E-diagnostic

Frédéric VANDERHAEGEN, Professeur des Universités, UVHC. Responsable du projet et équipe pédagogique.

David JOUGLET, Maître de conférences, Université d'Artois. Equipe pédagogique.

Stéphane DURIEZ, médiatisateur, cellule TICE, UVHC. Equipe technique, Médiatisation du cours en ligne.

Olivier Delville, infographiste, cellule de médiatisation, service informatique, UVHC. Equipe technique.

Yann Picco, développeur, cellule TICE, UVHC. Equipe technique, Développement du simulateur et de l'éditeur de scénarios pour le simulateur.

Yohan Colmant, développeur, service informatique, UVHC. Equipe technique, coordination

Céline Faure, coordinatrice de la cellule TICE, UVHC. Equipe technique, coordination.

Arnaud Moulard, service informatique de l'UVHC. Equipe technique, coordination.

Table des matières

Introduction

I

Posons le problème suivant: votre voiture ne démarre pas, pourquoi ?

- Batterie hors service ?
- Démarreur hors service ?
- Panne d'essence ?
- Mauvais carburant ?
- Pas la bonne clef de contact ?
- Bougies encrassées ?

...

A votre avis, quelle(s) démarche(s) peut-on suivre pour trouver la cause réelle du problème ?

En général, on peut exploiter des démarches de diagnostic de bon fonctionnement et/ou de mauvais fonctionnement afin de rejeter ou de retenir certaines causes de ce dysfonctionnement, et ce en se basant sur des observations ou résultats de tests divers.

Par exemples:

- Si les portes ont été ouvertes avec la clef et les serrures n'ont jamais été refaites, on peut conclure qu'il s'agit de la bonne clef de contact
- Si les voyants du tableau de bord s'allument, les phares et la radio fonctionnent normalement, on peut conclure que la batterie n'est pas hors service
- Si le plein d'essence vient d'être fait, on peut conclure que ce n'est pas la panne d'essence
- Etc...

Ce cours est une **sensibilisation** à des techniques de **diagnostic** de fiabilité et/ou d'erreur dans le contrôle de procédés industriels. Il illustre par de nombreux exemples différentes démarches du diagnostic, en précisant ce que l'on doit diagnostiquer et comment on le fait. Les aspects homme-machine y sont traités.

La sûreté de fonctionnement homme-machine

II

La sûreté de fonctionnement est définie comme la science des défaillances. Dans un cadre plus général, nous parlerons de la science des dérives de fonctionnement.

Différents concepts peuvent alors être défini :

- Un **symptôme** est une observation de dérive.
- L'**erreur** est une dérive entre ce qui se passe réellement (le réel) et ce qui aurait dû se passer (le prescrit).
- **Une défaillance** est une dérive d'aptitude.
- **Une faute** est une dérive inacceptable

Dans différentes communautés, la définition de ces notions peut varier.

En général, pour étudier la sûreté de fonctionnement d'un système, on évalue ses propriétés. Pour un composant technique, on s'attachera à étudier la fiabilité, la disponibilité, la maintenabilité ou la sécurité :

- **La fiabilité** est la capacité d'un composant à réaliser les fonctions qui lui sont allouées dans un intervalle de temps donné.
- **La disponibilité** est la capacité d'un composant à être prêt à réaliser ces fonctions à un instant donné
- **La maintenabilité** est la capacité d'un composant à être maintenu ou réparé afin de pouvoir réaliser ces fonctions
- **La sécurité** est la capacité d'un composant à éviter l'occurrence d'événements catastrophiques.

Les caractéristiques d'un opérateur humain peuvent être assimilées à celles des composants techniques. Toutefois, en général, la notion de **fiabilité humaine** est aux facteurs humains ce que la sûreté de fonctionnement est aux facteurs techniques.

La fiabilité humaine concerne souvent la tâche à réaliser plutôt que la fonction. La tâche et la fonction renvoient à une notion commune : le but à atteindre. La **fonction** est liée à l'objectif du procédé piloté, c'est-à-dire au service rendu par celui-ci, la **tâche** est liée à l'objectif du moyen technique ou humain qui réalise cette fonction. Pour réaliser une fonction donnée, le comportement humain est subordonné à une prescription appelée **tâche** et ce qui est mis en oeuvre pour la réaliser est l'**activité**. Une erreur humaine renvoie alors à une dérive entre tâche effective, modèle issu de l'analyse de l'activité, et tâche prescrite, modèle de ce qui devrait être réalisé. Toutefois, l'omission d'une tâche peut être assimilée à une cessation de l'aptitude humaine et la réalisation incorrecte d'une tâche à une altération des capacités humaines. Les notions d'erreur et de défaillance humaines peuvent donc être confondues, et les concepts d'erreur ou de fiabilité humaines se rattachent à la capacité d'un opérateur humain à réaliser ses tâches respectivement avec ou sans dérives de comportement.

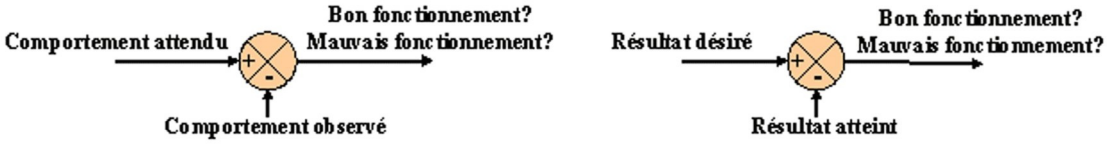
La fiabilité humaine est donc relative à l'exécution correcte de l'ensemble des tâches de l'opérateur regroupant les tâches de surveillance du comportement d'un

procédé donné, les tâches de contrôle de la sécurité du système homme-machine, les tâches de prévention et de récupération d'erreur humaine ou technique. En prenant en compte les contraintes d'interaction avec les tâches des autres opérateurs humains et celles des systèmes automatisés au travers d'interfaces de dialogue homme-machine, un opérateur humain doit par conséquent :

- prendre les décisions adéquates pour optimiser le fonctionnement du procédé dont il a la charge,
- récupérer les dérives anormales de fonctionnement du procédé ou de lui-même, en particulier celles que le système automatisé ne sait pas prendre en compte,
- contrôler les risques associés à ces dérives sans obligatoirement tenter de les récupérer mais en adaptant les modes opératoires initiaux,
- éviter l'occurrence d'événement catastrophique dû à ces dérives,
- et réguler sa propre activité afin d'être prêt à réagir ou de maintenir ses propres connaissances.

Ainsi, la fiabilité humaine est définie comme la capacité humaine à réaliser les tâches requises correctement et ne pas réaliser d'autres tâches nuisibles au bon fonctionnement du procédé. L'erreur humaine est son complémentaire : c'est la capacité humaine à ne pas réaliser les tâches prescrites correctement ou à réaliser d'autres tâches nuisibles au bon fonctionnement du procédé.

Le bon ou le mauvais fonctionnement d'un système est alors lié à une dérive entre un comportement réel et un comportement prescrit ou à un écart dans le résultat de cette dérive.



Le diagnostic d'une telle dérive de comportement ou de résultat est le processus d'évaluation d'un état de fonctionnement donné

III

Définitions des concepts relatifs au diagnostic

Le **diagnostic** est le processus d'évaluation d'un état de fonctionnement donné. L'élaboration d'un diagnostic nécessite de préciser sur quoi porte-t-il ?

A. Diagnostic de quoi

Le diagnostic de bon fonctionnement d'un procédé complexe tel un avion nécessite de connaître pourquoi et comment marche le système.

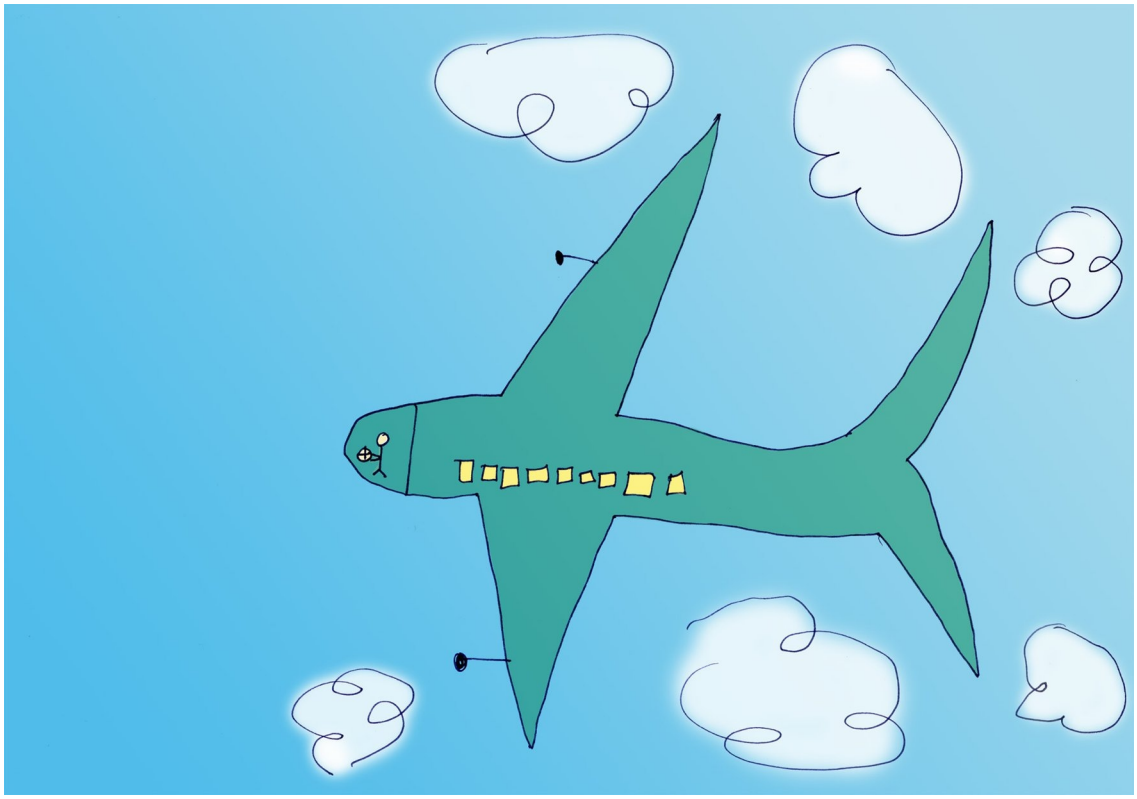


Image 1 : Auteurs : Frédéric Vanderhaegen et Olivier Delville

Le diagnostic de mauvais fonctionnement nécessite de comprendre pourquoi et comment un système ne fonctionne pas.

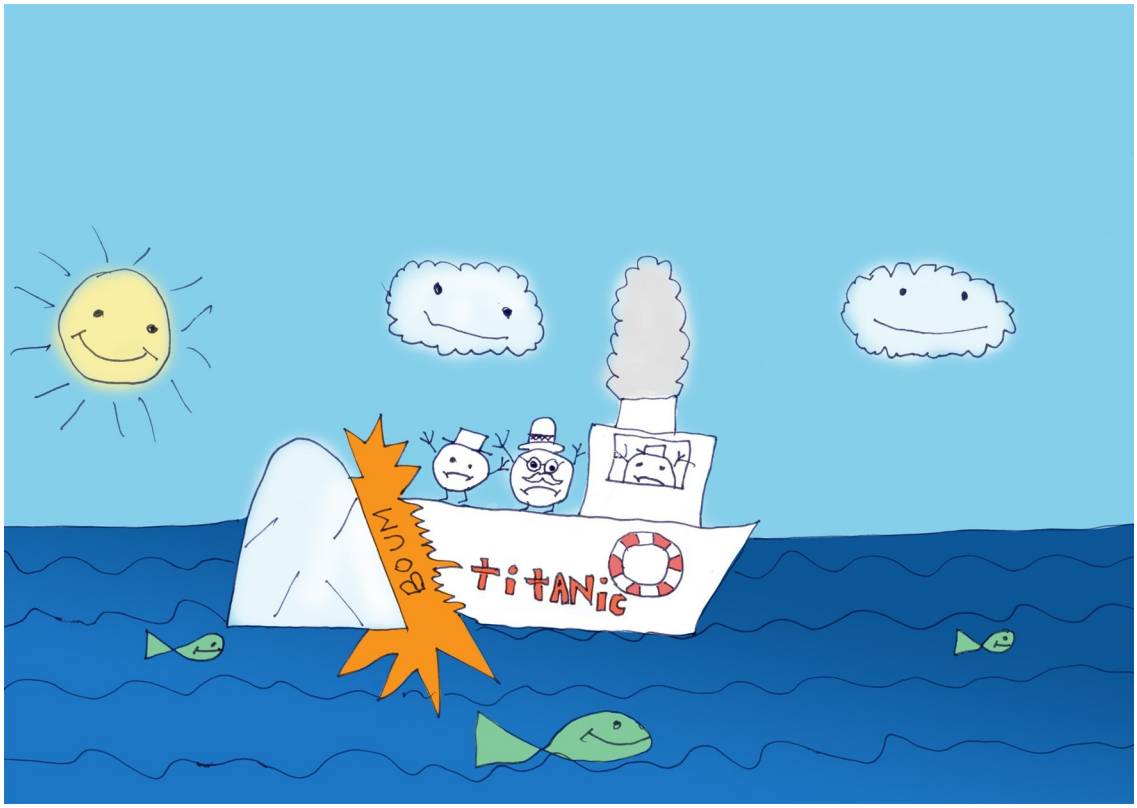


Image 2 : Source : Frédéric Vanderhaegen et Olivier Delville

Le diagnostic de performance en production nécessite de savoir pourquoi et comment optimiser les critères de rentabilité ou de qualité.

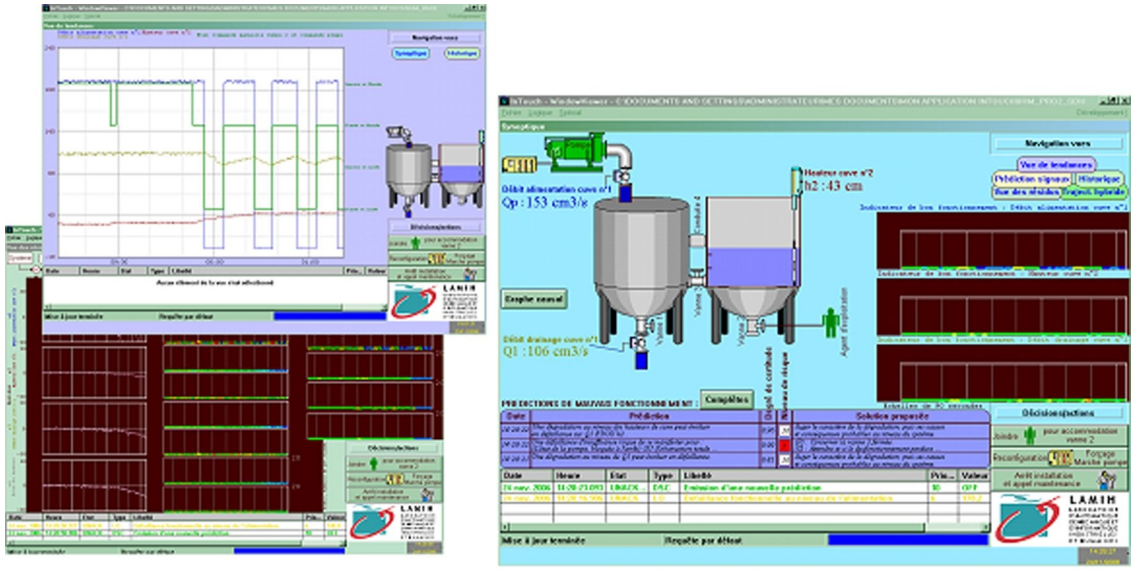


Image 3 : Source : LAMIH

Le diagnostic de situations nécessite de savoir pourquoi et comment les situations évoluent.

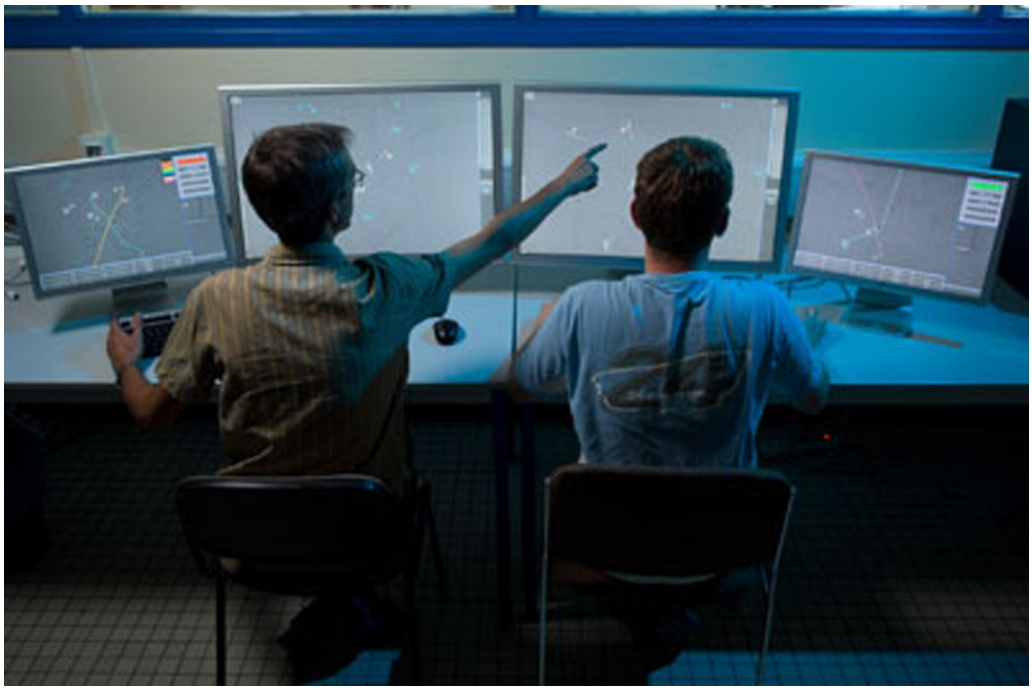


Image 4 : © CNRS Photothèque/ François JANNIN

B. Définition du diagnostic

Le diagnostic est le processus d'évaluation d'un état de fonctionnement donné. Si cet état est comparé avec un état de référence, il s'agit d'évaluation de dérive de fonctionnement.

Il intègre différentes étapes

- Détection de cet état de fonctionnement
- Evaluation des causes de l'occurrence de cet état. Elle consiste à identifier, analyser et localiser ces causes.
- Décision d'action pour modifier cet état

L'objet du diagnostic peut varier :

- Diagnostic de bon ou mauvais fonctionnement
- Diagnostic de panne ou de défaillance
- Diagnostic de performance ou de non-performance
- Diagnostic d'erreur humaine ou de fiabilité humaine
- Etc...

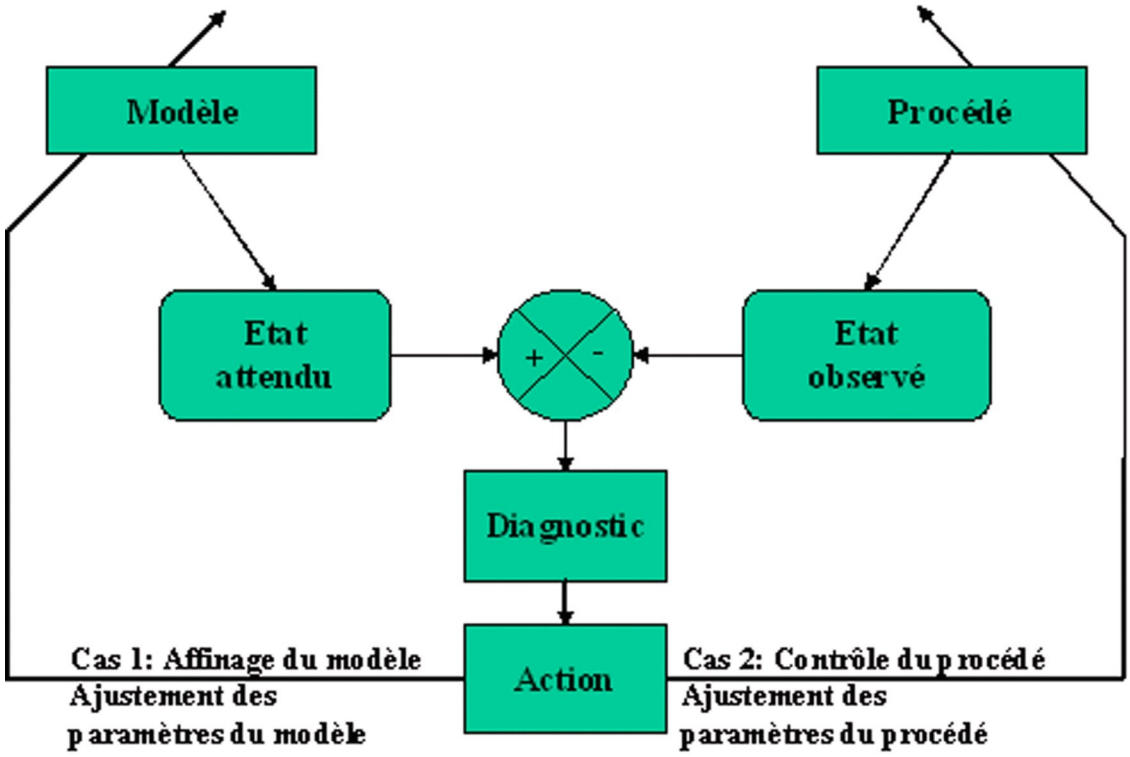
Les moyens pour le contrôle des dérives de fonctionnement sont par exemple les barrières et les systèmes redondants. Ils permettent de maîtriser le risque associé à un état de fonctionnement donné sur deux plans:

- En réduisant l'occurrence de cet état.
- En réduisant les conséquences de cet état, les conséquences pouvant être exprimées non seulement en termes de sécurité, mais également en termes de charge de travail, de qualité, de production, de performance, etc.

C. Diagnostic mono-modèle

Le diagnostic mono-modèle s'appuie sur un seul modèle de bon ou de mauvais fonctionnement. En fonction des observations, il permet :

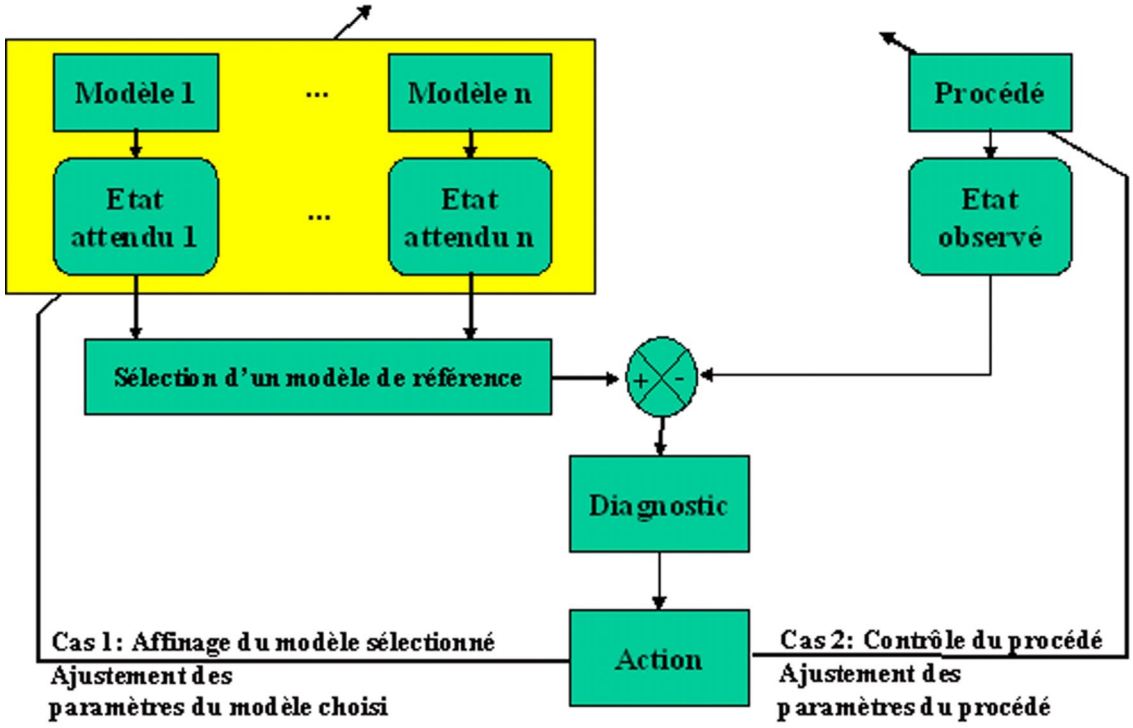
- de construire un modèle du procédé en ajustant les paramètres du modèle,
- ou de contrôler l'état du procédé en ajustant les paramètres de celui-ci.



D. Diagnostic multi-modèle

Le diagnostic multi-modèle s'appuie sur une série de modèles de bon ou de mauvais fonctionnement. Le choix du modèle exploité pour le diagnostic dépend du contexte opérationnel. Cette approche permet :

- de construire une base minimum de modèles et d'ajuster les paramètres de chacun d'eux en fonction des observations.
- d'activer un des modèles en fonction d'un critère prédéfini pour contrôler l'état du procédé en ajustant les paramètres de celui-ci.



E. Formalisation générale du diagnostic

L'étape d'évaluation des causes de l'occurrence d'un état de fonctionnement donné suit la démarche suivante :

$\{cause(état_i)\} = \{événement_j / ∩événement_j \rightarrow état_i\}_{j \in [1, m]}$

Où

- m = nombre d'événements causaux
- événement causal = état intermédiaire, performance, facteur, etc.

La recherche de toutes les causes de l'occurrence d'un état de fonctionnement donné est l'ensemble suivant :

$\{CAUSES(état_i)\} = U \{cause(état_i)\}$

Pour un ensemble d'événements observables Ω déterminant les états d'un procédé donné, plusieurs relations issues de l'algèbre des événements peuvent être définies :

- Tout événement A est un représentant de tous les événements observables Ω déterminant les états d'un procédé donné
- L'événement impossible est l'événement qui n'est jamais réalisé : il lui correspond l'ensemble vide, noté Ø
- L'événement ¬A est l'événement contraire ou complémentaire de l'événement A, i.e., ¬A indique que l'événement A n'est pas observé.
- L'événement (A et B) est la réalisation simultanée des événements A et B. Il lui correspond le sous-ensemble noté A ∩ B ou noté A.B
- Lorsque A et B sont incompatibles, A ∩ B = Ø
- L'événement (A ou B) est la réalisation de l'un au moins des événements. Il lui correspond le sous-ensemble noté A U B, ou noté A + B

- Lorsque A est inclus dans l'événement B (i.e. $A \subset B$), si A est réalisé, alors B l'est aussi.

L'ensemble des événements observables Ω d'un procédé donné comprend les opérations de complémentarité, d'intersection et d'union. Il suit une structure d'algèbre de Boole. Les règles en ont les suivantes :

Commutativité de l'union et de l'intersection
A U B = B U A
A.B = B.A
A ∩ B = B ∩ A
A + B = B + A

Tableau 1 : Commutativité de l'union et de l'intersection

Associativité de l'union et de l'intersection
A ∩ (B ∩ C) = (A ∩ B) ∩ C
A.(B.C) = (A.B).C
A U (B U C) = (A U B) U C
A + (B + C) = (A + B) + C

Tableau 2 : Associativité de l'union et de l'intersection

Distributivité de l'union et de l'intersection
A ∩ (B U C) = (A ∩ B) U (A ∩ C)
A.(B+C) = (A.B) + (A.C)
A U (B ∩ C) = (A U B) ∩ (A U C)
A + (B.C) = (A + B).(A + C)

Tableau 3 : Distributivité de l'union et de l'intersection

Idempotence
A ∩ A = A
A.A = A
A U A = A
A + A = A

Tableau 4 : Idempotence

Absorption
A ∩ (A U B) = A
A.(A+B) = A
A U (A ∩ B) = A
A + (A.B) = A

Tableau 5 : Absorption

Complémentarité
A ∩ ¬A = Ø
A. ¬A = 0
A U ¬A = Ω
A + ¬A = 1
¬ (¬A) = A

Tableau 6 : Complémentarité

Opérateur neutre et d'égalité
Ø ∩ A = Ø
0.A = 0
Ø U A = A
0 + A = A
Ω ∩ A = A
1.A = A
Ω U A = Ω
1 + A = 1
¬Ø = Ω
¬0 = 1
¬Ω = Ø
¬1 = 0

Tableau 7 : Opérateur neutre et d'égalité

Il en découle des théorèmes tels que celui de Morgan :

Théorème de Morgan
¬ (A ∩ B) = ¬A U ¬B
¬ (A.B) = ¬ A + ¬ B
¬ (A U B) = ¬A ∩ ¬B
¬ (A + B) = ¬A . ¬B

Tableau 8 : Théorème de Morgan

Il est possible d'associer une probabilité d'occurrence d'un événement noté P(A). Les principes de la théorie des probabilités peuvent alors être appliqués :

- $0 \leq P(A) \leq 1$
- $P(\neg A) = 1 - P(A)$
- $A \subset B \Rightarrow P(A) \leq P(B)$
- $P(A + B) = P(A) + P(B) - P(A.B)$
- P(A.B) = P(A/B).P(B) où P(A/B) signifie la probabilité que A se produise sachant que B s'est déjà produit.
- Si A et B sont indépendants alors P(A/B) = P(A), i.e., P(A.B) = P(A).P(B)

Un événement ou un groupe d'événements relatifs à un état observé ou observable d'un procédé donné pourra être vrai ou faux, appartenir à une liste prédéfinie de valeurs, ou être associé à un degré de vraisemblance à partir des probabilités d'occurrence.

Diagnostic inductif et déductif

IV

A. Introduction

Les notions de démarche inductive ou déductive se basent sur celles développées dans les approches d'analyse inductive ou déductive de risques. Par exemple, la méthode AMDEC *(Analyse des Modes de Défaillance, de leurs Effets et de leurs Criticité)* est une méthode d'analyse inductive car elle part des défaillances de composants pour en déterminer les conséquences alors que la méthode MAC *(Méthode des Arbres de Causes.Elle est également connue sous les noms de Méthode des Arbres des Défauts ou Méthode des Arbres des Défaillances)* est une approche déductive car elle se focalise sur les événements redoutés d'abord pour identifier leurs causes ensuite.

B. Formalisation du diagnostic inductif et déductif

La démarche inductive de diagnostic permet de déterminer les états associés à des événements initiaux : à partir des causes, on détermine les conséquences. Dans l'élaboration d'un diagnostic à partir d'un système expert, cette démarche est également appelée chaînage avant basé sur les faits ou raisonnement progressif.

La démarche déductive de diagnostic permet de déterminer les événements initiaux causant l'occurrence d'un état donné : à partir des conséquences, on détermine les causes. Dans l'élaboration d'un diagnostic à partir d'un système expert, cette démarche est également appelée chaînage arrière basé sur les buts ou raisonnement régressif.

Les chaînages avant ou arrière nécessitent l'exploitation de règles de la forme :

Si <conjonction de conditions> alors <conclusions>

Dans le cadre du diagnostic, les conditions et les conclusions peuvent être relatives à l'occurrence d'événements prédéfinis (i.e., événements initiateurs, événements intermédiaires, événements terminaux). Les raisonnements sont effectués à partir d'un moteur d'inférence qui déterminera les enchaînements possibles de règles pour identifier les conclusions éventuelles. Ces inférences sont effectuées avec une base de faits initiale, i.e. les événements initiaux qui sont observés.

Pour induire un fait particulier F à partir d'un algorithme de chaînage avant et d'une

base de faits BF initiale, il suffit :

- de déclencher les règles de la base de règles BR dont les conditions sont vraies et d'intégrer leurs conclusions dans la base de faits intermédiaire,
- de relancer le processus jusqu'à ce qu'il soit possible d'inclure ou d'exclure le fait à déterminer.

