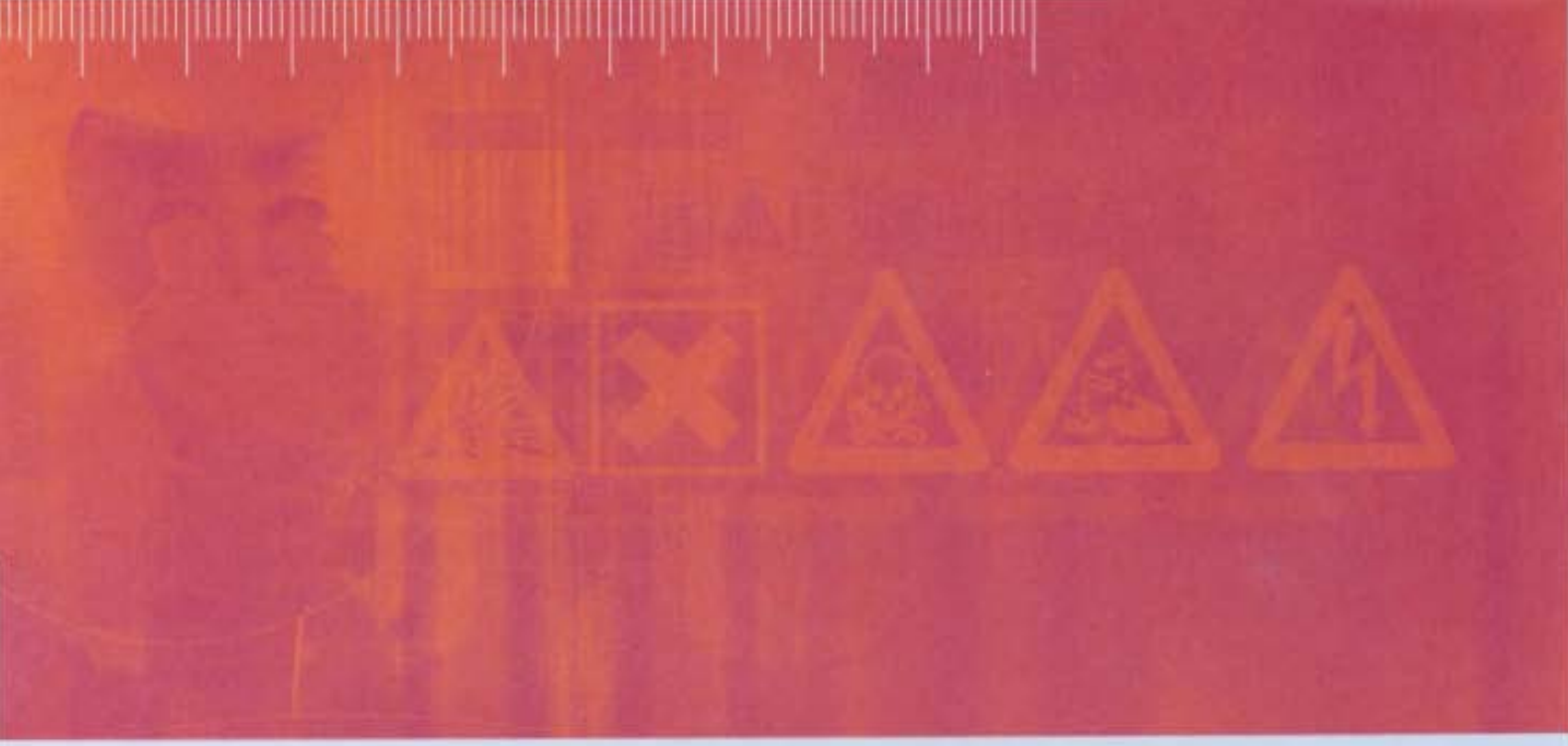


Rapport d'étude 21 / 03 / 2011

N° DRA-10-111793-01257A

État de l'art des méthodes d'évaluation probabiliste de la fiabilité humaine

INERIS

maîtriser le risque
pour un développement durable

État de l'art des méthodes d'évaluation probabiliste de la fiabilité humaine

Direction des Risques Accidentels
Verneuil-en-Halatte (Oise)

Liste des personnes ayant participé à l'étude : Romuald PERINET, T.N. VU, modifié pour mise en ligne par Franck PRATS

PRÉAMBULE

Le présent rapport a été établi sur la base des informations fournies à l'INERIS, des données (scientifiques ou techniques) disponibles et objectives et de la réglementation en vigueur.

La responsabilité de l'INERIS ne pourra être engagée si les informations qui lui ont été communiquées sont incomplètes ou erronées.

Les avis, recommandations, préconisations ou équivalent qui seraient portés par l'INERIS dans le cadre des prestations qui lui sont confiées, peuvent aider à la prise de décision. Étant donné la mission qui incombe à l'INERIS de par son décret de création, l'INERIS n'intervient pas dans la prise de décision proprement dite. La responsabilité de l'INERIS ne peut donc se substituer à celle du décideur.

Le destinataire utilisera les résultats inclus dans le présent rapport intégralement ou sinon de manière objective. Son utilisation sous forme d'extraits ou de notes de synthèse sera faite sous la seule et entière responsabilité du destinataire. Il en est de même pour toute modification qui y serait apportée.

L'INERIS dégage toute responsabilité pour chaque utilisation du rapport en dehors de la destination de la prestation.

	Rédaction	Relecture	Vérification	Approbation
NOM	Romuald PERINET	Ludovic MOULIN	Marie-Astrid SOENEN	Sylvain CHAUMETTE
Qualité	Unité HUGO (Facteurs HUmains et GOuvernance des risques) Direction des Risques Accidentels	Responsable de l'Unité HUGO (Facteurs HUmains et GOuvernance des Risques) Direction des Risques Accidentels	Déléguée Appui à l'Administration Direction des Risques Accidentels	Responsable du Pôle AGIR (Analyse et Gestion Intégrées des Risques Direction des Risques Accidentels
Visa				

TABLE DES MATIÈRES

1. GLOSSAIRE 5

2. INTRODUCTION 9

2.1 Cadre de l'étude 9

2.2 Objectif de l'étude 9

2.3 Périmètre de l'étude 10

2.4 Plan du rapport 10

3. ENJEUX DE L'INTÉGRATION DE LA FIABILITÉ HUMAINE DANS L'ANALYSE DES RISQUES 11

4. CADRE GÉNÉRAL DE L'ÉVALUATION DE LA FIABILITÉ HUMAINE 13

4.1 Définition de la fiabilité humaine 13

4.2 Ordres de grandeurs 13

4.2.1 Inventaire (non exhaustif) des méthodes 14

4.2.2 Classification des méthodes 16

4.3 Démarche générale d'évaluation de la fiabilité humaine 19

5. DESCRIPTION SUCCINTES DES MÉTHODES RETENUES DANS CETTE ÉTUDE 23

5.1 Liste des méthodes 23

5.2 Présentation synthétique de chacune des méthodes 25

5.3 Synthèse 41

6. CONCLUSIONS 45

7. RÉFÉRENCES 47

7.1 Références réglementaires 47

7.2 Références techniques 47

8. LISTE DES ANNEXES 55

1. GLOSSAIRE

ACIH	Analyse des Conséquences de l'Infiabilité Humaine
AEN	Agence pour l'énergie nucléaire
AFH	Analyse de la Fiabilité Humaine
AIEA	International Atomic Energy Agency
AIPA	Accident Investigation And Progression Analysis
AMDE(C)	Analyse des Modes de Défaillance, de leurs Effets (et de leur Criticité)
APJ	Absolute Probability Judgement
APOSCIH	Analyse a posteriori des conséquences de l'infiabilité
APR	Analyse Préliminaire des Risques
APRECIH	Analyse préliminaire des conséquences de l'infiabilité
ASEP	Accident Sequence Evaluation Procedure
ATEX	ATmosphères EXplosibles
ATHEANA	A Technique for Human Event Analysis
BHEP	Basic human error probability
BRF	Basic Risk Factors
CFP	Cognitive Failure Probability
CICA	Configuration Importante de la Conduite Accidentelle
COCOM	Contextual Control Model
COGENT	Cognitive Event Tree System
CORE-DATA	Computerised Operator Reliability Evaluation - DATA
CPC	Common Performance Conditions
CREAM	Cognitive Reliability & Error Analysis Method
CSIN	Comité sur la Sûreté des Installations Nucléaires
DRA	Direction des Risques Accidentels
ECOM	Error of Commission
EDD	Étude De Dangers
EDF	Électricité de France
EE	Effet Évalué
EN	European Standard
ENVID	Environmental Hazard Identification

EOC	Error of Commission (Erreur de Réalisation)
EOO	Error of Omission (Erreur d'Omission)
EOS	Emergency Operation System
EPC	Error Producing Conditions
EPFH	Évaluation Probabiliste de la Fiabilité Humaine
EPR	Évaluation Probabiliste des Risques
EPS	Étude Probabiliste de Sûreté
ETTO	Efficiency Thoroughness Trade Off (Efficacité, Minutie, Compromis)
FH	Facteur Humain
FOH	Facteur Organisationnel et Humain
FRAM	Functional Resonance Analysis Method
GTT	Generic Task Type
HAZID	Hazard Identification
HAZOP	Hazard and Operability
HCR	Human Cognitive Reliability
HEART	Human Error Assessment and Reduction Technique
HEP	Human Error Probability
HFE	Human Failure Event
HRA	Human Reliability Analysis
HTA	Hierarchical Task Analysis
IDA	Influence Diagrams Approach
IEC	International Electrotechnical Commission
INERIS	Institut National de l'Environnement Industriel et des Risques
IRS	Incident Reporting System (i.e. Système de Notification des Incidents)
ISO	International Organization for Standardization
JHEDI	Justification of Human Error Data Information
MTES	Ministère de la Transition Écologique et Solidaire
MERMOS	Méthode d'Évaluation de la Réalisation des Missions Opérateur pour la Sûreté
NARA	Nuclear Action Reliability Assessment
NF	Norme Française
NHEP	Nominal Human Error Probability
NRC	Nuclear Regulatory Commission

OAT	Operator Action Tree
OCDE	Organisation de coopération et de développement économiques
ORE	Operator Reliability Experiments
PC	Paired Comparisons
PD	Poids de Dégradation
PN	Probabilité Nominale
PRA	Probabilistic Risk Assessment
PSA	Probabilistic Safety Assessment
PSF	Performance-Shaping Factor
QRA	Quantitative Risk Assessment
REX	Retour d'EXpérience
SHARP	Systematic Human Action Reliability Procedure
SHERPA	Systematic Human Error Reduction and Prediction Approach
SIG	Système d'Information Géographique
SIL	Safety Integrity Level
SLI	Success Likelihood Index
SLIM-MAUD	Success Likelihood Index Method using Multi-Attribute Utility Decomposition
SMoC	Simple Model of Cognition
SPS	Safety Probabilistic Study
SRK	Skill Rule Knowledge
STAHR	Socio-Technical Assessment Of Human Reliability
TESEO	Technica Empirica Stima Errori Operatori
THERP	Technique for Human Error Rate Prediction
TRC	Time Reliability Correlation
US	United States

2. INTRODUCTION

2.1 CADRE DE L'ÉTUDE

Cette étude a été réalisée avec le soutien du Ministère en charge de la prévention des risques d'accidents majeurs et dans l'optique de consolider la base de méthodes disponibles pour les inspecteurs, les industriels et bureaux d'études concernant la prise en compte des dimensions humaines de la maîtrise des risques dans l'analyse des risques, l'élaboration des études de dangers et l'amélioration du niveau de sécurité des installations dangereuses.

Ce rapport est édité en support du rapport « Probabilité dans les études de sécurité et de dangers – Ω-24[1] ».

2.2 OBJECTIF DE L'ÉTUDE

L'objectif est d'étudier la manière dont la fiabilité humaine est prise en compte dans l'évaluation des risques d'accident majeurs. Cette étude comporte deux principales tâches :

1. La réalisation d'un état de l'art bibliographique des méthodes disponibles dans la littérature ;
2. La réalisation d'un état des lieux des méthodes et pratiques réellement mises en œuvre par les industriels et bureaux d'étude.

Ce rapport présente de manière détaillée les résultats relatifs à la tâche n°1. Ces résultats ont principalement vocation à alimenter les réflexions menées par l'INERIS à la fois pour la consolidation de la méthode Oméga 20 (référence [52]) d'évaluation des Barrières Humaines de Sécurité et pour la mise à disposition d'une démarche permettant de mieux prendre en compte les facteurs humains dans l'évaluation des événements initiateurs. D'une manière générale, ces résultats pourront être utilisés pour porter un regard critique et faire progresser les méthodes employées dans le domaine des installations classées.

[1] DRA-18-171229-00933A

2.3 PÉRIMÈTRE DE L'ÉTUDE

Ce rapport fait suite à une étude préliminaire. Parmi ses conclusions, cette étude attirait l'attention sur deux principaux points :

- L'existence de deux principales générations de méthodes se distinguant principalement selon deux critères : le niveau de prise en compte du contexte d'occurrence des erreurs humaines et le niveau de prise en compte des dimensions cognitives sous-jacentes ;
- L'existence d'un paradoxe : de très nombreuses méthodes sont référencées dans la littérature mais peu d'entre elles ont été validées ou mis à l'épreuve d'études de sensibilité et peu sont réellement mises en œuvre.

Dans ce contexte, la sélection des méthodes retenues dans cette étude a été guidée par la recherche d'un échantillon le plus représentatif possible de la diversité des méthodes existantes. Notre sélection a également privilégié les méthodes les plus « populaires », considérant que l'information disponible sur celles-ci serait plus abondante.

Compte tenu de ces critères et considérant en première analyse l'existence de plus de cinquante méthodes, nous avons finalement retenu les méthodes suivantes : THERP, HEART, HRC, SLIM-MAUD, ATHEANA, MERMOS, CREAM, TESEO, SHERPA, ACIH, TRIPOD et FRAM.

2.4 PLAN DU RAPPORT

Le rapport se compose de deux principales parties.

La première partie comprend un rappel succinct des enjeux de l'intégration de la fiabilité humaine dans l'analyse des risques industriels. Elle fournit également une vue d'ensemble des concepts utilisés dans le domaine de la fiabilité humaine des différentes méthodes étudiées dans ce rapport. Cette première partie propose enfin une grille d'analyse des différentes méthodes en vue de leur inter-comparaison.

La seconde partie présente, en annexe, une description détaillée de chacune des méthodes. Pour chacune d'elle, l'étude a porté sur leurs fondements, sur leur procédure d'évaluation de la fiabilité humaine, sur leurs données d'entrée et de sortie et sur leur validation. De plus, un même cas industriel (« redémarrage d'un four »), inspiré d'un exemple contenu dans l'ouvrage descriptif de la méthode CREAM (référence [44]), a été utilisé pour illustrer l'application de chaque méthode.

3. ENJEUX DE L'INTÉGRATION DE LA FIABILITÉ HUMAINE DANS L'ANALYSE DES RISQUES

Il est désormais évident que les facteurs humains et organisationnels jouent un rôle important dans l'occurrence de la plupart des accidents. Dans son inventaire 2009 des accidents technologiques, le BARPI [2] mentionne que seul ou associé à une défaillance matérielle, le facteur organisationnel et humain prime en 2008 dans au moins 61 % des accidents répertoriés (la part de cette cause dans les accidents était de 49% en 1992). Le BARPI souligne que ces facteurs restent sans doute encore sous-évalués dans nombre de cas d'accidents en ajoutant que leur prise en compte suppose une certaine profondeur d'analyse qui n'est pas toujours atteinte.

Suite à la catastrophe de Toulouse survenue le 21 septembre 2001, le rapport parlementaire Loos – Le Déaut [1], a mis en évidence la nécessité de « réhabiliter la place de la dimension sociale et humaine dans l'analyse des risques face à l'approche purement technique souvent privilégiée dans des secteurs caractérisés par la complexité des procédés et le haut niveau technologique des installations. » (Partie 2 – «Une meilleure prise en compte des facteurs humains de dangers est nécessaire», p. 62). Ce rapport mentionne également l'importance de prendre en compte les aspects organisationnels dans l'évaluation des risques (Partie 1 ; § 1.C.3a, p. 31).

Suite à cette catastrophe, la loi du 30 juillet 2003 (loi Bachelot) a introduit une nouvelle exigence en matière d'évaluation des risques. Cette loi impose aux installations classées pour la protection de l'environnement soumises à autorisation d'évaluer la probabilité d'occurrence des accidents susceptibles d'être générés par leurs installations, en évaluant la performance des barrières techniques et humaines mises en place pour prévenir l'occurrence de ces accidents. Ainsi, depuis cette évolution l'exercice obligatoire de démonstration de maîtrise des risques auquel doivent se livrer les exploitants d'installations dangereuses implique d'évaluer la fiabilité de certaines tâches humaines.

Comment procéder à cette évaluation ? La réponse à cette question soulève toujours, 50 ans après les premiers développements de méthodes, de nombreuses questions :

- Comment identifier les erreurs et leurs différentes causes probables parmi les nombreuses causes possibles ?
- Comment caractériser le poids des différentes causes dans l'occurrence de ces erreurs ?
- Comment représenter le rôle de ces événements humains dans les scénarios accidentels ?
- Comment proposer et justifier des mesures de maîtrise des risques adaptées ?

L'enjeu de cette étude est de constituer une base de connaissance de référence pour permettre de choisir la méthode ou les éléments méthodologiques les mieux adaptés aux contraintes propres de chaque industrie. Les critères d'évaluations permettent également de comparer les méthodes avec d'autres méthodes, comme l'OMEGA 20 par exemple.

4. CADRE GÉNÉRAL DE L'ÉVALUATION DE LA FIABILITÉ HUMAINE

4.1 DÉFINITION DE LA FIABILITÉ HUMAINE

Meister [69] a défini la fiabilité humaine comme la probabilité qu'une mission ou une tâche soit réalisée avec succès par le personnel à n'importe quelle étape nécessaire de l'opération dans un délai minimum requis (si l'exigence de temps existe).

Swain et Guttmann [88] définissent la fiabilité humaine comme la probabilité qu'une personne (1) exécute correctement l'activité requise dans un délai requis (si le temps est un facteur limitant) et (2) ne réalise aucune activité complémentaire (sans rapport avec la tâche) qui pourrait dégrader le système.

Dans la pratique, la fiabilité humaine est caractérisée par la probabilité d'échec d'une mission humaine.

4.2 ORDRES DE GRANDEURS

On trouve dans la bibliographie des valeurs chiffrées permettant de donner un ordre de grandeur des taux de défaillance des actions humaines ou probabilité d'erreurs humaines.

- L'annexe F de la norme NF-EN 61511-3 [6] propose les valeurs suivantes pour estimer la probabilité moyenne de défaillance à la demande (PFD) pour certaines tâches spécifiques :

Action d'un homme entraîné et sans stress	$1,0 \times 10^{-2}$ à $1,0 \times 10^{-4}$
Réponse d'un opérateur à une alarme	$1,0 \times 10^{-1}$
Action d'un homme stressé	0,5 à 1

- Swain et Guttmann ont proposé dans le Handbook of HRA [88] 27 tables qui fournissent des probabilités nominales d'échec d'actions humaines et des facteurs d'influence tels que le niveau de stress, l'expérience, la dépendance, etc. Selon type d'action, la probabilité nominale peut varier entre $5,0 \times 10^{-4}$ et 1.
- La méthode HEART propose des probabilités nominales pour neuf tâches génériques ; ces probabilités oscillent entre 0,55 et $2,0 \times 10^{-5}$ [102].
- Selon la méthode MERMOS la fiabilité des tâches humaines approche dans le meilleur des cas la probabilité de 10^{-5}.

4.2.1 INVENTAIRE (NON EXHAUSTIF) DES MÉTHODES

Les premières études de fiabilité humaine ont été réalisées dans les années 60-70, principalement dans le domaine nucléaire, avec le développement de la méthode THERP (Technique for Human Rate Prediction) [86],[95]. Parallèlement, s'est développée la technique d'évaluation probabiliste des risques avec, en 1975, la réalisation de la première Étude Probabiliste de Sûreté (EPS) d'un réacteur nucléaire aux États-Unis [95]. Cette étude considérait les actions des opérateurs comme un des trois principaux contributeurs du risque. Quatre ans plus tard, suite à l'accident de Three Mile Island [54], le développement de la technique d'évaluation de la fiabilité humaine a pris un essor considérable.

En effet, cet accident a révélé l'importance des facteurs humains : l'analyse de cet accident [54] avait en effet mis en évidence l'incompréhension des opérateurs devant le comportement du réacteur compte-tenu de la formation et de l'instrumentation dont ils disposaient. Depuis lors, l'industrie nucléaire a multiplié les évaluations probabilistes de sûreté intégrant généralement une Évaluation Probabiliste de la Fiabilité Humaine (EPFH) [50], [51], [83]. Ce secteur industriel est un des principaux contributeurs, avec l'industrie aéronautique, du développement de l'évaluation de la fiabilité humaine.

De nombreuses méthodes d'identification et de quantification de la fiabilité humaine sont aujourd'hui disponibles [15], [32], [37], [56], [77], [79], [85], mais peu ont fait l'objet d'une réelle validation. Les études de Bell et al. [15] ont identifié 72 méthodes et acronymes concernant la fiabilité humaine. Salmon et al. mentionnent une quarantaine de méthodes [79]. Stanton et al. [85] indiquent environ 70 méthodes. En résumé, le Tableau 1 présente environ 80 méthodes et acronymes qui abordent la fiabilité humaine et l'analyse des tâches.

Tableau 1: Liste des méthodes d'évaluation de la fiabilité humaine et analyse des tâches

N°	Méthode	Description
1	ACIH	Analyse des Conséquences de l'Infiabilité Humaine
2	ACTA	Applied Cognitive Task Analysis
3	AIPA	Accident Initiation and Progression Analysis
4	APJ	Absolute Probability Judgement
5	ASEP	Accident Séquence Évaluation Procédure
6	ATHEANA	A Technique for Human Event Analysis
7	CAHR	Connectionism Approach for Assessing the Reliability of Human actions
8	CARA	Controller Action Reliability Assessment
9	CBDT	Cause-Based Decision Tree method
10	CDM	Critical Decision method
11	CES	Cognitive Environmental Simulation
12	CESA	Commission Errors Search and Assessment
13	CM	Confusion Matrix
14	CODA	Conclusions from occurrences by descriptions of actions
15	COGENT	COGnitive EveNt Tree

N°	Méthode	Description
16	COSIMO	Cognitive Simulation Model
17	CPA	Critical Path Analysis for Multimodal activity
18	CREAM	Cognitive Reliability and Error Analysis Method
19	DAD	Decision Action Diagrams
20	DNE	Direct Numerical Estimation
21	EPRI	Electric Power Research Institute (EPRI) HRA Calculator
22	FACE	Framework for Analysing Commission errors
23	FLIM	Failure Likelihood Index Method
24	FMEA	Failure Modes and Effects Analysis
25	FRAM	Functional Resonance Accident Model
26	FTA	Fault Tree Analysis
27	GOMS	Goals, Operators, Methods and Selection Rules
28	HCR	Human Cognitive Reliability
29	HE HAZOP	Human Error Hazard and Operability Study
30	HEA	Human Error Analysis
31	HEART	Human Error Assessment And Reduction Technique
32	HEI	Human Error Identification
33	HEIST	Human Error Identification in Systems Technique
34	HERA	Human error and Recovery Assessment Framework
35	HET	Human error template
36	HFA	Human Factors Analysis
37	HF-RBE	Human Factors Reliability Benchmark Exercise
38	HORAAM	Human and Organisational Reliability Analysis in Accident Management
39	HPES	Human Performance Évaluation System
40	HRAET	Human Reliability Analysis Event Tree
41	HRAG	Human Reliability Assessor's Guide
42	HRMS	Human Reliability Management System
43	HRQ	Human Reliability Quantification
44	HTA	Hierarchical Task Analysis
45	IDA	Influence Diagrams Approach
46	IMAS	Influence Modelling and Assessment System
47	INTENT	Not an acronym
48	ITA	Initial Task Analysis
49	JHEDI	Justification of Human Error Data Information
50	MAPPS	Maintenance Personnel Performance Simulation
51	MC	Matrice de confusion
52	MDTA	Misdiagnosis Tree Analysis
53	MERMOS	Méthode d'Évaluation de la Réalisation des Missions Opérateur pour la Sûreté
54	NARA	Nuclear Action Reliability Assessment
55	OAT / OAET	Operator Action Tree / Operator Action Event Tree

N°	Méthode	Description
56	OHPRA	Operational Human Performance Reliability analysis
57	PC	Paired Comparisons
58	PEM	Psychological Error Mechanism
59	PHECA	Potential Human Error Causes Analysis
60	PHOENIX	Prediction of Human Operator Error using Numerical Index eXtrapolation
61	PHRA	Probabilistic Human Reliability Assessment
62	SCHEMA	System for Critical Human Error management analysis
63	SHARP	Systematic Human action Reliability Procedure
64	SHERPA	Systematic Human Error Reduction and Prediction Approach
65	SLIM-MAUD	Success Likelihood Index Method using Multi-Attribute Utility Decomposition
66	SLIM-SARAH	SLIM with Sensitivity Analysis and Reliability Assessment of Humans
67	SPAR-H	Standardized Plant Analysis Risk-Human Reliability Analysis
68	SPEAR	System for Predictive Error Analysis and Reduction
69	SRK	Skill-Rule-Knowledge
70	STA	Sequential Task Analysis
71	STAHR	Socio-Technical Assessment of Human Reliability
72	STAMP	System-theoretic model of accidents
73	TAFEI	Task Analysis For Error Identification
74	TAKD	Task Analysis Knowledge Decomposition
75	TEPPS	Technique for Estimating Personal Performance Standards
76	TESEO	Technica Empirica Stima Errori Operatori
77	THERP	Technique for Human Error Rate Prediction
78	TLA	Timeline Analysis
79	TRACEr	Technique for the Retrospective and Predictive Analysis of Cognitive Errors
80	TRC	Time Reliability Correlation
81	TRIPOD	Méthode de sécurité organisationnelle
82	VPA	Verbal Protocol Analysis

4.2.2 CLASSIFICATION DES MÉTHODES

Les méthodes d'évaluation de la fiabilité humaine peuvent être classées en deux manières :

- classification par générations,
- et classification par type d'approches.

4.2.2.1 CLASSIFICATION PAR GÉNÉRATIONS

La classification par générations est apparue dans les années 90 [44], [60]. Plusieurs auteurs ont adopté cette classification [15], [77].

Il est assez habituel de distinguer deux générations successives de méthodes (transition qui peut être datée des années 90s) marquant une évolution significative relative à la manière de prendre en compte les caractéristiques de l'homme et de sa fiabilité.

Les méthodes de 1ère génération : La première génération est classiquement dite centrée sur « l'erreur humaine » assimilant l'individu à un élément parmi d'autres du système technique (modèle mécaniste de l'individu). Ces méthodes visent à identifier les défaillances humaines, dépendante d'un contexte, mais sans recherche approfondie des causes de l'erreur.

Ces méthodes proposent une démarche de caractérisation des contextes des missions humaines en référence à un ensemble de tâches génériques et/ou de facteurs de contexte (exemples : défauts de procédures, ou de formation ou d'indications) auxquels sont associés des coefficients ou probabilités d'échec.

Exemples de méthodes de 1ère génération :

- AIPA (Accident Investigation And Progression Analysis)
- MC (Matrice de Confusion)
- OAT (Operator Action Tree)
- STAHR (Socio-Technical Assessment Of Human Reliability)
- THERP (Technique for Human Error Rate Prediction)
- TESEO (Technica Empirica Stima Errori Operatori)
- SLIM-MAUD (Success Likelihood Index Method using Multi-Attribute Utility Decomposition)
- HEART (Human Error Assessment And Reduction Technique)
- HCR (Human Cognitive Reliability)

Les méthodes de 2ème génération : Elles s'intéressent aux processus cognitifs permettant d'expliquer et de prédire les défaillances humaines. Ces méthodes postulent l'existence d'une certaine dépendance entre les différents facteurs de contexte et intègre cet aspect dans l'évaluation.

Exemples de méthodes de 2ème génération :

- CREAM (Cognitive Reliability and Error Analysis Method)
- COGENT (COGnitive EveNt Tree)
- ATHEANA (A Technique for Human Event Analysis)
- MERMOS (Méthode d'Évaluation de la Réalisation des Missions Opérateur pour la Sûreté)

Les méthodes de 3ème génération : Cette génération de méthode a été proposée par Bell et Holroyd [15]. Les publications sur les méthodes de 3ème génération sont très peu nombreuses. Selon Bell et Holroyd [15], cette génération est basée sur la méthode HEART de 1ère génération. Les méthodes de troisième génération s'intéressent à l'environnement organisationnel de travail susceptible de conduire et contraindre l'individu à l'erreur (revue RSE [78]).

Exemples de méthodes de 3ème génération :

- NARA (Nuclear Action Reliability Assessment) [25], [59]
- CARA (Controller Action Reliability Assessment) [60]
- TRIPOD [34], [35]
- WPAM (Work Process Analysis Model) [26]
- FRAM (Functional Resonance Analysis Method) [45]
- BORA (Barrier- and Operational Risk Analysis) [12]
- I-Risk [16]

4.2.2.2 CLASSIFICATION PAR TYPES D'APPROCHES

Ce type de classification a été proposé par Pyy P. [75]. Les méthodes EFH ou HRA peuvent être classifiées en fonction:

- du niveau de détail des analyses réalisées,
- du type de modélisation cognitive prise en compte,
- de la manière dont elle prend en compte :
  - la dimension temporelle,
  - les facteurs contextuels,
  - les données de fiabilité utilisées.

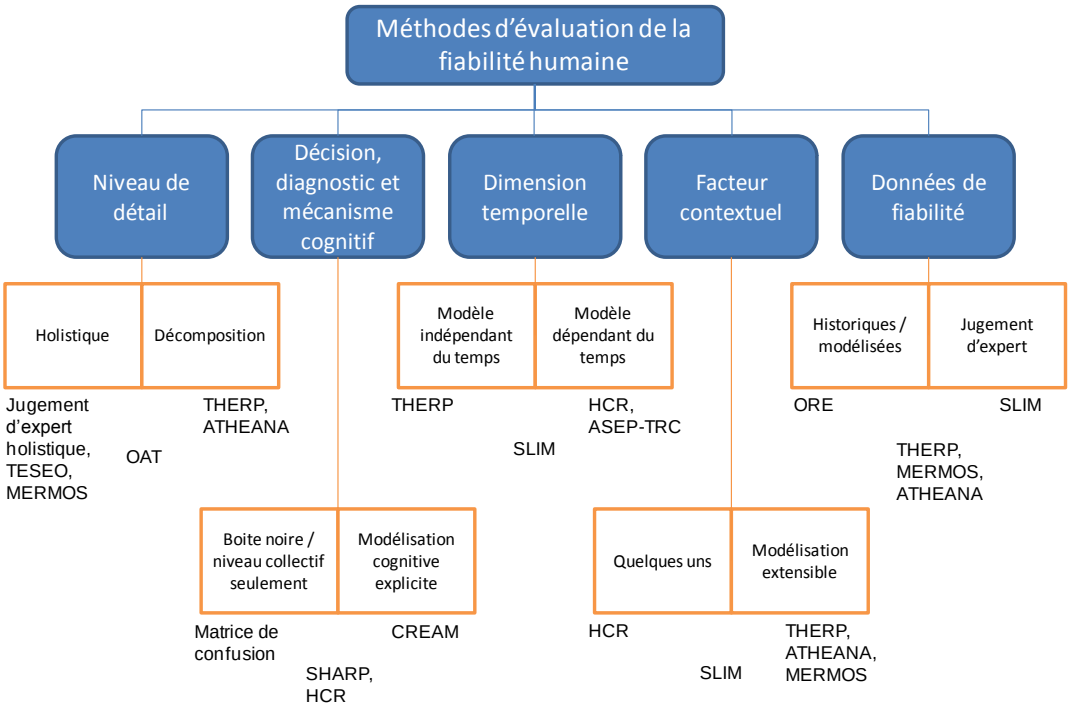


Figure 1 : Classification des méthodes d'évaluation de la fiabilité humaine selon Pyy P. [75]

4.2.2.3 CONCLUSIONS SUR LA CLASSIFICATION DES MÉTHODES

La classification par générations propose une vision historique du développement des méthodes, mettant implicitement en évidence que les méthodes les plus pertinentes sont celles de troisième génération, c'est-à-dire celles prenant le mieux en compte l'environnement organisationnel. Ces méthodes présentent effectivement l'avantage d'élargir le champ des dimensions prises en compte dans l'évaluation de la fiabilité humane. Néanmoins, ces méthodes semblent le plus souvent difficilement applicables dans le contexte de la réalisation d'une étude de dangers, en raison principalement de l'importance des ressources que leur mise en œuvre requiert.

La classification par types renseigne davantage sur les modes d'analyses et d'évaluation des tâches et ainsi sur les ressources à mettre en œuvre. Par exemple, la catégorie « niveau de détail » comporte deux items : holistique et décomposition. Les méthodes appartement à la famille « holistique » font appel à une appréciation globale pouvant être obtenue plus rapidement que le cas des méthodes appartenant à la famille « décomposition », beaucoup plus analytiques. Cette classification paraît plus adaptée pour choisir une méthode correspondant mieux aux objectifs poursuivis et aux contraintes de l'évaluation.

4.3 DÉMARCHE GÉNÉRALE D'ÉVALUATION DE LA FIABILITÉ HUMAINE

Kirwan [56] propose une démarche générale d'Évaluation de la Fiabilité Humaine (EFH) ou Human Reliability Assessment (HRA). La démarche présentée en Figure 2 est inspirée de celle proposée par Kirwan [56].

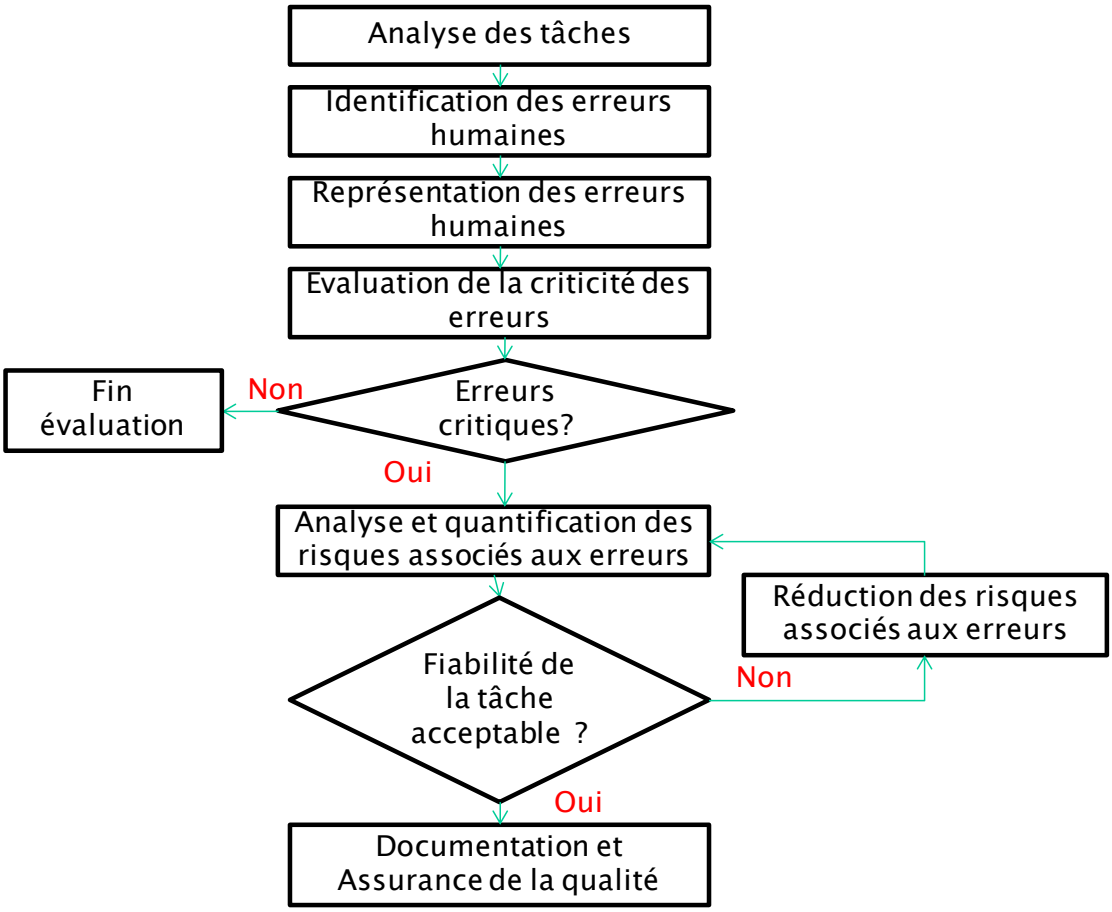


Figure 2 : Démarche générale d'évaluation de la fiabilité humaine

L'analyse des tâches vise à déterminer en détail le rôle des opérateurs et leurs interactions avec les systèmes. Exemples de méthodes : analyse hiérarchisée de tâche (HTA – Hierarchical Task Analysis), Diagramme décision – action (DAD – Decision Action Diagrams).

L'identification des erreurs humaines ou HEI (Human Error Identification) est probablement la partie la plus difficile de l'étude EFH. L'annexe n°1 propose quelques typologies d'erreurs parmi les plus connues et les plus utilisées dans les études d'analyse de risques. Exemples de méthodes :

- THERP (Technique for Human error Rate Prediction),
- Human Error HAZOP,
- SHERPA (Systematic Human Error Reduction and Prediction Approach),
- Approche SRK (Skill-, Rule-, and Knowledge-based behaviour),
- CREAM (Cognitive Reliability and Error Analysis Method).

La Représentation des erreurs humaines consiste à les représenter avec d'autres défaillances matérielles dans des arbres logiques, tels que l'arbre de défaillance et l'arbre d'événement.

L'évaluation des impacts des erreurs humaines vise à évaluer l'impact des erreurs sur la sécurité du système. Ce calcul permet de repérer des erreurs critiques pour la sécurité en répondant aux questions suivantes : le risque d'erreur humaine est-il acceptable ? Quels moyens peuvent permettre de réduire ce risque à un niveau acceptable ?

L'analyse et quantification des erreurs humaines est la partie la plus développée dans les méthodes identifiées dans la littérature. Exemples de méthodes :

- THERP (Technique for Human Error Rate Prediction)
- TESEO (Technica Empirica Stima Errori Operatori)
- SLIM- (Success Likelihood Index Method)
- HEART (Human Error Assessment And Reduction Technique)
- HCR (Human Cognitive Reliability)
- MC (Matrice de Confusion)
- OAT (Operator Action Tree)
- STAHR (Socio-Technical Assessment Of Human Reliability)
- APJ (Absolute Probability Judgement)
- ATHEANA (A Technique for Human Event Analysis)
- MERMOS (Méthode d'Évaluation de la Réalisation des Missions Opérateur pour la Sûreté)
- CREAM (Cognitive Reliability and Error Analysis Method)

La réduction des risques d'erreurs humaines est nécessaire si leur impact sur le niveau du risque global est jugé trop important. Cette réduction s'applique aux causes des erreurs identifiées ou sur les facteurs de performances utilisés dans la phase de quantification. Des dispositions doivent être prises pour maintenir dans le temps le niveau de performance.

La documentation et l'assurance de la qualité est la dernière étape du process d'une EFH, pendant laquelle les méthodes et les résultats sont documentés. Les méthodes et les résultats doivent pouvoir être audités par une équipe d'évaluation indépendante.

5. DESCRIPTION SUCCINTES DES MÉTHODES RETENUES DANS CETTE ÉTUDE

5.1 LISTE DES MÉTHODES

Les méthodes retenues pour cette étude figurent parmi les plus reconnues et les plus répandues. La liste de ces méthodes est donnée dans le Tableau 2 et la Figure 3.

Tableau 2: Liste des méthodes d'évaluation de la fiabilité humaine retenues pour une évaluation approfondie

Génération	Date	Méthode	Description
1ère génération	1963 (1983)	THERP	Technique for Human Error Rate Prediction
	1980	TESEO	Technica Empirica Stima Errori Operatori
	1983	SLIM	Success Likelihood Index Method
	1984	HCR	Human Cognitive Reliability
	1985	HEART	Human Error Assessment and Reduction Technique
	1986	SHERPA	Systematic Human Error Reduction and Prediction Approach
2ème génération	1996	ATHEANA	A technique for Human Event Analysis
	1998	CREAM	Cognitive Reliability & Error Analysis Method
	1998	MERMOS	Méthode d'Évaluation de la Réalisation des Missions Opérateur pour la Sûreté
	1998	ACIH	Analyse des Conséquences de l'Infiabilité Humaine
3ème génération	1998	TRIPOD	Méthode de Sécurité Organisationnelle
	2004	FRAM	Functional Resonance Analysis Method (Méthode de sécurité Résilience)

La Figure 3 présente un couplage entre le chronogramme des méthodes d'évaluation de la fiabilité humaine retenues et l'évolution des approches du management de la sécurité [35], [21].

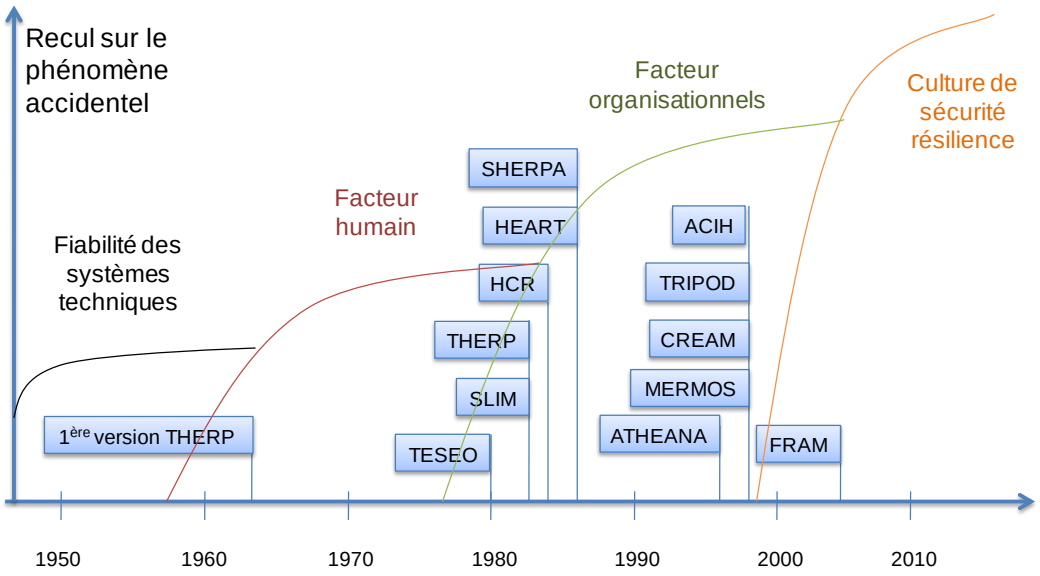


Figure 3 : Chronogramme des méthodes d'évaluation de la fiabilité humaine retenues pour une évaluation approfondie

Ces méthodes font l'objet d'une présentation synthétique et d'une inter-comparaison dans ce rapport. Elles font ensuite l'objet d'une description détaillée et illustrée en annexes.

5.2 PRÉSENTATION SYNTHÉTIQUE DE CHACUNE DES MÉTHODES

Le Tableau 3 présente de façon synthétique une description des méthodes d'évaluation de la fiabilité humaine étudiées dans ce rapport. Chaque méthode est illustrée par un schéma synthétique générique donné dans la Figure 4 ci-dessous.

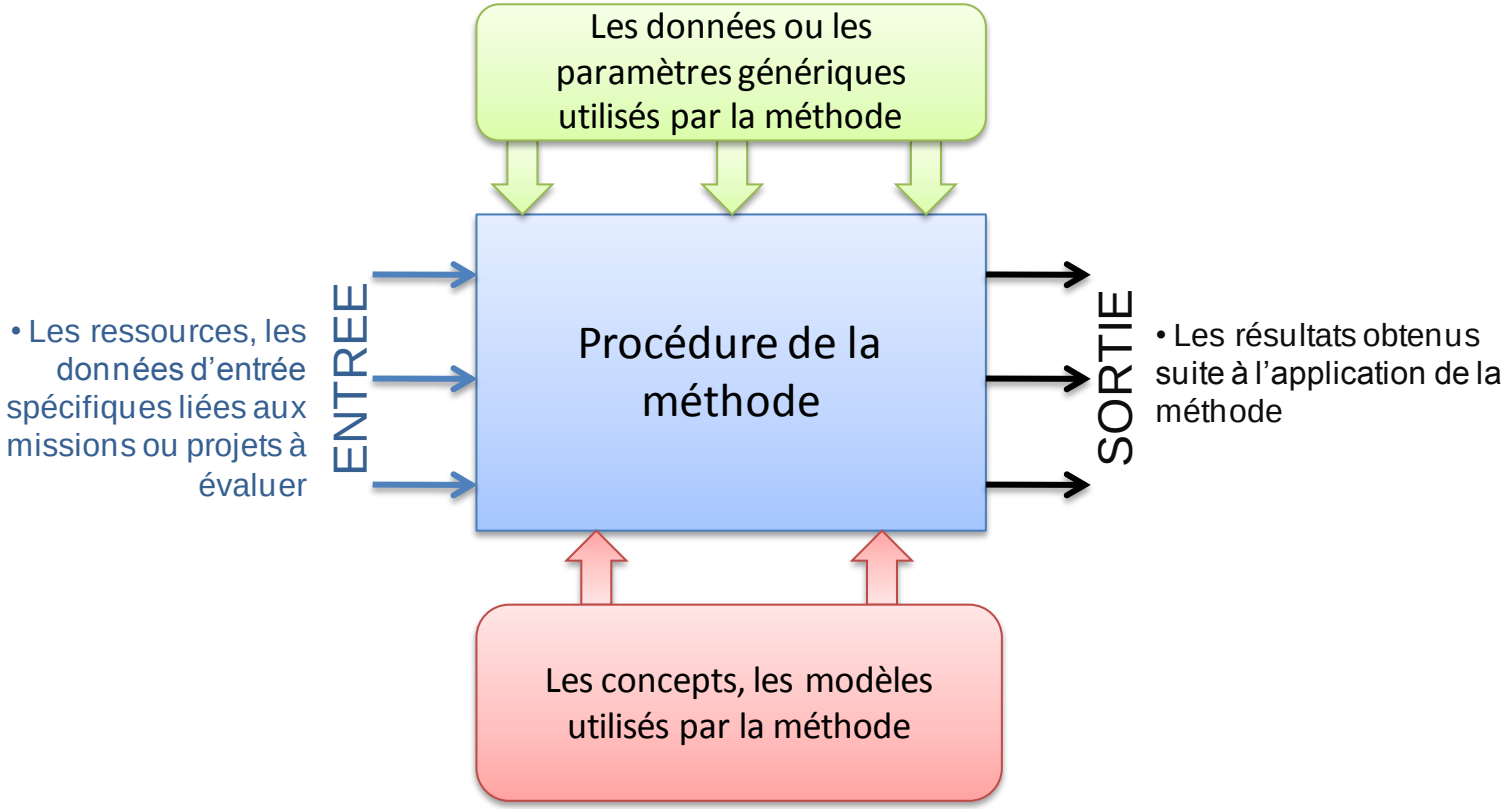
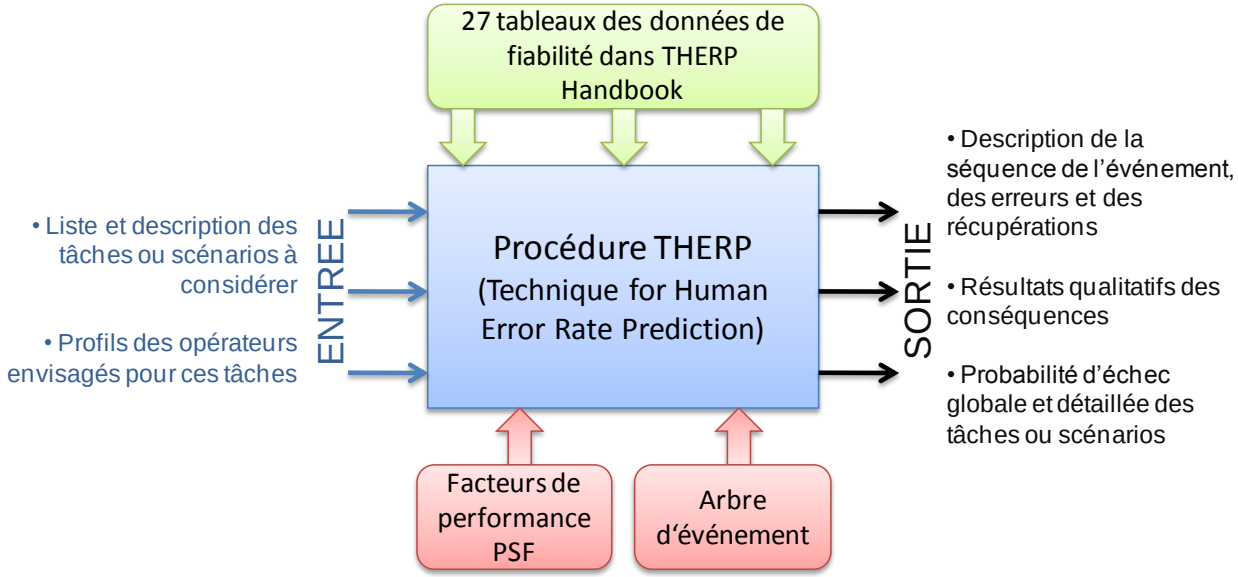
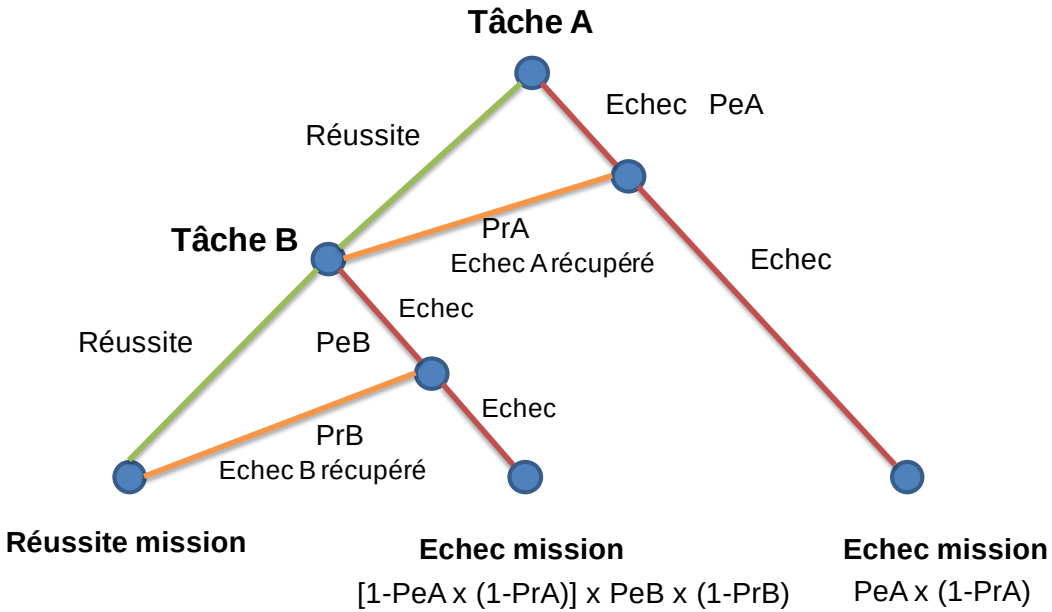
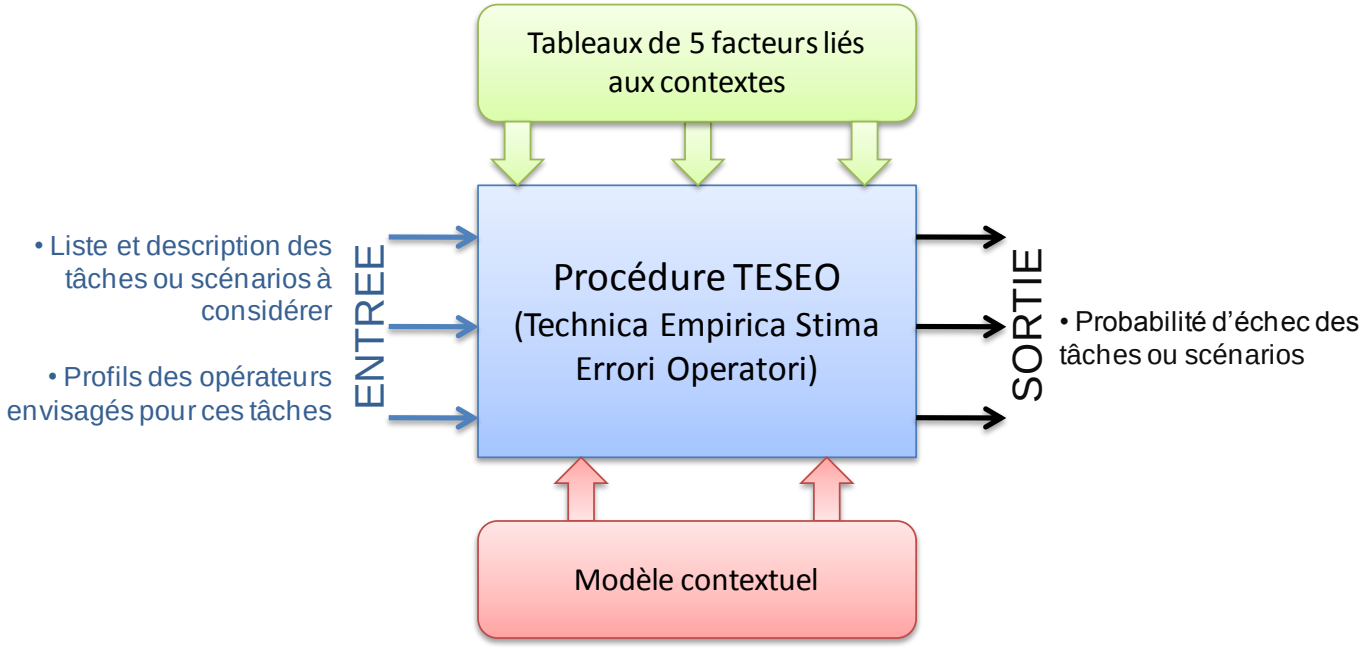


