Partie 7 : Analyse dysfonctionnelle des systèmes

L'analyse prévisionnelle des dysfonctionnements des systèmes consiste à identifier les conditions qui peuvent conduire à des défaillances et à prévoir leurs conséquences sur la fiabilité, la maintenabilité, la disponibilité et la sécurité des systèmes en cours de conception ou déjà opérationnels.

Elle est réalisée à partir d'informations diverses dont le tri et l'analyse permettent de concevoir un mode le du système. Les informations nécessaires à l'analyse sont :

– la description du système réel : structures physiques et fonctionnelles ;
– les caractéristiques des composants du système et des interactions entre eux (modes de défaillance et leurs conséquences…) ;
– les relations entre le système et son environnement ;
– la prise en compte des erreurs humaines en phase d'exploitation.

7.1/L'AMDE et l'AMDEC

7.1.1/ HISTORIQUE ET DOMAINE D'APPLICATIONS

L'analyse des Modes de Défaillance et de leurs Effets (AMDE) a été employée pour la première fois dans le domaine de l'industrie aéronautique durant les années 1960. Son utilisation s'est depuis largement répandue à d'autres secteurs d'activités telles que l'industrie chimique, pétrolière ou le nucléaire. De fait, elle est essentiellement adaptée à l'étude des défaillances de matériaux et d'équipements et peut s'appliquer aussi bien à des systèmes de technologies différentes (systèmes électriques, mécaniques, hydrauliques...) qu'à des systèmes alliant plusieurs techniques.

7.1.2/ PRINCIPES

L'analyse des Modes de Défaillance et de leurs Effets repose notamment sur les concepts de :
- **Défaillance**, soit la cessation de l'aptitude d'un élément ou d'un système à accomplir une fonction requise,
- **Mode de défaillance**, soit l'effet par lequel une défaillance est observée sur un élément du système,
- **Cause de défaillance**, soit les évènements qui conduisent aux modes de défaillances,
- **Effet d'un mode de défaillance**, soit les conséquences associées à la perte de l'aptitude d'un élément à remplir une fonction requise.

En pratique, il est souvent difficile de bien distinguer ces différentes notions. La maîtrise de ce vocabulaire est néanmoins primordiale pour une bonne utilisation de cet outil. Pour illustrer ces différents concepts, prenons l'exemple d'une pompe. Dans des conditions normales d'exploitation, la fonction de cette pompe est sera définie comme son aptitude à fournir un débit donné à sa sortie. Si le débit en sortie de pompe est nul, nettement inférieur ou supérieur à ce débit défini, la pompe sera dite « défaillante ». Si, en cours d'exploitation, la pompe s'arrête de façon non désirée, on assistera bien à une défaillance de la pompe. Le fait que la pompe s'arrête constitue donc un effet par lequel une défaillance est observée ; il s'agit d'un mode de défaillance. La coupure de courant qui a entraîné l'arrêt de la pompe sera alors définie comme une des causes de ce mode de défaillance. L'arrêt de l'approvisionnement du réacteur alimenté par cette pompe suivie d'une dégradation du

produit de synthèse constituera des conséquences de cette défaillance. L'AMDE est une méthode inductive d'analyse qui permet :
- d'évaluer les effets et la séquence d'évènements provoqués par chaque mode de défaillance des composants d'un système sur les diverses fonctions de ce système,
- Déterminer l'importance de chaque mode de défaillance sur le fonctionnement normal du système et en évaluer l'impact sur la fiabilité, la sécurité du système considéré,
- Hiérarchiser les modes de défaillances connus suivant la facilité que l'on a à les détecter et les traiter.

Lorsqu'il est nécessaire d'évaluer la criticité d'une défaillance (probabilité et gravité), l'Analyse des Modes de Défaillance, de leurs Effets et de leur Criticité (AMDEC) apparaît comme une suite logique à l'AMDE. L'AMDEC reprend en effet les principales étapes de l'AMDE et y ajoute une évaluation semi quantitative de la criticité. Cette dernière peut par exemple être réalisé sur la base des échelles proposées au chapitre 3.1.