Définition : Démarche inductive

Soient :

- BF la base de faits, BR les règles
- Conditions(R(i) les conditions de déclenchement de la règle R(i) de BR
- Conclusion(R(i)) les conclusions de la règle R(i) de BR
- F le fait à établir
- BOOL un booléen initialisé à VRAI

```
Tant que F⊄BF & BOOL=VRAI Faire
        BOOL ← FAUX
        Pour toutes les règles R(i) de BR Faire
                Si Conditions(R(i))⊂BF alors
                        BF ← BF ∪ Conclusion(R(i))
                        BR ← BR – {R(i)}
                        BOOL ← VRAI
                Fin Si
        Fin Pour
Fin Tant Que
Si F⊂BF alors
        F est observable
Sinon
        F n'est pas observable
Fin Si
```

L'algorithme de chaînage arrière consiste à partir du fait à établir et de la base de fait initiale :

- à déterminer les règles dont les conclusions sont le fait à établir
- à identifier les conditions de ces règles
- à considérer les conditions de ces règles comme de nouveaux faits à établir
- à renouveler le processus récursivement pour valider le déclenchement de règles à partir de la base de faits jusqu'à ce qu'il n'y ai plus de séquence de règles à traiter.

Définition : Démarche déductive

Soient :

- BF la base de faits
- BR les règles
- R un sous-ensemble de R
- Condition(R(i) les conditions de déclenchement de la règle R(i) de BR
- Conclusion(R(i)) les conclusions de la règle R(i) de BR,

- F le fait à établir

```
ChainageArriere(BF, BR, F)
Si F⊂BF alors
        F est observable
Sinon
        F n'est pas observable
Fin Si

ChainageArriere(BF, BR, F)
DEBUT TRAITEMENT
    Soit R les règles R(i) de BR telles que F⊂Conclusion(R(i))
    Si R = {∅} alors
          Retourner(∅)
    Sinon
          Pour toutes les règles R(i) de R telles que F⊂Conclusion(R(i)) Faire
                Si Condition(R(i))⊂BF alors
                      BR ← BR – {R(i)}
                      Pour toutes les règles R(j) telles que Conditions(R(j)) ⊂BF Faire
                            R ← R – {R(j)}
                      Fin Pour
                      Retourner(Conclusion(R(i)))
                Sinon
                      Pour tout F de Conditions(R(i)) Faire
                            BF ← BF ∪ ChainageArriere(BF, BR, F)
                      Fin Pour
                Fin Si
          Fin Pour
      Fin Si
FIN TRAITEMENT
```

A partir des algorithmes proposés, les règles exploitables de la base de règles doivent être codées de la manière suivante :

- Pour les règles de type : **Si A ou B alors C**
  deux règles sont alors nécessaires dans la base de règles :
  A → C
  B → C
- Pour les règles de type : **Si A alors B et C**
  deux règles sont alors nécessaires dans la base de règle :
  A → B
  A → C

Par contre, il n'est pas possible de coder les règles de type : **Si A alors B ou C**

C. Exemple de diagnostic inductif et déductif

1. Rappel de logique : démonstration du théorème de Morgan

Rappel : il s'agit de démontrer les relations de type :

¬(A ∩ B) = ¬A U ¬B
¬(A.B) = ¬A + ¬B
¬ (A U B) = ¬A ∩ ¬B
¬ (A + B) = ¬A . ¬B

Compléter le tableau suivant :

A	B	A + B	¬ (A + B)	¬ A	¬ B	¬ A . ¬ B
0	0	?	?	?	?	?
0	1	?	?	?	?	?
1	0	?	?	?	?	?
1	1	?	?	?	?	?

Correction :

A	B	A + B	¬ (A + B)	¬ A	¬ B	¬ A . ¬ B
0	0	0	1	1	1	1
0	1	1	0	1	0	0
1	0	1	0	0	1	0
1	1	1	0	0	0	0

De même, compléter le tableau suivant :

A	B	A . B	¬ (A . B)	¬ A	¬ B	¬ A + ¬ B
0	0	?	?	?	?	?
0	1	?	?	?	?	?
1	0	?	?	?	?	?
1	1	?	?	?	?	?

Correction :

A	B	A . B	¬ (A . B)	¬ A	¬ B	¬ A + ¬ B
0	0	0	1	1	1	1
0	1	0	1	1	0	1
1	0	0	1	0	1	1
1	1	1	0	0	0	0

Généralisation :

Compléter les égalités suivantes :

$\neg (X_1 + X_2 + ... + X_N) = ?$

$\neg (X_1 . X_2 . ... . X_N) = ?$

Corrections:

$\neg (X_1 + X_2 + ... + X_N) = \neg X_1 . \neg X_2 . ... . \neg X_N$

$\neg (X_1 . X_2 . ... . X_N) = \neg X_1 + \neg X_2 + ... + \neg X_N$

2. Raisonnement inductif et déductif à base de règles

Soient la base de règles BR suivante :
R1 : Si B et D et E alors F
R2 : Si D et G alors A
R3 : Si C et F alors A
R4 : Si B alors X
R5 : Si D alors E
R6 : Si A et X alors H
R7 : Si C alors D
R8 : Si X et C alors A
R9 : Si X et B alors D
BF = {B, C}
But à démonter : H
Faire le raisonnement par chaînage avant puis chaînage arrière

Correction :

Chaînage avant :
Etape initiale BF = {B, C}
Avec la règle R4, BF = {B, C, X}
Avec la règle R7, BF = {B, C, X, D}
Avec la règle R5, BF = {B, C, X, D, E}
Avec la règle R1, BF = {B, C, X, D, E, F}
Avec la règle R3, BF = {B, C, X, D, E, F, A}
Avec la règle R6, BF = {B, C, X, D, E, F, A, H}
H est établi

Chaînage arrière
Etape initiale BF = {B, C}
Avec la règle R6, il faut démonter A et X
Pour X : avec la règle R4, comme B⊂BF, BF={B, C, X}
Pour A : avec la règle R2, il faut démontrer D et G
Pour D : avec la règle R7, comme C⊂BF, BF={B, C, X, D}
Pour G : échec car pas de règle
ou
avec la règle R3, il faut démontrer C et F
Pour C : déjà vérifié
Pour F : avec la règle R1, il faut démonter B, D et E
Pour B : déjà vérifié
Pour D : déjà vérifié
Pour E : avec la règle R5, comme D⊂BF, BF = {B, C, X, D, E}
Comme {B, C, E}⊂BF, BF ={B, C, X, D, E, F}
Comme {D, G} ⊂BF, BF = {B, C, X, D, E, F, A}
Comme {A, X}⊂BF, BF={B, C, X, D, E, F, A, H}

H est établi

Diagnostic abductif multi-point de vue

V

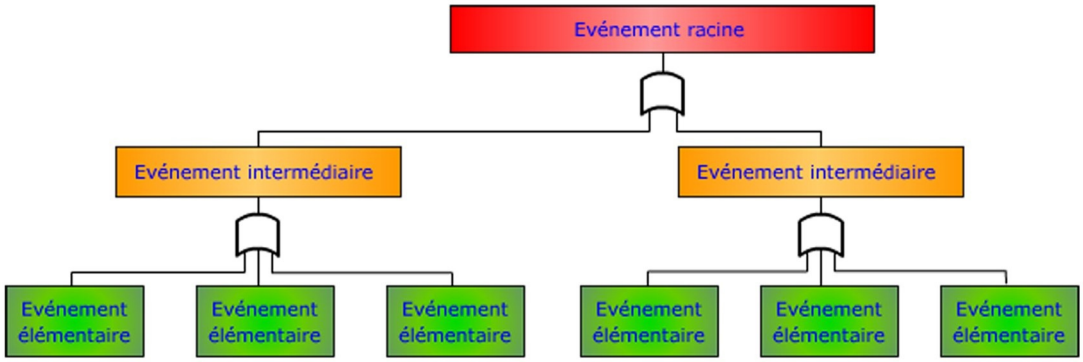
A. Introduction

La démarche abductive est basée sur des hypothèses explicatives. Elle suppose que la présence ou l'absence d'une cause s'explique par la possibilité de la présence ou de l'absence de tous les états associés. Il en est de même pour la présence ou l'absence d'une conséquence qui peut s'exliquer par la possibilité de la présence ou de l'absence des toutes les causes associées. Ce type de raisonnement est détaillé dans le cadre du diagnostic abductif multi-point de vue.

B. Formalisation du diagnostic abductif multi-point de vue

Les caractéristiques événementielles d'un système peuvent être décrites à partir d'un graphe causal. Un événement donné est soit un événement élémentaire, soit un événement intermédiaire qui est le résultat d'une combinaison d'événements élémentaires ou combinés.

Les événements élémentaires peuvent être regroupés hiérarchiquement : ce regroupement est appelé Point de Vue. Ce graphe causal ainsi obtenu peut être assimilé à une arbre de causes dans lequel toutes les portes logiques sont des OU car on ne s'intéresse pas ici à la dépendance entre les événements élémentaires générant l'occurrence d'événements intermédiaires ou racines :



→***Abduction :***
- Si un événement intermédiaire est observé alors il est possible que tous les événements élémentaires associés à cet événement soient suspects ou
- Si un événement intermédiaire n'est pas observé alors il est possible que tous les événements élémentaires associés à cet événement ne soient pas suspects

→***Un point de vue*** = arbre de défaillance avec des portes OU
→***Modèle multi-point de vue*** = modèle regroupant des points de vue différents sur une même liste d'événements élémentaires.

Plusieurs points de vue peuvent exister pour une même liste d'événements élémentaires. Par rapport aux événements observables sur le procédé piloté, le problème traité consiste à identifier le ou les événements élémentaires impliqués. Tous les événements élémentaires sont initialement suspectés. L'exploitation de plusieurs points de vue doit permettre de sélectionner une liste réduite d'événements élémentaires.

L'ensemble des événements élémentaires est noté C. Un point de vue sur C est noté PV. Comme PV est organisé hiérarchiquement et inclut des relations entre nœuds du type Ca→Ef, lorsqu'un événement Ef de PV n'est pas observé, alors son fils Ca peut être rejeté. Ca est soit un événement combiné, soit un événement élémentaire.

Fondamental

C = ensemble initial des événements élémentaires
PV = point de vue sur C
Plusieurs points de vue sur C

$Ca \rightarrow$ Ef : (1) *Ef* de *PV* n'est pas observé $\Rightarrow$ *Ca* est rejeté
(2) *Ef* de *PV* est observé $\Rightarrow$ *Ca* peut être observé (abduction)

Rappel du principe d'abduction :
Si Ca implique Ef alors il est possible que Ca soit suspect si Ef est observé

Ca = un événement intermédiaire peut avoir plusieurs causes et une cause plusieurs effets

Deux principes : FOCALISATION et EXCLUSION

De plus, quand l'événement Ef est observé, alors il se peut que son fils Ca le soit également. Cette inférence est appelée l'abduction qui est utilisée ici pour la gestion des hypothèses d'occurrence d'événements. Les relations causales sont exploitées en considérant qu'un même événement Ef peut avoir plusieurs causes Ca et un même événement Ca peut avoir plusieurs effets Ef. Une fonction FILS(Ef(PV)) permet de calculer tous les fils d'un événement donné Ef. Ainsi, quand un événement Ef de PV est observé, la fonction SC(Ef(PV)) permet de déterminer la

liste d'événements élémentaires relative à l'occurrence de Ef :

$$SC(Ef(PV)) = \begin{cases} Ef, & Ef \subset C \\ C \cap \bigcup_{X \in CHILD(Ef(PV))} SC(X(PV)), & \text{sinon} \end{cases}$$

La fonction SC permet de déterminer la liste des événements élémentaires de C pouvant provoquer l'occurrence de Ef

Il est alors possible de focaliser ou d'exclure les événements liés à Ef. Ces opérations s'effectuent à partir des fonctions de sélection d'événement FOCUS(Ef(PV)) et EXCLU(Ef(PV)) respectivement.

Chaque opération génère une mise à jour des opérations de masquage sur chaque événement élémentaire afin de recalculer la liste courante des événements élémentaires suspectés, notés Sc, initialisée à C. Chaque événement élémentaire c_i de C a donc une liste de masquage notée MASK(c_i) relative aux opérations effectuées sur l'ensemble des points de vue sur C.

Initialement, tous les ensembles MASK(c_i) sont vides. Après avoir réalisé des inférences sur C via les points de vue, si l'ensemble MASK(c_i) est vide, alors il n'y a aucune raison de rejeter c_i, tandis que s'il n'est pas vide, chacun des éléments de MASK(c_i) est une cause de rejet de c_i.

Une opération de focalisation ou d'exclusion d'un nœud à partir d'un point de vue entraîne la mise à jour des ensembles MASK(ci) et de la liste Sc. Une annulation d'une de ces inférences obtenues à partir des opérations FOCUS(Ef(PV)) et EXCLU(Ef(PV)) est réalisée par deux autres fonctions: $FOCUS^{-1}$(Ef(PV)) et $EXCLU^{-1}$(Ef(PV)) respectivement.

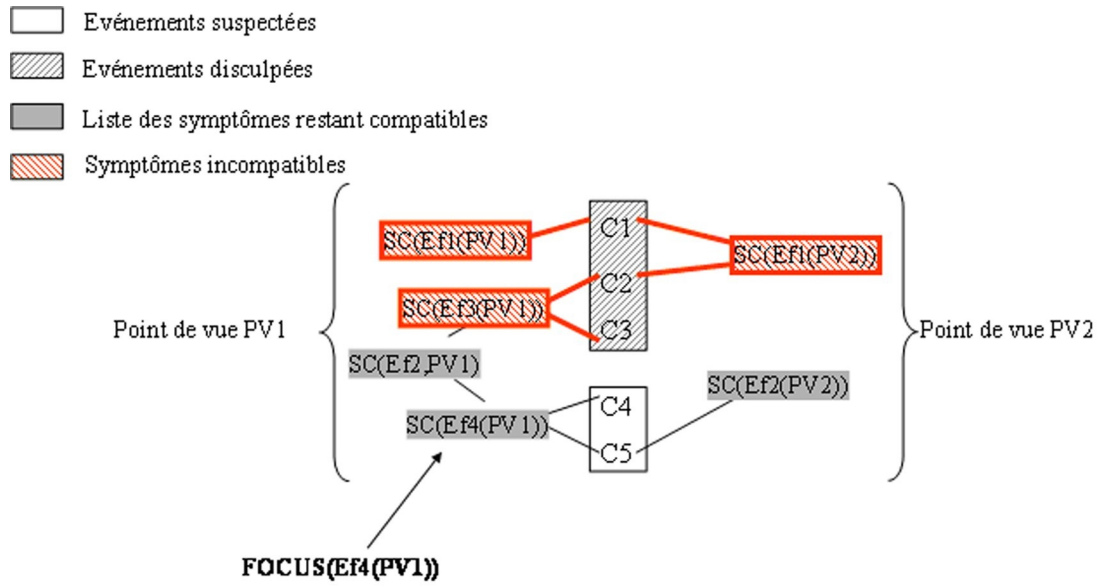
La formalisation des opérations de focalisation est la suivante :

$$FOCUS(Ef(PV) \Rightarrow \forall c_i \in C - SC(Ef(PV)),\ ((MASK(c_i) \leftarrow MASK(c_i) \cup \{"F" + Ef(PV)\}) \wedge (Sc \leftarrow Sc - c_i))$$

$MASK(c_i)$ contient toutes les actions permettant de justifier le rejet de l'événement c_i parmi les suspects

$$FOCUS^{-1}(Ef(PV))) \Rightarrow \forall ci \in C - SC(Ef(PV)),$$
$$((MASK(c_i) \leftarrow MASK(c_i) - \{"F" + Ef(PV)\}) \wedge (MASK(c_i) = \{\varnothing\} \Rightarrow Sc \leftarrow Sc + c_i))$$

Le schéma suivant illustre une opération de focalisation su un exemple simple comprenant deux points de vue permettant de regrouper hiérarchiquement 5 causes élémentaires :



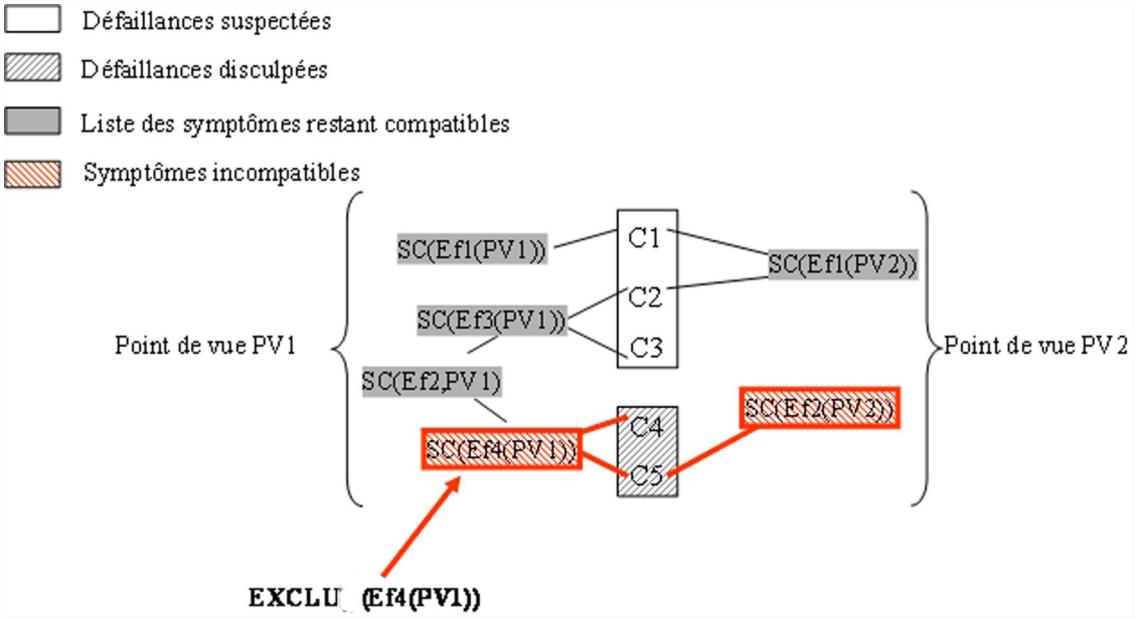
La formalisation des opérations d'exclusion est la suivante :

$$EXCLU(Ef(PV) \Rightarrow \forall c_i \in SC(Ef(PV)), ((MASK(c_i) \leftarrow MASK(c_i) \cup \{"E"+ Ef(PV)\}) \wedge (Sc \leftarrow Sc - c_i))$$

$MASK(c_i)$ contient toutes les actions permettant de justifier le rejet de l'événement c_i parmi les suspects

$$EXCLU^{-1}(Ef(PV)) \Rightarrow \forall ci \in SC(Ef(PV)),$$
$$(MASK(c_i) \leftarrow MASK(c_i) - \{"E"+ Ef(PV)\}) \wedge (MASK(c_i) = \{\varnothing\} \Rightarrow Sc \leftarrow Sc + c_i))$$

Le schéma suivant illustre une opération d'exclusion sur le même exemple précédent comprenant deux points de vue permettant de regrouper hiérarchiquement 5 causes élémentaires :



Dans les deux exemples illustrant une opération de focalisation, puis d'exclusion, il est important de noter que les conséquences d'une opération de focalisation ou d'exclusion sont répercutées sur les possibilités d'action sur les autres points de vue. Un modèle de cohérence est alors exploité. Ce modèle de cohérence entre causes et effets lors d'une opération selon un point de vue est nécessaire.

Ce modèle permet de propager, sur les autres points de vue, les opérations effectuées à partir d'un point de vue, telles que la focalisation ou l'exclusion d'un événement, ou encore l'annulation d'une opération.

Les sélections réalisées au travers d'un point de vue se propage sur les autres points de vue à partir de la fonction COHERENCE(Ef(PV)) :

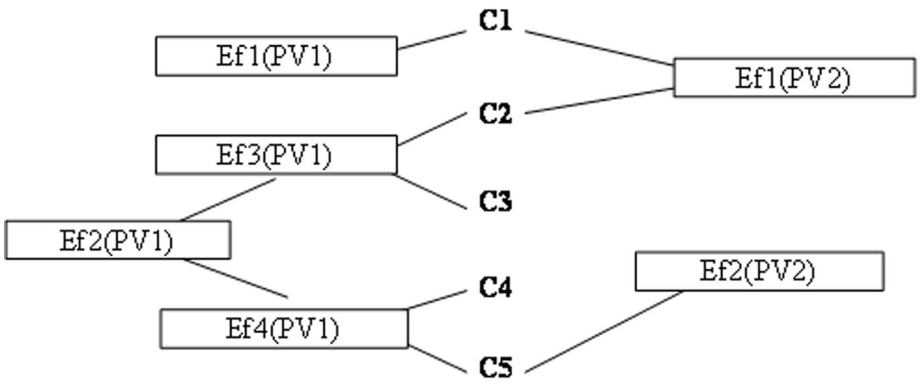
$$\text{COHERENCE}(\text{Ef}(\text{PV})) = \begin{cases} 1, & \exists c_i \in Sc / c_i \in SC(\text{Ef}(\text{PV})) \\ 0, & \text{sinon} \end{cases}$$

La fonction COHERENCE permet de répercuter les conséquences des actions de focalisation et d'exclusion sur tous les points de vue

Lors d'une opération de focalisation ou d'exclusion d'un événement à partir d'un point de vue donné, les événements intermédiaires des autres points de vue sont contrôlés par cette fonction. Chaque événement intermédiaire pour lequel la fonction renvoie 0 est désactivé afin de ne plus pouvoir le prendre en compte dans le raisonnement futur. Par contre, il est réactivé si la fonction renvoie 1 après une annulation par exemple.

C. Exercice de diagnostic abductif multi-point de vue

Soit l'exemple précédent comprenant deux points de vue qui regroupent 5 causes élémentaires.



Valeurs initiales
Sc={C1, C2, C3, C4, C5}
MASK(C1) = MASK(C2) = MASK(C3) = MASK(C4) = MASK(C5) = {∅}

Etape 1 : A partir des valeurs initiales de Sc et de MASK(C1), MASK(C2), MASK(C3), MASK(C4) et MASK(C5), donner le résultat de l'opération n°1 : **FOCUS(Ef2(PV1))**.
Choisir un des résultats suivants :

Résultat 1 de l'opération 1: FOCUS(Ef2(PV1))
Sc={C2, C3, C4}
MASK(C1) = MASK(C2) = {FEf2(PV1)}
MASK(C3) = MASK(C4) = MASK(C5) = {∅}

Résultat 2 de l'opération 1: FOCUS(Ef2(PV1))
Sc={C2, C3, C4, C5}
MASK(C1) = {FEf2(PV1)}
MASK(C2) = MASK(C3) = MASK(C4) = MASK(C5) = {∅}

Résultat 3 de l'opération 1: FOCUS(Ef2(PV1))
Sc={C1, C2 C4, C5}
MASK(C1) = MASK(C2) = MASK(C3) = MASK(C4) = MASK(C5) = {∅}

Le choix correct est le choix n°2.

Etape 2 : A partir des valeurs initiales de Sc et de MASK(C1), MASK(C2), MASK(C3), MASK(C4) et MASK(C5), donner le résultat de l'opération n°1 **FOCUS(Ef2(PV1))** puis de l'opération n°2 : **EXCLU(Ef4(PV1))**.
Choisir un des résultats suivants :

Résultat 1 de l'opération 2 après l'opération 1: EXCLU(Ef4(PV1))
Sc={C2, C3}
MASK(C1) = {FEf2(PV1)}
MASK(C2) = MASK(C3) = {∅}
MASK(C4) = MASK(C5) = {EEf4(PV1)}

Résultat 2 de l'opération 2 après à l'opération 1: EXCLU(Ef4(PV1))
Sc={C1, C2, C3}
MASK(C1) = MASK(C2) = MASK(C3) = {∅}
MASK(C4) = MASK(C5) = {EEf4(PV1)}

Résultat 3 de l'opération 2 après à l'opération 1: EXCLU(Ef4(PV1))
Sc={C1, C2, C3, C5}
MASK(C1) = MASK(C2) = MASK(C3) = MASK(C5) = {∅}
MASK(C4) = {EEf4(PV1)}

Le choix correct est le choix n°1.

Etape 3 : A partir des valeurs initiales de Sc et de MASK(C1), MASK(C2), MASK(C3), MASK(C4) et MASK(C5), donner le résultat de l'opération n°1 **FOCUS(Ef2(PV1))**, suivie de l'opération n°2 **EXCLU(Ef4(PV1))** puis de l'opération n°3 : **FOCUS(Ef1(PV2))**.
Choisir un des résultats suivants :

Résultat 1 de l'opération 3 après les opérations 1 puis 2
Sc={C2, C3}
MASK(C1) = MASK(C2) = {FEf2(PV1)}
MASK(C3) = {FEf1(PV2)}
MASK(C4) = MASK(C5) = {EEf4(PV1), FEf1(PV2)}

Résultat 2 de l'opération 3 après les opérations 1 puis 2
Sc={C2}
MASK(C3) = MASK(C2) = {FEf2(PV1)}
MASK(C1) = {FEf1(PV2)}
MASK(C4) = MASK(C5) = {EEf4(PV1), FEf1(PV2)}

Résultat 3 de l'opération 3 après les opérations 1 puis 2
Sc={C2}
MASK(C1) = {FEf2(PV1)}
MASK(C2) = {∅}
MASK(C3) = {FEf1(PV2)}
MASK(C4) = MASK(C5) = {EEf4(PV1), FEf1(PV2)}

Le choix correct est le choix n°3

Etape 4 : A partir des valeurs initiales de Sc et de MASK(C1), MASK(C2), MASK(C3), MASK(C4) et MASK(C5), donner le résultat de l'opération n°1 **FOCUS(Ef2(PV1))** suivie de l'opération n°2 **EXCLU(Ef4(PV1))** suivie de l'opération n°3 **FOCUS(Ef1(PV2))**, puis de l'opération n°4 : **FOCUS^{-1}(Ef2(PV1))**.
Choisir un des résultats suivants :

Résultat 1 de l'opération 4 après les opérations 1, 2 et 3
Sc={C1}
MASK(C1) = {∅}
MASK(C3) = MASK(C2) = {FEf1(PV2)}
MASK(C4) = MASK(C5) = {EEf4(PV1), FEf1(PV2)}

Résultat 2 de l'opération 4 après les opérations 1, 2 et 3
Sc={C1, C2}
MASK(C1) = MASK(C2) = {∅}
MASK(C3) = {FEf1(PV2)}
MASK(C4) = MASK(C5) = {EEf4(PV1), FEf1(PV2)}

Résultat 3 de l'opération 4 après les opérations 1, 2 et 3
Sc={C1, C2, C3}
MASK(C1) = MASK(C3) = MASK(C2) = {∅}
MASK(C4) = MASK(C5) = {EEf4(PV1), FEf1(PV2)}

Le choix correct est le choix n°2.

VI

Modèles de diagnostic chez l'opérateur humain

Les activités de diagnostic d'un procédé industriel concernent deux aspects différents :

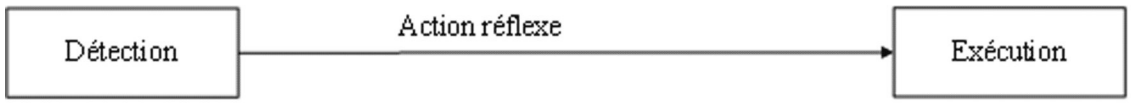
- La mise en oeuvre des étapes du diagnostic des états de fonctionnement du procédé contrôlé par l'opérateur humain.
- La mise en oeuvre des étapes du diagnostic des états de fonctionnement de l'opérateur humain qui contrôle le procédé.

Le premier cas nécessite des modèles de fonctionnement du procédé piloté, le deuxième cas des modèles de fonctionnement de l'opérateur humain.

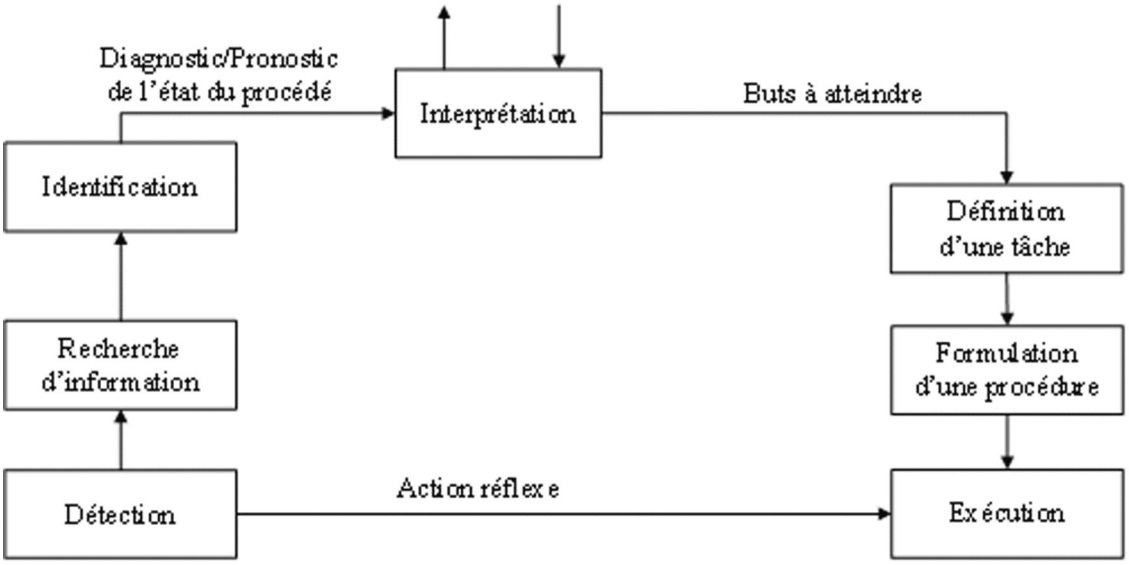
A. Modèles de bon fonctionnement

Le modèle de diagnostic humain le plus connu est certainement celui de RASMUSSEN. Il est décomposé selon trois niveaux comportementaux :

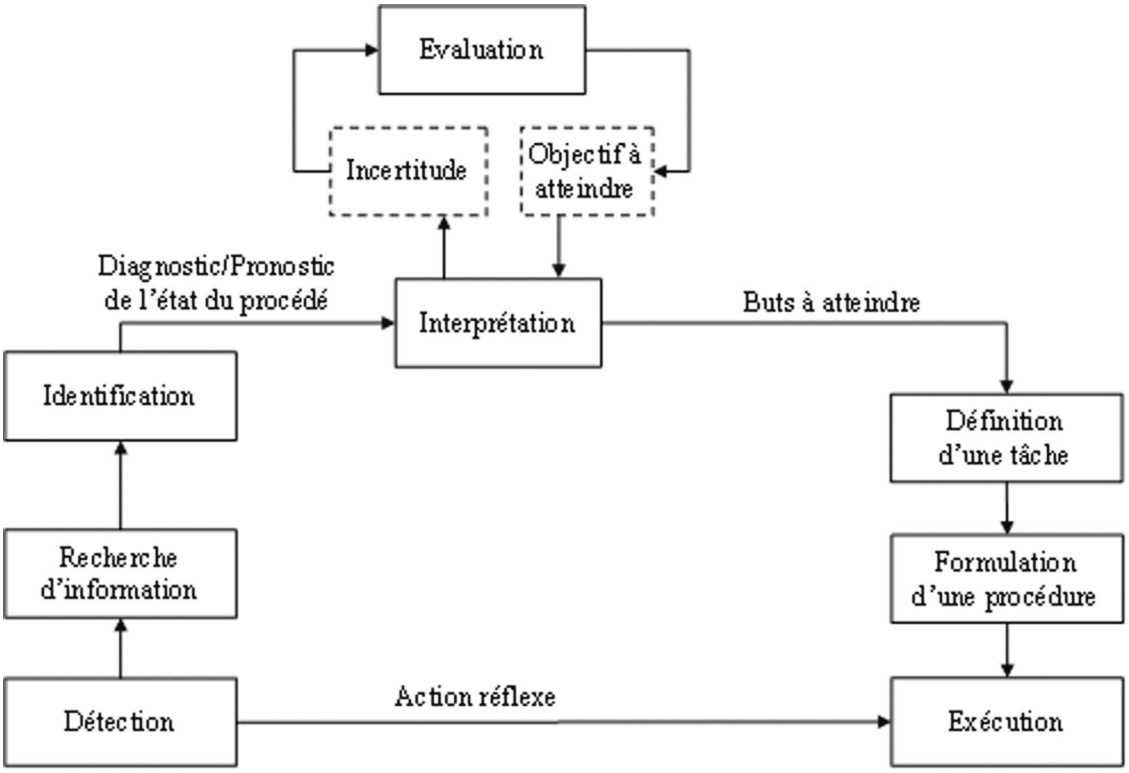
- Le premier comportement concerne les **habiletés**. L'opérateur exécute de façon quasi-automatique des actions en réponse à des informations sur la situation courante.



