Congrès sur la Sureté des systèmes électriques et électroniques.
Toulouse, France, 2 - 6 Octobre 1979.
CEA - CONF 5049

23.3.79

INIS

FR8001410

LES METHODES PROBABILISTES APPLIQUEES A DES PROBLEMES DE SOURCES ELECTRIQUES EN SURETE NUCLEAIRE

par : A. CARNINO - C.E.A.-DSN

M. LLORY - EdF - Etudes et Recherches/Clamart

R E S U M E

Il a souvent été demandé à la Sûreté Nucléaire de quantifier les marges de sécurité et d'évaluer le risque. Pour ce faire, ce sont les méthodes probabilistes qui se sont avérées les plus prometteuses. Sans remplacer pour autant complètement la sûreté déterministe, elles sont maintenant couramment employées tant au stade de la fiabilité ou disponibilité de systèmes que pour déterminer les séquences accidentelles envisageables. Nous montrons dans ce papier une application liée au problème des sources électriques, tout en indiquant les méthodes mises en oeuvre. Il s'agit du calcul de la probabilité de perte de l'ensemble des sources électriques d'une centrale nucléaire à eau sous pression, de l'évaluation par arbres de défaillances de la fiabilité des diésel et de la détermination de séquences accidentelles qui pourraient être engendrées par l'initiateur "perte totale des sources électriques" et avoir des conséquences sur l'installation ou l'environnement.

En matière de sûreté ou de sécurité, il est très difficile de procéder à des évaluations globales chiffrées et de savoir jusqu'où aller. Rappelons la célèbre phrase "How safe is safe enough ?". La sûreté nucléaire est pratiquée depuis de nombreuses années par des méthodes déterministes : méthode de défense en profondeur des barrières qui constituent un obstacle physique entre les matières radioactives et l'environnement, conception, protection, surveillance et moyens d'intervention sont les éléments des dispositions générales adoptées. Il est aussi défini des accidents de "dimensionnement" - c'est-à-dire des accidents qui par leurs conséquences enveloppent d'autres accidents moins graves - et servent de base au dimensionnement des systèmes de protection et de sauvegarde. La sûreté basée sur ces principes est certes fondamentale et efficace, mais elle ne peut être quantifiée. Pour cela, ce sont les méthodes probabilistes qui se sont avérées les plus efficaces. Elles permettent de quantifier en termes de probabilités et conséquences les accidents envisagés et étudiés, et de connaître la fiabilité disponibilité des systèmes qui composent un réacteur nucléaire. Elles peuvent de plus apporter une règle homogène d'évaluation de la sûreté, depuis la conception jusqu'à l'exploitation des systèmes importants pour la sûreté ou liés directement à cette dernière.

Il nous a paru ici intéressant non pas de développer les théories et méthodes que nous utilisons mais de montrer sur des exemples concrets la façon dont nous utilisons ces méthodes probabilistes en sûreté nucléaire.

Cette communication traite des exemples suivants :

- la probabilité de perdre l'ensemble des sources électriques (sources du réseau et sources internes) sur un réacteur à eau sous pression de 900 MW du type de FESSENHEIM.

- la fiabilité des groupes diésel de secours, ensemble intervenant dans les problèmes précédents.

- la probabilité des séquences accidentelles qui pourraient être engendrées par la perte des sources électriques.

./...

Nous concluons ensuite sur l'utilisation des méthodes probabilistes tout en indiquant leurs limites actuelles et les domaines de recherche qu'il reste à développer pour en accroître la crédibilité et déboucher ultérieurement sur des réglementations comportant des chiffres de probabilité.

1 - ETUDE DE LA PROBABILITE DE PERTE TOTALE DES SOURCES ELECTRIQUES SUR UN REACTEUR A EAU SOUS PRESSION DE 900 MWe

L'étude est basée sur les résultats d'exploitation observés par EdF sur des matériels analogues à ceux prévus dans les schémas des centrales actuelles en service et des futures centrales. Le nombre de données recueillies et la méthode utilisée pour les obtenir permettent une évaluation réaliste des paramètres de fiabilité de ces matériels (taux de défaillance et de réparation).

La méthode proprement dite fait appel, pour tenir compte du caractère réparable des matériels, au modèle de Markov qui permet de connaître pour chaque configuration du système l'évolution en fonction du temps de la probabilité Po de perte simultanée de toutes les sources d'alimentation.

L'application de cette méthode nécessite une transposition préalable du schéma réel en un schéma équivalent (figure 1).

Pour chaque situation possible des sources électriques, on effectue une étude de la sensibilité de Po aux différents paramètres. Elle permet de déterminer une plage d'incertitude raisonnable pour la probabilité Po.

Les défaillances de mode commun entre sources externes ou internes sont introduites sous forme paramètrique de façon à déterminer la valeur de ces paramètres au-delà desquelles elles peuvent être négligées.

1.1 - Schéma

Le schéma équivalent d'alimentation électrique qui a servi de base à l'étude est indiqué figure 1. Sa conception, conforme au critère 17 de l'USAEC et à la norme IEE 308, est tel que chaque ensemble d'auxiliaires de sécurité et de sauvegarde peut être alimenté par 3 sources différentes :

./...

- source externe principale (transformateur de soutirage)
- source externe auxiliaire (transformateur auxiliaire)
- source interne (groupe diésel électrogène)

De façon à faciliter la collecte des résultats d'exploitation, le schéma réel a été transposé en schéma équivalent (figure 1) dans lequel chaque zone correspond à un ensemble homogène de matériels pour lequel il est possible de recueillir des données de fiabilité et de réparabilité.

1.2 - Données issues d'exploitation

Pour chaque zone, on a retenu les seuls incidents dont le mode de défaillance conduisait à une perte de la zone considérée. Ce tri a nécessité une analyse incident par incident.

Les résultats portent sur les deux paramètres suivants caractérisant chaque zone :

- taux de défaillance (λ_i)
- temps moyen de réparation ($1/\mu_i$)

Ils sont indiqués dans le tableau n° 1.

1.3 - Position du problème et méthode utilisée

Rappelons brièvement que les auxiliaires de sûreté peuvent être alimentés de deux façons différentes :

- par l'une ou l'autre de deux sources externes,
- en cas de défaillance des sources précédentes par deux sources internes.

Une seule des quatre sources précédentes suffit à fournir la puissance nécessaire à l'alimentation du nombre minimal d'auxiliaires de sûreté requis.

Du point de vue de la fiabilité d'alimentation des auxiliaires de sûreté, le système d'alimentation électrique offre donc une redondance d'ordre 4.

On cherche à évaluer la probabilité de défaillance simultanée de toutes les sources d'alimentation P_o, à partir des différentes configurations imposées par l'indisponibilité d'une ou plusieurs sources.

Tous les éléments du système d'alimentation étant réparables, les quatre sources peuvent être considérées comme telles et il est alors possible de décrire le comportement global du système par un processus de "naissance et de mort". Le modèle dit "Markov" peut permettre de représenter un tel processus sous réserve d'un certain nombre d'hypothèses qui seront exposées par la suite.

