO pour laquelle l'utilité d'un plan est définie par sa probabilité de satisfaction d'un objectif logique, qui doit excéder un certain seuil. Rappelons que nous ne disposons pas d'un tel objectif pour la reprise de service, et que nos besoins en matière d'utilité sont plus complexes. Plus problématique,

ces algorithmes ne prennent pas en compte les contraintes d'intégrité. Donc, la description des actions doit énumérer toutes leurs ramifications dans tous les contextes possibles, ce qui est inenvisageable ici, car la taille de la description des ordres de fermeture et d'ouverture serait alors exponentielle en le nombre d'organes du réseau. Il n'est absolument pas clair qu'il soit possible d'étendre les algorithmes de [Draper et al.94] dans une de ces directions sans compromettre leurs avantages sur ceux de [Cassandra et al.94].

B.1.2 Environnements stochastiques totalement observables

Étant données ces difficultés, une autre possibilité est de renoncer à l'optimalité des plans vis à vis de l'optimalité partielle, et de planifier comme si l'environnement était totalement observable. Par rapport à l'état d'un environnement partiellement observable, celui d'un environnement totalement observable est inconnu lors de la planification, mais les plans sont construits en supposant que l'on pourra tout observer lors de leur exécution. Ainsi, les actions sont toujours stochastiques mais n'amènent pas d'information (celle-ci étant supposée disponible à l'exécution), et le planificateur produit une fonction (un plan) associant l'état de l'environnement à la prochaine action à exécuter. L'observabilité partielle n'ayant pas pour autant disparu du problème, il est nécessaire de la gérer à l'exécution du plan. Il convient donc d'introduire un nouveau composant en plus du planificateur, qui est chargé d'estimer l'état de l'environnement en fonction des informations disponibles. La prochaine action exécutée est alors celle que le plan prescrit pour cet état estimé.

Il est clair que cette approche n'est pas totalement satisfaisante: les plans produits ne cherchent pas à gagner de l'information sur l'état du système, et les risques ne sont vraiment pris en compte dans l'évaluation des plans que dans la mesure où l'on est capable d'observer un échec lorsqu'il se produit. Cependant, elle est intéressante pour essentiellement trois raisons. Elle permet de finir par réapprovisionner les portions non-fautives tout en induisant une complexité beaucoup plus abordable, elle nous donne une borne supérieure sur la taille des problèmes qui pourraient être traités par une approche pour environnements partiellement observables ou une approche intermédiaire, et elle nous permet d'évaluer l'intérêt d'une architecture à deux niveaux (un planificateur plus un estimateur) similaire à celle que l'on trouve dans les travaux en diagnostic et réparation décrits ci-dessous.

L'étendue des travaux en planification pour environnements stochastiques totalement observables est plus large que celle des travaux traitant les environnements partiellement observable. On peut distinguer trois types de travaux. Les premiers étendent les modélisations et algorithmes classiques en planification au traitement d'actions stochastiques [Kushmerick et al.94]. Tout comme leur équivalent partiellement observable et pour des raisons identiques (objectif logique, absence des contraintes d'intégrité), ces travaux ne sont pas applicables au problème de la reprise. D'autres travaux sont basés sur des méthodes issues de la recherche opérationnelle pour la résolution de processus de décisions Markoviens totalement observables (PDMTO) [Dean et al.93]. Ces travaux posent un problème similaire mais d'une ampleur bien moindre que ceux sur les PDMPO. Ils explorent successivement des sous-ensembles de plus en plus larges de l'espace d'états, et peuvent ainsi traiter des problèmes de l'ordre d'une dizaine de milliers d'états. Enfin, on trouve des travaux mixtes, alliant une extension de modélisations classiques aux actions stochastiques et aux contraintes d'intégrité, et des algorithmes de recherche intermédiaires mettant en jeu des techniques propres à l'intelligence artificielle et à la recherche opérationnelle [Thiébaux et al.93]. L'algorithmique est plus flexible, mais la modélisation des

actions impliquant des contraintes d'intégrité est coûteuse à exploiter, ce qui rend les performances équivalentes à celle des travaux précédents.