- Lorsque l'opérateur est face à une situation familière, il adopte un comportement basé sur des **règles**. Celles-ci permettent d'identifier l'état du procédé et de choisir rapidement la procédure appropriée. A ce stade, le diagnostic consiste à évaluer la situation courante et de la comparer avec les situations précédentes alors que le pronostic permet une évaluation de l'évolution future du procédé par rapport à la situation courante.

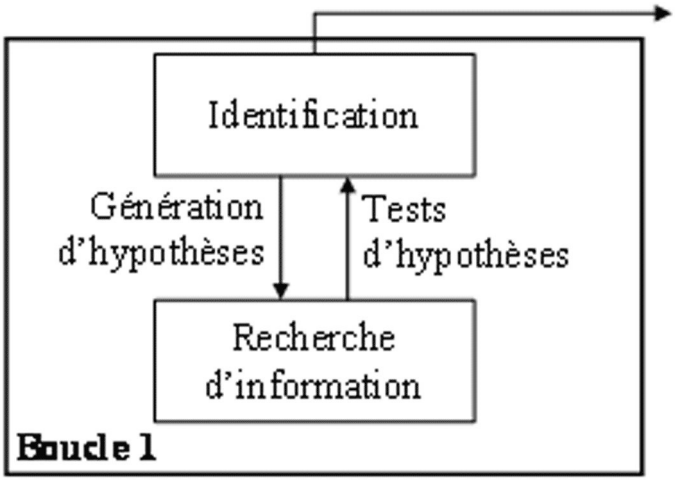


- Enfin, face à des situations nouvelles, l'opérateur adopte un comportement basé sur les **connaissances**.

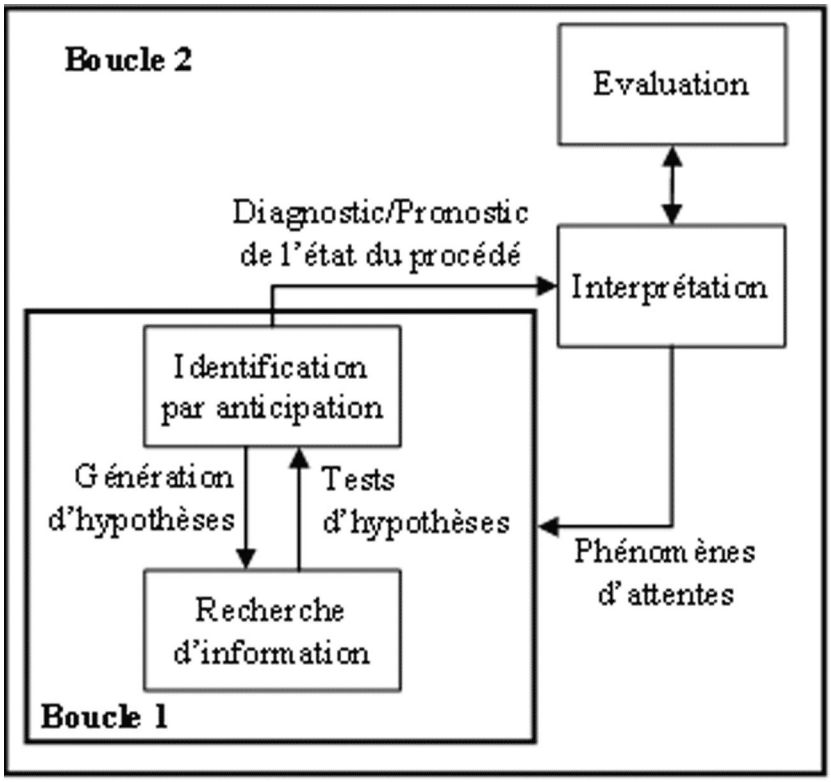


Le diagnostic peut être considéré comme non seulement comme un processus anticipatif mais pouvant également intégrer plusieurs boucles internes de régulation:

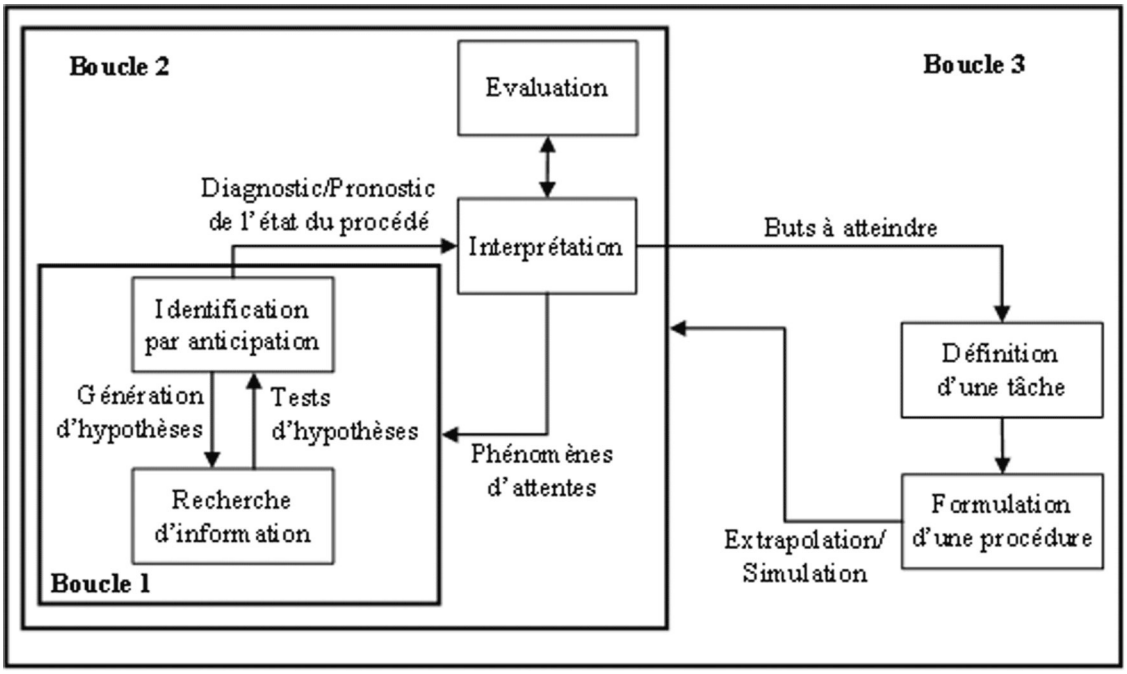
- Boucle 1 liée au pronostic et au diagnostic d'une situation courante. L'activité d'anticipation commence dès la phase ascendante d'évaluation qui comprend des cycles de diagnostic-pronostic de l'état courant du procédé, à savoir son évaluation d'une part et l'anticipation de son évolution, d'autre part. L'opérateur génère alors des hypothèses qu'il peut vérifier à partir de tests prédéfinis.



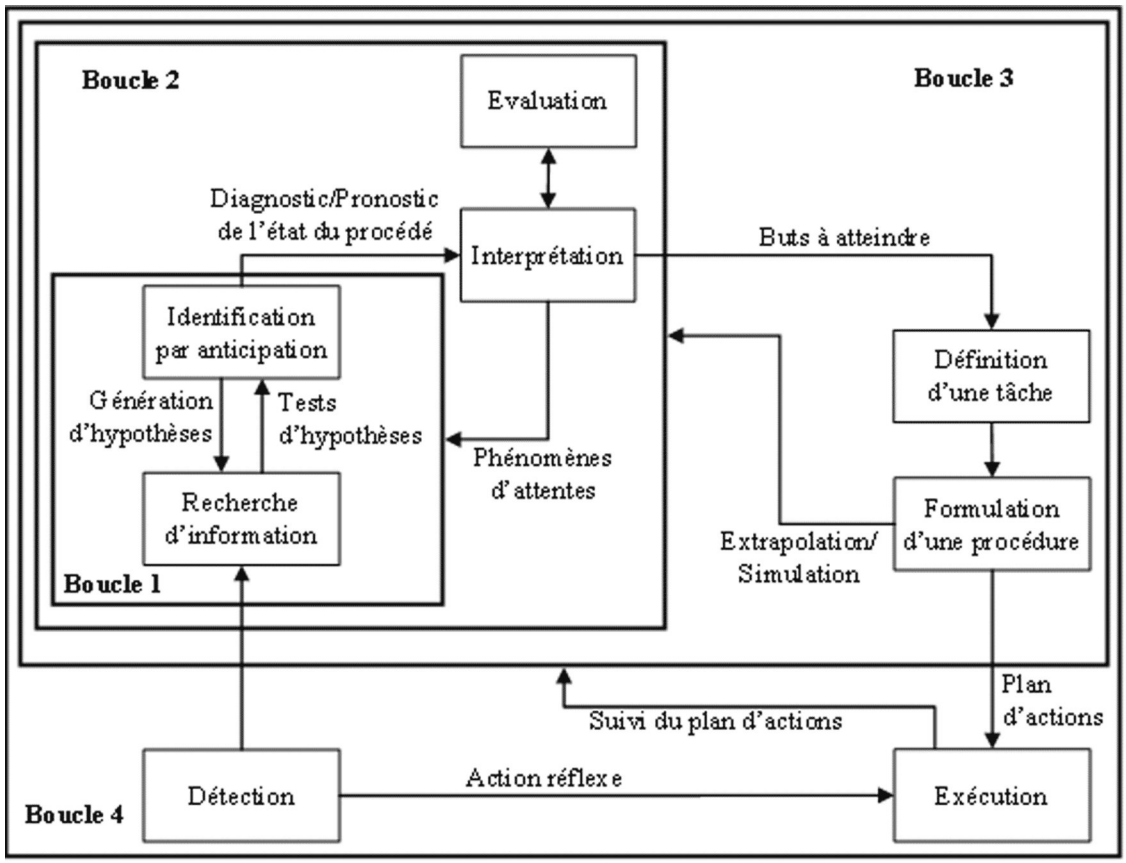
- Boucle 2 liée à la définition de buts pour réguler ou corriger l'état du procédé. L'activité d'anticipation permet une analyse de la situation courante afin de déterminer un but à atteindre. Ceci peut nécessiter de nouveaux cycles d'observation et d'évaluation de la stratégie à adopter. Il s'agit de phénomènes d'attentes relatives à la connaissance des caractéristiques dynamiques du procédé.



- Boucle 3 liée à la planification des actions pour atteindre les buts définis précédemment. Cette boucle rétroactive de régulation apparaît dans la phase descendante d'élaboration d'une solution sous forme de vérifications internes successives pour extrapoler ou simuler l'impact des actions envisagées sur le procédé.

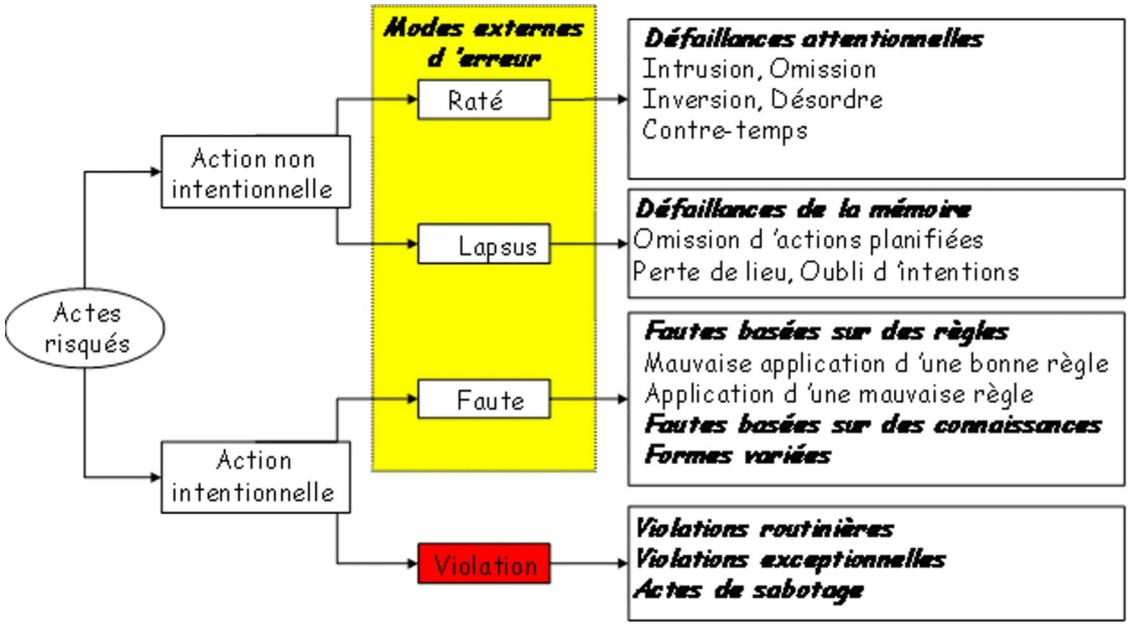


- Boucle 4 liée au suivi du plan d'actions. Cette activité permet de contrôler les conséquences réelles d'une action sur l'état du procédé.



B. Modèles de mauvais fonctionnement

Le modèle de mauvais fonctionnement de l'opérateur humain présenté ici est celui de REASON. Il permet d'établir un diagnostic d'erreur humaine à partir d'une taxonomie intégrant trois modes : les **ratés**, les **lapsus** et les **fautes**. Les ratés et les lapsus sont dus à des défaillances dans l'exécution et/ou la mémorisation d'actions préalablement sélectionnées, alors que les fautes sont dues à des défaillances dans la sélection de tâches, donc dans la planification.



Par rapport au modèle de bon fonctionnement de l'opérateur humain, les ratés et les lapsus se retrouvent dans le comportement de bas niveau basé sur les habiletés. Les fautes se manifestent dans les deux autres types de comportement humain, i.e. les comportements basés sur les règles et les connaissances. Elles concernent une dérive entre l'intention de l'opérateur et celle qu'il aurait du avoir pour satisfaire les objectifs du procédé.

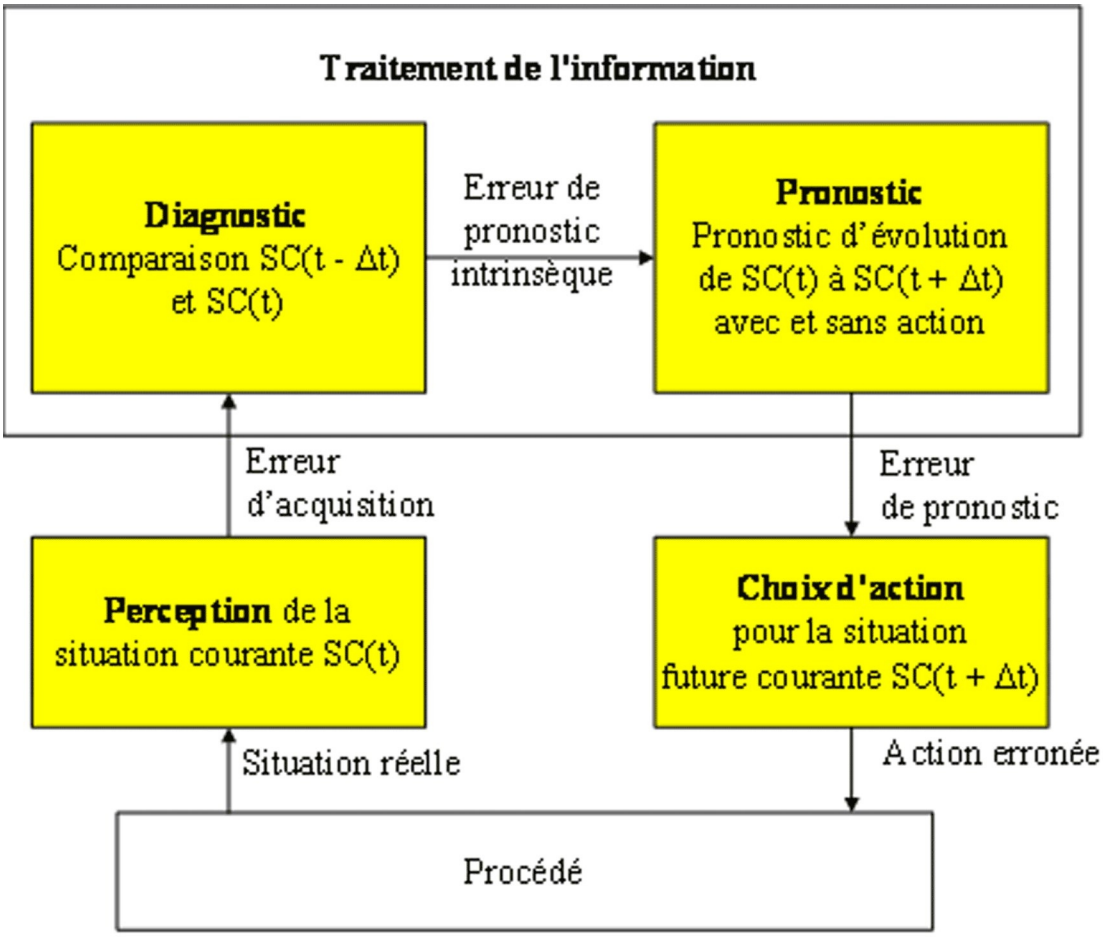
Les actes risqués présentent ici une intention préalable d'agir sur le procédé. Les actions dites **non intentionnelles** sont les actions pour lesquelles l'opérateur humain n'avait pas l'intention de diverger par rapport à ce qu'il avait prévu, mais pour lesquelles le résultat obtenu est néanmoins différent de celui attendu. Ce sont donc les ratés (i.e., défaillances attentionnelles comme l'omission, l'inversion, le désordre) et les lapsus (i.e., défaillances de la mémoire comme l'omission d'actions planifiées, l'oubli d'intentions). Dans les actions dites **intentionnelles**, il n'y a pas de divergence entre ce qu'avait prévu de faire l'opérateur humain et ce qu'il a fait réellement. On distingue alors la faute de la **violation** : il y a faute quand le résultat obtenu est différent du résultat prescrit sans intention de divergence, alors qu'il y a violation quand cette divergence est volontaire. Les actions intentionnelles regroupent donc les violations (e.g., violations routinières, actes de sabotage), les fautes basées sur les règles (i.e., mauvaise application d'une bonne règle, application d'une mauvaise règle) et les fautes basées sur les connaissances (i.e., difficulté de diagnostic, récapitulatif biaisé).

L'action erronée peut être diagnostiquée à partir des différentes caractéristiques de la tâche à réaliser : les paramètres temporels (i.e., la durée d'exécution, vitesse d'exécution, date de début de l'action, synchronisation, séquencement, etc), les paramètres physiques (i.e., intensité physique nécessaire à la réalisation de l'action, distance par rapport à son impact, espace dans lequel elle est réalisée,

etc.) ou les paramètres fonctionnels (i.e., complexité, objectif, décomposition, fréquence, etc.). Une action peut alors être omise, interrompue, remplacée, confondue ou inversée avec une autre action, répétée ou insérée dans un plan alors qu'elle ne le devrait pas, exécutée trop tôt ou trop tard, etc.

Une action erronée peut non seulement se définir à partir des caractéristiques ou conséquences observables, mais aussi être le résultat de facteurs internes relatifs aux différents stades comportementaux de la résolution de problème. Les erreurs se propagent alors de la manière suivante :

- Une **erreur d'acquisition** est le résultat du processus de perception ou d'interprétation d'une situation réelle. Lorsque le résultat de l'acquisition est erroné, ceci se traduit par une dérive entre la représentation que l'opérateur a du système et l'état réel de ce dernier. Cet écart de représentation peut alors avoir des conséquences sur le traitement de l'information et de ce fait sur l'action.
- Ensuite, **une erreur dans le processus du traitement de l'information** est soit une erreur de traitement d'informations correctes, soit le traitement d'informations erronées, soit une erreur de traitement de mauvaises informations. Le traitement de l'information est donc erroné lorsque son résultat ne correspond pas avec les prescriptions relatives à la situation réelle. L'erreur de traitement de l'information inclut non seulement l'erreur de pronostic intrinsèque de la situation réelle courante, c'est-à-dire l'opérateur décide de rester inactif alors que la situation courante nécessite une intervention de celui-ci, et l'erreur de pronostic de la situation future, c'est-à-dire l'erreur d'évaluation de l'évolution future du procédé suite à une action de l'opérateur. A ce stade, le diagnostic consiste à comparer la situation courante perçue avec la situation précédente et le pronostic permet une évaluation de l'évolution future du procédé par rapport à la situation actuelle.



- Enfin, contrairement aux processus internes d'acquisition et de traitement d'une situation, c'est une action sur le procédé qui peut modifier l'état de celle-ci. Une erreur d'action est soit une bonne exécution d'une mauvaise action, soit une erreur d'exécution d'une bonne action, soit une erreur d'exécution d'une mauvaise action. Le résultat de l'action est alors interprété par rapport aux exigences de la situation qui vient d'être analysée.

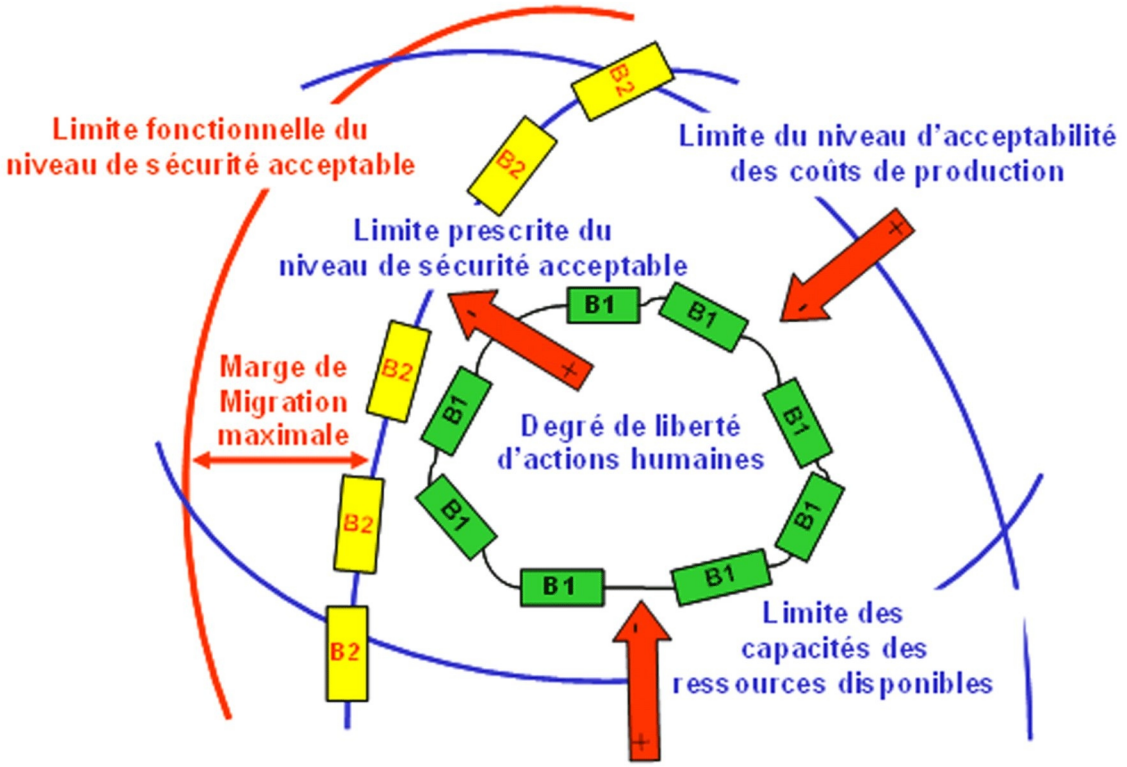
La propagation intra-individuelle d'une erreur se réalise de différentes manières selon les trois niveaux d'occurrence d'erreur, à savoir l'acquisition, le traitement de l'information ou l'action :

- Une erreur sur un niveau peut générer une erreur de même niveau.
- Une erreur sur un niveau peut générer une erreur dans un autre niveau.
- Une erreur peut générer une séquence d'erreurs.
- Etc

La propagation d'une erreur humaine est non seulement un processus individuel mais aussi collectif. Ainsi, par exemple, une erreur individuelle d'acquisition ou de traitement de l'information peut se propager à partir d'actions de communications orales via un téléphone ou une radio, ou de communications écrites via une messagerie électronique. Pour l'interlocuteur de cet opérateur humain, une erreur d'acquisition devient alors soit une erreur d'acquisition d'un message correct, soit l'acquisition d'un message incorrect, soit une erreur d'acquisition d'un message incorrect. Il est ainsi possible de déterminer le parcours des erreurs depuis leurs sources jusqu'à leurs cibles, en distinguant celui qui commet l'erreur et celui qui raisonne dans l'erreur.

D'autres facteurs externes tels que les facteurs environnementaux peuvent être intégrés dans le processus de diagnostic d'erreurs humaines. Par exemple, par rapport à différentes frontières déterminant les capacités des ressources

disponibles, l'acceptabilité des coûts de production et de la sécurité, des barrières ou des redondances peuvent être mises en oeuvre afin de garantir les possibilités d'actions humaines dans une zone prédéfinie et diagnostiquer les erreurs humaines au plus tôt pour optimiser les performances du procédé.



Toutefois, des contraintes diverses ayant pour objectif une réduction des coûts de production ou des ressources opérationnelles peuvent amener les opérateurs humains à outrepasser les limites fonctionnelles de sécurité par exemple et de définir une marge de migration acceptable tant qu'il n' y a pas d'accident ou d'interdiction répressive.

Moyens pour le diagnostic

VII

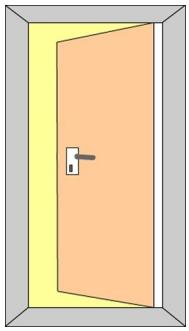
Les moyens proposés ne sont certes pas exhaustifs. Leurs spécifications peuvent être issues d'analyses préalables telles que des analyses de risque, de performance, de comportement avec des méthodes comme TESEO *(Tecnica Empirica Stima Errori Operatori)*, THERP *(Technique for Human Error Rate Prediction)*, MAC ou AMDEC.

A. Les barrières

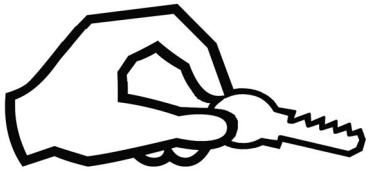
Une barrière est un moyen pour protéger le système contre l'occurrence ou les conséquences d'un état de fonctionnement donné.

Plusieurs types de barrières existent :

- Les barrières matérielles qui préviennent physiquement des actions exécutées ou de la propagation des conséquences. Elles n'ont pas besoin d'être perçues ou interprétées par l'opérateur humain pour qu'elles accomplissent leur fonction.

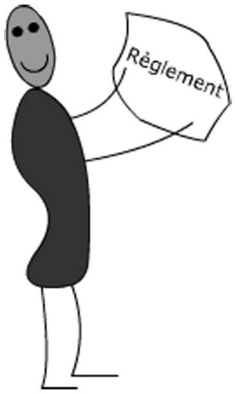


- Les barrières fonctionnelles gênent l'exécution de l'action en établissant, par exemple, une dépendance logique ou temporelle pour les activer. Ces barrières nécessitent la présence de pré-conditions qui doivent être vérifiées avant d'obtenir un résultat, mais qui n'ont pas besoin d'être perçues par l'opérateur humain.



- Les barrières symboliques nécessitent une interprétation pour qu'un opérateur humain puisse réagir ou répondre aux messages qu'elles contiennent.

- Les barrières immatérielles ne sont pas nécessairement présentes ou représentées dans la situation de travail, mais demandent d'être connues par l'opérateur pour être activées. Elles sont souvent représentées sur des supports physiques qui peuvent ne pas être matériellement sur le terrain lorsqu'elles sont utilisées. Il s'agit par exemple de réglementations ou de normes.



Ces barrières se retrouvent dans différents référentiels d'évaluation et d'interprétation du risque depuis la conception d'un outil de production jusqu'à son utilisation sur site. L'analyse hors-ligne ou en-ligne des risques permet donc de spécifier des barrières à différents niveaux décisionnels :

- Barrières placées par le concepteur du système. Suite aux études de risque, mais également par le biais du respect des normes et règles de sécurité, le concepteur équipe l'outil de production de barrières afin d'établir les défenses en série.

	Barrières matérielles	Barrières fonctionnelles	Barrières symboliques	Barrières immatérielles
CONCEPTEUR	Armoires électriques Grille de protection Carter Isolation	Capteurs de présence Inter-verrouillage Eloignement des commandes	Affichage Etiquetage sur l'outil Signalisation visuelle et sonore Supervision	Formation des futurs utilisateurs Manuels utilisateur

- Barrières placées par l'exploitant. L'outil est ensuite installé chez l'exploitant, dans un environnement de travail existant. Des barrières matérielles telles que les issues de secours ou les moyens individuels de protection sont ajoutées lors de l'aménagement des postes de travail et des ateliers. L'exploitant, pour répondre à la législation du travail (en tant qu'employeur) apporte également de nouvelles barrières.

	Barrières matérielles	Barrières fonctionnelles	Barrières symboliques	Barrières immatérielles
EXPLOITANT	Issues de secours Moyens individuels de protection	Détection incendie Limitation d'accès à certaines personnes	Affichage de consignes de sécurité Marquage au sol	Formation interne Règlement intérieur Procédures internes

- Barrières placées par les équipes d'opérateurs (le collectif de travail). Les conditions de travail amènent l'équipe des opérateurs humains/utilisateurs à se créer des barrières de sécurité afin de se prémunir d'incidents ou d'accidents.

	Barrières matérielles	Barrières fonctionnelles	Barrières symboliques	Barrières immatérielles
COLLECTIF DE TRAVAIL	Accès limité Consignation	Répartition des rôles	Communication orale, gestuelle ou sonore Affichage	Consignes lors d'une relève de postes Rapport

- Barrières des individus. Elles se traduisent, par exemple, la définition de barrières personnelles et individuelles.

	Barrières matérielles	Barrières fonctionnelles	Barrières symboliques	Barrières immatérielles
UTILISATEURS INDIVIDUELS	Agencement du poste de travail	Zone d'accès personnalisée	Affichage sauvage	Notes personnelles

La définition de ces barrières permet la mise en oeuvre d'une défense en série et en profondeur évitant ainsi l'occurrence d'incidents ou d'accident ou limitant leurs conséquences.

Le principe de redondance permet également le contrôle d'états de fonctionnement prédéfini en améliorant la sûreté de fonctionnement d'un procédé donné.

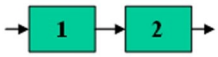
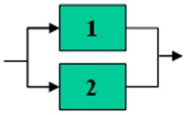
B. Les redondances

Le principe de **redondance** permet de mettre à disposition plusieurs ressources

pour réaliser une même fonction ou une même tâche. Certaines redondances permettent d'agir sur le procédé et d'en modifier le comportement alors que d'autres permettent à une ressource donnée de disposer de plusieurs moyens d'acquisition d'une même information.

D'une manière générale, une mesure notée R de la fiabilité ou de la disponibilité d'un système est une combinaison de probabilités $P(e_i)$ d'occurrence d'événements e_i du type « l'élément i du système est capable de fonctionner », et ce sur l'intervalle de temps [0,t] ou à l'instant t.

Dans une structure série, un système à deux éléments est fiable ou disponible si ces derniers le sont, tandis que dans une structure parallèle, il est fiable si au moins un élément l'est. Lorsque deux événements sont indépendants, l'occurrence de l'un ne peut affecter la probabilité d'occurrence de l'autre. Ainsi, le calcul de probabilités conditionnelles $P(e_1).P(e_2/e_1)$, multipliant la probabilité d'occurrence de e_1 par la probabilité d'occurrence de e_2 sachant l'occurrence de e_1, est simplifié par le produit $P(e_1).P(e_2)$. Lorsque les événements sont disjoints, ils ne peuvent apparaître simultanément.