7.1.3/ DEROULEMENT

De manière très schématique, une AMDEC se déroule sous la forme suivante : 1) Dans un premier temps, **choisir un élément ou composant** du système 2) **Retenir un état de fonctionnement** (fonctionnement normal, arrêt...) 3) Pour cet élément ou composant et pour cet état, retenir **un premier mode de défaillance**, 4) Identifier les **causes** de ce mode de défaillance ainsi que ces **conséquences** tant au niveau du voisinage du composant que sur tout le système, 5) Examiner les **moyens** permettant de **détecter** le mode de défaillance d'une part, et ceux prévus pour en **prévenir l'occurrence** ou en **limiter les effets**, 6) Procéder à **l'évaluation de la criticité** de ce mode de défaillance en terme de **probabilité et de gravité,** 7) Prévoir des **mesures ou moyens supplémentaires** si l'évaluation du risque en montre la nécessité, 8) Vérifier que le couple (P,G) peut être jugé comme acceptable, 9) Envisager un **nouveau mode de défaillance** et reprendre l'analyse au point 4), 10) Lorsque tous les modes de défaillances ont été examinés, **envisager un nouvel état de fonctionnement** et reprendre l'analyse au point 3) 11) Lorsque tous les états de fonctionnement ont été considérés, choisir **un nouvel élément ou composant** du système et reprendre l'analyse au point 2). Dans les faits, il est intéressant de se doter de tableaux tant en qualité de support pour mener la réflexion que pour la présentation des résultats.

1	2	3	4	5	6	7	8	9	10	11
Equipement Repère	Fonctions, états	Mode de défaillance	Causes de défaillance	Effet local	Effet final	Moyens de détection	Dispositifs de Remplacements	P	G	Remarques

Tableau 3 : Exemple d'un tableau de type AMDEC

A/ ÉQUIPEMENT (COLONNE 1)

Concrètement, il s'agit de passer en revue chaque équipement ou composant identifié lors de la description fonctionnelle. Il est généralement utile de repérer l'équipement considéré à partir des données fournies dans des diagrammes ou autres plans.

B/ FONCTIONS ET ETATS (COLONNE 2)

Pour chacun des équipements, il s'agit de lister ses fonctions et états de fonctionnements. Ces fonctions et états sont normalement identifiés au cours de la description fonctionnelle. Afin de mener l'analyse de la manière la plus complète possible, il est indispensable de

considérer l'ensemble des états susceptibles de survenir au cours de l'exploitation (ex. fonctionnement normal, arrêt, démarrage, stand-by...)

C/ MODES DE DEFAILLANCE (COLONNE 3)

Pour chaque équipement et en fonction de l'état de fonctionnement, le groupe de travail doit envisager de manière systématique les modes de défaillances possibles (Colonne 3). La définition des modes possibles de défaillance pour un équipement peut être réalisée à partir du retour d'expérience associé à l'exploitation d'équipements similaires, de tests ou essais... Par ailleurs, les modes de défaillance considérés devront tenir compte :

- Des utilisations du système,
- Des caractéristiques de l'équipement considéré,
- Du mode de fonctionnement,
- Des spécifications relatives au fonctionnement,
- Des délais fixés,
- De l'environnement.

Quel que soit le type d'équipement considéré, la liste suivante tirée de la norme CEI 60812:1985 : « Techniques d'analyse de la fiabilité des systèmes - Procédure d'analyse des modes de défaillance et de leurs effets (AMDE) » facilite l'identification des modes de défaillance par le groupe de travail.

1	Fonctionnement prématuré
2	Ne fonctionne pas au moment prévu
3	Ne s'arrête pas au moment prévu
4	Défaillance en fonctionnement

Tableau 5 : Modes de défaillance généraux (extrait de la norme CEI 60812:1985)

De plus, cette même norme propose une liste guide de modes de défaillance génériques, qui permet d'aider le groupe de travail dans l'analyse. Cette liste est reprise ci-après. Elle présente une série de modes de défaillance générique pouvant s'appliquer en théorie à tous les cas de figure envisageables. Néanmoins, elle pourra être utilement complétée en vue de tenir compte des spécificités du système étudié.

1	Défaillance structurelle (rupture)	18	Mise en marche erronée
2	Blocage physique ou coincement	19	Ne s'arrête pas
3	Vibrations	20	Ne démarre pas
4	Ne reste pas en position	21	Ne commute pas
5	Ne s'ouvre pas	22	Fonctionnement prématuré
6	Ne se ferme pas	23	Fonctionnement après le délai prévu (retard)
7	Défaillance en position ouverte	24	Entrée erronée (augmentation)
8	Défaillance en position fermée	25	Entrée erronée (diminution)
9	Fuite interne	26	Sortie erronée (augmentation)
10	Fuite externe	27	Sortie erronée (diminution)
11	Dépasse la limite supérieure tolérée	28	Perte de l'entrée
12	Est en dessous de la limite inférieure tolérée	29	Perte de la sortie
13	Fonctionnement intempestif	30	Court-circuit (électrique)
14	Fonctionnement intermittent	31	Circuit ouvert (électrique)
15	Fonctionnement irrégulier	32	Fuite (électrique)
16	Indication erronée	33	Autres conditions de défaillance exceptionnelles suivant les caractéristiques du système, les conditions de fonctionnements et les contraintes opérationnelles
17	Ecoulement réduit		