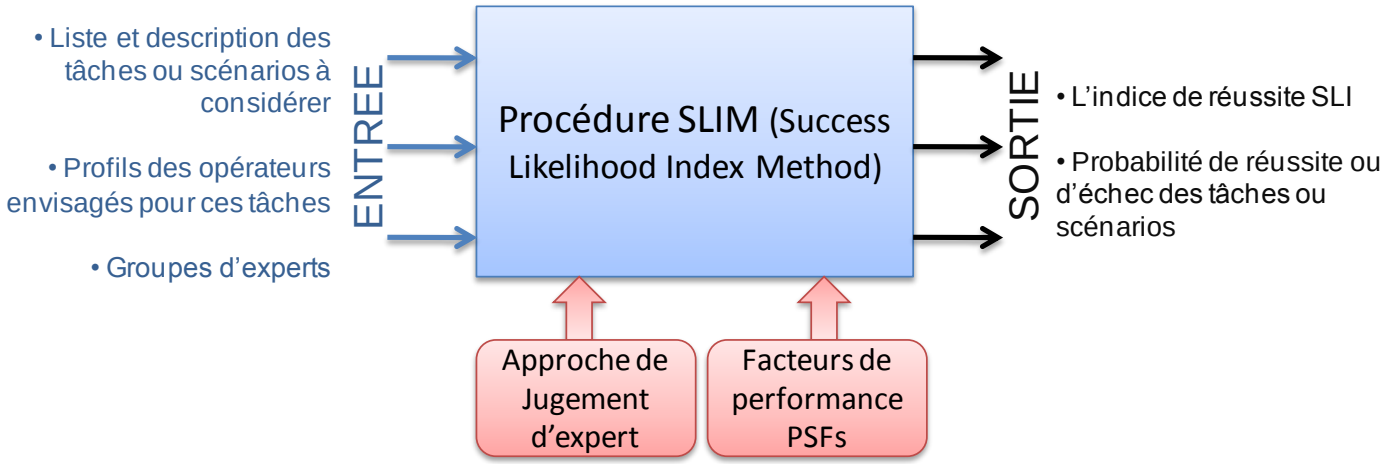
Figure 4 : Schéma synthétique des méthodes d'évaluation de la fiabilité humaine

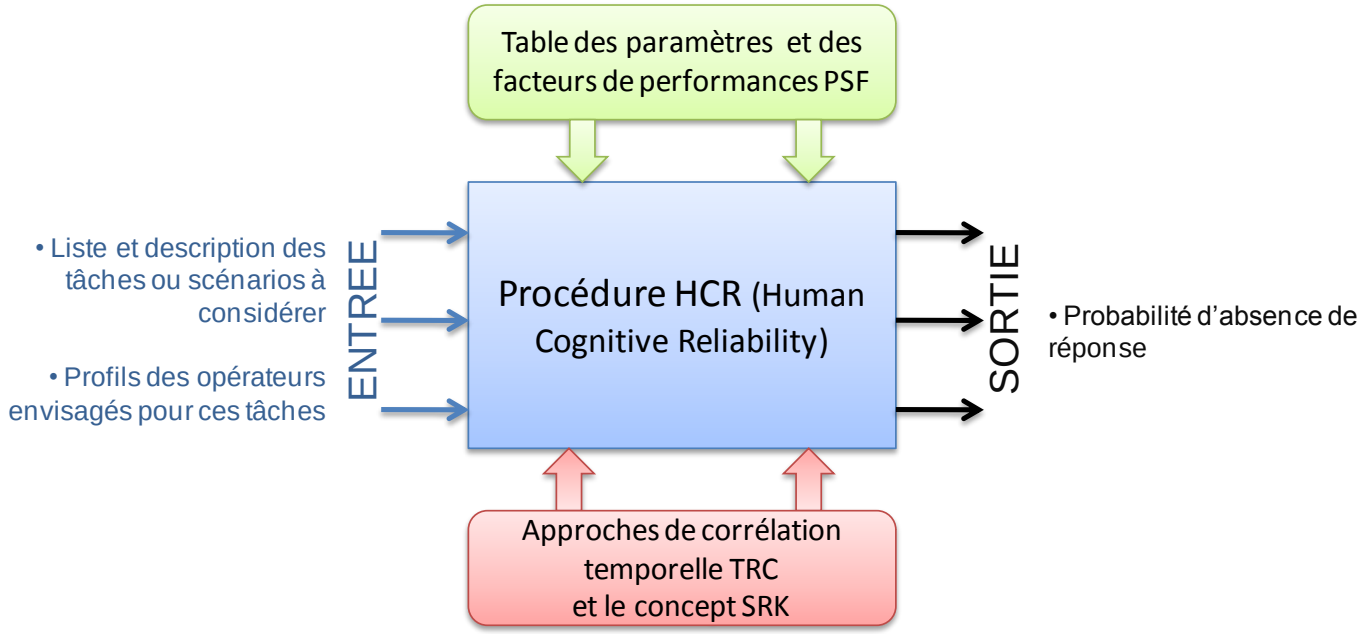
Tableau 3: Synthèse des méthodes d'évaluation de la fiabilité humaine retenues

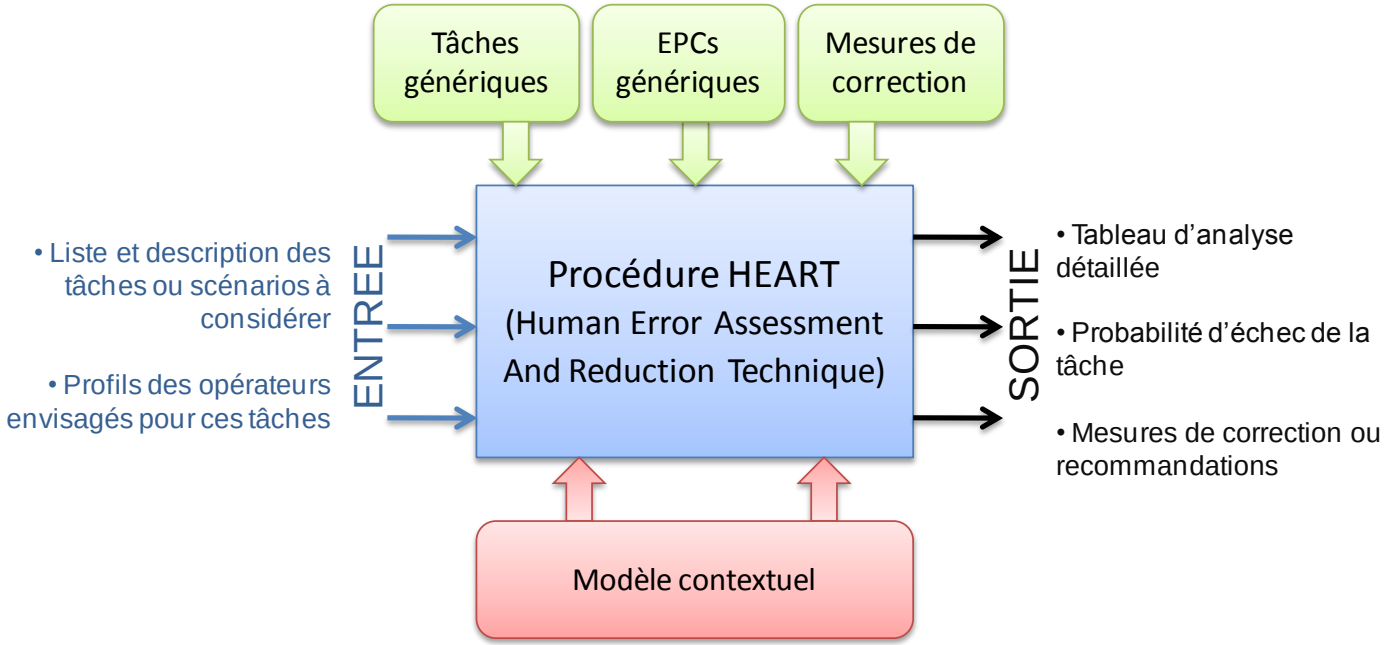
Méthode	Date et auteurs	Description	Domaine d'applicabilité
THERP	1960s (1983) par Swain	THERP [88] est une méthode structurée d'identification et de quantification des erreurs humaines basée sur une méthode de décomposition des tâches, sur un arbre d'événement et une analyse contextuelle utilisant des facteurs de performance PSFs (par exemple la qualité d'information, le stress, niveau d'expérience, la dépendance etc.). Les facteurs de performance PSFs permettent de prendre en compte les éléments contextuels dans l'évaluation de la probabilité d'échec à partir des probabilités nominales proposées pour les actions génériques, telles que diagnostic, préparation, contrôle administratif, sélection d'une valve, etc. Cependant, les données de fiabilité proposées sont basées principalement sur un retour d'expérience issu du domaine nucléaire. Afin de faciliter l'application de cette méthode dans d'autres domaines, il est préférable de constituer une base de données supplémentaire. Les possibilités de rattrapage sont aussi prises en compte lors de la réalisation de l'étude. THERP est une des méthodes les plus utilisées.  	Nucléaire

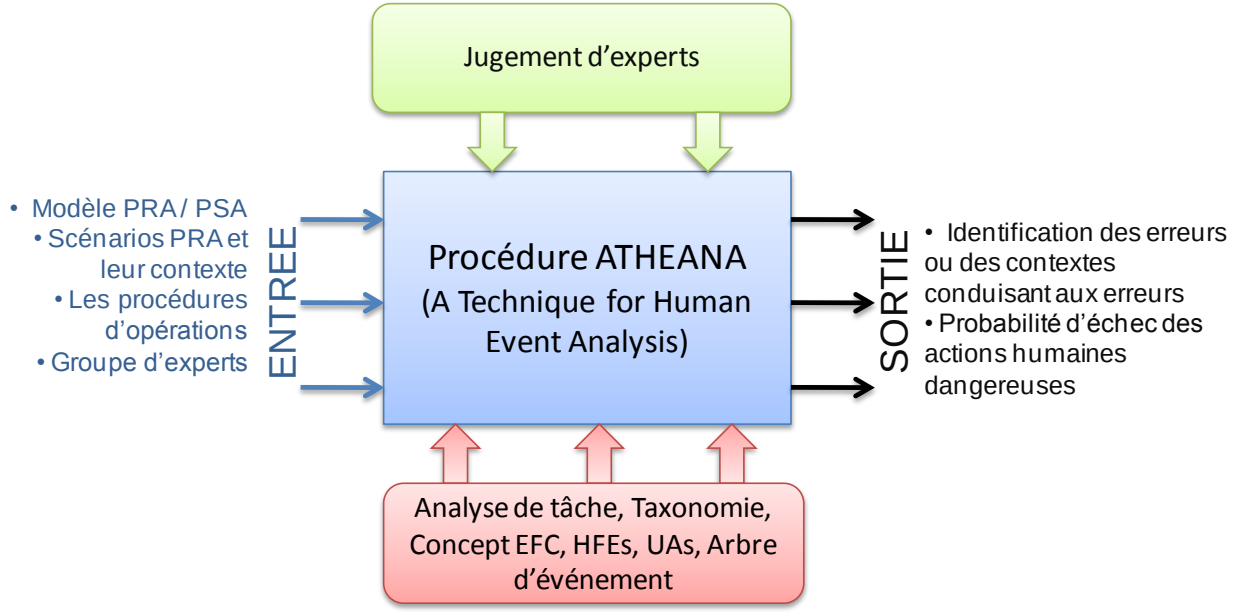
Méthode	Date et auteurs	Description	Domaine d'applicabilité
THERP (suite)		La méthode propose d'estimer la probabilité d'échec d'une mission à partir de l'estimation des probabilités d'échec des différentes tâches composant cette mission.  P(échec mission) = PeA x (1-PrA) +[1-PeA x (1-PrA)] x PeB x (1-PrB) Hypothèse: A et B indépendants	

TESEO	1980 par Bello et Colombari	TESEO est une méthode de quantification de la probabilité d'échec des missions humaines basée sur l'évaluation de cinq variables relatives aux caractéristiques de ces missions (par exemple K1 concerne la complexité de l'action, K2 est le facteur d'exigence temporelle [17]). Cependant, la description des tâches et contextes est très sommaire et limitée. Par ailleurs, la valeur de la probabilité estimée peut être supérieure à 100% pour plusieurs cas. Donc, TESEO n'est pas considérée comme une méthode rigoureuse. La méthode ne demande pas une décomposition détaillée des tâches, l'évaluation reste à un niveau très général. Cependant, la méthode est très simple à appliquer et elle demande peu de ressources. C'est une méthode générique et peut être appliquée pour une étude préliminaire.  $\text{Probabilité d'échec} = K1 \times K2 \times K3 \times K4 \times K5 = \prod_{i=1}^{N} K_i$	Tous domaines

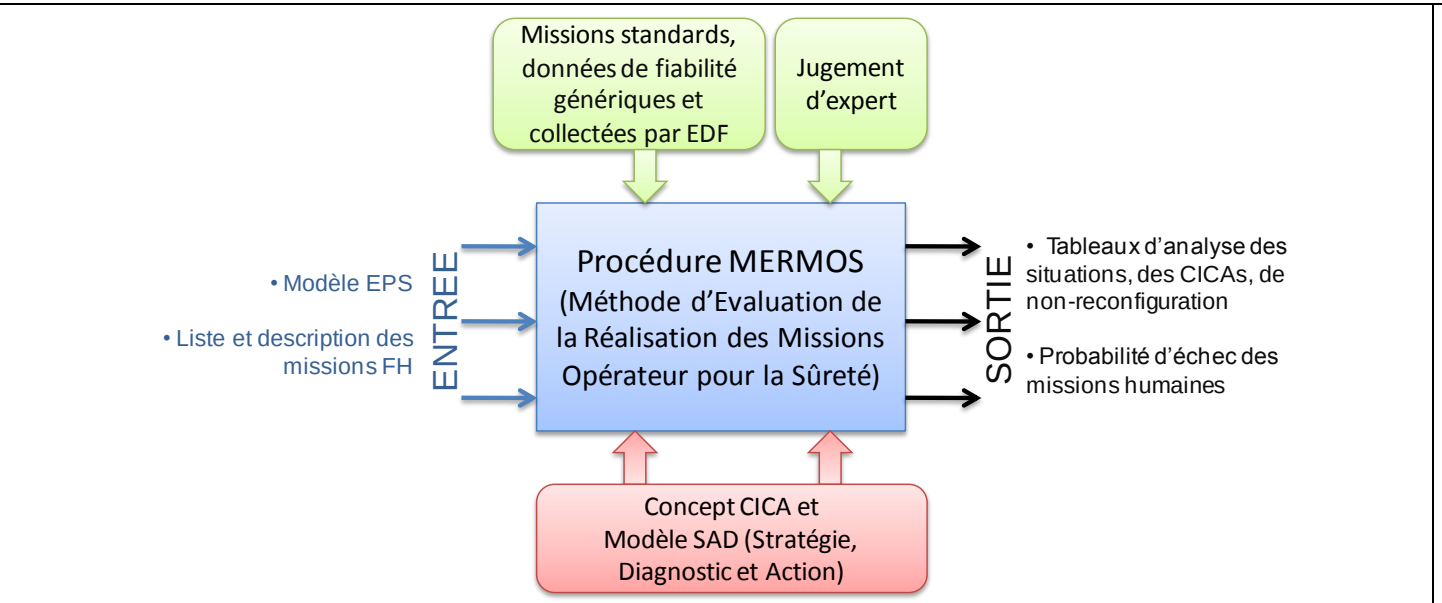
SLIM	1983 Par Embrey	SLIM [27] est une méthode de structuration de jugements d'expert basée sur une évaluation de facteurs de performance PSFs (Performance-Shaping Factors) qui incluent les caractéristiques de l'individu, de l'environnement et de la tâche. Cette évaluation se traduit par un indice de la probabilité de réussite SLI (Success Likelihood Index). L'application exige une ressource importante, car il faut faire appel à un groupe d'experts.  Log P (réussite) = a (SLI) + b a et b sont des constantes déterminées à partir d'au moins deux tâches ayant la probabilité de réussite bien connue.	Nucléaire

HCR	1984 Hannaman	HCR [40] est une méthode de quantification de la probabilité d'échec des erreurs humaines de type C (intervenant après l'événement initiateur) basée sur le modèle TRC (Time Reliability Correlation) [39], [104]. C'est une technique de fiabilité temporelle basée sur l'hypothèse que la performance humaine est fonction du temps disponible pour réaliser la tâche. Ce délai de réponse est lié aux différents types de comportements cognitifs SRK (Skill – Rule – Knowledge) de Rasmussen. La méthode exige des simulations pour déterminer le temps disponible et le temps de réponse de l'équipage nominal. Cependant, il est possible d'utiliser les jugements d'expert si nécessaire. Cette méthode est utilisée seulement lorsque la contrainte de temps est forte.  	Nucléaire

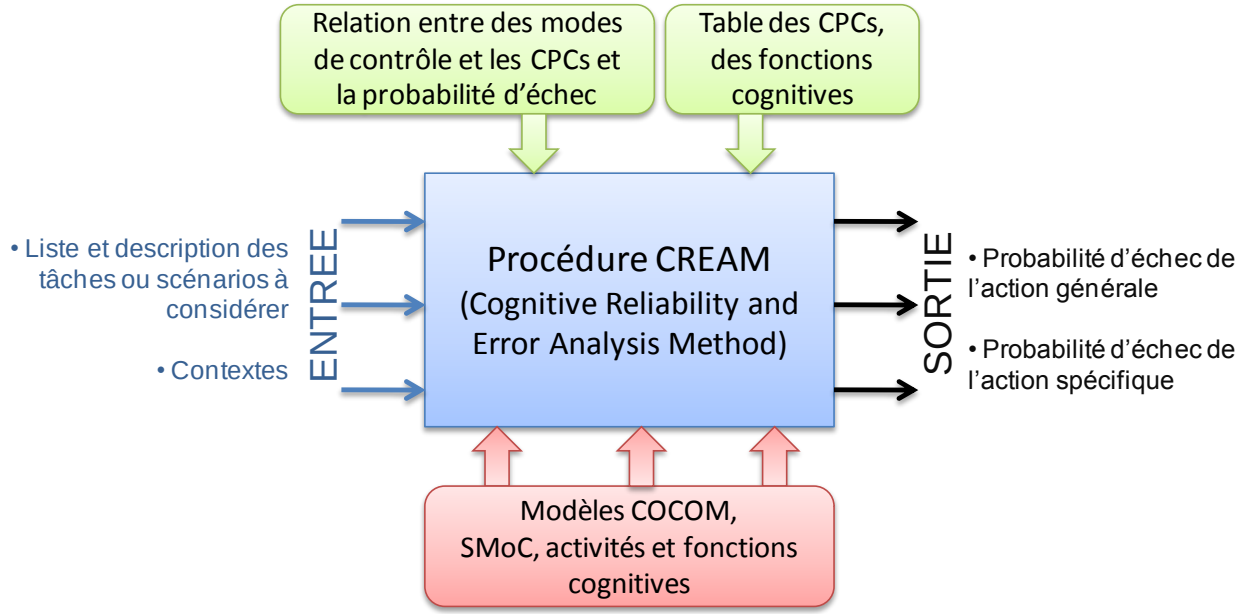
HEART	1985 Par Williams	HEART [102] est une technique d'identification et de quantification des erreurs humaines basée sur une description analytique des tâches. Elle fournit la probabilité d'erreur humaine nominale pour certaines tâches génériques. Cette probabilité est ensuite affinée en fonction du contexte de la tâche et du profil de l'opérateur, caractérisé par les conditions EPCs (Error Producing Conditions). Un coefficient de pondération des ECPC (W_k) est déterminé. HEART est basée sur un modèle générique de tâche et sur des probabilités des erreurs humaines fixées par la méthode.  $P_{échec_tâche} = P_{échec_tâche_nominale} \times \prod_{k=1}^{N} [(EPC_k - 1) \times W_k + 1]$	Tous domaines

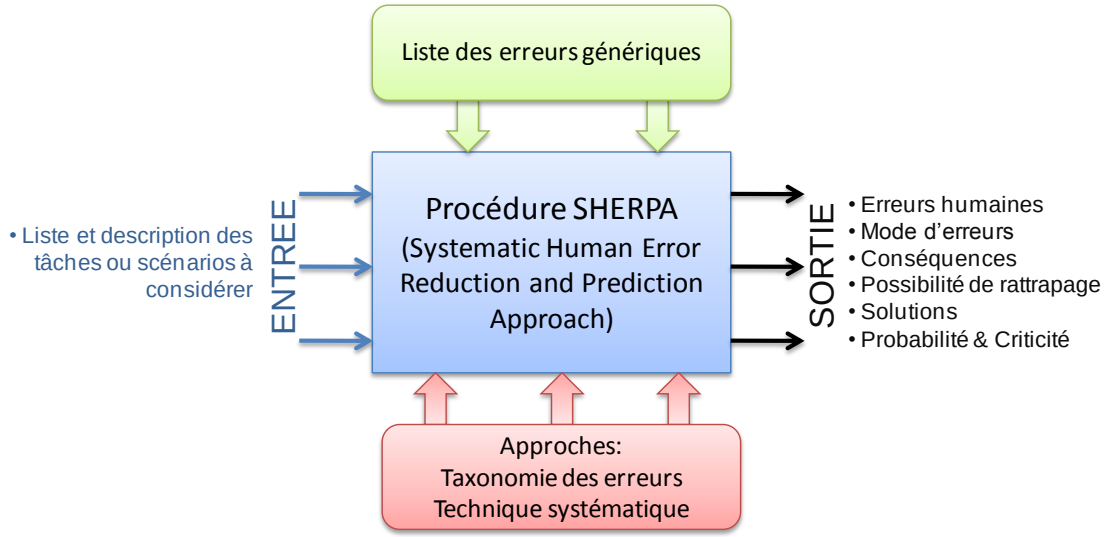
ATHEANA	1996 Par Cooper	ATHEANA est un guide méthodologique d'intégration des facteurs humains dans une analyse globale des risques de type PSA et PRA pour les centrales nucléaires. Elle a été développée par Cooper pour la commission de normalisation nucléaire américaine NRC. Elle fournit un guide pour identifier, quantifier et intégrer les erreurs humaines dans la structure globale des études PRAs. La probabilité d'échec des tâches élémentaires peut être estimée par le jugement d'expert si la donnée n'est pas disponible. La méthode intègre non seulement les erreurs par omission mais aussi les erreurs de réalisation. La méthode prend en compte les aspects contextuels caractérisés par les facteurs de performance PSFs et les conditions des installations. Ces deux éléments constituent les contextes susceptibles d'induire des erreurs ou EFC (Error Forcing Context). Bien que cette méthode ait été conçue pour le domaine nucléaire, elle est assez générique et peut être appliquée dans d'autres domaines. Le fondement et la formule de calcul de la méthode sont rigoureux et cohérents.  La probabilité de l'événement HFE dans le contexte d'un scénario PRA (S) peut être calculée selon	Nucléaire

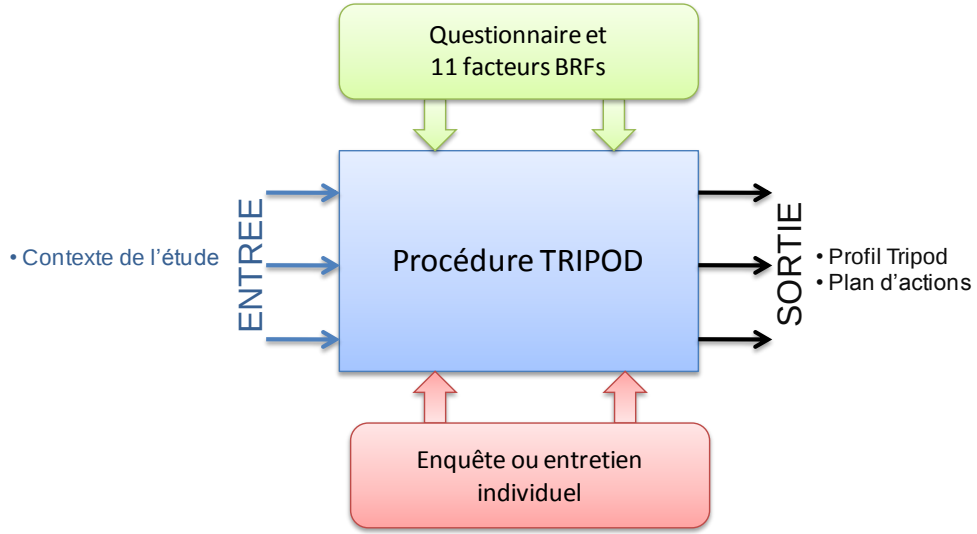
ATHEANA (suite)		la formule suivante : $$P(HFE|S) = \sum_j \sum_{i(j)} P(EFC_i|S) \times P(UA_j|EFC_i, S)$$ Les probabilités conditionnelles $P(EFC_i|S)$ et $P(UA_j|EFC_i, S)$ sont estimées dans de nombreux cas par les jugements d'experts.	
MERMOS	1998 par le Bot	MERMOS est une méthode développée par EDF. Elle est utilisée dans les études de sûreté EPS. MERMOS est basée sur un ensemble de concepts, tels que la mission FH « facteur humain », le concept CICA (Configuration Importante de la Conduite Accidentelle), les fonctions SAD (Stratégie – Action – Diagnostic). La CICA réfère à des situations particulières du système prenant en compte les équipements, les facteurs humains et les aspects organisationnels. MERMOS focalise sur les aspects collectifs. Elle suppose que l'erreur individuelle peut être évitée ou rattrapée au niveau collectif. La probabilité d'échec d'une mission HF est dépendante des scénarios identifiables et non-identifiables. La quantification est basée sur le recueil des données utilisant un simulateur et surtout sur les jugements d'expert.	Nucléaire



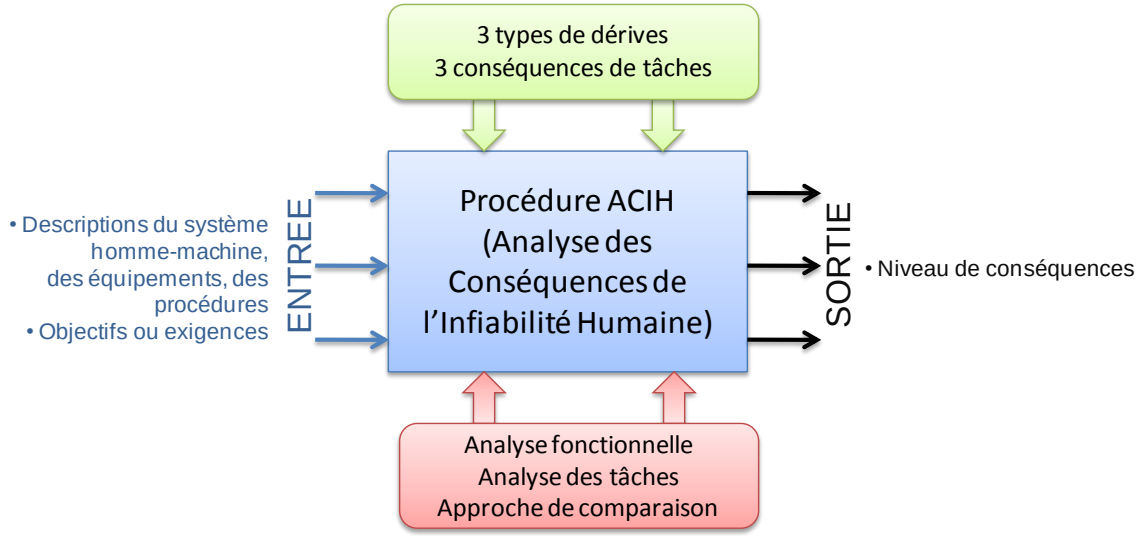
$$P(\text{échec_d'un_scénario}) = \prod_{j=1}^{m} P(\text{élément_contextuel}_j \mid \text{initiateur}) \times \prod_{k=1}^{n} P(CICA_k \mid \text{élément_contextuel}_j) \times P(\text{non_reconfiguration})$$

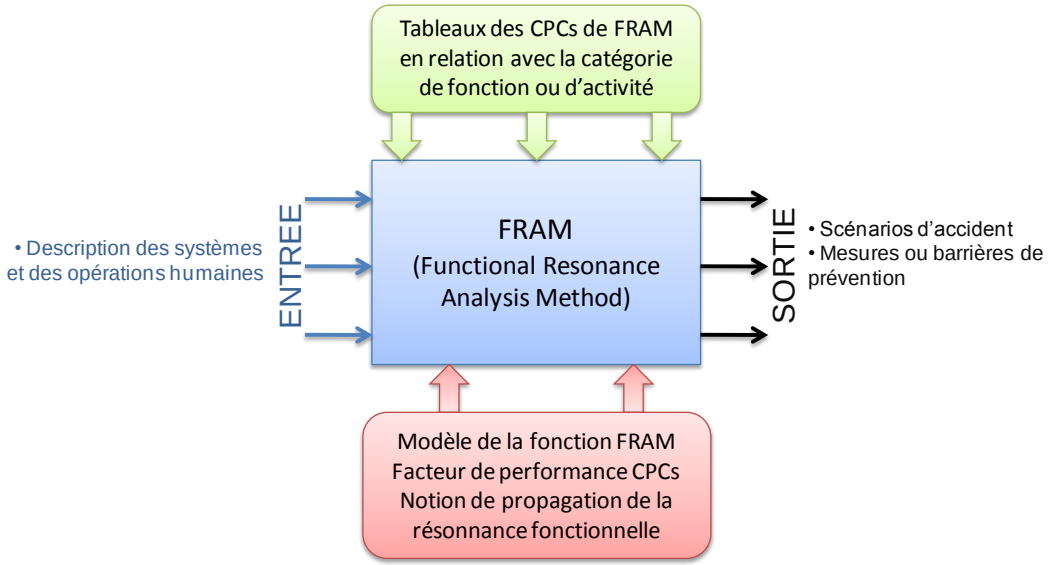
CREAM	1998 Par Hollnagel	CREAM est une méthode développée par Hollnagel en 1998 pour identifier, analyser et quantifier les erreurs cognitives. Elle est basée sur l'hypothèse que l'opérateur ajuste son niveau contrôle des situations en fonction de conditions de performances communes CPCs qui caractérisent la nature et l'environnement des tâches. Une fois que le niveau de contrôle est déterminé, la probabilité d'échec de la mission peut être estimée. La procédure d'application de CREAM comporte deux modules, « méthode basique » et « méthode étendue ». La méthode étendue exige d'analyser les activités cognitives des tâches et les défaillances des fonctions cognitives. Cette méthode permet de déterminer le profil d'exigences cognitives, le profil de défaillances des fonctions cognitives et la probabilité d'échec pour chaque étape de la mission. La probabilité de la mission globale est la valeur maximum des probabilités d'échec des étapes élémentaires.  	Tous domaines

SHERPA	1986 par Embrey	Méthode SHERPA basée sur une taxonomie des erreurs humaines a été développée par Embrey en 1986 [30]. C'est une technique structurée d'identification des erreurs humaines pouvant survenir lors de l'exécution des tâches. Elle a aussi pour but d'identifier des solutions potentielles pour prévenir les erreurs et limiter leurs effets. Elle a été créée initialement pour l'industrie de procédé, cependant elle peut être utilisée dans tous les domaines, grâce à son caractère générique. La méthode SHERPA est considérée comme la meilleure méthode d'identification des erreurs humaines par des experts ([58], [85]). Elle est comparable avec d'autres méthodes d'identification et d'évaluation qualitative des risques, telles que l'AMDEC, HAZOP, HAZID.  Néanmoins, SHERPA comporte certains points faibles, par exemple : la taxonomie est incomplète ; l'analyse de criticité est déficiente. D'autre part, partant d'une description et décomposition de tâches, elle ne s'appuie pas sur la réalité de l'activité de l'opérateur, et ne prend pas en compte le travail dans son contexte opérationnel (multi-activité, pression temporelle, contraintes organisationnelles, travail en équipe, dépendance avec d'autres tâches…).	Tous domaines

TRIPOD	1998 par Groeneweg et al.	La méthode Tripod [34], [35] est basée sur un modèle de sécurité organisationnelle ou un modèle de l'accident sous-jacent où l'organisation joue un rôle important (offrant les conditions de l'accident). Elle s'intéresse particulièrement aux facteurs organisationnels et aux erreurs latentes (actions erronées ayant des conséquences différées par rapport au moment d'occurrence l'accident – typique des actions de maintenance). Les erreurs de l'opérateur sont toujours des sources directes de risque, mais c'est l'organisation qui est considérée comme l'élément fondamental de sa performance. Les erreurs humaines et leurs conséquences apparaissent comme les résultats d'un environnement organisationnel défaillant. Les erreurs commises par les opérateurs s'inscrivent dans des conditions ou des contextes provenant de mauvaises décisions d'autres acteurs tels que des managers, cadres, ingénieurs, etc. Afin de traiter à la source des problèmes, il faut donc identifier des facteurs organisationnels favorisant l'erreur de l'opérateur, comme les conditions de travail, la formation, l'équipement technique, les modes de coopération et de coordination, etc.  Tripod regroupe les défaillances latentes initiatrices de séquences accidentelles en onze facteurs	Tous domaines

TRIPOD		types de risques, appelés « Basic Risk Factors » (BRF) [35]. Selon Tripod, ces facteurs BRFs peuvent contribuer à générer des actes dangereux et des perturbations opérationnelles et affaiblir les barrières de défense. L'objectif de la maitrise des risques est alors de diminuer voire d'éliminer les différents impacts de ces onze BRFs. Il existe deux outils méthodologiques de Tripod : - L'outil Tripod Beta pour chercher a posteriori les causes organisationnelles d'un accident, et - L'outil Tripod Delta pour identifier les défaillances organisationnelles d'un système industriel afin d'anticiper la survenue d'accidents. La procédure Tripod a pour but de caractériser l'environnement de travail par des indicateurs des onze facteurs BRFs. Ces indicateurs peuvent être obtenus via une enquête ou un entretien individuel anonyme réalisé sur l'ensemble des membres de l'organisation (y compris la direction et les sous-traitants ou les intérimaires). Cette enquête Tripod s'appuie sur une liste de questionnaires préétablis. Cependant, peu d'informations sont disponibles sur la liste des questions. Cela rend la méthode plus obscure et surtout très difficile à mettre en œuvre sans la mobilisation d'une expertise particulière pour la conception des questionnaires. De plus, même avec une liste indicative de départ, l'adaptation à l'entreprise et métiers visés exige des ressources importantes. La méthode Tripod est plutôt une méthode de sondage sur l'environnement de travail qu'une méthode d'évaluation de la fiabilité humaine. La méthode traite de façon générale de l'environnement organisationnel de travail. Elle peut donc être utile pour le management global de l'entreprise. Cependant comme elle ne se focalise pas sur les actions a priori identifiées comme dangereuses, elle ne permet pas d'entrer dans le détail d'un scénario d'accident. La méthode n'est pas adaptée pour être intégrée dans les études probabilistes de sûreté et de risque.	

ACIH	1998 par Vanderha-egen	La méthode ACIH (Analyse des Conséquences de l'Infiabilité Humaine) développée à la fin des années 90 par F. Vanderhaegen [96], [97] est une démarche d'analyse de l'erreur humaine sur une situation de travail donnée en se focalisant particulièrement sur les conséquences de l'erreur [98]. La méthode ACIH existe en deux versions, la méthode APRECIH (analyse préliminaire des conséquences de l'infiabilité) et la méthode APOSCIH (analyse a posteriori des conséquences de l'infiabilité). Cependant, elles ne prennent pas en compte la fréquence d'occurrence des erreurs humaines. ACIH propose un modèle de gestion des situations pour distinguer celles-ci par rapport à des dérives comportementales et des dérives situationnelles. L'analyse des conséquences est ensuite réalisée sur les dérives comportementales identifiées, en termes de bénéfice, de coût, de dégradation ou d'amélioration en comparant une situation cible à une situation source. La propagation intra-individuelle d'une erreur se réalise de différentes manières selon les trois niveaux d'occurrence d'erreur : l'acquisition, le traitement de l'information, ou l'action.  	Tous domaines

FRAM	2004	La méthode FRAM a été développée par Hollnagel en 2004 [45]. Elle permet de décrire le système sociotechnique par ses fonctions et ses activités plutôt que par sa structure. Hollnagel utilise la métaphore de l'émergence et de la résonnance pour expliquer l'apparition des accidents dans les systèmes sociotechnique complexes. Il justifie ce rapprochement vers l'étude de sécurité en s'appuyant sur la variabilité de performance des fonctions ou des activités dans les systèmes sociotechniques. La méthode FRAM est basée sur quatre principes basiques de l'équivalence de succès et d'échec, d'ajustement approximatif de l'émergence et de la résonnance fonctionnelle. La variabilité de performances humaines et organisationnelles vient de leur capacité à s'adapter aux conditions de travail et à l'absence de régularité dans les activités (perception, cognition, action, communication). La variabilité des performances, dû à ces ajustements approximatifs, est donc l'origine du succès, mais aussi à l'origine de l'échec. L'objectif de l'ingénierie résilience est de renforcer cette capacité d'ajustement, plutôt que d'éviter ou éliminer les défaillances. 	Tous domaines

5.3 SYNTHÈSE

Afin de fournir une vue globale des 12 méthodes décrites précédemment, le Tableau 4 en propose une analyse selon 13 critères :

1. **Type de méthode** : fondement, utilisé ou type d'approche de la méthode.
2. **Application** : domaines ou secteurs d'application de la méthode.
3. **Identification des erreurs humaines** : possibilités offertes par la méthode pour identifier les erreurs humaines.
4. **Évaluation des effets des erreurs** : possibilités offertes par la méthode pour évaluer les effets des erreurs humaines.
5. **Popularité ou acceptabilité** : ce critère a été apprécié à partir des éléments de validation et commentaires formulés dans la littérature et à partir du nombre de publications.
6. **Facilité d'utilisation** : complexité et exigence de la méthode en termes d'application.
7. **Maturité** : niveau de développement de la méthode.
8. **Précision** : niveau de précision des probabilités estimées par la méthode.
9. **Cohérence** : cohérence de la démarche avec la formule de calcul des probabilités.
10. **Ressource** : niveau d'exigence en terme de ressources (ex : compétences, temps de réalisation, équipements de simulation ou logiciels, etc.).
11. **Base de données** : origine des données de fiabilité utilisées pour évaluer la probabilité d'une tâche ou d'une mission. Ces données peuvent être :
    - Interne, si la méthode possède des probabilités nominales pour les tâches génériques ou l'utilisation de la méthode n'exige pas d'autres données de fiabilité supplémentaires.
    - Externe, si la méthode accepte l'utilisation des données de fiabilité qui ne sont pas fournies par la méthode.

    Note : On remarque que le jugement d'expert est utilisé dans toutes les méthodes quelle que soit la source des données de fiabilité, externe ou interne.
12. **Temps de réalisation** : ce paramètre est normalisé pour un analyste et pour une mission facteur humain (devant être considérée comme un ensemble de tâches humaines plus ou moins complexes). Par exemple, si le temps de réalisation donné dans le tableau est de 12 jours, c'est-à-dire un analyste travaille seul pendant 12 jours ou quatre analystes travaillent pendant 3 jours. Cette évaluation est corrélée aux valeurs de références fournies par Kirwan [56].
13. **Typologies contenues dans la méthode** : cet élément fournit la typologie, la taxonomie ou une liste des mots clés utilisés dans la méthode.

Tableau 4: Synthèse d'évaluation des méthodes d'évaluation probabiliste de la fiabilité humaine significatives

Classification par génération	**1ère génération**						**2è génération**				**3è génération et autre**	
Méthodes	**THERP**	**TESEO**	**HEART**	**SLIM**	**HRC**	**SHERPA**	**ATHEANA**	**MERMOS**	**CREAM**	**ACIH**	**TRIPOD**	**FRAM**
Type de méthode	Modèle générique basé sur la décomposition	Modèle générique contextuel	Modèle générique contextuel	Traitement de jugement expert	Technique de fiabilité temporelle ; actions post-initiateurs (type C)	Technique d'identification systémique d'erreurs et leurs conséquences	Démarche ad' hoc basée sur les scénarios d'accident	Démarche ad 'hoc basée sur les scénarios d'accident	Modèle générique basé sur la modélisation cognitive	Démarche d'analyse des conséquences de l'infiabilité humaine	Modèle de sécurité organisa-tionnelle	Modèle générique basé sur la modélisation cognitive
Application	Nucléaire, mais extensible dans d'autres secteurs	Pétrochimique, mais extensible dans d'autres secteurs	Nucléaire, mais extensible dans d'autres secteurs	Générique	Nucléaire, mais extensible dans d'autres secteurs	Générique	Nucléaire, mais extensible dans d'autres secteurs	Nucléaire, mais extensible dans d'autres secteurs	Générique	Générique	Générique	Générique
Identification des erreurs humaines	++++	+	+++	+	+	++++	+ +	++	+++	++	+	+++
Évaluation des effets des erreurs	+++	+	++	+	+	+++	+++	+++	+	++	+	++
Popularité ou acceptabilité	++++	+++	++++	+++	+++	++++	+++	++	++	+	++	+++
Facilité d'utilisation	+++	++++	++++	+++	+++	++++	+++	+++	+	++	+++	++
Maturité	++++	+++	++++	++++	+++	+++	+++	+++	++++	++++	+++	+++
Précision	+++	+	+++	++	++	++++	+++	+++	+++	++	+++	++
Cohérence	++++	++	+++	++++	+++	+++	++++	+++	+++	+++	+++	+++
Ressources	++	+	+++	+++	++	+++	+	+	++	++	+++	++
Base de	Interne	Interne	Interne	Interne	Interne et	Interne et	Interne	Interne	Interne	Interne et	Interne	Interne

Classification par génération	1ère génération						2è génération				3è génération et autre	
Méthodes	**THERP**	**TESEO**	**HEART**	**SLIM**	**HRC**	**SHERPA**	**ATHEANA**	**MERMOS**	**CREAM**	**ACIH**	**TRIPOD**	**FRAM**
données					externe	externe				externe		
Temps de réalisation	8-30 jours	1 jour	3-5 jours	20 jours	5-10 jours	2 jours	10 – 30 jours	10 – 30 jours	10 – 15 jours	5 – 10 jours	10 – 30 jours	5 – 10 jours
Typologies contenues dans la méthode	Types d'erreurs	Contexte	Types de tâches ; conditions EPC	Facteurs de performance	Facteurs de performance	Taxonomie d'erreurs	Types d'action ; types d'erreurs ; contexte ; what if	Pas de taxonomie particulière	Conditions de performance CPC, les activités et fonctions cognitives, les modes de contrôle	Taxonomie d'erreurs et de conséquence	Facteurs types de risques	Conditions de performance CPC

Signification :

+	Médiocre / bas / peu exigeante en ressources
++	Moyen / exigence moyenne en ressources
+++	Bien / élevé / assez exigeante en ressources
++++	Très bien / très élevé / très exigeante en ressources

6. CONCLUSIONS

On observe une quantité très importante des méthodes d'évaluation de la fiabilité humaine, basées sur différentes approches, telles que la décomposition des missions facteur humain (THERP, ATHEANA, CREAM,..), l'évaluation globale ou collective de ces missions (TESEO, SLIM, MERMOS, HEART), leur modélisation cognitive (CREAM, MERMOS,…), l'analyse temporelle (TRC, HCR), la modélisation des facteurs contextuels (THERP, HEART, ATHEANA, MERMOS), l'utilisation de jugements d'experts (SLIM, MERMOS, ATHEANA, ACIH).

L'étude de l'évolution de ces méthodes montre que la part nécessaire de jugement et d'expertise pour procéder à l'évaluation de la fiabilité humaine est de plus en plus importante. Cette caractéristique limite les possibilités d'inter-comparaison des méthodes. Ces méthodes tendent aussi à se complexifier, soit par une analyse de plus en plus précise des composantes cognitives des tâches (ex : CREAM) soit par une identification de plus en plus exhaustive des scénarios d'échec des missions « facteur humain » (ex : MERMOS). L'application de ces différentes méthodes à partir d'une même situation (redémarrage d'un four, cf. annexe 14) confirme qu'il existe des différences importantes en termes de complexité de mise en œuvre, cette complexité dépendant en particulier de l'adéquation entre les exigences des méthodes[2] et les outils proposés pour satisfaire ces exigences.

D'une manière générale, peu d'éléments de retour d'expérience sont disponibles pour apprécier la validité de ces méthodes. De plus, il est essentiellement issu des secteurs nucléaires, aéronautiques et de la défense. Des travaux de recherches sont actuellement menés dans le secteur du nucléaire à partir d'un simulateur pour évaluer les capacités prédictives de ces méthodes. Dans ce contexte, la validité de ces méthodes dans le secteur des installations classées ne peut pas être considérée comme un critère discriminant. Le choix d'une méthode dépend avant tout du projet de l'analyste et du type d'efficacité recherché (mieux connaître les risques liés à la fiabilité humaine, démontrer la robustesse d'une architecture de sécurité en place…). Enfin, la profondeur d'analyse d'une évaluation probabiliste de la fiabilité humaine et le niveau de ressource nécessaire dépend du niveau de précision des résultats visés et du niveau de justification recherché.

Néanmoins, à partir de l'étude comparative réalisée, trois méthodes semblent se distinguer du point de vue de leur applicabilité dans le contexte des installations classées. Il s'agit des méthodes THERP, HEART et SHERPA. Cette sélection tient compte des critères suivants : popularité, facilité d'utilisation, maturité, précision, cohérence et ressources. Les méthodes les moins applicables sont celles appartenant aux deuxième et troisième génération, principalement pour des raisons liées au niveau important de ressources à mobiliser, aux difficultés que peut présenter leur utilisation et à leur plus faible popularité (ces méthodes étant également les plus récentes).

[2] Par exemple : le niveau d'identification des erreurs humaines exigé, le nombre de facteurs de performance à considérer, le niveau d'appréciation des dépendances entre ces facteurs requis, la finesse d'analyse des tâches demandée, etc.

7. RÉFÉRENCES

7.1 RÉFÉRENCES RÉGLEMENTAIRES

[1] Assemblée Nationale – Constitution du 4 octobre 1958 – Onzième législature -Rapport fait au nom de la Commission d'Enquête sur la sûreté des installations industrielles et des centres de recherche et sur la protection des personnes et de l'environnement en cas d'accident industriel majeur, 2002.

[2] F. Loos et J.Y. Le Déaut

[3] Council Directive 96/82/EC on the control of major-accident hazards involving dangerous substances, 9 December 1996.

[4] LOI n° 2003-699 du 30 juillet 2003 relative à la prévention des risques technologiques et naturels et à la réparation des dommages.

[5] Comité de Bâle sur contrôle bancaire, Convergence internationale de la mesure et des normes de fonds propres, Banque des règlements internationaux, Juin 2004, p. 121.

[6] NF EN IEC 61511-3 : Sécurité fonctionnelle - Systèmes instrumentés de sécurité pour le secteur des industries de transformation. Partie 3: Conseils pour la détermination des niveaux d'intégrité de sécurité requis.

[7] NF EN IEC 61508-1 : Sécurité fonctionnelle des systèmes électriques/électroniques/électroniques programmables relatifs à la sécurité –Partie 1: Prescriptions générales.

7.2 RÉFÉRENCES TECHNIQUES

[8] AIChE (American Institute of Chemical Engineers), Guidelines for Chemical Process Quantitative Risk Analysis, CCPS, 2nd Ed., 2000.

[9] Amalberti.R. La conduite des systèmes à risques, le travail humain, Presses universitaires de France, 1996.

[10] Annett J. and Duncan K.D., Task Analysis and training design, Occupational Psychology, 41, 1967, p. 211-221.

[11] Annett J., Duncan K.D., Stammer R.B. and Gray M., Task Analysis (London: HMSO), 1971.

[12] Aven T., Hauge S., Sklet S. and Vinnem J.E., (2004), "Operational Risk Analysis – Total Analysis of Physical and Non-physical Barriers" Report 2004, Preventor, Stavanger, Norway.

[13] RIA – BARPI, Inventaire 2009 des accidents technologiques. http://www.aria.developpement-durable.gouv.fr/barpi_stats.gnc

[14] Baber C. & Stanton N. A., Human error identification techniques applied to public technology: predictions compared with observed use. Applied Ergonomics, 27(2), 1996, p. 119 – 131.

[15] Bell J., Holroyd J., Review of human reliability assessment methods, HSE Books, 2009.

[16] Bellamy L.J., Papazoglou I.A., Hale A.R., Aneziris O.N., Ale B.J., Morris M.I. and Oh J.I., (1999), “I-RISK Development of an Integrated Technical and Management Risk Control and Monitoring Methodology for Managing and Quantifying On-Site and Off-Site Risks”. Main Report, September 1999. Contract No. ENVA-CT96-0243.

[17] Bello G.C., Golombari V., The human factors in risk analysis of process plants : the control room model TESEO. 6th Advances in Reliability Technology Symposium, UKAEA-NCSR-R23, 1980

[18] Bello G.C., Golombari V., The human factors in risk analysis of process plants : the control room model TESEO. Reliability Engineering, 1, 1980

[19] Belmonte F., Schön W. et Boulanger J.L., Capel R., Évaluation du facteur humain dans le domaine de la supervision de trafic ferroviaire : le projet spica-rail, 16ème Congrès Lamda-Mu, Avignon, 2008.

[20] Bieder, C., Les facteurs humains dans la gestion des risques : évolution de la pensée et des outils, Hermes Science Publications, 2006.

[21] Cambon J., Guarnieri F., Maîtriser les défaillances des organisations en santé et sécurité au travail – La méthode Tripod, Ed. TEC & DOC Lavoisier, 2008, p. 21.

[22] Cambon J., Thèse : Vers une nouvelle méthodologie de mesure de la performance des systèmes de management de la santé-sécurité au travail, 2007.

[23] Cooper S.E., Ramey-Smith A.M., Wreathall J., Parry G.W., Bley D.C., Luckas W.J., Taylor J.H., Barriere M.T., A Technique for Human Error Analysis (ATHEANA). NUREG / CR-6350. Washingston, DC : US Nuclear Regulatory Commission ; 1996.

[24] Cooper S.E., Thompson C.M., Ramey-Smith A.M., Parry G.W., Wreathall J., Bley D.C., Luckas W.J., Taylor J.H., A Process for application of ATHEANA. BNL-NUREG-63257, 1996.

[25] CSNI WGRisk, HRA Data and Recommended actions to support the collection and exchange of HRA data, NEA/CSNI/R (2008)9.

[26] Davoudian K., Wu J.S. and Apostolakis G., (1994), "The Work Process Analysis Model (WPAM)”, Reliability Engineering and System Safety, Vol. 45, 1994, pp. 107-125.

[27] Embrey D.E., The Use of Performance Shaping Factors and Quantified Expert Judgment in the Evaluation of Human Reliability: An Initial Appraisal. NUREG/ CR-2986, Brookhaven National Laboratory, 1983.

[28] Embrey D.E. and Kirwan B. A comparative evaluation of three subjective human reliability quantification techniques. The Annual Ergonomics Society Conference Proceedings, Coombes, K. Taylor and Francis Ed., London, (1983).

[29] Embrey D.E., Humphreys P., Rosa E.A., Kirwan B., and Rea K., “SLIM-MAUD: An Approach to Assessing Human Error Probabilities Using Structured Expert Judgment,” NUREG/CR-3518, Vols. I & II, Brookhaven National Laboratory for the U.S. Nuclear Regulatory Commission, Washington DC, 1984.

[30] Embrey D. E., SHERPA : A Systematic Human Error Reduction and Prediction Approach, International Meeting on Advances in Nuclear Power Systems, Knoxville, Tennessee, 1986.

[31] Evans R.A., “Reliability Optimization,” p. 117 – 131 in E. J. Henley and J.W. Lynn (eds), Generic Techniques in Systems Reliability Assessment, Leyden, The Netherlands: Noordhoff International Publishing, 1976.

[32] Fadier E., Artigny B., Chollet M-G., Garoff-Mercier C., Poyet C., Drozdz-Verly C., L’état de l’art dans le domaine de la fiabilité humaine, OCTARES Ed., 1994.

[33] Ferrary M., Le facteur humain comme source de risque opérationnel dans le secteur bancaire. Dans Bouchet M.-H., le Fraper du Hellen A. G., Intelligence économique et gestion des risques, Pearson Education, 2007.

[34] Groeneweg J. Roggeveen V., 1998, Tripod: Controlling the human error components in accidents. Safety and Reliability, Lydersen, Hansen and Sandtorv ed., p. 809-816.

[35] Groeneweg, J. Controlling the controllable. Preventing business upsets, fifth edition. Global Safety Group Publication, 2002, p. 528.