Type	Série	Parallèle
Structure		
Mesure R de la fiabilité générale	$R=P(e_1 \cap e_2)$	$R=P(e_1 \cup e_2)$
Cas où e_1 et e_2 sont dépendants	$R=P(e_1).P(e_2/e_1)$	$R= P(e_1) + P(e_2) - P(e_1).P(e_2/e_1)$
Cas où e_1 et e_2 sont indépendants	$R=P(e_1).P(e_2)$	$R=P(e_1) + P(e_2) - P(e_1).P(e_2)$
Cas où e_1 et e_2 sont disjoints		$R=P(e_1) + P(e_2)$

(Remarque : Si un état de fonctionnement donné d'un élément n'est pas récupérable et entraîne l'arrêt du procédé, alors les calculs de la fiabilité et de la disponibilité de cet élément sont alors identiques).

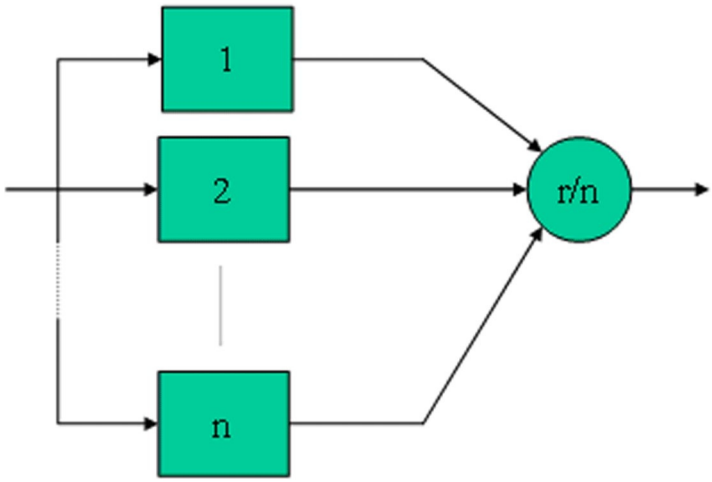
Un système redondant améliorant la sûreté de fonctionnement d'un système donné est basé sur des structures parallèles : un système constitué de n éléments redondants est fiable ou disponible si au moins un de ses éléments fonctionne. Deux types de redondance peuvent être mis en oeuvre :

- Une **redondance active** : les moyens sont mis en oeuvre simultanément (par exemple: redondance informationnelle).
- Une **redondance passive** : les moyens sont mis oeuvre à la demande (par exemple: redondance physique ou matérielle).

Différentes configurations peuvent être établies par combinaisons avec des structures en série selon lesquelles un système à n éléments en série est fiable ou disponible si tous ses éléments fonctionnent :

- La fiabilité ou la disponibilité d'une redondance active de type r/n nécessite qu'au moins r éléments parmi n fonctionnent. Si r=1 alors il s'agit d'une structure parallèle, et si r=n alors il s'agit d'une structure série.

Redondance active r/n



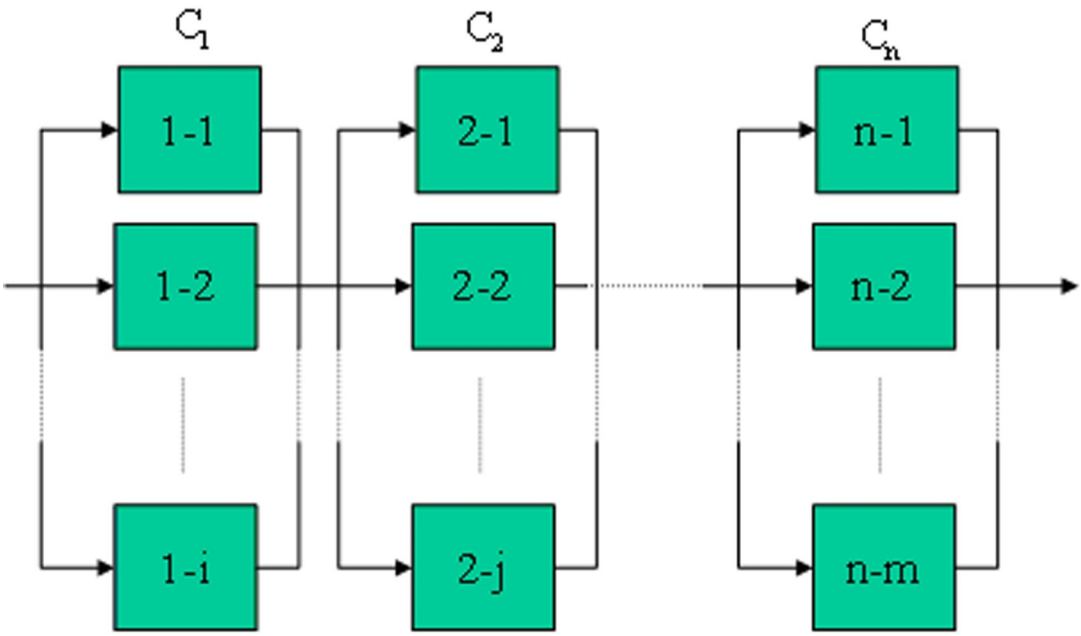
Probabilité de fiabilité R ?

$$R = P\left(\bigcup_{\forall I \in K_N^R} \left(\bigcap_{\forall e_i \in I} e_i \right) \right)$$

$$\left(K_N^R = \text{tous les sous} - \text{ensembles composés de R éléments parmi N}\right)$$

- Dans une redondance active de type parallèle/série, le système est fiable ou disponible si chaque colonne C_i a au moins un élément qui fonctionne.

Redondance active parallèle/série

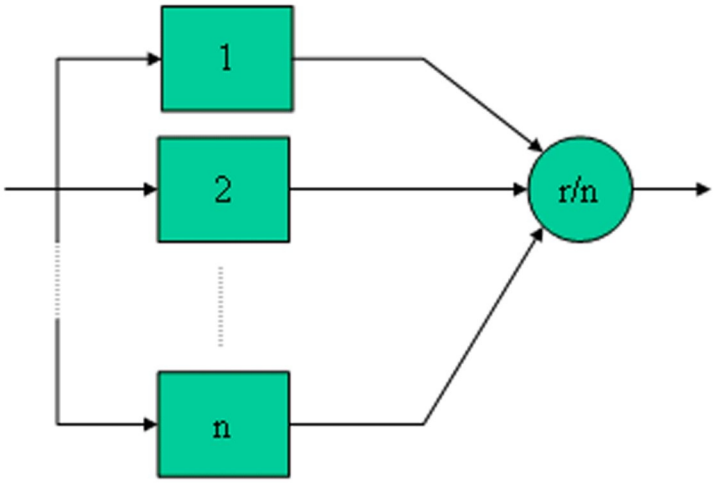


Probabilité de fiabilité R ?

$$R = P\left(\bigcap_{j=1}^{n}\left(\bigcup_{\forall e_i \in C_j} e_i\right)\right)$$

- Dans une redondance active de type série/parallèle, il l'est si au moins tous les éléments d'une ligne L_i fonctionnent.

Redondance active r/n



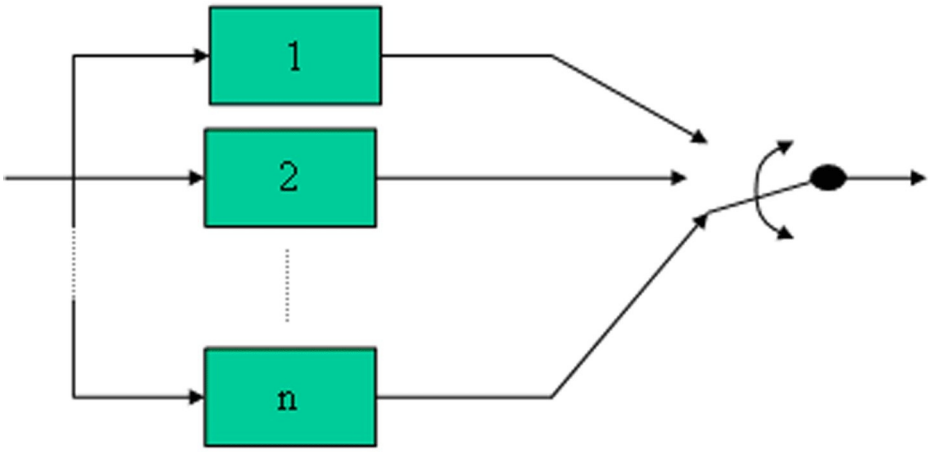
Probabilité de fiabilité R ?

$$R = P\left(\bigcup_{\forall I \subset K_N^T} \left(\bigcap_{\forall e_i \subset I} e_i \right) \right)$$

$$\left(K_N^T = \text{tous les sous} - \text{ensembles composés de T éléments parmi N}\right)$$

- La redondance passive requiert l'emploi d'un répartiteur pour sélectionner l'élément fiable à activer. Pour simplifier, ce répartiteur est considéré comme étant fiable. Il peut néanmoins être intégré dans le calcul global de la fiabilité ou de la disponibilité du système en le décomposant en deux éléments en série: un pour sa capacité à détecter un élément défaillant et un autre pour sa capacité à activer un élément qui fonctionne.

Redondance passive



Probabilité de fiabilité R ?

$$R = P\left(\bigcup_{i=1}^{n} e_i\right)$$

Les calculs de probabilité d'occurrence peuvent souvent être simplifiés avec l'exploitation des événements $\overline{e_i}$, complémentaires aux événements , tel que $P(\overline{e_i}) + P(e_i) = 1$:

$$P\left(\bigcup_{i=1}^{n} e_i\right) = 1 - P\left(\bigcap_{i=1}^{n} \overline{e_i}\right)$$

De plus, lorsque tous les événements e_i sont indépendants, il devient :

$$P\left(\bigcup_{i=1}^{n} e_i\right) = 1 - \prod_{i=1}^{n} P(\overline{e_i})$$

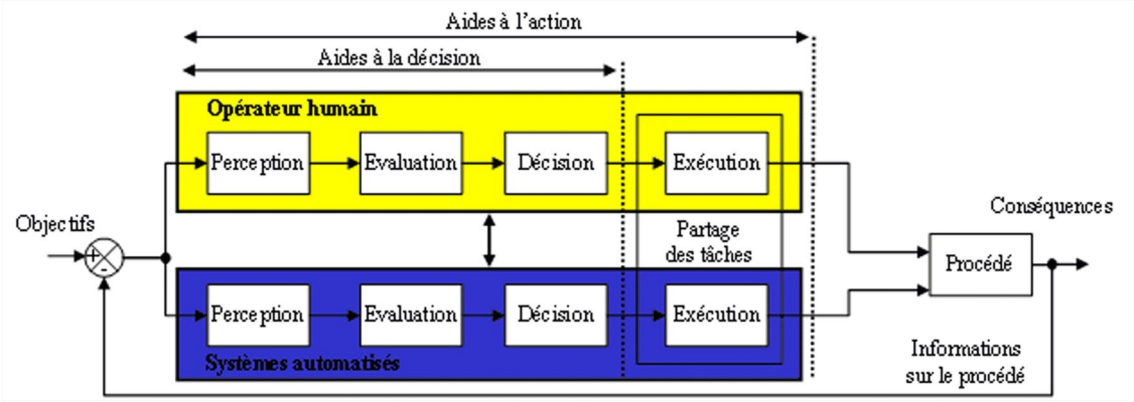
Les ressources redondantes peuvent parfois ne pas être de même nature. Il est en effet possible qu'une même fonction ou une même tâche soit réalisable par un système automatisé ou un opérateur humain. Les moyens sont donc interdépendants et une redondance interactive, voire coopérative est nécessaire.

C. Les redondances interactives

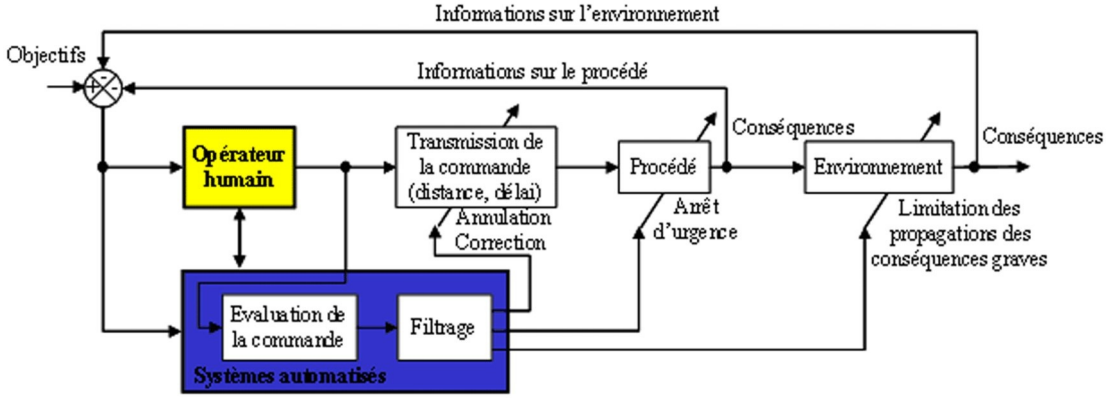
Dans une redondance interactive, voire coopérative, les éléments redondants travaillent ensemble afin d'atteindre des buts communs. Les activités de diagnostic (i.e., de détection d'un état de fonctionnement donné, d'évaluation des causes de

l'occurrence de cet état et de décision pour le modifier) peuvent alors être partagées entres différents décideurs (i.e. systèmes automatisés et/ou opérateurs humains). Ces décideurs sont alors capables de prévenir ou de récupérer en-ligne les dérives de fonctionnement :

- Les configurations de prévention les systèmes redondants sont activés avant l'action. Ils mettent en jeu une coopération pré-active ou pro-active. L'approche pré-active permet d'anticiper et d'éviter l'occurrence de dérives de fonctionnement (i.e., il s'agit d'un aide à la décision). L'approche pro-active permet de réguler l'activité par une répartition dynamique des tâches entre les décideurs (i.e., il s'agit d'une aide à l'action).



- Les systèmes correctifs sont post-actifs. Ce sont, par exemple, des outils de correction ou d'annulation de la transmission de la commande, des outils de gestion d'arrêt d'urgence du fonctionnement du procédé piloté, ou des outils d'aide à l'évacuation d'urgence.



Ces redondances interactives ou coopératives nécessitent un système de répartition et de communication pour optimiser le traitement des différentes étapes du diagnostic.

Le système de répartition peut se définir au travers des objectifs de la répartition, de l'objet à répartir, des modes de transformation d'un objet et des modes de contrôle du répartiteur pour l'activation de la répartition.

Système de répartition	
Objectif	Augmentation/Facilitation Prévention/Récupération
Objet	Fonction/Tâche/Action Donnée/Ressource/Connaissance/But
Transformation	Interruptible/Ininterruptible Récupérable/Irrécupérable Unique/Multiple Locale/Commune Séquentielle/Simultanée
Contrôle du répartiteur	Passif/Actif Préventif/Curatif Opportuniste/Tactique/Stratégique Manuel/Automatique Statique/Dynamique
Contrôle dynamique	Explicite/Implicite Préemptif/Définitif Interne/Externe/Mixte

Les objectifs de la répartition sont liés aux caractéristiques des capacités de prévention ou de récupération d'un décideur, ainsi qu'aux dérives affectant ces capacités. Il s'agit d'améliorer les performances du système, en augmentant les capacités d'un décideur et/ou en facilitant l'activité de celui-ci par l'intervention d'un autre décideur.

L'objet à répartir varie en fonction de ces objectifs. Il peut être une fonction du procédé piloté, une tâche pour la mise en oeuvre de cette fonction, ou une action sur le procédé pour modifier le comportement de celui-ci. Il peut s'agir d'une partie d'une fonction, d'une tâche ou d'une action. Une donnée, une ressource, une connaissance ou un but peuvent également être l'objet d'une répartition afin qu'un moyen puisse réaliser une fonction, une tâche ou une action. Ils peuvent être affectés à des moyens différents capables de les exploiter.

La transformation de l'objet à répartir dépend des caractéristiques de celui-ci. Elle peut être :

- interruptible si cette transformation peut être interrompue ou ininterruptible dans le cas contraire ;
- récupérable si cette transformation peut être corrigée ou irrécupérable dans le cas contraire ;
- unique si cette transformation concerne les mêmes décideurs ou multiple dans le cas contraire ;
- locale si cette transformation n'implique que les décideurs d'un même niveau organisationnel ou commun si elle concerne les décideurs de différents niveaux ;
- séquentielle s'il s'agit de répartir une à une chacune des étapes successives de la transformation d'un objet, simultanée si l'affectation concerne l'ensemble de ces étapes.

A partir de ces modes de transformation, l'activation de la répartition d'un objet donné peut s'effectuer selon des modes différents de contrôle du répartiteur :

- Mode passif et mode actif. Dans le mode passif, le contrôle de la répartition est activé à la demande alors que dans le mode actif, il est activé en permanence.
- Mode préventif et mode curatif. Le contrôle préventif est activé avant l'action sur le procédé et permet de minimiser l'occurrence d'erreurs. L'activité d'un décideur peut être régulée par celle d'un autre décideur ou confrontée à celle d'un autre. Le contrôle curatif est activé après l'action. Il permet de corriger une dérive d'un décideur afin de revenir à une situation

normale, de s'accommoder des conséquences d'une dérive d'un décideur mais en minimisant leurs effets, ou encore de reconfigurer les objectifs du système afin de se prémunir des effets des dérives d'un décideur.

- Mode opportuniste, mode tactique et mode stratégique. Le mode opportuniste est fonction d'opportunités du moment alors que les deux autres modes concernent des horizons temporels différents intégrant des critères prédéfinis. Le mode tactique est mis en oeuvre à court terme ou en temps réel, le mode stratégique à long ou moyen termes.
- Mode manuel et mode automatique. Dans le mode manuel, un opérateur humain contrôle l'activation de la répartition, alors que dans le mode automatique, c'est un système automatisé.
- Mode statique et mode dynamique. Pour le mode statique, les ensembles d'objets alloués aux systèmes redondants sont prédéfinis. Le mode dynamique est une répartition adaptative dans la mesure où un objet est affecté au décideur qui a, à ce moment là, les ressources matérielles et/ou cognitives disponibles pour le transformer.
- Mode explicite et mode implicite. Le mode explicite est un mode manuel dynamique et le mode implicite est un mode automatique dynamique.
- Mode préemptif et mode définitif. Ces modes sont particuliers au mode dynamique. Le mode préemptif prend en compte la possibilité de modifier l'allocation initiale d'un objet, à savoir d'interrompre la transformation d'un objet allouée à un décideur pour l'affecter à un autre décideur. Dans le mode définitif, cette ré-allocation est impossible.
- Modes interne, externe ou mixte. Le mode interne concerne les organisations dans lesquelles les décideurs appartiennent au même niveau décisionnel alors que le mode externe peut être appliqué à des organisations à plusieurs niveaux décisionnels dans lesquelles un niveau supérieur décide de la répartition des objets entre les décideurs d'un niveau inférieur. Le mode mixte combine les deux modes et s'applique aux organisations décomposées horizontalement et verticalement.

La communication permet d'intégrer l'activité d'un décideur et ses résultats dans ceux d'un autre décideur et peut s'organiser de diverses façons en engageant un processus interactif pour expliquer telle ou telle démarche de raisonnement, pour confronter plusieurs raisonnements conflictuels, pour solliciter une aide particulière ou pour simplement informer un décideur des intentions de l'autre. L'intégration de l'activité d'un décideur dans celle d'un autre par la communication est liée aux moyens utilisés pour interagir : intégration observable vs inobservable, intégration verbale vs non-verbale, intégration directe non-médiatisée vs médiatisée, intégration formelle vs informelle, intégration avec accusé de réception vs sans accusé de réception, etc. Ces communications intégratives s'organisent temporellement (i.e. communications séquentielles, simultanées, en différé ou à la demande), géographiquement (i.e. communications à distance ou de proximité), et en fonction de l'implication des décideurs (i.e. communications à tous les décideurs ou à une partie d'entre eux).

Système de répartition	
Objectif	Explicatif/Confrontatif Sollicitatif/Informatif
Intégration	Observable/Inobservable Verbale/Non verbale Non médiatisée/Médiatisée Formelle/Informelle Avec accusé réception/Sans accusé réception
Organisation	Séquentielle/Simultanée En différé/A la demande Distante/De proximité Totale/Partielle

Méthodes de diagnostic

VIII

De nombreuses méthodes d'analyse peuvent être utilisées afin de déterminer le diagnostic d'un état de fonctionnement donné. En fonction des objectifs des analyses associées à ces méthodes, le diagnostic de sécurité, de performance, de disponibilité, d'erreur humaine, etc. pourra être entrepris.

Deux catégories de méthodes sont présentées ici :

- Les méthodes d'analyse d'erreurs humaines telles que TESEO ou THERP
- Les méthodes d'analyse de défaillances telles que l'AMDEC ou la MAC.

Exemples	Principe	Objectif
THERP, TESEO	Analyse des actions erronées	Diagnostic d'erreur humaine
AMDEC, MAC	Analyse d'événement redouté	Diagnostic de défaillance

Le résultat des analyses effectuées à partir de ces méthodes pourra orienter les spécifications de moyens de contrôle de l'activité de diagnostic tels les barrières, les redondances ou les redondances interactives. Le formalisme de la méthode MAC sera retenu pour illustrer la genèse d'un niveau de performance, d'un comportement, d'une erreur, etc.

A. Diagnostic d'erreur humaine

1. TESEO

La méthode TESEO (Tecnica Empirica Stima Errori Operatori) permet de calculer une probabilité d'occurrence d'erreur humaine

La valeur de la probabilité d'erreur est une agrégation de plusieurs paramètres : complexité de l'action à réaliser, temps disponible pour la réaliser, expérience et formation de l'opérateur face à cette action, émotion de l'opérateur relative à la gravité de la situation, et caractéristiques ergonomiques des interfaces et de l'environnement.

La méthode TESEO permet d'obtenir une estimation rapide de la probabilité d'erreur P(E) par le produit de cinq facteurs K1, K2, K3, K4 et K5. 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.

K1, K2 et K5 sont des facteurs externes à l'opérateur humain réalisant une tâche, alors que K3 et K4 sont des facteurs internes :

- K1 est lié aux exigences fonctionnelles de la tâche, c'est-à-dire à la complexité de la tâche à réaliser.

TABLE 1 Facteur d'exigence fonctionnelle	
Type de tâche	K1
Simple routinière	0.001
Requiert l'attention mais routinière	0.01
Non routinière	0.1

Tableau 9 : TABLE 1 : Facteur d'exigence fonctionnelle

- K2 est lié aux exigences temporelles de la tâche en se limitant au temps disponible pour la réaliser.

TABLE 2a Facteur d'exigence temporel Tâche routinière		TABLE 2b Facteur d'exigence temporel Tâche non routinière	
Temps disponible en (s)	K2	Temps disponible en (s)	K2
2	10	3	10
10	1	30	1
20	0,5	45	0,3
		60	0,1

Tableau 10 : TABLE 2a : Facteur d'exigence temporel Tâche routinière et TABLE 2b : Facteur d'exigence temporel Tâche non routinière

- K3 est lié à la compétence de l'opérateur qui réalise la tâche.

TABLE 3 Facteur de compétence	
Compétence de l'opérateur	K3
Bien sélectionné - expert bien entraîné	0,5
Connaissance et formation moyenne	1
Peu de connaissance et de formation	3

Tableau 11 : TABLE 3 : Facteur de compétence

- K4 est un facteur émotionnel qui dépend de la gravité de la situation.

TABLE 4 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 12 : TABLE 4 : Facteur émotionnel

- K5 est un facteur environnemental relatif aux conditions ergonomiques de travail.

TABLE 5 Facteur ergonomique de travail	
Facteur ergonomique de l'environneme	K5
Excellent climat - excellentes interfaces	0,7
Bon climat - bonnes interfaces	1
Climat moyen – interfaces moyennes	3
Climat moyen – mauvaises interfaces	7
Mauvais climat – mauvaises interfaces	10

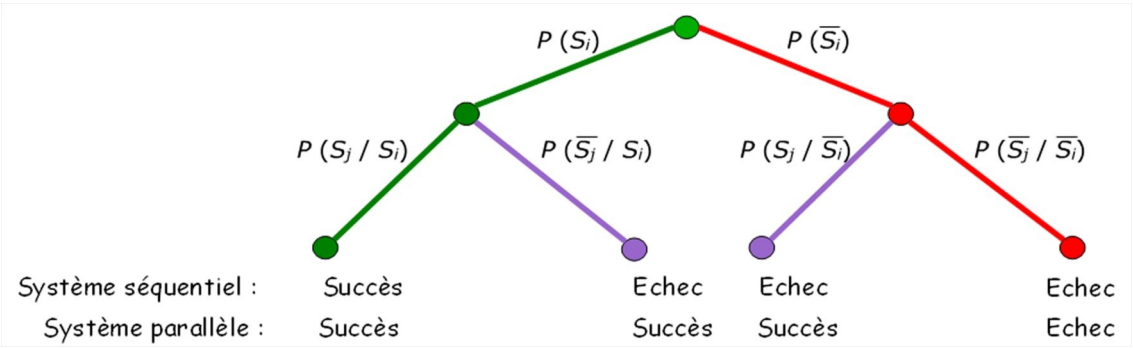
Tableau 13 : TABLE 5 : Facteur ergonomique de travail

Néanmoins, le calcul est borné à 1 pour éviter que la probabilité calculée soit supérieure à 1 ! Par conséquent, même si TESEO est une méthode rapide d'évaluation, il semble que le calcul de probabilité ne soit pas rigoureux. De plus, la description d'une tâche et les caractéristiques de l'opérateur humain sont extrêmement simplifiées face à la complexité des activités cognitives précédemment décrites dans les modèles de l'erreur humaine.

2. THERP

La méthode THERP (Technique for Human Error Rate Prediction) permet de calculer une probabilité d'occurrence d'erreur humaine.

La probabilité d'erreur est évaluée à partir de trois facteurs : une probabilité de base relative aux caractéristiques de la tâche à réaliser, un coefficient correctif pour la prise en compte des facteurs pouvant affecter l'exécution de cette tâche, et une probabilité de non-récupération de l'erreur.



Type	Séquentiel	Parallèle
Cas général	$P(Echec)=1-P(Succès)=1-P(S_i \cap S_j)$	$P(Echec)=P(\overline{S_i} \cap \overline{S_j})$
i et j dépendantes	$P(Echec)=1-P(S_i).P(S_j/S_i)$	$P(Echec)=P(\overline{S_i}).P(\overline{S_j}/\overline{S_i})$
i et j indépendantes	$P(Echec)=1-P(S_i).P(S_j)$	$P(Echec)=P(\overline{S_i}).P(\overline{S_j})$

La probabilité de non-récupération intègre les difficultés de récupérer une tâche erronée en fonction de délai de détection de l'erreur. Par exemple, il s'agira d'intégrer une probabilité de non-récupération avant 30 secondes, 10 minutes, 30 minutes, etc.

L'évaluation des probabilités d'erreur dans l'exécution de tâches élémentaires s'appuie sur des tables prédéfinies telles que celles présentées ci-dessous.

Exemples de tâches élémentaires	Probabilité moyenne d'erreur
Utiliser une liste de contrôle	0,5
Suivre des procédures ou des règlements	0,01
Lire une alarme sonore ou lumineuse	0,0001
Lire une alarme lumineuse	0,001
Lire un affichage digital	0,001
Lire un graphe	0,01
Lire un imprimé	0,05
Mémoriser plus de 3 digits	0,001
Détecter une déviation sur un écran qui possède des repères	0,05
Positionner un bouton	0,001
Brancher une connexion	0,01
Se rappeler des instructions	0,001
Traiter toutes les instructions d'une courte liste (10 instructions au plus) cochées après exécution	0,001
Traiter toutes les instructions d'une courte liste non cochées après exécution	0,003
Sélectionner un panneau de contrôle parmi un groupe	0,003
Sélectionner un panneau de contrôle similaire à un autre	0,0005
Etc…	

B. Diagnostic de défaillance

1. AMDEC

La méthode AMDEC (Analyse des Modes de Défaillance, de leurs Effets et de leurs Criticité) détermine les modes de défaillances potentielles, leurs causes possibles, et leurs effets sur le système homme-machine, en évaluant pour chacun d'eux la criticité à partir de la gravité et la fréquence d'apparition en y combinant éventuellement une probabilité de non-détection.

Dans une première phase, l'AMDEC consiste à examiner comment et pourquoi les fonctions du système étudié risquent de ne plus être assurées correctement. Elle permet d'identifier les modes de défaillances dont les effets sont observables à partir des performances du système en termes de fiabilité, de disponibilité ou de sécurité, un mode de défaillance d'un composant étant défini comme l'effet par lequel une défaillance de ce composant est observée. Mais, l'objectif est également d'évaluer les effets de chacun de ces modes de défaillances sur les fonctions du système.

La méthode repose sur une grille d'analyse qui peut être adaptée et modifiée selon les objectifs et le système de l'étude. Par exemple, elle peut permettre :

- d'identifier le composant étudié,
- de relever pour ce composant toutes ses fonctions,
- de recenser les modes de défaillance,

- de définir les causes possibles de ces défaillances et leurs conséquences sur le système,
- de proposer un indice de criticité,
- de lister les moyens de détection,
- de déterminer les parades de l'opérateur humain pour gérer les défaillances.
- etc.

Identification du composant	Fonctions Etats	Modes de défaillance	Causes possibles	Effets	Criticité	Moyens de détection	Parades de l'opérateur humain	Observations

Dans une seconde phase, l'AMDEC cherche à évaluer la criticité des modes de défaillances à partir en général de deux critères de cotation indépendants (table 2.3) : la gravité des effets sur le système et la fréquence d'apparition des défaillances. Ceci permet de hiérarchiser les défaillances potentielles, et de proposer des actions correctives pour les points critiques.

		Probabilité			
		Très faible	Faible	Moyenne	Forte
Gravité	Effets mineurs				
	Effets significatifs				
	Effets critiques				
	Effets catastrophiques				

De manière générale la criticité sera d'autant plus importante que la gravité et la probabilité d'occurrence sont importantes. Il est à noter que la criticité peut être pondérée par une probabilité de détection de la défaillance. Ainsi, si la défaillance est facilement détectable, l'élaboration d'un plan de récupération est envisageable afin de limiter son effet sur le système. Dans le cas contraire, des mesures telles qu'une modification de la configuration du système, l'ajout de capteurs de détection de pannes ou la définition d'une périodicité de contrôle de l'état des composants, peuvent être souhaitables.

2. MAC

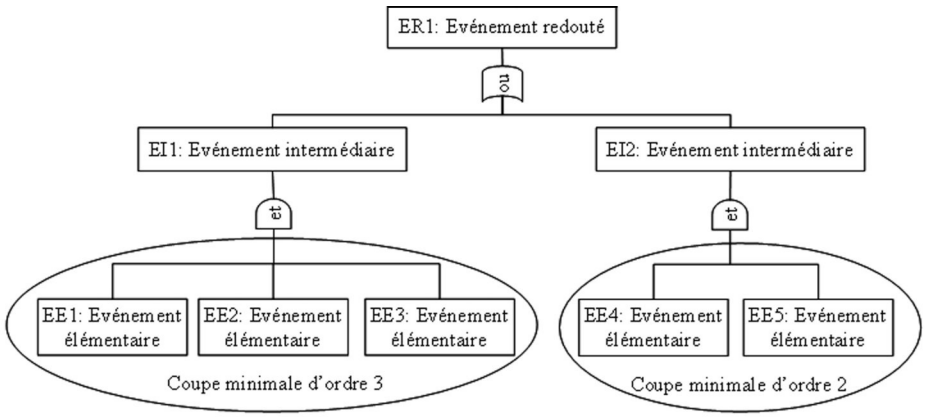
La Méthode des Arbres de Causes permet d'identifier les combinaisons d'événements élémentaires pouvant conduire à des événements redoutés, et de calculer leur probabilité d'occurrence. Elle est également connue sous les noms de Méthode des Arbres des Défauts ou Méthode des Arbres des Défaillances.

