Rébublique Algérienne Démocratique et Populaire
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

École Nationale Polytechnique

Département de Maîtrise des Risques
Industriels et Environnementaux (MRIE)
Filière QHSE-GRI
Centre de Recherche nucléaire de Draria

Mémoire de master en
QHSE-GRI

Étude de la fiabilité humaine et des défaillances de cause commune

Cas : Système d'arrêt d'urgence RPS d'un réacteur nucléaire

Ali BENZENOUNE

Sous la direction de

Pr. C.BOUTEKEDJIRET et **Mr. A. BENMOKHTAR**

Présenté et soutenu publiquement le : 18/06/2017

Composition du jury :

Président	M.Abdelmalek CHERGUI	Professeur, ENP
Promoteur	Mme. Chahrazed BOUTEKEDJIRET	Professeur, ENP
	Mr. Amine BENMOKHTAR	Maitre assistant, ENP
	M.Mouhamed BOUFENAR	Docteur, chercheur, CRND
Examinateur	Mme. Faiza ZIDOUNI	Docteur, USTHB
	M. Aboubaker KERTOUS	Maitre assistant, ENP
	M. Farid LEGUEBEDJ	Maitre assistant, ENP

ENP 2017

Rébublique Algérienne Démocratique et Populaire
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

École Nationale Polytechnique

Département de Maîtrise des Risques
Industriels et Environnementaux (MRIE)
Filière QHSE-GRI
Centre de Recherche nucléaire de Draria

Mémoire de master en
QHSE-GRI

Étude de la fiabilité humaine et des défaillances de cause commune

Cas : Système d'arrêt d'urgence RPS d'un réacteur nucléaire

Ali BENZENOUNE

Sous la direction de

Pr. C.BOUTEKEDJIRET et **Mr. A. BENMOKHTAR**

Présenté et soutenu publiquement le : 18/06/2017

Composition du jury :

Président	M.Abdelmalek CHERGUI	Professeur, ENP
Promoteur	Mme. Chahrazed BOUTEKEDJIRET	Professeur, ENP
	Mr. Amine BENMOKHTAR	Maitre assistant, ENP
	M.Mouhamed BOUFENAR	Docteur, chercheur, CRND
Examinateur	Mme. Faiza ZIDOUNI	Docteur, USTHB
	M. Aboubaker KERTOUS	Maitre assistant, ENP
	M. Farid LEGUEBEDJ	Maitre assistant, ENP

ENP 2017

A ma mère qui m'est la plus chère

A mon père, lumière de mes jours

A mes chères sœurs et frères

A la joie de ma vie, mes neveux

Asma et Abderrahmane

A mes amis

Je dédie ce modeste travail

BENZENOUNE Ali

Remerciements

La réalisation de ce mémoire a été possible grâce à ALLAH le tout puissant, pour le courage et la patience qu'il nous a donné pour accomplir ce travail.

Nous souhaiterions adresser nos remerciements les plus sincères aux personnes qui nous ont apporté leur aide et qui ont contribué à l'élaboration de ce mémoire. Nos profonds remerciements s'adressent à nos encadrants ; Madame BOUTEKEDJIRET Chahrazed et Monsieur BENMOKHTAR Amin qui se sont toujours montrés disponibles et à l'écoute tout au long du travail. Nous vous remercions aussi pour votre accueil et vos conseils. Veuillez trouver ici, les expressions de nos gratitudes et notre grande estime.

Nos profondes gratitudes et chaleureux remerciements s'orientent vers Monsieur BOUFENAR Mohamed, directeur adjoint du réacteur NUR pour ses judicieux conseils et son support permanent, ainsi que tout le personnel du Centre de Recherches Nucléaire de Draria qui ont su nous orienter par leurs conseils tout au long de ce travail.

Nos remerciements s'adressent aux membres du jury ; Mr CHERGUI Abdelmalek professeur à l'ENP qui a bien voulu présider ce jury, Mme ZIDOUNI Faiza, doctorante à l'USTHB, Mr KERTOUS Aboubaker et Mr LEGUEBEDJ Farid d'avoir bien voulu examiner ce travail modeste. Vous nous faites un grand honneur en acceptant de juger ce travail. Nous devons un remerciement à tous les enseignants de la filière QHSE-GRI qui nous ont fourni les outils nécessaires à la réussite de nos études universitaires.

Une pensée particulière est adressée aux étudiants qui nous ont côtoyés quotidiennement durant nos années d'étude au département qui nous ont apporté leur support moral et intellectuel tout au long de notre mémoire. Enfin, nous tenons à remercier chaleureusement, tous nos proches, amis et tous ceux qui, de près ou de loin, nous ont toujours soutenus et encouragés au cours de la réalisation de ce mémoire, pour leur confiance, leur support inestimable et leurs sollicitudes pour accomplir ce travail. À toutes ces personnes, nous présentons nos remerciements, notre respect et notre gratitude.

ملخص

تهدف هذه الدراسة إلى إدخال الخطأ البشري و الأعطاب ذات السبب المشترك في حساب إحتمالية عطب نظام التوقيف الإستعجالي لمفاعل البحث النووى نور بالدرارية (الجزائر العاصمة)

ويتالف هذا التقرير من فرعين رئيسيين : الجزء النظرى تطرق فيه للمفاهيم العامة للموثوقية البشرية و الأعطاب ذات السبب المشترك .الجزء الثانى يكرس لتقييم الخطأ البشري و دراسة الأعطاب ذات السبب المشترك.

سمحت هذه الدراسة الى استنتاج مفاده ان احنمالية عطب نظام التوقيف الإستعجالي للمفاعل النووي أكبر من التي عمل بها في الدراسات الإحتمالية للسلامة، و أن الخطأ البشري يشارك بنسبة تفوق في وقوع هذا الحدث

الكلمات المفتاحية: الموثوقية البشرية، الخطأ البشري، الأعطاب ذات السبب المشترك، نظام التوقيف الإستعجالي

Abstract

The objective of this study is the introduction of human error and common cause failures in the calculation of the probability of failure of RPS system of the NUR nuclear reactor at Draria Nuclear Research Center in Algiers.

The work consists of two main parts: a theoretical part, dealing with the general concepts of human reliability and failures of common cause. A second part dedicated to the evaluation of human error and the study of CCF.

This study led to the calculation that the probability of failure of the RPS system is higher than that calculated in the EPs analysis, and that human error contributes to more than 70% of the occurrence of this event.

Key words: Human reliability, Human error, Common Cause Failures, RPS.

Résumé

Cette étude a pour objectif l'introduction de l'erreur humaine et les défaillances de cause commune dans le calcul de la probabilité de défaillance du système RPS du réacteur nucléaire NUR, du Centre de Recherche Nucléaire de Draria (Alger).

Le travail est composé en deux parties principales : une partie théorique, traitant les concepts généraux de la fiabilité humaine et des défaillances de cause commune. Une deuxième partie dédiée à l'évaluation de l'erreur humaine et l'étude des DCC.

Cette étude a permet de conclure que la probabilité de défaillance du système RPS est plus élevée que celle calculée lors de l'analyse EPS, et que l'erreur humaine contribue à plus de 70% de l'occurrence de cet évènement.

Mots clés : Fiabilité humaine, Erreur Humaine, Défaillance de cause commune, RPS

Table des matières

Table des figures

Liste des tableaux

INTRODUCTION GENERALE

La diminution des accidents dans les dernières années est due au développement technologique considérable que connait le domaine de l'automatisation des systèmes de production et l'amélioration des systèmes de sécurité liés aux systèmes en questions. Cependant, ces systèmes hautement développés et qui possèdent un temps de réponses de l'ordre de la fraction de seconde n'élimine pas le rôle du facteur humain qui peut influencer par sa réaction et sa décision la sécurité du système.

Il a été observé que les échecs de système en raison de l'intervention humaine ne sont pas négligeables ; particulièrement quelques sources rapportent que l'erreur humaine est la cause des systèmes d'échecs qui, dans de nombreux cas, ont des conséquences désastreuses en raison de l'environnement homme-machine. En fait, les évaluations reconnaissent que les erreurs engagées par l'homme sont les causes de plus de 60% d'accidents et pour la partie restante les causes sont dues aux déficiences techniques. Généralement, dans des systèmes de fiabilité étudiés, l'évaluation se concentre sur des processus d'industrie et des technologies le constituant, ne tenant pas en compte des aspects qui dépendent de facteurs humains et sa contribution au même système de fiabilité [1].

Les défaillances de cause commune consiste en des pannes de composants répondant à quatre critères :

- deux ou plusieurs composants individuels échouent ou sont dégradés, y compris les défaillances pendant la demande, les tests en cours de service ou les lacunes qui auraient entraîné une panne si un signal de sollicitation avait été reçu ;
- les composants échouent dans une période de temps sélectionnée, de sorte que le succès de la mission PRA serait incertain ;
- les défaillances des composants résultent d'une seule cause partagée et d'un mécanisme de couplage ;
- une défaillance de composant se produit dans la limite de composant établie.

L'analyse de la fiabilité humaine (Human reliability analysis – HRA), a pour objet l'évaluation de l'intervention humaine dans un système de sécurité d'une chaine de production et la possibilité qu'une erreur commise par le facteur humain puisse conduire à un accident. La HRA est donc une étape clé dans une démarche de maîtrise des risques. Les études des

défaillances de cause commune vise en l'identification et la quantification des évènements pouvant altérer simultanément plusieurs composants d'un système et provoquent par la suite la panne de ce dernier.

La présente étude vise en l'introduction des notion de la fiabilité humaine et les défaillances de cause commune (DCC), dans le calcul de la probabilité de défaillance du système d'arrêt d'urgence (RPS) du réacteur nucléaire NUR de centre de recherche nucléaire de Draria. Pour ce faire l'étude comporte 04 chapitres :

- Le chapitre 01 traite les concepts généraux de la fiabilité humaine et présente par la suite les différentes méthodes de son évaluation ;
- Le chapitre 02 vise en l'introduction du concepts des défaillances de cause commune ;
- Le chapitre 03 est dédié à l'évaluation de la fiabilité humaine lors d'actionnement manuel du système RPS et la quantification des défaillances de cause commune du système de détection lié au système RPS.

Chapitre 1

FIABILITÉ HUMAINE

FIABILITÉ HUMAINE

Un système de production et ses systèmes périphériques sont constitués de nombreuses composantes techniques et humaines. Ces composantes peuvent être indépendantes les unes des autres comme il peut y avoir des interactions (interfaces homme-machines). Le facteur humain joue un rôle principal dans ces systèmes, notamment celui de la sécurité, où leur bon fonctionnement dépend du facteur humain (disponibilité, compétences, savoir-faire...).

Dans ce présent chapitre, nous allons aborder les notions et les concepts généraux de la fiabilité et l'erreur humaine. Nous donnerons ensuite la définition d'une barrière humaine de sécurité. Enfin, nous présenterons la démarche suivie pour l'évaluation de la fiabilité humaine.

1.1 DEFINITION DE LA FIABILITE HUMAINE

La fiabilité humaine est définie par : « *la probabilité qu'un opérateur accomplit correctement les tâches requises, dans des conditions données, et n'assume pas les tâches qui peuvent dégrader le contrôle du système* » [2]. Elle n'est pas réductible à la seule fiabilité du seul composant humain. C'est en réalité celle de l'homme pris dans son environnement, par nature complexe (matériel, procédural, organisationnel, culturel...). Elle dépend de ces différents facteurs humains et environnementaux, de leur complémentarité et de leurs influences sur les différents processus mis en jeu dans le travail des hommes (cognitif, affectif, sociologique, physique,...) [3].

1.2 HISTORIQUE DE LA FIABILITE HUMAINE

La fiabilité humaine a été reconnue en 1962 par l'Académie des Sciences comme une discipline et appartient aux Sciences de l'Ingénieur. Elle est appliquée aux systèmes à hauts risques : nucléaire et militaire. Le développement de cette discipline est dû à [4] :

- criticité grandissante des défaillances qui peuvent entraînent des pertes humaines et économiques très importantes.
- Surcoût croissant de l'exploitation lié à l'augmentation des défaillances et de la maintenance.
- Complexité des systèmes nécessitant la rationalisation des activités industrielles.

1.2.1 Etapes de développement de la Fiabilité humaine

1930-1950 la notion de fiabilité a commencé dans le domaine militaire, où a été mise en œuvre pour l'étude des dysfonctionnements des systèmes en vue d'augmenter la fiabilité du matériel.

1950-1960 la fiabilité technique (FT) a connu un essor durant cette période. Cependant, la notion de fiabilité en générale n'était pas satisfaisante, car la fiabilité humaine (FT) qui influe sur les systèmes n'est pas prise en compte. Ce qui a conduit à la naissance de la notion de la fiabilité humaine durant ces années.