[36] Forester J., Bley D., Cooper S., Lois E., Siu N., Kolaczkowski A., Wreathall J., Expert elicitation approach for performing ATHEANA quantification, Reliability Engineering and System Safety 83 (2004) 207-220

[37] Forester J., Kolaczkowski A., Lois E., Kelly D., Evaluation of human reliability analysis methods against good practices, NUREG-1842, 2006

[38] Forester J., Kolaczkowski A., Cooper S., Bley D., Lois E., ATHEANA User’s Guide, NUREG-1880, 2007

[39] Hall R.E., Fragola J.R., and Wreathall J. Post-Event Human Decision Errors : Operator Action Tree / Time Reliability Correlation, NUREG/CR-2010, US Nuclear Regulatory Commission, BNL-NUREG-51601, Brookhaven National Laboratory, 1982.

[40] Hannaman G.W., Spurgin A.J., and Lukic Y.D., Human Cognitive Reliability Model for PRA analysis, Electric Power research Institute, Palo Alto, Califonia, 1984.

[41] Hannaman G.W., Spurgin A.J., and Lukic Y.D., A model for assessing Human Cognitive Reliability in PRA Studies, in Processings of 1985 IEEE 3rd Conference on Human factors and Power plants, Monterey, California, 85CH22350, IEEE, New York, 1985.

[42] Hollnagel E. & Cacciabue P.C., Cognitive modelling in system simulation. Proceedings of Third European Conference on Cognitive Science Approaches to Process Control, Cardiff, September 2-6, 1991.

[43] Hollnagel E., Human reliability analysis : context and control, Academic Press, Londres, 1993.

[44] Hollnagel E., Cognitive Reliability and Error Analysis Method, Elsevier Science Ltd, Oxford, 1998.

[45] Hollnagel E., Barriers and Accident Prevention, Ashgate, 2004.

[46] Hollnagel E., Resilience Engineering and Safety Assessment, Eurocontrol Conference, 2008.

[47] Hollnagel, E., Pruchnicki, S., Woltjer, R. & Etcher, S. Analysis of Comair flight 5191 with the functional resonance accident model. In the 8th International Symposium of the Australian Aviation Psychology Association. Sydney, Australia, 2008.

[48] Humphreys P., Human reliability assessors guide, Safety and Reliability Directorate UKAEA (SRD) Report No TRS 88/95Q, 1988.

[49] Hone G. and Stanton N., HTA: The development and use of tools for Hierarchical Task Analysis in the Armed Forces and elsewhere, 2004.

[50] IAEA, Safety Assessment and Verification for Nuclear Power Plants, Safety Standards Series No. NS-G-1.2, 2001

[51] IAEA, Determining the quality of probabilistic safety assessment (PSA) for applications in nuclear power plants, IAEA-TECDOC-1511, 2006.

[52] INERIS, Omega 20 : Démarche d'évaluation des Barrières Humaines de Sécurité, 2009.

[53] IRSN – Direction de la sûreté des réacteurs, Analyse critique de la banque de données développée par la société ARKEMA relative aux probabilités de défaillance d'équipements, Rapport DSR/SESPRI n° 69.

[54] Kemeny J.G., Babbitt B., Haggerty P.E., Lewis C., Marks P.A., Marrett C.B., McBride L., McPherson H.C., Peterson R.W., Pigford T.H., Taylor T.B., Trunk A.D., Report of the President's Commission on the Accident at Three Mile Island, Washington D.C., October 1979.

[55] Kim J., Jung W., Jang S.-C. et Wang J.-B., A case study for the selection of a railway human reliability analysis method,

[56] Kirwan B., A Guide To Practical Human Reliability Assessment, London : Taylor and Françis, 1994.

[57] Kirwan B., The validation of three human reliability Quantification techniques – THERP, HEART and JHEDI : Part III – Practical aspects of the usage of the techniques, Applied Ergonomics, 28, 1, 1997.

[58] Kirwan B and Ainsworth L.K., A Guide to Task Analysis, London : Taylor and Françis, 1992.

[59] Kirwan B., Gibson H., Kennedy R., Edmunds J., Cooksley G. and Umbers I., Nuclear Action Reliability Assessment (NARA): a data-based HRA tool. *Proc. 7th Int. Conf. On Probabilistic Safety Assessment and Management*. (Spitzer C., Schmocker U., Dang V.N. Eds.), Berlin, 2004, Springer-Verlag.

[60] Kirwan B. and Gibson H., CARA: A Human Reliability Assessment Tool for Air Traffic Safety Management — Technical Basis and Preliminary

Architecture. Pp 197 –214 in The Safety of Systems Proceedings of the 15th Safety-critical Systems Symposium, Bristol, UK, 13–15 February 2007.

[61] Kletz T.A., An engineer's view of human error. The institution of chemical engineers, 1985.

[62] Le Bot P., Desmares E., Bieder C., Cara F., Bonnet J.-L., MERMOS : un projet d'EDF pour la mise à jour de la méthodologie EPFH. Revue générale nucléaire, 1998.

[63] Le Bot, P., "Le facteur humain dans les études probabilistes" dans "Les études probabilistes de sûreté", Dossiers de la revue Contrôle de l'Autorité de Sûreté Nucléaire n°155 novembre 2003.

[64] Le Bot, P., "Human reliability data, human error and accident models - illustration through the Three Mile Island accident analysis", Elsevier, 2003.

[65] Libmann J., "Sûreté des réacteurs français en service", Techniques de l'Ingénieur, Traité Génie Nucléaire, BN 3 820.

[66] Lydell B., Undetected latent failures of safety-related systems, SKI Report, rev 0, 1998.

[67] Macchi L., Hollnagel E. & Leonhardt J., Resilience Engineering Approach to Safety Assessment: an Application of FRAM for the MSAW system, Eurocontrol Safety R&D Seminar, Munich – Germany, 21-22 October, 2009.

[68] Magne L. et Vasseur D., Risques industriels – Complexité, incertitude et décision – une approche interdisciplinaire, Eds. TEC & DOC Lavoisier, 2006.

[69] Meister D., « Human Factors in Reliability », section 12 in W.G. Ireson (ed), Reliability Handbook, New York: McGraw-Hill, 1966.

[70] NEA/CSNI (2004), « Le facteur humain : un défi pour les autorités de sûreté nucléaire », ISBN 92-64-02090-x.

[71] NEA/CSNI (2004), « L'évaluation probabiliste de la fiabilité humaine dans les centrales nucléaires », ISBN 92-64-02158-2.

[72] NEA - CSNI-R(2007), « Use and development of probabilistic safety assessment »

[73] OCDE, Avis techniques du CSIN n°4 "L'évaluation probabiliste de la fiabilité humaine dans les centrales nucléaires", NEA n°5069, 2004.

[74] Pennycook W.A., Embrey D.E., An operating approach to error analysis. In proceedings of the first biennal Canadian conference on process safety and loss management. Edmonton 24th April. Waterloo, Ontario, Canada : Institute for Risk research, University of Waterloo, 1993.

[75] Pyy P., « Human reliability analysis methods for probabilistic safety assessment », VTT publications 422, Espoo 2000.

[76] Reason, J., L'erreur humaine, Presses Universitaires de France Ed., 1993. Traduction française de Human error, Cambridge University Press, 1990.

[77] Reer B., Human reliability analysis of errors of commission: a review of methods and applications, Paul Scherrer Institut, 2007.

[78] RSE, Erreurs humaines et défaillances organisationnelles, dans Revue Risque sécurité Environnement, n° 1, novembre – décembre 2009.

[79] Salmon P., Stanton N.A., Walker G., Human Factors Design methods Review, HFIDTC/WP1.3.1/1, version 1/28 November 2003.

[80] Schüller, J.C.H., Brinkman J.L., van Gestel P.J., van Otterloo R.W., Red Book – Methods for determining and processing probabilities, CPR-12E, 2nd Edition, 1997.

[81] Shepherd A., HTA as a framework for task analysis, Ergonomics, 41(11), 1998, p. 1537-1552.

[82] Smith D.J., Reliability, Mantenaibility and Risk, Butterworth Heinemann 6th edition, 2001.

[83] Stamatelatos M., Apostolakis G., Dezfuli H., Everline C., Guarro S., Moieni P., Mosleh A., Paulos, T., Youngblood R., Probabilistic Risk Assessment Procedure Guide For NASA Managers and Practitioners, NASA, version 1.1, August 2002.

[84] Stanton N. A. & Stevenage S.V., Learning to predict human error: issues of acceptability, reliability and validity. Ergonomics, 41(11), 1998, p. 1737-1756.

[85] Stanton N.A., Salmon P.M., Walker G.H., Baber C., Jenkins D.P., Human Factors Methods : A Practical Guide for Engineering and Design, Ashgate Ed., 2005.

[86] Swain A.D., A Method for Performing a Human Factors Reliability Analysis, Monograph SCR-686, Sandia National Laboratories, Albuquerque, NM, 1963.

[87] Swain, A.D., « Field calibrated simulation » in Proceedings of the Symposium on Human Performance Quantification in Systems Effectiveness, Naval Material Command and the National Academy of Engineering, Washington DC, January 1967.

[88] Swain, A.D., Guttmann, H.E., Handbook of Human Reliability Analysis with emphasis on Nuclear Power Plant Applications. NUREG/CR-1278, Washington, D.C. : US Nuclear Regulatory Commission, 1983.

[89] Swain A.D., Accident Sequence Evaluation Program Human Reliability Analysis Procedure, NUREG/CR-4772, U.S. Nuclear Regulatory Commission, 1987.

[90] System safety society, System Safety Handbook, New Mexico Chapter, July 1993.

[91] Telle B., Vanderhaegen F., Moray N., “Railways system design in the light of human and machine unreliability”, Proceedings of the IEEE International Conference on Systems, Man and Cybernetics, Beijing, Chine, 1996, p. 2780-2785.

[92] Telle B., Vanderhaegen F., Moray N., “Human centered dependability for railway system design”, Proceedings of the World Congress on railway Research, Florence, Italie, 1997, p. 859 – 869.

[93] UIC, "Sécurité des installations - Méthodologie de l'analyse de risques", cahier de sécurité n°13.

[94] Uijt de Haag P.A.M. et Ale B.J.M., Purple book : Guideline for quantitative risk assessment, 2005,

[95] US Nuclear Regulatory Commission, Reactor Safety Study : an Assessment of Accident Risks in US Commercial Nuclear Power Plants, WASH-1400, NUREG-75/CR-2254, Washington, DC : US NRC, 1975.

[96] Vanderhaegen F., Telle B., Gauthier J., « Toward a method to analyse consequences of human unreliability – Application to railway system », Proceedings of the 7th IFAC/IFIP/IFORS/IEA Symposium on Analysis, Design and Evaluation of man-Machine Systems, Tokyo, Japon, 1998, p.203-208.

[97] Vanderhaegen F., APRECIH : a human unreliability analysis method – application to railway system, Control Engineering Pratice, 7, 1999, p. 1395-1403.

[98] Vanderhaegen F., Analyse et contrôle de l'erreur humaine, Lavoisier, 2003.

[99] Vanderhaegen F., A non-probabilistic prospective and retrospective human reliability analysis method – application to railway system, Reliability Engineering and System Safety, 71, 2001, p. 1-13.

[100] Wagenaar W.A., Hudson P.T., Reason J.T., Cognitive failures and accidents. Applied Cognitive Psychology, 4, 273, 1990.

[101] Wagenaar W.A., Influencing Human Behaviour : Toward a pratical approach for exploration and production, Journal of petroleum technology, 1992.

[102] Williams J.C., HEART – a proposed method for achieving high reliability in process operation by means of human factors engineering technology, in « Achievement of reliability in operating plant » Safety and Reliability Society Symposium, Floral Hall, Southport, Merseyside, 1985.

[103] Williams J.C., HEART – a proposed method for assessing and reducing human error, in 9th Advances in Reliability Technology Symposium, University of Bradford, 1986.

[104] Wreathall J., Operator Action Tree, An approach to quantifying operator error probability during accident sequences. NUS 4159, NUS Corporation, Gaithesbury, MD, 1982.

8. LISTE DES ANNEXES

Repère	Désignation précise	Nombre de pages
Annexe 1	Les types d'erreurs utilisées dans les études d'analyse du risque	2
Annexe 2	La méthode THERP	10
Annexe 3	La méthode TESEO	4
Annexe 4	La méthode SLIM	5
Annexe 5	La méthode HCR	4
Annexe 6	La méthode HEART	6
Annexe 7	La méthode ATHEANA	4
Annexe 8	La méthode CREAM	19
Annexe 9	La méthode MERMOS	9
Annexe 10	La méthode SHERPA	5
Annexe 11	La méthode TRIPOD	7
Annexe 12	La méthode ACIH	7
Annexe 13	La méthode FRAM	8
Annexe 14	Exemples d'application	47

ANNEXE 1 :
Typologies d'erreurs utilisées dans les études d'analyse du risque

Les études d'évaluation probabiliste de la fiabilité humaine EPFH sont généralement intégrées dans les études probabilistes de sûreté et de risques (EPS, PSA, PRA) [70],[72],[77],[83] ou dans les études QRA [8]. Dans les études EPS, PSA, PRA, on distingue plusieurs types d'erreurs humaines ou interactions humaines [83]:

- ***Erreurs de types A, B, C***

La classification des erreurs est basée sur la séquence temporelle par rapport à l'accident ou à l'événement initiateur [83], [89].

- Type A : les erreurs commises avant l'événement initiateur. Elles sont aussi appelées « actions routinières », telles que les erreurs de maintenance, de test ou de calibration. Ce sont des erreurs latentes.
- Type B : les actions conduisant à un événement initiateur, par exemple, les actions humaines conduisant à l'arrêt du système ou à une perte de l'énergie.
- Type C : les échecs de la conduite après l'initiateur (action erronée ou action inopportune en urgence), par exemple, actionner un système de sûreté manuel, sauvegarder ou restaurer un système automatique.

Dans les études EPS de niveau 1 conduisant à la fusion de cœur de réacteur à EDF, la contribution du facteur humain à la fréquence de fusion de cœur est estimée selon les ordres de grandeur suivants [68]:

- Type A : 6%
- Type B : à noter qu'il n'y a quasiment pas d'évaluation de la contribution des actions de type B dans les EPS d'EDF, car les causes techniques et humaines no sont pas distinguées dans les statistiques à partir desquelles sont élaborées les fréquences des initiateurs.
- Type C : 17%

- ***Erreurs par omission et erreurs de commission***

Swain [88], [89] distingue trois types d'erreurs :

- les erreurs d'omission (EOO – error of omission ou missing human action), qui est un événement de défaillance humaine (HFE – human failure event) découlant de non actions, par exemple :
  - Ignorer une tâche entière
  - Ignorer une étape dans une tâche.
- les erreurs de commission ou erreurs de réalisation (EOC ou ECOM– erreur of commission ou wrong human action) ou erreurs par action, par exemple :
  - Erreur de sélection :
    - Sélectionner une mauvaise commande ou contrôle
    - Réaliser une mauvaise connexion
    - Activer ou diffuser une mauvaise commande ou une information
    - Réaliser la bonne étape sur les mauvais objets
  - Erreur de séquence :
    - Mauvais déroulement (ordre) des actions
    - Réaliser la mauvaise étape sur les bons objets

        - Mauvais timing :
            - Trop tôt
            - Trop tard
            - Performer la bonne étape au mauvais moment ou timing incorrect
        - Mauvaise quantité
            - Peu
            - Trop
        - Réaliser un mauvais diagnostic
        - Prendre une décision précoce lorsque l'information est encore insuffisante.
    - les erreurs exceptionnelles : réaliser une action non requise.

- ***Autres modes d'erreurs***

Hollnagel propose quatre modes d'erreurs utilisés dans CREAM [44] :

- Action au mauvais moment :
    - Omission,
    - Trop tôt,
    - Trop tard,
    - Trop longue,
    - Trop courte.
- Action de mauvais type :
    - Trop courte,
    - Trop loin,
    - Trop rapide,
    - Trop loin,
    - Trop rapide,
    - Trop lente,
    - Mauvais direction,
    - Mauvais type de mouvement.
- Action sur mauvais objet :
    - Objet voisin,
    - Objet similaire,
    - Objet non relié.
- Action au mauvais endroit :
    - Omission,
    - Saut en avant,
    - Recul en arrière,
    - Répétition,
    - Renversement,
    - Mauvais action.

ANNEXE 2 : La méthode THERP

Fondement

THERP (Technique for Human Error Rate Prediction) ou Technique de Prédiction du Taux d'Erreur Humaine est une méthode d'identification, de modélisation et de quantification des événements dangereux dus aux erreurs humaines ou HFEs (Human Failure Events) dans les études probabiliste de sûreté (EPS/PRA) pour le contexte nucléaire. Cette méthode a été développée par Swain A.D., psychologue travaillant pour l'armée américaine au Sandia National Laboratories et a été publiée officiellement en 1983 [88]. Auparavant, elle a été communiquée en 1975 par US NRC [95], et publiée en 1963 par Swain A.D. [86].

Les premières versions de THERP ont été focalisées sur les formes comportementales des erreurs. Les erreurs de diagnostic et erreurs cognitives de haut niveau ont été prises en compte dans les dernières générations de THERP [88].

THERP a été considérée comme une approche mixte, entre des modèles d'erreurs humaines utilisant des arbres de probabilité et des modèles de dépendance [32]. THERP distingue cinq niveaux de dépendance et fournit cinq équations de calcul de la probabilité conditionnelle pour ces cinq situations [88].

Tableau 5: Les équations de la probabilité conditionnelle d'échec de la tâche "N" à condition que la tâche précédente "N-1" soit en échec, pour différents niveaux de dépendance

Niveau de dépendance	Probabilité conditionnelle d'échec
ZD : zéro dépendant	Pr[F"N"|F"N-1"|ZD] = N
LD : dépendance basse	Pr[F"N"|F"N-1"|LD] = (1+19N)/20
MD : dépendance moyenne	Pr[F"N"|F"N-1"|MD] = (1+6N)/7
HD : dépendance élevée	Pr[F"N"|F"N-1"|HD] = (1+N)/2
CD : dépendance complète	Pr[F"N"|F"N-1"|CD] = 1

Où : N est la probabilité d'échec basique BHEP (Basic Human Error Probability) ou nominale NHEP (Nominal Human Error Probability) de la tâche "N". Par exemple, Pr[F"N"|F"N-1"|ZD] correspond à la probabilité de l'échec de la tâche N sachant l'échec de la tâche N-1 et sachant l'absence de dépendance entre les deux tâches.

THERP considère les actions humaines du même point de vue que le fonctionnement des équipements. Elle tient compte également de facteurs de performances (Performance Shaping Factors, PSFs) influençant la performance humaine [87],[88].

Les facteurs de performance PSFs sont divisés en trois classes [88]:

- Les facteurs PSFs externes vis-à-vis de l'individu.
- Les facteurs PSFs internes vis-à-vis de l'individu.
- Les facteurs PSFs de stress et d'expérience.

Ces facteurs de performance PSFs sont utilisés pour ajuster (réduire ou augmenter) les probabilités nominales d'erreurs humaines NHEP (Nominal Human Error Probability) selon les jugements portés par les analystes sur l'environnement de travail, la qualité des interfaces homme-machine ou de l'ergonomie et des procédures, ainsi que les habiletés, l'expérience, la motivation, les aspirations et les éventuels stress de l'opérateur.

THERP aborde les événements humains pré-initiateur et post-initiateur HFEs dans le contexte nominal, i.e. dans les conditions normales [37]. Cette méthode est une méthode d'estimation des taux d'erreur humaine pour évaluer la dégradation du système homme-machine causée par les erreurs humaines en association avec d'autres facteurs comme la fiabilité des équipements et des procédures.

La réalisation de la technique THERP est basée sur une identification des erreurs humaines, des facteurs de performance PSFs et de leurs effets, à l'aide d'une analyse des tâches par une équipe multidisciplinaire animée par un expert du facteur humain. Chaque tâche est divisée ou décomposée en étapes ou tâches élémentaires plus détaillées pour identifier les erreurs pouvant se produire au niveau de chaque étape élémentaire. La décomposition d'une tâche donnée en plusieurs opérations élémentaires est présentée sous forme d'un arbre d'événements illustré dans la Figure 7. Les branches représentent des décisions binaires qui contraignent le choix entre l'action correcte (branche gauche) et l'action incorrecte (branche droite) ou erreur. Chaque branche représente une combinaison d'activités humaines associées à des facteurs de performance i.e. les déterminants présumés de ces activités.

THERP propose 27 tableaux de probabilités d'erreurs humaines pour les actions les plus courantes [88]. Pour illustrer, le Tableau 6 présente un des 27 tableaux de THERP.

Tableau 6: Probabilités des erreurs d'omission par situation lorsque l'utilisation de procédures écrites est spécifiée (tableau 15-3 dans le Hanbbook [88])

N°	Situation	Probabilité d'échec HEP ou BHEP
	Lorsque les procédures avec les dispositions de vérification sont correctement utilisées :	
(1)	Liste courte, ≤ 10 éléments	0,001
(2)	Longue liste, > 10 éléments	0,003
	Lorsque les procédures sans les dispositions de vérification sont utilisées ; ou lorsque les dispositions de vérification sont utilisées incorrectement :	
(3)	Liste courte, ≤ 10 éléments	0,003
(4)	Longue liste, > 10 éléments	0,01
(5)	Lorsque les procédures décrites sont disponibles et devraient être utilisées, cependant elles ne sont pas utilisées	0,05

Les valeurs des probabilités d'erreur humaine données sont nominales et génériques. Elles sont basées sur des avis d'experts et sur des données recueillies lors d'activités similaires à celles que réalisent des opérateurs des centrales nucléaires.

La probabilité d'erreur pour chaque étape élémentaire est estimée en tenant compte des facteurs suivants :

- la vraisemblance d'une détection, d'un diagnostic,
- la possibilité d'un rattrapage,
- les conséquences de l'erreur du moment où cette dernière n'est pas corrigée,

- les facteurs de performance internes (expérience, condition physique, …), externes (poste de travail ou la complexité de travail, conditions environnementales telles que la température, ergonomie, structure organisationnelle…), ou de stress (rapidité de la tâche, fatigue, pression temporelle…).

Le principe de la méthode est illustré dans la Figure 5.

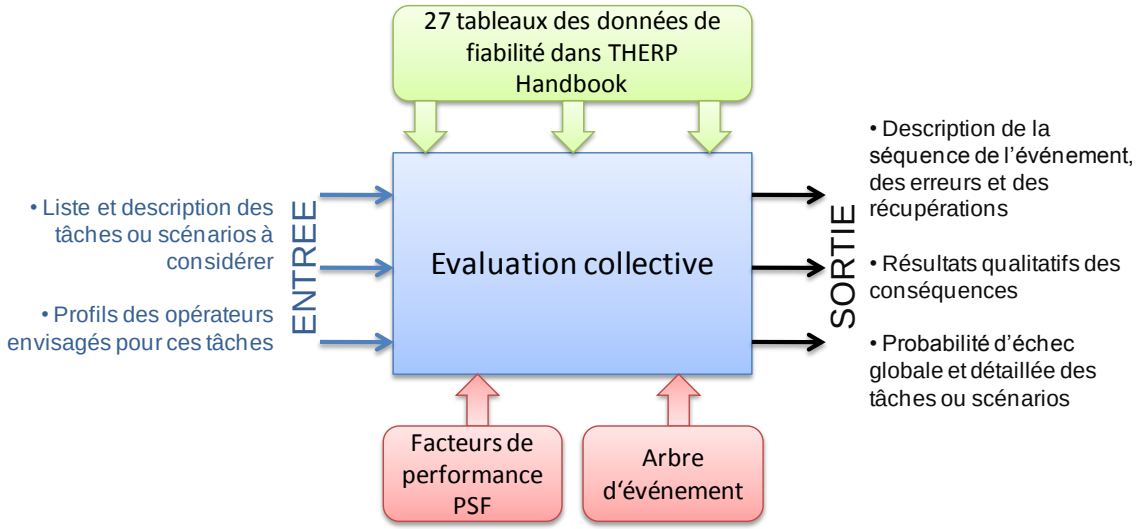


Figure 5 : Principe de la méthode THERP

Procédure

La procédure globale de THERP peut être présentée par cinq étapes suivantes [88]:

1. Définir les défaillances du système à considérer. Cette étape consiste à identifier les fonctions du système qui peuvent être affectées par les erreurs humaines.
    a) Identifier et lister toutes les opérations humaines concernées et leur relation avec le système, les tâches et les fonctions. Cette étape demande une analyse des tâches de tous les opérateurs et tous les agents chargés de la maintenance.
    b) Identifier et définir toutes les erreurs qui font l'objet d'une quantification. THERP propose les typologies d'erreurs suivantes :
        - Erreur d'omission EOO (Error Of Omission),
        - Erreur de commission, ou Erreur de réalisation EOC (Error Of Commission):
            - Erreur de diagnostic,
            - Erreur de sélection (mauvais contrôle, mauvaise position et mauvaise commande),
            - Erreur de séquence (mauvais ordre),
            - Erreur de planification (trop tôt, trop tard),
            - Erreur qualitative (trop/pas assez).

c) Estimer la probabilité des erreurs identifiées. Cette étape nécessite une estimation des probabilités nominales à l'aide de 27 tableaux fournis dans THERP (cf. Tableau 7), et une identification des conditions de performance PSFs liées aux erreurs et aux scénarios identifiés (cf. Tableau 8). La valeur numérique de ces facteurs de performance donnée dans les tableaux de THERP est ensuite utilisée pour ajuster la probabilité nominale des erreurs:

$$P_{erreur} = P_{erreur_nominale} \times \sum_{k=1}^{N} PSF_k \times W_k$$

Où :

- P_{erreur} = la probabilité de l'erreur humaine ajustée selon le contexte
- $P_{erreur_nominale}$ = la probabilité de l'erreur humaine nominale correspondante NHEP ou BHEP
- PSF_k = la valeur numérique du facteur de performance PSF_k
- W_k = le poids du facteur de performance PSF_k ou le facteur de correction, sa valeur est estimé par l'analyste entre 0,05 et 1
- N = le nombre des facteurs de performance PSFs liés à cette action humaine

Tableau 9 : Exemple de tableau d'estimation des erreurs humaines proposé par Swain [88]

Table 20-12 Estimated probabilities of errors of commission in operating manual controls* (from Table 13-3)

Item	Potential Errors	HEP	EF
(1)	Inadvertent activation of a control	see text, Ch. 13	
	Select wrong control on a panel from an array of similar-appearing controls**:		
(2)	identified by labels only	.003	3
(3)	arranged in well-delineated functional groups	.001	3
(4)	which are part of a well-defined mimic layout	.0005	10
	Turn rotary control in wrong direction (for two-position switches, see item 8):		
(5)	when there is no violation of populational stereotypes	.0005	10
(6)	when design violates a strong populational stereotype and operating conditions are normal	.05	5
(7)	when design violates a strong populational stereotype and operation is under high stress	.5	5
(8)	Turn a two-position switch in wrong direction or leave it in the wrong setting	†	
(9)	Set a rotary control to an incorrect setting (for two-position switches, see item 8)	.001	10††
(10)	Failure to complete change of state of a component if switch must be held until change is completed	.003	3
	Select wrong circuit breaker in a group of circuit breakers**:		
(11)	densely grouped and identified by labels only	.005	3
(12)	in which the PSFs are more favorable (see Ch. 13)	.003	3
(13)	Improperly mate a connector (this includes failures to seat connectors completely and failure to test locking features of connectors for engagement)	.003	3

*The HEPs are for errors of commission only and do not include any errors of decision as to which controls to activate.

**If controls or circuit breakers are to be restored and are tagged, adjust the tabled HEPs according to Table 20-15.

†Divide HEPs for rotary controls (items 5-7) by 5 (use same EFs).

††This error is a function of the clarity with which indicator position can be determined: designs of control knobs and their position indications vary greatly. For plant-specific analyses, an EF of 3 may be used.

Tableau 10 : Exemple de tableau d'estimation des facteurs d'erreurs humaines proposé par

Table 20-16 Modifications of estimated HEPs for the effects of stress and experience levels (from Table 18-1)

Item	Stress Level	Modifiers for Nominal HEPs* Skilled** (a)	Novice** (b)
(1)	Very low (Very low task load)	x2	x2
	Optimum (Optimum task load):		
(2)	Step-by-step†	x1	x1
(3)	Dynamic†	x1	x2
	Moderately high (Heavy task load):		
(4)	Step-by-step†	x2	x4
(5)	Dynamic†	x5	x10
	Extremely High (Threat stress)		
(6)	Step-by-step†	x5	x10
(7)	Dynamic† Diagnosis††	.25 (EF = 5) These are the actual HEPs to use with dynamic tasks or diagnosis--they are NOT modifiers.	.50 (EF = 5)

* The nominal HEPs are those in the data tables in Part III and in Chapter 20. Error factors (EFs) are listed in Table 20-20.

** A skilled person is one with 6 months or more experience in the tasks being assessed. A novice is one with less than 6 months or more experience. Both levels have the required licensing or certificates.

† Step-by-step tasks are routine, procedurally guided tasks, such as carrying out written calibration procedures. Dynamic tasks require a higher degree of man-machine interaction, such as decision-making, keeping track of several functions, controlling several functions, or any combination of these. These requirements are the basis of the distinction between step-by-step tasks and dynamic tasks, which are often involved in responding to an abnormal event.

†† Diagnosis may be carried out under varying degrees of stress, ranging from optimum to extremely high (threat stress). For threat stress, the HEP of .25 is used to estimate performance of an individual. Ordinarily, more than one person will be involved. Tables 20-1 and 20-3 list joint HEPs based on the number of control room personnel presumed to be involved in the diagnosis of an abnormal event for various times after annunciation of the event, and their presumed dependence levels, as presented in the staffing model in Table 20-4.

Pour les actions de diagnostic, Swain a proposé que la probabilité d'échec du diagnostic Pr[F] soit fonction du temps disponible (t) pour le réaliser. Trois courbes sont présentées dans la Figure 6, permettant de prendre en compte de manière globale les facteurs autres que le temps : la borne supérieure est à employer lorsque les caractéristiques de la situation sont défavorables, la borne médiane lorsqu'elles sont moyennes, la borne inférieure lorsqu'elles sont favorables.

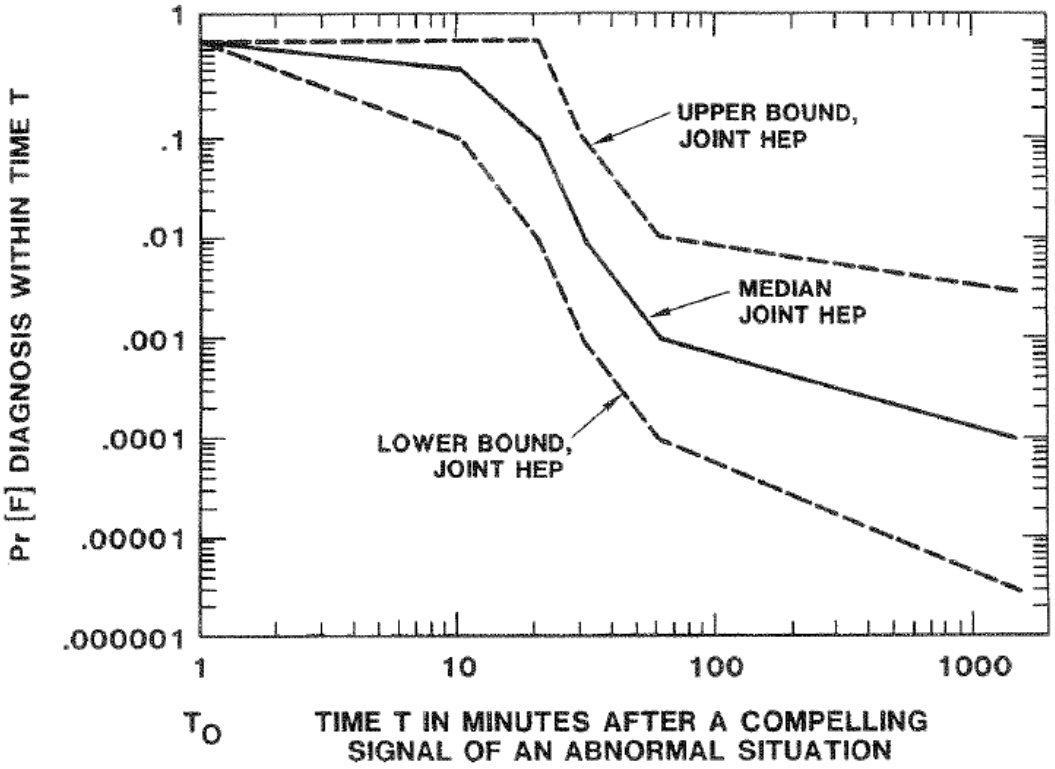
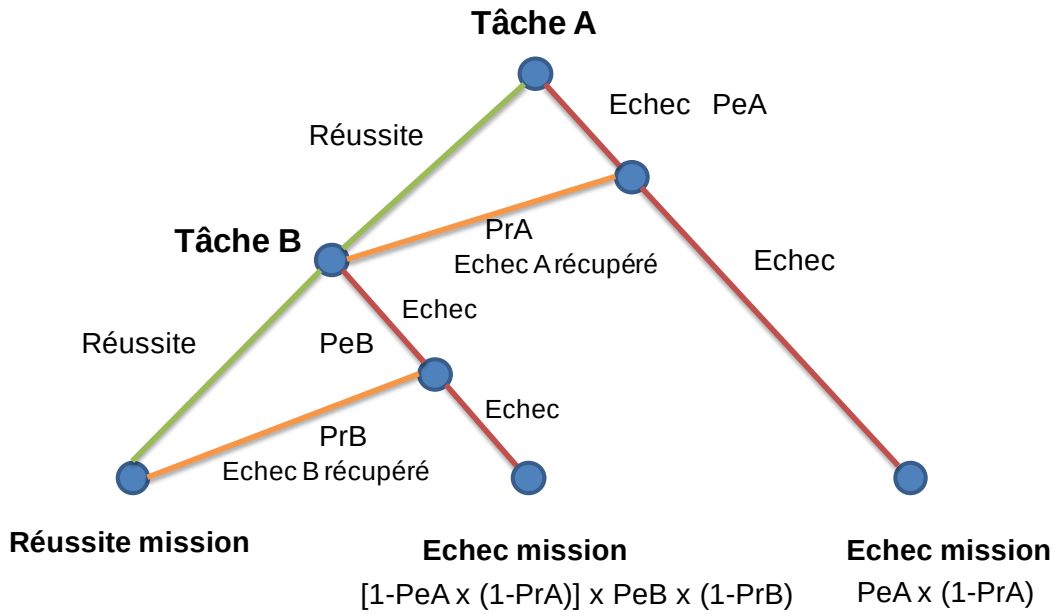


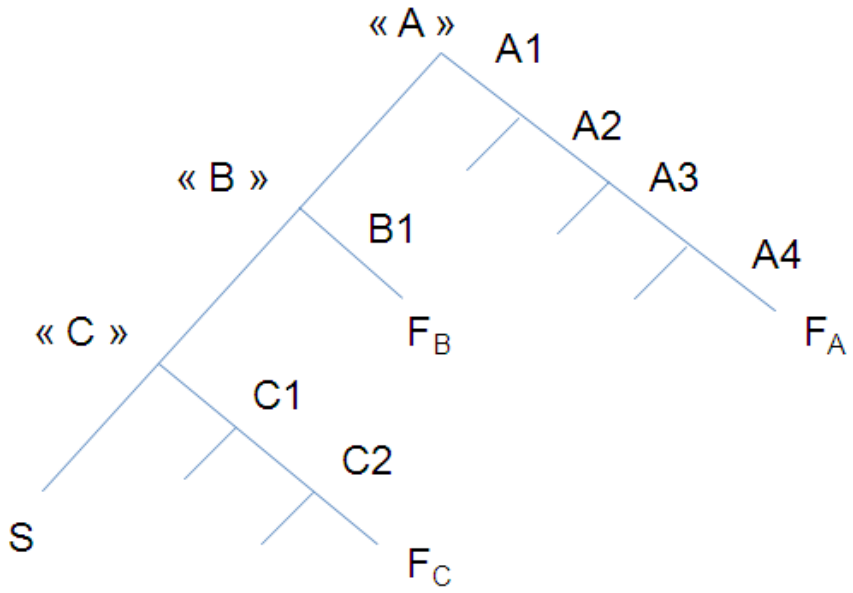
Figure 6 : Modèle de diagnostic de Swain [88]

2. Estimer la probabilité de la mission humaine globale. Cette quantification peut être conduite de la façon suivante :
   - Présenter les erreurs et les rattrapages sur un arbre d'événement du type HRAET (Human Reliability Analysis Event Tree) tel que décrit la Figure 7.
   - Identifier les possibilités de rattrapage. La probabilité de rattrapage doit être estimée.
   - Les différentes combinaisons sont calculées pour estimer la probabilité de la mission humaine globale à l'aide de l'arbre d'événement et des données de fiabilité estimées dans l'étape précédente.



P(échec mission) = PeA x (1-PrA) +[1-PeA x (1-PrA)] x PeB x (1-PrB)

Hypothèse: A et B indépendants



$$\text{Probabilité d'échec} = 1 - S = F_A + F_B + F_C$$

Figure 7 : Les arbres d'événement de THERP appliqués en pratique (S est la probabilité de succès de la mission ; FA, FB, FC sont les probabilités d'échec des étapes « A », « B » et « C »)

3. Déterminer les effets d'erreurs humaines sur le système ou procédé. Cette étape demande généralement d'intégrer l'évaluation de la fiabilité humaine dans l'étude de fiabilité du système.
4. Recommander des modifications du système et recalculer la probabilité de défaillance du système. (La procédure est itérative).

Données d'entrée (input)

- Les données d'entrée collectées à partir des sources disponibles du projet sont:
  - La description du système à considérer.
  - La description des opérations humaines.
  - Les données de fiabilité disponibles dans le Handbook [88].

Résultats (output)

- La probabilité de défaillance des opérations humaines.
- Les effets des erreurs humaines sur le système.
- Les recommandations pour améliorer le système ou le procédé.

Domaine d'application

- Industrie nucléaire

Validation

La méthode THERP est une des trois meilleures méthodes (HEART, THERP et JHEDI) sélectionnées à partir de neuf méthodes qui ont été validées par Kirwan en 1997 [57].

La méthode THERP a été sélectionnée comme une des meilleures méthodes d'identification des erreurs humaines [80]. Kim J. et coll. considèrent que HEART et THERP/ASEP sont les méthodes les plus populaires d'évaluation de la fiabilité humaine [55].

THERP a été inspirée et présentée dans de très nombreux ouvrages [37], [44], [56], [61], [80].

Commentaires

<u>Les points forts :</u>

- THERP est une méthode performante avec une bonne auditabilité.
- Le principe est simple et facile à utiliser.
- THERP propose ses propres probabilités des erreurs pour certaines activités génériques. Cela permet de cadrer la probabilité estimée par les experts dans une fourchette plus restreinte, ainsi la méthode augmente la reproductibilité des résultats.
- L'arbre d'événement est une bonne méthode pour présenter les événements et les conséquences de façon claire.
- THERP prend en compte les modes de récupération en cas d'erreur.

- La méthode de calcul est rigoureuse.

Les points faibles :

- La méthode exige des ressources importantes, avec des personnes ayant de l'expérience.
- THERP simplifie beaucoup la cognition humaine.
- S'il existe plusieurs modes d'échec différents, il est difficile de les présenter sur l'arbre d'événement.

ANNEXE 3 : La méthode TESEO

Fondement

La méthode TESEO (Technica Empirica Stima Errori Operatori) a été développée par Bello et Colombari pour la société pétrolière Italienne ENI en 1980 [17], [18], à partir de données issues d'entretiens, recueillies dans des installations pétrochimiques. Elle est également appliquée aux centrales nucléaires.

TESEO estime la probabilité d'erreur P(E) en fonction linéaire de cinq facteurs K1, K2, K3, K4, K5.

$$P(E) = K1 \times K2 \times K3 \times K4 \times K5$$

- K1 : type d'activité lié à la complexité de l'action ;
- K2 : facteur temporaire lié au temps disponible ;
- K3 : qualité de l'opérateur liée à la compétence de l'opérateur qui réalise la tâche ;
- K4 : facteur d'anxiété est un facteur émotionnel qui dépend de la gravité de la situation ;
- K5 : facteur ergonomique de l'environnement relatif aux conditions de travail.

Les valeurs pour chaque facteur sont déterminées à partir de tables prédéfinies empiriquement en fonction des caractéristiques supposées connues de la tâche et de l'opérateur humain.

Tableau 11: Coefficient K1 : Complexité de l'action

Type de tâche (complexité de l'action)	**K1**
Simple, routinière	0.001
Requiert l'attention mais routinière	0.01
Non routinière	0.1

Tableau 12: Coefficient K2 : Facteur d'exigence temporelle

Temps disponible (minutes)	**K2**	
	Tâche routinière	Tâche non routinière
2	10.0	
3		10.0
10	1.0	
20	0.5	
30		1.0
45		0.3
60		0.1

Tableau 13: Coefficient K3 : Facteur de compétence

Compétence de l'opérateur	**K3**
Bien sélectionné – expert bien entraîné	0.5
Connaissance et formation moyennes	1.0
Peu de connaissance et de formation	3.0

Tableau 14: Coefficient K4 : Facteur émotionnel

Niveau émotionnel	**K4**
Face à une situation d'urgence grave	3
Face à une situation d'urgence potentielle	2
Face à une situation normale	1

Tableau 15: Coefficient K5 : Facteur ergonomique de travail

Facteur ergonomique de l'environnement	**K5**
Excellent climat – excellentes interfaces	0.7
Bon climat – bonnes interfaces	1.0
Climat moyen – interfaces moyennes	3.0
Climat moyen – mauvaises interfaces	7.0
Mauvais Climat– mauvaises interfaces	10.0

En résumé, pour la méthode TESEO, la performance humaine maximale est atteinte lorsque :

- la tâche est simple et routinière,
- le temps disponible est ≥ 20 minutes,
- l'opérateur est bien entrainé,
- la situation est normale,
- le climat est excellent et
- les interfaces excellentes.

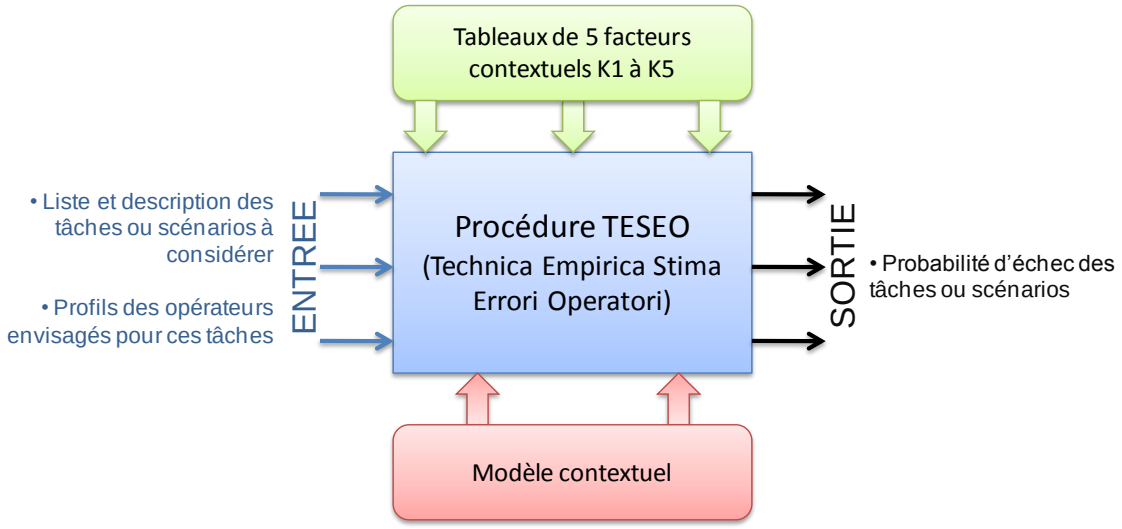


Figure 8 : Principe synthétique de la méthode TESEO

Procédure

La procédure de la méthode peut être présentée comme suit pour estimer la probabilité d'échec d'une mission identifiée:

Étape 1 : Estimer le facteur K1
Étape 2 : Estimer le facteur K2
Étape 3 : Estimer le facteur K3
Étape 4 : Estimer le facteur K4
Étape 5 : Estimer le facteur K5
Étape 6 : Calculer la probabilité d'erreur P(E) = K1 x K2 x K3 x K4 x K5

Données d'entrée (input)

La liste et la description des tâches / des missions.

Résultats (output)

Probabilité d'erreurs humaines par mission.

Domaine d'application

Générique

Validation

Aucune validation de la méthode n'a été publiée, bien que la méthode soit mentionnée dans plusieurs ouvrages [32], [76], [98].

Commentaires

Les points forts :

- La méthode est très simple.
- Elle est convenable pour une estimation grossière de la fiabilité humaine, utile dans les phases d'études de faisabilité ou de design.

Les points faibles :

- Les facteurs et les pondérations donnés par les auteurs ne sont pas basés sur des justifications théoriques solides garantissant les relations multiplicatives entre ces facteurs et une quelconque probabilité d'erreur humaine [32].
- Les valeurs K2 dans le Tableau 12 sont incomplètes.
- La méthode donne peu d'éléments pour estimer la valeur des coefficients Ki. L'estimation reste très subjective.
- Basée sur les coefficients k_i, la valeur de probabilité P(E) estimée peut être supérieure à 100%. Donc, TESEO n'est pas considéré comme une méthode rigoureuse.
- La description des tâches est très simplifiée face à la complexité des activités cognitives.
- L'application de la méthode ne donne pas d'éléments pour réduire les risques d'erreurs humaines.

ANNEXE 4 :
La méthode SLIM

Fondement

La méthode SLIM (Success Likelihood Index Method) a été développée par Embrey. La première communication date de 1983 [27]. À noter que la publication « SLIM-MAUD : An approach to assessing human error probabilities using structured expert judgment NUREG/CR-3518 » était la plus connue et mentionnée dans la littérature en 1984 [28].

SLIM / SLIM-MAUD est une méthode de jugement d'expert.

- SLIM est un ensemble de procédures pour réaliser les jugements d'experts lors de l'évaluation de la probabilité d'erreur humaine HEP.
- MAUD est un logiciel ou une procédure informatisée de SLIM.

Dans cette étude, on s'intéresse seulement au principe de la méthode SLIM. La méthode SLIM est fondée sur l'hypothèse que la probabilité d'échec liée à l'exécution de l'action dépend d'une combinaison des facteurs de performance (Performance Shaping Factors ou PSF) qui incluent les caractéristiques de l'individu, de l'environnement, et de la tâche. Elle suppose que l'expert est capable d'évaluer l'importance relative (ou poids) de chaque PSF à l'égard de ses effets sur la fiabilité de la tâche. On suppose également que, indépendamment de l'évaluation de leur importance relative, les PSFs peuvent avoir des effets positifs ou négatifs sur la tâche, les PSF améliorent ou dégradent la fiabilité.

L'indice de la probabilité de réussite (SLI - Success Likelihood Index) est une quantité, estimée par jugement d'experts, en ce qui concerne les effets positifs ou négatifs des PSFs sur la probabilité de réussite de la tâche en cours d'examen. L'indice SLI est lié à la probabilité de réussite qui est observée à long terme dans la situation considérée.

La méthode SLIM comme la méthode de Matrice de Confusion a été développée dans le but d'extraire et de structurer les jugements d'experts.

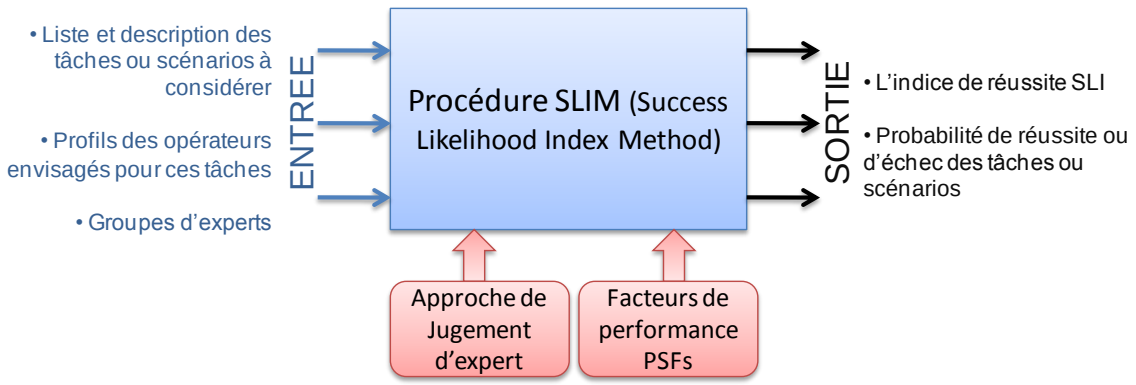


Figure 9 : Principe synthétique de la méthode SLIM-MAUD

Procédure

La procédure SLIM se compose des étapes suivantes [56]:

Étape 1 : Le choix du groupe d'experts

Étape 2 : La définition des situations et scénarios de défaillances

Les scénarios sont regroupés en trois catégories selon le type d'activité humaine concernée : scénarios basés sur la mise en œuvre d'habiletés (skill), des règles (rules) et des connaissances (knowledge). Les scénarios doivent être sélectionnés de telle manière que le poids des facteurs de performances soit homogène.

Étape 3 : Le choix des facteurs de performance PSFs

Les facteurs de performances PSFs sont sélectionnés par le groupe d'experts. Ces facteurs sont liés à l'individu, à l'environnement et à la tâche. Les facteurs de performances typiques sont les suivants :

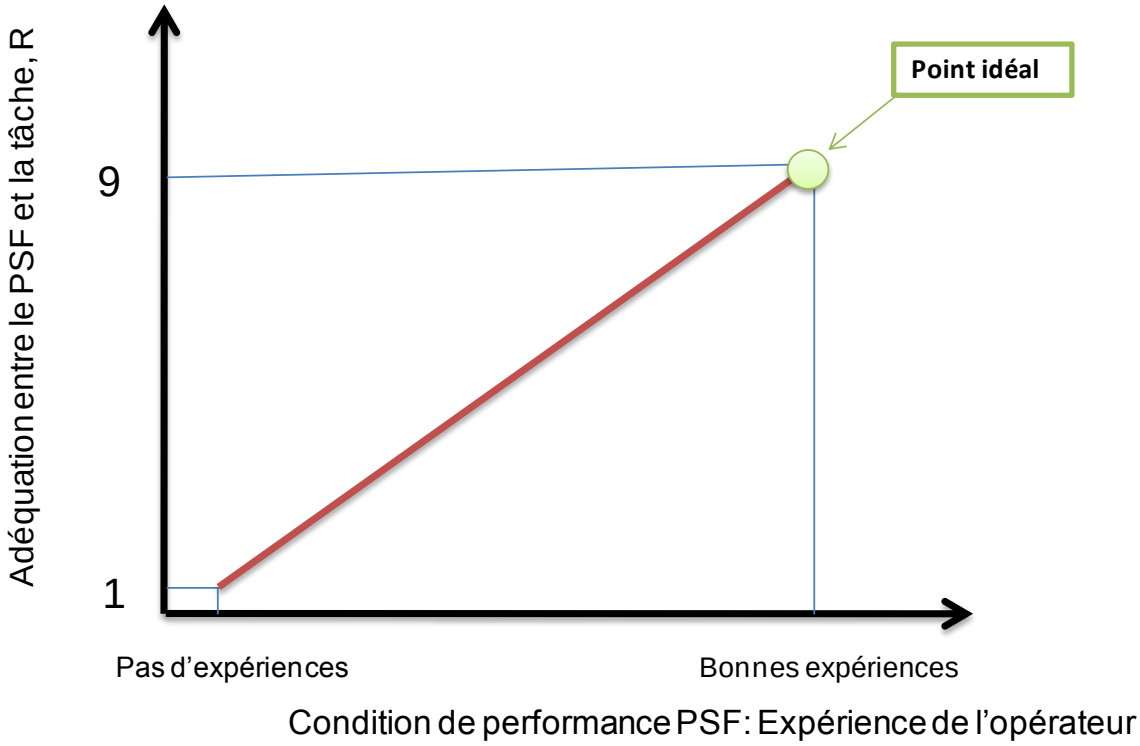
- Temps disponibles ou la pression du temps ou le niveau de stress
- Qualité de l'information ou de l'interface
- Qualité des procédures
- Conséquences perçues par l'opérateur
- Niveau de complexité de la tâche
- Formation, entraînement
- Quantité de travail en équipe exigée
- Adéquation entre le niveau d'expérience de l'opérateur et celui exigé par la tâche

Étape 4 : Attribution des notes R sur l'adéquation du facteur de performance PSF vis-à-vis de la tâche

Les tâches sont évaluées sur l'échelle visant à estimer l'adéquation entre chaque facteur de performance PSF et la tâche. Cette échelle est fixée de 1 à 9, 9 correspondant au point optimal du facteur de performance PSF. Ainsi, pour chaque tâche, une valeur R comprenant entre 1 et 9 est attribuée pour chaque facteur de performance PSF par le groupe d'experts.