Elle se base sur une représentation graphique de combinaisons de causes pouvant produire un événement redouté donné. Cette représentation permet une analyse qualitative à partir des relations logiques entre les causes ou une analyse quantitative à partir d'un calcul de probabilité d'occurrence des causes.

L'analyse qualitative permet d'identifier tous les scénarios de combinaison d'événement élémentaires qui conduisent à un événement redouté. Ces scénarios sont appelés des coupes. Une coupe est dite minimale lorsque l'absence d'au moins un des événements élémentaires qui la constitue ne permet pas de conduire à l'événement redouté. L'ordre d'une coupe correspond au nombre d'événements élémentaire constituant cette coupe.

Par exemple, dans la figure ci-dessous, la combinaison des événements élémentaires EE1, EE2 et EE3 est une coupe minimale d'ordre 3 alors que la combinaison des événements élémentaires EE4 et EE5 est une coupe minimale

d'ordre 2. Plus l'ordre des coupes est élevé, plus le système étudié est robuste face aux défaillances.

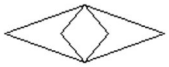


Analyse qualitative par combinaison logique :
$ER1 = EI1 \cup EI2 = (EE1 \cap EE2 \cap EE3) \cup (EE4 \cap EE5)$

Analyse quantitative par probabilité d'occurrence P(ER1) :
$P(ER1) = P(EI1 \cap EI2) = P((EE1 \cap EE2 \cap EE3) \cup (EE4 \cap EE5))$

Le formalisme de la méthode exploite des symboles associés à des portes logiques ou à des caractéristiques d'événements.

Symbole des portes logiques	Signification	Explication (a et b : entrées, s : sortie)
	ET logique	a b s 0 0 0 1 0 0 0 1 0 1 1 1
	NON ET logique (opposé de la porte ET)	a b s 0 0 1 1 0 1 0 1 1 1 1 0
	OU logique	a b s 0 0 0 1 0 1 0 1 1 1 1 1
	NON OU logique (opposé de la porte OU)	a b s 0 0 1 1 0 0 0 1 0 1 1 0
	OU EXCLUSIF	a b s 0 0 0 1 0 1 0 1 1 1 1 0

Symbole des événements	Signification	Explication
	Rectangle	Evénement résultant de la combinaison d'autres événements par l'intermédiaire d'une porte logique
	Losange	Evénement qui ne peut être considéré comme élémentaire mais dont les causes ne seront pas développées
	Double losange	Evénement dont les causes ne sont pas encore développées mais le seront ultérieurement
	Cercle	Evénement élémentaire qui ne nécessite pas d'être développé
	Maison	Evénement de base qui se produit normalement pendant le fonctionnement du système
	Ovale	Evénement conditionnel, utilisé avec certaines portes logiques telles que le OU (i.e. la sortie est vraie si au moins une des entrées l'est et si la condition est réalisée)

C. Exercices d'illustration

1. Application de TESEO

Calculer la probabilité d'erreur pour un conducteur apprenant à conduire depuis 12 mois, roulant sur une 2CV dans les situations suivantes : éviter une collision sur autoroute détectée 35 secondes avant l'impact, s'arrêter à un feu tricolore en trafic élevé avec forte visibilité, et faire un créneau en ville dans un trafic faible.

Probabilité d'erreur(éviter une collision sur autoroute) = 0,1 x 1 x 1 x 3 x 3 = 0,9

Probabilité d'erreur(s'arrêter à un feu tricolore en trafic élevé) = 0,01 x 0,5 x 1 x 2 x 3 = 0,03

Probabilité d'erreur(faire un créneau en ville dans un trafic faible) = 0.1 x 1 x 1 x 1 x 3 = 0,3

2. Application de THERP

Déterminer la probabilité d'erreur sans récupération de l'activité suivante : démarrer un véhicule, sachant que le conducteur est déjà placé sur son siège.

Solution :

L'activité est considérée comme séquentielle et décomposée de 4 sous-activités indépendantes, et ce de la manière suivante :

- Mettre le contact : Détecter le démarreur, Détecter la pédale d'accélération, Insérer la clef de contact, Tourner la clef, Accélérer.
- Embrayer : Détecter la pédale d'embrayage, Appuyer sur la pédale
- Mettre la première vitesse : Détecter la boite de vitesse, Enclencher la première vitesse
- Débrayer : Détecter la pédale d'embrayage, Détecter la pédale d'accélération, Relâcher la pédale, Accélérer

Chaque sous-activité comprend des tâches élémentaires pour lesquelles les probabilités moyennes d'occurrence d'erreur peuvent être déterminées à partir des tables prédéfinies de THERP (on se limitera ici à exploiter la table donnée dans ce cours) :

- Probabilité d'erreur(Mettre le contact) = 1 - ((1 - 0,003) x (1 - 0,0005) x (1 - 0,01) x (1 - 0,001) x (1 - 0,001)) = 0,0154
- Probabilité d'erreur(Embrayer) = 1 - ((1-0,0005) x (1-0,001)) = 0,006
- Probabilité d'erreur(Mettre la vitesse)= 1 - ((1-0,003) x (1-0,0005)) = 0,0035
- Probabilité d'erreur(Débrayer)= 1 - ((1 - 0,0005) x (1 - 0,0005) x (1 - 0,003) x (1 - 0,003)) = 0,0070

3. Application de l'AMDEC

Etablir une AMDEC d'un pneumatique de voiture et pour le mode de défaillance suivant : « éclatement du pneumatique ».

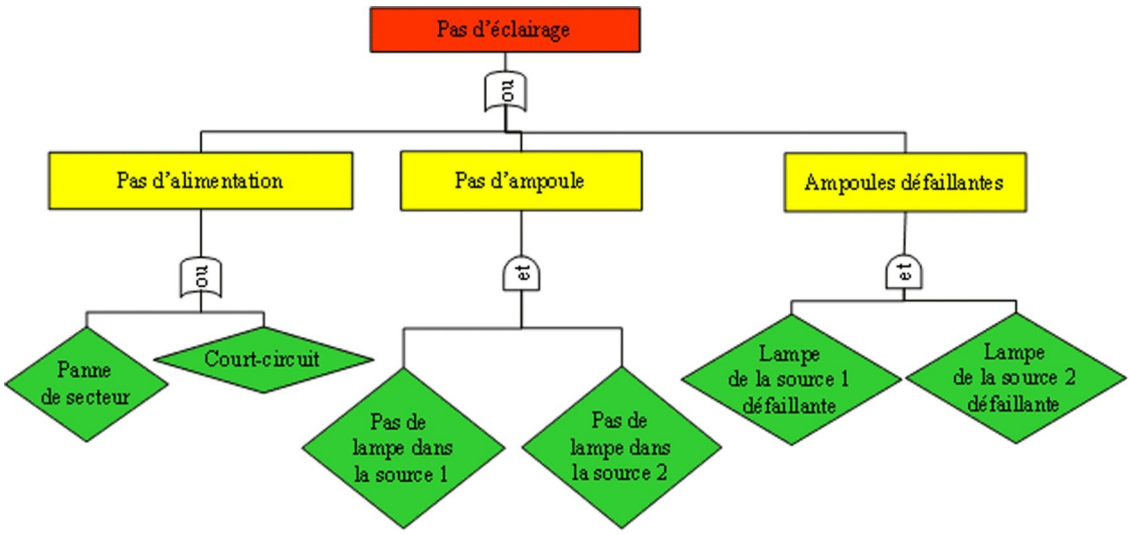
Solution :

Identification du composant	Fonctions	Etats	Modes de défaillance	Causes possibles	Effets	Moyens de détection	Parades de l'opérateur humain
Pneumatique	Adhérence Déplacement	Normal Dégradé (Dégonflé Crevé Usé, Eclaté, …)	Eclatement	Choc Usure Intrusion Frottement Malveillance	Immobilisation Perte de contrôle Choc Accident	Capteur de pression Capteur d'usure	Vérification périodique

4. Application de MAC

Faire l'arbre de causes pour l'événement suivant : « pas de lumière dans une rue ayant deux sources distinctes d'éclairage».

Solution :



Représentation de diagnostics par la méthode MAC

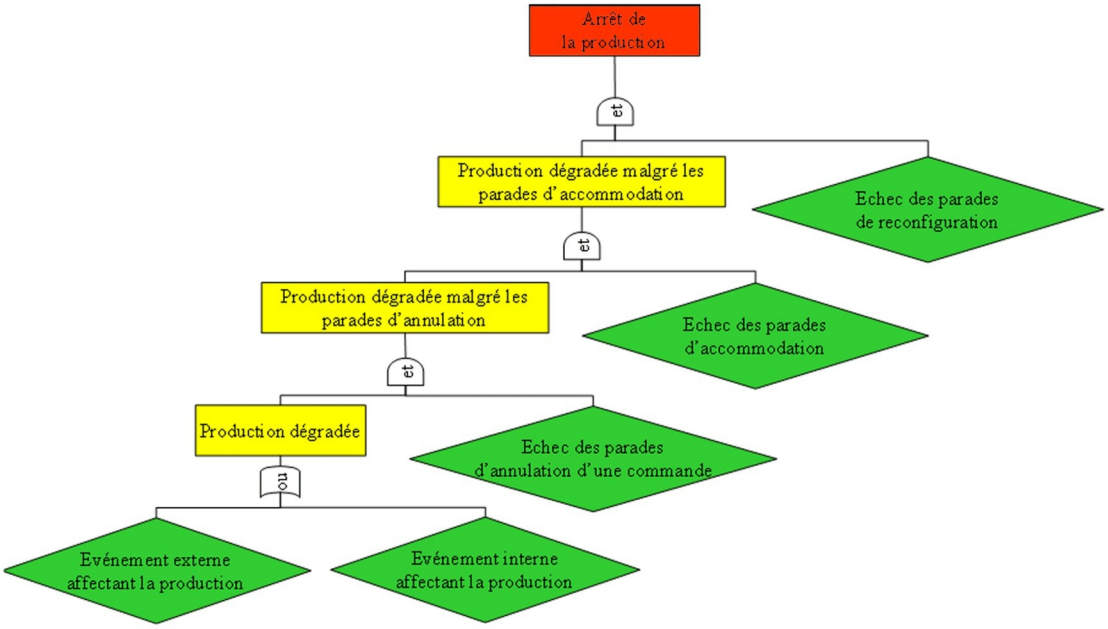
IX

Dans un soucis de simplification, le formalisme de la méthode MAC est retenu afin d'expliquer le cheminement d'un comportement, d'une erreur, d'un niveau de performance, etc... et d'en faciliter le diagnostic.

A. Diagnostic de panne

De même, à partir du formalisme de MAC, face à des événements externes ou internes à un système de production donné et à l'échec successif des parades de récupération de dérives en production, l'arrêt de la production est irrémédiable pour effectuer les réparations ou les réglages nécessaires.

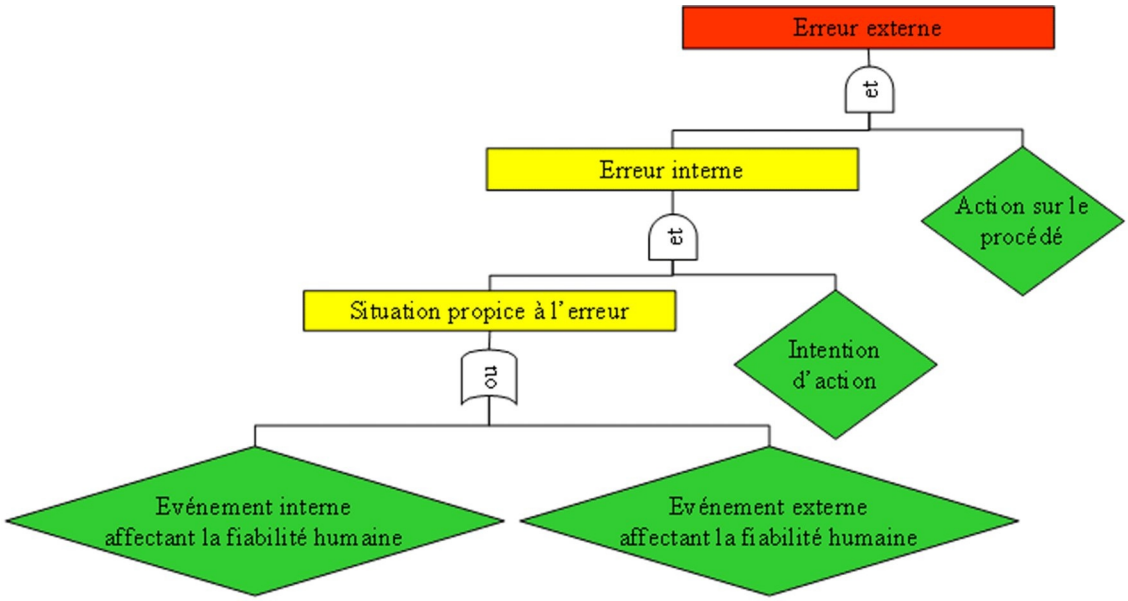
Ces parades sont par exemple, l'application de modes d'annulation d'une commande préalable, la modification des paramètres de contrôle du procédé (i.e. parades d'accommodation), ou l'adaptation des objectifs à suivre (i.e. parades de reconfiguration).



B. Diagnostic d'erreur humaine

A partir du formalisme de MAC, une erreur humaine peut être identifiée à deux niveaux : au niveau interne indépendamment de l'état du procédé piloté et au niveau externe résultant d'une action sur celui-ci.

L'occurrence d'un événement interne ou d'un événement externe affectant la fiabilité humaine peut générer un événement propice à la production d'une erreur humaine. Celle-ci étant indissociable avec la notion d'intention, l'erreur interne est la jonction d'un événement propice à l'erreur et d'une intention préalable d'agir sur le procédé. Lorsque l'action est effective, l'erreur devient externe.



Les événements externes ou internes sont propres à des facteurs favorisant leur apparition. Ces facteurs sont par exemple ceux présentés au paragraphe précédent

concernant la réversibilité du contrôle, la pilotabilité du procédé, l'excès de confiance des opérateurs humains, le masquage des erreurs, etc.

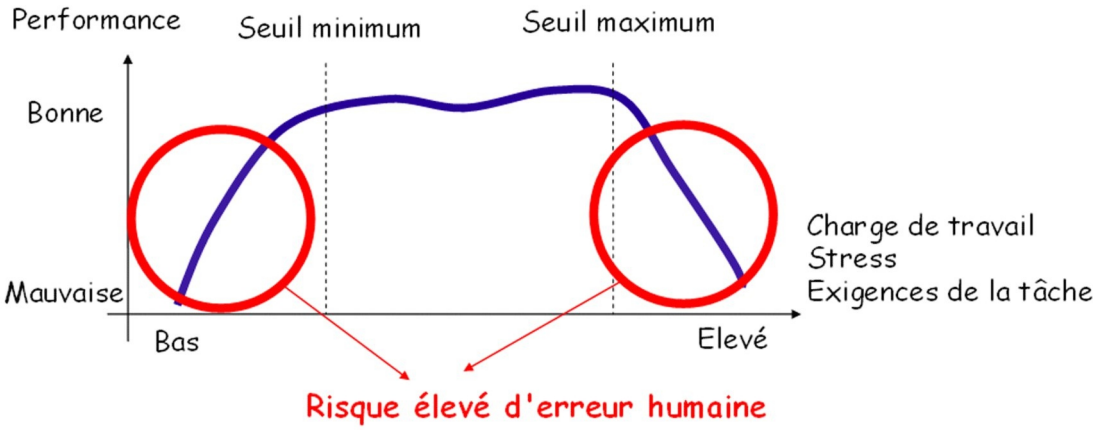
Les événements internes pouvant générer une situation propice à l'erreur sont par exemple l'expérience face à une situation courante, le niveau de motivation dans le travail ou le niveau de confiance accordé aux systèmes automatisés, la surcharge ou la sous-charge de travail mentale.

Les événements externes sont, quant à eux, liés aux caractéristiques de la tâche à réaliser, du procédé piloté ou de l'environnement de travail. Des exigences de tâche importantes, un comportement anormal du procédé, des interférences avec d'autres opérateurs humains ou des systèmes automatisés sont des exemples d'événements externes à l'opérateur pouvant affecter la fiabilité de celui-ci.

C. Diagnostic de non-performance

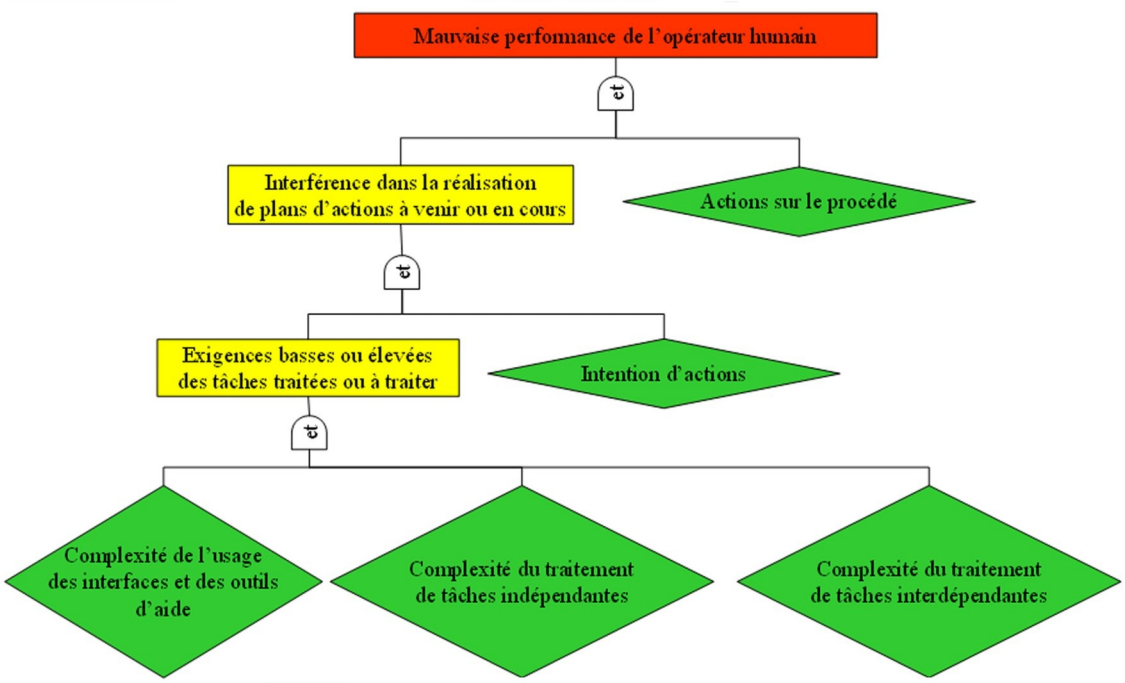
Une mauvaise performance ou l'absence de performances est liée à des facteurs affectant la performance dans le cadre du traitement de tâches prédéfinies.

L'identification et l'évaluation des tous les facteurs pouvant affecter la fiabilité humaine étant difficiles à réaliser, de nombreuses études ont tenté de limiter ces facteurs d'influence en se basant sur leurs interdépendances. Par exemple, différentes relations déterminées de manière empirique ou hypothétique peuvent être effectuées : des niveaux bas ou élevés des exigences de tâches, de la charge de travail mentale ou de stress peuvent générer des niveaux de performance dégradés ou de risques plus importants d'erreurs humaines. Entre deux seuils minimum et maximum, la performance et le risque d'erreur humaine restent acceptables.



Les exigences de tâches correspondent aux difficultés intrinsèques des tâches : elles sont quantifiables par des mesures temporelles, physiques, ou fonctionnelles. La charge de travail est, quant à elle, la difficulté que ressent l'opérateur humain lorsqu'il exécute une tâche, et ce en fonction de son état physiologique, psychologique et son savoir-faire.

Ainsi, un niveau de charge de travail élevé ou bas peut être mis en corrélation avec un niveau d'exigences de tâches bas ou élevé respectivement. Comme le calcul de la charge de travail telle qu'elle vient d'être définie ci-dessus semble difficile voire impossible, un estimateur d'exigences de tâche peut parfois être suffisant pour diagnostiquer un niveau de performance inacceptable.

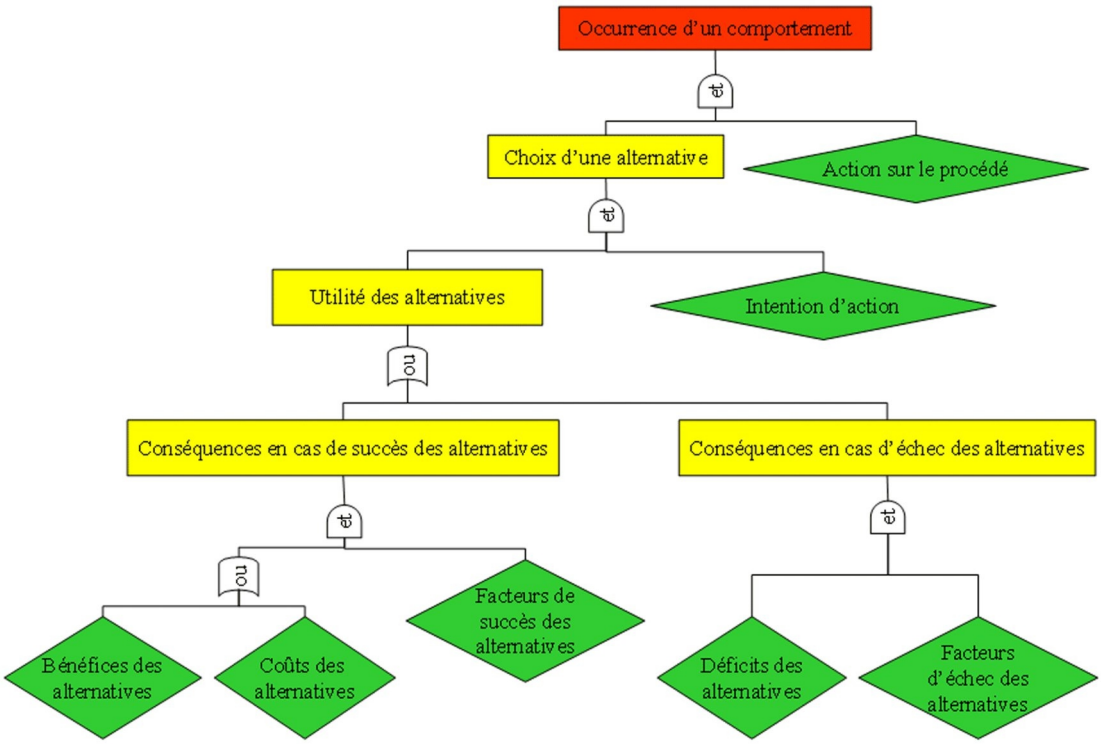


Un calcul des exigences fonctionnelles et temporelles du traitement des tâches indépendantes et interdépendantes et des exigences physiques d'exploitation des interfaces et des outils d'aide par exemple suffire pour identifier des niveaux bas et élevés de complexité des tâches traitées ou à traiter.

La mauvaise performance se traduit par la présence de ces niveaux élevé ou bas de complexité combiné avec des décisions d'action sur le procédé : ces décisions interfèrent avec les plans d'action, ces interférences facilitant l'occurrence d'erreur humaine.

D. Diagnostic de comportement

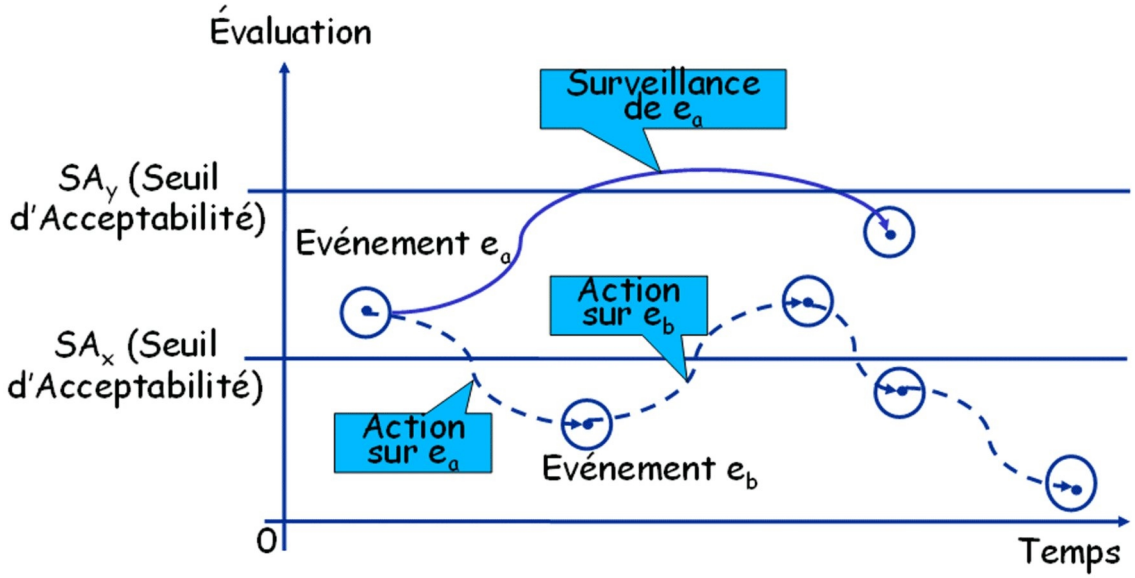
On peut associer les conséquences qui découlent des différentes alternatives d'actions possibles sur le procédé en termes de bénéfices, coûts ou dangers ou déficits potentiels. Par exemple, l'occurrence d'un comportement d'un opérateur humain (e.g., exécution d'un plan d'action, exécution d'une violation ou d'une action erronée, etc.) peut être déterminé à partir des bénéfices immédiats attendus malgré des coûts acceptables en cas de succès et en dépit des dangers ou déficits potentiels en cas d'échec de l'alternative choisie.



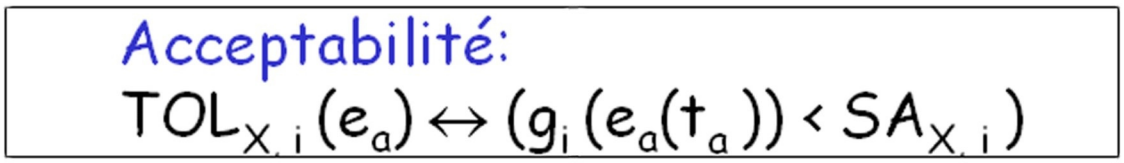
La combinaison des bénéfices, des coûts et des déficits potentiels en intégrant les facteurs de succès et d'échec permet de calculer l'intérêt ou l'utilité de telle ou telle alternative. Le choix de la meilleure alternative dépend du critère associé à l'intention d'action. Par exemple, l'alternative sélectionnée pourra être celle qui permet d'obtenir l'utilité maximale.

Le diagnostic de comportement en termes de bénéfices, coûts et déficits potentiels peut être effectué de manière qualitative ou quantitative, et ce pour différents critères d'évaluation.

Un événement donné peut être interprété différemment en fonction du référentiel utilisé pour l'analyse. Ainsi, en considérant par exemple les seuils d'acceptabilité distincts de X et Y, l'événement A est accepté par le décideur Y alors qu'il est inacceptable pour le décideur X :



Une fonction d'acceptabilité $TOL_{X,i}(e_a(t_a))$ doit donc être définie pour un événement e_a occurrent à la date t_a à partir d'une fonction de gravité g_i pour un critère i donné, et ce pour un décideur X :

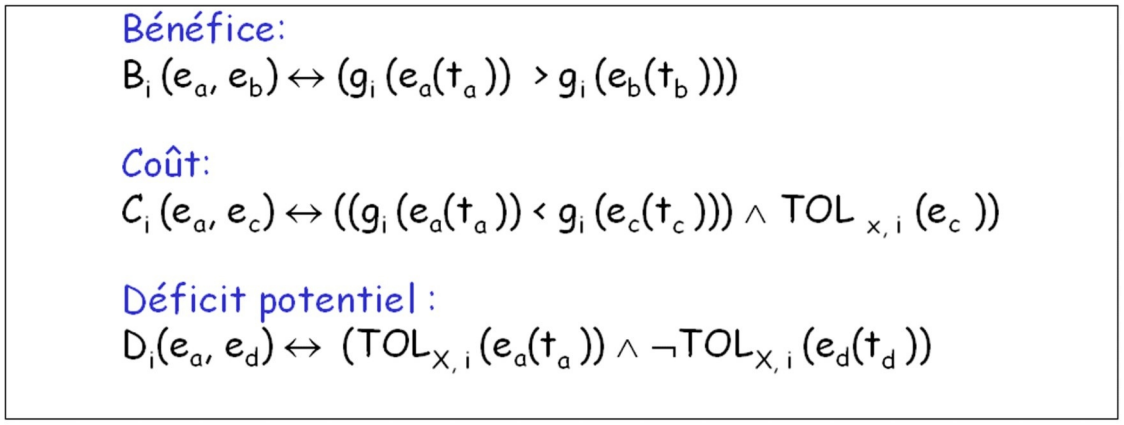


Deux types de comparaisons sont alors possibles :

- Comparer des événements dépendants lorsque qu'un événement résulte d'une autre du fait d'une activité humaine de contrôle ou de supervision ou d'une évolution normale ou anormale du procédé piloté sans aucune intervention humaine.
- Comparer des événements indépendants lorsqu'il s'agit d'évaluer plusieurs plans d'actions ou d'analyser les comportements réels par rapport aux prescriptions par exemple.

Dans les deux cas, deux types d'analyse sont possibles :

- une analyse qualitative permettant d'associer les bénéfices, les coûts ou les déficits potentiels aux critères d'évaluation :



- une analyse quantitative permettant de calculer les bénéfices, les coûts ou les déficits potentiels :

Fonction générique :

$$K_{J,i}(e_a, e_e) = g_i(e_e(t_e)) - g_i(e_a(t_a))$$

Bénéfice/Coût/Déficit:

$$K_{J,i}(e_a, e_e) = \begin{cases} K_{B,i}(e_a, e_e) & \text{si } B_i(e_a, e_e) \\ K_{C,i}(e_a, e_e) & \text{si } C_i(e_a, e_e) \\ K_{D,i}(e_a, e_e) & \text{si } D_i(e_a, e_e) \\ 0 & \text{sinon} \end{cases}$$

Cas d'études pratiques

X

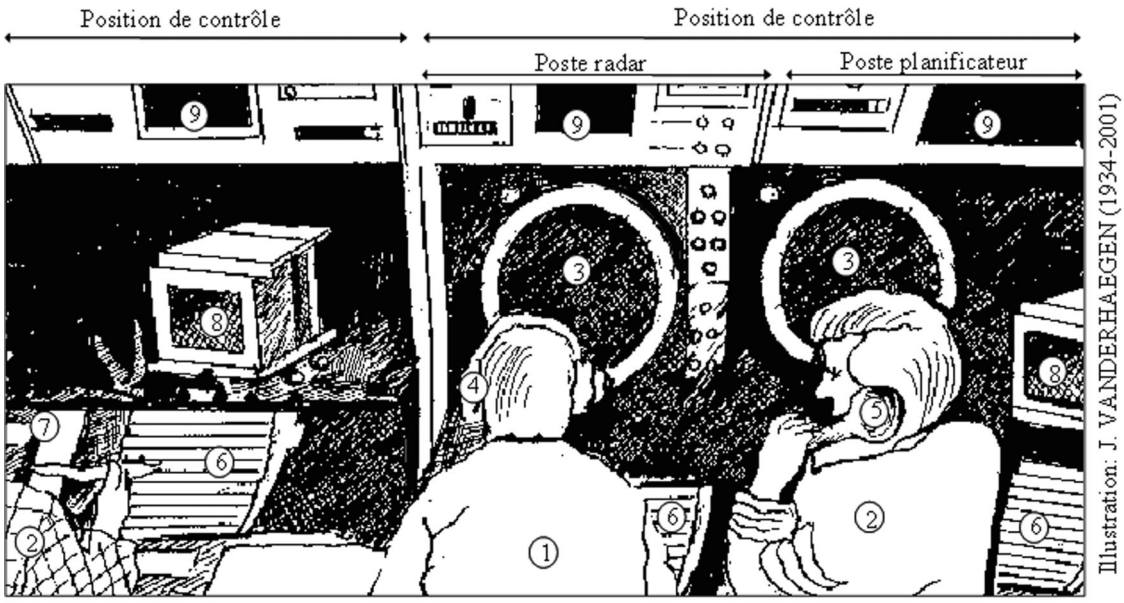
Les exemples d'application présentés ici sont issus de travaux de recherche menés à l'Université de Valenciennes et du Hainaut-Cambrésis.