Les années (1970) et la première moitié des années (1980) l'industrie nucléaire va contribuer à innover dans les méthodes de prévision des risques industriels. La première évaluation complète du risque lié à une installation industrielle est relative aux centrales nucléaires, et fut publiée en 1975. Elle constitue l'effort d'une cinquantaine d'ingénieurs consacrés à cette étude dirigée par le professeur Rasmussen [2].

1.3 FIABILITÉ HUMAINE ET SÉCURITÉ

Afin d'assurer la sécurité d'un système, une multitude de barrières de sécurité est mise en place pour faire face aux risques menaçant le bon fonctionnement de ce dernier. Le concept de barrière est apparu avec celui de défense en profondeur. Ce concept vise à la sécurisation d'un système par la mise en place d'un ensemble de mesures successives et indépendantes les unes des autres (techniques et humains).

1.3.1 Définition de la barrière humaine de sécurité

Les barrières humaines de sécurité sont constituées d'une activité humaine (une ou plusieurs opérations) qui s'oppose à l'enchaînement d'évènements susceptibles d'aboutir à un accident. Elles se définissent également par les éléments qui la composent : les barrières humaines de sécurité ont une composante humaine, le plus souvent associée à une composante technique (l'opérateur est à minima en interaction avec les éléments techniques du système qu'il surveille ou sur lesquels il agit) [3]. La figure 1.1, représente la typologie des barrières de sécurité.

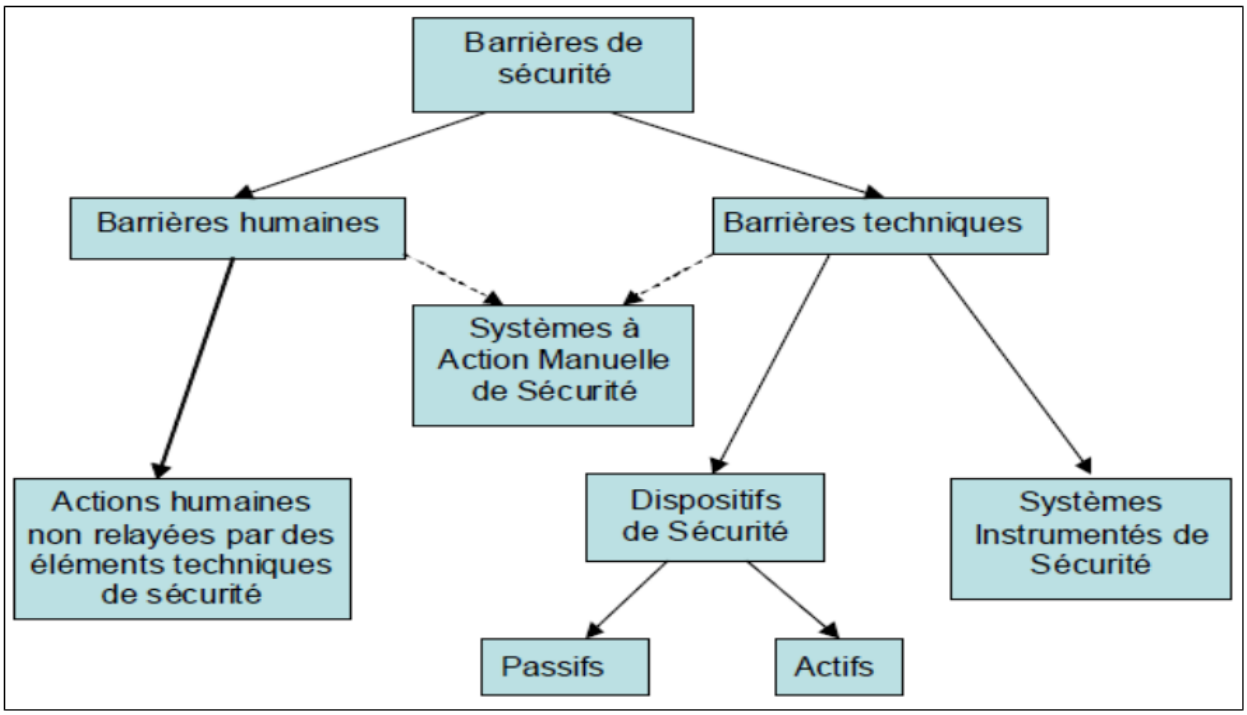

FIGURE 1.1 – **Typologie des barrières de sécurité**

1.3.2 Exemples des barrières humaines de sécurité

Dans les domaines industriels, nous constatons que plusieurs tâches effectuées par les opérateurs sont dédiées dans un premier lieu, à empêcher une aggravation d'une situation indésirable :

- L'opération de contrôle de l'étanchéité d'un circuit, qui conditionne le fonctionnement de ce dernier, est une tâche effectuée par un opérateur, celui-ci prendra les mesures adéquates en cas de détection d'une perte d'étanchéité (une rupture, une fuite ...etc.) pour éviter la perte de la fonction de circuit ou l'aggravation de la situation.
- La fermeture manuelle d'une vanne, réalisée par un opérateur, consiste aussi une barrière de sécurité en cas de détection visuelle ou même automatique d'une augmentation ou élévation au-dessus des seuils de l'un des paramètres (niveau, débit, pression ... etc.)

1.4 CATÉGORIE DE BARRIIERES HUMAINES DE SÉCURITÉ

La notion d'une barrière humaine de sécurité désigne plus particulièrement l'intervention humaine dans un procédé. C'est une intervention destinée pour prévenir une dérive qui peut dégrader le fonctionnement d'un procédé ou en cas où ces dérives ont lieu, rattraper et

corriger la situation. Dans ce cas-là, une activité humaine qui rentre dans le fonctionnement normal du procédé ne sera pas prise en compte comme étant une barrière de sécurité. L'application de ce principe conduit à identifier deux types d'actions susceptibles d'être considérées comme indépendantes [3] :

- - Les interventions humaines en amont d'un procédé, ou en phase du démarrage de ce dernier qui présentent des risques majeurs. Elles servent à la préparation du procédé en termes de sécurité ; la fonction de sécurité sera de vérifier que les conditions d'occurrence d'un scénario d'accident sont maîtrisées préalablement à une activité à risques. **Ces barrières seront appelées "barrières de vérification".**
- Les interventions ayant lieu en aval ou au cours de l'activité ou du procédé susceptible de présenter des risques d'accident majeur et dont la fonction de sécurité sera de détecter une dérive prévue et d'agir en vue de limiter ses conséquences. L'action de ces barrières s'inscrit dans la cinétique de la séquence incidentelle ou accidentelle. **Ces barrières seront appelées "barrières de rattrapage".** La détection de la dérive peut être réalisée à différents stades de l'activité dangereuse : par exemple très en amont de l'évènement redouté comme certaines rondes de surveillance et campagnes d'inspection des équipements ou encore en aval de l'évènement redouté comme les rattrapages de dérive de procédé (intervention sur montée en température anormale d'un réacteur) ou même en aval du phénomène dangereux (intervention sur un cas de feu).

1.5 ORIENTATIONS MÉTHODOLOGIQUES RETENUES POUR L'ÉVALUATION DES BARRIERES HUMAINES DE SÉCURITÉ

L'évaluation des barrières humaines de sécurité est réalisée en se basant sur plusieurs méthodes destinées à cet effet. Cependant, ces méthodes à leurs tours se reposent sur des principes tirés d'une approche ergonomique :

1.5.1 Principe d'évaluation de la tâche humaine de sécurité

L'homme en effectuant une tâche dans le but de rendre une situation dangereuse à un état normale, se comporte avec un raisonnement proche de celui d'un système instrumenté de sécurité (SIS), un système sensoriel, un système cognitif et un moteur. Dans ce contexte, la tâche humaine de sécurité peut être décomposée en trois tâches élémentaires :

La détection (obtention de l'information) cette tâche consiste en la collecte des informations indiquant la présence d'une dérive ou une défaillance pouvant conduire à un phénomène dangereux ou le phénomène lui-même.

Diagnostic (choix de l'action) l'opérateur dans ce cas-là, analysera les informations issues de la première tâche en faisant un diagnostic, qui lui donne ensuite la possibilité de faire le choix de l'action de sécurité qui doit être réalisée.

L'action il s'agit d'une action ou un enchaînement d'action s'opposant à un scénario prévu. Cette action peut être manuelle ou par le biais d'un système technique, ou l'opérateur agira sur un élément de sécurité ou sur l'élément agresseur.

1.5.2 Principes d'évaluation de l'environnement de travail

L'homme doit être considéré comme un utilisateur des ressources et moyens (en temps, compétences, informations...) mis à sa disposition pour lui permettre de remplir ses missions. En partant de ce principe, les méthodes d'évaluation de fiabilité humaine prennent en compte l'adéquation ou la suffisance de ces moyens vis-à-vis des objectifs à atteindre. Autrement dit, la fiabilité humaines dépend directement de ces facteurs (accès aux informations, disponibilité de l'opérateur, complexité de l'action, ...etc.;)

Dans ce but, l'évaluation de l'apparition d'une erreur humaine dépend des interactions entre l'homme et son environnement. Hollnagel considère la performance humaine comme le résultat des interactions entre trois principales catégories de facteurs : Homme, Technologie et Organisation [3], (figure 1.2).

1.5.3 Principes de quantification des barrières humaines de sécurité

Le taux de défaillance ou d'échec d'une mission confiée à un opérateur peut être rapproché d'une notion équivalente habituellement utilisée pour un dispositif technique : la probabilité de défaillance à la demande (PFD). On peut étendre cette notion à l'action humaine pour évaluer la probabilité de défaillance à la demande de l'opérateur en charge d'une action de sécurité [3]. Cependant, cette quantification peut se révéler insuffisante et dans ce cas la valeur doit être multipliée par d'autres facteurs liés à la situation du travailleur.

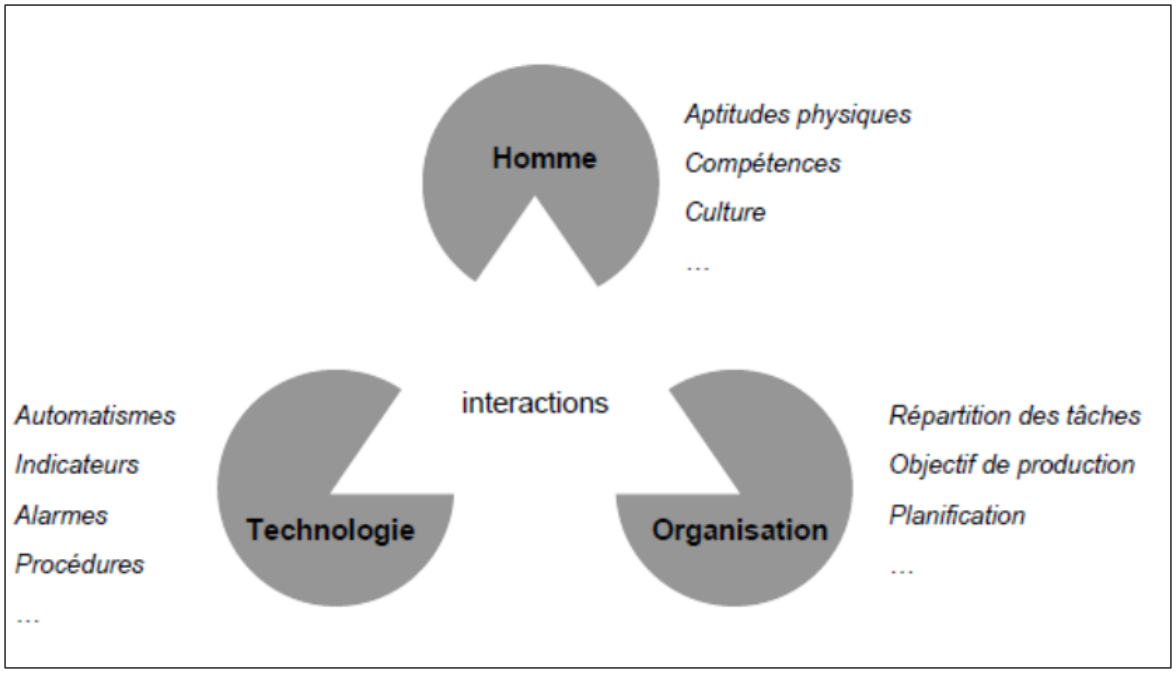

FIGURE 1.2 – **Modèle des causes et manifestations de l'erreur humaine (d'après Hollnagel, 1998)**

1.6 EVALUATION DE LA FIABILITÉ HUMAINE

L'évaluation de la fiabilité humaine peut être réalisée dans le cadre du développement des interfaces Homme-Machine pour la conception d'un poste de travail, pour la redéfinition des fiches de poste et des compétences associées, ou bien dans le cadre des études probabilistes de sûreté et de risque pour analyser les causes des incidents/accidents et leur probabilité d'occurrence. Elle représente souvent une activité intégrée dans une étude probabiliste de risque et de sûreté [5]. Elle tente d'évaluer le potentiel et le mécanisme des erreurs humaines qui peuvent affecter la sûreté des installations. L'analyse de tâche est souvent une étape centrale de l'évaluation de la fiabilité humaine [6]. L'évaluation de la fiabilité humaine passe par plusieurs étapes représentées sur la figure 1.3.