Étape 5 : Explication du point idéal

Le point idéal du facteur de performance PSF vis-à-vis de la tâche, c'est-à-dire le point 9, est l'extrémité de l'échelle. La Figure 10 donne deux exemples du point idéal



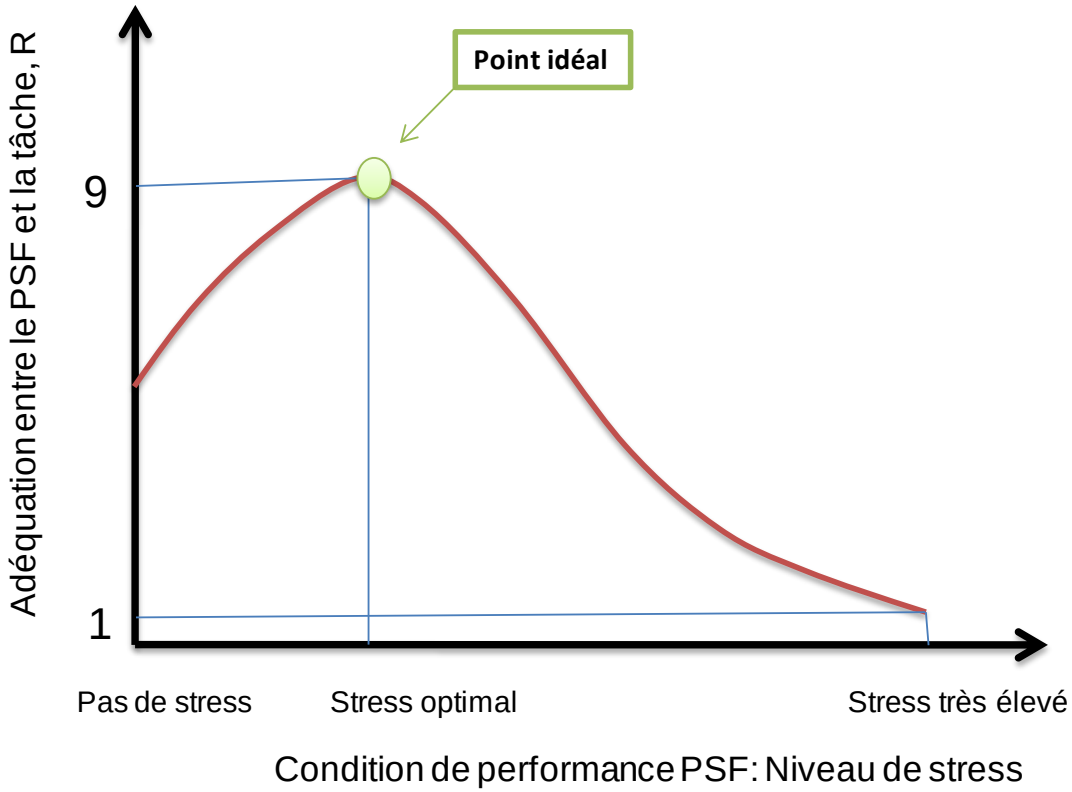


Figure 10 : Exemple du point idéal utilisé dans la méthode SLIM

Étape 6 : Vérification de l'indépendance

Si les notes des différents facteurs de performance PSFs sont similaires, il y a une forte probabilité que ces facteurs ne soient pas indépendants. Donc, ils peuvent être regroupés en un seul facteur de performance plus fondamental.

Par exemple, la pression du temps et le stress sont souvent reliés et rarement indépendants.

Étape 7 : Détermination du poids W des facteurs de performance PSFs

Cette étape détermine le poids W de chaque facteur de performance PSF. L'importance de chaque facteur de performance est différente selon la mission étudiée. Les facteurs PSFs qui ont le plus d'impacts sur la réussite ou l'échec de la mission doivent avoir le poids W le plus important.

En pratique, le poids W de chaque facteur de performance est attribué une valeur variant entre 1 et 10. Ensuite, on recalcule le poids de ces facteurs de performance pour que la somme des poids de l'ensemble des facteurs soit égale à 1.

Étape 8 : Le calcul des indexes de succès SLI

Pour la tâche j, l'index SLI de la tâche j est calculé par l'équation suivante :

$$SLI_j = \sum_{i=1}^{N} W_i \times R_{ij}$$

Où :

- N : le nombre des facteurs de performance PSFs
- W_{ij} est le poids du facteur de performance i pour la tâche j, avec $\sum_{i=1}^{N} W_i = 1$
- R_i est la note de l'adéquation entre le facteur de performance PSF_i et la tâche

Étape 9 : La conversion l'index SLI en probabilité P(réussite)

La probabilité de réussite est proportionnelle avec l'index SLI. La relation entre l'index SLI et la probabilité de succès est donnée dans l'équation suivante :

$$\text{Log P (réussite)} = a(SLI) + b$$

Pour convertir l'index SLI en probabilité absolue, il faut calibrer les valeurs SLIs pour déterminer les valeurs de a et b. Si la probabilité d'au moins deux tâches évaluées est connue, les valeurs de a et b seront déterminées.

Données d'entrée (input)

- Groupe d'experts
- Description des missions

Résultats (output)

- Probabilités P (réussite)

Domaine d'application

- Industrie nucléaire
- Applications dans d'autres domaines

Validation

Embrey et Kirwan [28] ont réalisé une étude de comparaison entre les approches de jugement d'expert APJ, PC et SLIM. Les résultats ont montré que la méthode APJ est la plus rigoureuse et les méthodes PC et SLIM ont besoin des développements supplémentaires et de calibration. Si le modèle est bien calibré avec les probabilités HEPs bien connues, la méthode peut produire des résultats corrects.

Humphreys a évalué plusieurs méthodes en considérant des critères tels que la précision, la validité, l'utilité, les ressources, l'acceptabilité et la maturité. Il a mentionné que SLIM est une méthode aussi bonne que les autres méthodes APJ, PC, TESEO, THERP, HEART, IDA et HCR [48].

Commentaires

Les points forts :

- SLIM est une bonne approche qui présente un bon rapport coût – bénéfice de l'évaluation. Le fondement de SLIM est cohérent et rigoureux.
- C'est une technique flexible qui permet d'évaluer la probabilité des actions humaines non génériques. La méthode ne demande pas une décomposition des tâches comme dans la méthode THERP.

Les points faibles :

- Le résultat dépend fortement de la qualité des experts. Il faut s'assurer que les connaissances des experts sont fiables.
- Le choix des facteurs de performance PSFs peut être arbitraire.
- Il manque des données de calibration des SLIs. Afin de bien calibrer les facteurs a et b, il faut préparer plusieurs points de référence sur des cas bien connus.
- La méthode exige la participation de nombreux experts1

.

ANNEXE 5 : La méthode HCR

Fondement

La méthode HCR (Human Cognitive Reliability) ou ORE (Operator Reliability Experiments) est initialement destinée à l'usage dans la quantification des actions humaines post-initiateur de type C [83] (par exemple, les actions menées par la salle de contrôle, associées aux procédures d'opération d'urgence et d'anomalies). Ces actions sont intégrées dans le modèle logique (arbre d'événement, arbre de défaillance) des études probabiliste de sûreté EPS. Cette méthode mentionnée dans les études de Hannaman et al. [40],[41] est en effet une forme de l'approche TRC (Time Reliability Correlation) apparue en 1982 dans les études de Wreathall [104] et Hall et al. [39]. Il existe différentes variantes de la méthode HCR [37], [56], [83]. Dans ce rapport, c'est l'approche [83] utilisée par la NASA qui est présentée.

L'approche TRC (Time Reliability Correlation) est basée sur des simulations pour estimer les probabilités des actions humaines de non-réponse dans le cadre de d'étude probabiliste de sûreté spécifiques.

TRC est la méthode la plus connue des techniques de fiabilité temporelle [37]. Ces techniques s'appliquent aux actions menées par les opérateurs intervenant dans une séquence postérieure à l'occurrence d'un événement initiateur. Le modèle de corrélation temporelle TRC de la méthode HCR suppose que dans les tâches de diagnostic, la probabilité de non-réponse dans une situation d'urgence est fortement influencée par le temps disponible pour réaliser le diagnostic.

Ce délai de réponse est lié aux différents types de comportements cognitifs SRK (Skill – Rule, Knowledge) de Rasmussen :

- Habileté (Skill-based) : les réponses qui demandent peu ou pas d'efforts cognitifs
- Règle (Rule-based) : les réponses qui sont guidées par les procédures ou règles.
- Connaissances (Knowledge-based) : les réponses qui demandent de résoudre les problèmes et de prendre des décisions.

Des variantes de cette méthode intègrent d'autres facteurs de performance PSFs comme l'expérience d'opérateurs, le stress, l'interface homme-machine qui peuvent affecter le temps de réponse médian de l'équipage $T_{1/2}$.

Le modèle HCR est représenté mathématiquement par une distribution Weibull suivante [83]:

$$P(\text{non-réponse au temps } t) = \exp-\{[(t/T_{1/2}) - \gamma_i]/\eta_i\}^{\beta i}$$

Où :

- t = temps disponible,
- γ_i, η_i, β_i sont les paramètres Weibull donnés dans le Tableau 16
- $T_{1/2}$ = temps de réponse de l'équipage, en fonction du temps nominal de réponse ajusté par les facteurs de performances PSFs donnés dans le Tableau 17.

$$T_{1/2} = T_{1/2}(\text{PSFs nominal}) \times \prod_{j=1}^{3}(1+PSF_j)$$

Tableau 16: Les paramètres du modèle HCR [39], [83]

Type du comportement cognitif	β_i	γ_i	η_i
Habileté (Skill-based)	1.2	0.7	0.407
Règle (Rule-based)	0.9	0.6	0.601
Connaissances (Knowledge-based)	0.8	0.5	0.791

Tableau 17: Les facteurs de performance PSFs et les valeurs de leur facteur correctif du modèle HCR [39], [83]

Facteur de performance PSF	**Valeur de PSF_j**
Expérience de l'opérateur (PSF_1)	
1. Expert, bien entraîné	-0.22
2. Connaissance et entraînement moyen	0.00
3. Novice, entraînement minimum	0.44
Stress (PSF_2)	
1. Situation d'urgence grave	0.44
2. Situation d'urgence potentielle	0.28
3. Actif, non urgence	0.00
4. Activité basse, vigilance basse	0.28
Qualité de l'interface homme-machine (PSF_3)	
1. Excellente	-0.22
2. Bonne	0.00
3. Moyenne	0.44
4. Mauvaise	0.78
5. Très mauvaise	0.92

La valeur de t est estimée en utilisant les techniques d'évaluation de la fiabilité humaine standards, par exemple soustraire le temps d'exécution de la réponse du temps total disponible.

Afin de déterminer $T_{1/2}$ nominal, il est recommandé de collecter, pour les événements et scénarios analysés, suffisamment de données de simulations. S'il est impossible de le faire, la valeur de $T_{1/2}$ peut être estimée par des jugements d'expert.

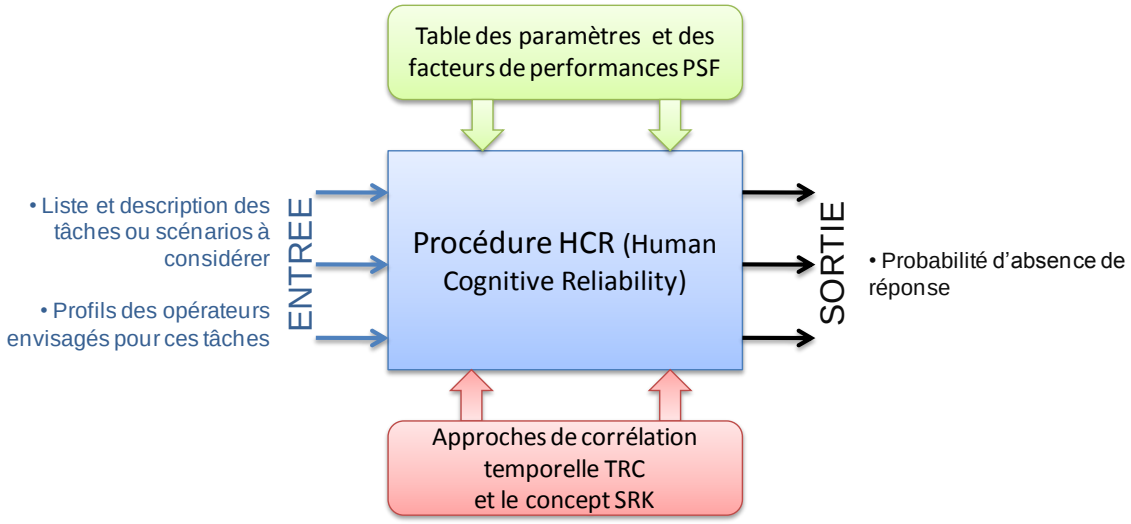


Figure 11 : Principe synthétique de la méthode HCR

Procédure

La procédure d'application de la méthode peut être présentée par les étapes suivantes:

Étape 1 : Évaluer la mission afin de déterminer le type du comportement cognitif prédominant et les facteurs de performances PSF de la mission.

Cette étape permet de déterminer les paramètres du modèle HCR.

Étape 2 : Réaliser des simulations pour collecter suffisamment les valeurs de t (temps disponible pour le diagnostic).

Étape 3 : Estimer le temps de réponse médian $T_{1/2}$ nécessaire pour réaliser une tâche donnée.

Étape 4 : Estimer le temps de réponse $T_{1/2}$ ajusté par les facteurs de performance.

Le temps $T_{1/2}$ (ajusté par PSFs) est estimé à partir du temps de réponse médian et d'une évaluation des facteurs de performance PSFs.

Étape 5 : Déterminer la probabilité d'absence de réponse P(non-réponse au temps t) après une analyse du comportement cognitif dominant de la tâche.

Données d'entrée (input)

- Expérience en analyse de la fiabilité humaine
- Expérience en analyse des tâches

Résultats (output)

Probabilité d'absence de réponse au temps t.

Domaine d'application

Nucléaire

Validation

Cette méthode a été mentionnée comme une des méthodes AFH appliquées dans le domaine nucléaire [37].

Commentaires

Les points forts :

- La méthode peut être adaptée pour estimer la probabilité d'échec des missions réalisées dans des situations d'urgence.

Les points faibles :

- Les erreurs de diagnostic et les erreurs de réalisation d'une mauvaise réponse ne sont pas identifiées dans la méthode HCR.
- Il semble que seules les actions dans la salle de contrôle ont été étudiées par la méthode.
- L'utilisation d'un simulateur ou des experts pour collecter des données augmente le coût et les délais d'application de cette méthode.
- On ne peut pas utiliser cette méthode pour évaluer une mission complète. Cette méthode est destinée à évaluer les actions intervenantes après l'événement initiateur. Donc, elle ne peut être qu'une méthode complémentaire dans l'évaluation des missions humaines pour traiter les situations d'urgence.

ANNEXE 6 : La méthode HEART

Fondement

La méthode HEART (Human Error Assessment And Reduction Technique) a été développée par Williams et publiée en 1985 [102],[103]. Cette méthode permet de déterminer la probabilité d'occurrence des erreurs. HEART est une technique d'identification et de quantification des erreurs humaines basée sur une approche très structurée. Elle traite seulement les erreurs qui présentent des impacts significatifs sur le système en question.

La méthode utilise ses propres données de fiabilité et le facteur d'effet (factor of effect) pour les conditions conduisant aux erreurs EPC (error producing conditions).

La Figure 12 illustre de façon synthétique la méthode HEART.

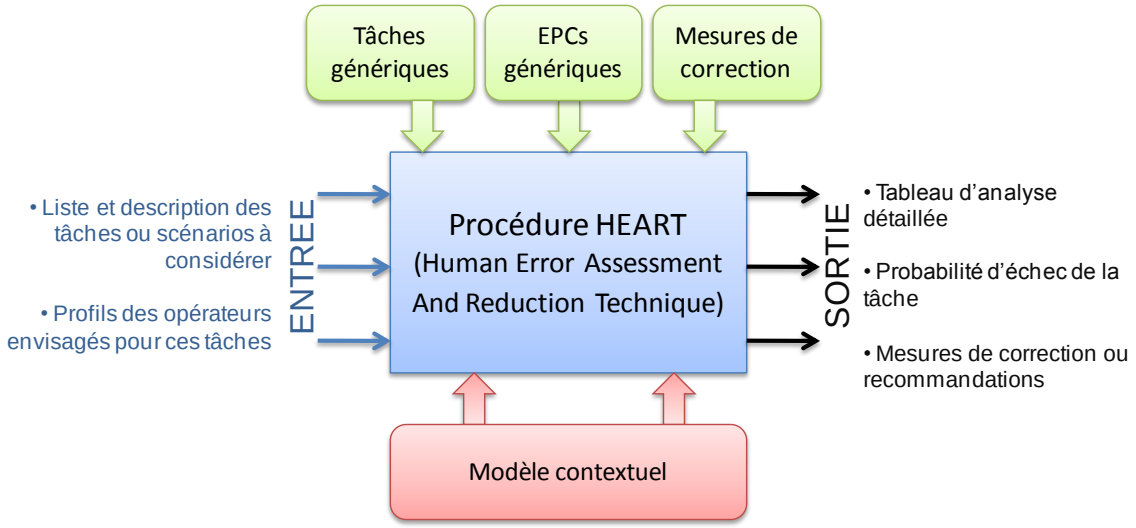


Figure 12 : Principe synthétique de la méthode HEART

Procédure

La procédure de la méthode HEART se compose des 9 étapes suivantes :

Étape 1 : Détermination des tâches ou scénarios à considérer

Cette première étape consiste à sélectionner les tâches appropriées du système en cours d'évaluation. Ces tâches doivent être les plus représentatives possibles du système considéré.

Étape 2 : Analyse hiérarchisée de tâche (HTA – Hierarchical Task Analysis) pour les tâches ou scénarios sélectionnés.

La technique HTA est utilisée pour décrire les tâches ou scénarios considérés. Les techniques de collection des données peuvent être utilisées pour recueillir les informations requises par la HTA.

Étape 3 : Conduite d'une procédure de screening HEART ou revue HEART

La méthode HEART utilise une procédure de screening sous forme de guides ou check-lists afin d'identifier les classes, les sources et l'intensité des erreurs humaines pour chaque tâche ou scénario considéré.

Étape 4 : Classification d'échecs des tâches ou évaluation de la probabilité nominale d'échec des tâches $HEP_{échec_mission_nominale}$.

Cette étape consiste à déterminer la probabilité nominale des défaillances humaines associées à la tâche analysée utilisant les tâches génériques HEART données dans le Tableau 18.

Étape 5 : Identification des conditions conduisant aux erreurs (EPCs – Error Producing Conditions)

Cette étape consiste à identifier les conditions conduisant aux erreurs EPCs en utilisant la liste des 38 EPCs génériques de HEART [102]. Le Tableau 19 représente ces 38 conditions EPCs.

Étape 6 : Évaluation de la pondération estimée W

Cette étape consiste à déterminer la pondération estimée pour chaque EPC identifiée dans l'étape 5. La pondération estimée peut prendre une valeur entre 0 et 1 (0 = bas, 1 = élevé).

Étape 7 : Calcul de la probabilité d'échec de la tâche

$$P_{échec_tâche} = P_{échec_tâche_nominale} \times \prod_{k=1}^{N} \left[\left(EPC_k - 1 \right) \times W_k + 1 \right]$$

Étape 8 : Mesures de correction

Cette étape consiste à identifier et proposer les mesures correctives éventuelles pour les erreurs identifiées. HEART propose aussi des mesures génériques pour chaque EPC [102]. Des mesures correctives spécifiques doivent être proposées en fonction de la nature et du système analysé.

Étape 9 : Documentation

L'étude HEART doit être bien documentée, tous les détails doivent être enregistrés par la personne qui réalise l'étude. Une fois que l'étude est achevée, l'étude HEART doit être formalisée.

Tableau 18: Les types de tâches génériques (GTTs) HEART [102]

Type	Tâches génériques	Probabilité d'erreur humaine nominale (Limites de 5% - 95%)
A	Tâche totalement non-familière et réalisée en cas d'urgence avec aucune idée sur les conséquences éventuelles	0.55 (0.35 – 0.97)

Type	Tâches génériques	Probabilité d'erreur humaine nominale (Limites de 5% - 95%)
B	Changer ou restaurer le système dans un nouvel état ou état d'origine par un seul essai sans supervision ou procédure	0.26 (0.14 – 0.42)
C	Tâche complexe qui demande un niveau élevé de compétences et de compréhension	0.16 (0.12 – 0.28)
D	Tâche assez simple réalisée rapidement ou avec peu d'attention	0.09 (0.06 – 0.13)
E	Routine ou tâche réalisée habituellement ou tâche rapide avec un niveau d'exigence relativement bas.	0.02 (0.007 – 0.045)
F	Déplacer ou restaurer le système dans un nouvel état ou état d'origine en utilisant des procédures avec quelques vérifications	0.003 (0.0008 – 0.0009)
G	Tâche complètement familière, bien désignée, tâche réalisée habituellement, ou tâche routinière effectuée quelques fois par heure, tâche réalisée par des personnes expérimentées, bien entrainées et très motivées, complètement conscientes des implications en cas d'échec, avec un temps suffisant pour corriger les erreurs potentielles, mais sans aucune aide significative.	0.0004 (0.00008 – 0.009)
H	Répondre correctement à la demande du système lorsqu'il y a un système de supervision automatisé qui fournit des indications précises sur l'état de système.	0.00002 (0.000006 – 0.009)
M	Tâches diverses pour lesquelles il n'existe aucune description.	0.03 (0.008 – 0.11)

Tableau 19 : Les conditions principales conduisant aux erreurs EPCs génériques de HEART [102]

N°	Conditions conduisant aux erreurs EPC	Poids de dégradation maximum de la fiabilité humaine
1	Non-familiarité avec la situation potentiellement importante qui ne se produit que rarement ou qui est nouvelle.	X 17
2	Manque de temps disponible pour détecter et corriger les erreurs	X 11
3	Faible rapport signal - bruit de fond	X 10
4	Moyens de suppression des informations ou des éléments sont trop facilement accessibles	X 9
5	Aucun moyen de transmission des informations spatiales et fonctionnelles aux opérateurs sous une forme facilement assimilable	X 8
6	Inadéquation entre le modèle d'exploitation réel et celui imaginé par le concepteur	X 8
7	Moyens pas clairs de renversement d'une action non-intentionnelle	X 8

N°	Conditions conduisant aux erreurs EPC	Poids de dégradation maximum de la fiabilité humaine
8	Surcharge de travail, notamment causée par une présentation simultanée des informations non-redondantes	X 6
9	Besoin de désapprendre une technique et d'appliquer une autre qui exige l'application d'une philosophie opposée	X 6
10	Besoin de transfert des connaissances spécifiques de tâche en tâche, sans perte d'information	X 5,5
11	Ambiguïté dans les normes de performance exigées	X 5
12	Décalage entre le risque perçu et le risque réel	X 4
13	Retour d'information pauvre, ambigu ou mal adapté du système	X 4
14	Pas de confirmation claire direct et en temps convenable des actions attendues de la partie du système dont le contrôle doit être exercé	X 4
15	Inexpérience de l'opérateur (e.g. une personne qualifiée récemment, mais pas un expert)	X 3
16	Pauvre qualité des procédures de transmission de l'information et de l'interaction personne-personne	X3
17	Peu ou pas de contrôle indépendant ou des tests de résultats	X 3
18	Conflit entre les objectifs à court et long termes	X 2,5
19	Pas de diversité de données d'entrée pour des contrôles de véracité	X 2
20	Décalage entre le niveau des résultats scolaires de l'individu et les exigences de la tâche	X 2
21	Incitation à utiliser d'autres procédures plus dangereuses	X 2
22	Peu de possibilité d'exercer le corps et l'esprit à l'extérieur de l'enceinte immédiate de l'emploi	X 1,8
23	Instrumentation peu fiable	X 1.6
24	Besoin de jugements absolus qui sont au-delà des capacités ou de l'expérience de l'opérateur	X 1,6
25	Répartition pas claire des fonctions et des responsabilités	X 1,6
26	Pas de moyen évident de garder la trace ou les progrès au cours d'une activité	X 1,4
27	Risques de dépassement des capacités physiques	X 1,4
28	Peu ou pas de signification intrinsèque dans une tâche	X 1,4
29	Haut niveau de stress émotionnel	X 1,3
30	Preuve d'une mauvaise santé parmi les opérateurs, particulièrement une fièvre.	X 1,2
31	Moral de l'équipe bas	X 1,2
32	Incohérence de la signification des affichages et des procédures	X 1,2
33	Environnement pauvre ou hostile	X 1,15
34	Inactivité prolongée ou un cycle hautement répétitif des	

N°	Conditions conduisant aux erreurs EPC	Poids de dégradation maximum de la fiabilité humaine
	tâches à faible charge de travail mental : - Pour la première une demi-heure - Pour chaque heure supplémentaire	 X 1,1 X 1,05
35	Perturbation des cycles de sommeil-travail	X 1,1
36	Stimulus de la tâche provoquée par l'intervention d'autrui	X 1,06
37	Les membres supplémentaires au-delà l'effectif nécessaire pour effectuer des tâches normalement et de manière satisfaisante	X 1,03 par personne supplémentaire
38	Âge du personnel exécutant les tâches perceptives	X 1,02

Données d'entrée (input)

- La liste et la description de l'ensemble des tâches et procédures

Résultats (output)

- Le tableau d'analyse détaillée des tâches.
- La probabilité de défaillance nominale de la tâche.

Domaine d'application

La méthode HEART a été développée pour les centrales nucléaires et l'industrie chimique. C'est une méthode générique.

Validation

La méthode HEART est une des trois meilleures méthodes (HEART, THERP et JHEDI) sélectionnées à partir de neuf méthodes qui ont été validées par Kirwan en 1997. Le niveau de validation est moyen [57], [85].

Kim J. et coll. Considère que HEART et THERP/ASEP sont les méthodes d'EFH les plus populaires [55]. La méthode HEART a été utilisée en Angleterre dans les études suivantes [85]:

- L'évaluation de risques Sizewell B,
- L'évaluation de risques pour UK Magnox et Advanced Gas-Cooled Reactor stations.

Commentaires

Les points forts :

- HEART est une méthode d'identification et de quantification des erreurs humaines. Elle est rapide et simple à utiliser, donc elle demande une formation minimale.
- Chaque condition conduisant aux erreurs est associée à une mesure corrective.

Les points faibles :

- Les guides d'utilisation sont légers, surtout pour l'évaluation des conditions conduisant aux erreurs EPCs.
- Ni la dépendance, ni l'interaction entre les EPCs n'est prise en compte dans HEART.
- La méthode est très générale et simpliste. Elle ne traite pas en détail des différents types d'erreurs.
- L'approche de HEART a été développée initialement pour le domaine nucléaire. Donc, des aménagements sont surement nécessaires pour l'appliquer dans d'autres domaines.
- En cas de décomposition d'une mission en différentes étapes, HEART permet d'estimer la probabilité d'échec de chaque étape. Cependant, HEART n'offre pas la méthode d'agrégation des probabilités des différentes étapes d'une mission pour estimer une probabilité d'échec globale pour la mission. Pour résoudre ce problème, on peut utiliser l'arbre de défaillance ou l'arbre d'événement de THERP.

ANNEXE 7 :
La méthode ATHEANA

Fondement

ATHEANA (A Technique for Human Event Analysis) est une méthode d'analyse de la fiabilité humaine dans le contexte d'une PSA (Probabilistic Safety Assessment) ou PRA (Probabilistic Risk Assessment) pour les centrales nucléaires [23][24][27]. Les études de cette méthodologie ont été réalisées et financées par la Commission de normalisation nucléaire américaine (U.S. Nuclear Regulatory Commission). La méthode repose sur une modélisation de l'interaction homme-système. Elle implique de nombreux domaines tels que la science des comportements, la psychologie cognitive, l'analyse des systèmes techniques et la fiabilité.

Dans le contexte nominal (i.e. les séquences PRA contenant les actions humaines), l'apparition des autres contextes particuliers, appelés les contextes conduisant aux erreurs EFCs (error-forcing contexts) rend l'occurrence des événements de défaillance humaine HFE (ou Human Failure Event) plus probable[3]. ATHEANA permet d'identifier et de définir, pour chaque événement HFE, les actions dangereuses UA (Unsafe Action)[4]. Ce sont une action spécifique, par exemple une omission ou une action humaine inappropriée [38] et les contextes conduisant aux erreurs EFCs associés [24]. La méthode intègre non seulement les erreurs d'omission EOO (Error Of Omission), comme les autres méthodes HRA, mais aussi les erreurs de commission EOC (Error Of Commission). Les conditions particulières EFCs regroupent :

- les conditions de la centrale,
- les facteurs de performance PSFs ou conditions humaines.

La hiérarchisation des événements HFEs est basée sur la probabilité des contextes EFCs associés.

L'estimation des probabilités d'erreurs humaines pour les événements HFEs est basée sur la construction d'un modèle probabiliste. Comme ATHEANA est une partie d'une PSA/PRA, les événements HFEs sont identifiés dans un contexte de PSA/PRA. La quantification implique le calcul de probabilité conditionnelle des événements HFEs/UAs. Chaque événement HFE contient une ou plusieurs actions dangereuses UAs, et chaque action UA peut se produire dans un ou plusieurs contextes EFCs.

Dans le cas le plus simple d'une seule action UA de l'événement HFE modélisé dans un scénario PRA (S), l'action dangereuse UA peut se réaliser dans plusieurs contextes EFCs, la quantification de la probabilité de l'événement HFE dans le scénario PRA (S) est calculée par la formule suivante :

$$P(HFE|S) = \sum_i P(EFC_i|S) \times P(UA|EFC_i, S)$$

$P(HFE|S)$ correspond à la probabilité conditionnelle d'une défaillance humaine (HFE) étant donné un scénario (S).

[3] L'événement HFE représente la défaillance ou l'indisponibilité d'un composant, d'un système ou d'une fonction causée par une omission ou par une action inappropriée humaine [38].

[4] UA est un mode d'erreur humaine impliqué dans l'événement HFE.

Dans le cas plus général où chaque événement HFE implique plusieurs actions UAs qui sont liées à plusieurs contextes EFCs, le schéma d'un événement ou un scénario d'erreur humaine HFE peut être illustré comme dans la Figure 13.

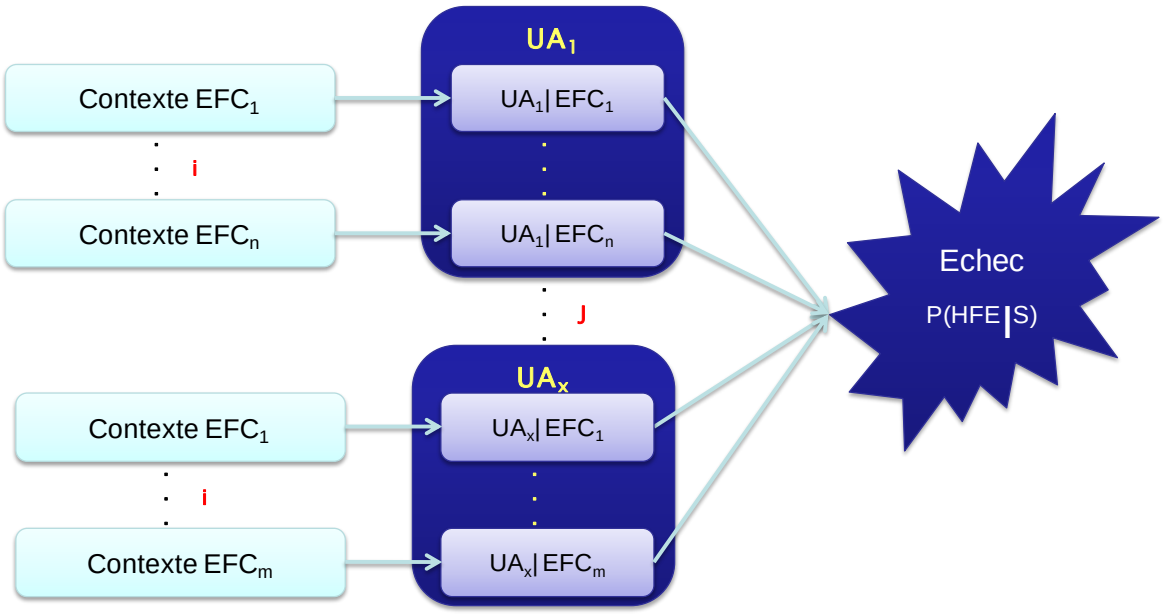


Figure 13 : Schéma d'un événement HFE dans le contexte d'un scénario PRA (S)

Ainsi, la probabilité de l'événement HFE dans le contexte d'un scénario PRA (S) peut être calculée selon la formule suivante :

$$P(HFE|S) = \sum_{j} \sum_{i(j)} P(EFC_i|S) \times P(UA_j|EFC_i, S)$$

Les probabilités conditionnelles $P(EFC_i|S)$ et $P(UA_j|EFC_i, S)$ sont estimées dans de nombreux cas par les jugements d'experts. ATHEANA propose cinq catégories typiques de probabilité présentées dans le Tableau 20.

Tableau 20: L'ensemble des points de calibrage initial de la probabilité pour les experts [38].

Situation	Probabilité
L'échec est certain	1,0
L'échec est probable	~ 0,5
L'échec est fréquent	~ 0,1
L'échec est peu probable	~ 0,01
L'échec est extrêmement improbable	~ 0,001

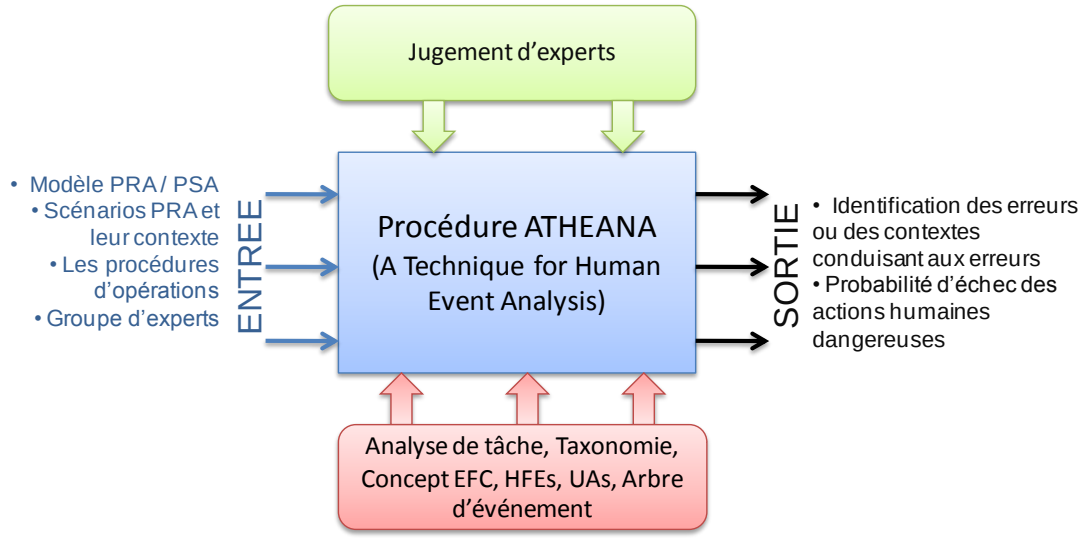


Figure 14 : Principe synthétique de la méthode ATHEANA

Procédure

L'application de la méthode ATHEANA est intégrée dans le contexte de réalisation d'une étude PRA [24] [38]. La procédure peut être synthétisée dans le schéma suivant :

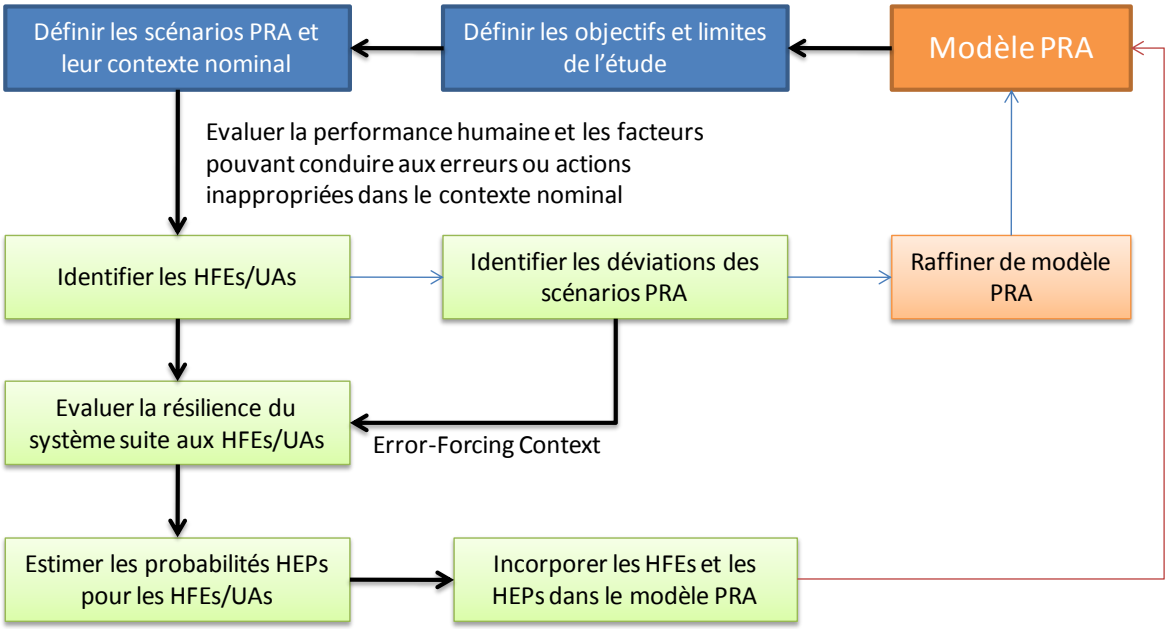


Figure 15 : Procédure d'application de la méthode ATHEANA

La méthode ATHEANA comporte les étapes suivantes [38]:

Étape 1 : Identifier les actions humaines à évaluer

Étape 2 : Définir les événements d'erreurs humaines HFEs pertinents conduisant à l'échec des actions humaines identifiées

Étape 3 : Déterminer la probabilité d'échec HEP pour les événements d'erreurs humaines HFEs identifiées, y compris les actions de rattrapage.

Les événements HFEs définis et quantifiés sont ensuite incorporés dans l'arbre d'événement ou l'arbre de défaillance du modèle PRA de façon appropriée.

Données d'entrée (input)

- Modèle PRA
- Description des équipements, des opérations, des organisations et du fonctionnement du système.
- Les procédures d'opérations
- L'équipe des experts HRA

Résultats (output)

- La probabilité HEPs des événements impliquant les facteurs humains.
- Les recommandations pour améliorer le système ou le procédé.

Domaine d'application

Pour l'industrie nucléaire, ATHEANA est une partie de l'étude probabiliste de sûreté PSA / PRA.

Cependant, on peut utiliser le même principe pour d'autres domaines.

Commentaires

Les points forts :

- La méthode permet d'intégrer le FH dans l'étude globale de sûreté PSA.
- Le concept d'ATHEANA est simple et clair.
- ATHEANA prend en compte l'aspect contextuel détaillé et global incluant les facteurs de performance PSFs et les conditions de la centrale pour connaître les différents niveaux de causes et effets.
- Il est possible d'estimer les probabilités HEPs pour toutes sortes de combinaison de différents facteurs et contextes.
- L'utilisation des jugements d'experts [38] rend la méthode plus flexible.
- C'est une méthode d'évaluation à la fois qualitative et quantitative de la fiabilité humaine.

Les points faibles :

- La méthode a été développée pour le domaine nucléaire. Il est probable que des efforts d'adaptation soient nécessaire pour l'application dans d'autres domaines industriels.
- Comme l'étude fait partie de l'étude PRA/PSA, l'analyse des erreurs humaines est limitée par les séquences prédéfinies des scénarios PRA/PSA. Il est possible que certaines erreurs ne soient pas traitées.
- ATHEANA suppose que les conditions de la centrale et les facteurs de performance PSFs influencent fortement sur les erreurs humaines, donc cette méthode demande des ressources importantes pour bien connaître le contexte.

ANNEXE 8 : La méthode CREAM

Fondement

CREAM (Cognitive Reliability and Error Analysis Method), développée par Hollnagel en 1998 [43],[44], est une méthode d'identification, d'analyse et de quantification des erreurs cognitives. Elle permet :

- d'identifier les missions, les actions ou activités de travail qui sollicitent ou dépendent de la cognition humaine, (la fiabilité cognitive étant sujette de variations),
- de déterminer les conditions où la fiabilité cognitive est faible,
- de fournir une estimation des conséquences de la performance humaine sur la sûreté du système,
- et de développer et spécifier les modifications ou recommandations qui améliorent ces conditions, donc afin d'augmenter la fiabilité de la cognition et réduire le risque.

L'approche de CREAM comporte deux modules « méthode basique » et « méthode étendue » [44], illustrés par la Figure 16.

javascript:void(0)

.

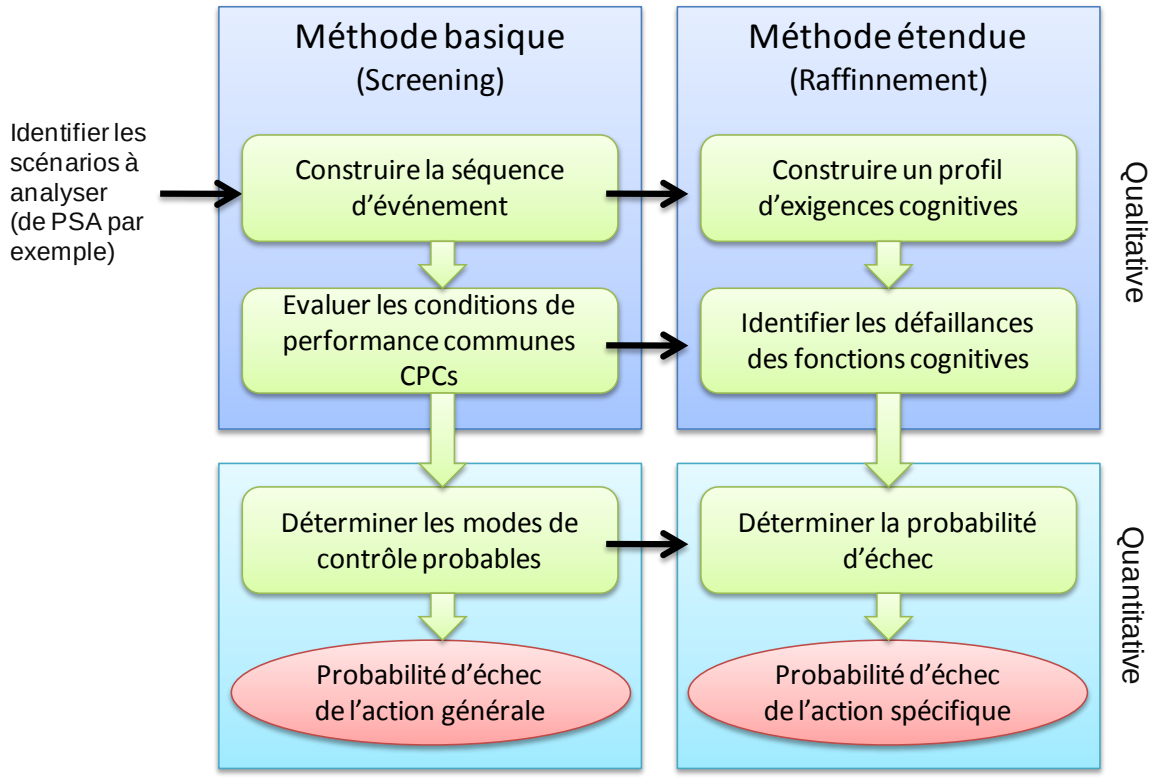


Figure 16 : Méthodes basique et étendue de CREAM [44]

CREAM est basée sur le modèle de cognition « Contextual Control Model (COCOM) » [43], qui :

- focalise sur comment les actions sont choisies par l'opérateur,
- suggère que le degré de contrôle d'action de l'opérateur est variable, et détermine la fiabilité de la performance de l'opérateur.

Le modèle COCOM a été développé à partir du modèle SMoC (Simple Model of Cognition) proposé par Hollnagel et Cacciabue [42]. Le modèle SMoC est illustré dans la Figure 17.

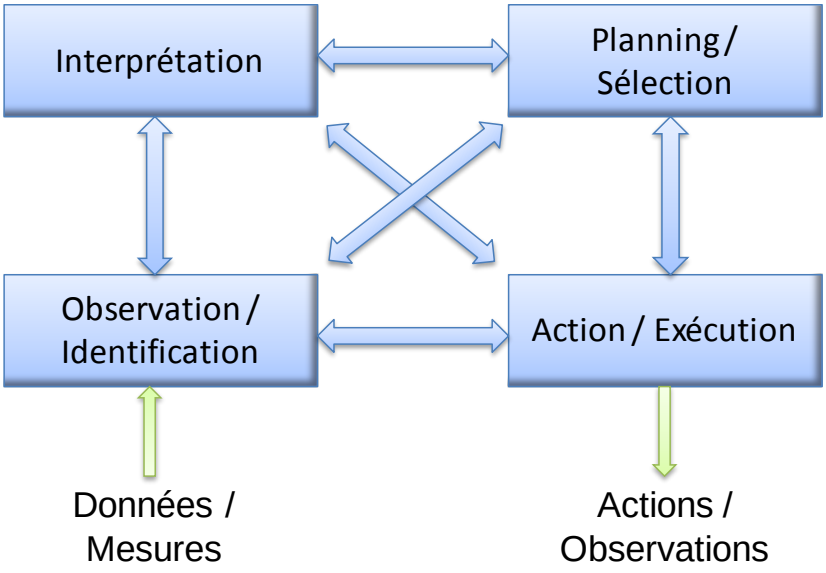


Figure 17 : Le modèle SMoC [44]

L'hypothèse basique de CREAM est que la performance humaine est le résultat de l'utilisation **contrôlée** des compétences adaptées aux exigences de la situation, plutôt que le résultat d'une séquence prédéterminée de réponses à l'événement. Autrement dit, la cognition ne correspond pas à un enchaînement d'étapes, mais plutôt à une utilisation contrôlée des compétences disponibles (habiletés, procédures, connaissances) et de ressources.

Cette hypothèse correspond au principe fondamental de l'ingénierie des systèmes cognitifs considérant que l'action humaine est intentionnelle ainsi que réactive.

La **compétence** peut être définie en termes de fonctions cognitives. Les compétences incluent les habiletés et les connaissances personnelles qui peuvent être combinées avec les procédures et les modèles de réponses (templates d'actions).

Le **contrôle** peut être décrit par référence à un continuum, allant d'une situation où une personne exerce peu ou pas de contrôle sur les événements à des conditions où l'opérateur exerce un contrôle important, et en insistant sur les modes caractéristiques de ces contrôles. Hollnagel a proposé quatre modes de contrôle :

- Contrôle brouillé (Scrambled control)
- Contrôle opportuniste (Opportunistic control)
- Contrôle tactique (Tactical control)
- Contrôle stratégique (Strategical control)

La combinaison entre les compétences et les contrôles conduit au modèle de COCOM, qui est illustré dans la Figure 18.

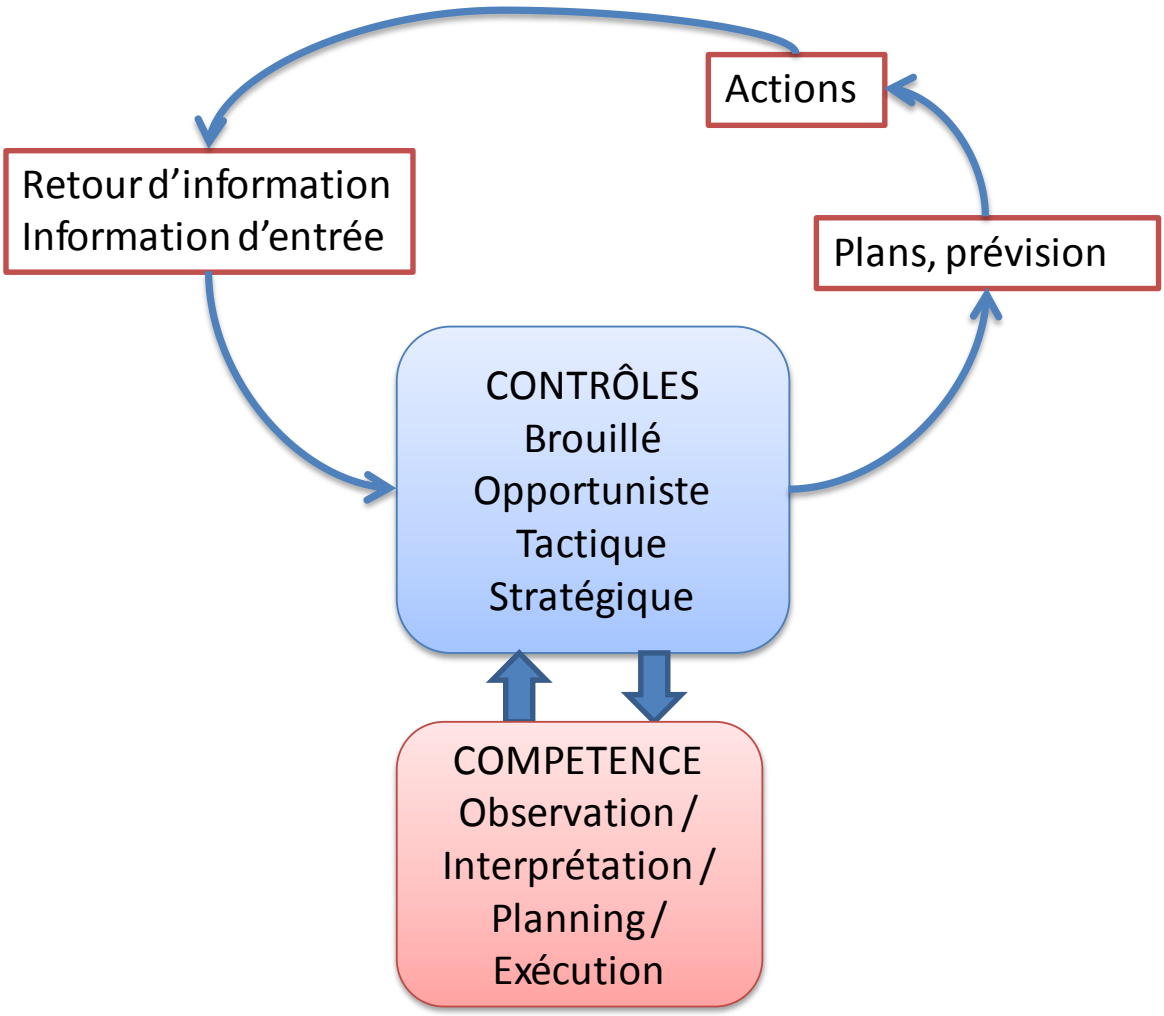


Figure 18 : Le modèle COCOM [44]

La fiabilité de la performance de l'opérateur est proportionnelle au niveau de contrôle.

Le niveau de contrôle est influencé par le contexte, car il est connu par la personne par anticipation à partir de ses connaissances ou expériences.

- Dans le contrôle brouillé, le choix de l'action suivante est imprévisible. C'est le cas où la demande de tâches est élevée et la situation est non-familière. Le cas extrême du contrôle brouillé est l'état de panique momentané. La fiabilité de la performance humaine est basse dans ce mode de contrôle.
- Dans le contrôle opportuniste, l'action est déterminée par les caractères saillants du contexte actuel plutôt que par les intentions ou les objectifs plus stables. Autrement dit, la personne réalise très peu de planning ou d'anticipation, peut-être parce que le contexte n'est pas clairement compris ou le temps est trop limité. Dans ce contexte, la personne est souvent affectée par les caractéristiques perceptives de l'interface ou par les expériences ou habitudes qui sont les plus utilisées dans les cas similaires. La fiabilité de la performance humaine est moyenne ou médiocre pour ce type de contrôle.
- Dans le contrôle tactique, la performance est basée sur une planification, ou sur une procédure ou règle connue. La fiabilité humaine dans ce type de contrôle est élevée.

- Dans le contrôle stratégique, la personne considère le contexte global, et anticipe en référence à un large horizon de temps. Le mode de contrôle stratégique fournit une performance plus efficace et plus robuste. La réalisation du contrôle stratégique est influencée par la connaissance et l'habileté de la personne, i.e. le niveau de compétence. La fiabilité humaine est élevée dans ce mode de contrôle.

CREAM distingue les causes (génotypes) et les effets ou manifestations (phénotypes). CREAM utilise un ensemble de catégories permettant de décrire la plupart des actions erronées ainsi que la majorité des causes possibles. Ces catégories ne sont pas hiérarchisées, car la connaissance sur les causes des actions humaines est insuffisante. La définition des catégories est basée sur deux principes :

- La catégorie doit respecter les principes de différenciation ou de spécialisation
- Le nombre de catégories est suffisamment grand.

CREAM propose les treize catégories de causes suivantes :

1. Modes d'erreur
2. Fonctions cognitive spécifiques
3. Fonctions personnelles générales (temporaire)
4. Fonctions personnelles générales (permanente)
5. Équipement
6. Procédures
7. Interface (temporaire)
8. Interface (permanente)
9. Communication
10. Organisation
11. Formation
12. Conditions ambiantes
13. Conditions de travail

Hollnagel considère que la classification des actions « Omission », « Réalisation » et « Autres actions» couvre tous types d'actions erronées. La première catégorie décrit les **modes d'erreurs** (ou **phénotypes**) [44]:

a) Timing : trop tôt, trop tard, omission
b) Durée : trop longue, trop courte
c) Séquence : renversement, répétition, commission, intrusion, mauvaise action
d) Objet : mauvais objet
e) Force : trop forte, trop faible
f) Direction : mauvaise direction, mauvais type de mouvement
g) Distance / magnitude: trop coute, trop loin
h) Vitesse : trop vite, trop lente

Au lieu d'utiliser les huit modes d'erreurs ci-dessus, il est plus pratique d'appliquer les quatre groupes de classification des phénotypes illustrés dans les tableaux suivants :

Tableau 21: Les groupes des modes d'erreurs (phénotypes)

Modes d'erreurs (phénotypes)	Effets généraux	Effets spécifiques
Action au mauvais moment	Temps	Trop tôt
		Trop tard
		Omission
	Durée	Trop longue
		Trop courte
Action de mauvais type	Force	Trop faible
		Trop fort
	Distance / magnitude	Trop courte
		Trop loin
	Vitesse	Trop rapide
		Trop lente
	Direction	Mauvaise direction
		Mauvais type de mouvement
Action sur mauvais objet	Mauvais objet	Objet voisin
		Objet similaire
		Objet non relié
Action au mauvais endroit	Séquence	Omission
		Saut en avant
		Saut en arrière
		Répétition
		Renversement
		Mauvais action

Dans le schéma de classification de CREAM, on distingue trois catégories de **causes** (**génotypes**):

- Causes individuelles :
    - l'observation,
    - l'interprétation,
    - le planning,
    - les fonctions cognitives spécifiques,
    - les caractéristiques individuelles temporaires et permanentes.