A. Diagnostic de non-performance en contrôle aérien.

Le diagnostic de non-performance se base sur un estimateur fonctionnel de la complexité de la situation à contrôler. Celle-ci comprend initialement une série d'événements statiques et dynamiques qu'il faut identifier, analyser, contrôler et résoudre le cas échéant. Les événements élémentaires (EE) sont les événements qui ne peuvent pas être décomposés en d'autres événements. Leur analyse permet de les regrouper en trois catégories fonctionnelles d'événements : les événements isolés (EI) qui sont indépendants des autres événements, les événements dépendants (ED) qui peuvent être résolus par une intervention sur au moins un des événements impliqués et les événements globaux (EG) qui ne demandent pas d'intervention directe mais un contrôle continu de leur état. La dépendance entre événements est prédéterminée à partir d'une fonction DEPEND(e', e). De ces catégories d'événements doivent se définir les tâches associées pour le contrôle de la situation correspondante. Enfin, un poids d'exigence de tâche doit être affecté à chacune d'entre elles. Il est prédéfini par la fonction POIDS(TACHE(e)).

```
T ← 0
TantQue ¬Fin
    {Recherche des types d'événement}
    Identifier tous les événements élémentaires EE à traiter à l'instant t
    FinIdentifier
    EI ← {Ø} ; ED ← {Ø} ; EG ← {EE}
    Pour tous les événements e de EE faire
        EED ← {e}
        Pour tous les événements e' ≠ e de EE faire
            Si DEPEND (e,e') alors
                EED ← EED U {e'}
            FinSi
        FinPour
        Si OD = {e} alors
            EI ← EI + OD
        Sinon
            Si EED ⊄ ED alors
                ED ← ED + EED
            FinSi
        FinSi
    FinPour
    {Calcul des exigences des tâches associées}
    EXIG ← 0
    Pour tous les événements e de EI faire
      EXIG ← EXIG + POIDS(TACHE(e))
    FinPour
    Pour tous les sous-ensembles E de ED faire
        EXIG ← EXIG + POIDS(TACHE(E))
    FinPour
    EXIG ← EXIG + POIDS(TACHE(EG))
    t ← t + 1
FinTantQue
```

Cet algorithme a été appliqué pour les tâches du contrôleur radariste du trafic aérien dans une position de contrôle. Celle-ci gère les flux entrant et sortant des avions d'une zone géographique délimitée par des altitudes et des périphéries prédéfinies appelée secteur. Elle nécessite deux types de postes de contrôle. En France, elle est en général composée de plusieurs supports informationnels, ainsi que des liaisons spécifiques de communication externe :



1 - Contrôleur radariste
2 - Contrôleur planificateur
3 - Ecran radar
4 - Radio
5 - Téléphone
6 - Tablette des strips
7 - Imprimante strip
8 – Interface CAUTRA
9 - Chaîne TV pour affichage de données opérationnelles (météo, zone militaire...)

Image 5 : Source : J. Vanderhaegen - 1993

Pour le poste radar, un écran radar permet de visualiser les évolutions en ligne des avions contrôlés, avec la possibilité à partir d'un clavier et d'une boule roulante de configurer les paramètres d'affichage, tels que le nombre de secteurs visualisés, le filtrage des avions affichés. Les communications avec les pilotes sont effectuées à l'aide d'une platine radio. De plus, une tablette sert de support pour le classement des « strips » transférés par le contrôleur organique. Un « strip » est une bande de papier cartonnée sur laquelle est présentée toutes les informations d'un plan de vol d'un avion. Enfin, un autre écran fournit des informations complémentaires générales telles que des données météorologiques, les zones militaires actives interdites au survol.

Quant au poste de contrôle organique, il est constitué non seulement d'écrans similaires (écran radar et écran TV) et d'une tablette pour placer ses strips, mais aussi de deux platines téléphoniques pour communiquer avec les autres positions de contrôle, d'une imprimante pour recevoir les strips et de l'écran tactile du digitatron pour communiquer avec le système CAUTRA (Coordonnateur AUtomatisé du TRafic Aérien) de gestion des plans de vol. En outre, le contrôleur organique agit indirectement sur le procédé puisque toutes les modifications d'un paramètre de vol s'effectuent en collaboration avec les contrôleurs des secteurs adjacents par téléphone et le contrôleur radar de la même position. Toutefois, l'ordre final de changement de cap pour éviter un conflit par exemple, n'est communiqué aux pilotes que par le contrôleur radar.

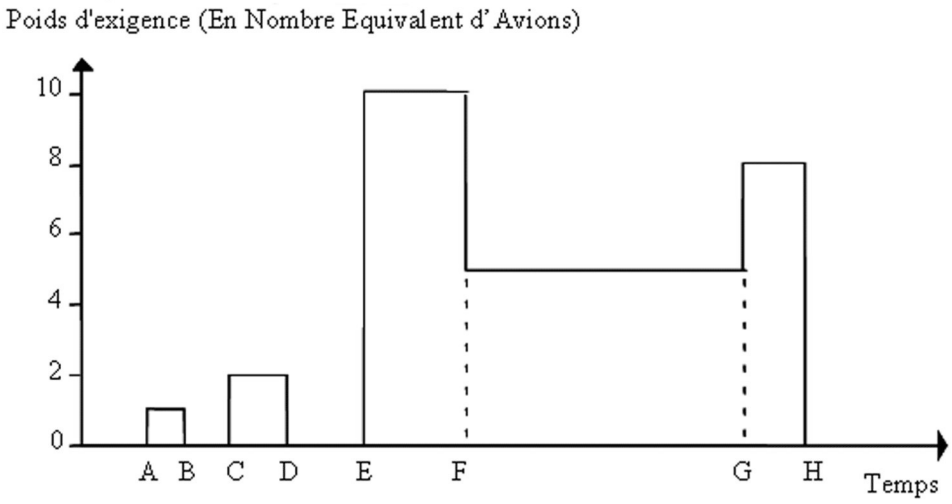
Par conséquent, le contrôleur radariste doit surveiller le trafic, prédire les conflits (deux ou plusieurs avions sont dits en conflit lorsqu'ils risquent de se croiser à une distance inférieure à 8 milles nautiques), et dans ce cas, il ordonne à l'un des pilotes de modifier sa trajectoire.

L'ensemble des événements élémentaires à considérer peut être les avions d'un même secteur géographique de contrôle. Leur analyse permet de les dissocier en événements isolés, i.e. les avions isolés, les événements dépendants, i.e. les conflits entre avions lorsque ceux-ci risquent de transgresser les normes minimales de séparation, et les événements globaux, i.e. la supervision du trafic global :

Type d'événement	Tâche associée	Poids d'exigence affecté
Avion isolé	Nouvel avion à prendre en charge	Nombre d'avions au même niveau + 1
	Avion dérouté à remettre sur sa trajectoire initiale	8
	Avion à mettre à son niveau demandé	8
	Faux conflit à surveiller	2
Conflit entre avions	Conflit à 2 avions à traiter	10
	Conflit à 3 avions à traiter	15
	Conflit résolu à surveiller	5
Trafic général	Recherche des informations (N= nombre d'avions présents sur l'écran radar)	$\frac{1}{45}N^2+\frac{1}{3}N$

Les poids d'exigence fonctionnelle de celui-ci ont été choisis de manière à assimiler le niveau d'exigence impliqué par la surveillance d'un certain nombre d'avions à celui d'un certain nombre de conflits. Ainsi, par exemple, un trafic d'une densité de 15 avions représente un poids d'exigence identique à la détection ou la résolution d'un conflit à deux avions, alors qu'une densité de 30 avions est assimilée aux exigences de 3 conflits. De ce fait, l'unité d'exigence, notée NEA, peut être considérée comme le Nombre Equivalent d'Avions puisque les différentes interférences entre avions se basent sur les exigences d'un avion isolé non problématique pour quantifier la difficulté d'une situation donnée. L'ensemble de ces poids d'exigences a été déterminé empiriquement avec l'aide de contrôleurs professionnels.

L'évolution des exigences pour deux avions conflictuels pour lesquels les niveaux de vol sont stables, sans tenir compte des exigences engendrées par le nombre total d'avions à superviser est la suivante :



A : Arrivée du premier avion

C : Arrivée du second avion

B et D : Prise en charge par le contrôleur

E : Détection d'un conflit entre les deux avions

F : Résolution par le contrôleur

G : Fin du conflit

H : Remise en directe de l'avion dévié qui est dirigé vers sa trajectoire initiale, par le contrôleur

Cet estimateur d'exigence de tâches du contrôle du trafic aérien a été intégré dans une plate-forme expérimentale SPECTRA (Système de Partage Expérimental des tâches de Contrôle du TRafic Aérien). SPECTRA a été conçue pour l'étude de faisabilité d'une répartition dynamique de tâches entre un contrôleur radariste et un système automatisé en collaboration avec le CENA (Centre d'Etude de la Navigation Aérienne).

Cette plate-forme permet de mettre en oeuvre plusieurs types d'environnements :

- un environnement sans aide où le contrôleur humain effectue le contrôle seul, sans aucune assistance,
- deux environnements mettant en oeuvre l'assistance du système automatisé selon deux modes : le mode manuel où la gestion de l'aide est faire par l'opérateur humain et le mode automatique où cette gestion est fate par le système automatisé à partir de l'estimateur d'exigence de tâches présenté ci-dessus.

SPECTRA comprend une vue radar pour l'affichage en ligne de l'évolution des avions dans un secteur aérien donné :

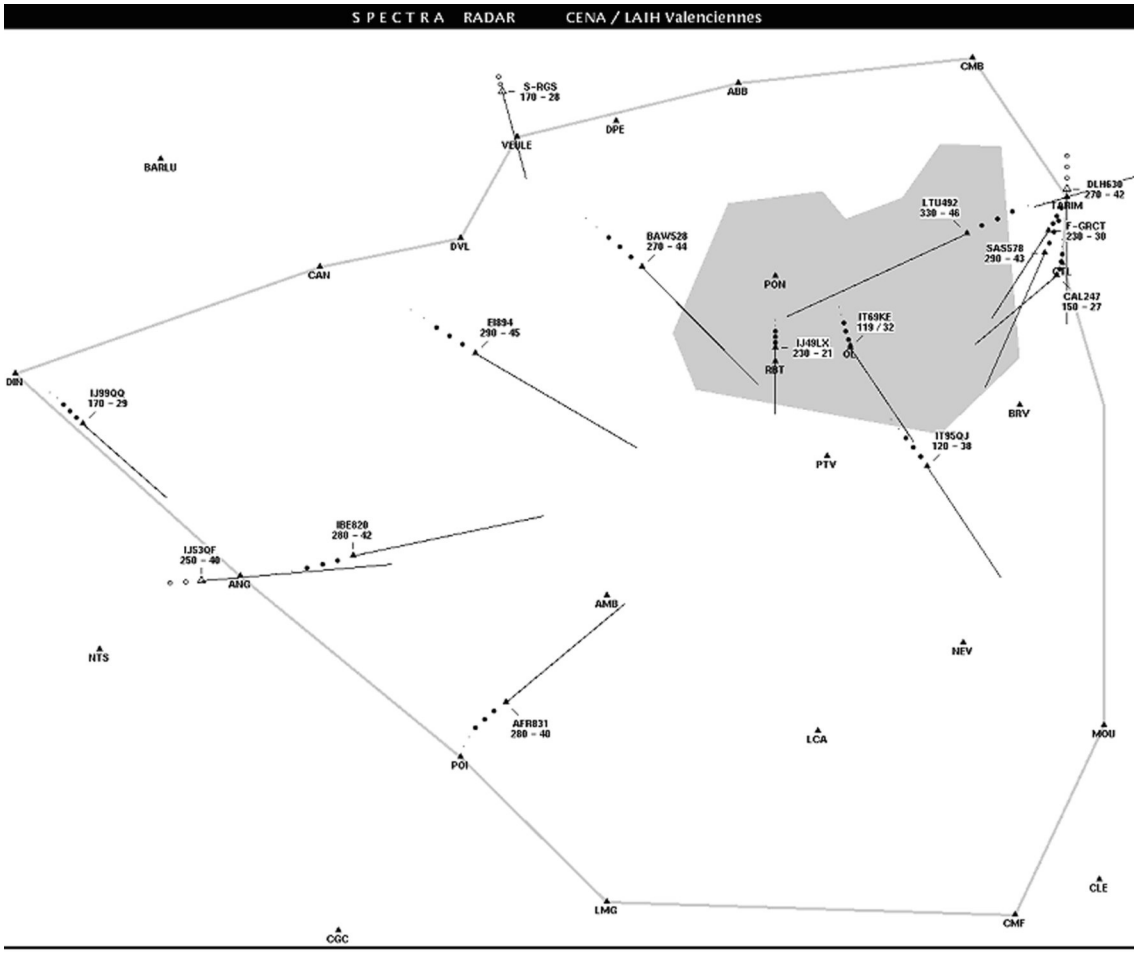


Image 6 : Source : LAMIH

SPECTRA comprend également un stripping électronique contenant les plans de vol des avions à contrôler, les options pour gérer la vue radar, et l'ensemble des données nécessaires à la réalisation des expérimentations :

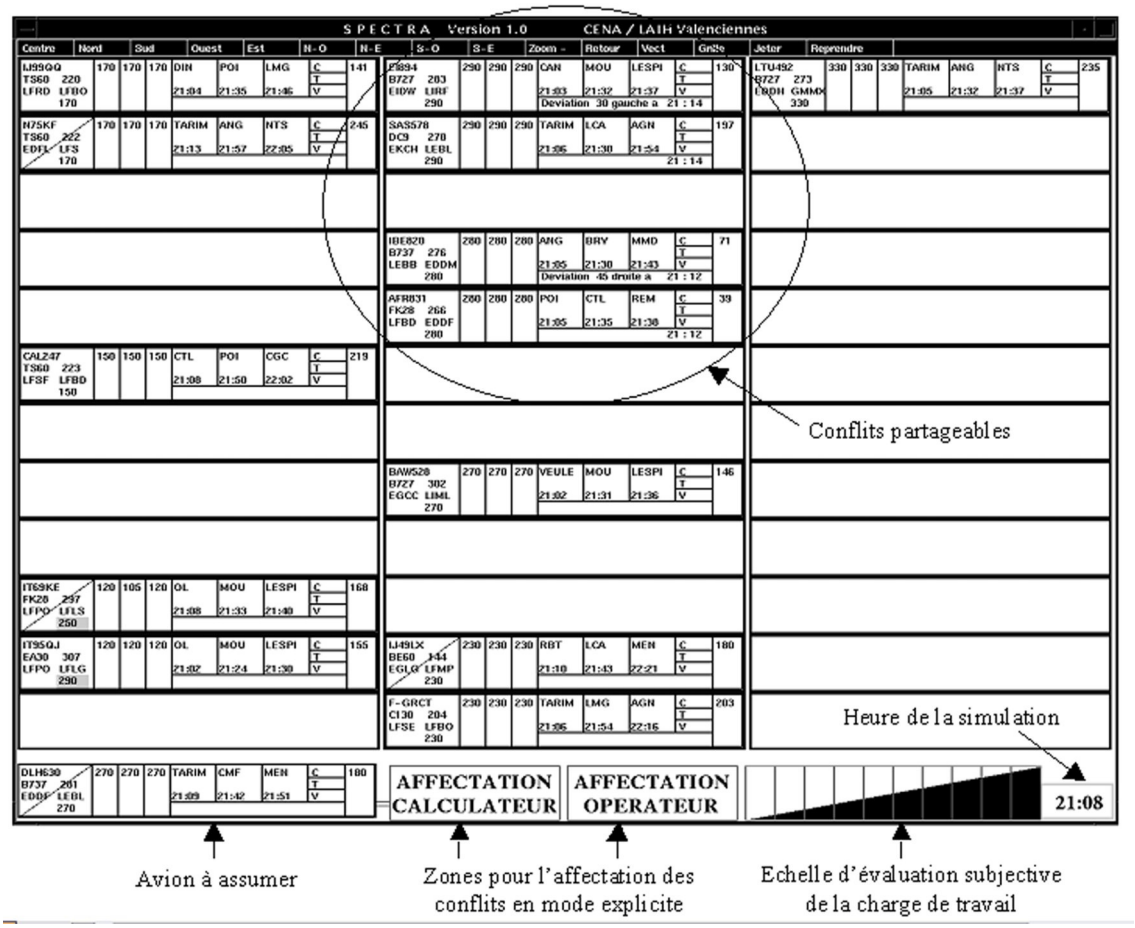
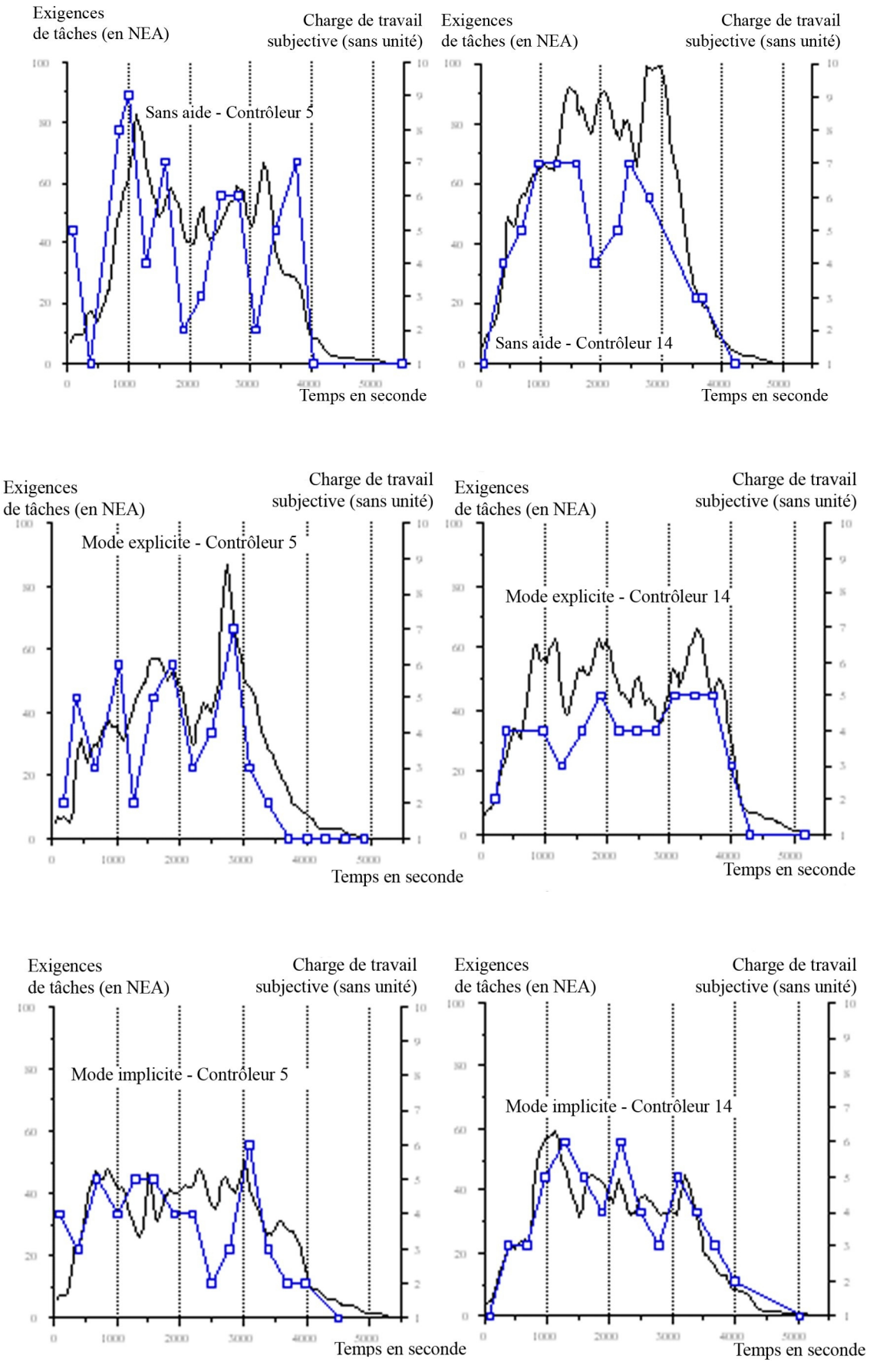


Image 7 : Source : LAMIH

Le système automatisé intégré dans SPECTRA peut détecter tous les conflits mais n'est capable de résoudre et de surveiller que les conflits entre deux avions dans des conditions relativement simples. Ses stratégies de résolution sont alors indiquées sur les plans de vols.

Des expérimentations sans aide et avec aide ont été réalisées au Centre de Contrôle d'Athis-Mons, avec neuf contrôleurs professionnels certifiés et six ingénieurs de la navigation aérienne. L'estimateur d'exigences de tâche a été activé dans chacune d'elles afin d'une part de comparer l'évolution des exigences avec les évaluations subjectives de la charge de travail par le contrôleur aérien à partir d'une échelle graduée, et d'autre part de comparer les résultats pour les différentes expérimentations. Dans la répartition automatisée, un seuil d'exigence au delà duquel le système automatisé décide d'affecter une ou plusieurs tâches au système automatisé a été déterminé à 45 NEA à partir d'expérimentations préalables avec un contrôleur certifié.

Voici un exemple de l'évolution, au cours du temps, d'une part des exigences de tâches, et d'autre part des réponses de deux contrôleurs sur l'échelle d'évaluation de la charge de travail. Dans la majorité des expérimentations, l'évolution de la charge de travail subjective suit assez fidèlement l'évolution des exigences mesurées par le modèle.



Cette corrélation a d'ailleurs été vérifiée par le test statistique non paramétrique de

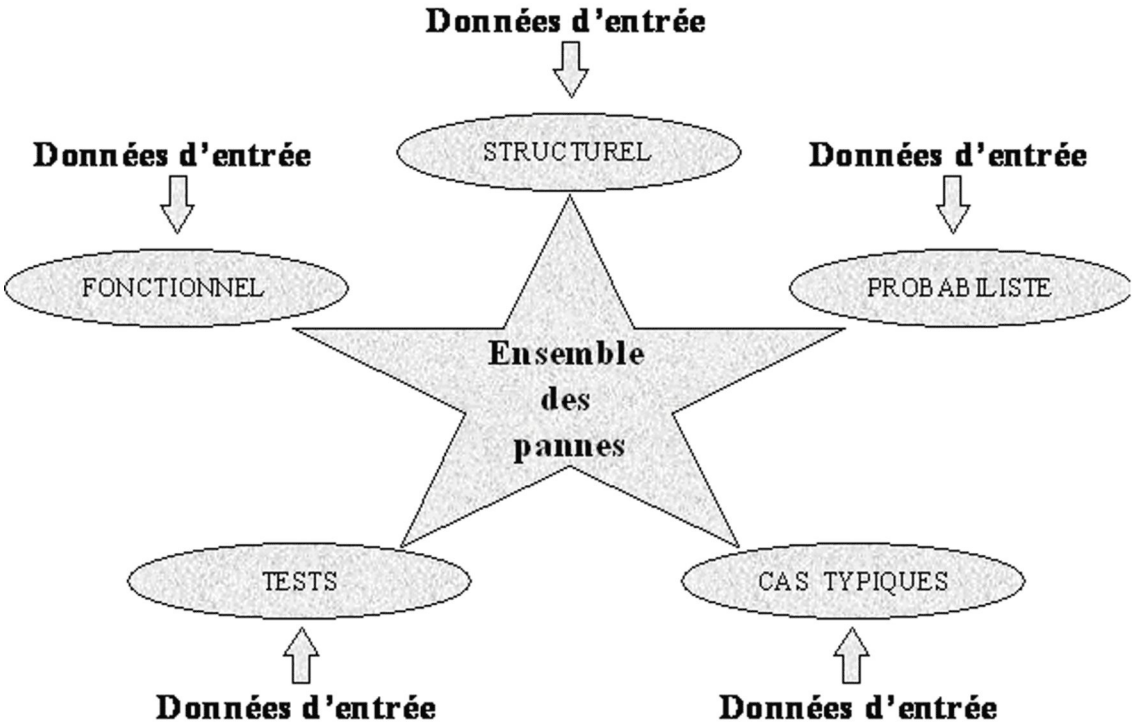
Kendall, qui permet de déceler une dépendance monotone entre deux variables X et Y, i.e. les exigences de tâches et les évaluations subjectives respectivement, au vu des couples (x_i, y_i) où les valeurs de x_i et y_i sont observées aux mêmes dates. Ce test compare alors le sens de l'évolution de valeurs de chaque couple (y_i, y_j) avec celui de chaque couple (x_i, x_j) correspondant. Sur les 45 expérimentations, 44 d'entre elles conduisent, au risque de 0,5%, à rejeter l'hypothèse qu'il n'y a pas de dépendance monotone entre les deux types de mesure. Ce résultat montre sans équivoque que le critère d'exigences de tâche caractérise fidèlement les difficultés réelles du trafic. Le partage des tâches géré par le système automatisé est donc basé sur un indicateur fiable. De plus, le diagnostic d'une surcharge ou d'une sous-charge de travail mentale peut être basé sur un estimateur d'exigences de tâches. Les tâches de diagnostic des contrôleurs aériens sont facilitées lors de l'exploitation des capacités du système automatisé. Cette aide facilite les tâches de détection, de localisation et du traitement d'événements dépendants et indépendants relatifs à la configuration des avions dans le secteur. Lorsque la gestion de l'aide est faite automatiquement, la qualité de la résolution des conflits et la performance humaine sont améliorées :

	Performance humaine pour 270 conflits traités sans aide	Avec aide	
		Performance humaine pour 166 conflits et gestion de l'aide faite par le contrôleur	Performance humaine pour 153 conflits et gestion de l'aide faite automatiquement
Taux de détection des conflits alloués aux contrôleurs	0.89 ± 0.10	0.97 ± 0.08	0.97 ± 0.04
Taux de conflits bien résolus parmi ceux détectés et alloués aux contrôleurs	0.83 ± 0.06	0.88 ± 0.10	0.95 ± 0.07
Taux de performance correcte	0.73 ± 0.14	0.85 ± 0.12	0.93 ± 0.08

B. Diagnostic de dérangements téléphoniques

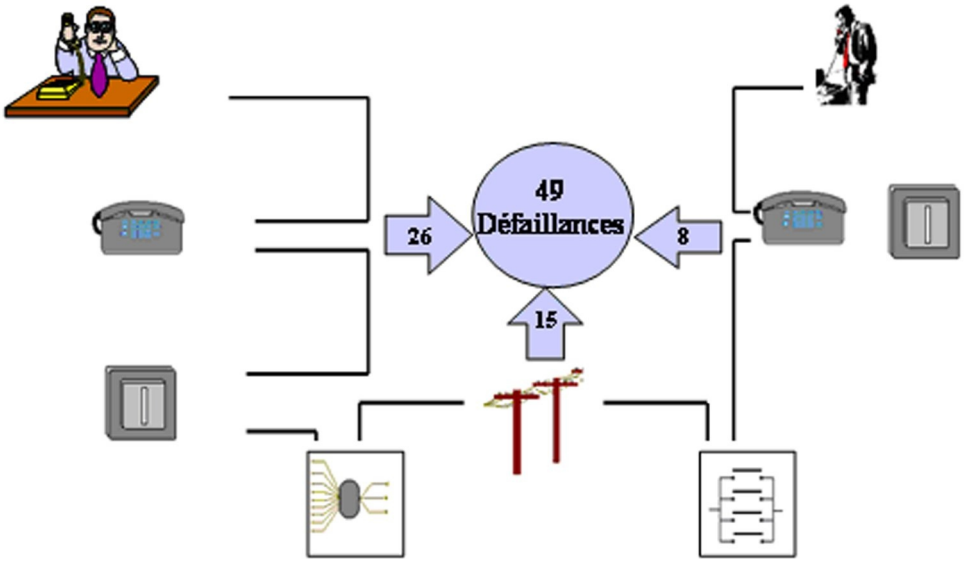
La démarche de diagnostic multi-point de vue a été appliquée dans le cadre des dérangements téléphoniques en collaboration avec le CNET (Centre National des Etudes sur les Télécommunications) et FRANCE TELECOM.

Plusieurs points de vue issus de modes de représentation humaine ont été intégrés: représentation fonctionnelle, représentation structurelle, représentation par analogie, représentation temporelle basée sur la fréquence d'occurrence des événements, représentation heuristique basée sur le principe hypothèses-tests :

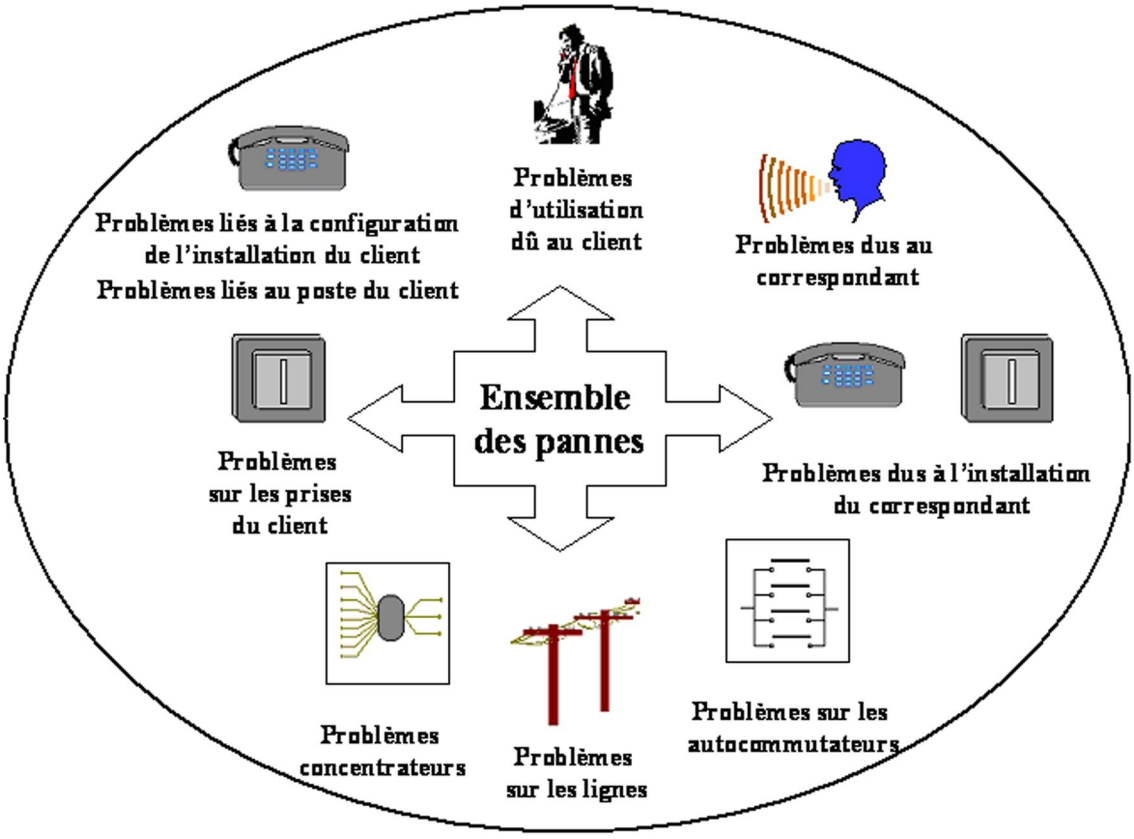


Dans la représentation fonctionnelle, le point de vue intègre les fonctionnalités du procédé et regroupe les fonctions sous trois classes distinctes : les fonctions liées à l'obtention d'un appel, les fonctions liées à la réception d'un appel, et les fonctions liées au transfert d'un appel. Le point de vue sur la représentation structurelle comporte les éléments structurels principaux du procédé, à savoir : l'équipement du client, l'équipement de son correspondant et l'équipement lié au réseau téléphonique. Dans la représentation par analogie ou par similarité, le point de vue est basé sur une liste de scénarios connus pour lesquels l'opérateur humain peut se fier s'il considère que la situation courante à diagnostiquer est similaire avec un des scénarios proposés. Le point de vue basé sur les fréquences d'apparition des défaillances regroupe celles-ci en trois niveaux d'occurrence : élevé, moyen et faible. Enfin, le point de vue basé sur les tests est une liste de tests par défaillances. Il intègre des essais physiques sur les lignes et le réseau téléphoniques.