C'est à partir d'un planificateur se situant dans le cadre de ce troisième type de travaux que nous avons tout d'abord expérimenté cette approche. Ces expérimentations et nos conclusions (l'approche est intéressante mais trop complexe si un planificateur à portée générale est utilisé) font l'objet de l'annexe qui suit.

B.2 Diagnostic et réparation basés sur les modèles

La reprise du service sur les réseaux de distribution d'électricité peut aussi être vue comme un problème de diagnostic et de réparation, les manœuvres d'organes constituant à la fois des actions de réparation et des jeux de test. Il est donc intéressant d'étudier les travaux sur l'intégration du diagnostic et des réparations effectués dans la communauté diagnostic basé sur les modèles.

L'approche préconisée par cette communauté se base sur une architecture à deux niveaux. Au niveau le plus haut, un module de diagnostic maintient une distribution de probabilité sur les diagnostics possibles, et choisit, à chaque étape et au vu des coûts des pannes, des observations, et des réparations, s'il est préférable de réparer ou de discriminer entre plusieurs diagnostics (i.e., de gagner de l'information). Au niveau inférieur, un planificateur classique est chargé par le module de diagnostic de fournir une séquence d'actions pour un diagnostic et un but de réparation donnés. Suite à l'exécution d'une action, resp. à une nouvelle observation, le module de diagnostic met à jour, resp. révisé, la distribution de probabilité, puis débute une nouvelle étape de choix. Ce module de diagnostic peut être vu comme une généralisation de l'estimateur d'état de l'approche introduite précédemment.

Deux travaux basés sur ce type d'intégration entre diagnostic et réparations existent, en l'occurrence [Friedrich et al.92, Sun et al.92]. Il s'avère qu'ils ne sont pas assez puissants pour traiter notre problème, comme nous l'expliquons maintenant.

B.2.1 Plans entrelaçant observations et réparations

[Friedrich et al.92] décrit des algorithmes pour le choix et l'entrelacement par le module de diagnostic de procédures d'observations et de plans de réparations pré-établis. A chaque étape, ces algorithmes partitionnent les diagnostics en groupes, de façon à ce que pour chaque groupe, exécuter un plan résultant de la fusion des plans individuels pour chaque membre du groupe soit préférable à discriminer parmi les membres puis exécuter le plan pour le diagnostic restant. Lorsque la partition courante est appropriée, des observations sont effectuées de manière à discriminer entre les groupes, les premières actions du plan de réparation-fusion pour ce groupe sont exécutées, et ce processus est réitéré avec la mise à jour des diagnostics du groupe. Cette itération (calcul et exécution) est effectuée n fois. La dernière exécution diffère des précédentes par le fait que l'on observe jusqu'à pouvoir discriminer parmi tous les diagnostics du groupe restant, et le plan de réparation pour le diagnostic restant est alors exécuté.

Le premier problème de cette approche est qu'une distinction explicite est faite entre observations (qui sont tout d'abord effectuées pour distinguer entre les groupes) et actions (qui sont ensuite effectuées pour réparer). Cette distinction est inadéquate pour le problème de la reprise de service, puisque l'information-capteur dont on dispose est gratuite mais limitée, et que des informations supplémentaires ne peuvent être acquises qu'en manœuvrant des organes

et en confrontant l'information-capteur résultante aux prédictions. De plus, l'approche se base sur l'hypothèse que les observations et les actions sont fiables, que l'on peut observer ce que l'on veut du moment que l'on est prêt à en payer le prix, et que l'on sera capable de tout observer à la dernière étape d'exécution.

Enfin, comment est-il possible de fusionner des plans pour différents diagnostics si ces plans sont incompatibles (par exemple un plan prescrivant de fermer un organe et un plan basé sur le fait que cet organe soit ouvert ou prescrivant de l'ouvrir)? Il semble que ceci implique des actions de réparation sommaires, comme par exemple des remplacements de composants dont la véracité des préconditions n'a plus d'importance une fois que l'action a été exécutée.