Tableau 6 : Modes de défaillance génériques (extrait du tableau II de la norme CEI 60812:1985)

D/ CAUSES DE DEFAILLANCE (COLONNE 4)

Pour chaque mode de défaillance, le groupe de travail doit ensuite identifier les causes potentielles conduisant à ce mode de défaillance. Un mode de défaillance peut résulter de plusieurs causes, qu'il convient donc d'inventorier et de numéroter pour plus de facilité. La liste présentée dans le Tableau 8 précédent permet également de préciser des causes de défaillance dans la mesure où ces causes peuvent parfois s'apparenter à des modes de défaillance. Par exemple, un mode de défaillance d'une vanne devant se fermer peut être « Ne se ferme pas » (mode de défaillance n°6). Une des causes de ce mode de défaillance peut être un blocage physique ou coincement (mode de défaillance n°2). Enfin, il convient de tenir compte des défaillances possibles sur les équipements adjacents du système. L'évaluation des effets d'une défaillance d'un élément peut effectivement conduire à l'occurrence d'un mode de défaillance sur un autre élément du système. Il est ainsi nécessaire de veiller à l'adéquation entre les effets de défaillance considérés au cours de l'analyse et les causes d'autres modes de défaillance envisagés.

E/ EFFETS DE LA DEFAILLANCE (COLONNES 5 ET 6)

De la même façon que le groupe de travail s'est attaché à identifier les causes potentielles de défaillance, il doit examiner les conséquences de cette défaillance, au niveau du composant lui-même tout d'abord (colonne 5) puis au niveau du système global (colonne 6).

F/ MOYENS DE DETECTION (COLONNE 7)

Pour le mode de défaillance envisagé, le groupe de travail examine et consigne ensuite les moyens prévus pour détecter ce mode de défaillance.

I/ DISPOSITIFS DE REMPLACEMENT (COLONNE 8)

Toutes les dispositions prises, par exemple au niveau de la conception de l'installation, en vue de prévenir ou atténuer l'effet du mode de défaillance doivent alors être examinées. Cette étape, dont les résultats sont consignés en colonne 8, vise d'une certaine façon à caractériser le comportement du système lorsqu'un de ces composants est affecté par un mode de défaillance.

J/ EVALUATION DE LA CRITICITE (COLONNES 9 ET 10)

Les colonnes 9 et 10 permettent de consigner les évaluations réalisées par le groupe de travail de la probabilité du mode de défaillance (P) et de la gravité associée à ses conséquences (G). Cette approche permet de mesurer l'influence des barrières de sécurité mises en place et de juger de la pertinence d'envisager de nouvelles barrières au regard du risque présenté. En pratique, il est parfois difficile de disposer de données précises et fiables pour procéder de manière fine à cette évaluation. On pourra alors se référer utilement à des échelles de cotations à plusieurs niveaux de probabilité et de gravité, semblable à celles présentées au paragraphe 3.3.3.1. Rappelons que les échelles de gravité et probabilité quels que soient les formats finalement retenus, doivent être présentés et acceptées en début d'analyse.

7.1.4 / LIMITES ET AVANTAGES

L'AMDEC s'avère très efficace lorsqu'elle est mise en œuvre pour l'analyse de défaillances simples d'éléments conduisant à la défaillance globale du système. De par son caractère systématique et sa maille d'étude généralement fine, elle constitue un outil précieux pour l'identification de défaillances potentielles et les moyens d'en limiter les effets ou d'en prévenir l'occurrence. Comme elle consiste à examiner chaque mode de défaillance, ses causes et ses effets pour les différents états de fonctionnement du système, l'AMDEC permet d'identifier les modes communs de défaillances pouvant affecter le système étudié. Les modes communs de défaillances correspondent à des événements qui de par leur nature ou la dépendance de certains composants provoquent simultanément des états de panne sur plusieurs composants du système. Les pertes d'utilités ou des agressions externes majeures constituent généralement des modes communs de défaillance. Dans le cas de systèmes particulièrement complexes comptant un grand nombre de composants, l'AMDEC peut être très difficile à mener et particulièrement fastidieuse compte tenu du volume important d'informations à traiter. Cette difficulté est décuplée lorsque le système considéré comporte de nombreux états de fonctionnement. Par ailleurs, l'AMDEC considère des défaillances simples et peut être utilement complété, selon les besoins de l'analyse, par des méthodes dédiées à l'étude de défaillances multiples comme l'analyse par arbre des défaillances par exemple.

7.2 / Analyse Préliminaire de Risques (APR)

7.2.1 / Notion de danger et de risque

• **DANGER :** état ou situation comportant une potentialité de dommage pour l'homme, la société, l'environnement.
Situation d'un système où sont présents des facteurs pouvant conduire à la réalisation d'un accident potentiel.