Chacune des sources peut présenter plusieurs états : disponible ou indisponible pour les sources externes ; disponible à l'arrêt, disponible en marche ou indisponible pour les sources internes.

Il en résulte pour le système un nombre élevé de combinaisons d'états élémentaires qui peut toutefois être réduit en considérant que, sur le plan de la fiabilité, les deux sources internes et les deux sources externes sont respectivement identiques (mêmes valeurs attribuées à leurs paramètres de fiabilité).

1.4 - Méthode de Markov et graphes correspondants

Le système se trouvant à l'instant t = 0 dans un état initial donné peut à un instant ultérieur t quelconque changer d'état pour se trouver dans un état intermédiaire plus dégradé. La transition se caractérise alors par le taux de défaillance de la source dont l'indisponibilité a provoqué le changement d'état.

D'une façon plus générale le système étant dans un état intermédiaire quelconque à l'instant t, une transition peut se produire qui se caractérise par :

- un taux de défaillance λ s'il s'agit d'une dégradation
- un taux de réparation μ s'il s'agit d'une réparation

On est donc amené à examiner dans chaque configuration toutes les transitions possibles entre états intermédiaires, en leur affectant les taux λ ou μ correspondants.

Ceci conduit à de nombreux graphes dont nous donnons figure 2 un exemple. Ils sont établis avec les hypothèses suivantes :

- dans l'intervalle de temps Δt on ne peut perdre ou retrouver la disponibilité que d'une seule source à la fois.

./...

- les possibilités de réparation (pièces détachées, personnel) sont telles que les travaux puissent être entrepris sans délai sur l'ensemble des sources quel que soit le nombre de sources indisponibles.

Cette dernière hypothèse permet d'adopter pour les configuration des taux de réparation μ identiques pour un type donné de sources.

Nous ne rappellerons pas ici le détail du principe de la méthode de Markov. Elle permet à partir des graphes précédemment tracés d'établir pour chaque cas étudié un système d'équations différentielles dont la résolution permet d'obtenir l'expression de la probabilité $P_o(t)$ de perdre toutes les sources à un instant donné, ce qui est l'état absorbant final du graphe.

Les conditions initiales sont telles que pour $t = 0$, $P_o(0) = 0$ quelle que soit la configuration étudiée.

La résolution de chaque système comporte l'établissement de la matrice de probabilité correspondante, les calculs étant effectués par un programme.

Lorsque nous avons évalué l'influence des modes communs sur le schéma, nous avons utilisé encore la même méthode avec des états de transition supplémentaires, séparés des précédents et générés par les modes communs seuls (figure n° 2)

1.5 - Interprétation des résultats obtenus (figure 3)

La configuration totale du système normal (2 R - 2 Da) peut-êt considéré comme celle de référence.

Lors du premier démarrage de la tranche, la vérification de chaque élément du système permet de conclure que ce dernier se trouve dar cette configuration de référence.

Pendant la période ultérieure de fonctionnement et quelle que soit la durée de cette période, l'évolution prévisible du système peut être décrite de la façon suivante :

- Tant qu'aucun évènement ne provoque une modification constatable de l'état des sources (indisponibilité d'une source quelconque, mise en service permanent d'une source interne), la probabilité P_o sur un intervalle de durée t est donnée par la courbe de référence.

./...

Les essais périodiques pratiqués pendant cette période n'entraînent, dans la mesure où ils sont réussis, aucune modification constatable du système et ne peuvent de ce fait modifier la valeur de P_o.

- Dès l'instant où l'on constate une modification de la situation précédente -indisponibilité d'une ou des sources (s) externe (s) ou échec d'un essai de source interne - la configuration devient dégradée et la probabilité P_o n'est plus donnée par la courbe de référence.

  Une nouvelle configuration est initialisée ($t = 0$, $P_o = 0$) et l'évolution prévisible du système sur une nouvelle période de durée t est décrite par la courbe représentative de la configuration rencontrée.

- Cette situation subsiste jusqu'à l'instant du retour à l'état disponible de la ou des sources (s) indisponible (s). Dès cet instant la configuration de référence est initialisée à nouveau ($t = 0$, $P_o = 0$) et la probabilité P_o sur une nouvelle période de durée t est à nouveau donnée par la courbe de référence. Si la réparation n'est que partielle, la configuration retrouvée est intermédiaire et la probabilité P_o est donnée par la courbe correspondante.

- Chaque arrêt de tranche provoque une modification constatable de l'état des sources (indisponibilité pour entretien ...). Les vérifications effectuées à cette occasion sont analogues à celles réalisées avant le premier démarrage. Lors du redémarrage qui suit cet arrêt, la situation du système est donc identique à la situation initiale et son évolution prévisible sur une durée t semblable à la précédente.

  La période de durée t à prendre en compte est donc celle qui s'écoule entre deux arrêts programmés consécutifs. Cette période est en principe de 1 an sur les tranches du type de FESSENHEIM.

- La sensibilité des paramètres de fiabilité a été étudiée et donne des marges sur le résultat final qui permettent toujours de déduire les courbes resultantes lorsque les paramètres sont trouvés différents des moyennes indiquées.

  Tous ces résultats sont reportés sur la figure 3 et permettent de juger de l'indisponibilité de chacune des situations initiales envisagées.

./...

2 - ETUDE DE LA FIABILITE DES GROUPES DIESEL DE SECOURS

L'étude de la fiabilité des groupes diésel de secours d'une centrale nucléaire à eau sous pression, du type de FESSENHEIM, est un exemple caractéristique d'application de la méthodologie utilisée dans l'approche probabiliste des systèmes de sûreté.

Dans ce chapitre, après un rappel des objectifs de l'étude et la description des groupes diésel, de leurs fonctions, des différents sous-systèmes et composants, et de leur fonctionnement, on présente les trois étapes principales de l'analyse de fiabilité :

- l'analyse qualitative, utilisant systématiquement la méthode des arbres de défaillance,
- l'analyse quantitative, qui consiste à calculer la probabilité d'occurrence de la défaillance d'un groupe diésel,
- la synthèse des résultats de l'étude qui permet, d'une part, d'orienter les améliorations éventuelles à apporter aux groupes diésel et, d'autre part, de préciser la politique de tests à adopter.

2.1 - Objectifs de l'étude

L'étude réalisée a été motivée, d'une part par l'importance, sur le plan de la sûreté, des groupes électrogènes de secours, et, d'autre part, par le souci d'approfondir le fonctionnement et la connaissance de ce type d'appareil, afin d'être en mesure d'apporter d'éventuelle modifications et améliorations. L'objectif était plus précisément d'effectuer une étude détaillée, afin d'obtenir des enseignements quant aux modes de défaillance de ces systèmes et à leurs points les plus faibles. L'étude a été réalisée conjointement par un Ingénieur généraliste pratiquant les méthodes de fiabilité et par les spécialistes de ces appareils : du constructeur pour le moteur proprement dit, et des bureaux d'étude d'EdF pour le relayage.