Cette représentation du processus d'évaluation de la fiabilité humaine présente une vision relativement séquentielle d'un processus composé de 7 principales étapes. Toutefois, ces différentes étapes n'ont pas toutes le même poids dans les différentes méthodes analysées dans le cadre de notre état de l'art. Par exemple, les méthodes TESEO, SLIM et HCR ne comportent pas explicitement d'étape d'identification des erreurs humaines. Les méthodes HEART, SLIM, HRC et TESEO ne proposent pas de système de représentation graphique des résultats de la démarche. [6]

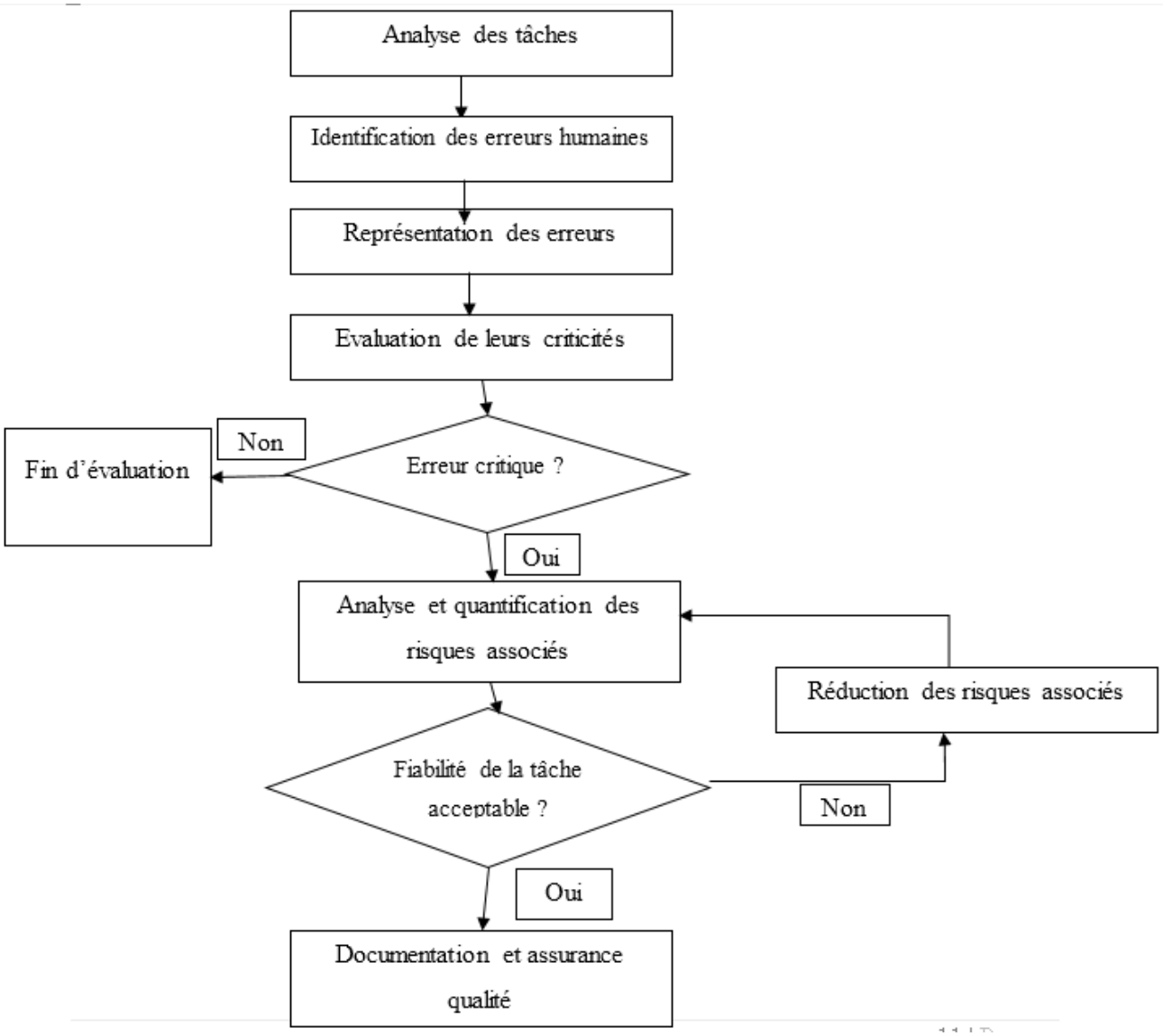

FIGURE 1.3 – **Démarche générale d'évaluation de la fiabilité humaine**

1.6.1 Quantification de la fiabilité des actions humaines

Une quantification de l'erreur humaine revient à faire un rapport entre le nombre d'erreurs commises et le nombre d'occasions de se tromper. L'accès à ces deux informations est facile, si la tâche est répétitive, mais quand la tâche ne l'est plus le recueil de ces informations devient de plus en plus difficile.

La gestion d'un accident nucléaire est beaucoup moins mécaniste et répétitive que l'activité humaine sur une chaine de montage. C'est pourquoi l'Évaluation Probabiliste de la Fiabilité Humaine (EPFH) nécessite un travail important d'analyse des tâches destiné à [7] :

- sélectionner et définir précisément les « missions de conduite » nécessaires et suffisantes pour éviter l'événement redouté ;
- analyser précisément le contexte dans lequel ces missions sont conduites et identifier

les principaux « facteurs de contexte » susceptibles d'augmenter (resp. de diminuer) la probabilité d'erreur.

1.7 ERREUR HUMAINE

Les chercheurs dans le domaine de la fiabilité humaine ne cessent pas de développer le concept de l'erreur humaine, ce dernier a été largement revu depuis les dernières décennies. Loin de la psychologie et la psychophysique, l'erreur humaine est devenue pour le scientifique un instrument de mesure de la fiabilité de l'homme et de sa performance.

Le développement de ce domaine a connu son essor à partir des années 80 suites aux accidents industriels (Tchernobyl et Three Miles Island) où la cause humaine était le principal facteur. Au début, les études de l'erreur humaine ont été orientées dans le but de comprendre le mécanisme de la survenue des erreurs ; dans une deuxième étape, et avec le progrès de la technologie l'objectif de ces études est réorienté vers les effets de la suppression quasi-totale du facteur humain des procédés industriels.

1.7.1 Définition de l'erreur humaine

La notion de l'erreur humaine est un concept très large car elle a des différentes dimensions. Actuellement, il est difficile de trouver un référentiel commun qui donne une définition exacte au terme de « l'erreur humaine ».

La définition de l'erreur humaine se diffère selon le domaine qui s'intéresse à ce concept (psychologie, ergonomie, juridique, ingénierie... etc.)

Pour un ergonome, l'erreur humaine désigne une inadéquation entre l'environnement du travail (caractéristiques organisationnelles, fonctionnelles et techniques) et celle du facteur humain (physique, mental et psychosocial). De ce fait, l'erreur humaine est liée à la notion de la tâche, ainsi qu'à la valeur accordée à cette tâche. [4].

Dans le domaine du travail, une erreur humaine est définie par Rasmussen, en 1983, comme étant la contrepartie négative de l'activité humaine qui est susceptible de conduire à une défaillance de l'opérateur. L'erreur est donc, à partir de cette définition, un indicateur de l'activité. Elle se traduit par une incompatibilité sur le système, action qui conduit à des résultats non conformes au but préétabli.

Les définitions multiples données pour le terme de « l'erreur humaine » peuvent être classifiées selon trois approches différentes [8] :

- Approche industrielle : elle met le point sur le mécanisme de l'apparition de l'erreur humaine ;

- Approche psycho-cognitive : se base sur les modes de production des erreurs humaines
- Approche psycho-dynamique du travail : c'est la prise en compte des deux approches susmentionnées.

1.7.2 Types d'erreurs humaines

Avant d'aborder les différentes approches de classification de l'erreur humaine, il est indispensable de faire les différences entre les termes : ratés, lapsus et fautes [9].

1. **Ratés** : c'est l'ensemble des erreurs commises par un opérateur lors de l'exécution d'une tâche. Ces erreurs sont dues à un manque du savoir-faire.
2. **Lapsus** : c'est une erreur due à un défaut de stockage des informations, elle se traduit par un choix inadéquat des actions à exécuter, compte tenu de la situation et des contraintes de la tâche.
3. **Les fautes** : c'est les erreurs basées sur les connaissances qui résultent d'une déficience de jugement et e planification. Elles reflètent un plan d'action ou une intention inappropriée aux caractéristiques de la tâche et de la situation.

Les différents types d'erreurs humaines sont donnés dans la figure 1.4.

1.7.3 Méthodes d'évaluation de l'erreur humaine

L'erreur humaine ne peut pas être considérée comme étant un évènement totalement imprévisible. A partir de ce concepts plusieurs méthodes et approche d'analyse de la fiabilité humaine ont été développées dans le but de quantifier l'erreur humaine, et d'évaluer ensuite la contribution de cette erreur dans la probabilité totale de l'échec d'un système donnée.

Les méthodes d'évaluation de la fiabilité humaine peuvent être ordonnées selon l'ordre chronologique de leurs apparitions (tableau 1.1). Elles sont classifiées par génération. Il est noté que les premières méthodes d'évaluation de la fiabilité humaine sont apparues dans le domaine de l'industrie nucléaire.

1.7.4 La décomposition de la tâche «THERP»

Parmi les premières méthodes d'évaluation de la fiabilité humaine apparues dans le monde, La méthode THERP (The Technique for Human Error Reduction and Prediction) qui a été élaborée par SWAIN et GUTTMAN en 1983, dans le domaine de l'industrie nucléaire. Cette méthode consiste à analyser les tâches, identifier et quantifier les erreurs.

TABLE 1.1 – **Méthodes d'évaluation de la fiabilité humaine**

	Nom de la méthode	Fondateur	Année
Génération 01	**THERP** (Technique for Human Error Rate Prediction)	Swain	1963
	TESEO (Technica Empirica Stima Errori Operatori),	Bello et Colombari	1980
	SLIM (Success Liklihood Index Method)	Embrey	1983
	HEART (Human Error Assessement and Reduction Technique)	Williams	1985
	HCR (Human Congnitive Reliability)	Hannman	1984
Génération 02	CREAM (Cognitive Reliability and Error Analysis Method)	Hollnagel	1998
	ATHEANA (A Technique for Human Event ANAlysis)	Cooper	1996
	MERMOS (Méthode d'Evaluation de la Réalisation des Missions Opérateur pour la Sûreté)	Le Bot	1998
Génération 03	**WPAM** (Work Process Analysis Model)	Davoudian	1994
	Tripod	Groeneweg	1998
	I-Risk	Bellamy	1999
	FRAM (Functional Resonance Analysis Method)	Hollnagel	2004
	BORA (Barrier and Operational Risk Analysis)	Aven	2004