49 événements élémentaires ont été retenus. Ce sont les défaillances à identifier et les événements combinés sont les symptômes associés à ces défaillances :



Ces défaillances sont décomposées en plusieurs groupes :



Une plate-forme MPV (Multipoint de Vue) a été élaborée pour mener une campagne expérimentale au Centre Principal d'Exploitation de Valenciennes de FRANCE TELECOM :

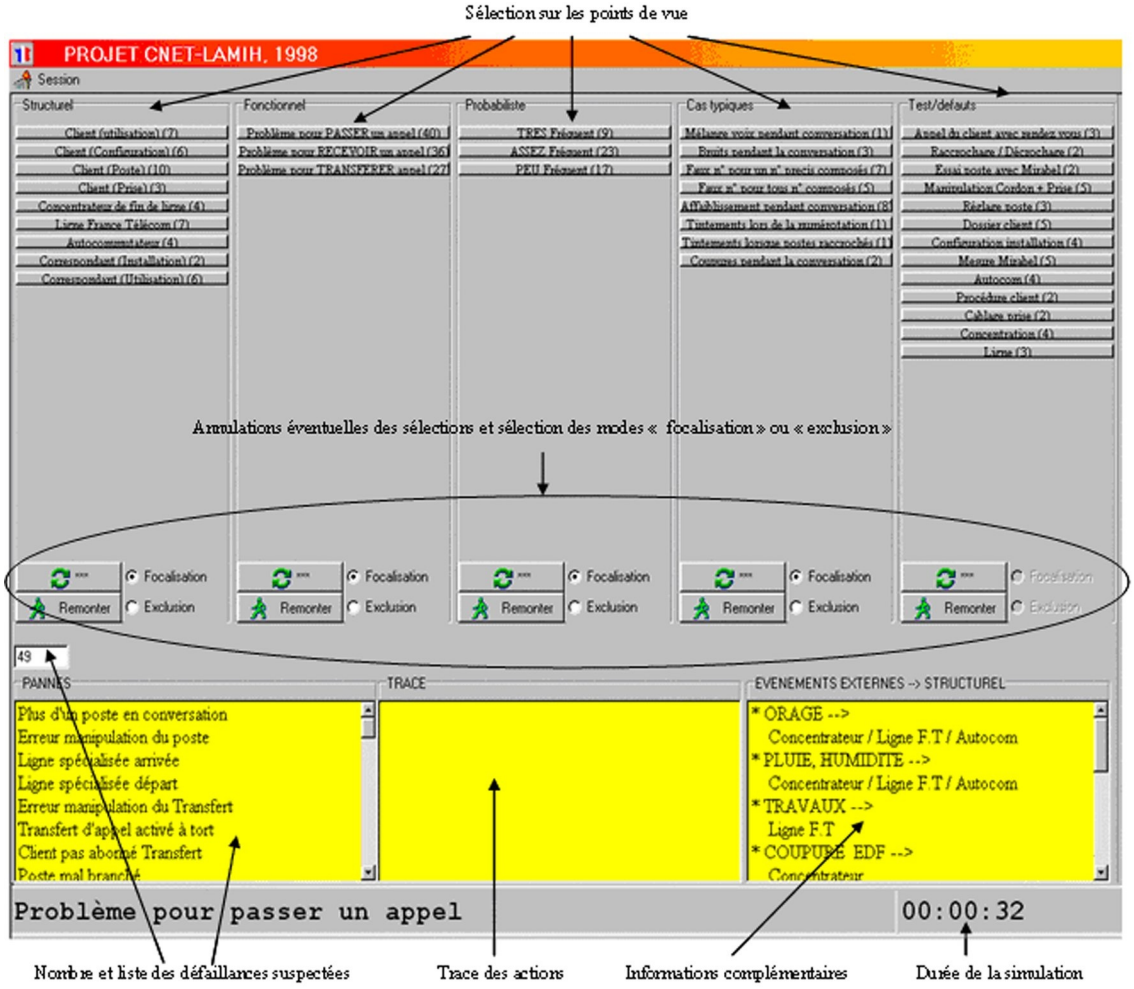
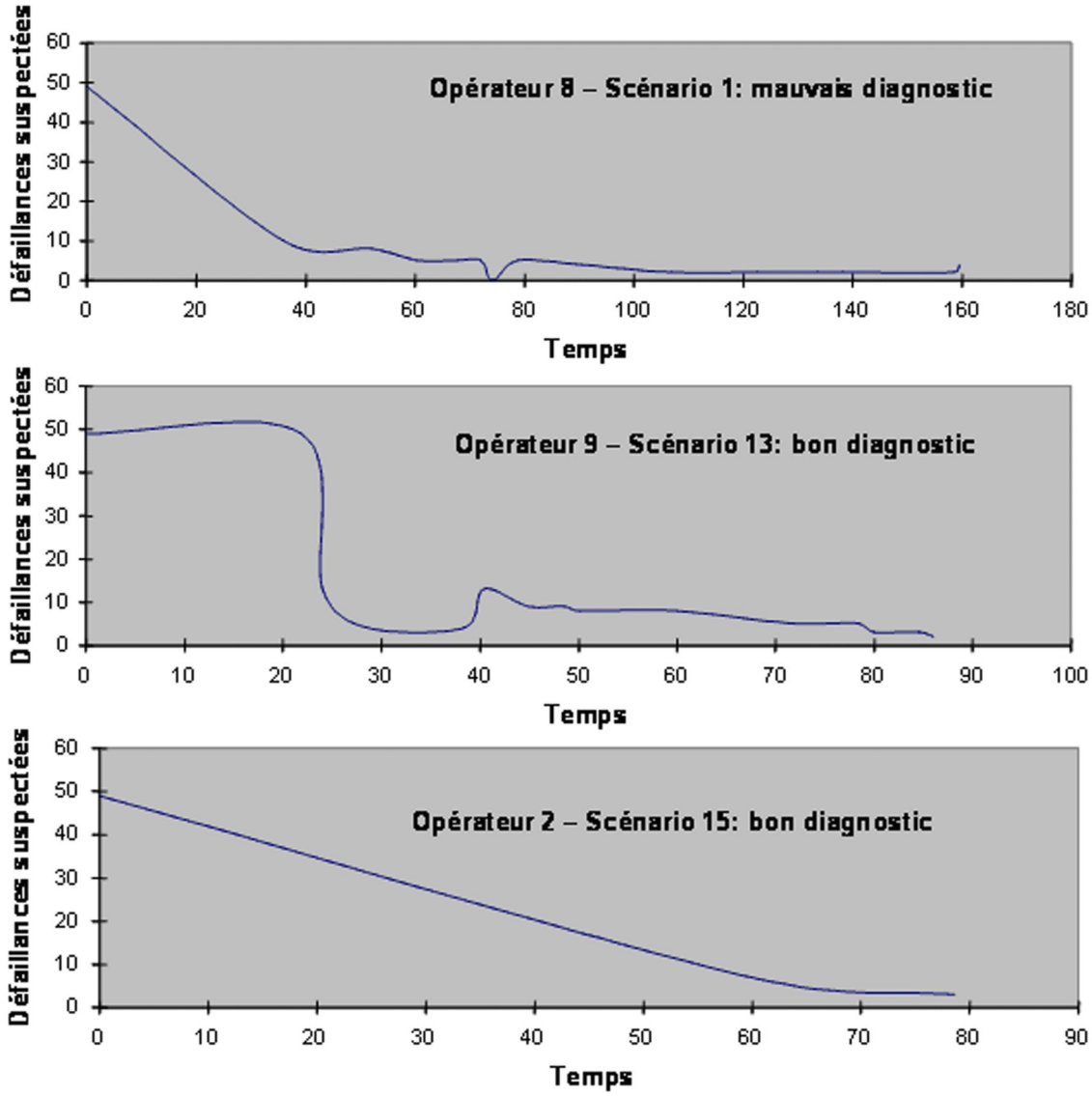


Image 8 : Source : LAMIH. UVHC.

Pour un même diagnostic, différentes stratégies peuvent être envisagées, avec la possibilité de récupérer une erreur de diagnostic ou de vérifier un raisonnement à partir d'un autre point de vue. Au départ, le nombre de défaillance suspectées est de 49, au cours d'un scénario donné, il s'agit de réduire ce nombre afin d'identifier un groupe de 4 défaillances maximum. La simulation s'arrête lorsque l'opérateur humain estime que la défaillance suspecte est dans ce groupe réduit. Le diagnostic peut alors être correcte ou erroné.



Les traces de l'activité des opérateurs ont été sauvegardées : les opérations d'exclusion, de focalisation, les actions sur les points de vue, les récupérations d'erreur ou retour arrière dans le raisonnement, le temps de la simulation.

Temps	Type Action	Libelle	Modele	Nbr pannes
0				49
21,86	Changer de mode	exclusion	F	49
24	Exclure	Problème pour RECEVOIR un appel (0)	F	13
28,62	Exclure	Problème pour PASSER un appel (0)	F	4
38,34	Changer de mode	focalisation	F	4
40,43	Backtrack	Fonctionnel	F	13
44,88	Focaliser	Problème pour PASSER un appel (9)	F	9
48,5	Changer de mode	exclusion	F	9
50,15	Exclure	Ne pas avoir la tonalite (0)	F	8
60,03	Changer de mode	focalisation	F	8
71,51	Focaliser	Pas de signal chez correspondant (5)	F	5
78,32	Changer de mode	exclusion	F	5
79,97	Exclure	Obtention d'un disque (0)	F	3
84,59	Changer de mode	focalisation	F	3
86,01	Focaliser	Aucun signal (2)	F	2

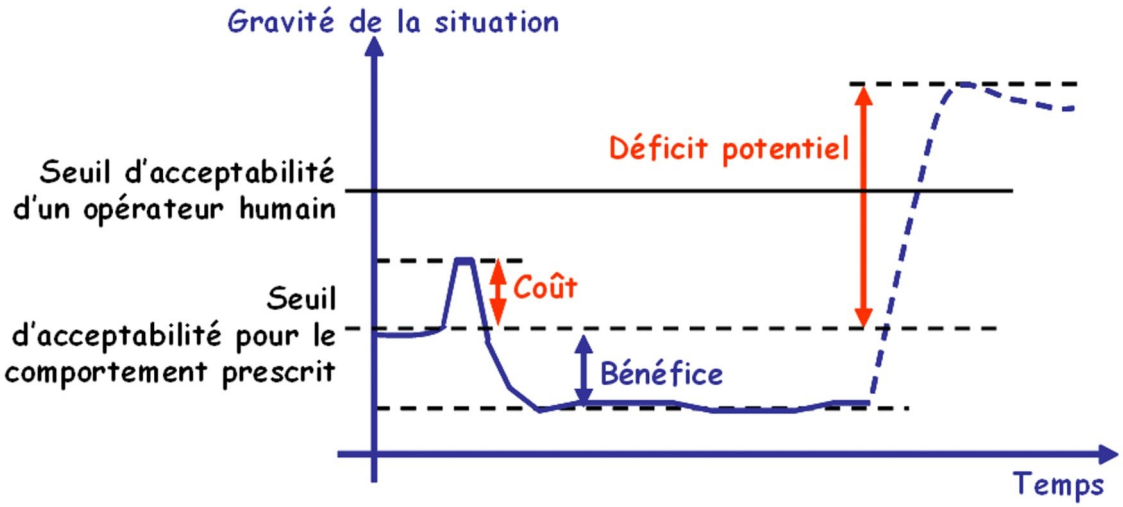
45 scénarios ont été réalisés sans aide et avec la plate-forme MPV. L'analyse des résultats montre que la démarche de diagnostic multi-point de vue facilite la détection d'une erreur de raisonnement ou la vérification d'un raisonnement par retour arrière et exploitation d'un autre point de vue.

	Sans modèle multi-point de vue (pour 45 scénarios)	Avec modèle multi-point de vue (pour 45 scénarios)
Taux de diagnostics correct	0,64 ± 0,03	0,82 ± 0,03
Taux d'absence de correction parmi les diagnostics corrects	0,93 ± 0,05	0,84 ± 0,06
Taux de réussite global	0,60 ± 0,04	0,69 ± 0,07

C. Diagnostic de comportement en contrôle ferroviaire

Cette étude sur les franchissements de barrières et les conséquences associées a fait l'objet d'une collaboration entre l'Université de Technologie de Delft et le LAMIH. Elle a permis de développer une plate-forme TRANSPAL, (TRANSformation de PALettes) pour le diagnostic de comportement particulier : les franchissements de barrières analysés en termes de bénéfices, coûts et déficits potentiels.

L'étude consiste à prendre en considération deux référentiels distincts pour une barrière : le concepteur de la barrière et l'utilisateur du système comprenant cette barrière. L'analyse du franchissement par l'utilisateur de la barrière prescrite par le concepteur se traduit alors par la combinaison de trois éléments :



- Le coût immédiat mais facultatif lors du franchissement. Par rapport au seuil d'acceptabilité du concepteur correspondant au critère de coût, la situation reste tolérable pour le concepteur et l'utilisateur.
- Le bénéfice immédiat issu du franchissement. Par rapport au seuil d'acceptabilité du concepteur correspondant au critère de bénéfice, la situation reste tolérable pour le concepteur et l'utilisateur, et présente un avantage pour l'utilisateur.
- Le déficit potentiel après le franchissement. Par rapport au seuil d'acceptabilité du concepteur pour le critère associé à ce déficit, la situation n'est plus tolérable pour le concepteur et présente un déficit potentiel pour l'utilisateur.

Les deux premiers attributs sont plus facilement évaluables que le troisième qui reste un paramètre flou tant que le déficit associé n'est pas observable.

Des hypothèses peuvent alors être déterminée concernant la probabilité d'occurrence de franchissement d'une barrière à partir des valeurs de ces trois attributs :

Cas	Perception du bénéfice immédiat	Perception du coût immédiat	Perception du déficit potentiel	Probabilité d'occurrence de violation
1	Élevé	Faible	Faible	Élevé ?
2	Élevé	Faible	Élevé	Élevé ?
3	Élevé	Élevé	Faible	Élevé ?
4	Élevé	Élevé	Élevé	Élevé ?
5	Faible	Faible	Faible	Faible ?
6	Faible	Faible	Élevé	Faible ?
7	Faible	Élevé	Faible	Faible ?
8	Faible	Élevé	Élevé	Faible ?

Deux valeurs sont prises en compte pour chaque paramètre (i.e. FAIBLE et ELEVE). Le diagnostic d'occurrence d'un franchissement de barrière est donc le résultat de combinaisons de valeurs des trois paramètres.

Deux études expérimentales avec la plate-forme TRANSPAL ont été menées afin de valider cette hypothèse, d'une part, et d'intégrer dans le diagnostic de comportement une pondération de l'évaluation des bénéfices, coûts et déficits potentiels par un niveau de certitude, d'autre part.

TRANSPAL permet la simulation d'un contrôle de convoyage par aiguillage sur rails de palettes contenant des produits à traiter. La plate-forme TRANSPAL permet de simuler le contrôle des mouvements de palettes d'un dépôt vers un autre dépôt en passant par des zones de transformation du contenu de ces palettes, telles que des zones d'usinage ou d'assemblage. Ces zones possèdent un nombre prédéfini de quais dont certains peuvent accueillir les palettes dans les 2 sens de circulation.

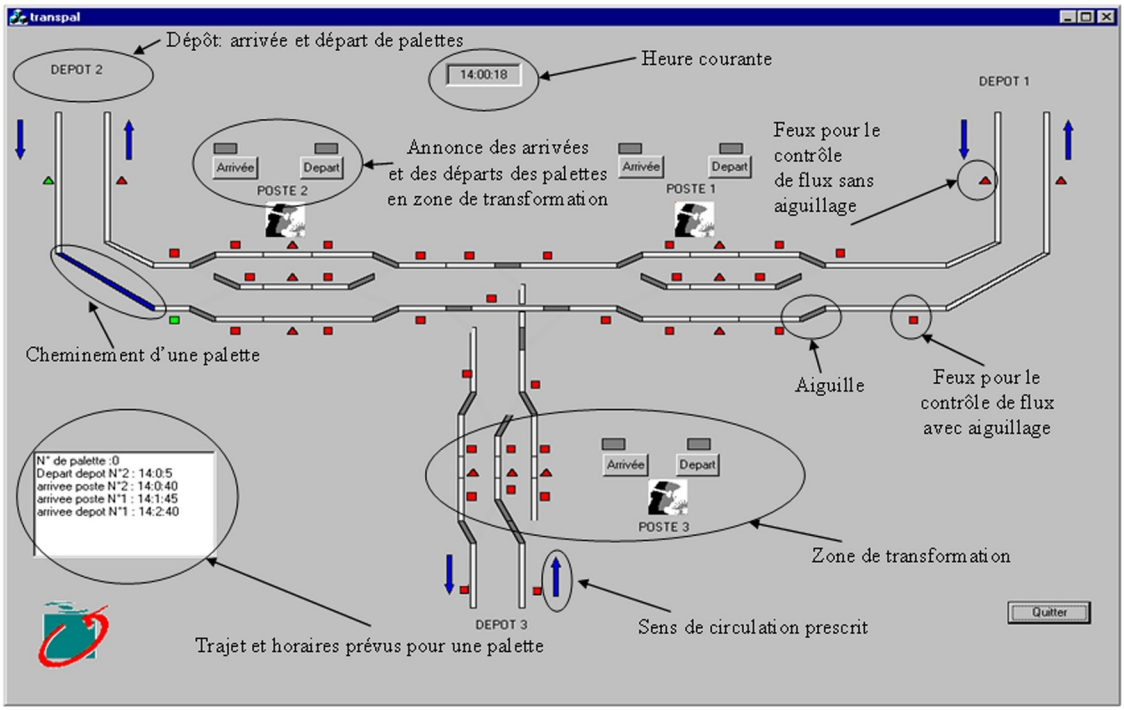


Image 9 : Source : LAMIH. UVHC.

Les opérateurs humains ont alors pour mission de contrôler les mouvements et le traitement des palettes, et de les aiguiller en respectant les trajets et les cadences prévus.

Différents déficits potentiels ont été préalablement identifiés : déraillement de palettes, collision entre palettes, collision entre palettes et opérateurs humains des zones de transformation, retard sur le planning, traitement partiel ou nul des palettes dans les zones de transformation. Ainsi, afin de contrôler les comportements pouvant générer ces déficits, différentes barrières ont été intégrées dans la plate-forme. Les barrières matérielles et fonctionnelles sont les suivantes : feux de signalisation contrôlant l'entrée et la sortie des palettes dans un dépôt, feux de signalisation contrôlant les palettes dans les zones de transformation, feux de signalisation pour synchroniser les annonces de mouvement de palette dans les zones de transformation, les feux de signalisation pour l'arrêt des palettes pour leur traitement dans les zones de transformation, feux de signalisation contrôlant les aiguilles.

Pour chaque protocole expérimental, différentes phases expérimentales ont été retenues pour mettre les sujets en situation de contrôle d'un procédé muni de barrières, avec la possibilité de les franchir : une phase d'entraînement de

familiarisation avec l'interface, le procédé à contrôler et l'ensemble des barrières mises en oeuvre, une phase d'enregistrement de données au cours d'une simulation avec toutes les barrières et une phase d'enregistrement de données au cours d'une seconde simulation avant laquelle le sujet choisit les barrières à maintenir et explique ce choix en termes de bénéfices, coûts et déficits potentiels. Les critères d'évaluation pris en compte sont :

- La sécurité en prenant en compte les collisions face à face ou de rattrapage, les déraillements, les absences et les erreurs de synchronisation des annonces au départ et à l'arrivée des palettes au niveau des zones de transformation.
- La charge de travail en terme d'exigences des tâches.
- La production par rapport au taux de produits traités par palette dans les zones de transformation. Un changement de couleur de la palette pendant un délai constant indique que cette opération de transformation est en cours.
- La qualité relative au respect des horaires prévues.

D'une manière générale, les résultats montrent que le diagnostic de comportement, i.e. de franchissement de barrière peut être expliqué à partir des bénéfices, coûts et déficits potentiels associés. Les résultats avec retraits de barrière montrent que le choix délibéré de opérateurs humains de franchir telle ou telle barrière ne pénalise pas significativement certains critères, comme le niveau de sécurité relatif aux annonces lors des arrêts en zone de transformation.

	TRANSPAL	
	Performance humaine avec retrait de barrières (pour 440 annonces)	Performance humaine sans retrait de barrières (pour 440 annonces)
Taux d'annonces réalisées	0.94 ± 0.06	0.90 ± 0.08
Taux d'annonces correctes parmi celles réalisées	0.85 ± 0.11	0.85 ± 0.11
Taux de performance correcte	0.80 ± 0.10	0.77 ± 0.14

Les franchissements de barrière permettent par contre de réduire le niveau de charge de travail physique. Ce sont donc des violations optimisantes.

Le diagnostic de tels comportements peut également intégrer dans les évaluations subjectives des bénéfices, coûts et déficits perçus par un niveau de certitude subjectif. Le deuxième protocole expérimental a permis d'étudier le diagnostic de franchissement de barrière à partir d'un réseau de neurones (i.e., cartes auto-organisatrices de Kohonen, non développées dans ce cours) permettant de reproduire les décisions des opérateurs humains.

Deux tests comparatifs ont été envisagés :

- Dans le premier, les vecteurs d'entrée de la phase d'apprentissage n'intégraient que les bénéfices, coûts et déficits potentiels perçus pour chaque critère, ainsi que le comportement associé i.e., respect ou franchissement de barrières)
- Dans le second, les vecteurs d'entrées sont complétés avec les valeurs de certitude dans l'évaluation des bénéfices, coûts et déficits potentiels perçus.

L'exploitation des niveaux de certitude a permis de tester une hypothèse de duplication de scénarios comportementaux observés, en suivant la démarche suivante : l'incertitude sur une des évaluations subjectives ne rend pas obsolète l'information mais permet d'inférer sur d'autres combinaisons possibles d'évaluations des bénéfices, coûts ou déficits potentiels pouvant donner l'occurrence d'un même comportement.

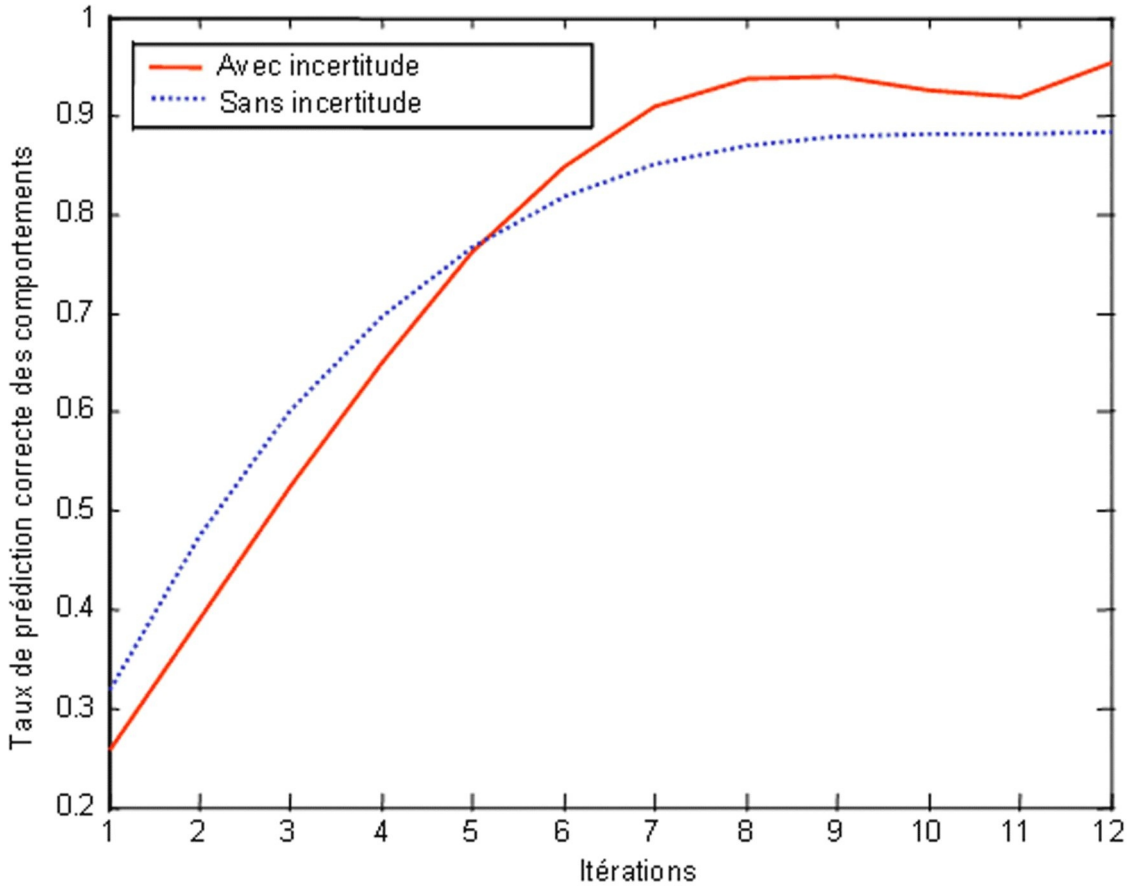
Un exemple simple permet de traduire cette hypothèse. Il donne une évaluation subjective élevée pour le coût alors que le niveau de certitude est bas, contrairement aux autres indicateurs. On peut donc supposer que quelle que soit la valeur du coût et de son niveau de certitude associé le comportement observé sera le même. Il faut noter que la valeur maximale pour le niveau de certitude est associée à la valeur du coût initialement choisie. L'algorithme n'est pas détaillé dans ce cours.

Exemple pour un comportement donné

Bénéfice		Coût		Déficit potentiel	
Valeur (B)	Certitude (α)	Valeur (C)	Certitude (β)	Valeur (D)	Certitude (γ)
Elevé	Elevé	Elevé	Faible	Faible	Elevé

Hypothèse d'occurrence du même comportement pour:
(β= Elevé ou Modéré) ou (C=Faible or Modéré)

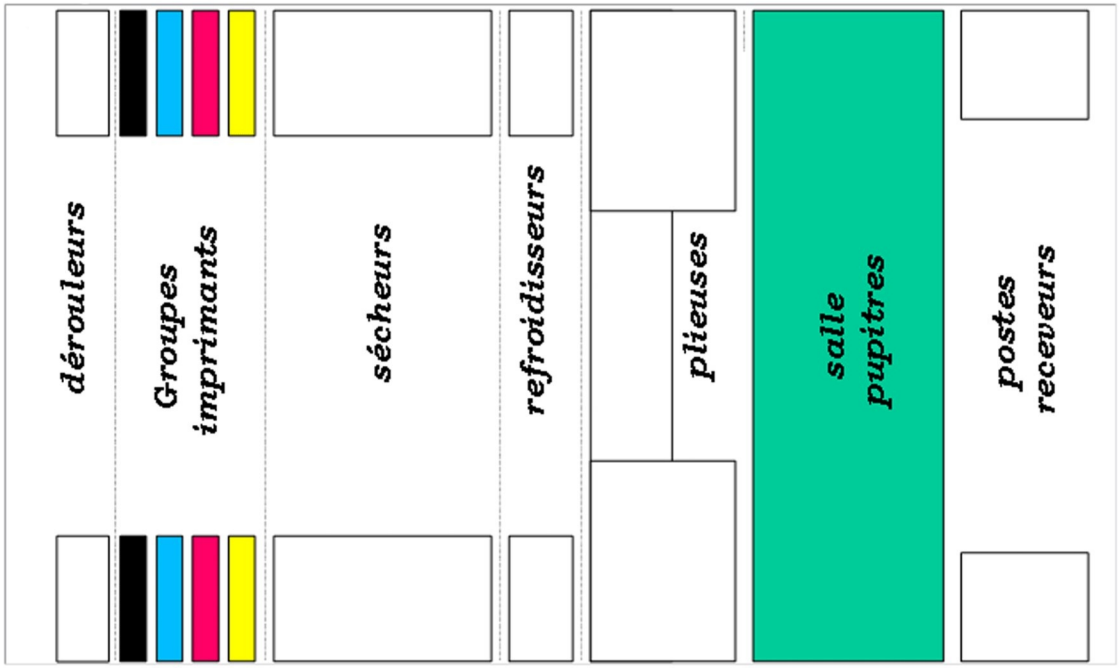
Les résultats par réseau de neurones montre la faisabilité de prédiction de comportements humains à partir des caractéristiques de leur diagnostic (i.e., les bénéfices, les coûts et les déficits potentiels). L'intégration de niveau de certitude sur les évaluations subjectives des coûts, bénéfices et déficits potentiels améliore le taux de prédiction correcte, ce qui valide l'hypothèse précédente :



D. Diagnostic de comportement en production.

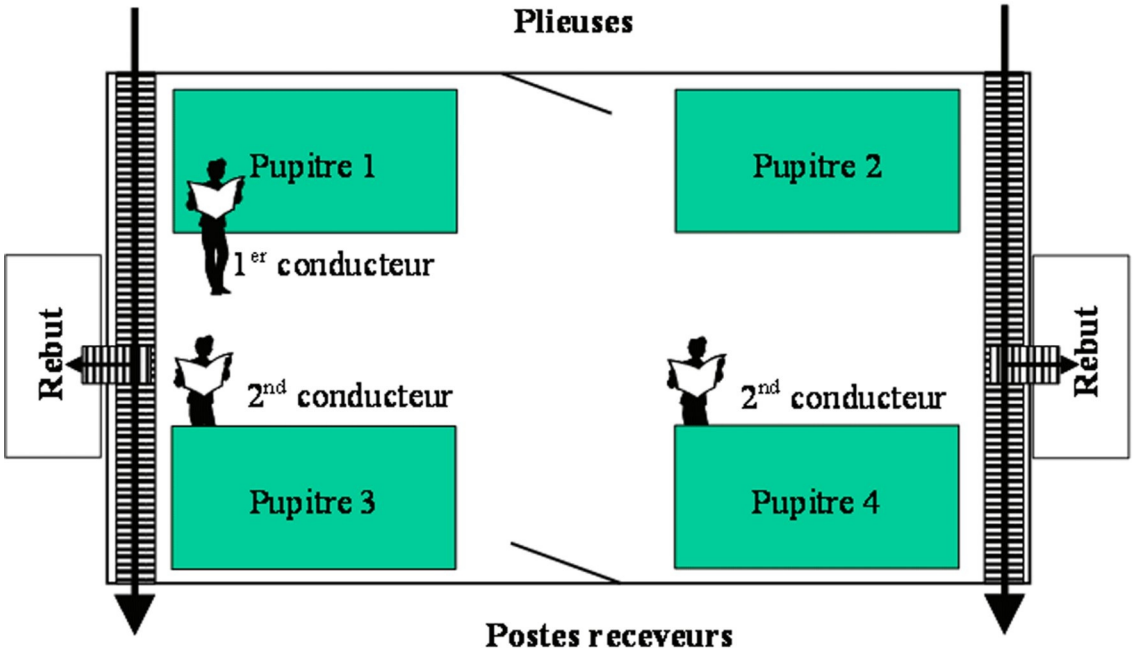
Le diagnostic de comportement en production consiste à analyser des conséquences de comportements observés en termes de bénéfice et de déficit potentiel associé, par rapport aux comportements prescrits du manuel d'exploitation de rotatives industrielles à gros débit. Cette étude s'inscrit dans le programme PROSPER du CNRS et en collaboration avec l'INRS, avec un constructeur de rotatives d'imprimerie et deux utilisateurs de ces rotatives.