2.2 - Description des groupes électrogènes de secours

En cas de perte totale de toutes les sources électriques extérieures au site d'une centrale nucléaire, les groupes diésel de secours doivent assurer l'alimentation des systèmes auxiliaires secourus qui ont un double rôle de sûreté :

./...

- permettre la mise à l'arrêt de la centrale dans des conditions sûres,
- assurer le maintien de l'intégrité du coeur du réacteur, c'est-à-dire permettre l'évacuation de la puissance résiduelle du coeur, même dans des circonstances accidentelles.

On est conduit à distinguer essentiellement 3 ensembles différents composant les diésels :

1 - La partie mécanique, comprenant notamment les sous-systèmes suivants :
   - les deux systèmes de lancement,
   - les circuits de combustible, de graissage et de prégraissage,
   - les deux circuits d'eau de refroidissement, et le circuit d'eau de préchauffage,
   - la station d'air comprimé à 4 bars,
   - le système de distribution du moteur, formé par l'ensemble des arbres à cames, des pignons de la chaîne cinématique et des culbuteurs,
   - le régulateur de vitesse,
   - le circuit d'admission et d'échappement, formé par les filtres à air, les deux turbo-compresseurs et les réfrigérants d'air de suralimentation.

2 - La partie électrique, constituée essentiellement de l'alternateur et du système d'excitation et de régulation de tension

3 - Les dispositifs de contrôle-commande, c'est-à-dire les ensembles de relayage

Sur signal de manque de tension notamment, chaque groupe diésel doit démarrer et prendre en 10 s. ses caractéristiques de vitesse et de tension. Dès que celles-ci sont atteintes, une double séquence a lieu : de délestage des auxiliaires, puis de relestage de ces auxiliaires

./...

sur les diésels. Le programme de relestage, réalisé par le relayage, dépend du type d'incident survenant. La durée de relestage est d'environ 1 mn.

Pour l'évaluation de la défaillance globale d'un groupe diésel, on distingue habituellement deux paramètres principaux :

- la probabilité de défaillance à la sollicitation δ . Cette défaillance peut résulter d'une défaillance pendant la phase d'attente, d'une défaillance au moment du démarrage, ou d'une défaillance non détectée, survenue pendant la dernière période de fonctionnement, qui aura été très probablement un test.

- la probabilité de défaillance en fonctionnement λ .

2.3 - Etude qualitative des groupes diésel

L'analyse qualitative d'un groupe a consisté à étudier systématiquement et de façon la plus complète possible, tous les modes de défaillance pouvant survenir sur les différents composants et sous-ensembles du groupe diésel, et à rechercher les combinaisons de défaillanc conduisant à celle du système entier. On a utilisé pour cette analyse la méthode des arbres de défaillance, les deux évènements : "défaillance du diésel à la sollicitation ou en fonctionnement" constituant les évènements indésirables. On retrouve ainsi la méthode de décomposition, déjà utilisée dans le chapitre précédent, appliquée dans ce cas de façon détaillée à un système particulier. On interrompt la décomposition au niveau des défaillances élémentaires de composants du diésel, pour lesquelles on dispose de données de fiabilité suffisamment sûres.

On insiste sur le fait qu'une telle étude n'apporte d'enseignements que si elle est approfondie. Il est nécessaire de tenir compte de tous les composants des différents circuits :

- pour les circuits hydrauliques : vannes, clapets, échangeurs de chaleur pompes, joints d'étanchéité, conduites, flexibles filtres, etc...
- pour les circuits électriques : on a distingué les défaillances propres aux bobines des défaillances propres à chaque contact de relais.

./...

Certains matériels élémentaires, paraissant importants ou spécifiques de l'équipement des groupes diésel, ont fait l'objet d'une étude particulière, également par arbres de défaillance.

2.4 - Etude quantitative

L'analyse quantitative consiste ensuite à calculer les probabilités δ et λ à partir des probabilités de défaillance élémentaires, en utilisant les règles simples du calcul des probabilités.

On précise que les taux de défaillance élémentaires sont supposés constants, c'est-à-dire correspondent à la durée de vie utile. Cette hypothèse parait fondée, du fait que les défauts de jeunesse sont éliminés par les essais de mise en service et les essais préliminaires, et que la période d'usure n'est pas atteinte sur les composants, en raison du faible taux d'utilisation des groupes diésel.

L'estimation ponctuelle des paramètres de fiabilité des diésel est, comme dans le cas précédent, complétée par un calcul d'incertitude tenant compte des marges d'erreur affectées aux taux de défaillance élémentaires

Les données de fiabilité utilisées sont généralement extraites de recueils de données. Pour certains composants particuliers, une enquête a été conduite auprès des spécialistes, et on a fait appel au "jugement de l'ingénieur", en affectant un facteur d'erreur important aux valeurs estimées.

2.5 - Résultats obtenus

Les résultats globaux sont présentés dans le tableau n° 2. Dans le tableau n° 3 on a fait figurer la contribution relative (en %) des différents sous-systèmes à la probabilité de défaillance d'un groupe diésel, ce qui permet de mettre en évidence les points les plus faibles de ces appareils.

L'étude réalisée a comporté également une analyse la plus complète possible des causes potentielles de défaillance de mode commun. On rappelle qu'en particulier les diésel d'une tranche nucléaire sont installés dans des locaux conçus pour résister aux séismes et aux missile:

./...

Deux causes communes potentielles de défaillance ont retenu notre attention :

- le risque d'incendie, dû à une fissuration d'une tuyauterie d'injection, et qui a conduit à gainer les tuyauteries d'injection,

- la présence d'eau dans le combustible : pour réduire ce risque, il est prévu de purger régulièrement les bâches contenant le combustible et d'installer une purge sur le point bas de la conduite d'alimentation.

Il est intéressant de comparer par ailleurs les résultats de calculs de fiabilité à ceux obtenus à partir de l'exploitation statistique de l'expérience d'utilisation des groupes diésel, à EdF (cf. tableau n° 2). Bien que cette étude statistique s'avère difficile, du fait de certaines imprécisions ou ambiguités des rapports d'incidents survenus sur ces appareils, on constate un bon accord entre ces valeurs expérimentales et les valeurs prévisionnelles. Cette concordance permet de valider globalement l'étude effectuée.

3 - ETUDE DE SEQUENCES ACCIDENTELLES PAR SUITE DE PERTE DE SOURCES ELECTRIQUES SUR UN REACTEUR A EAU SOUS PRESSION

Les études précédentes montrent comment on peut analyser des systèmes complexes. Elles ne peuvent cependant pas suffire à établir la probabilité de séquences engendrées par un évènement initiateur comme la perte des sources électriques. Pour cela il faut décomposer l'accident de telle sorte que les évènements rencontrés dans les séquences soient quantifiables. Il s'agit donc de pratiquer une méthode de décomposition, couramment utilisée pour calculer des évènements rares, soit par rapport à leur faible nombre, soit par rapport au temps d'observation, soit encor par rapport à leur population de référence. En effet, de telles séquences amènent à des calculs de probabilité de l'ordre de 10^{-6} ou 10^{-7} par année réacteur. Ces probabilités ne peuvent être bien entendu vérifiées par l'observation directe ; seule une méthode de décomposition peut permettre une approche du problème.