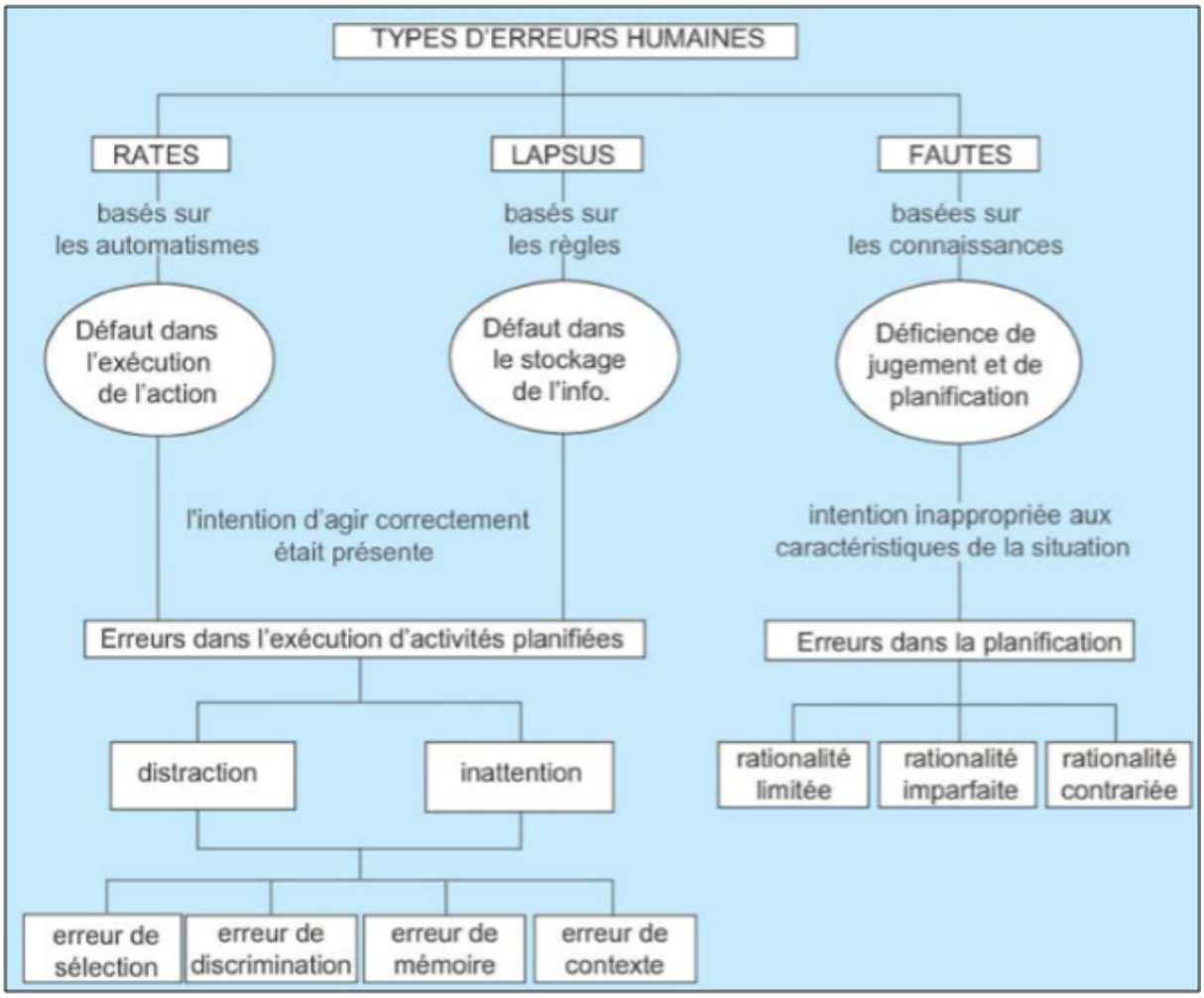

FIGURE 1.4 – **Distinction des types d'erreur humaine**

La méthode THERP se base sur la décomposition de l'enchaînement incidentelle ou accidentel en tâches élémentaires quantifiables. La possibilité de quantifier les tâches élémentaires permet alors de calculer la probabilité d'incident ou accident de la séquence L'analyse se décompose en 5 étapes [2] :

Définition des points faibles du système cette étape consiste à repérer les différentes fonctions du système où l'homme peut intervenir et dans ce cas-là la possibilité d'avoir une erreur humaine. Chacune de ces fonctions est ensuite décomposées en tâches et en tâches élémentaires pouvant être effectuées par l'homme ;

Listes et analyse des tâches une analyse approfondie de la tâche permet d'identifier les étapes de réalisation de la tâche, et pour chacune des sous tâches, les sous tâches et les informations qui sont nécessaires aux opérateurs pour l'acomplir. A chaque étape, l'analyste décide quelles erreurs peuvent se produire. Pour aider l'analyse, **THERP** inclut l'utilisation d'un arbre d'événement, qui présente une combinaison des erreurs relatives aux différentes

opérations élémentaires.

Estimation de la probabilité d'erreurs qui se rapportent aux tâches la probabilité P(E) d'une erreur élémentaire est obtenue par la formule :

$$P(E) = P_1 \times P_2 \times K$$

Avec

- P_1 : Probabilité de base, fonction de la caractéristique de l'opération,
- K : Coefficient correctif selon le niveau de stress de l'opérateur,
- P_2 : Probabilité de non-récupération de l'erreur.

Les valeurs de probabilité sont fournies par une vingtaine de tables des données d'analyse d'incidents, et des jugements subjectifs.

Estimation des effets de l'erreur humaine sur le système enfin d'évaluation de la fiabilité humaine, les résultats doivent être réintégrées dans la probabilité de dysfonctionnement totale de système. Si des critères d'évaluation de risque sont importants, il est alors nécessaire d'évaluer également la fréquence des événements indésirables.

Recommandations pour modifier le système et nouveau calcul de la probabilité de défaillance du système une analyse plus approfondie doit permettre de déterminer comment la disponibilité du système peut être améliorée par la réduction des probabilités d'erreurs humaines.

La démarche suivie pour une évaluation THERP est représentée sur la figure 1.5

Dans ce chapitre, nous avons traité les notions générales de la fiabilité humaine, et la chronologie du développement de ce domaine, nous avons pu donner la relation qui lie la fiabilité humaine et les différentes branche dans un process industriel (techniques et organisationnelles). Nous avons traité aussi l'erreur humaine et les différents facteurs influençant la probabilité qu'un opérateur commette une erreur conduisant à la dégradation d'un système voir l'avènement d'un accident. Les méthodes développées dans l'objectif d'évaluer l'erreur humaine sont multiples. Leur apparition était suite à des accidents où le facteur humain a été considéré comme étant la cause principale.

Nous avons également présenté la démarche suivie pour l'élaboration d'une étude de fiabilité humaine « THERP », méthode développée dans l'industrie nucléaire.

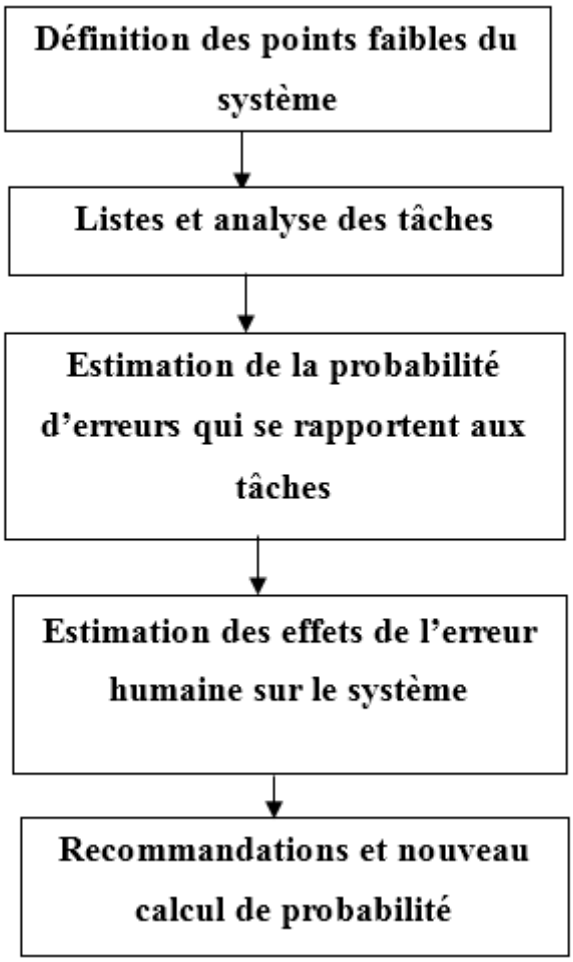

FIGURE 1.5 – **Démarche de réalisation d'une évaluation THERP**

Chapitre 2

DEFAILLANCES DE CAUSE COMMUNE

DEFAILLANCES DE CAUSE COMMUNE

Les Défaillances de Causes Communes (DCC) sont des défauts pouvants affecter plusieurs composantes en fonctionnement ou à la sollicitation. La particularité de ces défaillances, c'est qu'elles sont à l'origine de la même cause. Nous parlons des DDC quand il s'agit des groupes de composants identiques ou similaires, redondants, réalisant la même fonction et œuvrant dans des conditions comparables. Pour ces raisons, les DCC constituent l'un des branches primordiales de la sûreté de fonctionnement (SdF). Les DCC sont limitées par la diversité, mais jamais complètement. L'étude des Défaillances de Causes Communes (DCC) est un domaine actif de recherche dans les domaines du nucléaire, de la pétrochimie, de l'aérospatial... [10]

Dans ce chapitre, il s'agit d'introduire les concepts des DDC et d'identifier les différents modèles traitants ce sujet.

2.1 DEFAILLANCE DE CAUSE COMMUNE

2.1.1 Définition

Les défaillances désignées par l'appellation « défaillances de cause commune » sont des défaillances pouvant affecter simultanément, ou pendant la durée de la mission, plusieurs composants et qui ont la même cause de dysfonctionnement, par exemple une erreur de conception, de fabrication, d'installation ou de montage, une erreur de maintenance, ou un effet de l'environnement.[11]

Les conséquences des défaillances des systèmes supports (alimentations électriques, air comprimé, source froide...) et les agressions internes ou externes entraînant la défaillance de plusieurs équipements n'entrent pas dans cette appellation et sont traitées par ailleurs. Les défaillances liées à une mauvaise configuration de matériels ne sont pas considérées en tant que défaillance de cause commune.

2.1.2 Evaluation des DCC

L'évaluation des taux de défaillance de cause commune présente deux étapes majeures :

- La détermination des composants pour lesquels des défaillances de cause commune peuvent être envisagées (analyse qualitative) ;
- L'obtention de données (analyse quantitative).

Détermination des composants siège de DCC

Il convient de procéder tout d'abord à la sélection des groupes de matériels susceptibles d'être le siège de défaillances de cause commune. Cette sélection repose sur l'analyse de l'expérience d'exploitation et sur l'analyse a priori des conséquences des cumuls de défaillances. En pratique, lors de la sélection de ces groupes de matériels, sont au minimum associés les matériels identiques d'un même système et assurant la même fonction dans des conditions comparables.

Ainsi, suivant le type de dépendance mis en évidence, sont introduites, dans l'étude, selon les matériels considérés, des défaillances de cause commune pouvant affecter les matériels à la sollicitation ou en fonctionnement. Il convient également d'examiner, pour le fonctionnement en « normal-secours » de matériels, si certaines dépendances sont susceptibles de provoquer simultanément la défaillance du composant en fonctionnement et le refus de démarrage du composant en attente.

Obtention des données

L'obtention de valeurs de taux de défaillance de cause commune nécessite une analyse de l'expérience d'exploitation disponible. Compte tenu de la rareté des défaillances de cause commune réellement survenues, les observations peuvent être étendues aux événements révélateurs de possibilités de défaillances de ce type. Il peut également être fait appel à des recueils de données internationales. Pour estimer les valeurs associées, il convient alors d'effectuer des ajustements appropriés.

2.1.3 Principe de Défaillance de cause commune

Causes de bases (root causes)

Il existe de type des causes de bases : causes pré-opérationnelles et causes opérationnelles

- **Causes pré-opérationnelles** c'est l'ensemble des défauts de conception, de production, de l'installation et les erreurs de configuration.
- **Causes opérationnelles :** les opérations de maintenance et les procédures : une maintenance inappropriée, non-respect des procédures ; Environnement : les conditions de fonctionnement du matériel (humidité, température, vibrations ...)

Mécanismes de couplage

C'est les conditions dont ils peuvent se trouver plusieurs composants et qui peuvent être par conséquent, affectés par la même cause [12]. Il s'agit de la recherche des points de similarité entre les différents éléments en question [13]. Les points de similarité des composants peuvent être :

- **La conception** : les éléments rentrant dans le siège de DCC, peuvent être similaire en terme de conception.
- **Les équipements :** les composants du siège DCC peuvent avoir les mêmes équipements.
- **Les missions :** tout ensemble de composants ayant la même mission dans un système font l'objet d'une analyse des DCC.
- Le logiciel ;
- Les opérateurs ;
- La maintenance et l'exploitation ;
- Les procédures du travail ;
- L'environnement ;
- La location .

Groupe des composants de cause commune (CCCG)

la constitution de ce groupe peut être faite selon les hypothèses suivantes :

- S'il s'agit des composants actifs, redondants et ayant la même mission, ces composants forment un CCCG.
- Les éléments du CCCG sont considérés indépendants ;
- Les éléments passifs peuvent être exclus des CCCG, en se basant sur le fait que les composants actifs sont dominants.

La figure 2.1 montre le principe des défaillances de cause commune.