- Causes technologiques :
    - les défaillances des équipements,
    - les procédures,
    - l'interface homme-machine temporaire et permanente.
- Causes organisationnelles ou environnementales:
    - la communication,
    - l'organisation,
    - la formation,
    - les conditions ambiantes,
    - les conditions de travail et relation entre les personnels.

La méthode CREAM propose aussi neuf Conditions de Performances Communes (CPCs), données dans Tableau 21, visant à décrire le contexte du scénario ou de la tâche analysée. Il y a incontestablement des points communs importants entre les CPCs et les PSFs tels qu'envisagés dans la méthode THERP. Hollnagel précise que la différence entre les CPCs et les PSFs n'est pas due aux noms ou à la signification des catégories utilisées, mais liée à la manière de les utiliser [44]. Les CPCs sont utilisées dans les premières étapes de l'analyse pour décrire et caractériser le contexte global de la tâche, tandis que les PSFs sont utilisés pour ajuster la probabilité des événements individuels. Donc, les CPCs sont liées étroitement à l'étape d'analyse des tâches [44].

Tableau 22: Les conditions de performances communes CPCs de CREAM

N°	Nom de la CPC	Niveau / Descripteur
1	Adéquation de l'organisation	Qualité des rôles et responsabilité des membres de l'équipe, des supports supplémentaires, des systèmes de communication, des systèmes de management de la sécurité, des instructions et guides pour les activités tournées vers l'extérieur. Très efficace / Efficace / Inefficace / Déficient
2	Conditions de travail	Nature des conditions de travail physique telles que l'éclairage, niveau d'éblouissement des écrans, bruit provenant des alarmes, interruptions de tâche en cours, etc. Favorable / Compatible / Incompatible
3	Adéquation des interfaces Homme-Machine et des outils	Interactions Homme-Machine en général, incluant les informations disponibles à partir des écrans de contrôle, des postes de travail informatisés, et des supports opérationnels apportés en particulier par des systèmes d'aide à la décision. Positif / Adéquat / Tolérable / Inapproprié
4	Disponibilités de procédures et des plans	Procédures et plans incluant procédures opérationnelles et d'urgence, les heuristiques de réponses, les routines, etc. Approprié / Acceptable / Inapproprié

N°	Nom de la CPC	Niveau / Descripteur
5	Nombre de buts simultanés	Nombre de tâches à réaliser par une personne au même moment. Inférieur aux capacités / Correspond aux capacités / supérieurs aux capacités
6	Temps disponible	Temps disponible pour réaliser la tâche Adéquat / Temporairement inadéquat / Inadéquat en permanence
7	Rythme circadien	Période au cours de laquelle la tâche doit être réalisée. Jour / Nuit
8	Adéquation de l'entraînement et de l'expérience	Niveau et qualité de l'entraînement des agents tels que la familiarisation aux nouvelles technologies, recyclage, etc. Réfère également à l'expérience opérationnelle des agents. Adéquate, grande expérience / Adéquate, expérience limitée / Inadéquate
9	Qualité de la collaboration au sein de l'équipe	La qualité de la collaboration entre les membres de l'équipe, incluant les recouvrements entre les structures officielles et non officielles, niveau de confiance, climat social général parmi les membres de l'équipe. Très efficace / Efficace / Inefficace / Déficient

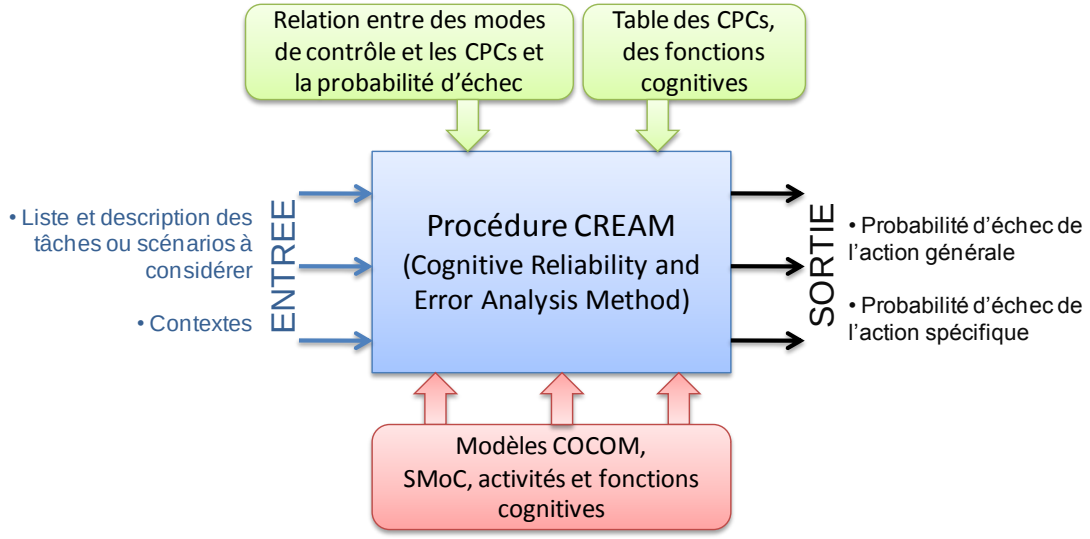


Figure 19 : Principe synthétique de la méthode CREAM

Procédure

La méthode CREAM comporte deux modules « la méthode basique » et « la méthode étendue ».

La méthode basique de CREAM

Cette méthode se compose des 3 étapes suivantes :

Étape n°1 : Construction des séquences d'événements ou analyse de la tâche

La première étape d'une AFH doit être une analyse ou une description systématique de la tâche ou du scénario à analyser. La méthode CREAM recommande une analyse hiérarchisée de la tâche HTA. Dans le cas des PSAs, l'arbre d'événement est utilisé pour organiser la description des tâches.

Plusieurs procédures de collectes de données peuvent être utilisées pour collecter les données requises.

Étape n°2 : Évaluation des conditions de performance communes CPCs

Le contexte peut être décrit à l'aide des CPCs qui sont utilisées pour caractériser la nature globale de chaque tâche. L'évaluation est exprimée par une note totale des CPCs. Comme les CPCs ne sont pas indépendantes, la note totale des CPCs ne peut pas être égale à la somme des CPCs individuelles, sauf si elles sont pondérées.

Les étapes d'évaluation des CPCs sont décrites comme suit :

1. Déterminer le niveau attendu de chaque CPC en utilisant le Tableau 23
2. Déterminer les effets sur la performance humaine en utilisant le Tableau 23

Tableau 23: Les CPCs et la fiabilité de performance

N°	Nom de la CPC	Niveau / Descripteurs	Effet sur la performance humaine
1	Adéquation de L'organisation	Très efficace	Positif
		Efficace	Non significatif
		Inefficace	Négatif
		Déficient	Négatif
2	Conditions de travail	Favorable	Positif
		Compatible	Non significatif
		Incompatible	Négatif
3	Adéquation des interfaces Homme-Machine et des outils	Positif	Positif
		Adéquat	Non significatif
		Tolérable	Non significatif
		Inapproprié	Négatif
4	Disponibilités de procédures et des plans	Approprié	Positif
		Acceptable	Non significatif
		Inapproprié	Négatif
5	Nombre de buts simultanés	Inférieur aux capacités	Non significatif
		Correspond aux capacités	Non significatif
		supérieurs aux capacités	Négatif
6	Temps disponible	Adéquat	Positif
		Temporairement inadéquat	Non significatif
		Inadéquat en permanence	Négatif
7	Rythme circadien	Jour (ajusté)	Non significatif
		Nuit (non-ajusté)	Négatif
8	Adéquation de l'entraînement et de	Adéquate, grande expérience	Positif
		Adéquate, expérience limitée	Non significatif

N°	Nom de la CPC	Niveau / Descripteurs	Effet sur la performance humaine
	l'expérience	Inadéquate	Négatif
9	Qualité de la collaboration au sein de l'équipe	Très efficace	Positif
		Efficace	Non significatif
		Inefficace	Non significatif
		Déficient	Négatif

3. Déterminer si les CPCs « Conditions de travail », « Nombre de buts simultanés », « Temps disponible » et « Qualité de la collaboration au sein de l'équipe » doivent être ajustées selon la règle décrite ci-dessous.

Afin de prendre en compte les dépendances entre les CPCs dans le calcul de la note totale des CPCs, il faut expliquer comment les dépendances peuvent être traitées. Le Tableau 24 présente les CPCs qui dépendent d'autres CPCs. La note de ces CPCs doit être ajustée.

Tableau 24: Les règles d'ajustement des CPCs

CPC	Dépend d'autres CPCs suivantes				
Conditions de travail	Adéquation de l'organisation	Adéquation des interfaces Homme-Machine et des outils	Temps disponible	Rythme circadien	Adéquation de l'entraînement et de l'expérience
Nombre de buts simultanés	Conditions de travail	Adéquation des interfaces Homme-Machine et des outils	Disponibilités de procédures et des plans		
Temps disponible	Conditions de travail	Adéquation des interfaces Homme-Machine et des outils	Disponibilités de procédures et des plans	Nombre de buts simultanés	Rythme circadien
Qualité de la collaboration au sein de l'équipe	Adéquation de l'organisation	Adéquation de l'entraînement et de l'expérience			

Par exemple, si on examine le cas « Conditions de travail », la note de cette CPC dépend de cinq autres CPCs. Selon le Tableau 24, ces CPCs sont :

- Adéquation de l'organisation
- Adéquation des interfaces Homme-Machine et des outils
- Temps disponible
- Rythme circadien
- Adéquation de l'entraînement et de l'expérience

La note de CPC « Conditions de travail » peut être évaluée selon la règle illustrée dans la Figure 20.

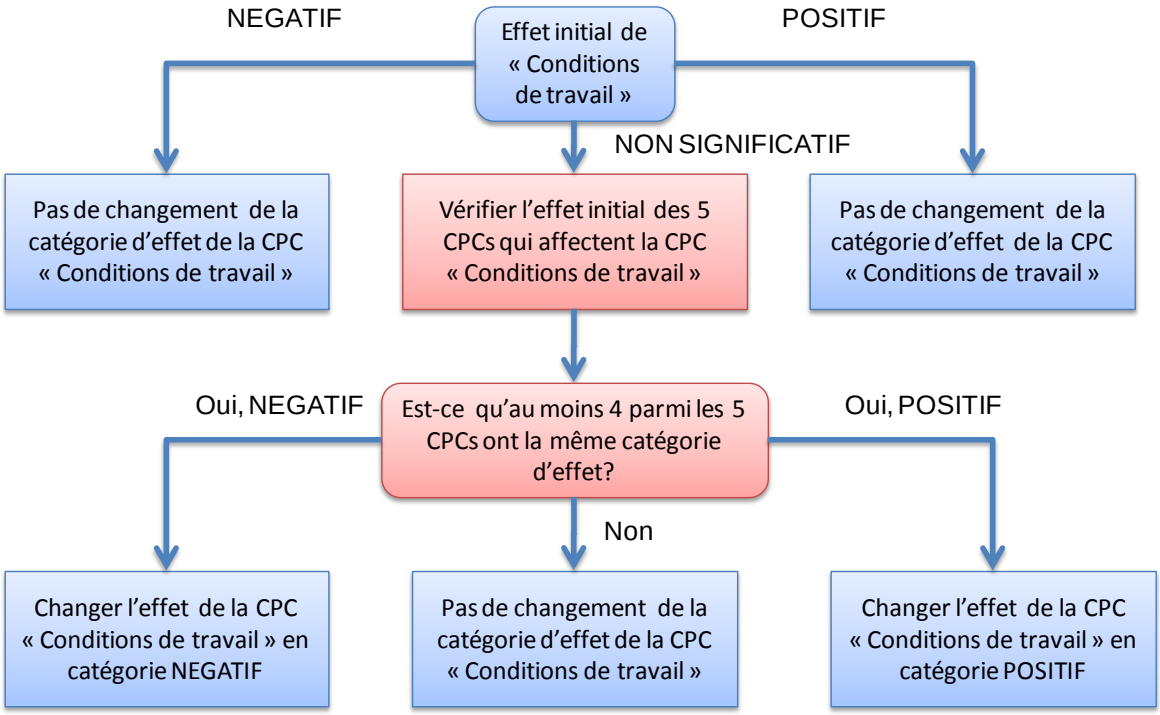


Figure 20 : Règle d'évaluation de la dépendance de la CPC « Conditions de travail »

Le même principe est appliqué pour toutes les CPCs :

- Pour les cas de « Conditions de travail » et « Temps disponible », il faut qu'au moins 4 parmi les 5 CPCs liées aient la même catégorie d'effet initial pour pouvoir changer la note d'effet initiale.
- Pour le cas de « Nombre de buts simultanés », il faut qu'au moins 2 parmi les 3 CPCs liées aient la même catégorie d'effet initial pour pouvoir changer la note d'effet initiale.
- Pour le cas de « Qualité de la collaboration au sein de l'équipe», il faut que toutes les 2 CPCs liées aient la même catégorie d'effet initial pour pouvoir changer la note d'effet initiale.

4. Additionner la note des effets attendus.

Chaque condition de performance commune CPC ne peut avoir qu'un des trois effets : négatif, non significatif ou positif. On compte le nombre de ces effets affectés pour neuf conditions de performance commune CPCs. Le résultat est exprimé sous forme [∑Négatif, ∑Non significatif, ∑Positif].

Étape n°3 : Déterminer les modes de contrôle probables

C'est la dernière étape de la méthodologie basique de CREAM pour déterminer le mode de contrôle et donc la probabilité d'échec de l'action.

À partir de la note combinée [∑Négatif, ∑Non significatif, ∑Positif], le mode de contrôle peut être déterminé à l'aide de la Figure 21.

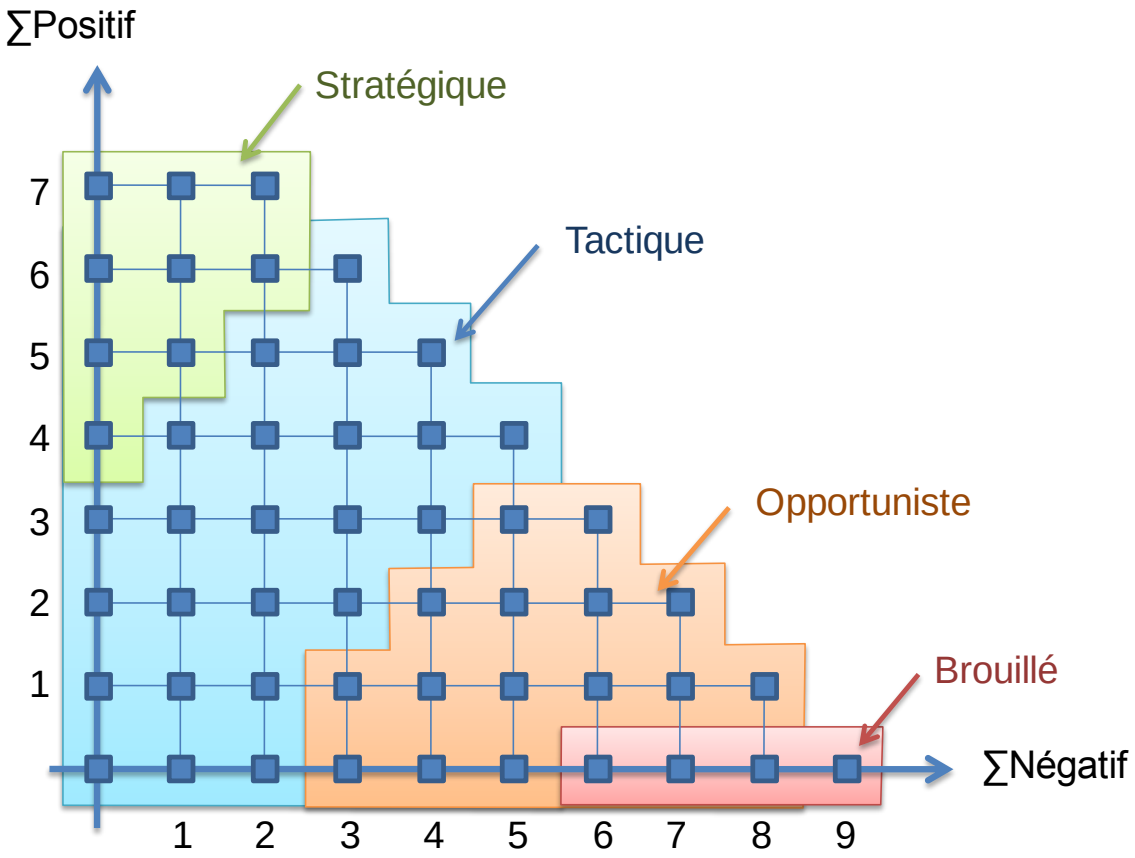


Figure 21 : Relation entre la note CPC et les modes de contrôle

La probabilité d'échec de l'action est ensuite déduite à partir du mode de contrôle selon le Tableau 25.

Tableau 25: Relation entre les modes de contrôle et l'intervalle de probabilité

Mode de contrôle	**Intervalle de fiabilité (probabilité d'échec de l'action)**
Stratégique	0,5 E-5 < p < 1,0 E-2
Tactique	1,0 E-3 < p < 1,0 E-1
Opportuniste	1,0 E-2 < p < 0,5 E-0
Brouillé	1,0 E-1 < p < 1,0 E-0

La méthode étendue de CREAM

La méthode étendue de CREAM ne peut pas être utilisée indépendamment de la méthode basique, car elle utilise les informations générées par la méthode basique.

La méthode étendue de CREAM se compose de 3 étapes suivantes :

Étape n°1 : Construire ou élaborer un profil d'exigences cognitives de la tâche

La description de la séquence d'événements est raffinée par une identification des activités cognitives qui caractérisent chaque étape ou action de la tâche. Ces activités cognitives, basées sur celles données dans le Tableau 26, sont ensuite utilisées pour élaborer un profil cognitif pour la tâche principale, basé sur les fonctions cognitives de CREAM (fonctions COCOM) données dans le Tableau 27.

Tableau 26: Liste des activités cognitives critiques

N°	Activités cognitives	Définition générale
1	Coordonner	Amener les états du système et/ou des configurations du système de contrôle dans l'état requis pour effectuer une tâche ou une étape de la tâche. Allouer ou sélectionner des ressources dans la préparation pour une mission / tâche, étalonner l'équipement, etc.
2	Communiquer	Transmettre ou recevoir de personne à personne des informations nécessaires à l'exploitation du système selon un mode soit verbal, électronique ou mécanique. La communication est un élément essentiel de la gestion.
3	Comparer	Examiner les qualités de deux ou plusieurs entités dans le but de découvrir des similitudes ou des différences. La comparaison peut exiger du calcul.
4	Diagnostiquer	Reconnaître ou déterminer la nature ou la cause d'une condition au moyen du raisonnement sur les signes ou les symptômes ou par la réalisation des tests appropriés. «Diagnostiquer» est plus approfondi que "identifier".
5	Évaluer	Évaluer une situation réelle ou hypothétique, selon les informations disponibles sans nécessiter d'opérations spéciales. Les termes associés sont «inspecter» et «vérifier».
6	Exécuter	Effectuez une action précédemment spécifiée ou un plan. L'exécution comprend des actions telles que ouvrir / fermer, démarrer / arrêter, remplir / vider, etc.
7	Identifier	Établir l'identité d'un état de l'installation ou l'état de sous-systèmes (composants). Cela peut impliquer des opérations spécifiques pour récupérer des informations et enquêter sur les détails. «Identifier» est plus approfondi que "évaluer".
8	Maintenir	Maintenir un état de fonctionnement spécifique. (Ceci est différent de la maintenance qui est généralement une activité hors ligne).
9	Surveiller	Suivre les états du système dans le temps, ou suivre le développement d'un ensemble de paramètres.
10	Observer	Chercher ou lire des valeurs de mesure spécifiques ou des indications du système.
11	Planifier	Formuler ou organiser un ensemble d'actions par lesquelles un but sera atteint avec succès. Planifier peut être à court terme ou à long terme.
12	Enregistrer	Écrire ou enregistrer les événements du système, les mesures, etc.
13	Réguler	Modifier la vitesse ou la direction d'un contrôle (système) en vue d'atteindre un but. Ajuster ou positionner les composants ou les sous-systèmes pour atteindre un état cible.
14	Balayer	Examiner rapidement les affichages ou les autres sources d'informations pour atteindre à une impression générale de l'état d'un système ou d'un sous-système.

N°	Activités cognitives	Définition générale
15	Vérifier	Confirmer l'exactitude de l'état ou des mesures du système, soit par une inspection ou un essai. Cela inclut également les vérifications des retours d'informations des opérations antérieures.

Tableau 27: Matrice générique des activités cognitives par les fonctions COCOM

N°	Activités cognitives	Fonctions COCOM			
		Observation	Interprétation	Planning	Exécution
1	Coordonner			x	x
2	Communiquer				x
3	Comparer		x		
4	Diagnostiquer		x	x	
5	Évaluer		x	x	
6	Exécuter				x
7	Identifier		x		
8	Maintenir			x	x
9	Surveiller	x	x		
10	Observer	x			
11	Planifier			x	
12	Enregistrer		x		x
13	Réguler	x			x
14	Balayer	x			
15	Vérifier	x	x		

Une fois que chaque activité cognitive est décrite par une fonction cognitive COCOM associée, la tâche peut être décrite synthétiquement par une addition du nombre d'occurrences de chacune des fonctions cognitives pour la tâche considérée.

Le profil d'exigences cognitives est décrit par le nombre d'occurrences ou le pourcentage des quatre fonctions COCOM. Il est souvent illustré par un graphique.

Étape n°2 : Identifier les défaillances des fonctions cognitives

Les défaillances des fonctions cognitives peuvent être identifiées à partir des activités et fonctions cognitives connues à l'étape 1, en utilisant les groupes de classification de CREAM, les phénotypes et les génotypes.

Le Tableau 28 présente les défaillances potentielles génériques pour les quatre fonctions cognitives, proposées par CREAM.

Tableau 28: Les défaillances des fonctions cognitives génériques

Fonctions cognitives	Défaillances potentielle des fonctions cognitives	
Observation	O1	Observer sur le mauvais objet. La réponse est donnée au mauvais stimulus ou événement.
	O2	Réaliser une mauvaise identification, due à un signal erroné ou une identification partielle.
	O3	L'observation n'est pas faite (i.e. omission), regarder par-dessus un signal ou une mesure.
Interprétation	I1	Défaut de diagnostic, comme un mauvais diagnostic ou diagnostic incomplet.
	I2	Erreur de décision, comme ne pas prendre de décision ou en prendre une mauvaise ou incomplète.
	I3	Interprétation retardée, i.e. ne pas faire au bon moment.
Planning	P1	Erreur de priorité, comme sélectionner un mauvais but (intention)
	P2	Élaborer un plan inadapté, comme le plan est incomplet ou mauvais.

Fonctions cognitives	Défaillances potentielle des fonctions cognitives	
Exécution	E1	Exécution d'un mauvais type, vis-à-vis de la force, la distance, la vitesse ou la direction.
	E2	Action réalisée au mauvais moment, comme trop tôt ou trop tard.
	E3	Action réalisée sur le mauvais objet (objet voisin, similaire ou non relié).
	E4	Action réalisée selon une mauvaise séquence, comme répétitions, saut en avant, et inversion.
	E5	Action manquée, n'est pas faite (i.e. omission), inclut l'omission des dernières actions dans la série.

La distribution des défaillances des fonctions cognitives est déterminée par le même principe de l'élaboration du profil d'exigences cognitives. Pour chaque tâche étudiée, on compte les défaillances identifiées et les regroupe en quatre classes correspondant à quatre fonctions COCOM. La distribution peut être exprimée en nombre ou pourcentage des défaillances.

Étape n°3 : Déterminer la probabilité d'échec de l'action spécifique

La probabilité des défaillances des fonctions cognitives spécifiques peut être déterminée en ajustant l'ensemble des probabilités d'échec des actions a priori avec l'impact des conditions de performances CPCs.

La probabilité des défaillances de chaque type de fonction cognitive est appelée probabilité de défaillance cognitive CFP (Cognitive Failure Probability) qui est similaire à la probabilité d'erreur humaine HEP classique. Elle peut être déterminée par les 3 étapes suivantes :

1. Déterminer la probabilité de défaillance cognitive CFP nominale pour chaque défaillance des fonctions cognitives, basée sur le Tableau 29.

Tableau 29: Les valeurs nominales et les limites d'incertitude des défaillances des fonctions cognitives

Fonctions cognitives	Type de défaillances génériques	Limite basse (0,5)	Valeur nominale	Limite haute (0,95)
Observation	O1. Observer sur le mauvais objet	3,0 E-4	1,0 E-3	3,0 E-3
	O2. Réaliser une mauvaise identification	2,0 E-2	7,0 E-2	1,7 E-2
	O3. L'observation n'est pas faite	2,0 E-2	7,0 E-2	1,7 E-2
Interprétation	I1. Défaut de diagnostic	9,0 E-2	2,0 E-1	6,0 E-1
	I2. Erreur de décision	1,0 E-3	1,0 E-2	1,0 E-1
	I3. Interprétation retardée	1,0 E-3	1,0 E-2	1,0 E-1
Planning	P1. Erreur de priorité	1,0 E-3	1,0 E-2	1,0 E-1
	P2. Élaborer un plan inadapté	1,0 E-3	1,0 E-2	1,0 E-1
Exécution	E1. Exécution d'un mauvais type	1,0 E-3	3,0 E-3	9,0 E-3

Fonctions cognitives	Type de défaillances génériques	Limite basse (0,5)	Valeur nominale	Limite haute (0,95)
	E2. Action réalisée au mauvais temps	1,0 E-3	3,0 E-3	9,0 E-3
	E3. Action réalisée sur mauvais objet	5,0 E-5	5,0 E-4	5,0 E-3
	E4. Action réalisée avec mauvais séquence	1,0 E-3	3,0 E-3	9,0 E-3
	E5. Action manquée	2,5 E-2	3,0 E-2	4,0 E-2

2. Évaluer l'impact ou effet des conditions de performances CPCs sur les valeurs CFP nominales pour estimer la valeur CFP ajustée.

   Il existe deux manières de réaliser cet ajustement :

   - La méthode la plus simple, dite approche simplifiée pour prendre en compte les effets des conditions de performances CPCs est d'utiliser les modes de contrôle décrits dans la méthode basique de CREAM. Le Tableau 30 fournit les valeurs des facteurs d'effet moyen pour les modes de contrôle. Cette approche utilise les facteurs d'effet moyen fournis dans le Tableau 35 en appliquant la formule suivante :

     CFP ajustée = CFP nominale x facteur d'effet moyen

Tableau 30: Facteurs d'effet moyen pour les modes de contrôle

Mode de contrôle	Facteurs d'effet moyen
Brouillé	2,3 E+01
Opportuniste	7,5 E+00
Tactique	1,9 E+00
Stratégique	9,4 E-01

     Les valeurs indiquées dans le Tableau 30 représentent les moyennes à travers les fonctions COCOM, calculées à partir du Tableau 32 et combinées selon le graphique de la Figure 21 [44].

   - La méthode la plus complexe consiste à prendre en compte les relations entre les conditions de performances communes CPCs et les fonctions cognitives de COCOM. Ces relations sont données dans le Tableau 31.

Tableau 31: Les liaisons entre les CPCs et les processus cognitifs

Nom de la CPC	Fonctions COCOM			
	OBS	INT	PLAN	EXE
Adéquation de L'organisation	Faible	Faible	Moyenne	Moyenne
Conditions de travail	Moyenne	Moyenne	Faible	Moyenne
Adéquation des interfaces Homme-Machine et des outils	Forte	Faible	Faible	Forte

Nom de la CPC	Fonctions COCOM			
	OBS	INT	PLAN	EXE
Disponibilités de procédures et des plans	Moyenne	Faible	Forte	Moyenne
Nombre de buts simultanés	Moyenne	Moyenne	Forte	Moyenne
Temps disponible	Forte	Forte	Forte	Forte
Rythme circadien	Faible	Faible	Faible	Faible
Adéquation de l'entraînement et de l'expérience	Moyenne	Forte	Forte	Moyenne
Qualité de la collaboration au sein de l'équipe	Forte	Forte	Forte	Forte

Il est supposé que les relations faibles sont toujours dominées par les influences moyennes et fortes. Donc, il n'est pas nécessaire de considérer les influences faibles. Cela peut être réalisé en considérant le facteur d'effet égal à 1 pour les relations faibles. Le Tableau 32 a pris en compte cette approche.

Cette approche approfondie utilise le facteur d'effet spécifique pour chaque activité cognitive. La valeur CFP ajustée est déterminée à partir des valeurs du facteur d'effet spécifique données dans le Tableau 32 en appliquant la formule suivante :

CFP ajustée = CFP nominale x facteur d'effet spécifique

Tableau 32: Facteurs d'effet spécifiques des CPCs

Nom de la CPC	Niveau	Fonctions COCOM			
		OBS	INT	PLAN	EXE
Adéquation de L'organisation	Très efficace	1.0	1.0	0.8	0.8
	Efficace	1.0	1.0	1.0	1.0
	Inefficace	1.0	1.0	1.2	1.2
	Déficient	1.0	1.0	2.0	2.0
Conditions de travail	Favorable	0.8	0.8	1.0	0.8
	Compatible	1.0	1.0	1.0	1.0
	Incompatible	2.0	2.0	1.0	2.0
Adéquation des interfaces Homme-Machine et des outils	Positif	0.5	1.0	1.0	0.5
	Adéquat	1.0	1.0	1.0	1.0
	Tolérable	1.0	1.0	1.0	1.0
	Inapproprié	5.0	1.0	1.0	5.0
Disponibilités de procédures et des plans	Approprié	0.8	1.0	0.5	0.8
	Acceptable	1.0	1.0	1.0	1.0
	Inapproprié	2.0	1.0	5.0	2.0
Nombre de buts simultanés	Inférieur aux capacités	1.0	1.0	1.0	1.0

Nom de la CPC	Niveau	Fonctions COCOM			
		OBS	INT	PLAN	EXE
	Correspond aux capacités	1.0	1.0	1.0	1.0
	supérieurs aux capacités	2.0	2.0	5.0	2.0
Temps disponible	Adéquat	0.5	0.5	0.5	0.5
	Temporairement inadéquat	1.0	1.0	1.0	1.0
	Inadéquat en permanence	5.0	5.0	5.0	5.0
Rythme circadien	Jour (ajusté)	1.0	1.0	1.0	1.0
	Nuit (non-ajusté)	1.2	1.2	1.2	1.2
Adéquation de l'entraînement et de l'expérience	Adéquate, grande expérience	0.8	0.5	0.5	0.8
	Adéquate, expérience limitée	1.0	1.0	1.0	1.0
	Inadéquate	2.0	5.0	5.0	2.0
Qualité de la collaboration au sein de l'équipe	Très efficace	0.5	0.5	0.5	0.5
	Efficace	1.0	1.0	1.0	1.0
	Inefficace	1.0	1.0	1.0	1.0
	Déficient	2.0	2.0	2.0	5.0

3. Incorporer la valeur CFP ajustée de la mission dans l'arbre d'événement de PSA.

   Si une mission se compose de plusieurs étapes élémentaires et l'échec d'une des étapes élémentaires entraînera l'échec de la mission, alors la probabilité d'échec globale de la mission est la valeur maximum des probabilités d'échec des étapes élémentaires, i.e. Max(CFP_i).

Données d'entrée (input)

- L'arbre d'événement de PSA
- Liste et description des tâches ou scénarios à étudier
- Liste des événements initiateurs

Résultats (output)

La probabilité d'échec des actions.

Domaine d'application

- Industrie nucléaire
- Applicable dans d'autres domaines qui concernent les opérations complexes ou systèmes dynamiques.

Validation

La validation empirique de cette méthode est encore très limitée.

Commentaires

Les points forts :

- La prise en compte de la dimension cognitive contextuelle de l'action humaine : l'approche est centrée sur l'individu mais avec une approche systémique basée sur le modèle COCOM.
- Cette méthode focalise sur les erreurs cognitives, elle est donc très adaptée pour les missions ou tâches complexes.
- CREAM permet d'être potentiellement exhaustif.
- CREAM est une approche structurée et systématique pour l'identification et la quantification des erreurs.
- CREAM peut être utilisée de manière proactive pour prédire les erreurs potentielles et de manière rétrospective pour analyser les erreurs survenues.
- La méthode n'est pas liée à un domaine spécifique et peut potentiellement être utilisée dans de nombreux domaines.
- La classification est détaillée, prenant en compte les causes systémiques et environnementales (sociotechnique) des erreurs.

Les points faibles :

- Pour les novices, la méthode est très difficile voire impossible.
- Le temps d'application est très élevé, même pour des scénarios simples.
- Le niveau de détail de la classification contribue à rendre la méthode très consommatrice en ressources.
- CREAM n'a pas été beaucoup utilisée.
- CREAM ne propose pas de mesure d'amélioration, comme les modes de récupérations des actions erronées.
- CREAM exige des connaissances poussées dans le domaine des facteurs humains et de l'ergonomie cognitive.
- La méthode de détermination de la probabilité d'échec globale de la mission à partir des probabilités d'échecs des étapes élémentaires (dans la méthode étendue) n'est pas très rigoureuse. Par exemple, CREAM propose que la probabilité d'échec globale de la mission soit la valeur maximum des probabilités d'échec des étapes élémentaires, i.e. Max(CFPi). En effet, la probabilité d'échec globale de la mission devrait être la somme des probabilités d'échec des étapes élémentaires, comme dans la méthode THERP.
- Comme les modes de récupérations des actions erronées ne sont pas pris en compte, le calcul de probabilité s'éloigne un peu de la réalité et le résultat peut être conservatif.

ANNEXE 9 : La méthode MERMOS

Fondement

La méthode MERMOS (Méthode d'Évaluation de la Réalisation des Missions Opérateur pour la Sûreté) a été développée par Le Bot et al. pour EDF en 1998 [62]. C'est une méthode HRA, développée en améliorant les méthodes de la première génération et intégrant le retour d'expérience de l'observation sur simulateur de conduite accidentelle. Cette méthode vise à intégrer les facteurs humains et l'impact de l'organisation et management dans les études probabiliste de sûreté EPS au niveau 1 [15], [68], i.e. les EPS permettant d'identifier les séquences menant à la fusion du cœur et de déterminer leur probabilité d'occurrence. Le but de MERMOS est d'évaluer les probabilités d'échec d'un système appelé « système de conduite », constitué l'ensemble opérateurs/procédures/interface homme-machine.

La méthode considère seulement les opérations intervenant pendant les quatre premières heures après l'incident initiateur, car elle suppose que l'équipe d'intervention d'urgence doit contrôler la situation avant quatre heures. Actuellement, la méthode MERMOS est la méthode de référence d'EDF pour l'analyse de la conduite après la survenance de l'initiateur (conduite dite post-accidentelle, échec de type C) [68].

La méthode MERMOS prend en compte globalement la conduite au niveau du « système de conduite ». Mermos ne s'intéresse pas seulement à l' « erreur individuelle », mais cherche à évaluer comment le « système de conduite » peut être mis en échec [68]. La méthode reconnaît la part importante de l'expertise et du jugement d'expert dans l'évaluation de la fiabilité humaine.

CICA (Configuration Importante de la Conduite Accidentelle) est un concept important de MERMOS pour décrire l'ensemble des conduites. Il prend en compte les aspects organisationnels, tels que la priorité de tâche ou la répartition des tâches entre les personnes et les systèmes. Une CICA désigne une orientation, une configuration du système de conduite accidentelle, une sélection ou priorisation de certaines informations pertinentes à surveiller. Les termes utilisés pour décrire les CICA sont en général des termes exprimant une attitude adoptée pendant un certain temps par le système de conduite, comme la focalisation, l'anticipation, la hiérarchisation, etc. Cependant, il n'existe ni typologie, ni taxonomie des CICA. On peut trouver quelques exemples des CICAs :

- La focalisation sur la restauration de…,
- Le suivi pas à pas des consignes,
- La tentative de redémarrage du système d'alimentation en eau des générateurs de vapeurs (ARE) en parallèle de l'application des consignes accidentelles (ou approche par état APE). Cela conduit à une suspension de l'APE.
- Les représentations et logiques de pensée des acteurs présents, par exemple : deux opérateurs ne pensent pas qu'ils vont pouvoir démarrer la pompe qui est en panne.
- Les difficultés que les opérateurs rencontrent dans la situation, par exemple : la pompe redémarre mais l'alarme température haute apparaît.
- …

Les CICA émergent des interactions entre acteurs, entre acteurs et procédure, entre acteurs et interface et entre le système de conduite et la situation. La description de la conduite au niveau du système permet de régler les erreurs individuelles. Les erreurs individuelles sont corrigées au niveau collectif grâce des formes de redondances qu'elles soient matérielles, procédurales ou organisationnelles (superviseur).

La méthode MERMOS considère la défaillance comme l'inadéquation fonctionnelle du système de conduite à une situation particulière. Les hypothèses fondamentales sont les suivantes :

- La défaillance peut survenir selon plusieurs scénarios d'échec indépendants. La probabilité d'échec de la mission est donc la somme de la probabilité d'échec de tous ces scénarios, plus une probabilité résiduelle limitant à une valeur minimum de 10^{-5} la probabilité d'échec de la mission [68]. Cette valeur qui peut être comprise entre 10^{-5} et 10^{-4} permet de couvrir les scénarios non-identifiés.
- L'erreur humaine n'est pas prédominante. Le système conçu est suffisamment robuste et redondant pour que les conséquences d'une erreur individuelle soient circonscrites.
- Les redondances sont prises en compte au sein du système de conduite. La méthode prend en compte le superviseur et l'ingénieur de sûreté, qui assument spécifiquement cette fonction de redondance.
- La conduite du système dans le temps est décrite au moyen du concept de CICA.
- C'est le contexte qui détermine les conditions d'émergence des CICA. Le contexte se compose de deux parties, contexte de caractéristiques structurelles consécutives à l'initiateur et contexte particulier. Le contexte particulier peut être des événements aléatoires mineurs (défaillance des équipements), de la variabilité au niveau de l'équipe (formation, expérience, style de conduite) ou lié à l'historique possible depuis le début de l'incident… Les principaux composants examinés sont :
    - les procédures
    - la formation
    - les systèmes du contrôle-commande
    - la dynamique du process
    - l'organisation formelle
    - les orientations données par le management
    - la structure et la dynamique du collectif
    - le profil et l'histoire des membres du collectif
- La défaillance est définie à partir des exigences fonctionnelles requises de la conduite, dont la non satisfaction entraîne l'échec de la mission.
- Par hypothèse, une mission FH peut être décrite par trois fonctions « Stratégie », « Action » et « Diagnostic », modèle SAD. L'échec d'une des fonctions fait échouer la mission. Le mode de défaillance désigne l'effet par lequel une défaillance survient. Par exemple : absence de stratégie ; stratégie erronée ; pas d'action ; action erronée.

- La propriété contextuelle permet de décrire les particularités de la situation et définit le contexte nécessaire à l'émergence éventuelle des CICA.
- La propriété structurelle est intrinsèque à chaque mission. Elle est caractérisée de façon complète par la séquence accidentelle dans laquelle la mission FH est définie. Leur probabilité conditionnelle est égale à 1.
- La récupération ne fait pas l'objet d'un modèle spécifique dans MERMOS. L'échec de la mission n'est pas défini de manière ponctuelle, mais de manière temporelle. Il n'y a pas d'échec de la mission FH tant que celle-ci peut être encore réalisée dans le temps disponible. La récupération d'une erreur ponctuelle est prise en compte au sein de l'analyse de la mission FH. Donc, dans MERMOS, l'échec est irréversible et irrécupérable.
- La notion « requis » désigne les conditions nécessaires et suffisantes pour réussir une mission FH.
- La notion « prescrit » désigne l'ensemble des procédures et dispositifs organisationnels censés donner à l'équipe les moyens de satisfaire le « requis » dans toutes les situations.
- L'échec d'une mission HF est analysé comme le résultat des scénarios identifiables et non-identifiables.

  P (échec de la mission FH) = P (échec des scénarios identifiables) + P (échec des scénarios non-identifiables) = $\sum_{i=1}^{nbescidentifiables} P(scénario_i) + P_{résiduelle}$

  Où : $P_{résiduelle}$ est la probabilité résiduelle

  P(scénario_i) est la probabilité d'un scénario qui est calculé selon la formule suivante :

$$P(scénario_i) = \prod_{j=1}^{m} P(contexte_j \,/\, initiateur_et_aggravants) \times \prod_{k=1}^{p} P(CICA_k \,/\, contexte) \times P(non_reconfiguration)$$

  $P(contexte_j \,/\, initiateur_et_aggravants)$ correspond à la probabilité conditionnelle d'un contexte étant donné l'occurrence d'un initiateur et d'aggravants.

  $P(CICA_k \,/\, contexte)$ correspond à la probabilité conditionnelle d'une CICA étant donné un certain contexte.

  La non reconfiguration est la probabilité d'occurrence du scénario d'échec compte tenu du maintien des CICAs pendant un certain de temps, rendant impossible l'atteinte des objectifs fonctionnels.

La Figure 22 présente le schéma générique d'un scénario d'échec.

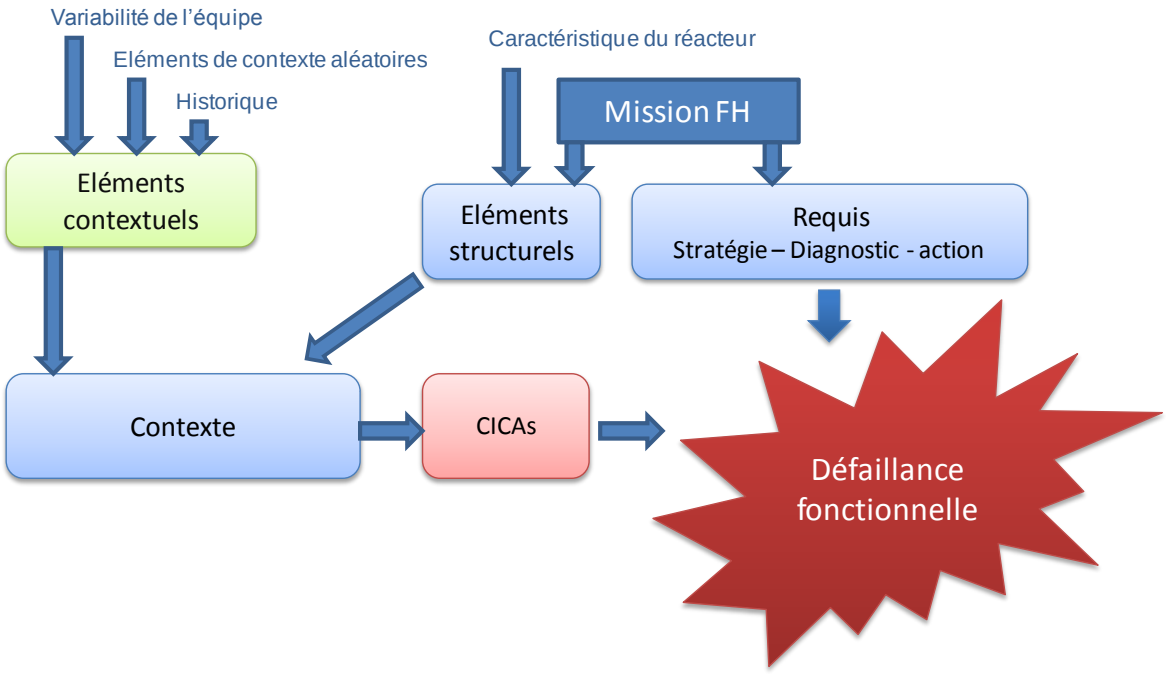


Figure 22 : Schéma d'un scénario d'échec

Pour faciliter l'utilisation de la méthode, les développeurs ont établi une base de données des missions FH et les scénarios d'échec.

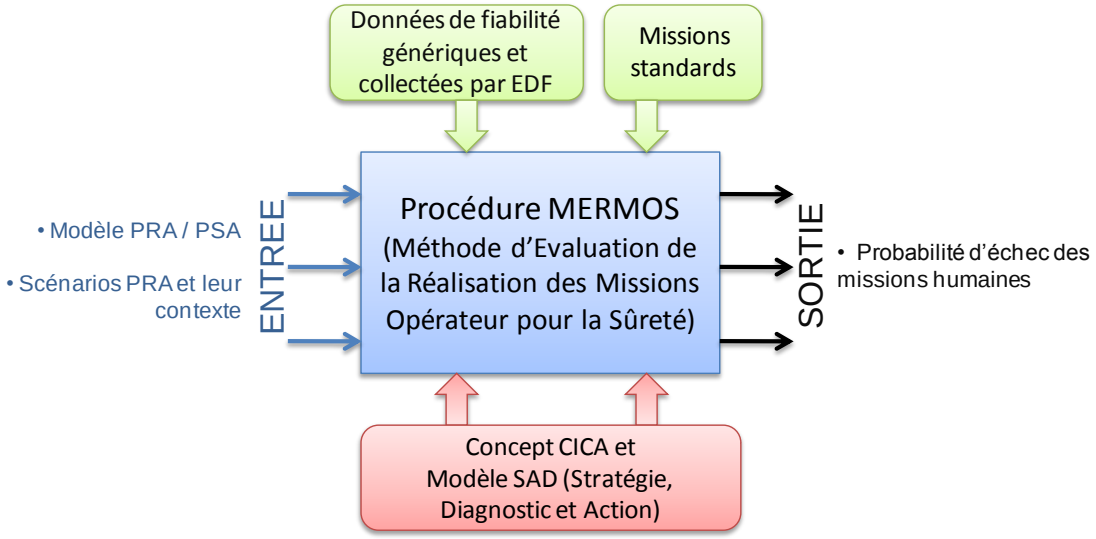


Figure 23 : Principe synthétique de la méthode MERMOS

Procédure

Le processus de la méthode MERMOS est illustré dans la Figure 24.

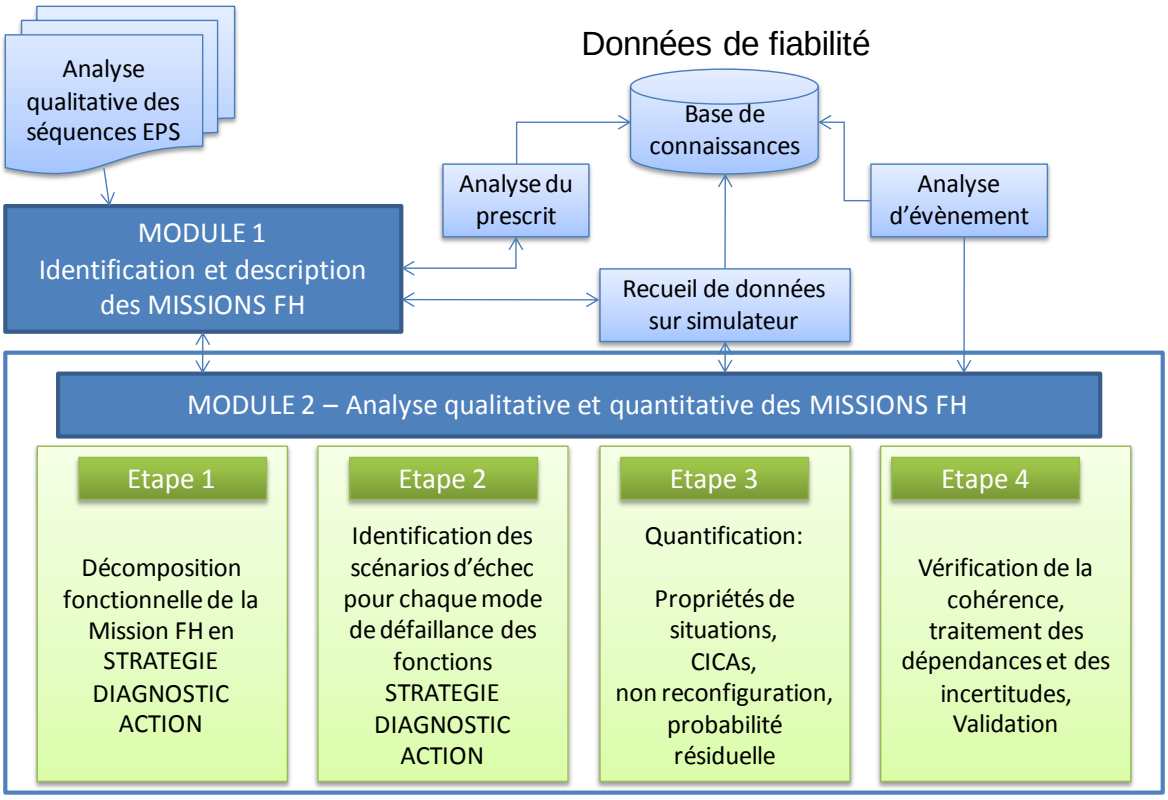


Figure 24 : Processus de la méthode MERMOS

La méthode se compose des deux modules suivants :

Module 1 - L'identification et la définition des missions facteur humain (missions FH)

L'identification et le screening des missions FH ont été en effet réalisés en amont lors de la réalisation de l'étude probabiliste de sûreté.

La définition des missions FH est structurée selon les quatre étapes suivantes :

- Étape 1 : analyse du requis, i.e. l'exigence fonctionnelle de la mission ;
- Étape 2 : analyse de la conduite prescrite, i.e. les procédures et les détails techniques de la mission ;
- Étape 3 : examen des essais sur simulateur ou d'autres sources de retour d'expérience et définition des exigences temporelles T0, T1, T2 :
    - à T0 : la mission est requise du point de vue des EPS,
    - à T1 : une information disponible en salle de commande permet de savoir que la mission est requise,
    - à T2 : les actions pour la mission sont lues dans les consignes.
- Étape 4 : élaboration de la fiche de mission facteur humain (FH)

À partir de l'analyse fonctionnelle de l'état de la centrale après l'initiateur, les caractéristiques de chaque mission FH et leur contexte sont décrits sous un format standard. Il est nécessaire de le vérifier et de l'enrichir avec des éléments provenant d'autres sources d'information telles que les procédures d'opération d'urgence et les rapports des simulateurs.

Module 2 - L'analyse qualitative et quantitative des missions FH

Le but de l'analyse qualitative MERMOS est d'identifier le plus grand nombre de scénarios possibles menant à l'échec de la mission HF. Cette étape est réalisée sous forme d'une revue AMDEC collective pour identifier les scénarios et les CICAs associées à travers une analyse des modes de défaillances des fonctions « Stratégie », « Action » et « Diagnostic ». Chaque mission FH doit être décomposée en ces trois fonctions SAD. Ensuite, pour chaque fonction il faut identifier l'ensemble des scénarios d'échec de la mission à travers une analyse des modes de défaillance.

L'échec de la mission se produit si l'un des scénarios décrits dans l'analyse quantitative se produit et conduit à l'échec. Les scénarios de défaillance d'une mission sont un ensemble d'événements qui sont exclusifs. La probabilité d'échec d'une mission est donc la somme des probabilités d'occurrence de chacun des scénarios décrits pour une mission.

Ce module se déroule selon les étapes suivantes [68]:

- Étape 1 : Décomposition fonctionnelle de la mission FH en trois fonctions SAD : STRATEGIE – ACTION - DIAGNOSTIC
    - Requis du point de vue de la STRATEGIE :
        - Identification des objectifs de la mission.
        - Identification des moyens possibles pour aboutir au critère de succès.
    - Requis du point de vue de l'ACTION:
        - Identification des actions nécessaires et suffisantes pour le succès de la mission
        - Détermination des séquences requises si nécessaire
    - Requis du point de vue de du DIAGNOSTIC :
        - Identification des paramètres pertinents pour la mission
        - Identification de la nature de l'accident en cours
        - Identification des systèmes indisponibles pertinents pour la mission
        - Identification de l'évolution des paramètres pertinents
        - Identification des parades à envisager
        - Identification des parades à écarter
- Étape 2 : Identification des scénarios d'échec pour chaque mode de défaillance des fonctions SAD à l'aide de la méthode AMDEC.
- Étape 3 : Vérifications et précautions (disjonction des scénarios et indépendance des missions)
- Étape 4 : Quantification

Pour chaque scénario, il faut quantifier :

- Les propriétés de situations,
- Les CICAs,
- La non reconfiguration (i.e. la survenue du scénario suite à un maintien des CICAS pendant une certaine durée),
- La probabilité résiduelle $P_{résiduelle}$

  $P_{résiduelle} = K \times Prb$

  Prb est la probabilité résiduelle de base d'échec d'une mission = 10^{-5}

  K représente la spécificité de la mission (l'influence de ses propriétés structurelles : délai, indisponibilités, réticence…)

  K = 10 si leur influence est très pénalisante

  K = 3 si leur influence est moyennement pénalisante

  K = 1 si leur influence est peu pénalisante

  Donc, la valeur de la probabilité résiduelle $P_{résiduelle}$ peut varier entre 10^{-5} et 10^{-4}. En pratique, si $\sum_{i=1}^{nbescidentifiables} P(scénario_i) > 10^{-2}$ alors on prend $P_{résiduelle} = 10^{-4}$.