Dans la suite, nous entendrons par "accident" le fait que les barrières physiques qui existent entre les matières radioactives et l'environnement ont été atteintes simultanément ou en cascades. C'est donc l'enchaînement de ces évènements que nous allons analyser lorsque

il se produit une perte totale de sources externes sur un réacteur du type à eau sous pression.

3.1 - Méthodologie

Après avoir identifié les évènements possibles initiateurs d'accidents en analysant systématiquement les sources de rupture des barrières, il faut traiter le problème de la chronologie de l'accident. Deux parties sont importantes dans cette chronologie : les intervalles entre les divers évènements et les séquences. Il est nécessaire de connaître ces intervalles de façon à déterminer les valeurs atteintes par les paramètres caractéristiques des barrières (paramètres physiques et liés à l'environnement) pour connaître la façon dont ces valeurs sont atteintes. Ceci implique l'utilisation de codes de calculs dynamiques thermo-neutroniques. La connaissance des séquences est également nécessaire pour déterminer les actions qui peuvent avoir lieu pour éviter un accident ainsi que les "défaillances" de certains systèmes d'intervention et leurs conséquences.

Pour chaque barrière, il existe des systèmes de surveillance et de commande. Il existe également des systèmes conçus pour une intervention éventuelle de protection de la barrière. Après l'apparition d'un évènement initiateur, la perte de chaque barrière, l'une après l'autre, en ordre séquentiel, est considérée.

Pour chacune des barrières, on évalue, pour les différents dispositifs qui protègent les barrières et qui indiquent l'apparition d'un évènement initiateur, les probabilités de fonctionnement et de non fonctionnement. Des interventions possibles sont postulées et on détermine le délai dans lequel elles doivent agir. Si la barrière est intacte, la séquence d'accident est terminée sans conséquences graves. Si l'intervention a échoué, les conséquences sur les autres barrières sont déterminées. On évalue les effets sur les autres barrières d'une manière similaire.

Il est alors possible de tracer des arbres d'évènements montrant les intervalles de temps entre évènements ainsi que les délais de perte des barrières, et de construire les séquences d'accidents. Les probabilités de défaillance des détecteurs et des systèmes de sauvegarde

nous permettent de calculer la probabilité de toute séquence conduisant à un accident..

3.2 - Détermination des séquences accidentelles induites par une perte de sources électriques

On suppose que l'évènement initiateur a lieu quand le réacteur fonctionne à pleine puissance dans des conditions normales. Durant la première phase de l'accident, considérée ici comme étant approximativement la première minute, il est impossible de contrôler manuellement le réacteur et les systèmes de sauvegarde.

Dans l'éventualité d'une perte de sources électriques externes, les pompes primaires du réacteur, les pompes d'eau alimentaire et les pompes du condenseur s'arrêtent lentement sous l'effet de leurs volants d'inertie. Le circuit de contrôle volumétrique et chimique s'arrête d'injecter de l'eau dans les garnitures des pompes primaires et ces garnitures commencent à fuir. Quelques secondes après l'évènement initiateur, les signaux "perte d'énergie électrique externe", "faible débit primaire" "faible débit secondaire", etc... parviennent aux disjoncteurs d'arrêt d'urgence qui commandent la chute des barres.

Il existe une probabilité finie que ces signaux ne parviennent pas aux disjoncteurs (panne de mode commun) ou que certaines barres de contrôle ne tombent pas pour des raisons mécaniques très improbables. Au cours du régime transitoire qui suit, d'une durée inférieure à dix secondes, les soupapes de sûreté du pressuriseur sont activées ; la défaillance de ces vannes pourrait produire une perte de réfrigérant primaire.Au même moment, les diésels atteignent leur vitesse nominale. Ils peuvent alors être connectés aux systèmes de sauvegarde l'un après l'autre, à moins qu'ils ne tombent en panne (défaillance d'un diésel ou défaillance de mode commun de deux diésel). Si l'un des diésel démarre, le circuit d'injection de sécurité (RIS), le circuit de contrôle volumétrique et chimique (RCV) et le système d'aspersion de l'enceinte de confinement (EAS) deviennent opérationnels environ 30 secondes après la détection du premier signal. Juste avant cet instant, 20 secondes après l'évènement initiateur, les générateurs électriques des barres de contrôle s'arrêtent par leur propre inertie. Par conséquent, si le signal

de chute des barres n'a pas encore eu d'effet, il y a chute des barres sans signal du fait du manque d'énergie dans les électro-aimants de maintien des barres de contrôle (figure 4).

Les seules branches importantes des séquences d'accident sont celles correspondant à l'absence de diésel , car pour elles les systèmes RIS, RCV et EAS ne sont pas opérationnels. Cependant, le système d'alimentation de secours des générateurs de vapeur (ASG) peut encore fonctionner car il possède une pompe actionnée par une turbine à vapeur. La principale conséquence de la perte d'énergie externe ou interne est donc la défaillance du RCV à injecter de l'eau dans les garnitures des pompes primaires. La seconde barrière perd son intégrité par ces garnitures le débit de fuite approximatif peut être évalué à 20 m^3/h . Au cas où aucune des sources électriques externes et internes n'aurait été récupérée en une heure, le niveau d'eau dans le pressuriseur et dans les générateurs de vapeur s'abaisse et le système d'alimentation de secours ASG ne peut pas refroidir le réacteur. La deuxième barrière est entièrement perdue, et par conséquent, la première aussi (figure 5).

Les séquences d'accident ne sont pas encore terminées car la troisième barrière est intacte. Il est encore possible de récupérer une source électrique et, dans ce cas, d'utiliser le système d'aspersion de l'enceinte (EAS). Autrement, la température augmente rapidement dans l'enceinte jusqu'à la perte de la troisième barrière (figure 6).

On voit que connaissant la fiabilité ou la disponibilité, selon le cas, des systèmes concernés par ces séquences on peut en déduire la probabilité que l'évènement initiateur entraîne des conséquences importantes au niveau de l'installation et vis-à-vis de l'environnement.

4 - CONCLUSION

Par les différents exemples que nous venons de traiter rapidement, on voit bien apparaître l'utilisation que nous faisons, en sûreté nucléaire, des méthodes probabilistes. Les études de fiabilité/disponibilité des systèmes ou même des fonctions liées à la sûreté apportent des éléments quantitatifs intéressants à plusieurs niveaux :

./...

- pour la conception on peut comparer diverses solutions ou situations, vérifier la conformité à la réglementation, déterminer les points faibles éventuels et utiliser les résultats comme indications de l'ordre de grandeur des probabilités que l'on peut atteindre.

- pour l'exploitation et la sûreté, on peut obtenir par les mêmes méthodes, d'une part, une certaine homogénité depuis la conception jusqu'à l'exploitation et, d'autre part, envisager les scénarios accidentels et les quantifier pour déterminer les mesures complémentaires éventuelles à prendre.