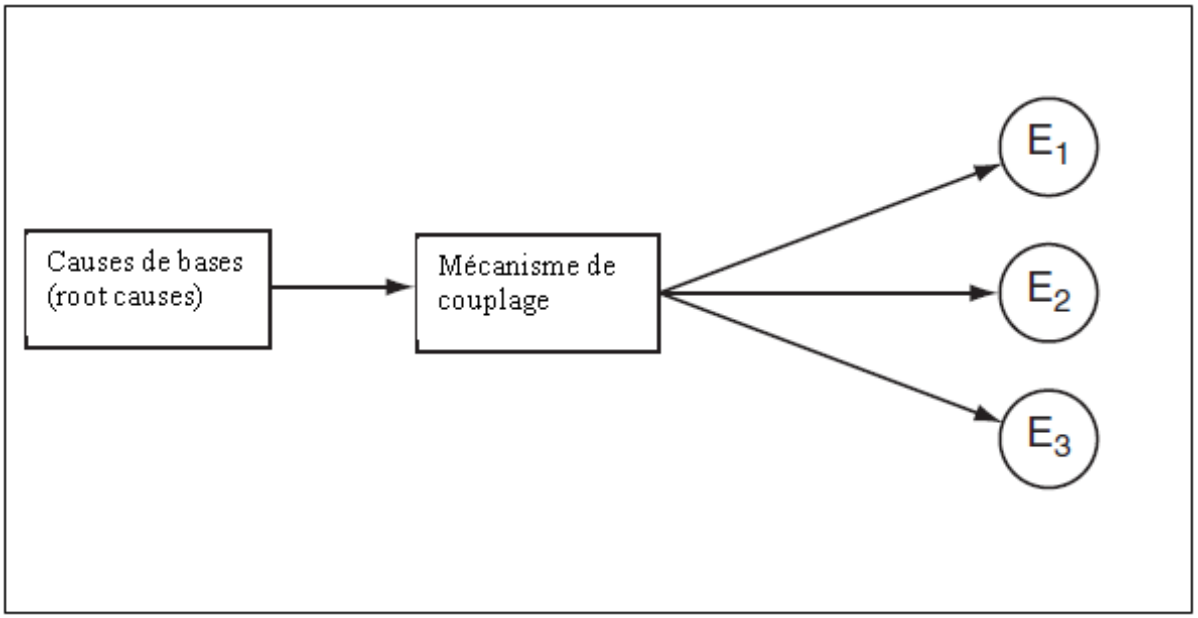

FIGURE 2.1 – **Principe de défaillances de cause commune**

2.2 ANALYSE QUANTITATIVE DETAILLEE DES DCC

L'analyse détaillée des défaillances de cause commune peut être réalisée même si une étude qualitative n'est pas faite. Néanmoins, les résultats d'une analyse qualitative peuvent être utiles dans les étapes de l'analyse quantitative.

L'étude quantitative des DCC est réalisée suivant les étapes :

- Identifications des évènements de bases des causes communes CCBE ;
- Incorporation des CCBE dans l'AdD du système ;
- Estimation des paramètres de CCBE ;
- Quantification de l'indisponibilité du système ;
- Analyse des résultats.

2.2.1 Identification des CCBE

Un évènement de base de cause commune est un évènement qui provoque par son occurrence la défaillance de plusieurs composants d'un système due à une même cause.

Par exemple, un système composé de trois composants A, B, et C ; les CCBE dans ce cas sont : C_{AB}, C_{AC}, C_{BC}, et C_{ABC}. Cela peut être traduit comme suit :

- A_i : le composant A tombe en défaillance, (élément indépendant) ;
- C_{AB} : l'élément A et B (et non C) tombent en défaillance par la même cause ;
- C_{AC} : l'élément A et C (et non B) tombent en défaillance par la même cause ;
- C_{ABC} : les éléments A, B, C tombent en défaillance par la même cause.

Donc nous pouvons conclure que l'élément A tombe en défaillance si l'un des évènements susmentionnés a lieu, la simplification booléenne de l'arbre est donnée par l'équation 2.1.

$$A_T = A_i + C_{AB} + C_{AC} + C_{ABC} \tag{2.1}$$

2.2.2 Incorporation des CCBE dans l'AdD du système

Cette étape consiste en le développement de l'arbre des défaillances du système, en prenant en compte les CCBE identifié dans l'étape précédente.

Considérons un système composé de trois éléments identiques fonctionnant avec une logique de 2/3. L'arbre de défaillance du système sans la considération des CCBE est représentée sur la figure 2.2.

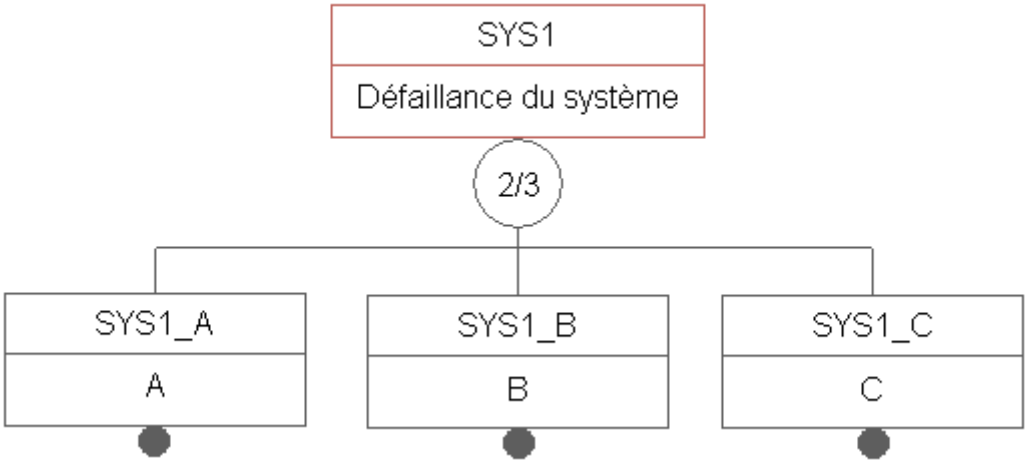

FIGURE 2.2 – **Arbre de défaillances du système sans CCBE**

En cherchant les coupes minimales de cet arbre, nous aurons :

$$\{A, B\}; \{A, C\}; \{B, C\}$$

En introduisant les CCBE dans l'arbre de défaillance, la défaillance de l'élément A ne sera pas prise comme un évènement de base mais elle est développée. la figure 2.3 représente le développement de la défaillance de l'élément A.

Dans ce cas, les coupes minimales de la défaillance su système sont :

$$\{A_i, B_i\}; \{A_i, C_i\}; \{B_i, C_i\}$$

$$\{C_{AB}\}; \{C_{AC}\}; \{C_{BC}\}$$

$$\{C_{ABC}\}$$

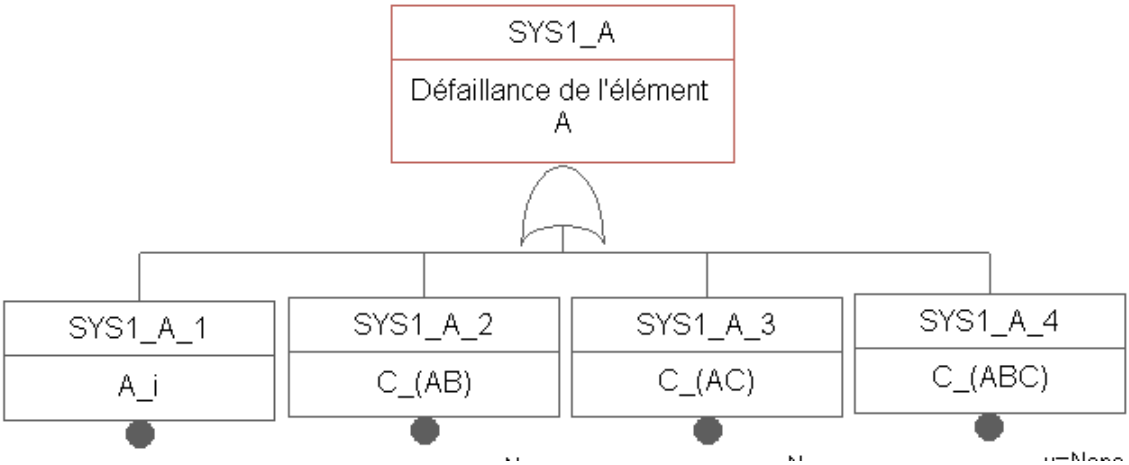

FIGURE 2.3 – **Arbre de défaillances de l'élément A**

d'où la simplification booléenne de l'arbre de défaillance du système comme suit :

$$S = A_i \times B_i + A_i \times C_i + B_i \times C_i + C_{AB} + C_{AC} + C_{BC} + C_{ABC} \tag{2.2}$$

2.2.3 Quantification de l'indisponibilité du système

Pour calculer la probabilité de défaillance du système, il suffit de convertir l'équation booléenne en équation algébrique en introduisant les probabilités de défaillance des évènement de base.

$$P(S) = P(A_i)\times P(B_i)+P(A_i)\times P(C_i)+P(B_i)\times P(C_i)+P(C_{AB})+P(C_{AC})+P(C_{BC})+P(C_{ABC}) \tag{2.3}$$

Dans le domaine de la fiabilité, il est supposé souvent que les éléments identiques ont une même probabilité de défaillance :

$$P(A_i) = P(B_i) = P(C_i) = Q_1$$
$$P(C_{AB}) = P(C_{AC}) = P(C_{BC}) = Q_2$$
$$P(C_{ABC}) = Q_3$$

En simplifiant l'équation 2.3, nous aurons :

$$P(S) = 3(Q_1)^2 + 3Q_2 + Q_3 \tag{2.4}$$

avec :

Q_k^m : probabilité d'un CCBE de **k** éléments dans un group CCCG de taille **m**.

Mdèles de calcul des DCC

Parmi les modèles existants pour le calcul des défaillances de cause commune : **le modèle de facteur alpha**. Nous choisissons de travailler avec le modèle alpha, plusieurs raisons :

- est un modèle multi-paramètres qui peut gérer n'importe quel niveau de redondance, ;
- Il est basé sur les taux de taux de défaillance qui rend l'évaluation de ses paramètres plus facile quand aucune donnée statistique n'est disponible ;
- Il a un modèle statistique plus simple et produit des estimations ponctuelles plus précises.

Le modèle de facteur alpha développe des fréquences de DCC à partir d'un ensemble de rapports de défaillances et du taux de défaillance total des composants. Les paramètres du modèle sont

- Q_t : fréquence totale d'échec de chaque composant, (somme de la probabilité de défaillance indépendante de A et les probabilités de défaillances de cause commune)
- α_k : fraction de la fréquence totale d'échec des événements qui se produisent dans le système et impliquent l'échec de **k** composants en raison d'une cause commune

En utilisant ces paramètres, en fonction de l'hypothèse concernant la manière dont les systèmes sont testés, la fréquence d'un CCBE impliquant une défaillance de **k** composants dans un système de **m** composants est donnée par :

Pour un système d'essai échelonné :

$$Q_k^m = \frac{1}{\begin{pmatrix} m-1 \\ k-1 \end{pmatrix}} \alpha_k Q_t \tag{2.5}$$

Pour un système d'essai non-échelonné :

$$Q_k^m = \frac{1}{\begin{pmatrix} m-1 \\ k-1 \end{pmatrix}} \frac{\alpha_k}{\alpha_t} Q_t \tag{2.6}$$

où le coefficient binomial est donné par :

$$\begin{pmatrix} m-1 \\ k-1 \end{pmatrix} = \frac{(m-1)!}{(k-1)!(m-k)!} \tag{2.7}$$

et

$$\alpha_t = \sum_{k=1}^{m} k\alpha_k \tag{2.8}$$

À titre d'exemple, les probabilités des événements de base du système à trois composantes de l'équation 3.4 sont écrit comme suit (en supposant des tests échelonnés) :

$$Q_1^3 = \alpha_1 Q_t$$
$$Q_2^3 = 1/2\alpha_2 Q_t$$
$$Q_3^3 = 3\alpha_3 Q_t$$

Par conséquent, l'indisponibilité du système de l'équation 3.4 peut maintenant être écrite comme suit :

$$Q_S = 3(\alpha_1 Q_t)^2 + 3/2\alpha_2 Q_t + 3\alpha_3 Q_t \tag{2.9}$$

En simplifiant l'équation 3.9, nous aurons :

$$Q_S = \frac{3\alpha_2 + 3\alpha_3}{\alpha_1 + 2\alpha_2 + 3\alpha_3} Q_t \tag{2.10}$$

Les valeurs de fractions α peuvent être calculées à partir de la relation suivante :

$$\alpha_k = \frac{\begin{pmatrix} m \\ k \end{pmatrix} Q_k}{\sum_{k=1}^{m} \begin{pmatrix} m \\ k \end{pmatrix} Q_k} \tag{2.11}$$

Pour le système de l'équation 3.4, les valeurs des facteurs α sont données par :

$$\alpha_1 = \frac{Q_1}{Q_1 + 2Q_2 + Q_3} \tag{2.12}$$

Quand il s'agit de grands CCCG, l'apllication de la relation devient complexe, nous avons recours aux bases de données qui nous fournissent les valeurs des facturs α.

