Sûreté de fonctionnement

Méthodes qualitatives pour l'analyse de risques

Nicolae Brînzei

Introduction

- les méthodes dites qualitatives de la sûreté de fonctionnement sont essentiellement des **méthodes d'analyse destinées à mieux connaître les systèmes ou installations** de manière à prendre en compte leurs dysfonctionnements potentiels afin de réduire leurs conséquences
- un dysfonctionnement, une **défaillance** dans un système peut induire un **danger** qui fait courir à celui-ci, à l'homme qui le manipule ou l'utilise et à son environnement, un **risque** que l'on voudrait aussi faible que possible ou en tous cas inférieur à un niveau admissible
- l'objectif des méthodes qualitatives est de tendre à la réduction de ce risque
- puisqu'elles sont qualitatives, elles ne permettent pas de quantifier le gain en « sûreté » mais donnent seulement des indicateurs ; elles devront donc toujours être complétées par des études de quantification plus fines, surtout lorsque l'on recherche une optimisation du processus d'amélioration de la sûreté (avec des contraintes de coût par exemple)

Introduction

• les notions de risque et de danger ont une extension large et s'appliquent à de nombreux domaines ; on les rencontre dans le domaine de la sécurité des personnes (risque de blessure, de maladie professionnelle, de mort), de la sécurité ou de l'intégrité des biens (détérioration ou destruction de matériels, d'installations), de la disponibilité des systèmes (risque de pertes d'exploitation), des systèmes financiers (risque commercial, risque d'investissement, risque boursier…), des systèmes sociaux (risque de troubles sociaux, grèves…) et même dans le domaine politique…

Classification des risques

Risques liés aux systèmes conçus par l'homme	*Risques industriels (ou technologiques)*	Liés à l'exploitation des systèmes technologiques : bruits, explosions, pollutions de l'air, de l'eau, du sol, radiations et rayonnements…
		Liés aux produits utilisés, fabriqués : matières et produits dangereux ; énergie ; information ; aliment ; médicament…
		Liés à la présence de l'homme dans les systèmes technologiques : accidents du travail et maladies professionnelles…
		Liés au démantèlement des systèmes technologiques : friches industriels et militaires ; abandon des galeries de mines…
	Risques sociaux, économiques financiers	Comportements collectifs
		Mouvements sociaux
		Phénomènes boursiers et monétaires
		Equipements et infrastructures publics transport des personnes (sécurité) ; transport de l'information (confidentialité, intégrité)…
Risques liés à la présence de l'homme dans son milieu naturel :	*Risque maladie*	Contagions, épidémies, pandémies…
	Risques naturels (catastrophes)	Tremblements de terre, volcans, cyclones et tornades, inondations, feux de forêts…

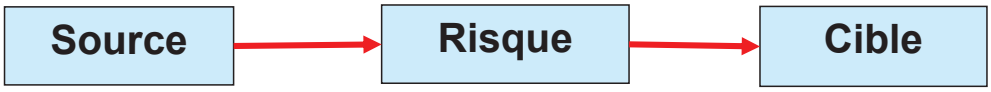
Introduction

• les notions de risque, danger, dommage, gravité, etc. sont définies dans de nombreuses normes relatives aux différents domaines évoqués