Cependant, il faut être conscient des lacunes ou des limites dans l'utilisation de ces méthodes probabilistes. Il reste un effort important à faire en ce qui concerne la collecte de données opérationnelles, car on ne peut encore en général accorder beaucoup de crédibilité aux valeurs absolues calculées actuellement. D'autre part, le domaine des probabilités étudiées correspond à des évènements rares ; il y a donc également une voie de recherche à développer sur le plan des méthodes, car on ne dispose actuellement d'outils éprouvés que pour des statistiques avec échantillons importants. Il reste enfin deux domaines pour lesquels un effort important a été entrepris, ce sont les modes communs de défaillances et les facteurs humains qui peuvent avoir une influence considérable sur les calculs que nous réalisons. Il s'agit donc de mieux les identifier, de les quantifier et de déterminer des protections pour que leurs conséquences ne soient pas importantes.

TABLEAU N° 1

ETUDE DE LA PROBABILITE DE PERTE TOTALE DES SOURCES ELECTRIQUES

TAUX DE DEFAILLANCES PAR ZONE (cf. figure 1)

	Taux de défaillance λ_i		Temps moyen de réparations/zone (heures) ($\overline{Ti}$)	$\lambda i\overline{Ti}.10^{-6}$	Temps mini. de réparations (heures)	Temps maxi. de réparations (heures)
	(Zone x an)$^{-1}$	(Zone x heure)				
1	0,100	11,4 .10^{-6}	12	137	1	24,75
2	0,140	16,0 "	120	1 920	1,5	1344
3	0,010	1,14 "	8,75	10,0	0,2	17
4,4a,4b,4c,	0,045	5,13 "	89	456	1,5	624
5,5a,5b,5c, 5e,5f,5g	0,025	2,85 "	7,6	21,7	0,2	18,6
6	0,140	16,0 "	21	336	0,2	168
7	0,425	48,5 "	0,2	9,7	ε	1,5
8	0,010	1,14 "	8,75	10,0	0,2	17
9	0,140	16,0 "	21	336	0,2	168
10	0,760	86,8 "	0,2	17,4	ε	1,5
11	0,120	13,7 "	0,03	0,41	-	-
12	Au lancement : 1,5 % Au démarrage : 1,5 % En marche continue : $0,7.10^{-3}$/groupexheure		173		1440	0,1

TABLEAU N° 2

COMPARAISON DES RESULTATS DE CALCUL ET DE L'EXPERIENCE D'EXPLOITATION DES GROUPES DIESEL

Probabilité de défaillance totale	Résultats de calculs	Résultats expérimentaux
		Source : données EdF
au démarrage (γ)	$1,1.10^{-2}$ Facteur d'erreur : 2	3.10^{-2}
en fonctionnement	9.10^{-4}/h Facteur d'erreur : 3	7.10^{-4}/h

TABLEAU N° 3

CONTRIBUTION DES PRINCIPAUX SOUS-SYSTEMES AUX PROBABILITES DE DEFAILLANCE D' UN GROUPE DIESEL

SOUS-SYSTEME	Contribution relative (en %) à la probabilité de défaillance :	
	à la sollicitation	En fonctionnement
ENSEMBLE MECANIQUE		
- Circuit de combustible	34	53
- Circuit de graissage	2	6
- Circuits d'eau de refroidissement	4	12
- Circuits d'air-distributeur	13	11
- Régulateur de vitesse	2	1
- Systèmes de lancement	4	
- Circuits d'admission et d'échappement		13
ENSEMBLE ELECTRIQUE		
- Système d'excitation et de régulation de tension	3	4
ENSEMBLE DE CONTROLE-COMMANDE		
- Relayage	31	
- Disjoncteurs	7	