Nous avons traité dans ce chapitre les concepts généraux des défaillance de cause commune. Nous avons ensuite, abordé le modèle de facteur alpha servant à calculer les probabilité des DCC.

Le chapitre suivant sera dédié à l'aplication d'une étude de fiabilité humaine et une étude de défaillances de cause commune sur le système d'arrêt d'urgence du réacteur nucléaire NUR de CRND.

Chapitre 3

ETUDE DE CAS : LE SYSTEME D'ARRÊT D'UN REACTEUR NUCLEAIRE

ETUDE DE CAS : LE SYSTEME D'ARRÊT D'UN REACTEUR NUCLEAIRE

L'industrie nucléaire est un domaine très exigent en matière de sécurité. Dans ce contexte la conception d'un réacteur nucléaire nécessite la mise en œuvre d'un ensemble de fonction de sûreté dans le but d'éviter le développement d'une séquence accidentelle indésirable.

L'arrêt d'urgence du réacteur (RPS) est la première fonction de sûreté dans un réacteur nucléaire. Cette fonction fait partie du principe de défense en profondeur. Le système conçu pour accomplir cette fonction est caractérisé par une faible probabilité de défaillance. Or cette caractéristique n'élimine pas le fait qu'il peut tomber en défaillance et par conséquent la tâche n'est pas effectuée. Pour éviter cette circonstance, le RPS peut être déclenché manuellement.

Ce présent chapitre a pour but l'analyse de la fiabilité humaine lors de l'accomplissement de l'arrêt manuel du réacteur face une situation d'urgence, et le traitement des défaillances de cause commune des canaux de détection du système RPS.

3.1 LE SYSTEME D'ARRÊT D'URGENCE

Le système d'arrêt d'urgence a pour fonction l'inhibition de la réaction voir l'arrêt de cette dernière en cas accidentel, dans le but de rendre minimum le risque de l'installation. Il est constitué de différents composants qui assurent d'une façon complémentaire la fonction globale du système :

3.1.1 Le mécanisme de commande

La fonction de ce mécanisme est de commander le mouvement des barres de contrôle. Les barres sont caractérisées par deux mouvements :

Le premier est vertical ascendant-descendant assurant le contrôle de la réactivité dans le cœur ou l'arrêt lent du réacteur ; par l'action d'un moteur pas à pas.

Le deuxième mouvement est vertical descendant, assuré par l'enlèvement de l'énergie électrique de l'électro-aimant, dans ce cas les barres s'introduisent dans le réacteur subitement par le fait de leurs propre poids (SCRAM). Cependant, un système de freinage pneumatique léger assure un arrêt rapide et sécurisé.

Il n'y a pas de demande de SCRAM si les conditions représentées dans le tableau 3.1 sont rempliés :

TABLE 3.1 – **Conditions pour que la logique de SCRAM ne se déclenche pas**

Condition	**Discription**
DPijV4	Différence de pression du cœur canal i, chaîne de SCRAM j, est dans les limites de niveau du sécurité 4
RPIjV4	Débit du circuit de refroidissement primaire de chaîne SCRAM i, chaîne SCRAM j, est dans les limites de sécurité 4
CijC	Clapet fermé
ANIjB4	Niveau d'eau du réservoir du réacteur de chaîne de SCRAM i, chaîne de SCRAM j, est sous le niveau de sécurité B
DTijV4	Différence de température du cœur de canal i, chaîne de SCRAM j, est dans les limites de niveau du sécurité 4
OMijV4	Flux linéaire de marche de la chaine i, chaine de SCRAM j, est dans les limites du niveau de sécurité 4
MAijV4	Moniteur de l'air chaine i, chaine de SCRAM j, est dans les limites de sécurité du niveau 4
LAijV4	Flux logarithmique de chaine de démarrage, de chaine de SCRAM j, est dans les limites du niveau de sécurité 4
SLM	Sécurité pour flux logarithmique de marche 2 des trois chaine, en fonctionnement
MP	Marche permise
LMijV4	Flux logarithmique de chaine de marche i, de chaine de SCRAM j, est dans les limites de niveau de sécurité 4
TMijV4	Période de la chaine de marche i, chaine de SCRAM j, est dans les limites de niveau de sécurité 4
NSijA4	Niveau d'intensité sismique i, chaine de SCRAM j, se trouve au-dessus de niveau supérieur de sécurité 4
STijV4	Température de sortie du cœur chaine i, chaine de SCRAM j, est dans les limites de niveau de sécurité 4
LMiA1	Flux logarithmique de marche chaine i, au-dessous du niveau de sécurité 1, inhibe SCRAM en condition de démarrage de : débit de refroidissement du cœur, clapet ouvert et différence de pression du cœur

3.1.2 Barres de contrôle de sûreté

Ce sont des alliages métalliques (80% Argent, 15% Indium 5% Cadmium) absorbants de neutrons, leurs fonction est de rendre l'état de la réaction nucléaire moins critique, et de

le maintenir pendant le temps nécessaire.

3.1.3 Le canal de détection

Ces dispositifs servent à surveiller les différents paramètres liés au fonctionnement du réacteur (pression, débit, température, population neutronique ...)

La détection ce fait au moyen de trois ensembles différents de détection. Ceux qui comprennent de façon conservative tous l'ensemble de paramètres de déclanchement sont présentés dans le tableau 3.1. Les trois ensembles susmentionnés sont :

- Détection par un paramètre avec une logique 2/3 ;
- Détection par un paramètre avec une logique 1/1 ;
- Détection par deux paramètres avec une logique 2/3 et 1/1 ;

La figure 3.1 suivante représente la logique de l'arrêt de réacteur SCRAM :

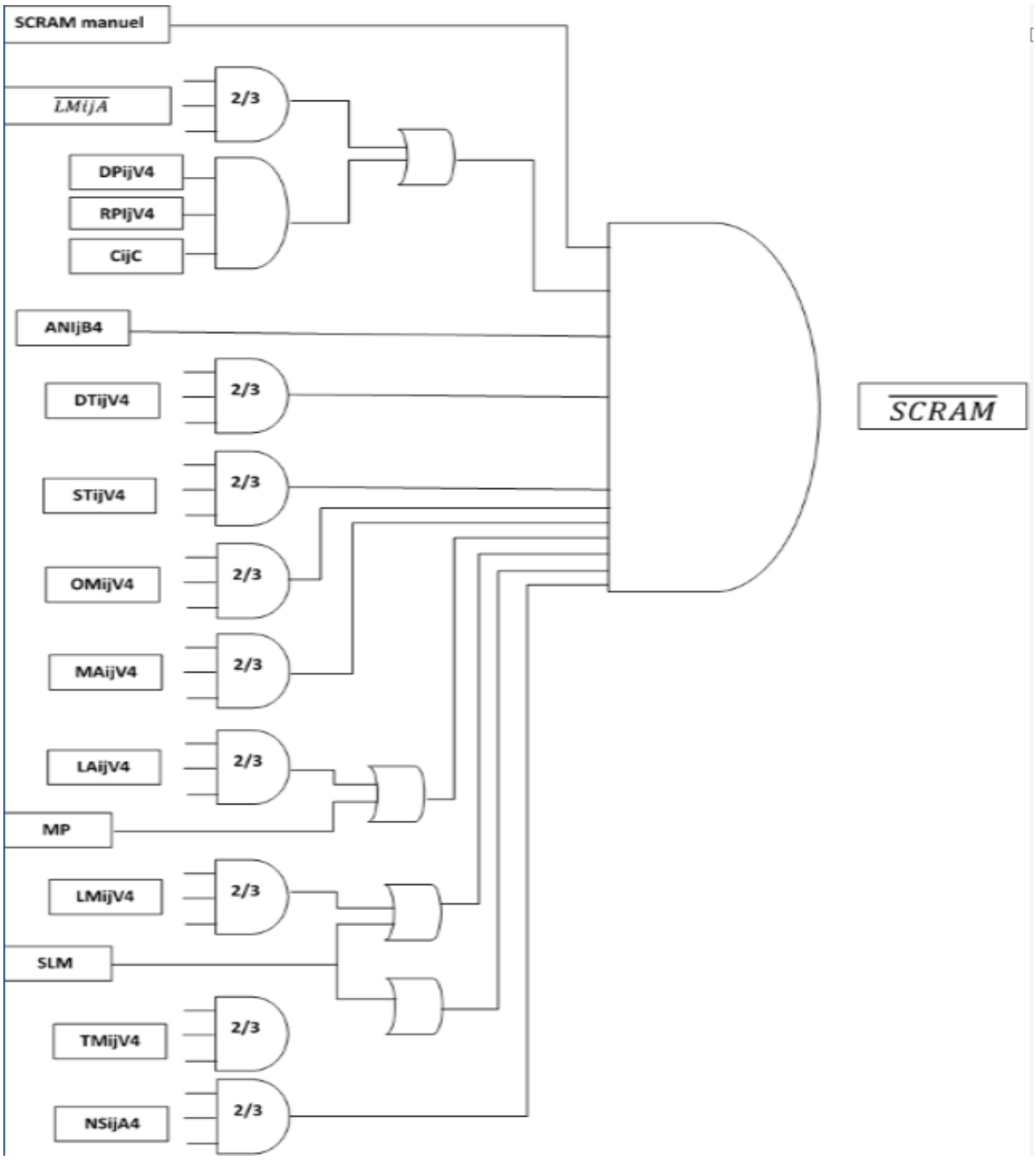

FIGURE 3.1 – **Logique de SCRAM**

3.2 DECLENCHEMENT DU SYSTEME

Le système d'arrêt est actionné de deux manières :

3.2.1 L'actionnement automatique

Dans ce cas d'actionnement l'arrêt du réacteur est régi par une logique qui permet, en analysant le signal provenant des différents capteurs, la coupure de l'électricité qui alimente l'électro-aimant et par conséquent, la chute libre des barres dans le réacteur. La défaillance du

système d'arrêt d'urgence dans le cas d'actionnement automatique, revient à une défaillance dans l'un des composants de ce système :

1. Une défaillance des capteurs du système ;
2. Une défaillance dans la logique de SCRAM
3. Une défaillance dans le mécanisme des barres
4. Une défaillance dans la logique.

La défaillance du système d'arrêt d'urgence est évaluée pour la détection de l'évènement initiateur au moyen de trois ensembles de détection :

- Détection par un paramètre avec une logique 2/3 ;
- Détection par un paramètre avec une logique 1/1 ;
- Détection par deux paramètres avec une logique 2/3 et 1/1 ;

La construction de l'arbre de défaillance du système d'arrêt revient à construire les Arbres des Défaillances des trois ensembles. Cette étude nous a permis de donner la valeur finale de la défaillance du RPS en cas d'actionnement automatique est égale à :

$$P(RPS_{Auto}) = 8,19 \times 10^{-03}$$

3.2.2 Actionnement manuel

Le fonctionnement de ce cas dépend de l'action humaine qui réagit face à une situation d'urgence. L'opérateur tombe dans deux situations :

- **Avec activation d'alarmes** : l'opérateur agit directement en voyant les alarmes.
- **Sans activation d'alarmes** : l'opérateur doit effectuer une analyse des données avant d'agir sur le système.

3.3 ELABORATION D'UNE ETUDE THERP

Dans cette étape, nous allons appliquer la méthode THERP, pour évaluer la fiabilité humaine lors de l'actionnement manuel du RPS, ce qui se traduit par la quantification du fait que l'opérateur commet une erreur et par conséquent la tâche d'arrêt n'est pas accomplie.

3.3.1 Définition des points faibles du système

L'actionnement manuel de système RPS est réalisé suivant les deux cas suivants :

- **Avec activation d'alarmes** : l'opérateur agit directement en voyant les alarmes.
- **Sans activation d'alarmes** : l'opérateur doit effectuer une analyse des données avant d'agir sur le système.

3.3.2 Listes et analyse des tâches

Avec activation d'alarmes Dans ce cas, des alarmes spécifiques dans la salle de contrôle mettent à l'évidence pour l'opérateur le fait qu'un évènement initiateur it lieu.