D'une manière générale, ce type de machines se décompose en blocs fonctionnels principaux :



En début de chaque ligne un dérouleur permet d'alimenter la ligne en papier. Il est suivi de quatre blocs imprimant (noir, bleu, magenta et jaune) qui assurent l'impression offset. Ensuite, la bande de papier passe dans un sécheur, puis dans un refroidisseur. C'est alors que la bande entre dans la plieuse pour être coupée et pliée selon le type de produit ou cahier. Les cahiers sont alors convoyés dans la salle des pupitres. Si les exemplaires sont acceptables (selon le point de vue des opérateurs), les exemplaires sont convoyés vers le poste receveur, sinon ils sont mis au rebut. Les lignes étudiées permettent d'imprimer des produits de 24 pages et peuvent être assemblées afin de permettre une production de cahiers de 48 pages.

L'effectif minimum est de quatre personnes pour une ligne simple: un premier conducteur, un second conducteur, un bobinier et un receveur. Lorsque les lignes sont doublées, un autre second conducteur est nécessaire :



Le poste de travail du bobinier se trouve en début de lignes. Celui-ci alimente en bobines les dérouleurs. De plus, il veille à ce que l'opération de collage entre bobines s'effectue correctement. Le receveur est en fin de ligne pour alimenter en plaquettes les empileuses, veiller au bon approvisionnement en palettes, contrôler le bon fonctionnement du stacker (système d'empilage automatique), etc. Quant aux conducteurs, leur poste de travail est constitué de plusieurs pupitres de contrôle, à partir desquels ils peuvent paramétrer les lignes.

Quatre phases principales de fabrication d'un produit ont été identifiées :

- La phase de réglage et de préparation d'un nouveau travail. Il s'agit de préparer les bandes de papier nécessaires, de mettre en place les plaques contenant le négatif du motif à imprimer, de contrôler l'état de différents éléments de la rotative (par exemple, contrôle de l'état des blanchets qui permettent l'impression de type offset par mélange entre l'encre et l'eau, contrôle de l'état de la plieuse, etc.), de placer le papier depuis le dérouleur jusqu'à la plieuse, de saisir les caractéristiques du papier, de l'encre, de paramétrer les plis et les découpes du papier, etc.
- La phase de mise aux bonnes. Durant cette phase, les conducteurs effectuent les réglages en ligne en contrôlant les premiers exemplaires d'essai produits à vitesse réduite. Le premier conducteur s'attache au contrôle de la précision du pli et du repérage (i.e., superposition des couleurs). Le second conducteur se charge des niveaux de couleurs, en contrôlant l'ouverture ou la fermeture de 32 visses pour le jet d'encre sur chaque face d'impression et chaque couleur. Quand le premier conducteur juge que la qualité est satisfaisante, les exemplaires sont aiguillés vers le poste receveur. A cet instant, la vitesse est augmentée jusqu'à la vitesse de croisière.
- La phase d'émission du BAT (Bon A Tirer). Durant une courte période après la phase de mise aux bonnes, les seconds conducteurs optimisent l'ajustement des niveaux des couleurs. Leur référentiel jusqu'à présent est un "cromalin", exemplaire sur papier de qualité supérieure qui a été établi par le client. Comme le papier n'est pas de même nature et le procédé d'impression différent, il est impossible d'obtenir un rendu de couleur exactement identique. Quand le second conducteur a obtenu le réglage optimal, selon l'avis du contremaître, un exemplaire est retiré. Cet exemplaire, le BAT, constitue le nouveau référentiel. De plus, il est archivé et accessible par le client en cas de litige.
- La phase de roulage. Durant cette phase, les conducteurs ont principalement une tâche de surveillance. La fréquence de contrôle des exemplaires diminue (1 à 2 exemplaires par quart d'heure). Les contrôles sont souvent déterminés par les changements de bobines de papier au cours desquels un lavage automatique des blanchets et un collage manuel des bandes sont réalisés. Ce lavage et ce collage nécessitent une mise au rebut et peuvent modifier la qualité d'impression. Les niveaux des couleurs ou le repérage par exemple doivent alors être corrigés.

Des observations ont été effectuées sur le terrain chez deux clients exploitant ce type de rotative industrielle à gros débit. Les comportements réels ont pu être identifiés et comparés avec ceux prescrits au travers des manuels d'utilisation ou des règles de sécurité ou d'usage fournis par le concepteur de celle-ci. Pour les comportements ajoutés, le comportement de référence est celui qui existerait sans l'existence du comportement observé, et ce dans les mêmes conditions d'exploitation.

Les comportements observés ont été évalués en terme de bénéfice et de déficit potentiel. L'analyse de ces conséquences s'appuie sur quatre critères de performance :

- La charge de travail est définie comme le nombre d'opérations sur la

machine.

- La sécurité est analysée par rapport aux consignes du concepteur. Celles-ci permettent d'éviter l'exposition des utilisateurs à certains dangers: dangers de chute, d'écrasement, de coupure, dangers liés au bruit, à l'utilisation de produits toxiques, dangers d'incendie, d'électrocution, etc.
- La qualité des exemplaires est définie par rapport au résultat de l'impression et de son suivi. Elle prend en compte le nombre d'exemplaires acceptés (i.e. , mis aux bonnes).
- La production prend en compte le temps de roulage de la machine. Elle est liée au fait qu'un arrêt de celle-ci coûte relativement cher (environ 1550 € par heure).

En prenant en considération qu'un même comportement peut affecter plusieurs de ces critères, 20 comportements détournés, et 4 comportements ajoutés ont été identifiés. Deux contextes ont été retenus : le contexte individuel si un opérateur est concerné, et le contexte collectif lorsqu'un groupe d'opérateur est impliqué. Pour les comportements ajoutés, les bénéfices et déficits potentiels sont identifiés à partir d'une situation avec le même contexte opérationnel mais sans le comportement observés. Pour les comportements détournés, ils sont identifiés à partir des comportements prescrits dans le manuel d'utilisation de l'outil de production. Les bénéfices et déficits potentiels prédominants de l'ensemble des comportements observés ont été reportés ci-dessous :

		Comportements détournés		Comportements ajoutés	
		Contexte individuel	Contexte collectif	Contexte individuel	Contexte collectif
Bénéfice immédiat	Charge de travail	7	3	1	0
	Qualité	2	0	1	0
	Production	4	4	2	0
	Sécurité	0	0	0	0
Déficit potentiel	Charge de travail	0	0	0	0
	Qualité	2	2	1	0
	Production	4	2	2	1
	Sécurité	9	5	0	1

Les comportements détournés sont des violations par rapport à des prescriptions prédéfinies :

Comportement détourné	Explications
1	La procédure de lavage de blanchets observée sur le terrain n'est pas celle prescrite par le concepteur. Elle est plus dangereuse car les opérations se font en rotation continue.
2	Il s'agit des saisies d'exemplaires avant leur contrôle. Lors de la phase de mise aux bonnes, au lieu d'attendre l'arrivée des exemplaires dans la salle des pupitres, les conducteurs sortent et vont les chercher à la sortie de la plieuse pour réduite leur temps de contrôle.
3	Il s'agit d'une cadence de roulage de croisière inférieure à celle prescrite par le concepteur et la hiérarchie. Le chef d'atelier reproche aux conducteurs de rouler trop lentement (environ 10 000 exemplaires par heure en moins). La raison invoquée par les conducteurs est de garantir la qualité.
4	Il s'agit d'un relâchement en phase de roulage diminuant fortement la fréquence de contrôle des exemplaires imprimés. Un suivi tous les 15000 exemplaires est normalement prescrit. Lors d'un problème (cassure de plaque, par exemple), si le suivi n'est pas continu, le diagnostic peut avoir lieu tardivement et cela peut avoir des conséquences graves sur la qualité et la production.
5	Il s'agit d'interventions sur l'outil en marche et à grande vitesse alors que celui-ci doit être arrêté (intervention des conducteurs dans les blocs imprimant pour débloquer des vis d'encrier ou régler les soufflettes d'air ou les filets d'eau ; intervention du receveur dans le stacker pour débourrer).
…	…

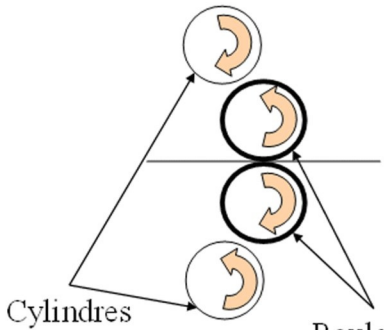
Les comportements ajoutés correspondent à de nouvelles utilisations ou exploitations de l'outil de production sans qu'il existe de référence explicite dans le manuel d'utilisation des machines :

Comportements ajoutés	Explications
21	Il s'agit d'un ajout de procédure pour la mise au rebut au cours d'un changement de bobines. Normalement la mise au rebut et la remise aux bonnes sont automatisées. Afin de garantir la qualité, les opérateurs retirent manuellement quelques exemplaires avant la mise au rebut automatique, puis retardent la remise aux bonnes.
22	Sur les machines d'un autre constructeur, le capteur de présence situé au niveau des blocs imprimant est prévu pour arrêter la machine si une personne est à l'intérieur des blocs. En production, la cassure d'une plaque peut activer ce capteur. Celui-ci devient alors un détecteur de plaque cassée. Le déficit potentiel est en production car ce diagnostic peut ne pas être correct.
23	La communication à distance est une procédure ajoutée qui est appliquée pour accélérer la vitesse de roulage et détecter au plus vite une éventuelle cassure de bande. Une mauvaise interprétation de gestes et l'ajout de cette fonction non prévue par le concepteur peuvent affecter la production.
24	Cette procédure ajoutée concerne le retrait d'un laveur automatique défaillant. Celui-ci est nécessaire pour le nettoyage des blanchets en cours de production. Lorsqu'il est défaillant, après l'avoir retiré afin de faciliter l'accès aux rouleaux, cette fonction peut être réalisée par les opérateurs humains. La sécurité de ces derniers peut alors être affectée.

A titre d'exemple, la dérive n°1 concerne un non respect de procédure lors du lavage de rouleaux (i.., blanchets) à l'arrêt. En effet, avant chaque nouvelle impression, les blanchets doivent être nettoyés suivant la procédure préconisée par le concepteur. La procédure observée montre que le blanchet est lavé et séché alors qu'il est en rotation. Ainsi, la procédure appliquée par les opérateurs permet de gagner 50 secondes en moyenne par lavage. L'intervention sur l'outil en marche et l'absence du port de protections adéquates exposent les opérateurs à plusieurs dangers : écrasement de la main, agression de la peau par le solvant et projection de solvant dans les yeux.

Procédure de nettoyage de rouleaux

Procédure concepteur	Procédure observée
1. Porter les moyens de protection adéquats	1. Appuyer sur le bouton IMPRESSION.
2. Appuyer sur le bouton IMPRESSION.	2. Mettre en rotation continue lente.
3. Enfoncer le bouton d'ARRET D'URGENCE.	3. Nettoyer toute la surface du blanchet avec une éponge et le solvant correspondant.
4. Nettoyer la surface visible avec une éponge et un solvant adapté.	4. Sécher toute la surface du blanchet.
5. Sécher la surface exposée avec un chiffon.	5. Appuyer sur le bouton STOP
6. Tirer le bouton d'ARRET D'URGENCE.	
7. Appuyer sur le bouton MARCHE PAR APPUI MAINTENU.	
8. Répéter les étapes 3 à 7 tant que nécessaire.	



Sources de danger :
- Écrasement de la main
- Agression par le solvant
- Projection de solvant dans les yeux

Protections associées :
- Intervention avec arrêt d 'urgence
- Port de gants caoutchoutés
- Port de lunette de protection

Une fiche diagnostic peut alors être réalisée pour chaque comportement observé, en intégrant les effets à court, moyen et long termes. Par exemple, pour la dérive n °1 qui permet de gagner 50 secondes en moyenne par rouleau, comme il y a 8 rouleaux à nettoyer, la phase de préparation des blanchets est diminuée de 6 minutes et 40 secondes, ce qui peut représenter un gain de 10h par mois voire 121h par an :

Gain en productivité au travers du temps d'opération
➔ Diagnostic en performance: situation admissible

Horizon temporel	ΔT	Public concerné
Lavage d'un blanchet	50s	*Un opérateur*
8h de travail	6min 30s	*L'équipe*
Un mois	10h	*Le chef d'atelier*
Un an	121h	*Direction du site*

Perte en sécurité en termes d'exposition à des sources de danger sans protection
➔ Diagnostic en sécurité: situation à risques

3 sources de danger :
Ecrasement de la main
Agression par le solvant
Projection de solvant dans les yeux

E. Diagnostic de comportement en crash automobile

Il s'agit de diagnostiquer les déficits potentiels en situation de pré-crash. Un scénario reproduisant un crash a été modélisé à partir d'une plate-forme de simulation de conduite automobile :

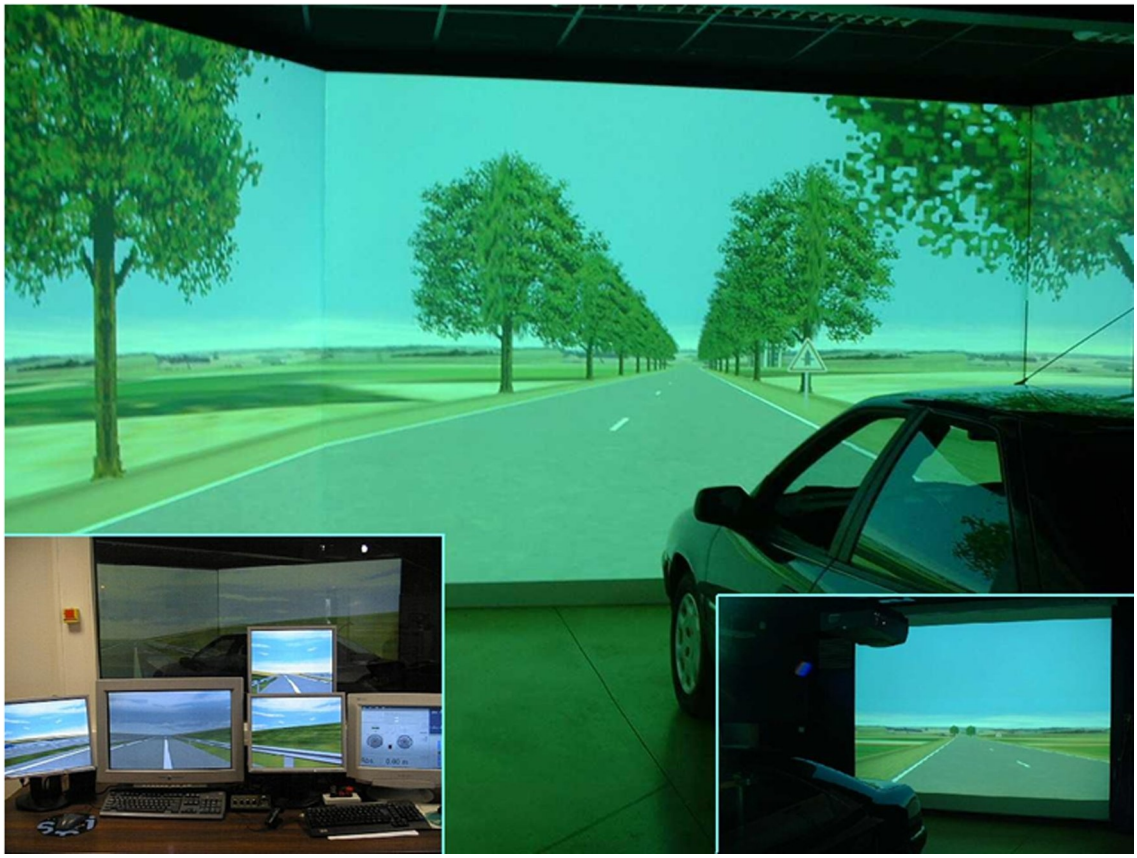
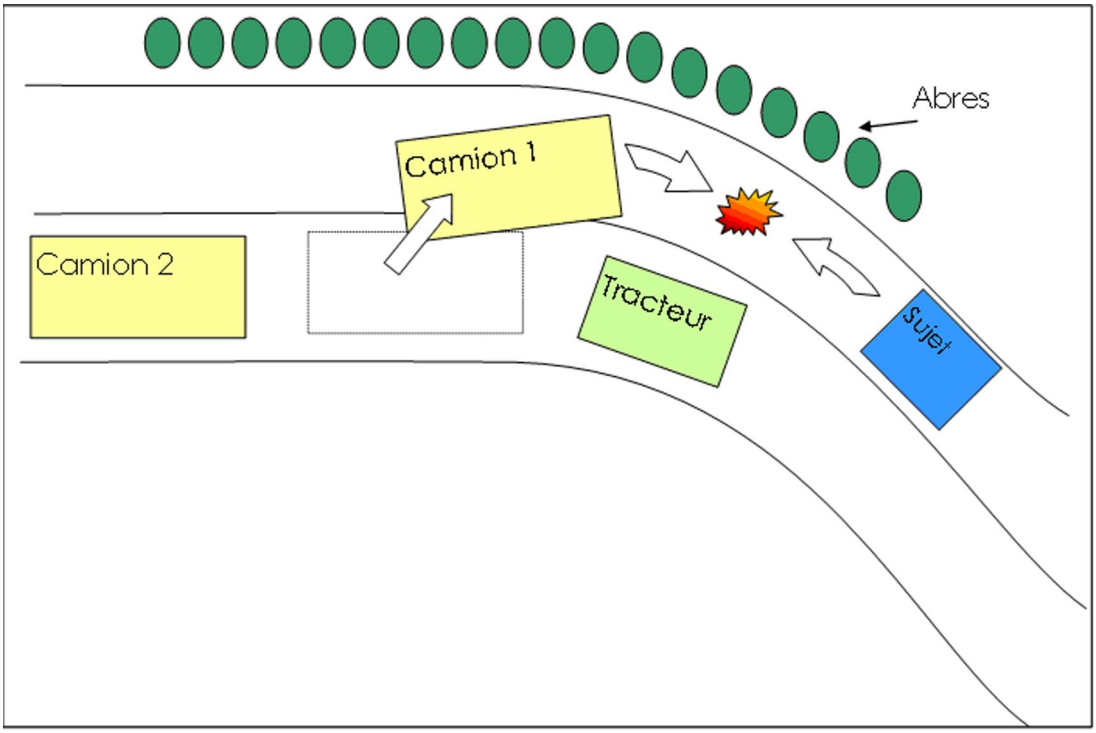


Image 10 : Source : LAMIH. UVHC

Le scénario de crash implique le véhicule sujet qui se trouve face à un camion :



35 sujets ont ainsi été testés. Avant le crash, ils ont conduit pendant 50km avec un trafic normal, sur autoroute, sur route nationale et en agglomération.

Plusieurs mesures anthropométriques et des positions physiques avant le crash ont été faites pour réaliser le mannequin virtuel de chacun des sujets :

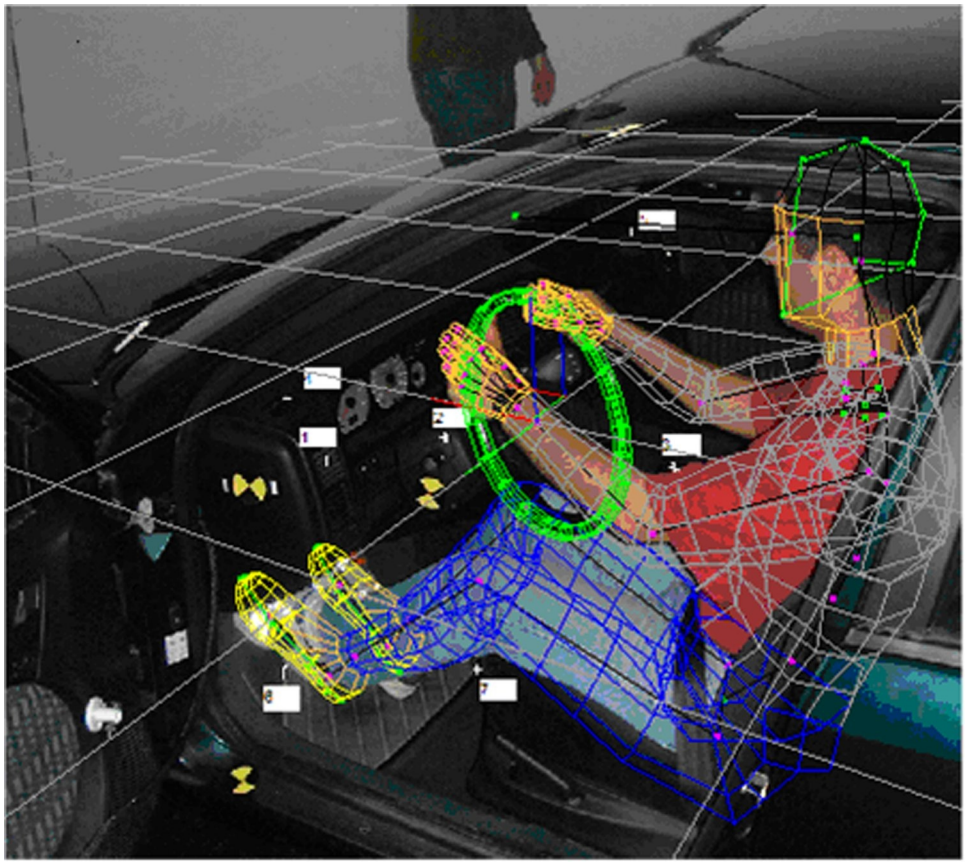


Image 11 : Source : LAMIH. UVHC.

L'intégration a posteriori d'un déclenchement d'airbag au moment du choc a pu être réalisé pour étudier son impact en fonction des caractéristiques statiques et dynamiques des conducteurs.

20 minutes après le début des simulations, les conducteurs adoptent une conduite dite de confort, i.e. la position du corps et des membres reste stable. Avant le crash, différents comportements ont pu être observés :

- 22% des sujets ne changent pas de position face au danger imminent.
- 29% des sujets ont un mouvement de recul sans rotation du tronc
- 38% des sujets ont un mouvement de recul avec rotation du tronc
- 3% des sujets ont un mouvement de rotation du tronc
- 8% des sujets ont un mouvement en avant

78% des sujets ont réagi face au danger. L'exemple qui suit montre que, lors de la détection du danger imminent, le conducteur tente une action d'évitement, ce qui met son bras gauche en position potentiellement dangereuse en cas de déclenchement d'airbag :

Pour la version web de ce cours, ci dessous une vidéo d'un sujet lors d'un crash.

Cette vidéo a une taille de 17Mo.

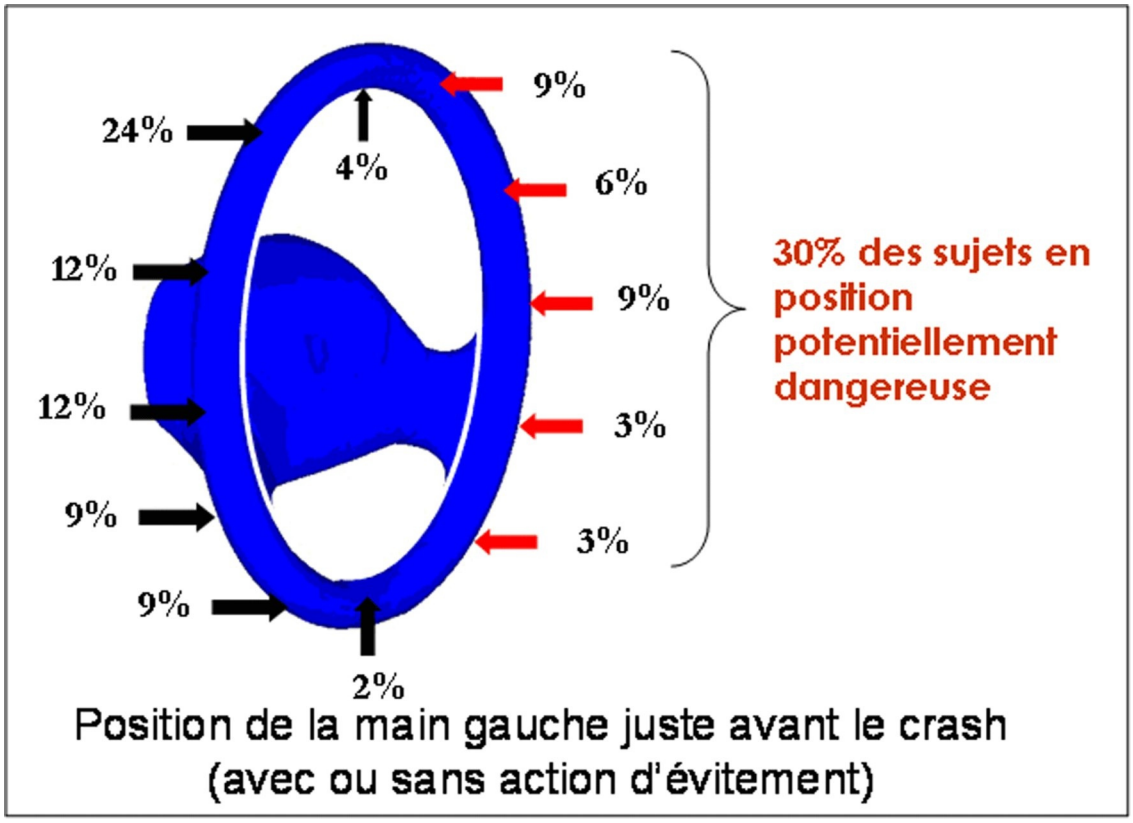
Si vous ne voyez pas cette vidéo vous pouvez la télécharger ci dessous sous format d'archive compressée Zip (taille : 10 Mo) et lire la vidéo avec le lecteur multi-format VLC (Video Lan Client) téléchargeable à l'adresse *http://www.videolan.org/vlc/*[1]. Il est disponible pour de multiples systèmes d'exploitation. Ou vous pouvez aussi la lire avec le lecteur *QuickTime d'apple*[2].

Comme alternative à la vidéo, pour la version du cours en PDF imprimable, voici une image tirée de la vidéo d'un sujet lors d'un crash :

1 - http://www.videolan.org/vlc/
2 - http://www.apple.com/fr/quicktime/download/

Les crash-tests effectués en laboratoire pour étudier l'impact des airbags considèrent les positions des mains au moment de l'impact à 10h10 :

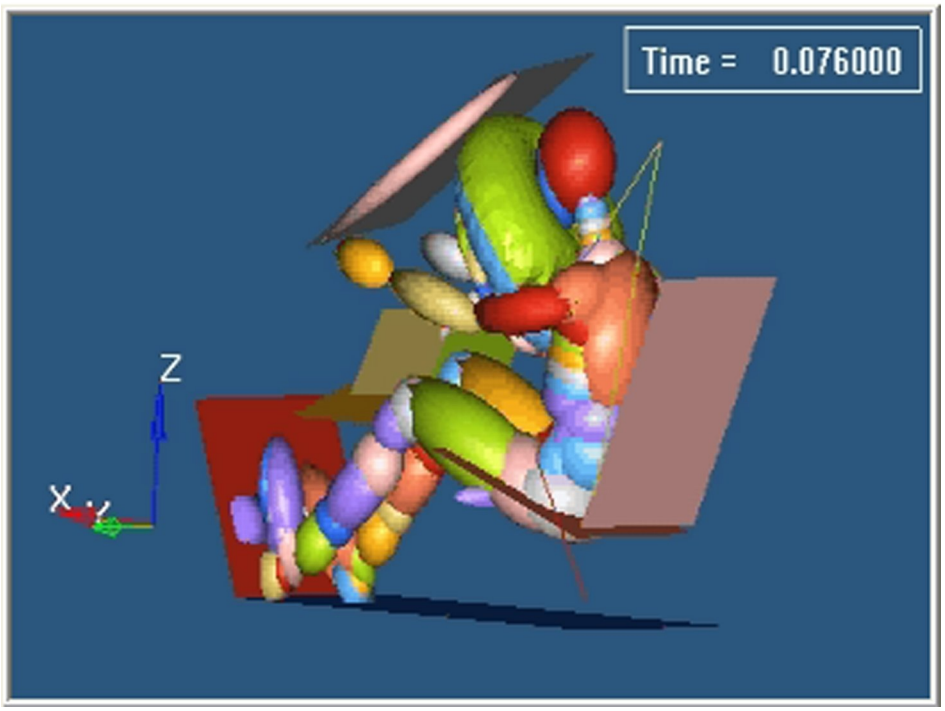
Au moment de l'impact, pour 30% des sujets, la position de la main gauche présente un déficit potentiel supplémentaire par rapport à la position dite normative si l'airbag se déclenche :



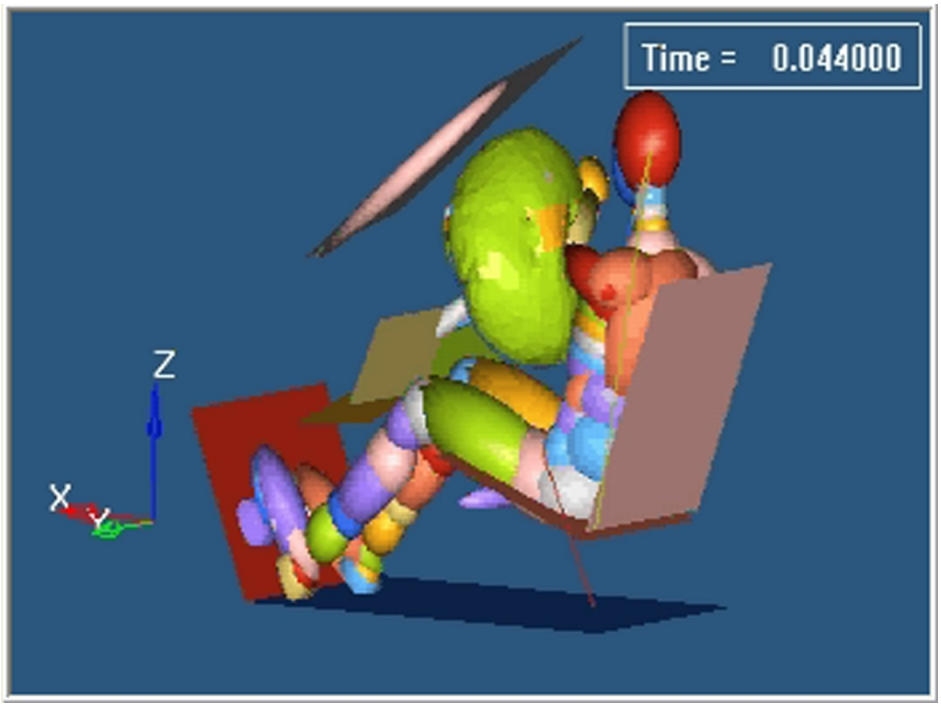
En effet, ces positions atypiques peuvent présenter des chocs dangereux entre les bras et la tête lors du déclenchement. La comparaison de simulations de

déclenchement d'airbag avec la position normative et une position atypique permet d'identifier de tels dangers :

Dans la version web de ce cours, une vidéo de simulation est présente. Comme alternative, pour la version PDF imprimable, voici une image tirée de la vidéo de simulation de déclenchement d'airbag avec la position normative :



Dans la version web de ce cours, une vidéo de simulation est présente. Comme alternative, pour la version PDF imprimable, voici une image tirée de la vidéo de simulation de déclenchement d'airbag avec la position atypique :



Les positions atypiques des bras lors du choc présentent des dangers potentiels

pouvant provoquer des blessures graves voire la mort.

Lien de téléchargement de ces deux vidéos en archives ZIP compressées (1,6 Mo chacune) :

Signification des abréviations

- AMDEC Analyse des Modes de Défaillance, de leurs Effets et de leurs Criticité
- MAC Méthode des Arbres de Causes.Elle est également connue sous les noms de Méthode des Arbres des Défauts ou Méthode des Arbres des Défaillances
- TESEO Tecnica Empirica Stima Errori Operatori
- THERP Technique for Human Error Rate Prediction