• **RISQUE :** Mesure du niveau de danger (associé à une phase précise de la vie d'un système) caractérisant un accident potentiel (événement redouté).
Cette mesure s'exprime par :

- sa probabilité d'occurrence (ou sa fréquence),
- sa gravité (importance de sa conséquence, dommage).

7.2.2 / Notion d'accident

• **ACCIDENT :** Événement causant des dommages corporels ou matériels.
Rupture de l'équilibre dans une situation donnée.

Il est le résultat d'au moins un des cinq éléments suivants :

- méconnaissances des sources de danger,
- inobservation ou inadéquation des règles,
- dysfonctionnements techniques (panne, rupture…),
- dysfonctionnements humains opératoires,
- concours de circonstances qui fait survenir un ou plusieurs éléments (1 à 4 ci-dessus) ou combinaison d'événements.

7.2.3 / Notion de sécurité

• **SECURITE :** Aptitude d'un système à éviter de faire apparaître, dans des conditions données, des événements critiques ou catastrophiques.

Ensemble des situations destinées à assurer la protection des personnes et des biens contre les dangers, nuisances et gênes résultant de la création, du fonctionnement (du dysfonctionnement), de l'arrêt et du démantèlement d'un dispositif technique ou d'une installation.

La sécurité :

- s'applique à un système en mettant l'accent sur les problèmes d'interaction,
- intègre les facteurs humains,
- envisage toutes les circonstances pouvant conduire à une situation dangereuse,
- s'attache à des combinaisons d'événements qui échappent à l'expérience.

7.2.4 / Méthodologie générale de recherche et d'analyse des risques

Cette méthodologie comporte 4 étapes :

1. Définir le sujet de l'étude (recherche du besoin fondamental),
2. Définir l'objet sur lequel porte l'étude (par les méthodes fonctionnelles),
3. Analyser les dangers et les risques (par les méthodes fonctionnelles et qualitatives utilisées en Sûreté de Fonctionnement),
4. Tirer les conclusions de l'étude selon le sujet défini.

7.2.5 / Définir le besoin fondamental de l'étude

Répondre à 3 questions et valider le besoin :

1 : pour qui ?
une autorité de sûreté, la hiérarchie, un groupe de travail, …

2 : sur quoi ?
une organisation, un système, un sous-système, une procédure, un essai, …

3 : dans quel but ? Pourquoi cette action ?
identifier les risques, informer le demandeur, améliorer la sécurité du personnel, reconcevoir un système, valider une procédure…

Réaliser une APR/APD, c'est :
• Rechercher les dangers d'un système,
• Analyser les milieux extérieurs,
• Analyser les phases de mission et d'utilisation,
• Estimer le niveau des dangers (mesure du risque) en les classant par hiérarchisation,
• Réduire leur probabilité (prévention) et réduire leur gravité (protection).

Remarque : si l'étude le nécessite, faire appel aux méthodes classiques de SdF pour rechercher les événements indésirables, leurs causes, leurs effets, leurs probabilités.

7.2.6 / Établir un tableau de criticité

Il est souhaitable que ce découpage soit en nombre pair pour éviter l'attirance du jugement pour la valeur médiane d'un découpage en 3 ou 5.

Niveau	Gravité G	Probabilité P
1	Blessures légères	Improbables
2	Blessures graves	Très rare
3	Blessures très graves	Rare
4	Mort	Probable

Tableau 7 : Tableau de criticité

Éléments dangereux	Événement causant une situation dangereuse	Situation dangereuse	Événement causant un accident potentiel	Accident potentiel	Conséquences	Risque P	G	R	Mesures préventives
Bouteille d'azote	Choc sur la bouteille	Chute de la bouteille	Rupture du col sur obstacle	Déplacement brutal de la bouteille	Chocs sur trajectoire	1 à 4	1 à 4		fixer la bouteille réserver un espace libre
Énerge électrique	Ouverture d'une armoire électrique	Manipulation d'organes de commande	Contact accidentel avec pièces sous tension	électrocution	Atteintes corporelles + ou - graves	2 à 4	2 à 8		Placer des écrans isolants Former et informer
Eau de javel	Avoir accès à la bouteille	Prendre la bouteille	Ouvrir la bouteille	Ingérer l'eau de javel	Atteintes corporelles + ou - graves	2 à 4	2 à 8		Limiter les accès

Tableau 8 : Exemple de tableau d'APR

Exemple de carte de risques

Principe (organigramme)

7.3 / Hazards and Operability Study (HAZOP)

7.3.1 / Description de l'étude HAZOP

Une étude HAZOP (*Hazards and Operability Study*), exécutée par une équipe, est un processus détaillé d'identification des dangers et des problèmes d'exploitation. L'étude HAZOP s'attache à l'identification des déviations potentielles par rapport à l'intention de conception, à l'examen de leurs probabilités d'occurrence et des causes possibles et à l'évaluation de leurs conséquences.