Pour résumer, il est évident que cette approche a été conçue pour résoudre un problème substantiellement différent de celui qui nous préoccupe : en supposant qu'observations et actions sont fiables, que l'on peut tout observer si on le souhaite, et que les plans de réparations pour les différents diagnostics sont compatibles, trouver un entrelacement entre observations et actions induisant un bon compromis entre coûts des pannes, des observations et des réparations.

B.2.2 IRS

En substance, the système IRS [Sun et al.92] a été conçu pour résoudre le même problème, mais ses caractéristiques le rendent plus proche des besoins de la reprise. A chaque étape, le module de diagnostic choisit le meilleur but, parmi les buts de réparation (rétablir une fonctionnalité), et les buts test (effectuer une nouvelle mesure). Pour cela, il projette chaque choix possible sur les diagnostics de la distribution de probabilité et évalue ses conséquences sur un horizon donné. Puis, la séquence d'actions produite par le planificateur pour le meilleur but est exécutée, la distribution est mise à jour et révisée, et le processus est réitéré jusqu'à ce qu'un seuil de fiabilité du système soit atteint. IRS est basé sur le langage UWL, dans lequel buts, actions et états peuvent être décrits et pris en entrée par le planificateur.

Pour notre problème, l'avantage principal de cette approche sur la précédente est qu'UWL ne fait pas de distinction entre observations et actions, tout comme le module de diagnostic n'en fait pas entre buts de réparation et buts de test. Cependant, IRS ne lève pas certaines des restrictions de [Friedrich et al.92], comme l'hypothèse de fiabilité des actions et des observations, et est explicitement limité à des remplacements de composants. La véritable cause de ces restrictions est le choix des auteurs de ne pas planifier avec des contraintes d'intégrité (et dans une moindre mesure avec des actions stochastiques), afin de ne pas rendre le processus de planification trop complexe — Curieusement, ils justifient par ce même choix l'intérêt de l'architecture à deux niveaux par rapport à l'architecture ne comportant qu'un planificateur effectuant simultanément diagnostic et planification de réparations.⁴

En l'absence de contrainte d'intégrité, le planificateur ne peut quasiment rien prédire quant à l'effet des actions qu'il prescrit sur le comportement du système, d'où la limitation des réparations aux remplacements de composants. Comment, par exemple, pourrait-il décider des organes à manœuvrer, s'il ne dispose pas d'un modèle de la propagation du courant dans le réseau? Il est certain que les contraintes d'intégrité sont coûteuses, mais leur absence pour la génération de plans de réparation implique de se restreindre à des actions très élémentaires, ou

4. "However, this is impractical, since all of these approaches require domain theories to specify the behavior of the device, and planning with axiomatic domain theories is expensive and ill understood. Instead, we choose to put a diagnostic reasoner at the top level of the architecture with the planner as a subroutine." [Sun et al.92, p. 70].

d'adopter des descriptions d'action de taille prohibitive, ou encore de renoncer à la planification à portée générale au profit d'un modèle et d'un planificateur spécifique au domaine. Au vu des conclusions de nos expérimentations avec PASCALÉ, c'est d'ailleurs cette dernière solution, que nous avons retenue pour le prototype final du CERD.

Contrairement à la justification donnée par les auteurs, il semble donc que le vrai avantage de l'architecture préconisée par la communauté diagnostic sur l'utilisation d'un planificateur pour environnements partiellement observables, n'est pas la planification sans contrainte d'intégrité. L'avantage est plutôt que la séparation du module de diagnostic et du planificateur, ainsi que la projection sur un horizon restreint, rendent simple et naturel l'entrelacement de phases de calcul, d'exécution et de révision du plan courant. Cet entrelacement, qui est aussi un des intérêts de l'approche planification pour environnements totalement observables couplé à un estimateur d'état, produit des plans sous optimaux mais gagne fortement en complexité. C'est pour cette raison que nous avons retenu cette architecture dans la suite de l'étude.