- Observation de l'alarme de l'E.I ;
- Arrêter le réacteur

Sans activation d'alarmes Dans ce cas, l'arrêt manuel du réacteur se base sur le diagnostic des différents indicateurs (flux neutronique, température...) par l'opérateur pour décider si le réacteur doit être arrêté ou non :

- Observation des indicateurs ;
- Diagnostic de la situation ;
- Décision (arrêt du réacteur ou non)

3.3.3 Estimation de la probabilité d'erreurs qui se rapportent aux tâches

Avec activation d'alarmes Deux opérateurs sont présents dans la salle de contrôle, l'un est supposé être présent pendant toute la journée, quant au deuxième opérateur il se trouve dans la salle pendant une demi-journée en raison de son déplacement pour effectuer d'autres tâches administratives.

La probabilité qu'un opérateur commet une erreur, c'est-à-dire qu'il n'arrête pas le réacteur est de : 3×10^{-03} ***(rapport de sûreté du réacteur NUR)***

En admettant que lors de l'activation des alarmes les deux opérateurs sont dans la salle de contrôle, dans ce cas, nous devons prendre en compte cette situation. Pour cela le modèle qui est appliqué est celui de « dépendance moyenne »

La probabilité relative au fait de la dépendance moyenne des opérateurs est de **0,15** ; Donc la probabilité que le réacteur ne sera pas arrêté manuellement est la suivante :

$$P(PRS.Man.) = (0,003 \times 0,5) + (0,003 \times 0,15 * 0,5) = 0,0017$$

$$P(PRS.Man.) = 2.10^{-03}$$

Sans activation d'alarmes Dans le cas où aucune alarme n'est pas déclenchée, l'opérateur doit observer les changements anormaux des paramètres à contrôler. La décision d'arrêter le réacteur se base sur le diagnostic et l'analyse des signaux des paramètres et des indications présentes.

L'occurence d'un évènement initiateur (obstructions des canaux de coeur par exemple) peut donner lieu à

- des oscillations du flux neutronique
- visualisation des canaux sur le moniteur dans la salle de contrôle

Dans ce cas, l'évaluation de l'erreur humaine se résume à un arbre d'évènements vertical (figure 3.2). les lettres en majuscule signifient un "Succès "de la tâche et celle en minuscule "Echec"

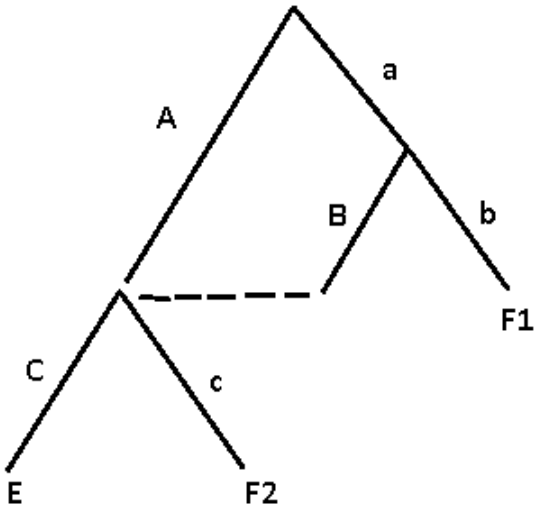

FIGURE 3.2 – **Arbre d'évènements de l'erreur humaine**

- Si l'opérateur observe un changement du flux neutronique et qu'il fait un diagnostic correct de la situation il procède à un arrêt du réacteur,
- Si l'opérateur n'observe pas un changement du flux et observe le moniteur, il revient au diagnostic de la situation. Si l'analyse et fausse le réacteur n'est pas arrêté,
- Si l'observation des deux paramètres n'est pas faite, le réacteur n'est pas arrêté.

Nous allons calculer la probabilité que le réacteur soit arrêté par l'opérateur :

$$p(E) = (A + B \times a) \times C$$

$$p(E) = (0,8 + 0,84 \times 0,2) \times 0,99$$

$$p(E) = 0,024 \qquad = 3 \times 10^{-02}$$

TABLE 3.2 – **Signification des lettres de l'AdE**

La lettre	**Signification**	Probabilité
A	Observation de flux neutronique	0,8
B	Observation des canaux sur le moniteur	0,84
C	Diagnostic correct de la situation	0.99
E	Arrêt manuel du réacteur	—
F1 et F2	Arrêt du réacteur n'est pas fait	—
a, b, c	Echec des tâches	p (a) = 1-p(A)

3.4 ETUDE DE DEFAILLANCE DE CAUSE COMMUNE

Le système d'arrêt d'urgence du réacteur est déclanché suite à une analyse des signaux provenant des canaux de détection installés dans la cuve du réacteur, et servant à contrôler les différents paramètres.

Un canal de détection est composé de plusieurs éléments complémentaires (capteur, unité de traitement, amplificateur...). Dans l'industries nucléaire, les canaux de détection sont multipliés (redandés), dans le but d'éviter les erreurs résultantes des défaillances de ces dérniers et par conséquence un développement d'une séquence accidentelle.

Dans l'étude effectuée dans le cadre du projet de fin d'étude ; le développement de l'arbre de défaillance du système RPS à pris les canaux de détection comme étant des entités indépendantes. Autrement dit, l'étude n'a pas considéré le fait que ces canaux tombent en défaillance simultanément suite à une cause commune.

Dans cette section, il s'agit de traiter les défaillances de cause commune des canaux de détection, dans le but de rendre la probabilité de défaillance du système RPS plus précise.

3.4.1 Analyse qualitative

Le système de détection associé au système RPS du réacteur est composé de trois canaux de détection similaires.

Cause de base (Root Cause) Les canaux de détection sont alimentés par le même réseau électrique. Ce qui fait que si une **coupure électrique** a lieu, tous les canaux ne marchent pas.

Les capteurs des différents canaux de détection sont installés au niveau de la cuve. ils sont noyés dans l'eau du réfrigérant. Ces capteurs sont exposés au risque d'**erosion** dû au contact de ces derniers avec les traces de minéraux dans l'eau.

Mécanisme de couplage Pour composer notre groupe CCCG, nous devons identifier les points de similarité de ses composants. Pour le cas des canaux de détection, plusieurs mécanismes de couplage peuvent être constatés :

- Conception : la conception de base de tous les canaux est identique ;
- Equipements : les canaux ont les même composants ;
- Mission : la mission des canaux est le contrôle des différents paramètres du réacteur ;
- Environnement : les canaux se trouvent dans le même environnement ;
- Localisation : les canaux sont installés dans le réacteur.

Groupe CCCG Les groupes des composants de défaillance de cause commune, pouvant être formés sont :

1. Trois canaux de détection d'un paramètre donné ;
2. Trois capteurs des canaux de détection donné.

Les résultats de l'analyse qualitative sont résumés dans le tableau 3.3.

TABLE 3.3 – **Résumé de l'analyse qualitative**

Root cause	**Mécanismme de couplage**	**CCCG**
Coupure totale d'électricité	Environnement	Trois canaux de détection d'un même paramètre
Erosion	Localisation	Trois Capteurs des canaux du détection

3.4.2 Analyse quantitative

Identification des CCBE dans ce qui suit, le groupe de composants CCCG considéré est les trois canaux de détection (A, B, C). La compostition de ces canaux est réduite aux capteurs.

La figure 3.3 représente l'arbre de défaillance d'absence du signal, en prenant en compte les canaux indépendamment. Sachant que la réponse du système RPS est régi par la réception d'un signal d'au moins deux canaux ; cela veut dire qu'une absence du signal est traduite par une défaillance de deux canaux d'une façon indépendante (figure 3.3) et leurs défaillances par une cause commune.

Pour un seul canal du détection A, les CCBE sont : C_{AB}, C_{AC}, C_{BC}, et C_{ABC} auxquelles nous devons ajouter le fait de la défaillance indépendante.

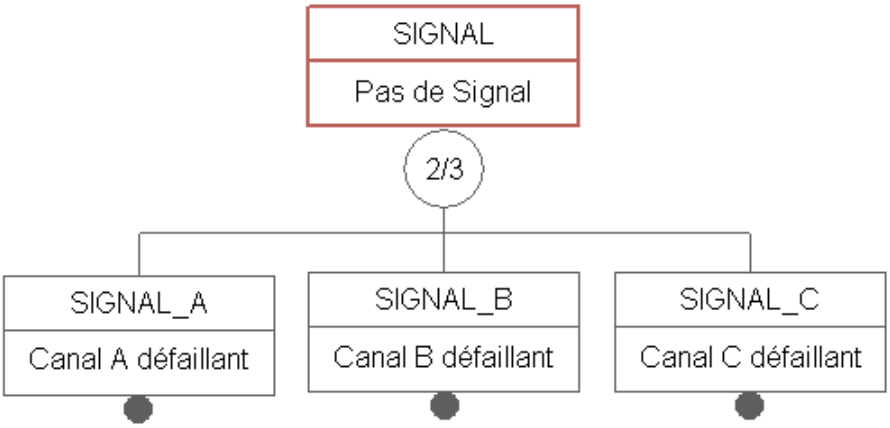

FIGURE 3.3 – **Arbre de défaillance avec EB indépendants**

Incorporation des CCBE dans l'AdD nous supposons que la défaillance simultanée de deux canaux (C_{AB} ou C_{AC} ou C_{BC},) est due à l'erosion des capteurs, et que la défaillance simultanée de trois canaux (C_{ABC}) est due à la coupure d'électricité.

Les canaux de détection sont supposés simélaires, ayant la même probabilité de défaillance. pour les CCBE nous allons affécter la probabilité d'érosion pour C_{AB} , C_{AC} et C_{BC}, et celle de la coupure électrique pour C_{ABC}.

Les Probabilités de défaillance sont données dans le tableau 3.4.

TABLE 3.4 – **Probabilités de défaillances des évènement de base**

Evènements de base	**Probabilité**	**Référence**
Défaillance indépendante du canal	$3,3.10^{-03}$	NUREG/CR-6928
Erosion (C_{AB} , C_{AC} , C_{BC})	3.10^{-03}	NUREG/CR-6928
Coupure électrique (C_{ABC})	$1,9.10^{-06}$	NUREG/CR-6928

La figure 3.4 illustre le développement de l'évènement de base de la défaillance du canal de détection.

Calcul de la nouvelle valeur de probabilité en introduisant les défaillances de cause commune dans l'arbre de défaillance du système de détaction, nous avons l'équation booléenne su système suivante :

$$S = A_i \times B_i + A_i \times C_i + B_i \times C_i + C_{AB} + C_{AC} + C_{BC} + C_{ABC}$$

En incorporant la notion de la probabilité de défaillance, l'équation algébrique du système est donnée par l'équation 2.3.

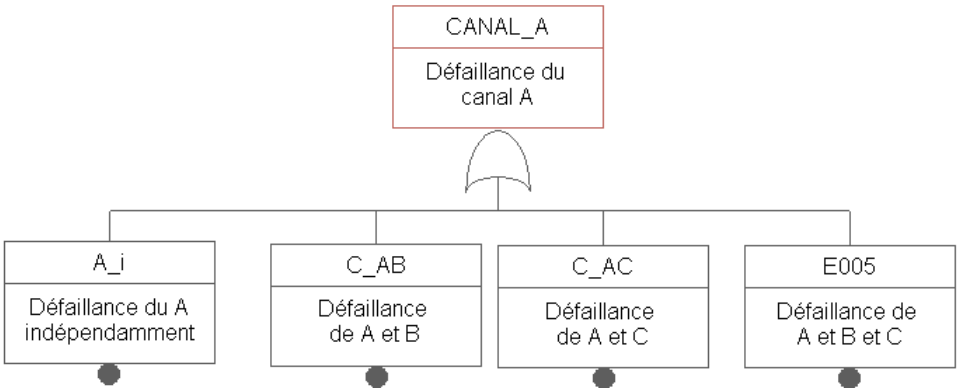

FIGURE 3.4 – **Défaillance du canal A**

Nous simplifions l'équation :

$$P(S) = 3(Q_1)^2 + 3Q_2 + Q_3$$

avec :

- Q_1 : Défaillance indépendante de chaque canal ;
- Q_2 : Défaillance de cause commune due à l'érosion ;
- Q_3 : Défaillance de cause commune due à la coupure électrique.