7.3.2 / Objectifs et caractéristiques de l'étude HAZOP

Les principales caractéristiques d'une étude HAZOP sont entre autres :

- L'étude est un processus créatif. Elle consiste à utiliser une série de mots guides pour identifier des déviations potentielles par rapport à l'intention de conception et à employer ces déviations comme « déclencheurs » stimulant l'imagination des membres de l'équipe dans la recherche des causes de la déviation et dans l'évaluation des conséquences qu'elles peuvent engendrer.
- L'étude se déroule sous la direction d'un chef d'étude qualifié et expérimenté. Celui-ci s'assure de mener un examen exhaustif du système en s'appuyant sur une pensée logique et analytique. De préférence, le chef d'étude est assisté par un scribe qui note les dangers et/ou les perturbations identifiés en vue de leur évaluation et de la recherche de solutions.
- La qualité de l'étude repose sur les qualifications et l'expérience des spécialistes formant l'équipe. Ces spécialistes de diverses disciplines doivent faire preuve d'intuition et de perspicacité.
- Il convient d'effectuer l'examen dans un climat de pensée positive et de franche discussion. Lorsqu'un phénomène est identifié, il est noté pour être ultérieurement évalué et résolu.
- Les solutions aux problèmes ne constituent pas le principal objectif de l'étude HAZOP, mais elles peuvent, le cas échéant, être notées et transmises aux responsables de la conception.

TITRE DE L'ÉTUDE : Chemin de fer « Ligne courte » MI-0 – MI-11.2									FEUILLE : 1 de 2				
N° du dessin : Carte A			N° de révision : 3						DATE : 2002-09-01				
COMPOSITION DE L'ÉQUIPE :			LA, RJ, JPL						DATE DE LA REUNION : 2002-08-16				
PARTIE CONSIDÉRÉE :			Convoi de 60 wagons tirés par 2 locomotives. Fréquence de circulation 4 / jour.										
					Avant mise en place des propositions d'amélioration				Après mise en place des propositions d'amélioration				
N°	Scénarios Et-si?	Causes	Conséquences	Barrières de sécurité	Gravité	Probabilité	Risques	Propositions d'amélioration	Gravité	Probabilité	Risques	Commentaires	Resp./date cible
1	Déraillement de plusieurs wagons train direction est, déraillement à l'ouest du pont rt 1	1.1 Défaillance du matériel roulant	1.1.1 Décès, blessures des conducteurs de train	1.1.1. Système d'inspection au défilé (Roll by)	4	3	Inacceptable	1.1.1 Améliorer le programme de maintenance préventive, le garder en place et à jour.	4	2	Tolérable avec atténuation	Appliquer la recommandation .	LA 2/12/31
			1.1.2 Décès, blessures de personnes circulant sur la route 1.	1.1.2. Inspection des wagons au triage				1.1.1 Augmenter la fréquence des inspections				Faire une étude pour déterminer la fréquence optimale	RJ 3/02/28
			1.1.3 Dommages aux équipements roulants	1.1.3. Essai de freins				1.1.3. S'assurer que des inspections rigoureuses soient faites selon l'échéancier et que les dossiers soient maintenus à jour				Appliquer la recommandation	LA Immédiat
			1.1.4 Dommages aux structures du pont	1.1.4. Système de maintenance préventive des wagons et des locomotives								Faire audit des mesures d'atténuation en place	BC 3/09/01
			1.1.5 Arrêt des opérations minières et du concentrateur suite à l'impossibilité de transporter le minerai										
			1.1.6 Chômage technique										

Tableau 9 - Exemple d'analyse « Et-si? »/Liste de contrôle - Transport de minerai par rail (exemple non complet)

Matrice de risques Chemin de fer Ligne Courte

PROBABILITÉ	GRAVITÉ			
	Négligeable - 1 -	Faible - 2 -	Critique - 3-	Catastrophique - 4-
Fréquent - 5-	Tolérable avec atténuation	Inacceptable	Inacceptable	Inacceptable
Probable - 4 -	Tolérable avec atténuation	Tolérable avec atténuation	Inacceptable	Inacceptable
Occasionnel - 3 -	Tolérable	Tolérable avec atténuation	Tolérable avec atténuation	Inacceptable
Rare - 2 -	Tolérable	Tolérable avec atténuation	Tolérable avec atténuation	Tolérable avec atténuation
Improbable - 1 -	Tolérable	Tolérable avec atténuation	Tolérable avec atténuation	Tolérable avec atténuation

CATÉGORIES DE GRAVITÉ	
Catastrophique :	Décès ou invalidité permanente; Important dommage matériel; ou Perte pour l'ensemble du réseau.
Critique :	Invalidité partielle permanente; Invalidité totale temporaire de plus de trois mois; Important dommage matériel; ou Important dommage au réseau.
Faible :	Blessure mineure; Maladie professionnelle mineure; Accident entraînant une absence; Dommage matériel mineur; ou Dommage mineur pour le réseau.
Négligeable :	Premiers soins ou traitements médicaux mineurs; ou Perturbation mineure du réseau.