- Étape 5 : Mise en cohérence des résultats

La probabilité de survenance de l'échec de la mission, pour un scénario, peut être estimée à partir de la probabilité d'occurrence de chaque événement dans le scénario. La quantification est basée sur le recueil et le jugement d'experts. MERMOS propose quatre catégories de probabilité génériques:

Très peu probable	: 0,01
Peu probable	: 0,1
Probable	: 0,3
Très probable	: 0,9

Données d'entrée (input)

- Analyse quantitative des séquences EPS.
- Les données de fiabilité provenant des observations sur les simulateurs avec l'application du principe de la méthode TRC [68] ou HCR [64].
- Les jugements d'expert sont utilisés dans de nombreuses situations.
- Les données de fiabilité génériques de THERP sont utilisées en cas d'absence de données d'observations sur les simulateurs ou sur site.

Résultats (output)

Les tableaux d'analyse des scénarios d'échec.

La probabilité d'échec des missions HF.

Domaine d'application

Nucléaire : pour les études de sûreté des EPR.

Validation

La méthode MERMOS est utilisée par EDF. Cependant, l'utilisation de cette méthode est limitée dans le cadre des études menées par EDF.

Commentaires

Les points forts :

- MERMOS est une méthode ad 'hoc, elle tente d'approcher la réalité des opérations et situations.
- Les données de fiabilité sont basées principalement sur des observations sur simulateur de tranche nucléaire (salle de conduite) et sur des jugements d'experts.
- L'identification des scénarios d'échec de la mission pour chaque mode de défaillance des fonctions SAD aide à l'identification des scénarios possibles.
- La méthode permet de mieux connaître la réalité des caractéristiques opérationnelles et les contraintes du système, car MERMOS demande une analyse fonctionnelle approfondie de la mission (objectif, critère de succès, définition des exigences temporelles, etc.). L'application de la méthode peut être un outil aux situations dégradées ou permettre de tester les procédures.
- MERMOS est une démarche globale d'appréciation des risques du système intégrant l'ensemble des éléments tels que les équipements, les procédures, l'organisation et les facteurs humains.

Les points faibles :

- Peu d'informations sont disponibles sur la méthode et ses applications.
- Peu d'éléments sont disponibles pour aider à l'identification des modes de défaillance fonctionnelle des fonctions SAD, des CICAs, des caractéristiques de situation et de la non reconfiguration.
- La quantification est basée principalement sur des données spécifiques des installations EDF.
- Il est difficile d'obtenir l'indépendance des scénarios. Par exemple, il est difficile de prouver l'indépendance entre les fonctions « Stratégie » et « Diagnostic ». Ainsi, les scénarios conduisant à l'échec de la fonction « Stratégie » présentent souvent les liens avec les scénarios menant à l'échec de la fonction « Diagnostic ».
- Pour obtenir l'exigence d'indépendance des scénarios, il est possible d'éliminer de nombreux scénarios élémentaires pour ne retenir que quelques scénarios caractérisés par des éléments contextuels très particuliers. Cette pratique peut conduire à des résultats très optimistes. L'exemple d'application de cette méthode illustre ce point.
- L'utilisation de la méthode demande des ressources importantes en temps.
- La mise en œuvre de la méthode exige de très bonnes connaissances en FH.
- La méthode ne propose pas d'outils de représentation (sous forme d'arbre d'événement, d'arbre de défaillance ou d'autres types de schéma) des scénarios.

- Selon la formule de calcul de MERMOS, plus le nombre d'éléments contextuels (ou de propriété de situation) d'une CICA augmente, plus la probabilité du scénario diminue. En revanche, la probabilité conditionnelle d'une CICA augmente lorsque le nombre d'éléments contextuels augmente. Cependant, cette augmentation ne compense pas dans de nombreux cas la rareté de la situation.

ANNEXE 10 : La méthode SHERPA

Fondement

La méthode SHERPA (Systematic Human Error Reduction and Prediction Approach) a été développée par Embrey en 1986 [30]. C'est une technique structurée d'identification des erreurs humaines pouvant survenir lors de l'exécution des tâches. Elle a aussi pour but d'identifier des solutions potentielles permettant de prévenir les erreurs et de limiter leurs effets.

Cette technique est basée sur une taxonomie des erreurs humaines.

La méthode SHERPA a été créé initialement pour l'industrie de procédé, telle que les centrales nucléaires, les procédés pétrochimiques et pétroliers, les extractions du pétrole et du gaz, la distribution d'énergie [30]. Cependant, comme cette méthode a un caractère générique, elle peut être utilisée dans tous les domaines. Des exemples d'application de SHERPA son disponibles dans lesquelles sont analysées des procédures ou des opérations, telles que la procédure de remplissage du chlorine dans le camion-citerne [56], la procédure de programmation d'un enregistrement de vidéocassette [14], [79], le guichet automatique [84].

Le principe de la méthode peut être illustré par la Figure 25.

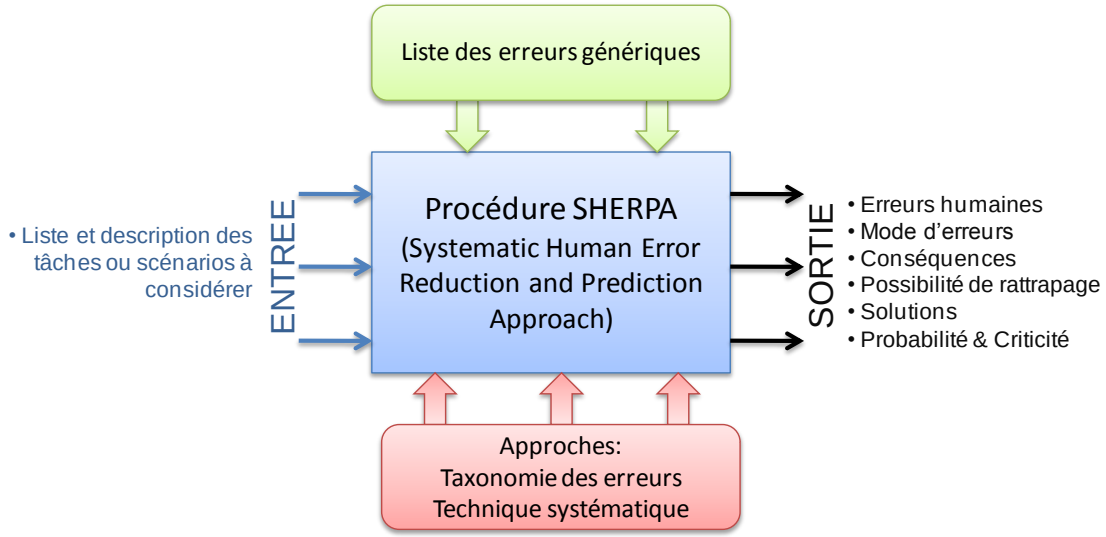


Figure 25 : Principe synthétique de la méthode SHERPA

Procédure

La procédure d'application de la méthode peut être présentée par les étapes suivantes:

Étape 1 : Analyse hiérarchisée de tâche (HTA – Hierarchical Task Analysis)

Cette analyse de tâche est basée sur une hiérarchisation des objectifs, des opérations (activités à exécuter pour atteindre les objectifs) et des plans ou procédures (séquence des opérations). Cette démarche a été étudiée et proposée par Annett et Duncan [10], [11]. Ensuite, elle a été mentionnée dans de nombreux travaux [58], [81], [49].

La structure hiérarchisée de l'analyse permet d'approfondir le niveau de détail si nécessaire. Donc, l'analyse commence à partir du niveau de l'objectif global de la tâche, qui est ensuite divisé en objectifs élémentaires plus détaillés. Parallèlement, les plans doivent être mentionnés pour indiquer la séquence d'exécution des activités élémentaires. La décomposition de tâche peut être continue jusqu'à un niveau suffisamment détaillé et compréhensif.

Étape 2 : Classification de tâche

Cette étape consiste à répartir les tâches les plus élémentaires identifiées à l'étape précédente parmi les familles de tâches suivantes :

- Acquisition (par exemple, acquisition d'information auditive, visuelle ou tactile)
- Sélection (par exemple, sélection d'un objet, d'une solution ou d'une action parmi des alternatifs disponibles)
- Action (par exemple, appuyer sur un bouton, ouvrir ou fermer une porte ou une vanne, etc.)
- Vérification (par exemple, réaliser une vérification procédurale)
- Communication (par exemple, communiquer, discuter ou parler à d'autres équipes)

Étape 3 : Identification des erreurs humaines

Cette étape consiste à identifier le mode d'erreur crédible pour chaque tâche élémentaire à l'aide d'une taxonomie d'erreur et de la classification de tâche réalisée à l'étape précédente.

Tableau 33: Taxonomie d'erreurs de SHERPA

Classification de tâche	Mode d'erreur	Description
Action	A1	Action trop longue / trop courte
	A2	Action trop tôt / trop tard
	A3	Action dans mauvaise direction
	A4	Action trop faible / trop forte
	A5	Désalignement (mauvais ordre ou séquence)
	A6	Bonne action sur mauvais objet
	A7	Mauvaise action sur bon objet
	A8	Action omise
	A9	Action incomplète
	A10	Mauvaise action sur mauvais objet
Vérification (Checking (C))	C1	Vérification omise
	C2	Vérification incomplète
	C3	Bonne vérification sur mauvais objet
	C4	Mauvaise vérification sur bon objet
	C6	Mauvaise vérification sur mauvais objet

Classification de tâche	Mode d'erreur	Description
Acquisition (Retrieval (R))	R1	Information n'est pas obtenue
	R2	Acquisition de mauvaise information
	R3	Acquisition d'une information incomplète
Communication (Information (I))	I1	Information n'est pas communiquée
	I2	Communication d'une mauvaise information
	I3	Communication incomplète
Sélection (S)	S1	Sélection omise
	S2	Mauvaise sélection

Étape 4 : Analyse des conséquences

Les conséquences associées à chaque erreur identifiée doivent être analysées. Cela permettra de déterminer la criticité de chaque erreur.

Étape 5 : Analyse de rattrapage

Cette étape consiste à identifier les rattrapages potentiels pour chaque erreur identifiée.

Étape 6 : Analyse de probabilité

Cette étape consiste à estimer la probabilité d'occurrence de l'erreur identifiée. La probabilité est classée en trois catégories :

- Faible ou rare (L – Low)
- Moyenne ou occasionnelle (M – Medium)
- Élevée ou fréquente (H – High)

Cette évaluation est basée sur le retour d'expérience (données de fiabilité) ou sur l'avis d'expert.

Étape 7 : Analyse de criticité

La criticité est basée plutôt sur les conséquences perçues. Généralement, si l'erreur peut conduire à des dommages importants liés aux installations, de l'environnement ou à la vie des personnels, elle peut être évaluée comme critique. La criticité est classée aussi en trois catégories :

- Faible (L – Low)
- Moyenne (M – Medium)
- Élevée ou critique (H – High)

Étape 8 : Analyse de mesure de réduction des risques

Cette dernière étape consiste à proposer des stratégies de réduction d'erreurs. Ces mesures peuvent être des changements du système de travail pouvant prévenir l'apparition de l'erreur ou limiter les conséquences. Les stratégies peuvent être regroupées en quatre catégories suivantes :

- Équipements : Modifier des équipements ou procédés existants.
- Entrainement ou formation : Créer ou modifier le programme de formation.
- Procédures : Améliorer ou créer des nouvelles procédures.
- Organisation : Changer la politique organisationnelle ou la culture.

Données d'entrée (input)

- Liste et description des tâches et des procédures.
- Description des équipements.

Résultats (output)

- Liste des erreurs, leurs conséquences et probabilité d'occurrence.
- Les moyens, les mesures de réductions de la probabilité d'occurrence et des conséquences des erreurs.

Domaine d'application

Tous domaines.

Validation

La méthode SHERPA est considérée comme la meilleure méthode d'identification des erreurs humaines par des experts [58], [85]. La fiabilité de la méthode augmente avec le niveau de l'utilisateur. Si la méthode est mise en pratique par un expert, la reproductibilité peut être très élevée, de l'ordre de 80% à 90%.

Commentaires

<u>Les points forts :</u>

- La procédure est très structurée et compréhensible pour la plupart des utilisateurs.
- La taxonomie est courte, synthétique et générique.
- La validation de la méthode est réalisée par des experts et les utilisateurs.
- L'apprentissage et l'application de la méthode sont simples et demandent peu de temps.
- La méthode SHERPA est compatible avec d'autres méthodes d'identification et d'évaluation qualitative des risques, telles que l'AMDEC, HAZOP, HAZID.

Les points faibles :

- La taxonomie est incomplète, par exemple la méthode n'aborde pas les activités cognitives telles que le diagnostic et la prise de décision, ou les défaillances organisationnelles ou systémiques.
- L'analyse de la probabilité n'est pas prise en compte dans l'analyse de criticité. Cette dernière n'est basée que sur les conséquences.
- La méthode exige une analyse de tâche HTA. Donc si cette dernière n'est pas faite, il faut prévoir un temps supplémentaire.
- Pour des tâches complexes, la méthode peut devenir fastidieuse et demande beaucoup de temps.
- La méthode partant d'une description de tâches et de la décomposition en sous tâche, elle ne s'appuie pas sur la réalité de l'activité de l'opérateur,
- La méthode ne prend pas en compte le travail dans son contexte opérationnel (multi-activité, pression temporelle, contraintes organisationnelles, travail en équipe, dépendance avec d'autres tâches…).

[105]

ANNEXE 11 : La méthode TRIPOD

Fondement

La méthode Tripod est basée sur un modèle de sécurité organisationnelle. Elle est le fruit d'un programme de recherche lancé par le groupe Royal Dutch / Shell au milieu des années 80. Les recherches ont été réalisées par différents experts de l'Université de Manchester (Royaume-Uni) et de l'Université de Leiden (Pays-Bas), tels que Reason, Wagenaar, Groeneweg, Roggeveen [34], [35].

La méthode Tripod s'intéresse particulièrement aux facteurs organisationnels et aux erreurs latentes (actions erronées ayant des conséquences différées par rapport au moment d'occurrence de l'action – typique des actions de maintenance). Ici encore, les erreurs de l'opérateur sont des sources directes de risque, mais c'est l'organisation qui est considérée comme l'élément fondamental de sa performance. Les erreurs humaines et leurs conséquences apparaissent comme les résultats d'un environnement organisationnel défaillant. Les erreurs commises par les opérateurs s'inscrivent dans des conditions ou des contextes provenant de mauvaises décisions d'autres acteurs tels que des managers, cadres, ingénieurs, etc. Afin de traiter à la source des problèmes, il faut donc identifier des facteurs organisationnels favorisant l'erreur de l'opérateur, comme les conditions de travail, la formation, l'équipement technique, les modes de coopération et de coordination, etc.

La méthode Tripod est basée sur un modèle de l'accident où l'organisation joue un rôle important (offrant les conditions de l'accident).

Modèle Tripod de l'accident

Dans ce modèle, la séquence accidentelle est vue comme la résultante de mauvais processus de décision et de gestion en amont. Ces mauvaises décisions peuvent être considérées comme les résultats des pressions économiques ou financières pesant sur l'organisation. Les mauvaises décisions de gestion introduisent des défaillances latentes. Ces défaillances latentes peuvent influencer la sécurité du système selon deux trajectoires accidentelles, illustrées par la Figure 26 [35].

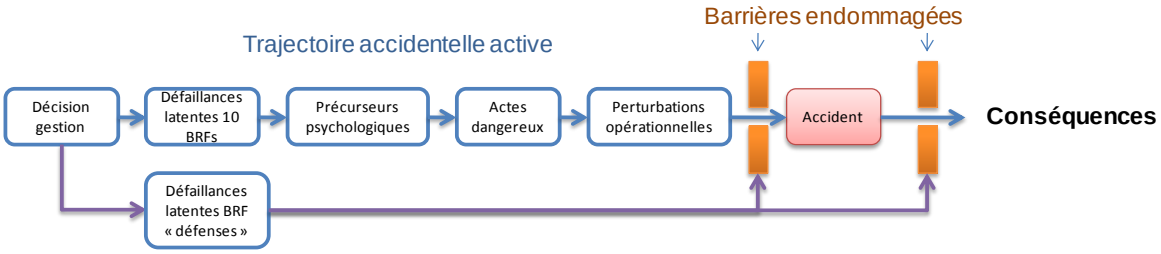


***Figure 26** : Modèle Tripod de l'accident*

Modèle organisationnel Tripod

Au lieu de s'attaquer aux perturbations opérationnelles ou aux actes dangereux comme la plupart des méthodes existantes, Tripod remonte jusqu'aux défaillances latentes initiatrices de séquences accidentelles. Ces défaillances latentes peuvent être regroupées en onze facteurs types de risques, appelés « Basic Risk Factors » (BRF) [35], et donnés dans le Tableau 34.

Tripod distingue les facteurs types de risques BRFs en trois catégories :

- Les facteurs BRFs préventifs génériques indépendants de l'activité qui sont applicables à tout type d'environnement (tels que la communication, la formation, etc.). Ces facteurs concernent plutôt des aspects de management.
- Les facteurs BRFs préventifs spécifiques aux activités, aux opérations et de la nature du système organisationnel étudié, tels que la conception d'équipements, le matériel utilisé, la conduite de la maintenance, etc. Ces facteurs concernent plutôt de la maîtrise opérationnelle.
- Le facteur BRF de protection qui regroupe l'ensemble des équipements et dispositifs de protection visant à mitiger les conséquences d'un accident, par exemple : équipements de protection, système d'alarme, plans de secours, extincteurs, etc.

Selon Tripod, ces facteurs BRFs peuvent contribuer à générer des actes dangereux et des perturbations opérationnelles et à affaiblir les barrières de défense. L'objectif de la maitrise des risques est alors de diminuer voire d'éliminer les différents impacts de ces onze BRFs.

Tableau 34: Facteurs types de risques de Tripod

Facteurs types de risques BRF		**Descriptif**
BRFs préventifs génériques	Procédures (PR)	Disponibilité, clarté, mise à jour, pertinence, utilité des procédures, instructions et modes opératoires.
	Formation (FO)	Planification, coordination et efficacité des formations. Expériences professionnelles des individus.
	Communication (CM)	Qualité de la communication entre employés, départements ou sites en termes de disponibilité, des moyens et d'efficacité des canaux de communications.
	Objectifs Incompatibles (OI)	Façon dont la sécurité est gérée par rapport à d'autres objectifs : contraintes de temps, limitation de budget, etc.
	Organisation du travail (OT)	Organisation structurelle, philosophie de l'organisation, répartition des tâches, définition des responsabilités, de la ligne hiérarchique.
BRFs préventifs spécifiques	Conception (CP)	Qualité de la conception de lieu de travail, équipements et matériaux en termes d'ergonomie et de fonctionnalité.
	Matériel (MT)	Qualité, état, disponibilité. des outils et équipements.
	Maintenance (MN)	Planification, qualité et conduite des activités de maintenance et de réparation.
	Ordre et Propreté (OP)	Ordre, rangement des différents espaces de travail.
	Circonstances causant des erreurs (CE)	Qualité de l'environnement de travail en termes de luminosité, niveau sonore, température ambiante mais aussi en termes d'ambiance de travail entre les individus.
BRF de protection	Défenses (DF)	Disponibilité et efficacité des équipements de protection et des mesures de protection.

Il existe deux outils méthodologiques de Tripod :

- L'outil Tripod Beta pour chercher a posteriori les causes organisationnelles d'un accident, et
- L'outil Tripod Delta pour identifier les défaillances organisationnelles d'un système industriel afin d'anticiper la survenue d'accidents.

Dans le but de prévenir les accidents majeurs, cette étude se limite à l'outil Tripod delta [35]. Le terme « Tripod » sera utilisé pour désigner « Tripod Delta ».

Tripod a pour but de caractériser l'environnement de travail par des indicateurs des onze facteurs BRFs mentionnés ci-dessus. Ces indicateurs peuvent être obtenus et renseignés via une enquête ou des entretiens individuels anonymes réalisés auprès de l'ensemble des membres de l'organisation (y compris la direction et les sous-traitants ou les intérimaires).

Cette enquête Tripod s'appuie sur une liste de questionnaires préétablis. Les questions Tripod sont de type fermé (les réponses possibles sont « Oui » ou «Non ». Elles sont fondées sur des faits précis et observables. Les questions types élaborées par l'Université de Leiden ont été regroupées dans une base de questions « Delta base ». Généralement, environ 25 questions sont nécessaires pour évaluer chaque facteur BRF. Cependant, le nombre de questions peut varier selon le profil de l'entreprise, des services ou bien selon les acteurs. Il est recommandé d'utiliser plus de 75% des questions de la Delta Base pour assurer la validité et fiabilité du questionnaire utilisé. L'échantillon analysé doit être assez large (au minimum 40 personnes [22]).

Un exemple de questions concernant le facteur BRF « Communication » est proposé ci-après [21]:

- La direction communique-t-elle de façon claire ses objectifs en matière d'hygiène, santé et sécurité au travail ?
- Votre hiérarchique laisse-t-il tout le monde s'exprimer librement ?
- Au cours des trois derniers mois, vous est-il arrivé de vous rendre à une réunion et d'apprendre sur place que celle-ci était annulée ?

L'indicateur de chaque facteur BRF est le pourcentage moyen de réponses obtenues « Oui » ou « Non » sur l'ensemble du groupe interrogé et sur l'ensemble des questions concernées. La Figure 27

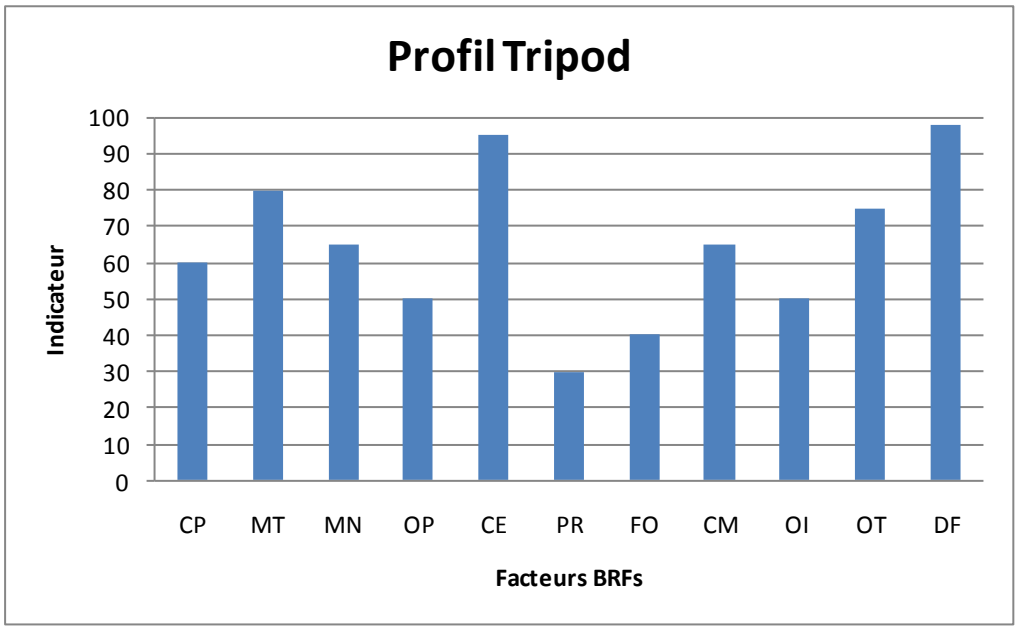


Figure 27 : Exemple du profil Tripod

Dans cet exemple, les points critiques se trouvent pour les facteurs PR (procédure) et FO (Formation). L'entreprise a l'intérêt d'améliorer ces points faibles.

Le principe de la méthode Tripod peut être illustré par la Figure 28.

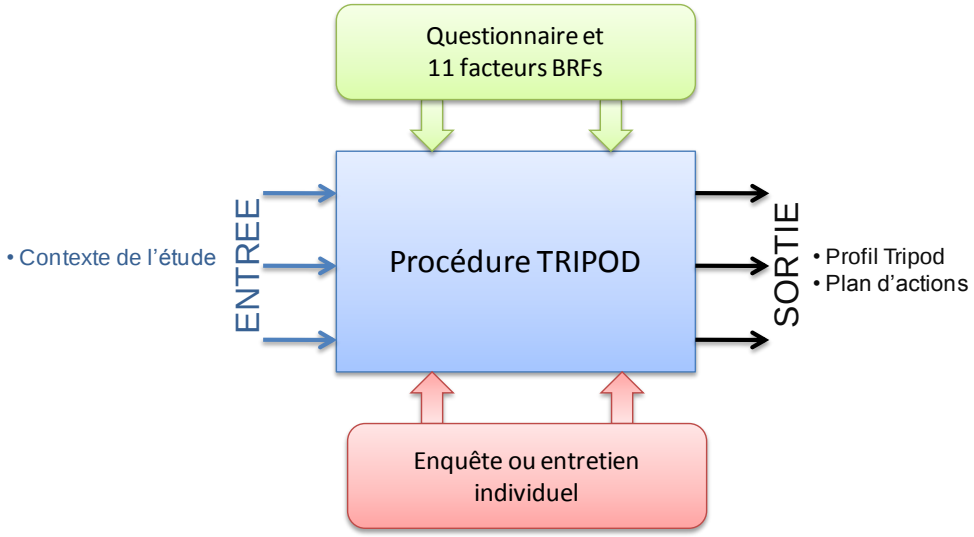


Figure 28 : Principe synthétique de la méthode Tripod

Procédure

La procédure d'application de la méthode Tripod peut être synthétisée par les quatre étapes successives suivantes :

Étape 1 : Préparation de l'étude

Cette étape comprend les activités suivantes :

- Organiser des réunions, par exemple la réunion de lancement de l'étude et celle de la préparation de l'enquête.
- Définir le périmètre de l'étude et l'équipe de l'étude
- Informer les personnels dans le périmètre de l'étude
- Choisir et adapter les questions da la base « Delta Base » aux contextes du site. Créer de nouvelles questions si nécessaire.
- Découper le site en sous-systèmes organisationnels homogènes.
- Définir les conditions de mise en œuvre de l'enquête :
  - Information du personnel : par lettre d'information ? par réunion de service ? par affichage ? par session d'information ?
  - Moyens de diffusion des questionnaires : par chef de service ? par courrier au domicile du salarié ? par le responsable sécurité ? par le CHSCT ?
  - Moyens de collecte des questionnaires : par chef de service ? par le responsable sécurité ?

Étape 2 : Collecte des informations

Cette étape concerne :

- la diffusion des instructions relatives à l'enquête,
- la diffusion des questionnaires à l'ensemble des personnels,
- la collecte des réponses aux questionnaires.

Étape 3 : Validation des réponses et Analyse des résultats

Cette étape comprend le traitement des réponses aux questionnaires et leur validation statistique. Cette étape permet de déterminer le profil Tripod qui indique des points forts ainsi que des défaillances latentes dans l'entreprise.

Étape 4 : Interviews et proposition d'actions correctives

Cette étape concerne les entretiens avec la direction de l'entreprise afin :

- d'analyser les points faibles et leurs causes profondes, et
- de proposer un plan d'actions pour améliorer les situations.

Données d'entrée (input)

- Contexte de l'étude.

Résultats (output)

- Les profils Tripod.
- Un plan d'actions.

Domaine d'application

Tous domaines.

Validation

La méthode a été le sujet de nombreuses études [22]. L'outil Tripod Delta semble être acceptée par un grand nombre d'utilisateur dans le monde. La méthode a été appliquée dans différents secteurs d'activité (pétrolier, ferroviaire, maritime, chimique, pétrochimique, administratif, fabrication, nucléaire) ainsi que dans différents environnements culturels anglo-saxons français, scandinaves et asiatiques [21], [22]. Cependant, nous n'avons pas de preuves pour valider cette constatation. La méthode Tripod est plutôt une méthode de sondage sur l'environnement de travail qu'une méthode d'évaluation de la fiabilité humaine.

Commentaires

Les points forts :

- L'application de la méthode et l'analyse des résultats sont simples.
- Le résultat est basé sur l'avis d'un grand nombre d'acteurs, cela permet de réduire la sensibilité de la méthode par rapport aux autres méthodes d'évaluation de la fiabilité humaine (ici on parlerait plutôt de fiabilité organisationnelle).
- La méthode présente des effets positifs sur les salariés, car ils pensent que leurs avis sont considérés dans le management de l'entreprise.
- La méthode permet de traiter à l'origine les causes d'actions opérationnelles potentiellement dangereuses en évitant le processus simplificateur de focalisation sur l'opérateur. La chaîne causale est enrichie.

Les points faibles :

- La méthode traite de façon générale de l'environnement organisationnel de travail. Elle peut donc être utile pour le management global de l'entreprise. Cependant comme elle ne se focalise pas sur les actions a priori identifiées comme dangereuses, elle ne permet pas d'entrer dans le détail d'un scénario d'accident.
- La méthode n'aborde pas les caractéristiques particulières de la tâche. Si la situation d'exécution d'une tâche donnée est très particulière par rapport aux environnements généraux de l'entreprise, la réflexion risque de ne pas prendre en compte cette spécificité.
- La méthode n'est pas adaptée pour être intégrée dans les études probabilistes de sûreté et de risque.
- Peu d'informations sont disponibles sur la liste des questions. Cela rend la méthode très difficile à mettre en œuvre sans la mobilisation d'une expertise FH pour la conception des questionnaires.
- De plus, même avec une liste indicative de départ, l'adaptation à l'entreprise et métiers visés exige des ressources importantes.

- Il existe des problèmes concernant l'échantillonnage. La méthode recommande un échantillon d'au minimum 40 personnes, ce qui est trop peu pour une analyse statistique poussée. La méthode peut permettre une analyse statistique descriptive ou une analyse qualitative surtout dans les petites entreprises ou petits services, ce qui requiert une expertise FH spécifique.
- Le recours au questionnaire est pratique mais ne pourra pas prendre en compte les différences entre services. Le questionnaire devra donc rester très générique et les résultats risquent de passer à côté d'élément de contexte essentiel vis-à-vis de la sécurité. Il est en effet très probable que les conditions organisationnelles ne soient pas homogènes entre différents services d'une l'entreprise.

ANNEXE 12 : La méthode ACIH

Fondement

L'infiabilité humaine est associée à la notion de dérive comportementale (c'est-à-dire définie par rapport à ce qui doit être fait) et/ou situationnelle (c'est-à-dire définie par rapport à ce qui doit être obtenu) [98].

La méthode ACIH (Analyse des Conséquences de l'Infiabilité Humaine) est une démarche d'analyse de l'erreur humaine sur une situation de travail donnée en se focalisant particulièrement sur les conséquences de l'erreur [98].

Les premières démarches ont été développées à la fin des années 90 par F. Vanderhaegen [96], [97] pour déterminer les différentes étapes d'une analyse préliminaire des conséquences de l'infiabilité humaine pour un critère de performance donné.

La méthode ACIH existe en deux versions :

- La méthode APRECIH (analyse préliminaire des conséquences de l'infiabilité) est la version prospective d'analyse et permet de comparer les comportements prescrits (la tâche) avec les comportements réels obtenus par prédiction (imaginés).
- La méthode APOSCIH (analyse a posteriori des conséquences de l'infiabilité) est la version rétrospective et permet de comparer les comportements prescrits avec les comportements réels obtenus par observations sur le terrain. Cette méthode est appliquée pour analyser des incidents/accidents.

Ces deux méthodes ont été basées sur les modèles issus de la psychologie cognitive pour analyser les conséquences de l'infiabilité humaine sur les performances du système homme-machine, en déterminant les causes des dégradations des comportements humains ou du système [99]. Elles ne prennent pas en compte la fréquence d'occurrence des erreurs humaines.

Selon la méthode, l'infiabilité humaine et l'erreur humaine peuvent-être exprimées en termes de dégradation du comportement humain [99]. Ces actions humaines erronées provoqueront à leur tour des dégradations dans le système.

La démarche comprend différentes étapes d'analyse. Un modèle de gestion des situations permet de distinguer celles-ci par rapport à des dérives comportementales et des dérives situationnelles. L'analyse des conséquences est ensuite réalisée sur les dérives comportementales identifiées, en termes de bénéfice, de coût, de dégradation ou d'amélioration en comparant une situation cible à une situation source.

Modèle de gestion de situations

Le modèle de gestion de situations établit des liens entre les dérives situationnelles et comportementales. Une dérive situationnelle peut être le résultat d'une dérive comportementale de l'opérateur humain ou la conséquence d'événements externes, indépendants du comportement de celui-ci. Le modèle de gestion permet d'identifier les différentes dérives situationnelles possibles dues à l'opérateur humain, ainsi que leur propagation au cours des différents stades comportementaux de la résolution de problème [91]. Les mécanismes de propagation de telles erreurs sont illustrés par la Figure 29 [92] :

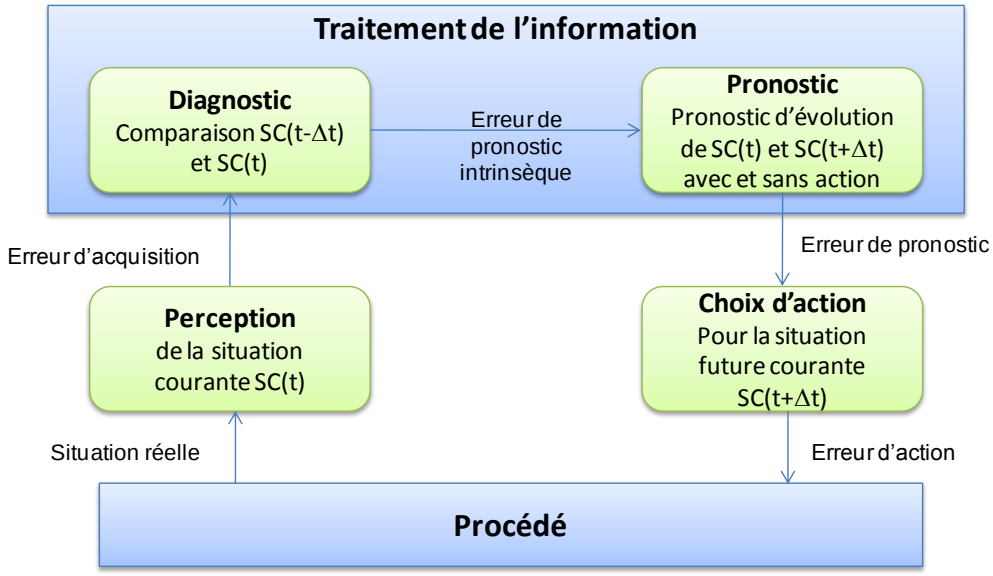


Figure 29 : Modèle de gestion de situations

La propagation intra-individuelle d'une erreur se réalise de différentes manières selon les trois niveaux d'occurrence d'erreur : l'acquisition, le traitement de l'information, ou l'action.

Une erreur sur un niveau peut générer une autre erreur dans le même niveau ou dans un autre niveau. Une erreur peut générer une séquence d'erreurs, etc.

La propagation d'une erreur humaine est non seulement interne à un agent cognitif humain ou technique, mais aussi externe (action de l'agent sur l'environnement technique ou humain).

La démarche générale de la méthode [98] est présentée dans la Figure 30.

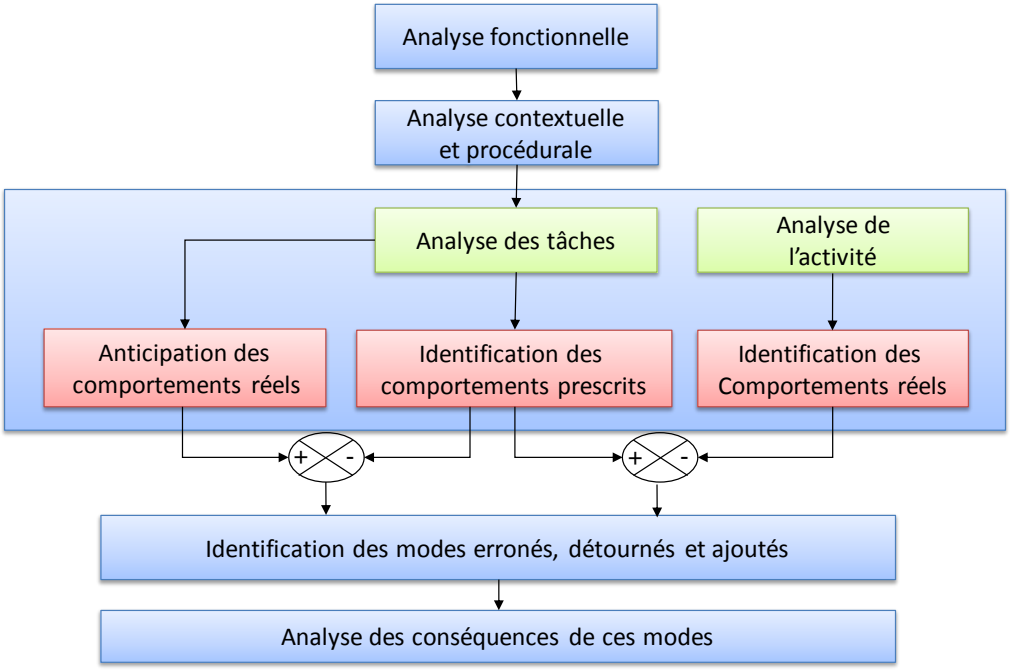


Figure 30 : Démarche pour l'analyse des conséquences de l'infiabilité humaine (ACIH)

Le principe de la méthode ACIH peut être illustré par la Figure 31.

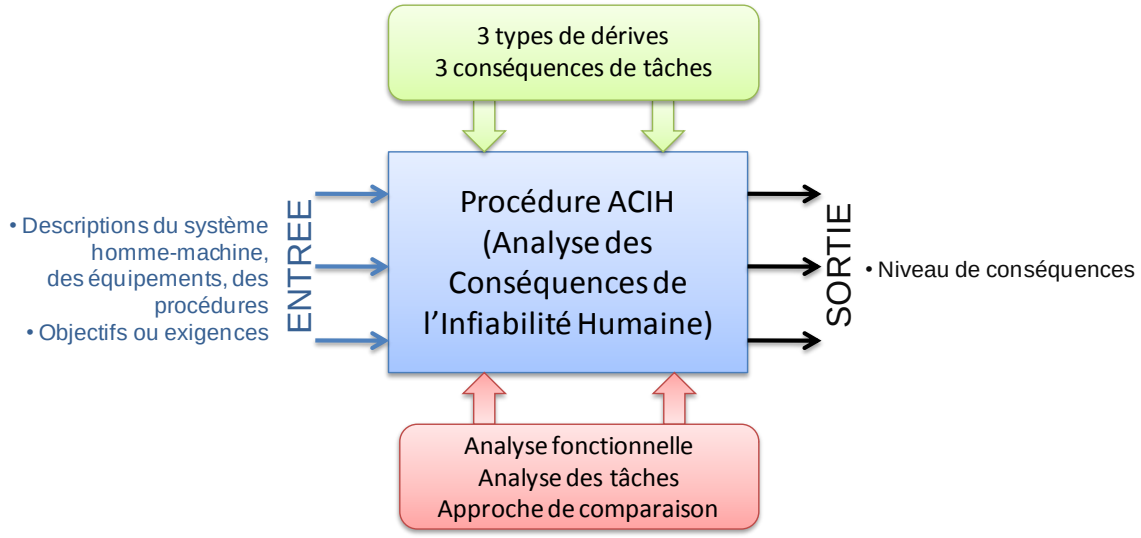


Figure 31 : Principe synthétique de la méthode ACIH

Procédure

Étape 1 : Analyse fonctionnelle du système homme-machine

Cette analyse a pour objectif d'identifier les fonctions du système et le rôle des opérateurs humains pour les réaliser. Les fonctions sont ensuite couplées avec les procédures décrivant des listes de tâches à réaliser en fonction du contexte. Le résultat est donné dans un tableau, illustré dans le Tableau 35.

Tableau 35: Interaction entre les procédures et les fonctions du système

Procédures	Fonctions			
	F1	F2	F3	F4
P1	1	1	1	1
P2	1	1	0	0
P3	1	1	0	0
P4	1	1	1	1

(0 : pas d'interaction ; 1 : interaction)

Étape 2 : Analyse procédurale et contextuelle

Cette étape consiste à identifier pour chaque procédure, les contextes associés et les tâches à réaliser dans ces contextes. Les contextes peuvent être des situations normales, des situations accidentelles ou d'autres situations particulières, etc. Par exemple, dans le domaine ferroviaire, on peut distinguer les situations normales, trafics denses, trains retardés, mouvements dangereux des trains, etc.

Étape 3 : Analyse des tâches et de l'activité

Cette étape se distingue entre les versions APRECIH et APOSCIH :

- Version APRECIH : L'analyse des tâches vise à déterminer les prescriptions et à anticiper les comportements réels à partir de dérives possibles pour une tâche donnée.
- Version APOSCIH : L'analyse de l'activité permet d'identifier les comportements réels.

Le modèle de gestion de situations présenté antérieurement permet de déterminer le type de comportement sollicité pour réaliser une tâche donnée et d'identifier les propagations possibles des dérives par rapport à la dépendance entre les tâches pour une procédure et un contexte donnés.

Étape 4 : Identification des caractéristiques de tâches ou des modes de dérives comportementales

Cette étape est différente selon les versions APRECIH et APOSCIH.

Selon la version APRECIH, cette étape consiste à identifier les caractéristiques de tâches.

La méthode a été basée sur un modèle d'infiabilité humaine comprenant trois types de défaillances:

- Défauts d'acquisition,
- Défaillances de traitement de l'information,
- Défaillances relatives aux actions.

Donc, cette étape consiste à associer chaque tâche à une des trois activités.

L'acquisition de l'information, le traitement de l'information et l'action peuvent être réalisés correctement, incorrectement ou ne sont pas réalisés du tout, c'est-à-dire omis.

Selon la version APOSCIH, cette étape consiste à comparer les comportements prescrits avec les comportements réels ou anticipés pour identifier trois classes de modes de dérives :

- Les modes erronés,
- Les modes détournés, et
- Les modes ajoutés.

En prenant l'hypothèse qu'il n'y a pas d'erreur de prescription, les modes de dérive sont des écarts entre le comportement réel ou anticipé des opérateurs et celui prescrit par le concepteur. La détermination de ces modes de dérive est illustrée par la Figure 32.

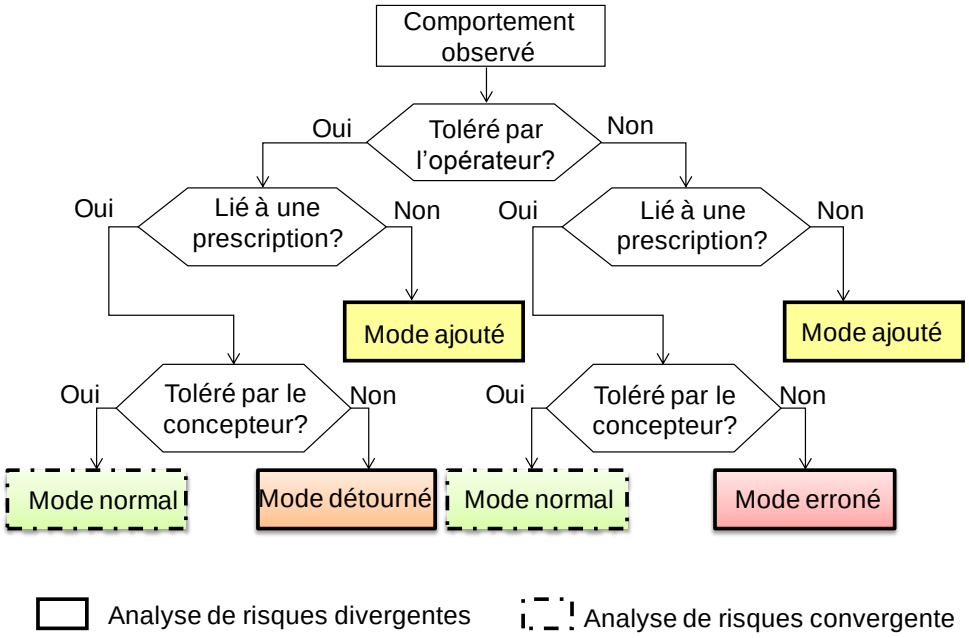


Figure 32 : Technique d'identification des modes de dérive

Étape 5 : Analyse des conséquences

Cette étape finale consiste à coupler les modes d'infiabilité humaine et leurs impacts sur le système, pour une procédure donnée associée à son contexte, et également pour une combinaison de procédures associées au même contexte.

On observe deux démarches rapportées pour cette étape.

Démarche 1 : Cette démarche a été présentée dans les premières publications de la méthode [97], [99]. L'analyse des conséquences consiste à établir les scénarios possibles des états des tâches pour chaque procédure et à combiner leur conséquence. Au niveau global, la méthode distingue trois niveaux de conséquences pour un scénario :

- Niveau 0 : pas de conséquence
- Niveau 1 : conséquence problématique
- Niveau 2 : conséquence catastrophique

Le niveau de conséquences est évalué par avis d'expert pour chaque scénario.

Démarche 2 : Les conséquences des dérives peuvent être estimées en comparant les gravités d'une situation prescrite avec celles d'une situation observée ou de dérive en termes d'amélioration / dégradation ; bénéfice / coût ; ou déficit / tolérance / reprise [98]. Par rapport à la procédure prescrite, les valeurs des bénéfices, des déficits potentiels, des maîtrises et pertes de contrôle peuvent être calculées pour chacune des procédures déviées par simulation ou par observation sur site.

Données d'entrée (input)

- Descriptions du système homme-machine, des équipements, des procédures.
- Objectifs ou exigences.

Résultats (output)

- Niveau de conséquences
- ou le gain / la perte

Domaine d'application

Tous domaines

Validation

Aucune information de validation de la méthode n'est disponible. Cette méthode a été appliquée pour évaluer certaines situations de circulation dans le domaine ferroviaire [97], [99].

Commentaires

Les points forts :

- La méthode ACIH peut être adaptée pour évaluer des situations de travail, où les contextes peuvent être changés couramment comme dans le domaine des transports.
- Cette méthode permet de faire le point sur les modes d'adaptation (appelé ici mode de dérive) mis en œuvre ou pouvant être mis en œuvre par les opérateurs. Et ainsi de réfléchir à leur pertinence selon les contextes opérationnels ou l'évolution organisationnelle et technique du système.
- La cartographie des modes d'adaptation (ici appelé de dérives) peut être utilisée pour préparer le transfert de compétence dans des situations de renouvellement générationnel des opérateurs.

Les points faibles :

- La méthode ne propose pas des moyens concrets pour évaluer le niveau des conséquences. En effet, le niveau des conséquences est évalué par avis d'expert. Un groupe de travail pourrait être plus efficace.
- La détermination des conséquences en terme d'amélioration / dégradation ; bénéfice / coût ; ou déficit / tolérance / reprise demande des ressources assez importantes afin d'obtenir des résultats satisfaisants.
- L'absence d'évaluation probabiliste des scénarios supposés pose des problèmes pour l'intégration de la méthode dans des démarches classiques (technique) d'étude de danger.
- La méthode demande de déterminer l'activité dominante pour chaque tâche en trois catégories « acquisition de l'information », « traitement de l'information » et « action ». Or il n'est pas toujours facile de séparer ces activités cognitives pour une tâche donnée, étant parfois juxtaposées. Ici encore une expertise FH peut être requise pour un découpage correct.

- Si la procédure comprend un grand nombre d'étapes ou d'états possibles, le nombre des scénarios peut être très important. Par exemple, le nombre des scénarios possibles pour une procédure de 5 tâches seulement est environ de 500 ; le nombre des scénarios pour une procédure de 10 tâches est d'environ 3. 10^{15}. Donc la méthode ne peut être déployée de manière exhaustive. Des choix importants sont à faire pour échantillonner les tâches à traiter (principe du sondage).
- D'autre part, l'évaluation des conséquences est assez grossière car leurs caractérisations sont réparties qu'en trois catégories 0, 1 et 2.

ANNEXE 13 : La méthode FRAM

Fondement

La méthode FRAM (Functional Resonance Analysis Method) a été développée par Hollnagel en 2004 [45]. Initialement FRAM était l'acronyme de Functional Resonance Analysis Model. La méthode FRAM permet de décrire le système sociotechnique par ses fonctions et ses activités plutôt que par sa structure. L'objectif de FRAM est de représenter la dynamique du système par la modélisation des dépendances non linéaires qu'elle contient et par une représentation originale de la performance des fonctions et des activités. Le modèle de dépendance repose sur le concept de résonance fonctionnelle emprunté à la physique ondulatoire, métaphore de la résonance stochastique. Le principe de résonance stochastique consiste en la surimposition d'un signal non linaire (bruit) sur un signal périodique de faible amplitude difficilement détectable. L'addition du bruit permet alors d'établir une résonance avec le signal de faible amplitude et de le rendre ainsi détectable. Hollnagel utilise la métaphore de l'émergence et de la résonnance pour expliquer l'apparition des accidents dans les systèmes sociotechniques complexes. Il justifie ce rapprochement vers l'étude de sécurité en s'appuyant sur la variabilité de la performance des fonctions ou des activités dans les systèmes sociotechniques.

La méthode FRAM est basée sur les quatre principes basiques suivants :

- **Le principe de l'équivalence de succès et d'échec**

  L'échec est généralement exprimé comme une panne ou un dysfonctionnement d'un système ou de ses composants. Ce point de vue suppose que le succès et l'échec sont d'une nature fondamentalement différente.

  L'ingénierie de Résilience reconnaît que les individus et les organisations doivent s'adapter à la situation dans toutes leurs activités.

  L'information, les ressources et le temps sont toujours précis (signal périodique de faible amplitude), tandis que les ajustements seront toujours approximatifs (bruit non linéaire).

  Le succès est dû à la capacité des organisations, groupes et individus de réaliser correctement ces ajustements, en particulier d'anticiper les risques avant que les défaillances et les dangers se produisent. Les échecs peuvent être compris comme l'absence temporaire ou permanente de cette capacité.

  L'objectif de l'ingénierie de la résilience est de renforcer cette capacité, plutôt que d'éviter ou éliminer les défaillances.

- **Le principe d'ajustement approximatif**

  Les objectifs de nombreux systèmes sociotechniques ne sont jamais totalement réalisables. Les conditions de travail ne correspondent jamais complètement à ce qui a été spécifié ou prescrit. Donc, les individus, les groupes, les organisations ajustent leurs performances pour répondre aux conditions réelles (les ressources, les exigences, les possibilités, les conflits, les interruptions…).

  Les ressources (le temps, la main-d'œuvre, l'information, etc.) étant souvent limitées, les ajustements sont souvent approximatifs plutôt que précis.

La variabilité des performances, dû à ces ajustements approximatifs, est donc l'origine des succès, mais aussi à l'origine des échecs.

- **Le principe de l'émergence**

  La variabilité de la performance normale est rarement assez grande pour être la seule cause d'un accident ou pour constituer un dysfonctionnement. Cependant la variabilité des fonctions multiples peut se combiner de manière inattendue pour conduire à des conséquences qui sont très importantes voire disproportionnées par rapport aux conditions de départ. C'est l'effet de la non-linéarité des relations entre les différents éléments fonctionnels. Les échecs sont souvent des émergences plutôt que des phénomènes répondant à une causalité simples, car ils ne peuvent pas être attribués ou expliqués en se référant uniquement aux mauvais fonctionnements de certains composants ou des pièces, et ne peuvent complètement être prédits à l'avance.

- **Le principe de la résonnance fonctionnelle**

  La variabilité d'un certain nombre de fonctions peut, de temps en temps, résonner, c'est à dire, se renforcer mutuellement et provoquer ainsi une variabilité d'une fonction anormalement importante. Les conséquences peuvent se propager par le biais de couplage (interdépendances) important entre les éléments constitutifs plutôt que par les liens causes-effets simples, identifiables et énumérables. Cela peut être décrit comme une résonance de la variabilité normale des fonctions, donc comme la résonance fonctionnelle. Ce phénomène est dynamique, donc il ne peut pas être imputable à une simple combinaison de liens de causalité.

  La résonance fonctionnelle apparaît à partir de l'interaction inattendue de la variabilité normale de nombreux signaux.

Selon Hollnagel, la variabilité de performance dans les systèmes techniques est relative aux imperfections en conception et en production, aux spécifications non exhaustives des conditions de travail (effets de l'environnement et des entrées non prévues qui rendent toute exhaustivité impossible – y compris au niveau des procédures) [45]. La variabilité de performances humaines et organisationnelles vient de leur capacité à s'adapter aux conditions de travail et à l'absence de régularité dans les activités (perception, cognition, action, communication).

D'autre part, Hollnagel utilise la superposition des signaux comme modèle de dépendance fonctionnelle entre les fonctions et les activités du système. Le signal faible correspond à la variabilité de performance de chaque fonction exercée par les différents sous-systèmes. Cette variabilité de performance est faible dans le sens où les écarts de performance des fonctions n'ont pas ou peu d'impact sur la performance globale du système et sur la sécurité. Le signal non linéaire permettant d'établir la résonance correspond à la variabilité de performance du reste du système lorsqu'on considère une fonction ou une activité prise à part. Le signal faible peut être la variabilité de performance de n'importe quelle fonction ou activité du système et le bruit correspond à l'agrégation des variabilités de performance du reste du système (environnement compris). Hollnagel appelle ce phénomène la « résonance fonctionnelle ».