B.3 Choix effectués suite à cette étude

Suite à notre examen de ces travaux, nous nous sommes donc orientés vers une architecture à deux niveaux comportant un planificateur et un estimateur d'état. Dans un premier temps, nous avons réalisé des expérimentations avec un planificateur à portée générale pour environnement stochastiques totalement observables. Puis, au vu des résultats de ces expérimentations, nous avons construit un prototype dédié au domaine capable de traiter des réseaux de taille réelle.

C Expérimentations réalisées avec PASCALE

Cette annexe, qui reprend largement le second rapport du CERD [Jehl et al.95], décrit l'utilisation du planificateur PASCALE combiné à un estimateur d'état sur le problème de la reprise. Nous présentons tout d'abord PASCALE et le formalisme sur lequel il se base, justifions le choix de ce planificateur pour nos premières expérimentations, modélisons le problème dans ce formalisme, donnons un exemple de plan de reprise généré, décrivons précisément le rôle de l'estimateur d'état, et concluons sur ces expérimentations et leurs implications pour la suite de l'étude.

C.1 PASCALE

C.1.1 Un planificateur à portée générale pour ESTO

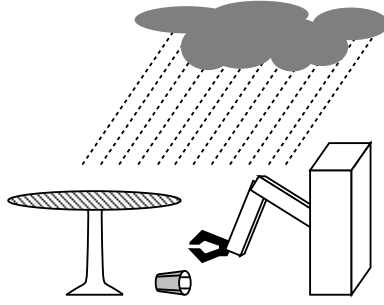
Pour générer des plans, un planificateur à portée générale s'appuie sur les éléments suivants. Un modèle de l'environnement et des actions sert à effectuer des prédictions sur l'état de l'environnement, i.e., à déterminer quels états peuvent résulter de l'exécution d'une action pouvant être prescrite par le planificateur. Un modèle des plans que l'on souhaite générer sert à déterminer dans quelle mesure un plan satisfait les objectifs donnés. Des algorithmes de recherche ont pour rôle de chercher un plan satisfaisant au mieux les objectifs dans l'espace des plans possibles.

Les travaux sur la planification réalisés à l'IRISA visent à proposer une modélisation des actions et des plans adaptée à la prise en compte de l'incertitude intervenant dans les environnements stochastiques totalement observables (ESTO), et à celle de contraintes de temps de génération. Cette modélisation, mise en œuvre au sein d'un planificateur baptisé PASCALE, a les caractéristiques suivantes.

La modélisation de l'environnement et des actions gère une information incertaine sur l'état de l'environnement au moment de la planification, ainsi que des actions stochastiques. Elle permet de prédire quelle est la probabilité que l'environnement se trouve dans tel ou tel état suite à l'exécution d'une action.

Les plans sont des programmes réactifs modélisés par des automates d'états finis. Ils décrivent une fonction associant l'état de l'environnement à l'action à exécuter en réaction à l'évolution de l'environnement vers cet état. Du fait des actions stochastiques, cette évolution était incertaine lors de la génération. La modélisation des plans permet de prédire si un plan satisfait les objectifs donnés. Dans le cas où le temps de génération alloué pour produire un plan complètement satisfaisant est insuffisant, elle permet d'évaluer l'utilité d'un plan partiel, grâce aux informations probabilistes disponibles au niveau de la modélisation des actions, en utilisant des principes de la théorie de la décision [Raiffa70]. L'utilité prend par exemple en compte la probabilité de satisfaction des objectifs d'un plan partiel, le coût des actions prescrites par ce plan, ainsi que la pénalité pour faire passer l'environnement par des états indésirables. Elle permet aussi de guider la recherche d'un plan satisfaisant au mieux les objectifs, puisqu'elle évalue l'adéquation de plans partiels (plans en cours de construction).

Ce modèle permet différentes formes de planification, notamment une planification en temps contraint, qui produit des plans dont l'utilité est une fonction croissante du temps de génération alloué, et une planification en-ligne, réactive, qui modifie le plan courant en cas d'événement

FIG. 2 – *Le robot et la tasse*

imprévu à l'exécution, ou qui étend ce plan (s'il était partiel) à la prise en compte des sources d'incertitudes les plus importantes pour le reste de l'exécution.