CATÉGORIES DE PROBABILITÉ	
Fréquent :	Susceptible de survenir fréquemment (élément individuel); Survient continuellement (parc de matériel roulant).
Probable :	Susceptible de se produire plusieurs fois au cours de la vie utile d'une unité; Susceptible de se produire fréquemment pour l'ensemble du matériel
Occasionnel :	Susceptible de se produire à l'occasion durant la vie utile d'une unité; Susceptible de se produire plusieurs fois pour l'ensemble du matériel.
Rare :	Peu probable, mais peut survenir durant la vie utile d'une unité; Peu probable, mais on peut s'attendre à le voir survenir pour l'ensemble du matériel roulant.
Improbable :	Dont la probabilité est si faible qu'on peut supposer que l'incident ne se produira pas; Ne risque guère de survenir, mais peu le faire.

Tableau 10 - Exemple de matrice de décision – Transport de minerai par rail

7.3.3 / Applications des études HAZOP

À l'origine, l'étude HAZOP était une technique développée pour les systèmes impliquant le traitement d'un milieu fluide ou autres flux de matière dans les industries de transformation, notamment l'industrie des procédés chimiques et pétroliers. Cependant, son domaine d'application n'a cessé de s'étendre au cours des dernières années, et la technique HAZOP s'applique aujourd'hui, par exemple :

- aux applications logicielles, y compris les systèmes électroniques programmables;
- aux systèmes assurant le déplacement des personnes par différents modes, tels que le transport routier et le transport ferroviaire;
- à l'examen de différentes séquences de fabrication et aux procédures d'exploitation;
- à l'évaluation des procédures administratives dans différentes industries;
- à l'évaluation de systèmes spécifiques, tels que les appareils médicaux.

L'étude HAZOP est particulièrement utile dans l'identification des faiblesses des systèmes nécessitant la circulation de matières, de personnes ou de données, nécessitant un certain nombre d'événements ou d'activités d'une séquence planifiée ou des procédures contrôlant cette séquence. L'étude HAZOP n'est pas seulement un outil précieux pour la conception et le développement de nouveaux systèmes. Elle peut être utilisée avec profit pour l'examen des dangers et des problèmes potentiels liés à différents états de l'exploitation d'un système donné (démarrage, attente, fonctionnement normal, arrêt normal, arrêt d'urgence, etc.). Elle peut également être employée dans le processus et les séquences de fabrication par lot et en régime instable, ainsi que dans les séquences continues. L'étude HAZOP peut être considérée comme une partie intégrante du processus global de bonne ingénierie et de la gestion du risque.

A / Relation avec d'autres outils d'analyse

L'étude HAZOP peut être utilisée en combinaison avec d'autres méthodes d'analyse de la sûreté de fonctionnement, telles que l'analyse des modes de défaillance, de leurs effets et criticité (AMDEC) et l'analyse par arbre de panne (AAP). De telles combinaisons peuvent être utilisées dans les situations exposées ci-dessous :

- L'étude HAZOP indique clairement que les qualités de fonctionnement d'une entité spécifique de l'équipement sont critiques et doivent être examinées en profondeur. Dans ce cas, il est avantageux de compléter l'étude HAZOP par une AMDEC de cette même entité.
- À la suite de l'étude HAZOP des déviations par élément ou par caractéristique, il est possible d'analyser l'effet de déviations multiples ou de quantifier l'éventualité des défaillances en utilisant une AAP.

L'étude HAZOP est une approche centrée essentiellement sur le système, contrairement à l'AMDEC qui est centrée sur la composante. En effet, l'AMDEC part d'une défaillance possible d'une composante, pour étudier ensuite les conséquences de cette défaillance sur l'ensemble du système. L'étude est donc uniquement dans le sens cause à effet. Ce concept diffère de celui d'une étude HAZOP qui commence par identifier les déviations possibles par rapport à l'intention de conception et, à partir de là, procède dans deux directions, l'une pour chercher les causes possibles de la déviation et l'autre pour en déduire les conséquences.