Le principe de la méthode FRAM peut être illustré par la Figure 33.

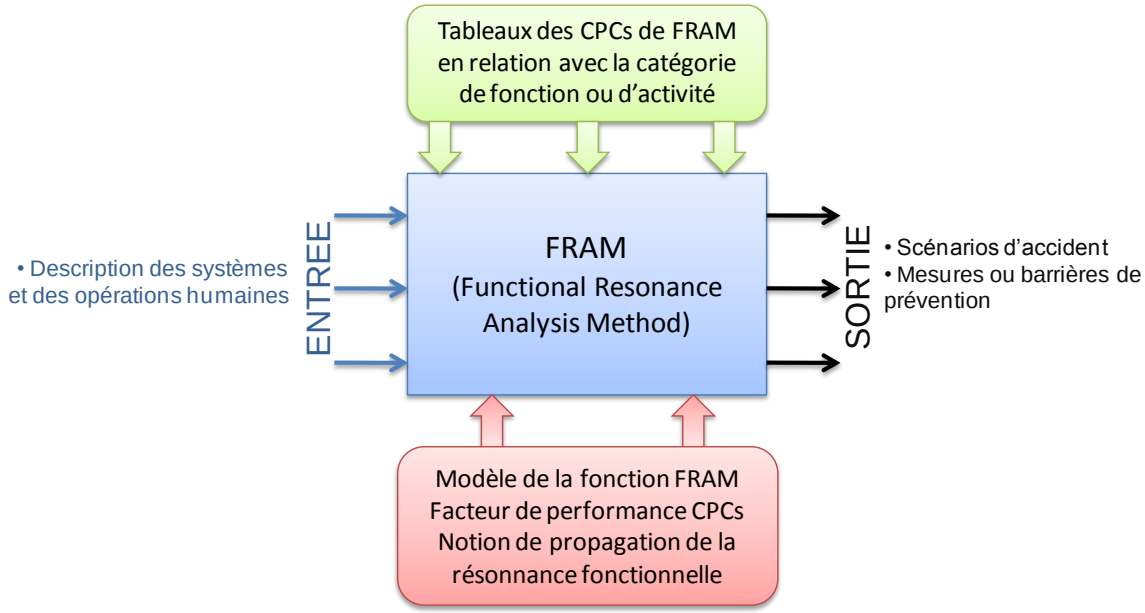


Figure 33 : Principe synthétique de la méthode FRAM

Procédure

La procédure d'application de la méthode FRAM comporte quatre étapes suivantes.

Étape 1 : Identifier et caractériser les fonctions essentielles

Cette étape comprend une analyse fonctionnelle des activités et des fonctions et une caractérisation des fonctions/activités par six paramètres ou attributs. Chaque fonction est représentée par un hexagonale munie de six attributs (voir Figure 34). Ces attributs servent de connecteurs entre les fonctions ou activités élémentaires :

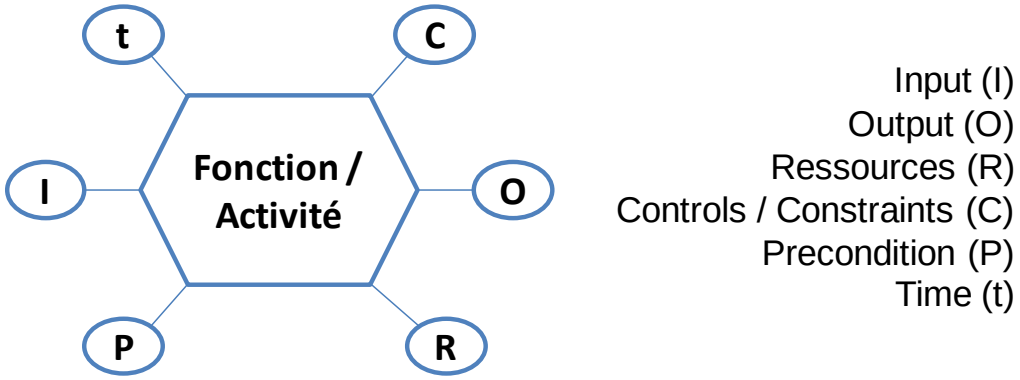


Figure 34 : Codage des fonctions FRAM (I : Entrée ; O : Sortie/Résultat ; R : Ressources ; C : Contrôle/Contrainte ; P : Préconditions; t : temps)

- Entrée (Input): représente ce qui sera traité ou transformé par la fonction ;
- Sortie/résultat (Output): représente le ou les résultats / produits de la fonction ;
- Ressources (R) : représente ce qui sera consommé ou utilisé par la fonction ;
- Temps (t) : représente le temps nécessaire à la réalisation de la fonction et tout ce qui concerne les pressions temporelles ;
- Control (C) : représente le ou les contrôles et contraintes qui gouvernent l'exécution de la fonction (boucle de rattrapage, procédures, méthodes, etc.) ;
- Pré-condition (P) : représente les éléments qui doivent être satisfaits avant que la fonction soit exécutée.

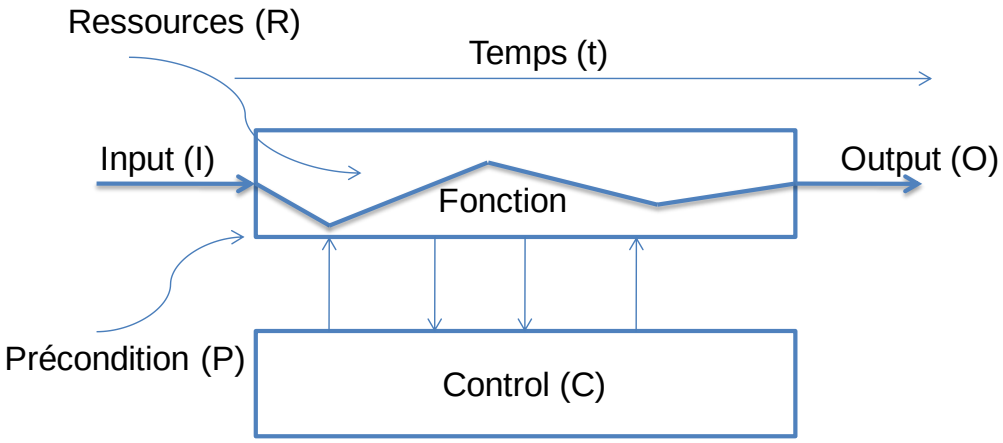


Figure 35 : Représentation schématisée des fonctions FRAM

Étape 2 : Déterminer la variabilité potentielle du contexte dépendant

La variabilité potentielle du contexte dépendant est déterminée par onze « conditions de performance communes » (CPC – Common Performance Conditions). FRAM classe les fonctions ou les activités en trois catégories : humaines (H), techniques (T) ou organisationnelles (O) selon la nature des acteurs exécutant les fonctions.

Les CPCs utilisées dans FRAM sont basées sur celles utilisée dans CREAM [44] avec deux CPCs supplémentaires. Le Tableau 36 présente les onze CPCs de FRAM en comparaison avec neuf CPCs de CREAM et la catégorie de fonction à laquelle elles s'appliquent.

Tableau 36: Les conditions de performances communes CPCs de FRAM en relation avec la catégorie de fonction ou d'activité

N° CPC		Nom de la CPC	Catégorie de fonction
FRAM	CREAM		
C1		Disponibilité des ressources	H - T
C2	N° 8	Entraînement et expérience	H
C3		Qualité des communications	H - T
C4	N°3	Qualité des interfaces opérateurs - machines	H
C5	N°4	Accessibilité et disponibilité des méthodes et des procédures	H
C6	N°2	Conditions de travail	H – T
C7	N°5	Nombre d'objectifs simultanés	H – O
C8	N°6	Temps disponible	H
C9	N°7	Rythme circadien	H
C10	N°9	Qualité de collaboration en équipe	H
C11	N°1	Qualité et support de l'organisation	O

Les fonctions ou les activités ne sont pas affectées de la même façon par les CPCs. Par exemple, une fonction de catégorie H est potentiellement affectée par toutes les CPCs incluant la catégorie H. Par contre une fonction de catégorie O est potentiellement affectée par deux CPCs, C7 et C11, seulement. Donc, il faut déterminer la catégorie de chaque fonction/activité avant d'identifier les conditions de performance pouvant affecter la performance de la fonction.

À l'issue de cette étape, une liste des CPCs est établie pour chaque fonction ou activité. Les CPCs identifiées sont ensuite contextualisées pour chaque étude. Il est possible d'identifier plusieurs conditions différentes pour chaque CPC.

L'étape suivante consiste à évaluer la qualité des CPCs afin de déterminer le potentiel de variabilité de chaque fonction. L'action des CPCs peut être positive ou négative sur la performance des fonctions, cependant l'étude de sécurité se place toujours dans le contexte le moins favorable, c'est pourquoi seul l'effet négatif est considéré dans la méthode. La qualité de chaque CPC est appréciée, par une expertise collective entre les différents spécialistes de chaque domaine, en trois valeurs possibles de variabilité suivantes :

- $\nu 1$: stable ou variable mais adapté ;
- $\nu 2$: stable ou variable mais inadapté ;
- $\nu 3$: imprévisible.

Il s'agit de déterminer pour chaque fonction/activité la qualité des CPCs concernées. Cette évaluation doit être effectuée par des experts de chaque domaine dont dépendent les CPCs.

Si une condition de performance CPC est stable ou variable mais adaptée, la variabilité de performance associée à la fonction sera faible. Dans le cas stable ou variable mais inadapté, la variabilité de performance est élevée. Enfin, si une condition de performance est imprévisible, la variabilité associée est très élevée.

Les CPCs déterminent donc la contrainte de variabilité commune ou propre aux fonctions de l'activité étudiée. L'évaluation des effets des CPCs sur les fonctions doit être précisée à l'aide d'un modèle causal, issu d'une expertise interdisciplinaire et indiquant le potentiel de variabilité de la performance d'une fonction à partir des CPCs et ce pour chaque fonction. Hollnagel utilise le modèle ETTO [45], acronyme de Efficiency Thoroughness Trade Off (efficacité minutie compromis) qui permet d'inférer le comportement potentiel d'un opérateur humain à partir du contexte de la fonction et des pressions auquel il est soumis.

Étape 3 : Appliquer le principe de résonance fonctionnelle sur les dépendances entre les activités et les fonctions

Cette étape établit les dépendances entre les fonctions ou activités. Ceci est effectué par la mise en correspondance des attributs assignés à la première étape. Graphiquement cela revient à connecter les entrées et les sorties des fonctions représentées par leur hexagone. Le réseau ainsi créé permet de visualiser le flux des informations et des matières lors de l'exécution normale de l'activité étudiée. La Figure 36 représente un exemple du réseau FRAM.

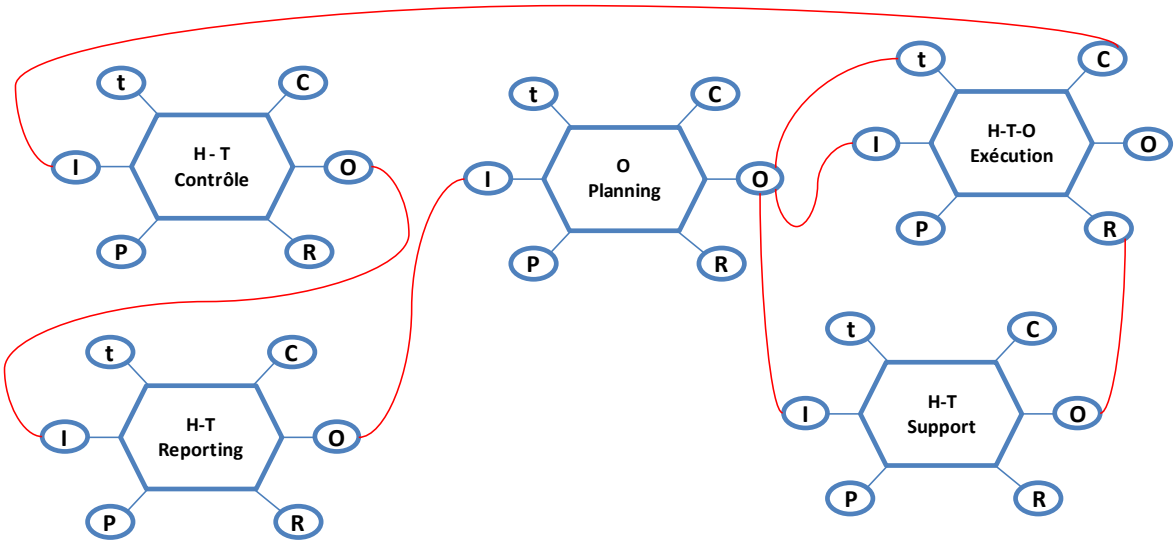


Figure 36 : Exemple du réseau FRAM

Les mentions H, T ou O dans l'en-tête des fonctions indique la catégorie des entités participant à la fonction. Il s'agit alors de rechercher les résonances fonctionnelles issues de la variabilité de performance des fonctions et propagées par les interrelations entre les fonctions. De même, un raisonnement causal doit être utilisé pour déterminer l'effet de la variabilité d'une fonction connectée à un attribut d'une autre fonction sur la performance de cette dernière. Seul le contexte de l'étude et une expertise interdisciplinaire permet d'élaborer un tel raisonnement.

Cette étape permettra donc d'identifier les scénarios d'accident et leurs conséquences.

Étape 4 : Identifier les barrières contre la variabilité et spécifier les nécessaires mesures de surveillance de la performance.

Cette étape consiste à identifier les mesures, les barrières à mettre en place afin de prévenir les scénarios d'accident identifiés.

Données d'entrée (input)

- Description de l'installation, des tâches, des procédures

Résultats (output)

- Liste et description des scénarios d'accident
- Mesures ou barrières de prévention
- Moyens de surveillance de la performance des fonctions/activités.

Domaine d'application

Tous domaines

Validation

La méthode FRAM a été testée par l'auteur dans les domaines ferroviaires [19] et de l'aviation [47], [67]. Dans le domaine du contrôle de trafic aérien, la méthode FRAM sert de support à une étude prospective des risques dans le cadre de l'introduction d'automatismes dans le système de management du trafic aérien. Un modèle de gestion des conflits aériens par le contrôleur aérien a été développé. Ce modèle FRAM a permis, selon l'auteur, de relever des questions sur les risques lors de l'utilisation du futur système automatisé.

Commentaires

<u>Les points forts :</u>

- La méthode FRAM fournit un bon outil pour présenter des interactions entre les fonctions/activités. Elle permet de représenter l'exécution d'une activité dans tous ses modes d'exploitation (mode normal et modes dégradés).
- La méthode FRAM s'appuie sur l'aspect fonctionnel détaillé de l'activité et offre l'avantage de modéliser plusieurs scénarios (stressés, dégradés, voire accidentels) sur un schéma commun.
- C'est une méthode originale d'identification des scénarios d'accidents dans un système complexe.
- Comme toute modélisation systémique, la construction même du modèle apporte des éléments de connaissance du système dans son fonctionnement et notamment en ce qui concerne les interrelations complexes qu'il renferme. En effet, l'analyse systémique requiert de nombreuses informations et nécessite de comprendre en détail les différents contextes d'exécution des fonctions et leurs effets sur l'activité.
- Cette démarche constructive propose à l'ingénieur de sécurité une méthode dirigée qui lui permet de comprendre les phénomènes complexes intervenant dans le système avec un regard interdisciplinaire nécessaire.

Les points faibles :

- Le besoin d'une expertise interdisciplinaire approfondie de chaque fonction afin de déterminer son modèle causal est un désavantage majeur de la méthode, car cela demande des ressources très importantes (expertises poussées, temps) qui gênent la faisabilité de l'étude.
- FRAM n'est pas une méthode simple. Elle exige une compréhension élevée de la méthode et du système étudié. Donc, elle s'adapte plutôt pour les systèmes de haute complexité, tels que le réseau de ferré et le trafic aérien, etc.

ANNEXE 14 : Exemples d’application

Descriptif de la mission facteur humain choisie pour cette étude de cas

La mission facteur humain choisie pour illustrer l'application des différentes méthodes s'intitule « Redémarrer un four suite à un arrêt du système » ou « Réchauffer un four ». Cette mission est issue de l'ouvrage décrivant la méthode CREAM [44]. Supposons que le four doit être redémarré pour une échéance donnée et doit être maintenu pour une durée donnée, tous les retards dus à des défaillances d'une des étapes élémentaires de la mission sont considérés comme échec de la mission. Toutes les défaillances menant à des pertes économiques ou humaines sont aussi considérées comme échec de la mission.

Les hypothèses retenues pour l'évaluation de cette mission sont les suivantes :

- Il n'existe ni support procédural, ni formation ou entraînement spécifique pour la tâche « Réchauffer un four ».
- Cette tâche n'est pas considérée comme importante, au moins du point de vue de la sécurité, bien que les conséquences puissent être très graves.
- Tout opérateur peut être amené à réaliser la tâche, quelle que soit sa formation (apprentis, apprentissage à partir de son collègue plus expérimenté, etc.…).

Donc, l'organisation doit être considérée comme insuffisante.

Par ailleurs, le temps de réponse nominal pour le diagnostic $T_{1/2}$(PSFs nominal) est de 30 min. Le diagnostic considéré consiste à s'assurer de la conformité de l'installation avant le redémarrage et à sélectionner les actions appropriées.

La mission peut être analysée selon la méthode d'analyse hiérarchisée des tâches (HTA – Hierarchical Task Analysis) et est présentée dans la Figure 37.

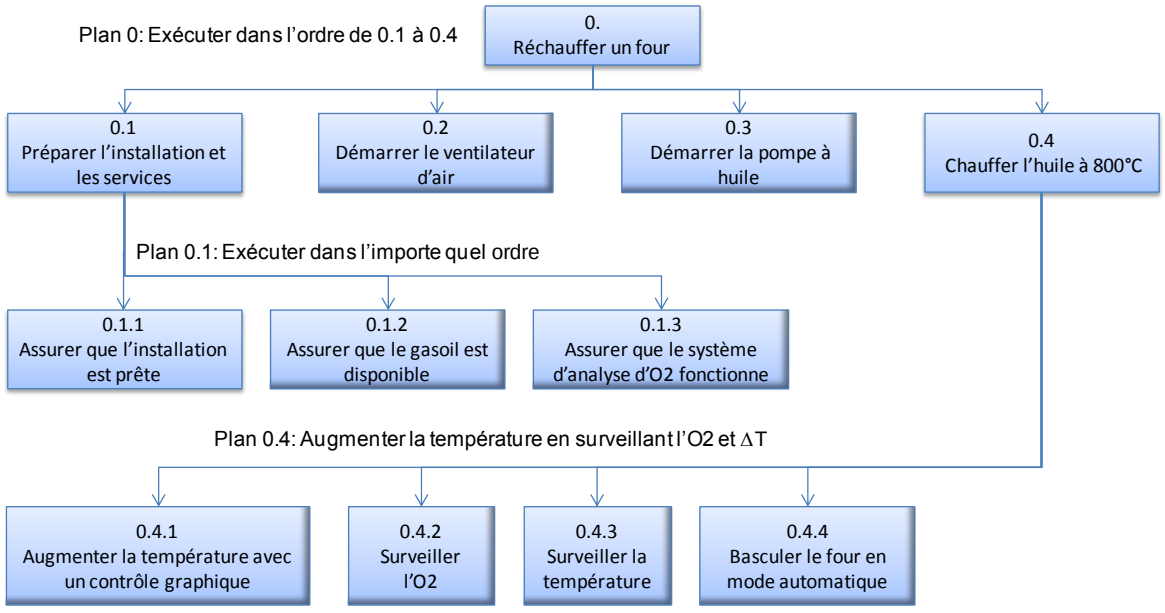


Figure 37 : Analyse de tâche hiérarchisée HTA de la mission « Réchauffer un four »

La liste des opérations humaines est fournie dans le Tableau 37.

Tableau 37: Les étapes de la mission « Réchauffer un four »

N° de l'étape		Objectif	Étape ou activité de la tâche
0.1	0.1.1	Préparer l'installation et les services	Assurer que l'installation est prête
	0.1.2		Assurer que le gasoil est disponible
	0.1.3		Assurer que le système d'analyse d'O2 fonctionne
0.2		Démarrer le ventilateur d'air	Démarrer le ventilateur d'air
0.3		Démarrer la pompe à huile	Démarrer la pompe à huile
0.4	0.4.1	Chauffer l'huile à 800°C	Augmenter la température avec un contrôle graphique
	0.4.2		Surveiller l'O2
	0.4.3		Surveiller la température
	0.4.4		Basculer le four en mode automatique lorsque la température atteint 800 °C

Application de la méthode THERP

Identification des erreurs potentielles et estimation des probabilités des erreurs en tenant compte des facteurs de performance PSFs

Les résultats de cette étape sont donnés dans le

Tableau 38

Tableau 38: *Les erreurs et leurs probabilités estimées (Pe : probabilité d'erreur ; Pr : probabilité de rattrapage ; BHEP : probabilité d'échec basique ; PSF : le facteur de performance identifié selon le contexte)*

Erreurs et récupération	Probabilité estimée = BHEP x PSF	Commentaires
Pe(0.1.1)	0.01 x 2 = 0.02	T20-6(3) et T18-1(1) (i.e. erreur n° 3 du tableau 20-6 et facteur de performance n° 1 du tableau 18-1 donnés dans le Handbook [88]) : c'est un contrôle dans les conditions d'opération normales. Facteur de performance : niveau de stress bas et inexpérience.
Pr(0.1.1)	0	Pas de rattrapage
Pe(0.1.2)	0.02 x 2 = 0.02	T20-6(3) et T18-1(1): c'est un contrôle dans les conditions d'opération normales. Facteur de performance : niveau de stress bas et inexpérience.
Pr(0.1.2)	0	Pas de rattrapage
Pe(0.1.3)	0.03 x 2 = 0.02	T20-6(3) et T18-1(1) : c'est un contrôle dans les conditions d'opération normales. Facteur de performance : niveau de stress bas et inexpérience.
Pr(0.1.3)	0	Pas de rattrapage
Pe(0.2)	0.005 x 2 = 0.01	T20-12(4) et T18-1(1): supposons que la défaillance des matériels est négligeable, et que le contrôle est bien conçu. Facteur de performance : niveau de stress bas et inexpérience.
Pr(0.2)	0.9	La possibilité de redémarrage du ventilateur est prévue
Pe(0.3)	0.005 x 2 = 0.01	T20-12(4) et T18-1(1): supposons que la défaillance des matériels est négligeable, et que le contrôle est bien conçu. Facteur de performance : niveau de stress bas et inexpérience.
Pr(0.3)	0.9	La possibilité de redémarrage de la pomme à l'huile est prévue
Pe(0.4.1)	0.009 x 4 = 0.036	T20-11(6), T20-12(10) et T18-1(4): c'est une combinaison des deux actions, surveiller et manipuler le contrôle de température. Facteur de performance : niveau de stress étape-par-étape et inexpérience.
Pr(0.4.1)	0.9	La possibilité de rattrapage est importante
Pe(0.4.2)	0.001 x 2 = 0.002	T20-11(1): supposons que l'indicateur du niveau d'O2 soit digital. Facteur de performance : niveau de stress bas et inexpérience.
Pr(0.4.2)	0.9	La possibilité de rattrapage est importante
Pe(0.4.3)	0.001 x 2 = 0.002	T20-11(1): supposons que l'indicateur de température soit digital. Facteur de performance : niveau de stress bas et inexpérience.

Erreurs et récupération	Probabilité estimée = BHEP x PSF	Commentaires
Pr(0.4.3)	0.9	La possibilité de rattrapage est importante
Pe(0.4.4)	0.009 x 4 = 0.036	T20-11(6) et T20-12(10) : c'est une combinaison des deux actions, surveiller et manipuler le contrôle de température. Facteur de performance : niveau de stress étape-par-étape et inexpérience.
Pr(0.4.4)	0	Pas de rattrapage : i.e. absence d'alarme de température haute et de vérification

Étape 3: *Estimer la probabilité globale de la mission*

Les erreurs et les rattrapages identifiés et quantifiés sont présentés sur un arbre d'événement THERP dans la Figure 38.

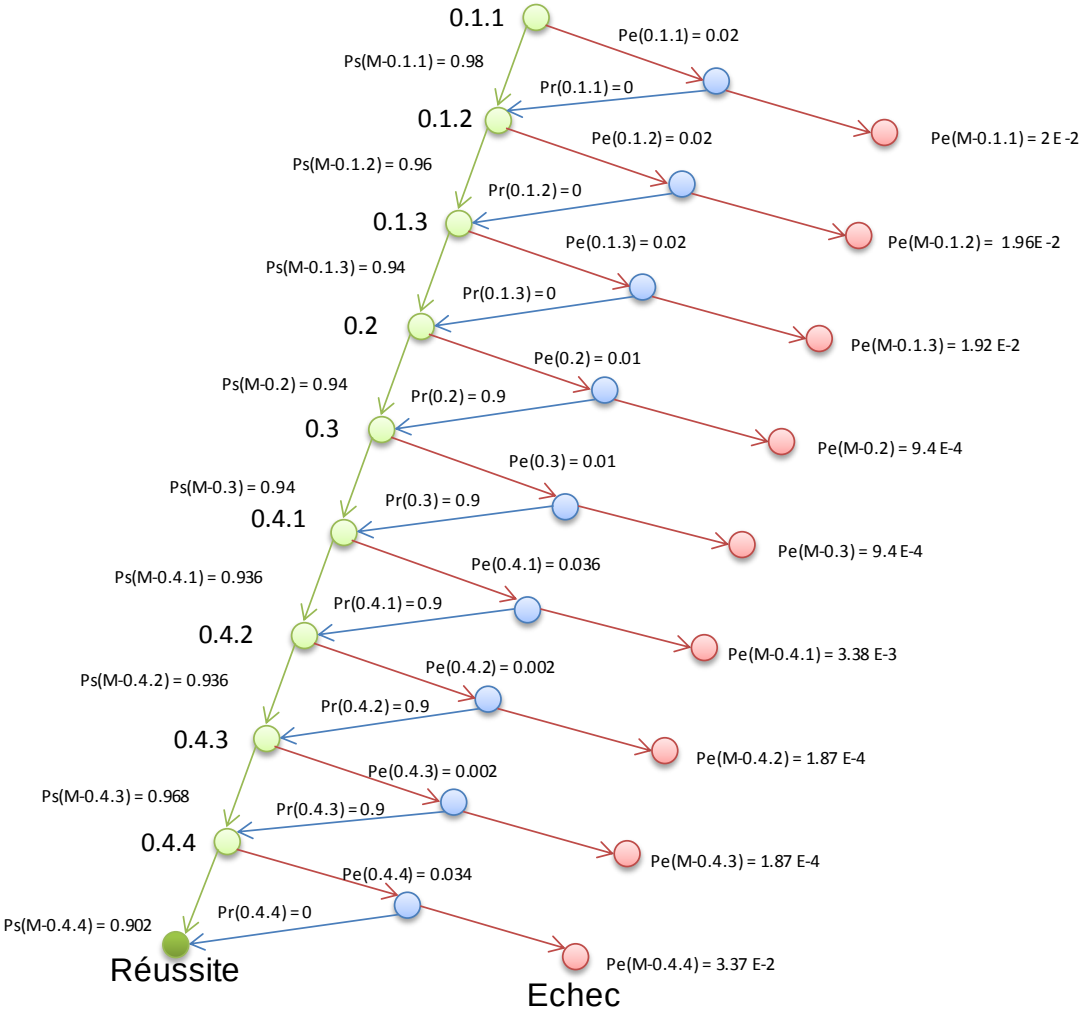


Figure 38 : Arbre d'événement THERP de la mission « Réchauffer un four »

La probabilité de succès de cette mission est de l'ordre de 90%. Donc, la probabilité d'échec de cette mission est de l'ordre de 10%.

Conséquences et recommandations

L’erreur de chaque étape de la mission peut conduire à des conséquences différentes. L’échec de l’étape 0.1 conduit généralement aux conséquences sur la disponibilité du système. Par contre, les erreurs commises dans l’étape 0.4 peuvent provoquer des conséquences plus graves sur l’intégrité du système et sur la sécurité des personnels.

En plus, la probabilité d’échec de ces deux étapes est la plus élevée. Des moyens supplémentaires pour limiter les risques dus à ces deux étapes paraissent être nécessaires, par exemple :

- Une procédure complète de la mission,
- Système d’alarme sur la température du four,
- Système d’arrêt d’urgence en cas de la température haute du four.

Application de la méthode TESEO

Supposons que cette mission a été analysée selon la méthode d'analyse hiérarchisée des tâches (HTA) et est présentée dans la Figure 37.

La liste des activités que l'opérateur doit réaliser pour réussir la mission est fournie dans le Tableau 37.

Dans cette étude, les facteurs contextuels K1, K2, K3, K4 et K5 sont évalués de façon globale pour la mission.

a. Estimer le facteur K1 (complexité de l'action)

   Selon la description des tâches de la mission, la mission n'apparaît pas très complexe. On suppose que cette tâche est routinière. Donc la valeur du facteur K1 estimée est égale à 0.01.

b. Estimer le facteur K2 (facteur d'exigence temporelle)

   C'est une tâche routinière et l'exigence de temps est faible. Supposons que le temps disponible est d'environ 10 minutes, donc la valeur du facteur K2 est égale à 1.

c. Estimer le facteur K3 (Facteur de compétences)

   Selon la description du contexte, l'opérateur possède peu de connaissance et de formation. Donc, le facteur K3 est estimé à 3.

d. Estimer le facteur K4 (Facteur émotionnel)

   Cette mission est plutôt une situation normale, redémarrage du four suite à un arrêt du système. Alors, le coefficient K4 est égal à 1.

e. Estimer le facteur K5 (Facteur ergonomique de travail)

   La tâche n'est pas considérée comme importante donc on fait l'hypothèse que l'ergonomie et l'organisation correspond à la catégorie « Climat moyen – mauvaises interfaces » ou à la catégorie « mauvais climat – mauvais interface ». Dans ce cas, la valeur du facteur K5 est égale à 7 ou à 10.

f. Calculer la probabilité d'échec de la mission P(E)

   P(E) = K1 x K2 x K3 x K4 x K5

P(E) = 0,01 x 1 x 3 x 1 x 7 = 0,21 ou ~ 20% d'échec pour chaque mission.

Application de la méthode SLIM

Supposons que cette mission a été analysée selon la méthode d'analyse hiérarchisée des tâches HTA et présentée dans la Figure 37. La liste d'activités que l'opérateur doit réaliser pour réussir la mission est fournie dans le Tableau 37.

Étape 1 : Choix du groupe d'experts

Étape 2 : Identification des scénarios

Supposons que le four doit être redémarré pour une date prévue, tous les retards dus aux défaillances d'une des étapes élémentaires de la mission sont considérés comme échec de la mission.

Toutes les défaillances conduisant à des conséquences économiques ou humaines sont aussi considérées comme échec de la mission.

- Scénario 1 : Mauvaise préparation de l'installation et des services associés à la mission
- Scénario 2 : Exécution d'une mauvaise séquence de la procédure

Par exemple : chauffer l'huile avant le démarrage de la pompe ou du ventilateur.

- Scénario 3 : Actions erronées lors de la procédure de chauffage d'huile

Les deux actions suivantes sont retenues pour le calibrage :

- Action A0.2 : Démarrer le ventilateur d'air
- Action A0.4.3 : Surveiller la température

Sélection des facteurs de performance

Dans cet exemple les facteurs de performance retenus sont les suivants :

- PSF1 : Temps disponibles ou la pression du temps ou le niveau de stress
- PSF2 : Qualité de l'information ou de l'interface
- PSF3 : Qualité des procédures
- PSF4 : Conséquences perçues par l'opérateur
- PSF5 : Niveau de complexité de la tâche
- PSF6 : Formation, entraînement
- PSF7 : Adéquation entre le niveau d'expérience de l'opérateur et celui exigé par la tâche

Le facteur de performance concernant la quantité de travail en équipe n'est pas retenu, car on suppose que l'opérateur travaille seul.

L'échelle de ces facteurs de performance varie de 1 à 9. Le point 9 correspond à un niveau optimal.

Tableau 39: Notes R des facteurs de performances PSFs et leur poids W

Facteurs de performance PSFs	Poids des PSFs, W	Notes R de l'adéquation entre les PSFs et la tâche				
		A0.2	A0.4.3	Scénario 1	Scénario 2	Scénario 3
PSF1 - Temps disponible	7	5	6	6	7	3
PSF2 - Interface	6	7	7	2	6	4
PSF3 - Procédure	8	6	7	2	2	4
PSF4 - Conséquences perçues	2	6	3	4	6	3
PSF5 - Complexité de la tâche	7	5	7	4	8	4
PSF6 - Formation	2	6	7	3	7	7
PSF7 – Adéquation entre la tâche et les compétences de l'opérateur	5	6	5	4	6	7

Tableau 40: Valeur de l'index SLIs des facteurs de performances PSFs et leur poids normalisée

Facteurs de performance PSFs	Poids des PSFs normalisé, W	Valeur de l'index SLIs des facteurs de performances PSFs				
		A0.2	A0.4.3	Scénario 1	Scénario 2	Scénario 3
PSF1 - Temps disponible	0.19	0.9	1.1	1.1	1.3	0.6
PSF2 - Interface	0.16	1.1	1.1	0.3	1.0	0.6
PSF3 - Procédure	0.22	1.3	1.5	0.4	0.4	0.9
PSF4 - Conséquences perçues	0.05	0.3	0.2	0.2	0.3	0.2
PSF5 - Complexité de la tâche	0.19	0.9	1.3	0.8	1.5	0.8
PSF6 - Formation	0.05	0.3	0.4	0.2	0.4	0.4
PSF7 – Adéquation entre la tâche et les compétences de l'opérateur	0.14	0.8	0.7	0.5	0.8	0.9
TOTAL	1.0	5.8	6.3	3.6	5.8	4.3

Conversion des indexes SLIs en probabilité

Les constantes a et b peuvent être évaluées par deux actions : A0.2 et A0.4.3. La probabilité d'échec de ces deux actions est bien connue dans le Handbook de Swain (voir l'exemple de THERP) :

La probabilité d'échec de l'action A0.2 est de 0.005 x 2 = 0.01 avec les facteurs de performance : niveau de stress bas et inexpérience. La probabilité d'échec de l'action A0.4.3 est de 0.001 x 2 = 0.002 avec les facteurs de performance: niveau de stress bas et inexpérience. Les valeurs de a et b sont ainsi déterminées :

a = 0.00647

b = -0.0418

Tableau 41: Probabilité de réussite

Facteur de performance PSFs	**A0.2**	**A0.4.3**	**Scénario 1**	**Scénario 2**	**Scénario 3**
SLI(Total)	5.8	6.3	3.6	5.8	4.3
Probabilité de réussite	0.990	0.998	0.96	0.99	0.97
Probabilité d'échec	0.010	0.002	0.04	0.01	0.03

La probabilité d'échec de la mission est la somme de la probabilité d'échec des trois identifiés scénarios. Donc, la probabilité générale d'échec de la mission est estimée à 0.04 + 0.01 + 0.03 = 0.08 ou 8%.

Application de la méthode HCR

L'analyse de la tâche montre que la mission exige des actions basées plutôt sur l'habileté de l'opérateur. En effet, la complexité de la mission est faible, la procédure prescrite n'est pas exigée. La mission ne demande pas de connaissances approfondies. Ainsi, les paramètres du modèle HCR appliqués pour cet exemple sont les suivants :

Type du comportement cognitif	β_i	γ_i	η_i
Habileté (Skill-based)	1.2	0.7	0.407

L'entreprise considère que les opérateurs peuvent réaliser la tâche, quelle que soit leur formation, il est possible que l'entreprise fasse appel à des opérateurs débutants pour réaliser cette mission. Ainsi, le facteur de performance PSF1 sur l'expérience de l'opérateur est évalué au niveau 3 comme « Novice, entraînement minimum ».

Cette tâche n'étant pas considérée comme importante, nous faisons l'hypothèse que, l'opérateur ne prend aucunes dispositions particulières. Ainsi, le facteur de performance PSF2 concernant le niveau de stress est évalué au niveau 4 comme « Activité basse, vigilance basse ». On suppose que la qualité de l'interface homme-machine est moyenne.

Les valeurs des facteurs de performance évalués pour cette mission sont données dans le tableau suivant :

Tableau 42: Les facteurs de performance PSFs et les valeurs de leur facteur correctif déterminés pour la mission « redémarrage d'un four »

Facteur de performance PSF	**Valeur de PSF_j**
Expérience de l'opérateur (PSF_1) : *Novice, entraînement minimum*	0,44
Stress (PSF_2) : *Activité basse, vigilance basse*	0,28
Qualité de l'interface homme-machine (PSF_3) : *Moyenne*	0,44

Donc le temps de réponse de l'équipage est calculé dans la formule suivante :

$$T_{1/2} = 30 \times \prod_{j=1}^{3}(1+PSF_j) = 30 \times (1 + 0{,}44) \times (1 + 0{,}28) \times (1 + 0{,}44) = 80 \text{ min}$$

Selon les situations, les temps disponibles peuvent variés. Le Tableau 43 et la Figure 39 présentent la probabilité de non réponse en fonction du temps disponible.

Tableau 43: La probabilité de non réponse pour l'action de diagnostic en fonction du temps disponible dans les conditions de la mission «redémarrage d'un four»

Temps disponible, min	30	40	50	60	70	80	90	100	110
Probabilité	1	1	1	0.92	0.69	0.49	0.34	0.23	0.16

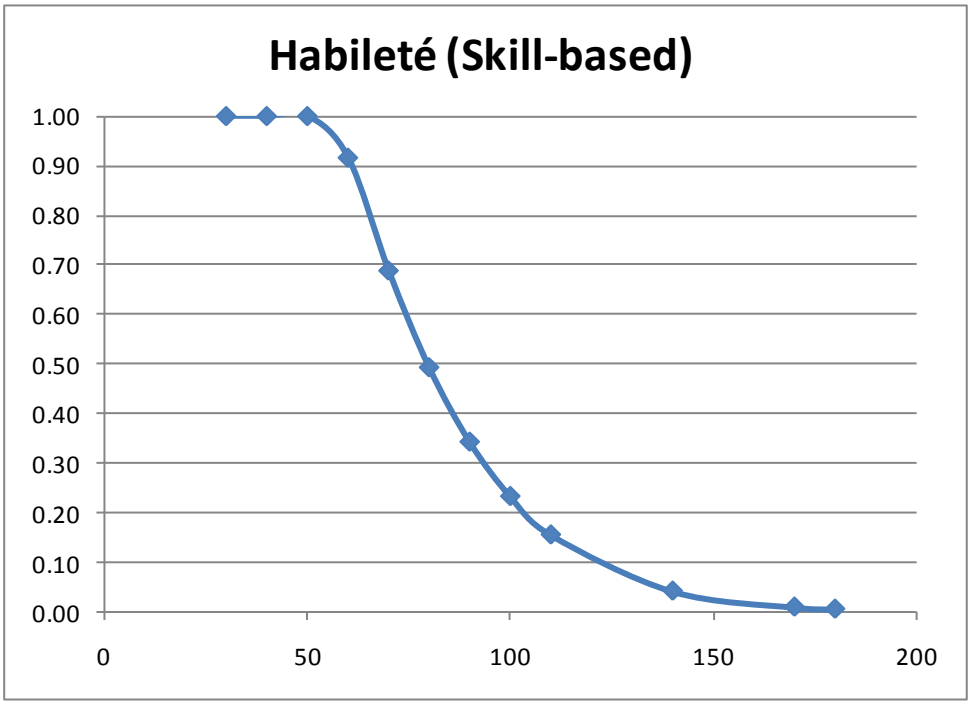


Figure 39 : La probabilité de non réponse pour l'action de diagnostic en fonction du temps disponible dans les conditions de la mission « redémarrage d'un four »

On observe que, dans le contexte de la mission « redémarrage d'un four », la probabilité d'échec de l'action de diagnostic pouvant être réalisée en 30 min dans les conditions standards avoisine 100% si le temps disponible est inférieur à 60 minutes.

Application de la méthode HEART

Supposons que cette mission a été analysée selon la méthode d'analyse hiérarchisée des tâches HTA et présentée dans la Figure 37.

La liste d'activités que l'opérateur doit réaliser pour réussir la mission est fournie dans le Tableau 37.

Cette mission peut être considérée comme une tâche de type E « Routine ou tâche réalisée habituellement ou tâche rapide avec un niveau requis relativement bas » de la méthode HEART. Donc, la probabilité d'échec nominale PN de cette mission est de 0.02 ou 2%.

Dans le contexte décrit pour cette mission, les facteurs EPCs suivants peuvent affecter la probabilité nominale de la mission :

- Un décalage entre le risque perçu et le risque réel.
- Inexpérience de l'opérateur.
- Une pauvre qualité des procédures de transmission de l'information et de l'interaction personne-personne.

La pondération est aussi estimée pour les trois facteurs identifiés ci-dessus. Le résultat d'analyse est donné dans le Tableau 44 suivant :

Tableau 44: Évaluation de la fiabilité de la tâche « Redémarrer un four suite à un arrêt du système »

Facteurs EPCs	**Poids de dégradation**	**Pondération estimée, W**	**Effet évalué**
Décalage entre le risque perçu et le risque réel	X 4	0,4	(4-1) x 0,4 + 1 = 2.2
Inexpérience de l'opérateur	X 3	0.6	(3-1) x 0,6 + 1 = 2.2
Pauvre qualité des procédures	X 3	1,0	(3-1) x 1,0 + 1 = 3

La probabilité d'échec de la mission $P_{échec_mission}$ « *Redémarrer un four suite à un arrêt du système »* est ainsi estimée comme suit :

$$P_{échec_mission} = HEP_{échec_mission_nominale} \times \prod_{k=1}^{N} (EPC_k - 1) \times W_k + 1$$

$$= 0.02 \times 2{,}2 \times 2{,}2 \times 3 = 0.29$$

Donc la probabilité d'échec de cette mission est de l'ordre de 29%.

Application de la méthode ATHEANA

Supposons que cette mission a été analysée selon la méthode d'analyse hiérarchisée des tâches HTA et présentée dans la Figure 37.

Supposons que le four doit être redémarré pour une échéance donnée et doit être maintenu pour une durée donnée, tous les retards dus aux défaillances d'une des étapes élémentaires de la mission sont considérés comme échec de la mission. Toutes les défaillances menant aux pertes économiques ou humaines sont aussi considérées comme échec de la mission.

Identification des scénarios d'échec de la mission HFE

Suite à une analyse de la mission, les événements d'échec HFEs suivants ont été identifiés :

- HFE 1 : Non-respect de l'échéance requise
- HFE 2 : Non-respect de la durée requise
- HFE 3 : Défaut de maîtrise de la température du four
- HFE 4 : Explosion du four

Pour chaque scénario, les contextes EFC et les actions dangereuses UA doivent être identifiés et détaillés. Pour illustrer cela, le scénario 3 est développé en détail et présenté dans le tableau suivant :

Tableau 45: *Identification des actions dangereuses UAs et contextes particuliers EFCs associés pour l'événement HFE 3.*

N° EFC	Type d'erreurs	Contextes EFC	Actions dangereuses UA
EFC1	EOO	Inattention de l'opérateur dans la surveillance de température.	UA1 : Échec de passage en mode automatique à 800°c
EFC2	EOO	L'opérateur focalise sur une autre tâche concurrente (secondaire).	
EFC3	EOC	L'opérateur réalise une action erronée en basculant en mode automatique.	
EFC4	EOC	Défauts de maintenance sur les équipements autorisant le passage en mode automatique.	
EFC5	EOO	Défaillance du système d'information de température et l'opérateur n'aperçoit pas les défauts.	
EFC6	EOO	Défaillance du système d'information de température et l'opérateur aperçoit les défauts. Cependant, l'opérateur ne sait pas ce qu'il faut faire, donc l'action nécessaire n'est pas faite.	
EFC7	EOO	Défaillance du système	

N° EFC	Type d'erreurs	Contextes EFC	Actions dangereuses UA
		d'information de température et l'opérateur aperçoit les défauts. Cependant, l'opérateur focalise sur la recherche pour comprendre ce qui se passe, il ne fait pas attention à la sécurité du four. Donc, il ne fait rien pour baisser la température ou arrêter l'opération.	
EFC8	EOC	Défaillance du système d'information de température et l'opérateur aperçoit les défauts. Cependant, l'opérateur sait qu'il faut arrêter le four, mais il commet une erreur dans cette action.	
EFC9	EOO	Inattention de l'opérateur dans la surveillance de température.	UA2 : Vitesse d'augmentation de la température du four excessive
EFC10	EOO	L'opérateur focalise sur une autre tâche concurrente.	
EFC11	EOC	L'opérateur réalise un mauvais réglage de température.	
EFC12	EOO	Défaillance du système d'information de température et l'opérateur n'aperçoit pas les défauts.	
EFC13	EOC	L'opérateur trouve que la température n'augmente pas assez vite, mais il ne sait pas que l'indication de température est erronée. Donc il essaie d'augmenter la température au lieu de la baisser.	
ECF14	EOC	L'opérateur trouve l'anomalie sur la température. Cependant, il effectue une mauvaise action.	

Comme il n'existe aucune donnée sur les probabilités conditionnelles $P(EFC_i|S)$ et $P(UA_j|EFC_i,S)$, ces dernières peuvent être estimées par les jugements d'experts à l'aide du Tableau 20. Le résultat de l'estimation des probabilités conditionnelles est donné dans le tableau suivant.

N° EFC	UA	Contextes EFC	$P(EFC_i\|S)$	$P(UA_j\|EFC_i)$	$P(EFC_i\|S) \times P(UA_j\|EFC_i)$
EFC1	UA1	Inattention de l'opérateur dans la surveillance de température	0,1	0,01	0,001
EFC2	UA1	L'opérateur focalise sur une autre tâche concurrente	0,01	0,01	0,0001
EFC3	UA1	L'opérateur réalise une action erronée en basculant en mode automatique	0,001	0,001	0,000001
EFC4	UA1	Défauts de maintenances sur les équipements autorisant le passage en mode automatique	0,001	0,1	0,0001
EFC5	UA1	Défaillance du système d'information de température et l'opérateur n'aperçoit pas les défauts	0,0001	0,5	0,00005
EFC6	UA1	Défaillance du système d'information de température et l'opérateur aperçoit les défauts. Cependant, l'opérateur ne sait pas ce qu'il faut fait, donc l'action nécessaire n'est pas faite.	0,0001	1	0,0001
EFC7	UA1	Défaillance du système d'information de température et l'opérateur aperçoit les défauts. Cependant, l'opérateur focalise sur la recherche pour comprendre ce qui se passe, il ne fait pas attention à la sécurité du four. Donc, il ne fait rien pour baisser la température ou arrêter l'opération.	0,0001	1	0,0001
EFC8	UA1	Défaillance du système d'information de température et l'opérateur aperçoit les défauts. Cependant, l'opérateur sait qu'il faut arrêter le four, mais il commet une erreur dans cette action.	0,0001	1	0,0001
EFC9	UA2	Inattention de l'opérateur dans la surveillance de vitesse d'augmentation de température	0,1	0,01	0,001
EFC10	UA2	L'opérateur focalise sur une autre tâche concurrente et la vitesse est excessive	0,01	0,01	0,0001

N° EFC	UA	Contextes EFC	$P(EFC_i\|S)$	$P(UA_j\|EFC_i)$	$P(EFC_i\|S)$ x $P(UA_j\|EFC_i)$
EFC11	UA2	L'opérateur réalise un mauvais réglage de température	0,1	0,01	0,001
EFC12	UA2	Défaillance du système d'information de température et l'opérateur n'aperçoit pas les défauts et la vitesse est excessive	0,0001	0,5	0,00005
EFC13	UA2	L'opérateur trouve que la température n'augmente pas assez vite, mais il ne sait pas que l'indication de température est erronée. Donc il essaie à augmenter la température de façon excessive au lieu de la baisser.	0,0001	0,5	0,00005
ECF14	UA2	L'opérateur trouve l'anomalie sur la température. Cependant, il effectue une mauvaise action.	0,0001	0,1	0,00001

Ainsi, la probabilité de l'événement HFE 3 peut être calculée par la formule suivante : $P(HFE3|S) = \sum_j \sum_{i(j)} P(EFC_i|S) \times P(UA_j|EFC_i, S)$ = 3,8 E-03

Application de la méthode CREAM

Cette mission sera étudiée par les méthodes basique et étendue de CREAM.

La méthode basique

Étape 1 : Construction des séquences d'événement ou analyse de tâche

Supposons que cette mission a été analysée selon la méthode d'analyse hiérarchisée des tâches HTA et présentée dans la Figure 37.

La liste d'activités que l'opérateur doit réaliser pour réussir la mission est fournie dans le Tableau 37.

Étape 2 : Évaluer les conditions de performances communes CPCs

Le niveau et l'effet attendu des neuf CPCs est évalué à partir du Tableau 23 et du contexte de l'installation avec les hypothèses mentionnées pour cet exemple. Le résultat de cette évaluation est donné dans le Tableau 46.

Tableau 46: L'évaluation des conditions de performances CPCs pour la mission « Réchauffer un four »

N°	conditions de performances communes CPC	Niveau	Effet attendu sur la fiabilité de performance
1	Adéquation de l'organisation	Inefficace	Négatif
2	Conditions de travail	Compatible	Non significatif
3	Adéquation des interfaces Homme-Machine et des outils	Tolérable	Non significatif
4	Disponibilités de procédures et des plans	Inapproprié	Négatif
5	Nombre de buts simultanés	Correspond aux capacités	Non significatif
6	Temps disponible	Adéquat	Positif
7	Rythme circadien	Jour (ajusté)	Non significatif
8	Adéquation de l'entraînement et de l'expérience	Inadéquate	Négatif
9	Qualité de la collaboration au sein de l'équipe	Efficace	Non significatif

L'ajustement des CPCs « Conditions de travail », « Nombre de buts simultanés », «Temps disponible », et « Qualité de la collaboration au sein de l'équipe » doit être réalisé en utilisant les règles de CREAM décrits dans la méthodologie basique.

Le résultat de cet ajustement est donné dans le Tableau 47.

Tableau 47: L'ajustement des conditions de performances CPCs

Nom de la CPC	Effet attendu initial	Effet attendu initial des CPCs liées	Effet attendu ajusté
Conditions de travail	Non significatif	Négatif :2 Non significatif : 2 Positif :1	Non significatif
Nombre de buts simultanés	Non significatif	Négatif :1 Non significatif : 2 Positif :0	Non significatif
Temps disponible	Positif	Pas de changement	Positif
Qualité de la collaboration au sein de l'équipe	Non significatif	Négatif :2 Non significatif : 0 Positif :0	Négatif

Après l'ajustement, l'effet de la condition de performance CPC « Qualité de la collaboration au sein de l'équipe » est changé de « Non significatif » en « Négatif ». Le Tableau 48 résume le résultat d'évaluation des conditions de performances CPCs pour la tâche « Réchauffer un four ».

Tableau 48: L'ajustement des conditions de performances CPCs

N°	Nom de la CPC	Effet attendu initial	Effet attendu ajusté
1	Adéquation de L'organisation	Négatif	Négatif
2	Conditions de travail	Non significatif	Non significatif
3	Adéquation des interfaces Homme-Machine et des outils	Non significatif	Non significatif
4	Disponibilités de procédures et des plans	Négatif	Négatif
5	Nombre de buts simultanés	Non significatif	Non significatif
6	Temps disponible	Positif	Positif
7	Rythme circadien	Non significatif	Non significatif
8	Adéquation de l'entraînement et de l'expérience	Négatif	Négatif
9	Qualité de la collaboration au sein de l'équipe	Non significatif	Négatif

On observe 4 « Négatif », 4 « Non significatif » et 1 « Positif ». Donc, la note d'effet attendu de la tâche « Réchauffer un four » déterminée est [4, 4, 1].

Étape n°3 : Déterminer les modes de contrôle probables

Selon la note [4, 4, 1] déterminée au-dessus et le schéma présenté dans la Figure 21, le mode de contrôle pour cette tâche est évalué comme « Opportuniste ». Ainsi, selon le Tableau 25, la probabilité d'échec de cette mission peut être estimée entre 0,01 et 0,5.

Afin d'avoir une estimation de la probabilité plus fine, la méthode étendue de CREAM doit être utilisée.

La méthode étendue

Étape n°1 : Construire ou élaborer un profil d'exigences cognitives de la tâche

Dans cette étape, il faut caractériser chaque étape de la séquence d'événements par une activité cognitive donnée par CREAM dans le Tableau 26. Si une tâche ne peut pas être attribuée à une seule activité cognitive, cette tâche doit être décomposée jusqu'à un niveau suffisamment détaillé afin de trouver une activité cognitive adéquate. Dans cet exemple, la tâche 0.4.4 doit être décomposée en deux tâches :

- Vérifier si la température atteint 800 °C.
- Ensuite, basculer le four en mode automatique.

Tableau 49: Les activités cognitives de la mission « Réchauffer un four »

N° de l'étape		Objectif	Étape ou activité de la tâche	Activité cognitive
0.1	0.1.1	Préparer l'installation et les services	Assurer que l'installation est prête	Évaluer
	0.1.2		Assurer que le gasoil est disponible	Vérifier
	0.1.3		Assurer que le système d'analyse d'O2 fonctionne	Vérifier
0.2		Démarrer le ventilateur d'air	Démarrer le ventilateur d'air	Exécuter
0.3		Démarrer la pompe à huile	Démarrer la pompe à huile	Exécuter
0.4	0.4.1	Chauffer l'huile à 800°C	Augmenter la température avec un contrôle graphique	Régulariser
	0.4.2		Surveiller l'O2	Surveiller
	0.4.3		Surveiller la température	Surveiller
	0.4.4		Vérifier si la température atteint 800 °C	Vérifier
			Ensuite, basculer le four en mode automatique.	Exécuter

Les fonctions cognitives sont ensuite déterminées, utilisant le Tableau 27 de CREAM, pour chaque activité. Le résultat est donné dans le Tableau 50.