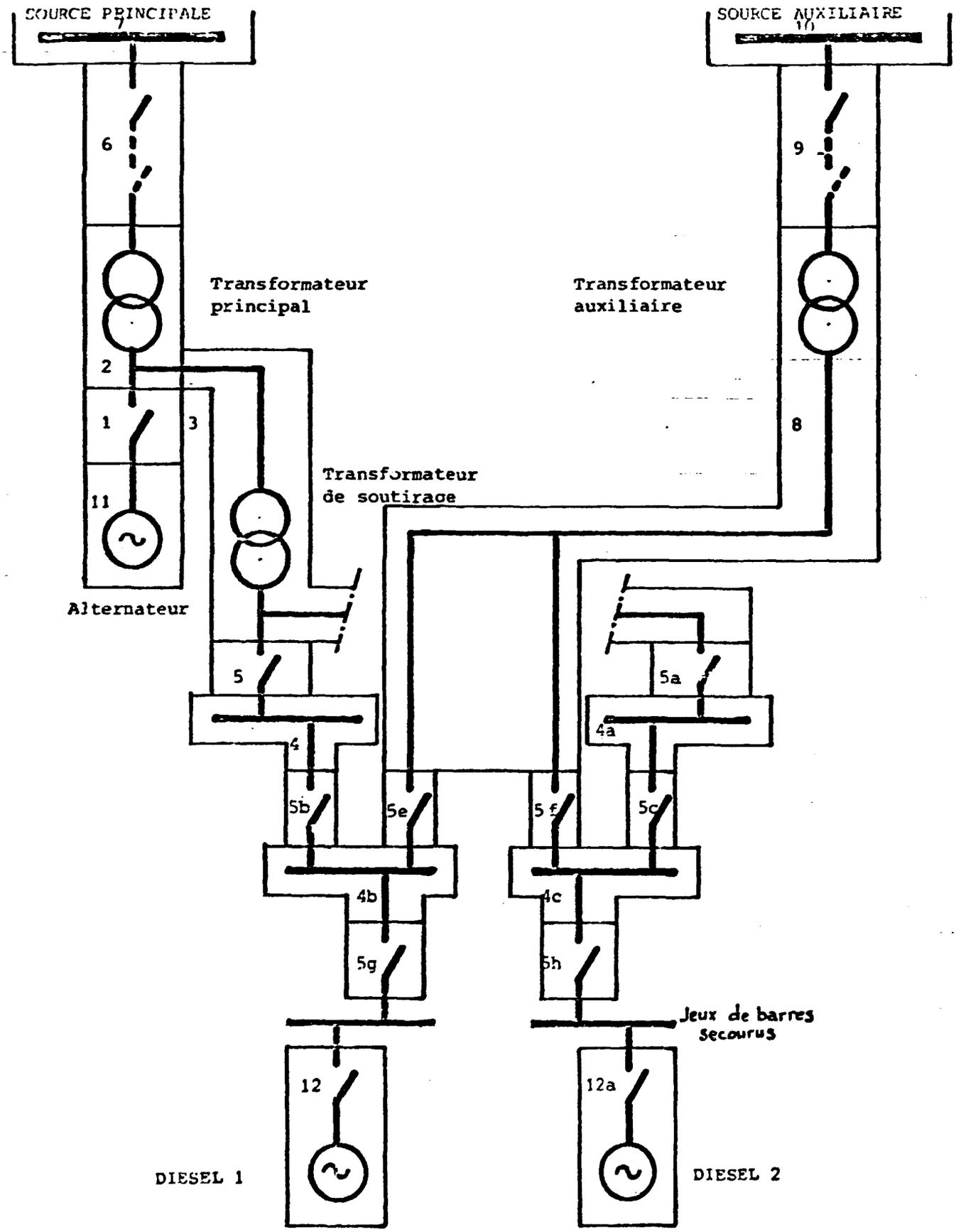
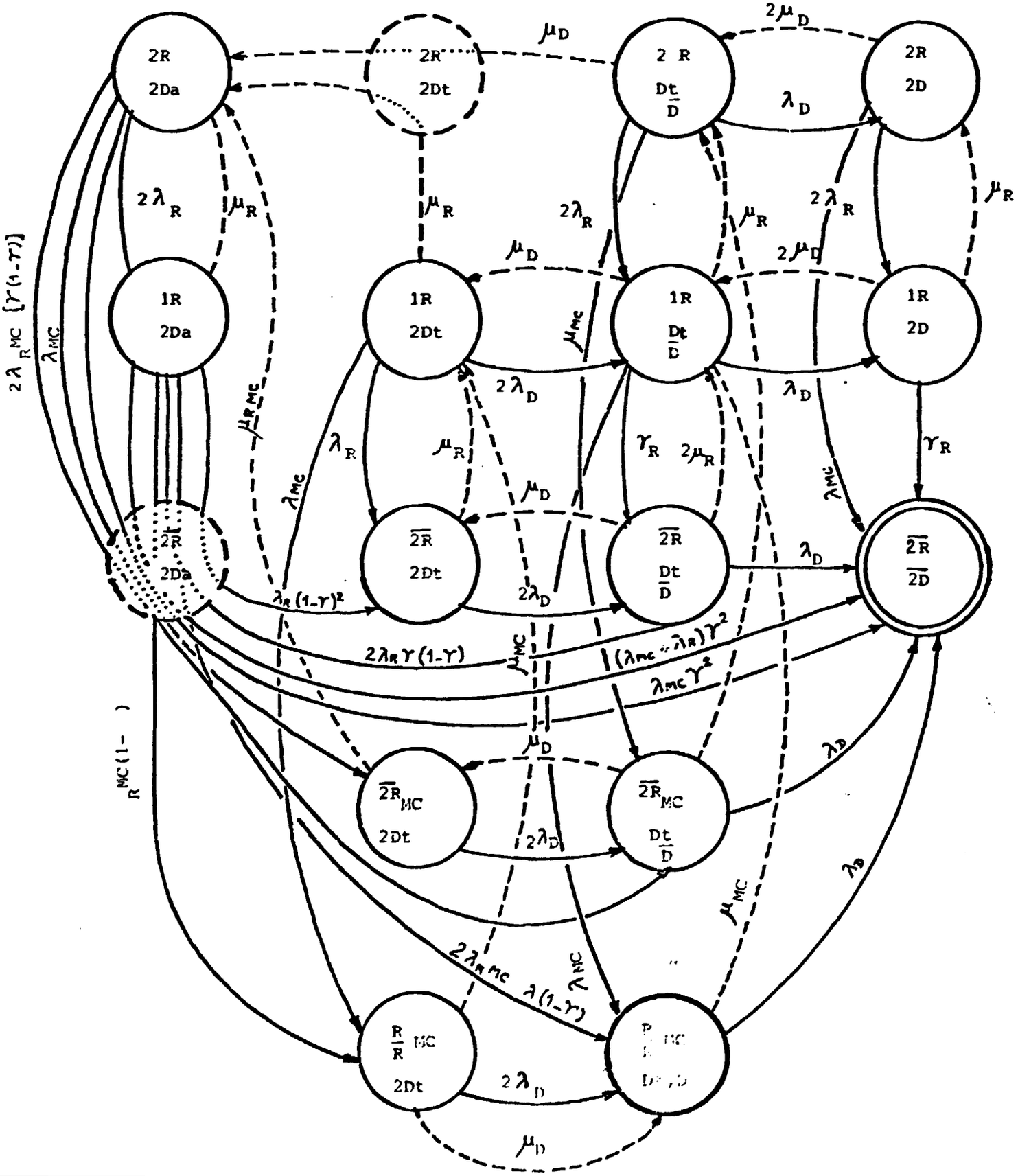


Figure 1

ALIMENTATION ELECTRIQUE

GRAPHE DE MARKOV (2 R - 2 Da)