B / Limites de l'étude HAZOP

Bien que les études HAZOP aient fait preuve d'une extrême utilité dans différents milieux, la technique a des limites dont il faut tenir compte dans le choix de son application :

- L'étude HAZOP est une technique d'identification des dangers qui examine méthodiquement les effets des déviations sur chaque partie. Parfois, un danger provient d'une interaction entre un certain nombre de parties du système. Ceci impose une étude plus détaillée du danger, faisant appel à des techniques telles que l'analyse par arbre d'événements ou l'analyse par arbre de panne.
- Comme pour toute technique d'identification de dangers ou de problèmes d'exploitation, il n'y a aucune garantie que l'étude HAZOP identifie tous les dangers ou tous les problèmes d'exploitation. Par conséquent, il est préférable que l'étude d'un système complexe ne repose pas uniquement sur une étude HAZOP. En général, cette technique est utilisée en combinaison avec d'autres techniques appropriées au système étudié. Il est essentiel d'intégrer d'autres études pertinentes pour obtenir un système efficace de gestion des risques.
- Un grand nombre de systèmes sont étroitement liés entre eux et une déviation dans l'un d'eux peut avoir une cause ailleurs. Une intervention locale appropriée peut ne pas cibler la cause réelle et ne pas empêcher un accident de se produire ultérieurement. Beaucoup d'accidents se sont produits à la suite de modifications locales mineures dont les effets par contrecoup ailleurs n'avaient pas été prévus. Bien qu'il soit possible de remédier à ce problème en reportant les implications des déviations d'une partie à une autre, ceci n'est souvent pas réalisé dans la pratique.
- Le succès d'une étude HAZOP dépend en grande partie de la capacité et de l'expérience du chef d'étude, de la connaissance des membres de l'équipe ainsi que de leurs interactions.
- L'étude HAZOP ne considère que les parties qui apparaissent sur les plans de conception. Les activités et les opérations qui n'y apparaissent pas ou qui ne sont pas mentionnés par les membres de l'équipe ne sont pas prises en compte.

7.3.4 / Principes de l'étude HAZOP

Le principe de la méthode HAZOP est l'utilisation de « mots guides » pour effectuer une recherche systématique des déviations par rapport à l'intention de conception. Pour faciliter l'examen, un système est divisé en parties (sous-systèmes, aussi appelés « nœuds ») de telle sorte que l'intention de conception puisse être définie de manière adéquate pour chacune d'elles. La taille de la partie choisie varie selon la complexité du système et la sévérité du danger. Elle est petite pour les systèmes complexes ou pour ceux qui présentent des dangers importants. Pour les systèmes simples ou pour ceux engendrant des faibles dangers, l'utilisation de grandes parties réduit le temps d'étude. L'intention de conception pour une partie d'un système est formulée sur la base des éléments qui possèdent les caractéristiques essentielles de la partie et en représentent les divisions naturelles. Le choix des éléments à examiner est, dans une certaine mesure, une décision subjective puisqu'il existe plusieurs combinaisons menant au but recherché. Les éléments du système peuvent être des étapes ou des phases discrètes d'une procédure, des signaux individuels et des entités d'un système de commande, un équipement ou des composantes d'un processus ou d'un système électronique, etc. La figure 11 illustre le déroulement d'une étude HAZOP.