Nous présentons maintenant ces travaux un peu plus en détail. Pour une description plus formelle, le lecteur peut se référer à [Thiebaux et al.93, Thiebaux95]. Nous illustrerons cette présentation par un exemple très simple. Comme le montre la figure 2, il s'agit d'un robot fixe dont la tâche est de manipuler une tasse grâce à certaines actions qui seront détaillées plus tard. La tasse peut être **sur-table**, ou bien **par-terre** sur le sol. Lorsqu'elle est par-terre, elle peut être soit **face** au robot, comme sur la figure, soit orientée dans le sens inverse, le **fond** de la tasse faisant face au robot, soit encore **debout**. Nous distinguons ces différentes positions, car le robot utilisera des actions spécifiquement adaptées à telle ou telle position pour saisir la tasse. Les performances de ces actions peuvent être affectées s'il **pleut**, la scène se déroulant en plein-air.

C.1.2 Modélisation de l'environnement et des actions

Le formalisme utilisé dans PASCALÉ pour modéliser les états de l'environnement se base sur la logique et comporte les éléments suivants.

Tout d'abord, les *contraintes d'intégrité*, i.e., les propriétés vérifiées par tous les états de l'environnement physiquement possibles, sont modélisées par un ensemble de formules logiques du premier ordre. Pour l'exemple du robot et de la tasse, nous avons les contraintes suivantes, qui définissent les différentes positions dans laquelle la tasse peut se trouver (i.e., la tasse est soit sur la table, soit par terre, et lorsqu'elle est par terre, elle peut être dans une des trois positions de face, de fond, ou debout):

$$\left\{ \begin{array}{l} \text{sur-table} \Leftrightarrow \neg\text{par-terre}, \\ \text{par-terre} \Leftrightarrow \text{debout} \vee \text{face} \vee \text{fond}, \\ \text{debout} \Rightarrow \neg\text{face} \wedge \neg\text{fond}, \\ \text{face} \Rightarrow \neg\text{debout} \wedge \neg\text{fond}, \\ \text{fond} \Rightarrow \neg\text{face} \wedge \neg\text{debout} \end{array} \right.$$

Les modèles de cet ensemble de formules (i.e., les interprétations rendant ces formules vraies), représentent les états possibles de l'environnement. Pour notre exemple, ces modèles sont M_1, \dots, M_8 situés dans la colonne de gauche du tableau 1.

Un ensemble de formules en logique probabiliste, appelé *contraintes probabilistes*, définit les contraintes vérifiées par la distribution de probabilité sur les états de l'environnement à chaque instant, à défaut d'information supplémentaire aux contraintes d'intégrité. Par exemple, la première des contraintes probabilistes ci-dessous exprime qu'il y a 40% de chances qu'il pleuve,

état M	$\Pr(M)$
$M_1 = \{\text{il-pleut}, \neg\text{face}, \neg\text{fond}, \neg\text{debout}, \neg\text{par-terre}, \text{sur-table}\}$	0.08
$M_2 = \{\text{il-pleut}, \text{face}, \neg\text{fond}, \neg\text{debout}, \text{par-terre}, \neg\text{sur-table}\}$	0.14
$M_3 = \{\text{il-pleut}, \neg\text{face}, \text{fond}, \neg\text{debout}, \text{par-terre}, \neg\text{sur-table}\}$	0.14
$M_4 = \{\text{il-pleut}, \neg\text{face}, \neg\text{fond}, \text{debout}, \text{par-terre}, \neg\text{sur-table}\}$	0.04
$M_5 = \{\neg\text{il-pleut}, \neg\text{face}, \neg\text{fond}, \neg\text{debout}, \neg\text{par-terre}, \text{sur-table}\}$	0.12
$M_6 = \{\neg\text{il-pleut}, \text{face}, \neg\text{fond}, \neg\text{debout}, \text{par-terre}, \neg\text{sur-table}\}$	0.21
$M_7 = \{\neg\text{il-pleut}, \neg\text{face}, \text{fond}, \neg\text{debout}, \text{par-terre}, \neg\text{sur-table}\}$	0.21
$M_8 = \{\neg\text{il-pleut}, \neg\text{face}, \neg\text{fond}, \text{debout}, \text{par-terre}, \neg\text{sur-table}\}$	0.06