AVEC MODE COMMUN ENTRE SOURCES EXTERNES



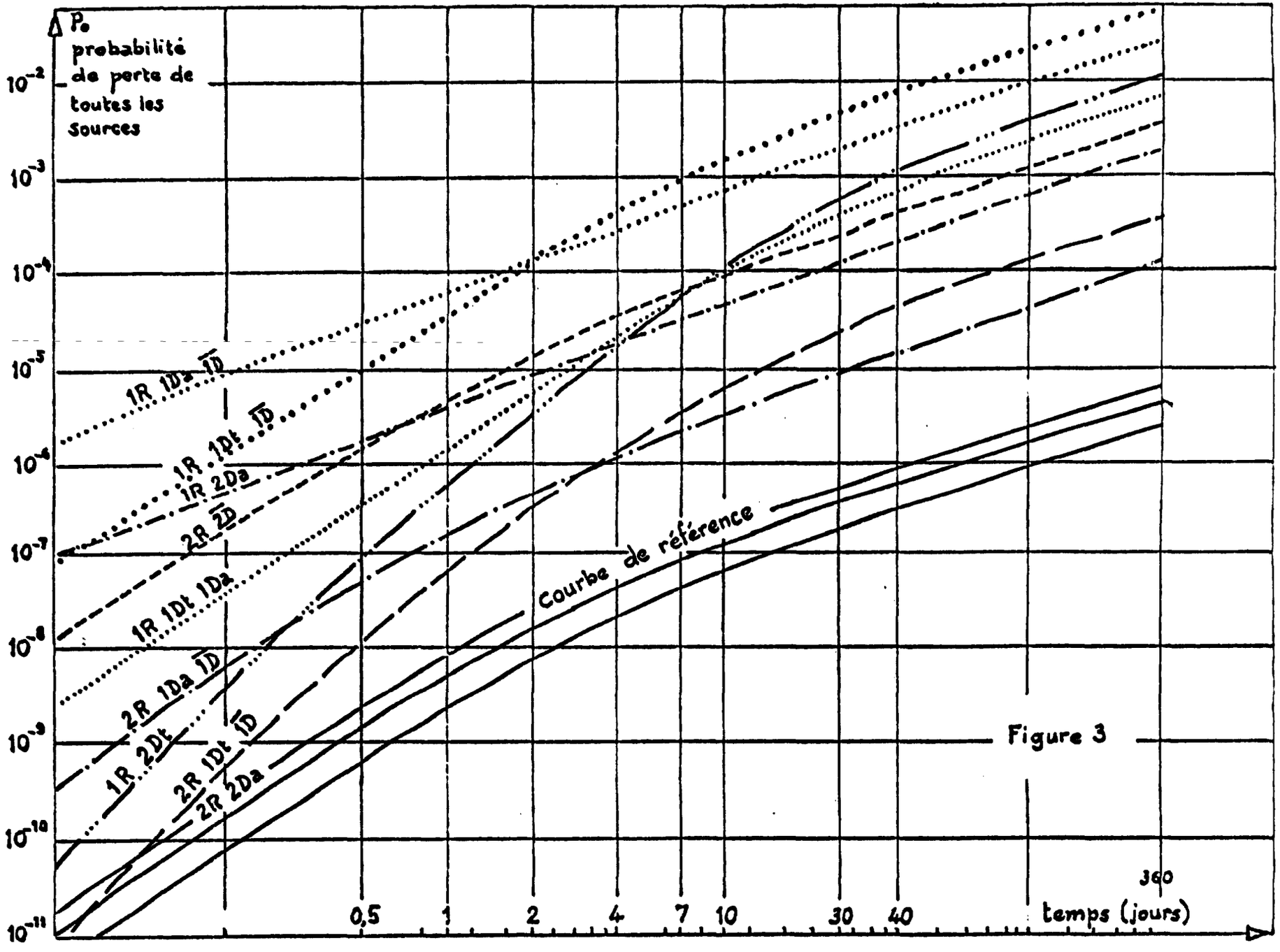

P_e
probabilité de perte de toutes les sources
10^{-2}
10^{-3}
10^{-4}
10^{-5}
10^{-6}
10^{-7}
10^{-8}
10^{-9}
10^{-10}
10^{-11}
1R 1Da $\overline{1D}$
1R 1Dt $\overline{1D}$
1R 2Da
2R $\overline{2D}$
1R 1Dt 1Da
2R 1Da $\overline{1D}$
1R 2Dt
2R 1Dt $\overline{1D}$
2R 2Da
Courbe de référence
0,5
1
2
4
7
10
30
40
360
temps (jours)

Figure 3

PROTECTION DES 3 BARRIERES.

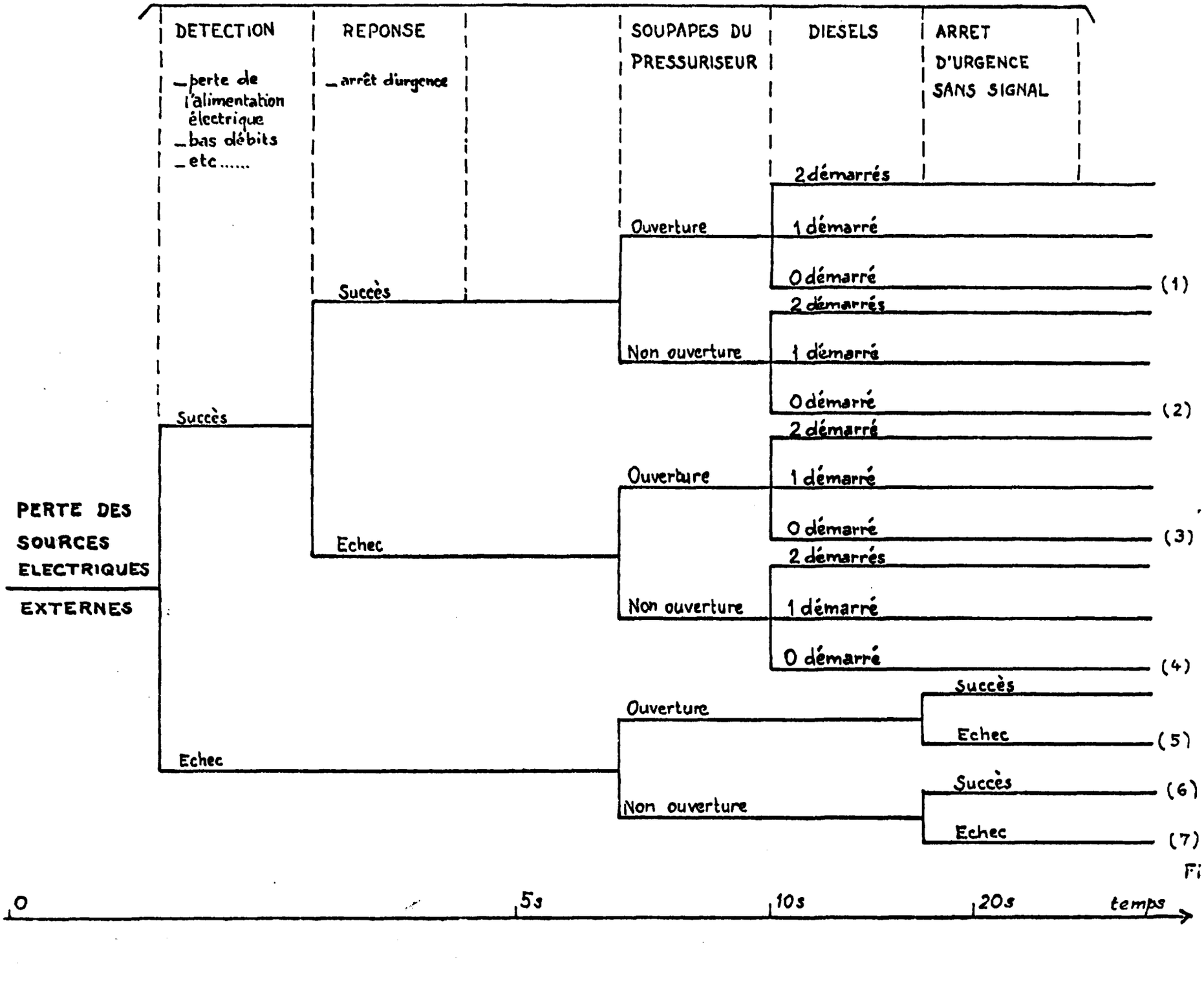


Figure 4.