En utilisant le modèle du facteur alpha pour le calucl de la probabilité de défaillance de cause commune, l'équation précedente s'écrit comme suit :

$$Q_S = 3(\alpha_1 Q_t)^2 + 3/2\alpha_2 Q_t + 3\alpha_3 Q_t$$

Calcul des facteurs α_k les facteurs α sont donnés par la formule suivante

$$\alpha_1 = \frac{Q_1}{Q_1 + 2Q_2 + Q_3}$$

Calculons le facteur α_1 :

$$\alpha_1 = \frac{3,3.10^{-03}}{3,3.10^{-03} + 2 \times 3.10^{-03} + 1,9.10^{-06}}$$

$$\alpha_1 = 0,35$$

De même, nous calculons les deux autres facteurs :

$$\alpha_2 = 0,64 \qquad \alpha_3 = 0,01$$

De ce fait la probabilité de défaillance du système s'écrit comme suit :

$$Q_S = \frac{3 \times 0,64 + 3 \times 0,01}{0,05 + 2 \times 0,64 + 3 \times 0,01} Q_t$$

donc :

$$Q_S = 1,17 \times Q_t$$

avec :

$$Q_t = Q_1 + Q_2 + Q_3$$
$$Q_t = 3,3.10^{-03} + 3.10^{-03} + 1,9.10^{-06}$$

$$Q_t = 6,3.10^{-3}$$

En remplaçant la valeur de Q_t, la probabilité de défaillance du système de détection est égale à :

$$Q_S = \qquad 7,4.10^{-03}$$

Nous allons ensuite introduire cette valeur dans les arbres de défaillances du système RPS dans le cas d'un LOCA.

$$P(RPS - LOCA) = 7,4.10^{-03} + 4 \times 2,4.10^{-04} + 1,38.10^{-03}$$

$$P(RPS - LOCA) = \qquad 9,7.10^{-03}$$

Nous constatons que cette valeur est supérieure à la valeur donnée précédemment.

$$4,91.10^{-03} \quad < \quad 9,7.10^{-03}$$

3.5 NOUVEAU CALCUL DE LA PROBABILITE DE DEFAILLANCE DU SYSTEME RPS

Après avoir obtenu la probabilité de défaillance de l'actionnement manuel du système d'arrêt, nous allons l'introduire dans la probabilité de défaillance du système RPS.

La figure 3.5 représente l'AdD du système d'arrêt automatique du réacteur, en introduisant l'erreur humaine.

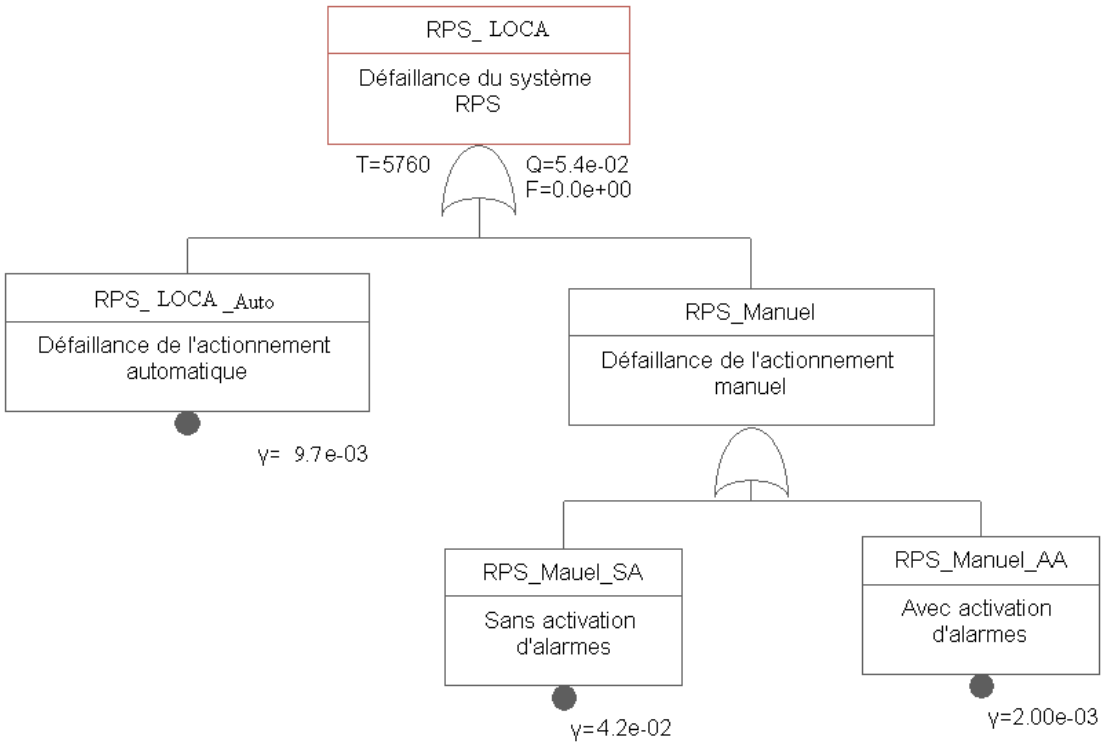

FIGURE 3.5 – **Arbre de défaillance finale du système RPS**

3.5.1 Analyse des résultats

Dans ce paragraphe, nous allons calculer les contributions des coupes minimales dans la probabilité finale de défaillance du système RPS.

Le tableau 3.5 donne le taux de contribution des coupes minimales dans l'occurence de l'évènement de défaillance de RPS :

TABLE 3.5 – **Liste des coupes minimale de défaillance de RPS**

Coupes minimales	**Probabilité**	**Contribution (%)**
Activation manuelle sans activation d'alarmes	0,003	75
Activation automatique	0,0097	20
Activation manuelle avec activation d'alarmes	0,002	5

La figure 3.6 représente le diagramme circulaire de la distribution de la probabilité de défaillance du système RPS sur les coupes minimales.

Nous constatons, à partir de la figure 3.6, que 75% de la défaillance du système d'arrêt d'urgence est due à l'intervention humaine dans le cas ou les alarmes ne sont pas activées.

L'intervention pour la diminution de la probabilité de défaillance du système d'arrêt

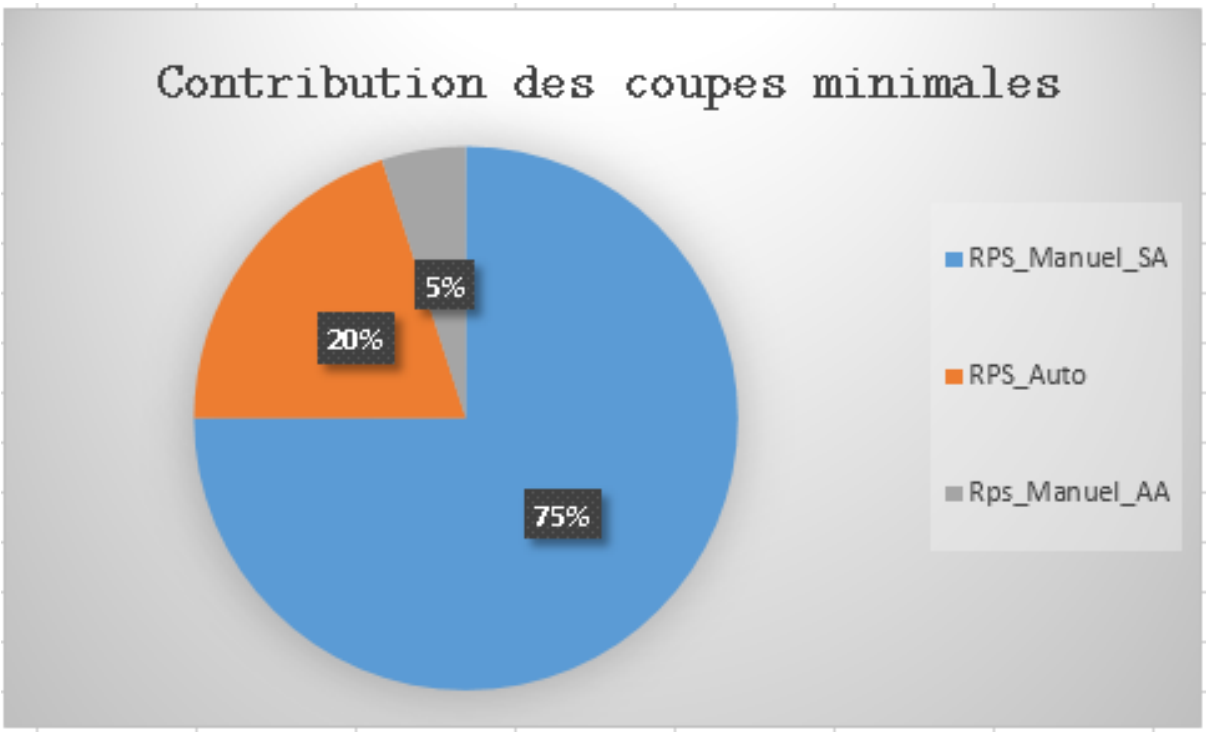

FIGURE 3.6 – **Contribution des coupes minimales**

d'urgence doit prendre en compte en premier lieu l'actionnement manuel de ce dernier, dans le cas où les alarmes ne sont pas activées. Il est recommandé la présence permanante de deux opérateurs dans la salle de contrôle. les agents travaillant doivent être hautement qualifiés pour interpréter les déviations possibles des paramètres du coeur du réacteur.

L'application de la méthode THERP, dans la première partie de l'étude, nous a permis de quantifier l'action humaine dans le cas l'actionnement manuel du système d'arrêt d'uregence RPS. Dans la deuxième partie nous avons introduit les défaillances de cause commune (DCC) sur le système de détection.

L'introduction des probabilités dans l'arbre de défaillance du système RPS, permet du calculer la probabilité excate de défaillance de ce dernier.

CONCLUSION GENERALE

Ce travail effectué au niveau de Centre de Recherche de Draria, nous a permis d'introduire les concepts de la fiabilité humaine ainsi que les défaillances de cause commune sur le système d'arrêt d'urgence d'un réacteur nucléaire de recherche.

L'étude de la fiabilité humaine a montré qu'une grande proportion de la défaillance d'un système d'arrêt RPS est due à l'intervention humaine. Nous avons constaté qu'elle contribue avec plus de 75 % de la probabilité totale de défaillance du système RPS.

Dans une deuxième partie du travail, nous avons effectué une étude des défaillances de cause commune sur le système de détection lié au système RPS. Nous avons appliqué pour cela, le modèle de facteur alpha. L'étude nous a conduit à dire que la probabilité de défaillance du système de détection augmente de $3,3.10^{-03}$ à $7,4.10^{-03}$

La probabilité globale de défaillance du système RPS dans le cas d'un LOCA en introduisant l'erreur humaine et les défaillance de cause commune augmente de $4,91.10^{-03}$ à $9,7.10^{-03}$.

Cette étude nous permet de confirmer que les erreurs humaines et les défaillances de causes communes sont considérées comme les contributeurs principaux des accidents industriels.

REFERENCES BIBLIOGRAPHIQUES

[1] A. P. ,. A. C. ,. U. R. Fabio De Felice, Modelling application for cognitive reliability and error analysis method, Italy : International Journal of Engineering and Technology (IJET), Nov 2013.

[2] D. A. AZZABI, Optimisation multicritère de la fiabilité : application du model de GOAL programming avec les fonctions de satisfaction dans l'industrie du traitement de gaz, Université d'Angers, 2010.

[3] R. P. Elodie MICHE, «Démarche d'évaluation des Barrières Humaines Oméga 20,» INERIS, 2009.

[4] H. H. M. Abderaouf HADJ MABROUK, «Approche d'intégration de l'erreur humaine dans le retour d'expérience,» Institut National des Recherches sur les Transports et leurs Sécurité , Joinville, France, Janvier 2003.

[5] H. J. P. J. L. P. B. J. O'Hara J.M., «Human Factors Engineering Program Review Model, NUREG-0711,» NRC, 2004.

[6] T. N. V. Romuald Perinet, «Evaluer la fibilité humaine : quelle(s) méthode(s) à chisir,» INERIS, France, 2014.

[7] F. Ménage, «L'homme probabiliste ? prendre en compte les facteurs humains dans les études probabilistes de sûreté,» IRSN, France, 2011.

[8] J. Resmaussen, «Skills, rules, end knowledge ; signals, signs and symbols, and other distenctions in human performance models,» IEEE transaction systems, man and cybernetics, vol. 13, pp. 257-266, 1983.

[9] J. M. Stellman, Encyclopédie de sécurité et de santé au travail, V2, ILO , 2000.

[10] G. D., N.B. et N. VILLAUME, REPRESENTATION DES DEFAILLANCES DE CAUSE COMMUNE D'UN SYSTEME PROGRAMME DE GRANDE TAILLE PAR RESEAUX DE PETRI COLORES, TEMPORISES ET HIERARCHIQUES, France, 2013.

[11] JURVILLIER I., LAVIRON A., VERS UN SIMULATEUR SANS CABLAGE POUR LES ANALYSES DE FIABILITE, Londres, 1991.

[12] M. WONG, Common Cause Failure (CCF) Analysis and Generic CCF Data US Experience, IAEA Technical Review Meeting, November 06-08, 2013

[13] MOSLENLIV ; D. RASMUSON ; F. M.MARSAL, Guidelines on Modeling Common-Cause Failures in Probabilistic Risk Assessment, U.S. Nuclear Regulatory Commission, 1998.