TAB. 1 – Distribution de probabilité par défaut du domaine du robot et de la tasse

à défaut d'information sur la météo d'aujourd'hui, et la seconde que la tasse à 70% de chances d'être de face ou de fond avec à défaut d'information sur sa position actuelle :

$$\left\{ \begin{array}{l} \Pr(\text{il-pleut}) = 0.4, \\ \Pr(\text{face} \vee \text{fond}) = 0.7, \\ \Pr(\text{sur-table}) = 0.2 \end{array} \right\}$$

Il est possible de calculer une *distribution de probabilité par défaut* sur les états, qui respecte ces contraintes, et qui sera celle sur laquelle le planificateur se basera en l'absence d'information fournie par les capteurs sur l'état courant de l'environnement. Pour notre exemple, les probabilités par défaut des différents états sont représentées dans la colonne de droite du tableau 1.

L'information disponible sur la situation actuelle de l'environnement, qui peut être incomplète, est représentée par une formule logique. Par exemple, $\text{il-pleut} \wedge (\text{sur-table} \vee \text{face})$ exprime qu'il pleut en ce moment, et que la tasse est sur la table ou de face. Lorsque cette information est acquise, il est possible de déterminer quels sont les états dans lequel l'environnement peut se trouver : ce sont tous les modèles vérifiant à la fois les contraintes d'intégrité et la nouvelle information. De plus, il est possible de *réviser* la distribution de probabilité par défaut de manière à tenir compte de la nouvelle information.⁵ Par exemple, avec l'information ci-dessus, on obtient les deux états et les probabilité suivantes :

$$\begin{array}{ll} M_1 = \{\text{il-pleut}, \neg\text{face}, \neg\text{fond}, \neg\text{debout}, \neg\text{par-terre}, \text{sur-table}\} & 0.36 \\ M_2 = \{\text{il-pleut}, \text{face}, \neg\text{fond}, \neg\text{debout}, \text{par-terre}, \neg\text{sur-table}\} & 0.64 \end{array}$$

Les actions dont on dispose pour faire évoluer l'environnement sont stochastiques, i.e, elle produisent certains effets avec une probabilité différente selon l'état dans lequel elles sont exécutées. Elles sont modélisées par un ensemble de paires $\langle pre, Eff \rangle$, où pre est une formule logique exprimant la *précondition* sous-laquelle l'action a certains effets. Eff est un ensemble de paires $\langle eff, \pi \rangle$, où π est la probabilité que *l'effet* eff (décrit par une formule logique) soit produit, sachant que la précondition pre est vérifié dans l'état dans lequel l'action est exécutée.

Pour notre exemple, le robot dispose des actions montrées en figure 3.

- *déposer* est utilisée pour déposer la tasse debout sur le sol lorsqu'elle est initialement sur la table. S'il ne pleut pas, l'action réussit avec une probabilité de 0.8. Lorsqu'elle échoue,

5. On se référera à [Thiebaut et al.93] pour la définition formelle de la révision de la distribution de probabilité par défaut.