Tableau 50: Exigences cognitives pour la mission « Réchauffer un four »

N° de l'étape		Étape ou activité de la tâche	Activité cognitive	Fonctions COCOM			
				Obs	Int	Plan	Exe
0.1	0.1.1	Assurer que l'installation est prête	Évaluer		x	x	
	0.1.2	Assurer que le gasoil est disponible	Vérifier	x	x		
	0.1.3	Assurer que le système d'analyse d'O2 fonctionne	Vérifier	x	x		
0.2		Démarrer le ventilateur d'air	Exécuter				x
0.3		Démarrer la pompe à huile	Exécuter				x
0.4	0.4.1	Augmenter la température avec un contrôle graphique	Régulariser	x			x
	0.4.2	Surveiller l'O2	Surveiller	x	x		
	0.4.3	Surveiller la température	Surveiller	x	x		
	0.4.4	Vérifier si la température atteint 800 °C	Vérifier	x	x		
		Ensuite, basculer le four en mode automatique.	Exécuter				x
TOTAL				6	6	1	4
Profil d'exigences cognitives				35%	35%	6%	24%

Ainsi, le profil d'exigences cognitives est déterminé et présenté dans la Figure 40.

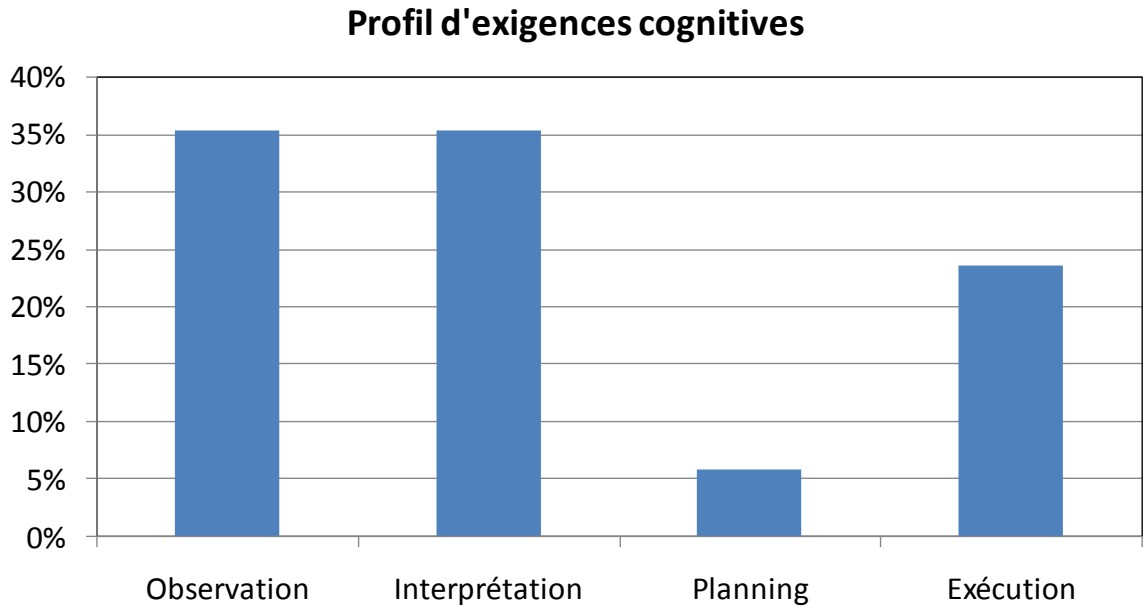


Figure 40 : Profil d'exigences cognitives de la mission « Réchauffer un four »

Étape n°2 : Identifier les défaillances des fonctions cognitives

Dans cette étape, il faut identifier les modes de défaillances plausibles pour chaque activité cognitive identifiée, à partir des défaillances génériques données dans le Tableau 28 et de toutes les données concernant le contexte de la mission. Chaque activité peut avoir plusieurs modes de défaillances différents, comme indiqués dans les Tableau 28 et Tableau 50. Cependant, il faut désigner un seul mode de défaillance crédible pour chaque activité.

Par exemple, l'activité « 0.1.1 Assurer que l'installation est prête » associée à l'activité cognitive « Évaluer » peut avoir cinq modes de défaillances, I1, I2, I3, P1 et P2 liés aux fonctions cognitives « interprétation et planning ». La sélection du mode de défaillance le plus plausible pour le contexte de travail est basée sur les informations découlant de l'analyse de tâche, et des conditions de performances CPCs. Dans cet exemple, il est assumé que le mode de défaillance le plus crédible est l'erreur de décision (mode I2) sur la préparation de l'installation.

De même façon, on détermine le mode de défaillance le plus crédible pour toutes les activités. Le Tableau 51 présente le résultat de cette évaluation.

Tableau 51: Les modes de défaillances cognitives crédibles pour la mission « Réchauffer un four ».

N°	Activité cognitive	Observation			Interprétation			Planning		Exécution				
		O1	O2	O3	I1	I2	I3	P1	P2	E1	E2	E3	E4	E4
0.1.1	Évaluer					x								
0.1.2	Vérifier			x										
0.1.3	Vérifier			x										
0.2	Exécuter											x		
0.3	Exécuter												x	
0.4.1	Réguler									x				
0.4.2	Surveiller			x										
0.4.3	Surveiller			x										
0.4.4	Vérifier					x								
	Exécuter										x			
TOTAL				4		2				1	1	1	1	

Ainsi, le profil de défaillances des fonctions cognitives est déterminé et présenté dans la Figure 41.

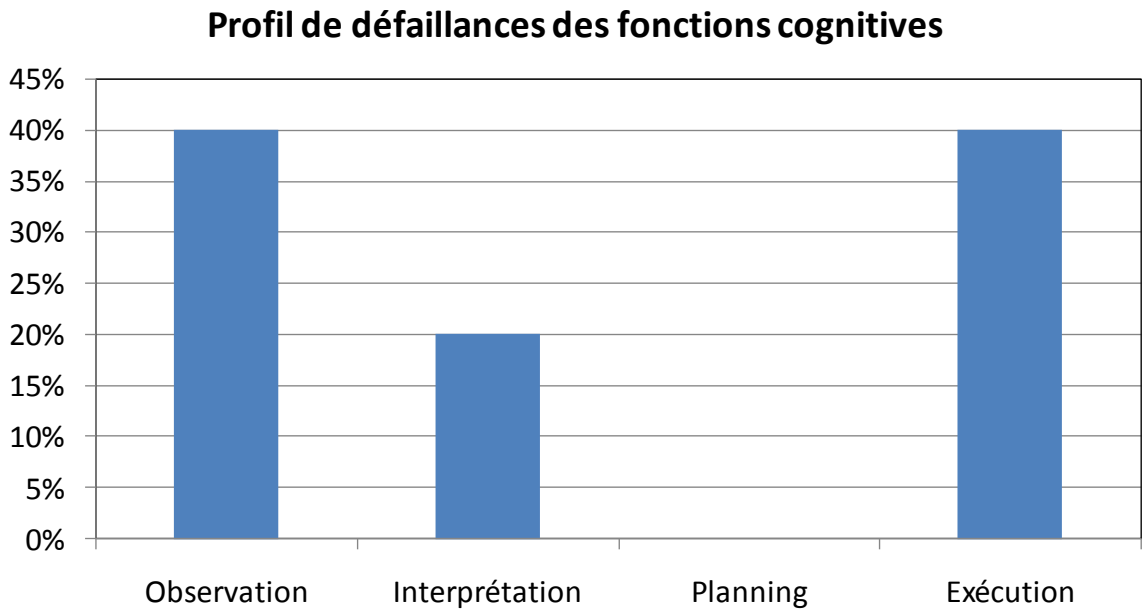


Figure 41 : Profil de défaillances des fonctions cognitives de la mission « Réchauffer un four »

Étape n°3 : Déterminer la probabilité d'échec de l'action spécifique

La probabilité de défaillance cognitive CFP (Cognitive Failure Probability) nominale peut être déterminée pour chaque activité, en combinant les Tableau **29** et Tableau 51. Le résultat est donné dans le Tableau 52.

Tableau 52: La probabilité CFP nominale pour la mission « Réchauffer un four »

N° de l'étape		Étape ou activité de la tâche	Mode d'erreur	Probabilité CFP nominale
0.1	0.1.1	Assurer que l'installation est prête	I2. Erreur de décision	1,0 E-2
	0.1.2	Assurer que le gasoil est disponible	O3. L'observation n'est pas faite	7,0 E-2
	0.1.3	Assurer que le système d'analyse d'O2 fonctionne	O3. L'observation n'est pas faite	7,0 E-2
0.2		Démarrer le ventilateur d'air	E3. Action réalisée sur mauvais objet	5,0 E-4
0.3		Démarrer la pompe à huile	E4. Action réalisée avec mauvais séquence	3,0 E-3
0.4	0.4.1	Augmenter la température avec un contrôle graphique	E1. Exécution d'un mauvais type	3,0 E-3
	0.4.2	Surveiller l'O2	O3. L'observation n'est pas faite	7,0 E-2
	0.4.3	Surveiller la température	O3. L'observation n'est pas faite	7,0 E-2
	0.4.4	Vérifier si la température atteint 800 °C	I2. Erreur de décision	1,0 E-2

N° de l'étape		Étape ou activité de la tâche	Mode d'erreur	Probabilité CFP nominale
		Ensuite, basculer le four en mode automatique.	E2. Action réalisée au mauvais temps	3,0 E-3

La probabilité CFP ajustée peut être déterminée selon deux approches ci-après.

- ***Approche simplifiée :*** La valeur CFP ajustée est calculée par la formule suivante :

  CFP ajustée = CFP nominale x facteur d'effet moyen

  Où : le facteur d'effet moyen est basé sur les valeurs du Tableau 30 et le mode de contrôle déterminé dans la méthode basique.

  Dans cet exemple, le mode de contrôle a été déterminé comme « Opportuniste ». Donc, le facteur d'effet moyen est égal à 7,5. En appliquant ce facteur, la probabilité CFP ajustée peut être calculée pour toutes les activités de la mission. Le résultat est donné dans le Tableau 53.

Tableau 53: La probabilité CFP ajustée pour la mission « Réchauffer un four »

Étape ou activité de la tâche	Mode d'erreur	Probabilité CFP nominale	Facteur d'effet des CPCs	Probabilité CFP ajustée
0.1.1 Assurer que l'installation est prête	I2. Erreur de décision	1.00E-02	7.5	7.50E-02
0.1.2 Assurer que le gasoil est disponible	O3. L'observation n'est pas faite	7.00E-02	7.5	5.25E-01
0.1.3 Assurer que le système d'analyse d'O2 fonctionne	O3. L'observation n'est pas faite	7.00E-02	7.5	5.25E-01
0.2 Démarrer le ventilateur d'air	E3. Action réalisée sur mauvais objet	5.00E-04	7.5	3.75E-03
0.3 Démarrer la pompe à huile	E4. Action réalisée avec mauvais séquence	3.00E-03	7.5	2.25E-02
0.4.1 Augmenter la température avec un contrôle graphique	E1. Exécution d'un mauvais type	3.00E-03	7.5	2.25E-02
0.4.2 Surveiller l'O2	O3. L'observation n'est pas faite	7.00E-02	7.5	5.25E-01
0.4.3 Surveiller la température	O3. L'observation n'est pas faite	7.00E-02	7.5	5.25E-01
0.4.4.1 Vérifier si la température atteint 800 °C	I2. Erreur de décision	1.00E-02	7.5	7.50E-02
0.4.4.2 Ensuite, basculer le four en mode automatique.	E2. Action réalisée au mauvais temps	3.00E-03	7.5	2.25E-02

- ***Approche détaillée :*** La valeur CFP ajustée est calculée par la formule suivante :

CFP ajustée = CFP nominale x facteur d'effet spécifique

Afin d'évaluer les effets spécifiques des CPCs sur la probabilité CFPs nominale de chaque activité, il faut combiner les informations données dans les tableaux : Tableau 32, Tableau 46, Tableau 51 et Tableau 52. Les facteurs d'effet sont ainsi déterminés et présentés dans le Tableau 54

Tableau 55 : Évaluation des facteurs d'effets spécifiques des CPCs sur les défaillances des fonctions cognitives

		Tâches / Défaillances cognitives									
Nom de la CPC	**Niveau**	**0.1.1**	**0.1.2**	**0.1.3**	**0.2**	**0.3**	**0.4.1**	**0.4.2**	**0.4.3**	**0.4.4**	
		I2	**O3**	**O3**	**E3**	**E4**	**E1**	**O3**	**O2**	**I2**	**E3**
Adéquation de l'organisation	Inefficace	1.0	1.0	1.0	1.2	1.2	1.2	1.0	1.0	1.0	1.2
Conditions de travail	Compatible	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0
Adéquation des interfaces Homme-Machine et des outils	Tolérable	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0
Disponibilités de procédures et des plans	Inapproprié	1.0	2.0	2.0	2.0	2.0	2.0	2.0	2.0	1.0	2.0
Nombre de buts simultanés	Correspond aux capacités	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0
Temps disponible	Adéquat	0.5	0.5	0.5	0.5	0.5	0.5	0.5	0.5	0.5	0.5
Rythme circadien	Jour (ajusté)	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0
Adéquation de l'entraînement et de l'expérience	Inadéquate	5.0	2.0	2.0	2.0	2.0	2.0	2.0	2.0	5.0	2.0
Qualité de la collaboration au sein de l'équipe	Déficient	2.0	2.0	2.0	5.0	5.0	5.0	2.0	2.0	2.0	5.0
Note totale des CPCs ou facteur d'effets spécifiques des CPCs		**5**	**4**	**4**	**12**	**12**	**12**	**4**	**4**	**5**	**12**

Ainsi, la probabilité CFP ajustée peut être calculée pour toutes les activités de la mission en appliquant les facteurs spécifiques des CPCs donnés dans le Tableau 55. Le résultat est présenté dans le Tableau 56.

Tableau 56: *La probabilité CFP ajustée pour la mission « Réchauffer un four »*

Étape ou activité de la tâche	Mode d'erreur	Probabilité CFP nominale	Facteur d'effet des CPCs	Probabilité CFP ajustée
0.1.1 Assurer que l'installation est prête	I2. Erreur de décision	1.00E-02	5	5.00E-02
0.1.2 Assurer que le gasoil est disponible	O3. L'observation n'est pas faite	7.00E-02	4	2.80E-01
0.1.3 Assurer que le système d'analyse d'O2 fonctionne	O3. L'observation n'est pas faite	7.00E-02	4	2.80E-01
0.2 Démarrer le ventilateur d'air	E3. Action réalisée sur mauvais objet	5.00E-04	12	6.00E-03
0.3 Démarrer la pompe à huile	E4. Action réalisée avec mauvais séquence	3.00E-03	12	3.60E-02
0.4.1 Augmenter la température avec un contrôle graphique	E1. Exécution d'un mauvais type	3.00E-03	12	3.60E-02
0.4.2 Surveiller l'O2	O3. L'observation n'est pas faite	7.00E-02	4	2.80E-01
0.4.3 Surveiller la température	O3. L'observation n'est pas faite	7.00E-02	4	2.80E-01
0.4.4.1 Vérifier si la température atteint 800 °C	I2. Erreur de décision	1.00E-02	5	5.00E-02
0.4.4.2 Ensuite, basculer le four en mode automatique	E2. Action réalisée au mauvais temps	3.00E-03	12	3.60E-02

La moyenne des facteurs d'effets spécifiques des CPCs est de 7,4 pour l'approche détaillée. Il est cohérent de trouver que cette valeur est quasi identique à celle du facteur d'effet moyen (7,5) déterminé par l'approche simplifiée. Cependant, l'approche détaillée nous permet d'étudier de façon plus fine les effets des CPCs sur chaque tâche. Dans cet exemple, on constate que le contexte de la mission a un effet négatif sur toutes les activités cognitives, cependant cet effet est plus prononcé sur les activités cognitives d'exécutions 0.2 ; 0.3 ; 0.4.1 ; 0.4.4.2.

Étape n°4 : Incorporer les valeurs CFPs ajustées dans l'arbre d'événement.

Afin d'incorporer la probabilité CFP ajustée dans l'arbre d'événement de PSA, il faut déterminer une valeur de la probabilité CFP ajustée pour l'événement intéressé. Par exemple, on a besoin de la probabilité d'échec globale de la mission « Réchauffer un four ». Selon l'analyse de tâche, les quatre étapes de la mission doivent être réalisées correctement afin d'assurer la réussite de la mission. Donc, l'échec de l'une des quatre étapes entraînera l'échec de la mission. La probabilité d'échec globale est la valeur maximum des probabilités d'échec des étapes élémentaires. Donc elle est égale à 0,28 ou 28% qui correspond aux étapes 0.1.2 ; 0.1.3 ; 0.4.2 et 0.4.3 qui concernent les activités cognitives d'observation et de surveillance.

Application de la méthode MERMOS

Exemple 1 : Analyse de l'accident « Three Mile Island » : Le Bot P. a réalisé une analyse rétrospective cet accident [64], [68] en utilisant la méthode MERMOS.

Exemple 2 :

La mission « Redémarrer un four suite à un arrêt du système » ou « Réchauffer un four » donnée dans CREAM [44] est utilisée pour illustrer la méthode MERMOS, avec les hypothèses suivantes :

- Il n'existe ni support procédural, ni formation ou entraînement spécifique pour la tâche « Réchauffer un four ».
- Cette tâche n'est pas considérée comme importante, au moins du point de vue de la sécurité, bien que les conséquences puissent être très graves.
- Tout opérateur peut être amené à réaliser la tâche, quelle que soit sa formation (apprentis, apprentissage à partir de son collègue plus expérimenté, etc…).

Donc, l'organisation doit être considérée comme insuffisante.

Module 1 : L'identification et définition des missions FH

- Description de la mission
    - Objectifs fonctionnels de la mission :
        - Le four doit être redémarré et opérationnel à l'échéance donnée.
    - Critère de succès :
        - Le four doit être réchauffé à 800 °C à l'échéance donnée,
        - Le four doit être maintenu à 800°C pour une durée donnée,
        - Maîtrise de la température pendant la phase de redémarrage,
        - Maîtrise des risques d'explosion du four.

Module 2 : L'analyse qualitative et quantitative des missions FH

- Décomposition fonctionnelle de la mission en fonctions SAD

  En pratique, cette étape n'est pas réalisée systématiquement.
    - Fonction de la STRATEGIE
        - Objectifs :
            - Augmenter la température du four jusqu'à 800°C en conformité au contrôle graphique.
            - Maintenir la température du four à 800°C pendant une durée requise.
        - Objectifs concurrents : pas d'objectif concurrent.

- Fonction de l'ACTION
  - Pour réussir la mission, les actions et leur séquence présentées dans la Figure 42 doivent être réalisées avec succès.

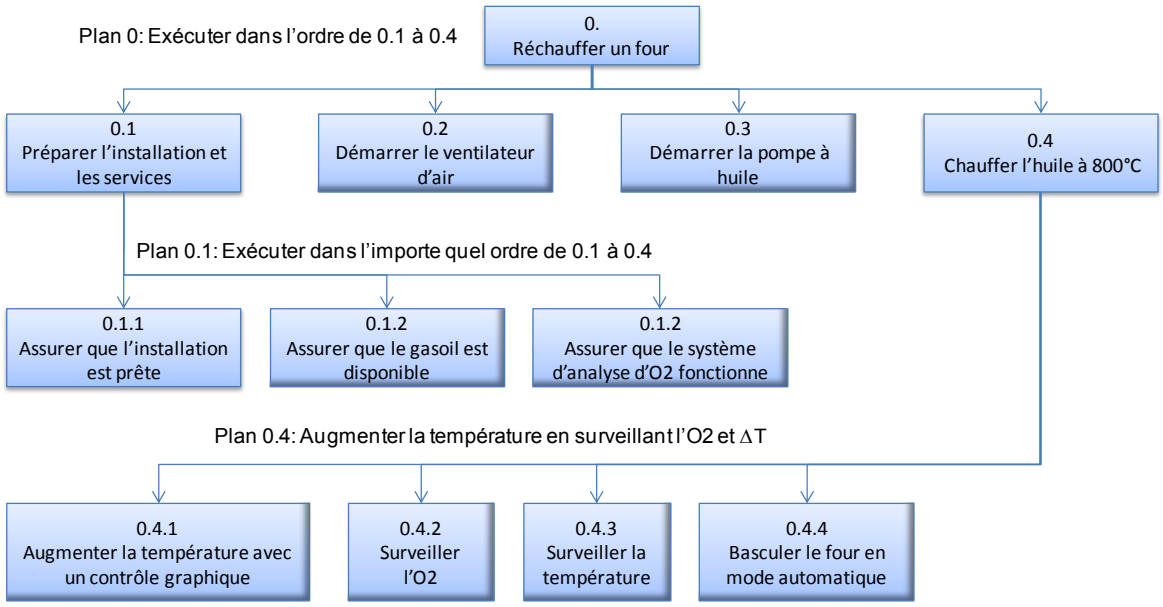


Figure 42 : Les actions et leur séquence de la mission « Réchauffer un four »

- Fonction du DIAGNOSTIC
  - Les paramètres pertinents de la mission :
    - Le niveau du gasoil,
    - L'indicateur de l'état du système d'analyse de l'oxygène,
    - La température du four en conformité au gradient de température.
  - La nature des accidents
    - Surchauffement du four
    - Arrêt accidentel du four
  - L'évolution des paramètres
    - Variation de la température du four
    - Variation du niveau du gasoil et de l'oxygène
  - Les parades à envisager
    - Indicateur du niveau de gasoil en salle de contrôle
    - Alarme sur un surchauffement du four
    - Alarme sur l'arrêt de flamme du four

L'analyse qualitative de la mission est réalisée à travers une revue quasi-AMDEC pour identifier les scénarios, les CICAs, les éléments contextuels et les modalités de non satisfaction. Suite à cette analyse de la mission, les scénarios et leur modalité de non satisfaction (ou non reconfiguration) sont identifiés et présentés dans le ***Tableau 57***.

Tableau 57: Étude AMDEC de la mission « Réchauffer un four »

Modes de défaillance	Scénarios/CICAs	Modalités de non satisfaction
Pas de stratégie	L'opérateur s'interroge trop longtemps sur la séquence d'action à prendre. Cela peut conduire à un non-respect de l'échéance requise ou à un défaut de la maîtrise de la température	Hésitation sur le moyen à retenir, ou sur les actions à réaliser
Stratégie erronée	Priorité à la recherche des causes au lieu de maîtriser la sécurité du four	Retard dans les actions nécessaires pour la sécurité du système ou pour la mission
Pas d'action	L'oubli dans la préparation de l'installation et des services	Défaillances des équipements ou manque de gasoil
Pas d'action	Inattention de l'opérateur dans la surveillance de température entrainant à une augmentation de la température excessive.	Pas d'action corrective à temps
Pas d'action	Inattention de l'opérateur dans la surveillance de température : la température dépasse 800°C	Pas d'action pour basculer le four en mode automatique
Action erronée	L'opérateur réalise une séquence d'action erronée. Cela peut conduire à un non-respect de l'échéance requise ou à un défaut de la maîtrise de la température ou à une explosion	Pas d'actions correctives à temps
Pas de diagnostic de situation	Le système ne réalise pas un diagnostic à temps	Retard dans le déroulement des consignes
Diagnostic de situation erronée	Le système réalise un diagnostic erroné	Des actions non appropriées sont mises en œuvre

Une fiche d'analyse détaillée doit être rédigée contenant les informations sur les éléments contextuels ou propriétés de situation, les CICAs, la modalité de non satisfaction. Pour illustrer cette démarche, le scénario « le système ne réalise pas un diagnostic à temps » est développé en détail ci-dessous.

Tableau 58: Fiche du scénario global «Le système ne réalise pas un diagnostic à temps»

	Probabilité
Scénario Le système ne réalise pas un diagnostic à temps	**8,00E-05**
Modalité de non satisfaction Retard dans le déroulement des consignes	9,00E-01
CICA Les indicateurs présents en salle de contrôle informent que la température n'augmente plus; l'opérateur ne sait pas ce qu'il faut faire ou il focalise sur la recherche des causes de cette panne.	9,00E-01
Propriétés de situation ou éléments contextuels	
1) La défaillance du système d'information de température et il n'existe pas de système de signalisation ou ce dernier est aussi défaillant	1,00E-02
2) Le niveau du gasoil est insuffisant et il n'existe pas le système de signalisation ou ce dernier est défaillant	1,00E-01
3) Le niveau de l'oxygène est insuffisant et il n'existe pas le système de signalisation ou ce dernier est défaillant	1,00E-01
4) La procédure de traitement de cette situation n'est pas disponible	1,00E-00

Ainsi la probabilité du scénario peut être calculée en utilisant la formule de la méthode

$$P(scénario_i) = \prod_{j=1}^{m} P(contexte_j / initiateur_et_aggravants) \times \prod_{k=1}^{p} P(CICA_k / contexte) \times P(non_reconfiguration)$$

$$\prod_{j=1}^{m} P(contexte_j / initiateur_et_aggravants) = 1{,}00E-02 \times 1{,}00E-01 \times 1{,}00E-01 \times 1{,}00E-00 = 1{,}00E-04$$

$$\prod_{k=1}^{p} P(CICA_k / contexte) = 9{,}00E-01$$

$$P(non_reconfiguration) = 9{,}00E-01$$

P(scénario) = 1,00E-04 x 9,00E-1 x 9,00E-01 = 8,00E-05

Cependant, on remarque que la présence simultanée des trois premiers éléments contextuels n'est pas nécessaire pour la survenance de la CICA. Un de ces trois éléments contextuels peut éventuellement conduire à la survenue de la CICA, donc trois autres scénarios qui correspondent aux trois premiers éléments contextuels sont aussi possibles. Dans ce cas, la probabilité d'occurrence de la CICA devrait être ajustée pour chaque scénario. Ces trois scénarios sont présentés dans les tableaux (Tableau 59,Tableau 60 et Tableau 61).

Tableau 59 : Fiche du scénario : « Le système ne réalise pas un diagnostic à temps, dû à défaut du système de température »

	Probabilité
Scénario Le système ne réalise pas un diagnostic à temps	**9,00E-04**
Modalité de non satisfaction Retard dans le déroulement des consignes	9,00E-01
CICA Le système informe que la température n'augmente plus et l'opérateur ne sait pas ce qu'il faut faire ou il focalise sur la recherche des causes de cette panne.	1,00E-01
Propriétés de situation ou éléments contextuels 1) La défaillance du système d'information de température et il n'existe pas le système de signalisation ou ce dernier est défaillant 2) La procédure de traitement de cette situation n'est pas disponible	1,00E-02 1,00E-00

Tableau 60 : Fiche du scénario :
«Le système ne réalise pas un diagnostic à temps, dû au niveau de gasoil »

	Probabilité
Scénario Le système ne réalise pas un diagnostic à temps	**9,00E-03**
Modalité de non satisfaction Retard dans le déroulement des consignes	9,00E-01
CICA Le système informe que la température n'augmente plus et l'opérateur ne sait pas ce qu'il faut faire ou il focalise sur la recherche des causes de cette panne.	1,00E-01
Propriétés de situation ou éléments contextuels 1) Le niveau du gasoil est insuffisant et il n'existe pas le système de signalisation ou ce dernier est défaillant 2) La procédure de traitement de cette situation n'est pas disponible	1,00E-01 1,00E-00

Tableau 61 : Fiche du scénario :
«Le système ne réalise pas un diagnostic à temps, dû au niveau de d'oxygène »

	Probabilité
Scénario Le système ne réalise pas un diagnostic à temps	**9,00E-03**
Modalité de non satisfaction	

Retard dans le déroulement des consignes	9,00E-01
CICA Le système informe que la température n'augmente plus et l'opérateur ne sait pas ce qu'il faut faire ou il focalise sur la recherche des causes de cette panne.	1,00E-01
Propriétés de situation ou éléments contextuels 1) Le niveau de l'oxygène est insuffisant et il n'existe pas le système de signalisation ou ce dernier est défaillant 2) La procédure de traitement de cette situation n'est pas disponible	1,00E-01 1,00E-00

La probabilité globale de ces trois scénarios de l'ordre de 1,90E-02 = (9,00E-04 + 9,00E-03 + 9,00E-03) qui est sensiblement supérieur à la valeur de 8,00E-05 du scénario précédent, bien que la probabilité d'occurrence de la CICA du scénario global soit très élevée par rapport aux trois scénarios supplémentaires. Cependant, cela ne compense pas la rareté de la situation du scénario global qui est une combinaison des situations exceptionnelles.

Cet exemple prouve que si l'on focalise trop sur les CICAs générés par des contextes très particuliers, certes la probabilité conditionnelle de survenue de ces CICAs est très élevée, proche de 1, et l'on ne retient que ces scénarios, on peut être piégé par des conclusions sur la fiabilité très optimistes.

La probabilité résiduelle est estimée en fonction de la valeur de probabilité globale de tous les scénarios retenus et les éléments structurels.

Si le scénario global est le seul scénario retenu, la probabilité résiduelle $P_{résiduelle}$ est estimée comme suit :

$P_{résiduelle} = 10^{-5} \times 3 = 3{,}00$ E-05, supposons que l'influence des propriétés structurelles est moyennement pénalisante.

Si les trois scénarios supplémentaires sont retenus avec le scénario global, la probabilité globale des scénarios sera supérieure à 1,00E-02. Dans ce cas, $P_{résiduelle} = 1{,}00$E-04.

Application de la méthode SHERPA

La même mission « Redémarrer un four suite à un arrêt du système » ou « Réchauffer un four » est utilisée pour tester la méthode SHERPA.

L'analyse hiérarchisée des tâches (HTA) est réalisée et présentée dans la Figure 37.

Le Tableau 62 représente la liste des activités et leur classification.

Tableau 62: La classification des tâches de la mission « Réchauffer un four »

N° de l'étape		Objectif	Étape ou activité de la tâche	Classe d'activité
0.1	0.1.1	Préparer l'installation et les services	Assurer que l'installation est prête	Vérification
	0.1.2		Assurer que le gasoil est disponible	Vérification
	0.1.3		Assurer que le système d'analyse d'O2 fonctionne	Vérification
0.2		Démarrer le ventilateur d'air	Démarrer le ventilateur d'air	Action
0.3		Démarrer la pompe à huile	Démarrer la pompe à huile	Action
0.4	0.4.1	Chauffer l'huile à 800°C	Augmenter la température avec un contrôle graphique	Action - Vérification
	0.4.2		Surveiller l'O2	Acquisition
	0.4.3		Surveiller la température	Acquisition
	0.4.4		Basculer le four en mode automatique lorsque la température atteint 800 °C	Vérification - Action

L'identification des erreurs humaines est ensuite réalisée sur les activités identifiées et classées ci-dessus. Le résultat est donné dans le Tableau 63.

Tableau 63: Résultat SHERPA de la mission « Réchauffer un four »

N° de l'étape	Mode d'erreurs	Description d'erreurs	Conséquence	Rattrapage	Probabilité	Criticité	Mesure de réduction de risque
0.1.1	C1	Vérification omise	L'opération peut être interrompue	Non	L	M	Check-list
			Peut causer des accidents avec les installations	Non	L	C	Check-list
	C2	Vérification incomplète	L'opération peut être interrompue	Non	M	M	Check-list
			Peut causer des accidents avec les installations	Non	M	C	Check-list
0.1.2	C1	Vérification omise	L'opération peut être interrompue	Non	L	M	Check-list
0.1.3	C1	Vérification omise	L'opération peut être interrompue	Non	L	M	Check-list
0.2	A2	Action trop tard	Le four peut être rempli par un mélange explosif → explosion	Non	M	H	Check-list, Alarme
	A8	Action omise	Le four peut être rempli par un mélange explosif → explosion	Non	L	H	Check-list, Alarme
0.3	A2	Action trop tôt	Le four peut être rempli par un mélange explosif → explosion	Non	M	H	Check-list, Alarme
	A8	Action omise	Pas de démarrage	Oui, immédiate	L	L	Check-list

N° de l'étape	Mode d'erreurs	Description d'erreurs	Conséquence	Rattrapage	Probabilité	Criticité	Mesure de réduction de risque
0.4.1	A2	Action trop tôt / trop tard	Le profil de la température n'est pas conforme	Oui	H	M	Système automatique ? alarme
	A8	Action omise	Retarder le redémarrage du four	Oui	L	M	Alarme
	C2	Vérification incomplète	Le profil de la température n'est pas conforme	Non	M	M	Système automatique ? alarme
0.4.2	R1	Information n'est pas obtenue	L'opération peut être interrompue	Non	L	M	Système en parallèle
	R2	Acquisition de mauvaise information	L'opération peut être interrompue	Non	L	M	Système en parallèle
0.4.3	R1	Information n'est pas obtenue	Le four peut être surchauffé ou pas assez chauffé	Non	L	M	Système en parallèle
	R2	Acquisition de mauvaise information	Le four peut être surchauffé ou pas assez chauffé	Non	L	M	Système en parallèle
0.4.4	C1	Vérification omise	Surchauffe	Non	L	H	Alarme, système automatique ?
	A2	Action trop tôt / trop tard	Le four peut être surchauffé ou pas assez chauffé		M	M	Alarme, système automatique ?
	A8	Action omise	Surchauffe	Non	L	H	Alarme, système automatique ?

Application de la méthode TRIPOD

Pour la mission « Redémarrer un four suite à un arrêt du système » ou « Réchauffer un four », il semble que la méthode TRIPOD fournit difficilement des résultats adéquats. Car le meilleur échantillon pour réaliser la méthode Tripod est l'équipe qui réalise la mission. D'autre part, la liste des questions n'est pas disponible pour réaliser l'étude.

Application de la méthode ACIH

La même mission « Redémarrer un four suite à un arrêt du système » ou « Réchauffer un four » est utilisée pour tester la version APRECIH de la méthode ACIH (Analyse des Conséquences de l'Infiabilité Humaine).

Étape 1 : Analyse fonctionnelle du système homme-machine

L'analyse fonctionnelle identifie toutes les fonctions nécessaires pour réaliser la mission.

Fonction 1 (F1) : Organiser la mission

- Définir les besoins, les objectifs
- Planifier la mission
- Réguler la mission :
    - Surveiller la mission
    - Modifier la mission
    - Contrôler la mission

Fonction 2 (F2) : Assurer le bon fonctionnement du système

- Assurer que les ressources humaines sont suffisantes
- Assurer que l'installation est prête
- Assurer que le gasoil est disponible
- Assurer que le système d'analyse d'oxygène fonctionne

Fonction 3 (F3) : Démarrer les équipements

- Démarrer le ventilateur d'air
- Démarrer la pompe - d'huile

Fonction 4 (F4) : Augmenter la température à 800 °C avec un contrôle graphique de température

Fonction 5 (F5) : Maintenir la température du four à 800 °C

Pour cette mission, on identifie une seule procédure P1 disponible qui concerne toutes les fonctions du système mentionnées au-dessus sauf la fonction F1.

Tableau 64: Interaction entre les procédures et les fonctions du système

Procédures		**Fonctions**			
	F1	**F2**	**F3**	**F4**	**F5**
P1	0	1	1	1	1

(0 : pas d'interaction ; 1 : interaction)

Étape 2 : Analyse procédurale et contextuelle

La procédure P1 se compose des tâches suivantes :

T1 : Assurer que l'installation est prête

T2 : Assurer que le gasoil est disponible

T3 : Assurer que le système d'analyse d'O_2 fonctionne

T4 : Démarrer le ventilateur d'air

T5 : Démarrer la pompe à huile

T6 : Augmenter la température avec un contrôle graphique

T7 : Surveiller l'O_2

T8 : Surveiller la température

T9 : Basculer le four en mode automatique lorsque la température atteint 800 °C

Il peut exister des contextes différents d'exécution de cette mission :

- Contexte 1 (C1) : Redémarrage du four après la période de la maintenance.
- Contexte 2 (C2) : Redémarrage suite à un arrêt accidentel du four

Pour le contexte C2, plusieurs procédures spécifiques doivent être préparées pour faire face aux différentes situations, telles que :

- Arrêt dû à l'épuisement de gasoil,
- Arrêt dû aux défaillances du ventilateur d'air, ou de la pompe à l'huile,
- Etc.

Étape 3 : Analyse des tâches et de l'activité

Chaque tâche est analysée pour identifier les comportements humains en trois catégories :

- Phase d'acquisition
- Phase de traitement de l'information
- Phase d'action.

Tableau 65: Identification des comportements réels lors d'exécution de tâche

Tâche	**Comportement humain**
T1 : Assurer que l'installation est prête	Traitement de l'information
T2 : Assurer que le gasoil est disponible	Traitement de l'information
T3 : Assurer que le système d'analyse d'O_2 fonctionne	Traitement de l'information
T4 : Démarrer le ventilateur d'air	Action
T5 : Démarrer la pompe à huile	Action
T6 : Augmenter la température avec un contrôle graphique	Action
T7 : Surveiller l'O_2	Acquisition

Tâche	Comportement humain
T8 : Surveiller la température	Acquisition
T9 : Basculer le four en mode automatique lorsque la température atteint 800 °C	Action

Étape 4 : Identification des caractéristiques de tâches ou des modes de dérives comportementales

Cette étape consiste à identifier les modes de défaillances du comportement humain pour chaque tâche. Le résultat est résumé dans le Tableau 66 suivant.

Tableau 66: Identification des modes de dérives des comportements humains

Tâche	Comportement humain	Mode de dérives
T1 : Assurer que l'installation est prête	Traitement de l'information	- Omis - Incorrectement
T2 : Assurer que le gasoil est disponible	Traitement de l'information	- Omis - Incorrectement
T3 : Assurer que le système d'analyse d'O_2 fonctionne	Traitement de l'information	- Omis - Incorrectement
T4 : Démarrer le ventilateur d'air	Action	- Omis
T5 : Démarrer la pompe à huile	Action	- Omis
T6 : Augmenter la température avec un contrôle graphique	Action	- Incorrectement
T7 : Surveiller l'O_2	Acquisition	- Incorrectement
T8 : Surveiller la température	Acquisition	- Incorrectement
T9 : Basculer le four en mode automatique lorsque la température atteint 800 °C	Action	- Omis - Incorrectement

Étape 5 : Analyse de conséquences

Les scénarios d'infiabilité humaine peuvent être établis par des combinaisons possibles des états des tâches élémentaires donnés dans le Tableau 66. Les conséquences sont ainsi estimées pour chaque scénario.

Le nombre de scénario peut être estimé ci-après à partir de 10 tâches élémentaires, supposons qu'un seul mode de dérive est retenu pour chaque tâche :

Le nombre de scénario = 10 + $C_{10}^{2}+C_{10}^{3}+C_{10}^{4}+C_{10}^{5}+C_{10}^{6}+C_{10}^{7}+C_{10}^{8}+C_{10}^{9}+C_{10}^{10}$

= $3{,}24 \cdot 10^{15}$

Il est impossible de décrire tous les scénarios pour cet exemple.

Un extrait des résultats est donné dans le Tableau 67.

Tableau 67: Extrait des scénarios et leurs conséquences

Scénarios	**État de tâches**									**Conséquences**
	T1 Assurer que l'installation est prête	T2 Assurer que le gasoil est disponible	T3 Assurer que le système d'analyse d'O_2 fonctionne	T4 Démarrer le ventilateur d'air	T5 Démarrer la pompe à huile	T6 Augmenter la température avec un contrôle graphique	T7 Surveiller l'O_2	T8 Surveiller la température	T9 Basculer le four en mode automatique lorsque la température atteint 800 °C	
1	Omis	Correct	Correct	Correct	Correct	Correct	Correct	Correct	Correct	1
2	Incorrect	Correct	Correct	Correct	Correct	Correct	Correct	Correct	Correct	1
3	Correct	Omis	Correct	Correct	Correct	Correct	Correct	Correct	Correct	1
4	Correct	Correct	Omis	Correct	Correct	Correct	Correct	Correct	Correct	1
5	Correct	Correct	Correct	Omis	Correct	Correct	Correct	Correct	Correct	1
6	Correct	Correct	Correct	Correct	Omis	Correct	Correct	Correct	Correct	1
7	Correct	Correct	Correct	Correct	Correct	Incorrect	Correct	Correct	Correct	1
8	Correct	Correct	Correct	Correct	Correct	Correct	Incorrect	Correct	Correct	1
9	Correct	Correct	Correct	Correct	Correct	Correct	Correct	Incorrect	Correct	1
10	Correct	Correct	Correct	Correct	Correct	Correct	Correct	Correct	Omis	-
11	Correct	Correct	Correct	Correct	Correct	Correct	Correct	Correct	Incorrect	1
12	Omis	Omis	Correct	Correct	Correct	Correct	Correct	Correct	Correct	2
13	Omis	Correct	Omis	Correct	Correct	Correct	Correct	Correct	Correct	2
14	Omis	Correct	Correct	Omis	Correct	Correct	Correct	Correct	Correct	2
15	Omis	Correct	Correct	Correct	Omis	Correct	Correct	Correct	Correct	2
16	Omis	Correct	Correct	Correct	Correct	Incorrect	Correct	Correct	Correct	2

Scénarios	État de tâches									Conséquences
	T1 Assurer que l'installation est prête	T2 Assurer que le gasoil est disponible	T3 Assurer que le système d'analyse d'O_2 fonctionne	T4 Démarrer le ventilateur d'air	T5 Démarrer la pompe à huile	T6 Augmenter la température avec un contrôle graphique	T7 Surveiller l'O_2	T8 Surveiller la température	T9 Basculer le four en mode automatique lorsque la température atteint 800 °C	
17	Omis	Correct	Correct	Correct	Correct	Correct	Incorrect	Correct	Correct	2
18	Omis	Correct	Correct	Correct	Correct	Correct	Correct	Incorrect	Correct	2
19	Omis	Correct	Correct	Correct	Correct	Correct	Correct	Correct	Incorrect	2
20	Correct	Omis	Omis	Correct	Correct	Correct	Correct	Correct	Correct	2
21	Correct	Omis	Correct	Omis	Correct	Correct	Correct	Correct	Correct	2
22	Correct	Omis	Correct	Correct	Omis	Correct	Correct	Correct	Correct	2
23	Correct	Omis	Correct	Correct	Correct	Incorrect	Correct	Correct	Correct	2
24	Correct	Omis	Correct	Correct	Correct	Correct	Incorrect	Correct	Correct	2
25	…									

Application de la méthode FRAM

La même mission « Redémarrer un four suite à un arrêt du système » ou « Réchauffer un four » est étudiée avec la méthode FRAM.

Les hypothèses retenues pour l'évaluation de cette mission sont les suivantes :

- Il n'existe ni support procédural, ni formation ou entraînement spécifique pour la tâche « Réchauffer un four ».
- Cette tâche n'est pas considérée comme importante, au moins du point de vue de la sécurité, bien que les conséquences puissent être très graves.
- Tout opérateur peut être amené à réaliser la tâche, quelle que soit sa formation (apprentis, apprentissage à partir de son collègue plus expérimenté, etc.…).

Donc, l'organisation doit être considérée comme insuffisante.

Étape 1 : Identifier et caractériser les fonctions essentielles

L'analyse fonctionnelle de la mission permet d'identifier les fonctions essentielles de la mission. Ces fonctions identifiées sont données dans le Tableau 68.

Tableau 68: Les fonctions de la missions « redémarrer un four »

Id.	Nom	Description	Catégorie
F1	Préparation de l'installation et des services	Fonction réalisée par un opérateur à l'aide d'une procédure pour assurer si : - l'installation est prête - le gasoil est disponible - le système d'analyse d'O_2 fonctionne	H-T-O
F2	Démarrage des équipements auxiliaires	Fonction réalisée par un opérateur à l'aide d'un système de commande pour démarrer - le ventilateur d'air - la pompe à l'huile	H-T
F3	Allumage du four	Fonction réalisée par un opérateur à l'aide d'un système de commande	H-T
F4	Surveillance et contrôle du four	Fonction réalisée par un opérateur à l'aide d'un système de commande et de surveillance informatisée : - Surveiller l'O_2 - Surveiller la température - Augmenter la température avec un contrôle graphique - Basculer le four en mode automatique lorsque la température atteint 800 °C	H-T

Les caractéristiques de chaque fonction sont ainsi identifiées et analysées. Le Tableau 69 représente la description des attributs pour toutes les fonctions.

Tableau 69: Les attributs des fonctions de la missions « redémarrer un four »

Attribut	Fonction			
	F1 Préparation de l'installation et des services	***F2*** Démarrage des équipements auxiliaires	***F3*** Allumage du four	***F4*** Surveillance et contrôle du four
Input	- Ordre de mission	- Autorisation de démarrage	- Disponibilité d'air et d'huile	- Démarrage du four
Pré-condition		- Gasoil est disponible		
Ressource	- Un opérateur - Moyen de communication - Autres moyens techniques	- Un opérateur - Interface Homme-machine	- Un opérateur - Interface Homme-machine	- Un opérateur - Interface Homme-machine
Control	- Procédure	- Visuel	- Visuel	- Visuel
Time				- Minuteur
Output	- Autorisation de démarrage des équipements - Disponibilité des installations et services	- Disponibilité d'air et d'huile	- Température du four	- Actions appropriées

Étape 2 : Déterminer la variabilité potentielle du contexte dépendant

Cette étape consiste tout d'abord à identifier les conditions de performances communes (CPCs) applicables à chaque fonction. Les CPCs sont présentées dans le Tableau 70.

Tableau 70: Les conditions de performance CPCs applicables à chaque fonction

Id.	Nom	Conditions de performance CPCs
F1	Préparation de l'installation et des services	C1 – C4 – C5 - C10 – C11
F2	Démarrage des équipements auxiliaires	C4
F3	Allumage du four	C4
F4	Surveillance et contrôle du four	C4 - C5 – C6 – C7 – C8

Pour chaque fonction, les conditions de performance sont contextualisées pour la situation de la mission. Le Tableau 71 résume l'ensemble des CPCs dans le contexte de la mission.

Tableau 71: Les conditions de performance CPCs contextualisées

Id.	CPC	Conditions de performance contextualisées
F1	C_1^1	Disponibilité du moyen de communication avec des différents services
	C_4^1	Qualité de l'IHM des installations
	C_5^1	Disponibilité de la procédure de vérification des installations
	C_{10}^1	Qualité de collaboration avec d'autres équipes
	C_{11}^1	Qualité et support de l'organisation pour faciliter la vérification
F2	C_4^2	Qualité de l'IHM ventilateur d'air
	C_5^2	Disponibilité de la procédure de démarrage du ventilateur d'air
	C_4^3	Qualité de l'IHM pompe à huile
	C_5^3	Disponibilité de la procédure de démarrage de la pompe à huile
F3	C_4^4	Qualité de l'IHM four
	C_5^4	Disponibilité de la procédure de l'allumage du four
F4	C_4^5	Qualité de l'IHM système de contrôle du four
	C_5^5	Disponibilité de la procédure de contrôle de la température du four
	C_6^1	Qualité de conditions de travail de contrôle du four
	C_7^1	Nombre d'objectifs simultanés
	C_8^1	Temps disponible

L'étape suivante consiste à évaluer la variabilité des CPCs identifiées, par une expertise collective entre les différents spécialistes de chaque domaine, en trois niveaux de variabilité :

- $\nu 1$: stable ou variable mais adapté ;
- $\nu 2$: stable ou variable mais inadapté ;
- $\nu 3$: imprévisible.

Selon les hypothèses de la mission, aucune procédure et aucun support ne sont disponibles. Donc, la variabilité CPCs concernant les procédures et de l'organisation est considérée comme très élevée.

Pour chaque CPC, les fonctions impactées sont aussi identifiées.

Les résultats de cette évaluation est donnée dans le Tableau 72.

Tableau 72: Variabilité des conditions de performance CPCs et les fonctions impactées

CPC	Conditions de performance ajoutées	Valeur	Fonctions impactées
C_1^1	Disponibilité du moyen de communication avec différents services	$\nu 1$	F1
C_4^1	Qualité de l'IHM des installations	$\nu 1$	F1
C_4^2	Qualité de l'IHM ventilateur d'air	$\nu 1$	F1, F2
C_4^3	Qualité de l'IHM pompe à huile	$\nu 1$	F1, F2
C_4^4	Qualité de l'IHM four	$\nu 1$	F1, F3, F4
C_4^5	Qualité de l'IHM système de contrôle du four	$\nu 1$	F1, F3, F4
C_5^1	Disponibilité de la procédure de vérification des installations	$\nu 3$	F1, F2, F3, F4
C_5^2	Disponibilité de la procédure de démarrage du ventilateur d'air	$\nu 3$	F1, F2
C_5^3	Disponibilité de la procédure de démarrage de la pompe à huile	$\nu 3$	F1, F2
C_5^4	Disponibilité de la procédure de l'allumage du four	$\nu 3$	F1, F3
C_5^5	Disponibilité de la procédure de contrôle de la température du four	$\nu 3$	F4
C_6^1	Qualité de conditions de travail de contrôle du four	$\nu 1$	F4
C_7^1	Nombre d'objectifs simultanés	$\nu 2$	F1, F2, F3, F4
C_8^1	Temps disponible	$\nu 2$	F1, F4
C_{10}^1	Qualité de collaboration avec d'autres équipes	$\nu 1$	F1
C_{11}^1	Qualité et support de l'organisation pour faciliter la vérification	$\nu 1$	F1

Étape 3 : Appliquer le principe de résonance fonctionnelle sur les dépendances entre les activités et les fonctions

Le diagramme FRAM (Figure 43) est créé en mettant en relation des attributs identifiés dans le Tableau 69.

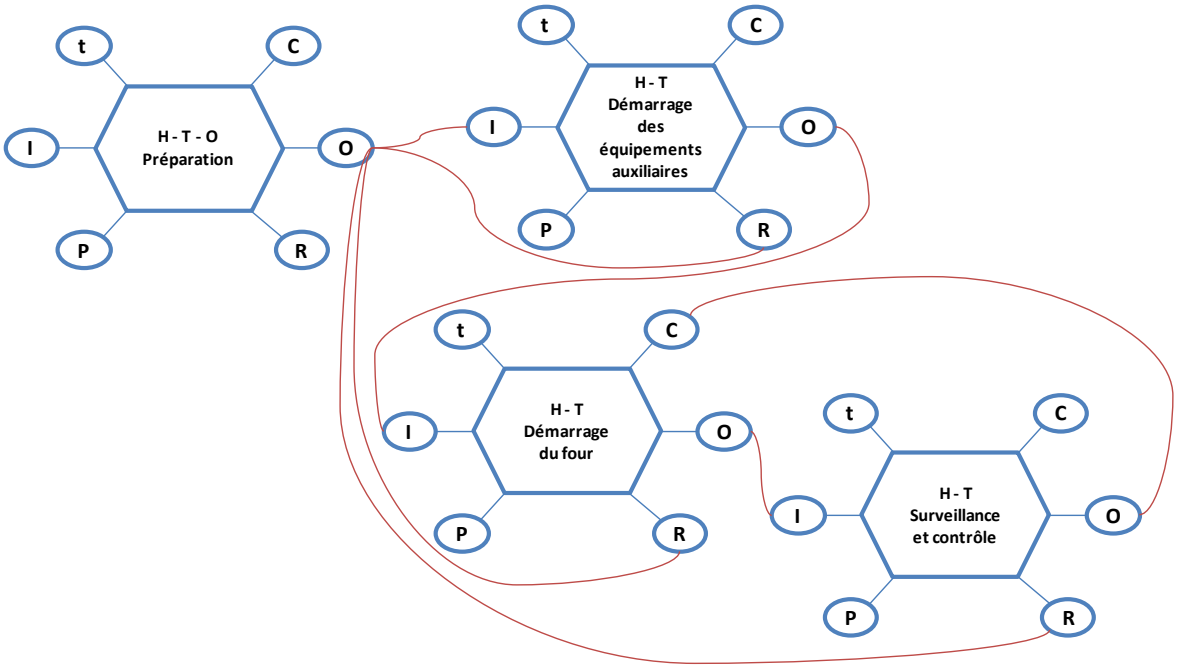


Figure 43 : Le réseau FRAM de la mission « Réchauffer un four »

On trouve que la fonction de préparation des équipements et des services a un impact important sur les autres fonctions. La variabilité de performance de cette fonction peut se propager vers d'autres fonctions de la mission et conduire à l'échec de la mission. L'indisponibilité des procédures conduit à une variabilité très élevée de la performance de la fonction de préparation des installations et des services. Cette fonction devient encore plus vulnérable si l'opérateur manque d'expérience, car ce critère n'est pas exigé par l'organisation.

L'absence de procédure peut causer aussi des variabilités pour les autres fonctions.

Étape 4 : Identifier les barrières contre la variabilité et spécifier les nécessaires mesures de surveillance de la performance

Afin de limiter la variabilité des fonctions, il faut établir les procédures pour toutes les opérations de la mission. Il est aussi nécessaire de former l'opérateur pour qu'il puisse se familiariser avec la mission.

INERIS

maîtriser le risque
pour un développement durable

Institut national de l'environnement industriel et des risques

Parc Technologique Alata
BP 2 - 60550 Verneuil-en-Halatte

Tél. : +33 (0)3 44 55 66 77 - Fax : +33 (0)3 44 55 66 99

E-mail : ineris@ineris.fr - **Internet :** http://www.ineris.fr