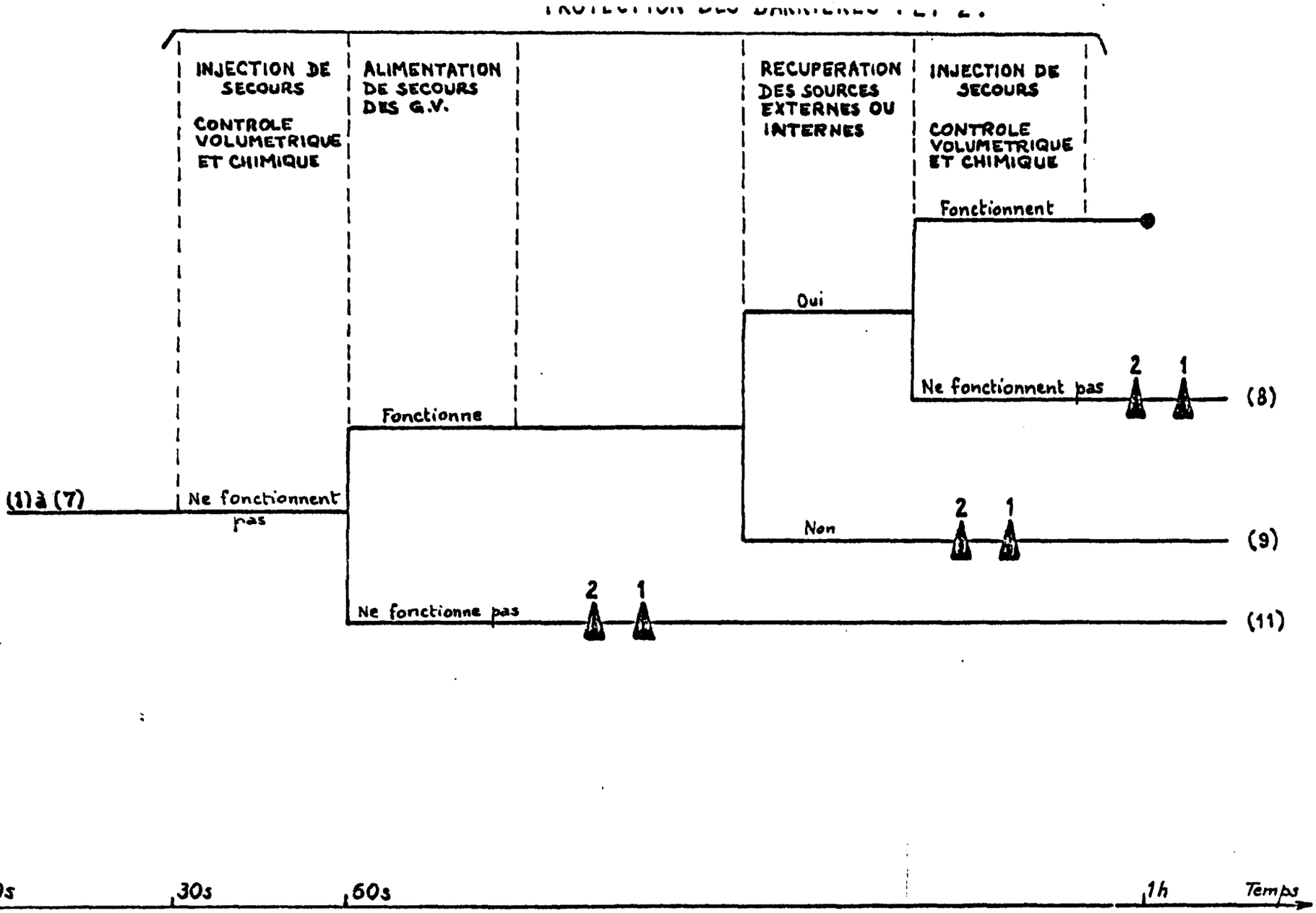

INJECTION DE SECOURS
CONTROLE VOLUMETRIQUE ET CHIMIQUE
ALIMENTATION DE SECOURS DES G.V.
RECUPERATION DES SOURCES EXTERNES OU INTERNES
INJECTION DE SECOURS
CONTROLE VOLUMETRIQUE ET CHIMIQUE
Fonctionnent
Oui
Ne fonctionnent pas
2
1
(8)
Fonctionne
(1) à (7)
Ne fonctionnent pas
Non
(9)
Ne fonctionne pas
(11)
20s
30s
60s
1h
Temps
X
Perte de la barrière X
Fin de la séquence

Figure 5.

PROTECTION DE LA 3E BARRIERE.

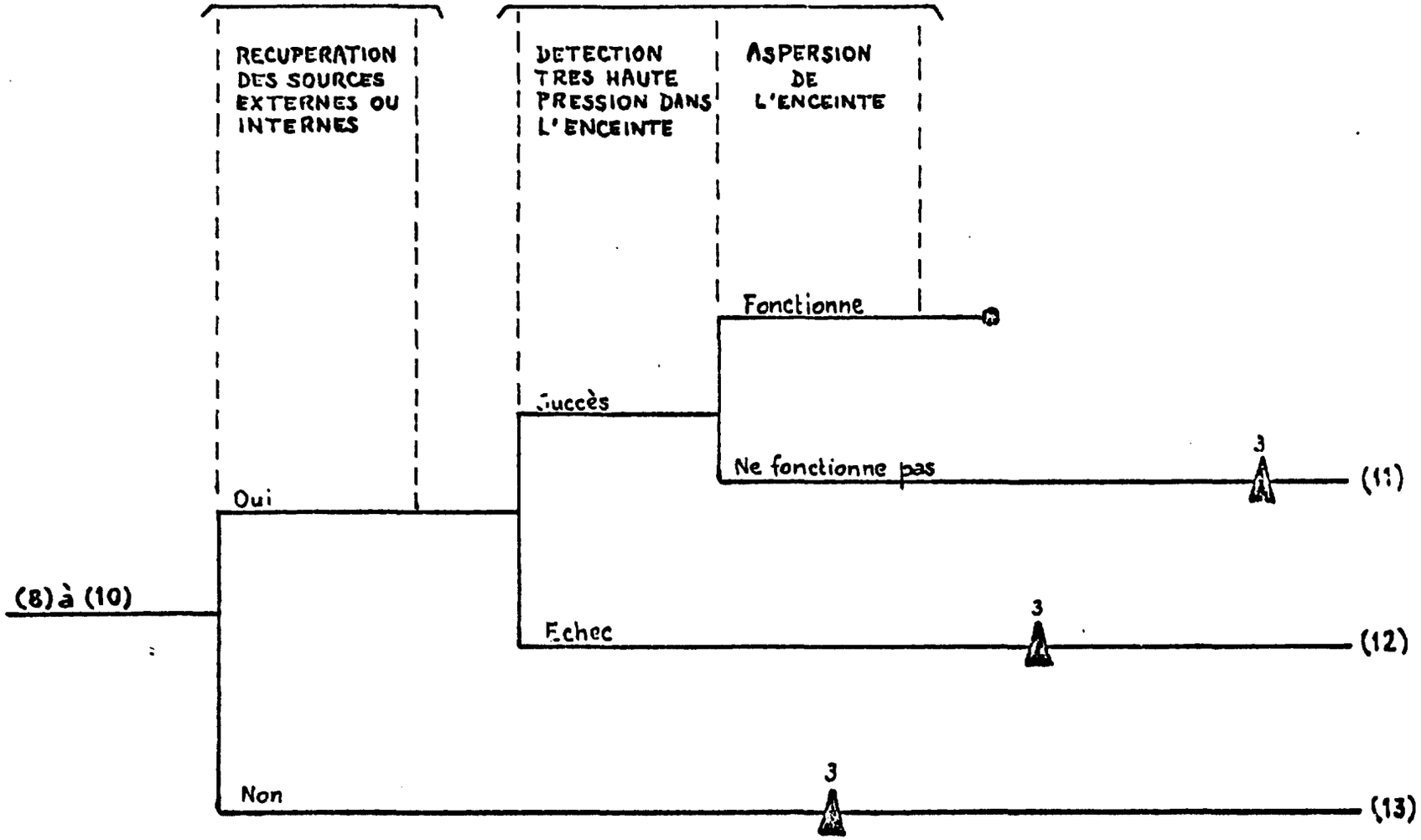


Figure 6.