$$\begin{aligned}
déposer &= \left\{ \left\langle \begin{array}{l} \neg\text{il-pleut} \wedge \text{sur-table}, \{ \langle \text{debout}, 0.8 \rangle, \langle \text{face}, 0.2 \rangle \} \\ \text{il-pleut} \wedge \text{sur-table}, \{ \langle \text{debout}, 0.6 \rangle, \langle \text{face}, 0.4 \rangle \} \\ \neg\text{sur-table}, \{ \langle \text{vrai}, 1.0 \rangle \} \end{array} \right\rangle, \right\} \\
redresser &= \left\{ \left\langle \begin{array}{l} \neg\text{il-pleut} \wedge \text{fond}, \{ \langle \text{debout}, 1.0 \rangle \} \\ \text{il-pleut} \wedge \text{fond}, \{ \langle \text{debout}, 0.8 \rangle, \langle \text{fond}, 0.2 \rangle \} \\ \neg\text{fond}, \{ \langle \text{vrai}, 1.0 \rangle \} \end{array} \right\rangle, \right\} \\
tourner &= \left\{ \left\langle \begin{array}{l} \text{face} \vee \text{fond}, \{ \langle \text{face}, 0.5 \rangle, \langle \text{fond}, 0.5 \rangle \} \\ \neg(\text{face} \vee \text{fond}), \{ \langle \text{vrai}, 1.0 \rangle \} \end{array} \right\rangle, \right\} \\
attendre &= \left\{ \left\langle \begin{array}{l} \text{il-pleut}, \{ \langle \neg\text{il-pleut}, 0.1 \rangle, \langle \text{il-pleut}, 0.9 \rangle \} \\ \neg\text{il-pleut}, \{ \langle \text{il-pleut}, 0.1 \rangle, \langle \neg\text{il-pleut}, 0.9 \rangle \} \end{array} \right\rangle, \right\}
\end{aligned}$$

FIG. 3 – Description des actions du domaine du robot et de la tasse

la tasse se retrouve de face, le bras du robot étant emporté par son inertie. S’il pleut, le pourcentage d’échecs s’accroît, la tasse devenant glissante. Si la tasse n’était initialement pas sur la table, l’action est inapplicable : rien n’est changé (effet *vrai*).

- *redresser* est utilisée pour redresser la tasse lorsque son fond fait face au robot. Cette action réussit toujours s’il ne pleut pas. S’il pleut, la tasse devient glissante et le robot risque de la lâcher avant qu’elle ait atteint la position debout avec une probabilité de 0.2. La tasse retombe alors dans sa position de fond.
- *tourner* sert à faire tourner la tasse de sa position de face vers sa position de fond, et vice versa. Le bras du robot n’étant pas conçu pour effectuer des mouvements latéraux, la seule solution est de donner une poussée à la tasse. Celle-ci se retrouve dans une nouvelle position complètement aléatoire.
- *attendre*. Il s’agit pour le robot d’attendre un laps de temps prédéfini, avec une probabilité de 0.1 que les conditions météo aient changé à la fin du délai. Cette attente peut s’avérer fructueuse si l’on désire accroître la probabilité de succès des actions.

Notons que les effets des actions sont exprimés de façon assez concise : il n’est pas nécessaire de spécifier explicitement ce qu’une action a laissé inchangé (par exemple, la pluie pour les trois premières actions), ni tous les faits que l’action a modifié (ou *ramifications*, par exemple, il n’est pas nécessaire de spécifier que la première action amène la tasse par terre). Les ramifications et les faits inchangés sont déduits automatiquement à partir des contraintes d’intégrité via le calcul du résultat d’une action. Ce calcul, qui est assez complexe, encode l’hypothèse que les états résultant de l’exécution d’une action sont ceux qui changent minimalement l’état dans lequel l’action est exécutée (car l’action n’est pas censée avoir changé radicalement l’état de l’environnement) tout en vérifiant les effets décrits et les contraintes d’intégrité. Par exemple, si l’on exécute *déposer* dans un état sur lequel l’information disponible est $\text{il-pleut} \wedge (\text{sur-table} \vee \text{face})$ comme précédemment, on obtient les états résultants suivants :

$$\begin{aligned}
M_2 &= \{ \text{il-pleut}, \text{face}, \neg\text{fond}, \neg\text{debout}, \text{par-terre}, \neg\text{sur-table} \} \\
M_4 &= \{ \text{il-pleut}, \neg\text{face}, \neg\text{fond}, \text{debout}, \text{par-terre}, \neg\text{sur-table} \}
\end{aligned}$$