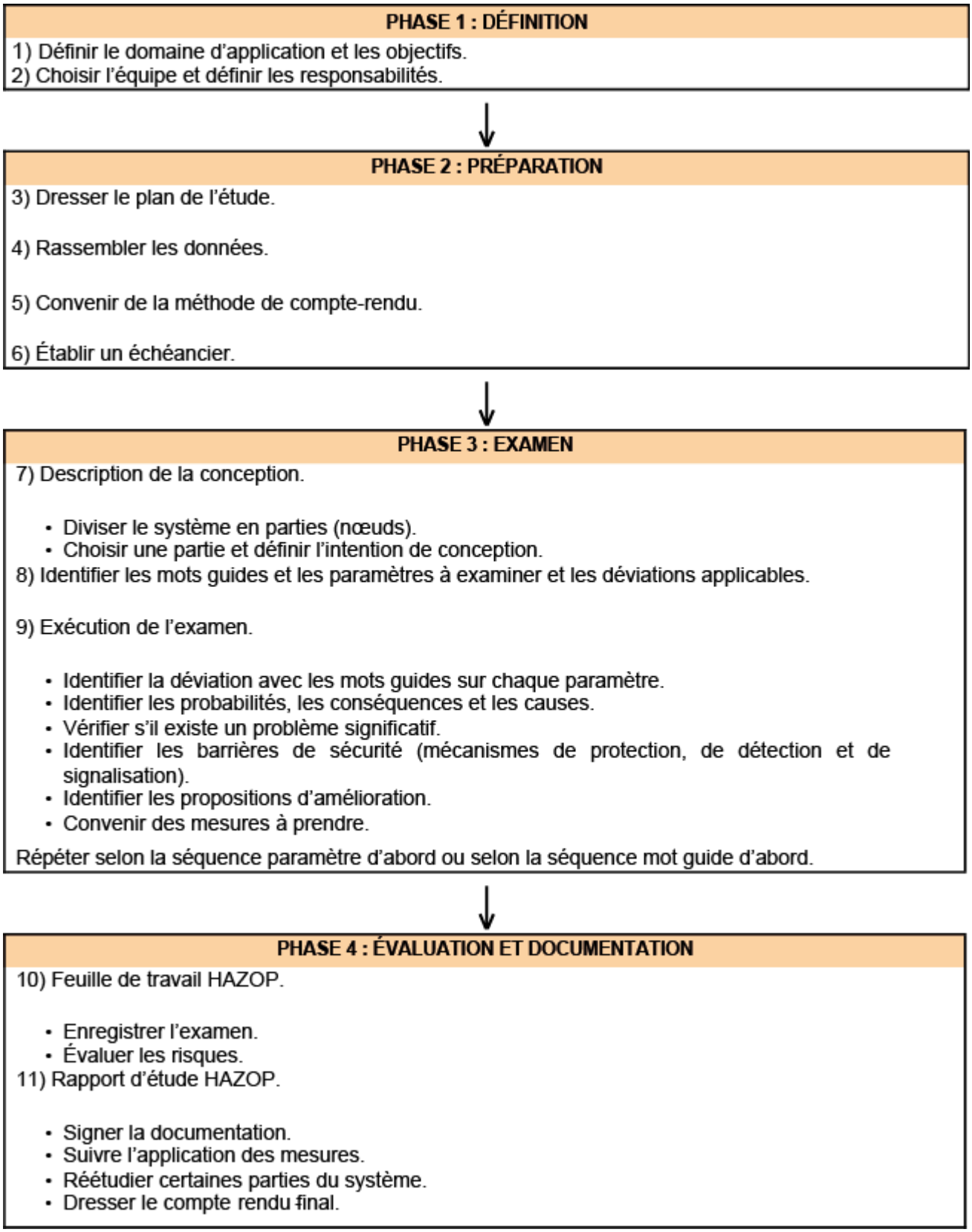

Figure 6 - Déroulement d'une étude HAZOP

Il est important de bien identifier l'origine, la fonction et la sortie du nœud, par exemple selon les termes suivants :

- matériau d'entrée provenant d'une certaine source;
- operation sur un matériau;
- produit(s) de sortie transporté(s) vers une destination.

L'intention de conception d'un nœud contiendra donc les éléments suivants : matériaux, activités, sources et destinations, qui peuvent être considérés comme éléments du nœud. Il est aussi utile de définir les éléments en termes de caractéristiques quantitatives ou qualitatives. Par exemple, dans un système chimique, l'élément « matériau » peut être défini en termes de caractéristiques telles que la température, la pression et la composition. Pour l'activité « transport », des caractéristiques telles que la vitesse de déplacement ou le nombre de passagers peuvent être pertinentes. Pour les systèmes informatiques, les informations plutôt que les matériaux seront prises en considération dans chaque partie.

L'équipe HAZOP examine chaque élément (et, le cas échéant, sa caractéristique) pour y rechercher les déviations par rapport à l'intention de conception susceptibles d'entraîner des conséquences indésirables. Pour identifier ces déviations, elle emploie un système de questions dans lequel interviennent des « mots guides » prédéfinis. Le rôle d'un mot guide est de stimuler l'imagination, de focaliser l'étude et de soulever des idées et des discussions, de façon à augmenter les chances de réalisation d'une étude complète. Les principaux mots guides et leurs significations sont présentés dans le tableau 5.

Mot-guide	Signification
NE PAS FAIRE	Négation totale de l'intention de conception
PLUS	Augmentation quantitative
MOINS	Diminution quantitative
EN PLUS DE	Modification/diminution qualitative
INVERSE	Contraire logique de l'intention de conception
AUTRE QUE	Remplacement total

Tableau 11 - Principaux mots guides avec leur signification générale

D'autres mots guides relatifs au temps, à un ordre ou à une séquence sont également définis dans le tableau 6.

Mot-guide	Signification
PLUS TÔT	Relatif au temps
PLUS TARD	Relatif au temps
AVANT	Relatif à un ordre ou une séquence
APRÈS	Relatif à un ordre ou une séquence
AUTRE QUE	Remplacement total

Tableau 12 - Mots guides relatifs au temps ou une séquence