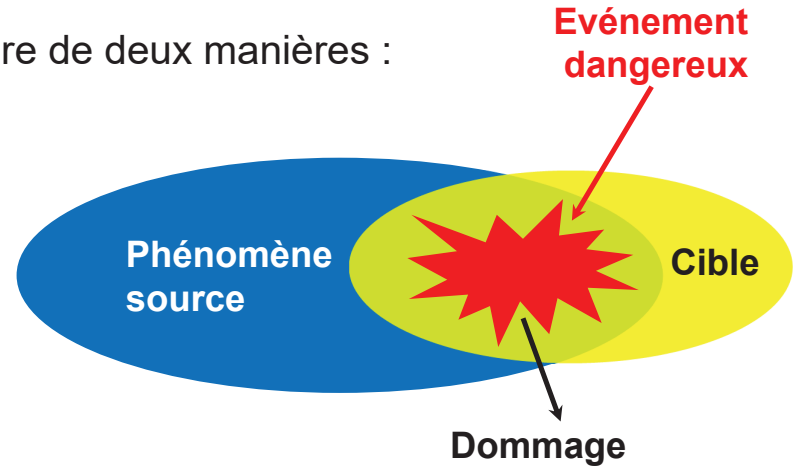
Dommage : blessure physique ou atteinte à la santé affectant des personnes soit directement soit indirectement comme conséquence à un dégât causé aux biens ou à l'environnement.	CEI 61508, *CEI 1050*
Phénomène dangereux : source potentielle de danger. *La norme EN 292 indique source potentielle de blessure ou d'atteinte à la santé.*	CEI 61508
Situation dangereuse : situation dans laquelle une personne est exposée à un (des) phénomène(s) dangereux. La norme EN 292 donne une définition identique	CEI 61508
Zone dangereuse: Toute zone à l'intérieur et/ou autour d'une machine, dans laquelle une personne est exposée à un risque de lésion ou d'atteinte à la santé.	EN 292-1
Evénement dangereux : situation dangereuse qui conduit à un dommage. *La norme CEI 1050 donne une définition identique*	CEI 61508
Risque : combinaison de la probabilité d'un dommage et de sa gravité.	CEI 61508
Risque : combinaison de la probabilité et de la gravité d'une lésion ou d'une atteinte à la santé pouvant survenir dans uns situation dangereuse	EN 292-1
Risque tolérable : risque accepté dans un certain contexte et fondé sur les valeurs actuelles de la société. *La norme EN 292 donne une définition semblable*	CEI 61508
Risque résiduel : risque restant après que toutes les mesures de prévention ont été prises. *La norme CEI 1050 donne une définition proche*	CEI 61508
Sécurité : absence de risque inacceptable.	CEI 61508

Introduction

D'une manière générale, un risque est dû à une source et s'exerce sur une cible :



Réduire un risque peut donc se faire de deux manières :
- s'attaquer à la source
- protéger la cible



Deux moyens sont possibles relativement aux deux composantes du risque :

- **prévention :** réduire la probabilité de l'événement source initiateur ou de la fréquence d'exposition de la cible
- **protection :** réduire la gravité du dommage causé à la cible par des dispositifs de protection, de confinement ou de mitigation

Introduction

Le processus général de réduction d'un risque se résume par les trois verbes :

Comprendre – Diagnostiquer – Agir

- **comprendre** implique de trouver les **modèles** (de connaissance, de comportement, …) des phénomènes mis en jeu dans les situations dangereuses et de valider ces modèles (simulation, retour d'expérience, …)
- **diagnostiquer**, c'est tout ce qui permet de détecter, localiser, prévoir ou prédire les défaillances ; bien sûr on s'appuiera sur les modèles précédents et sur des méthodes d'extraction des indicateurs pertinents
- **agir** peut être réalisé de différentes manières :
  - **corriger** (maintenance corrective, thérapeutique,…)
  - **prévenir** (maintenance préventive, prédictive, prophylaxie, vaccination…)
  - **éviter** (concerne les systèmes conçus par l'homme, c'est l'action à la conception dans laquelle les risques sont analysés et les choix faits pour minimiser le hasard). Cela relève de l'utilisation de **méthodes**.
  - **tolérer** de manière statique (redondance) ou dynamique (reconfiguration)

Introduction

Dans tous les cas, il faut faire la preuve de l'efficacité des actions proposées aux décideurs ! Cela implique d'évaluer (quantitativement si possible), de simuler, et cela met en œuvre des **modèles**, des **méthodes** et les **outils** supports.

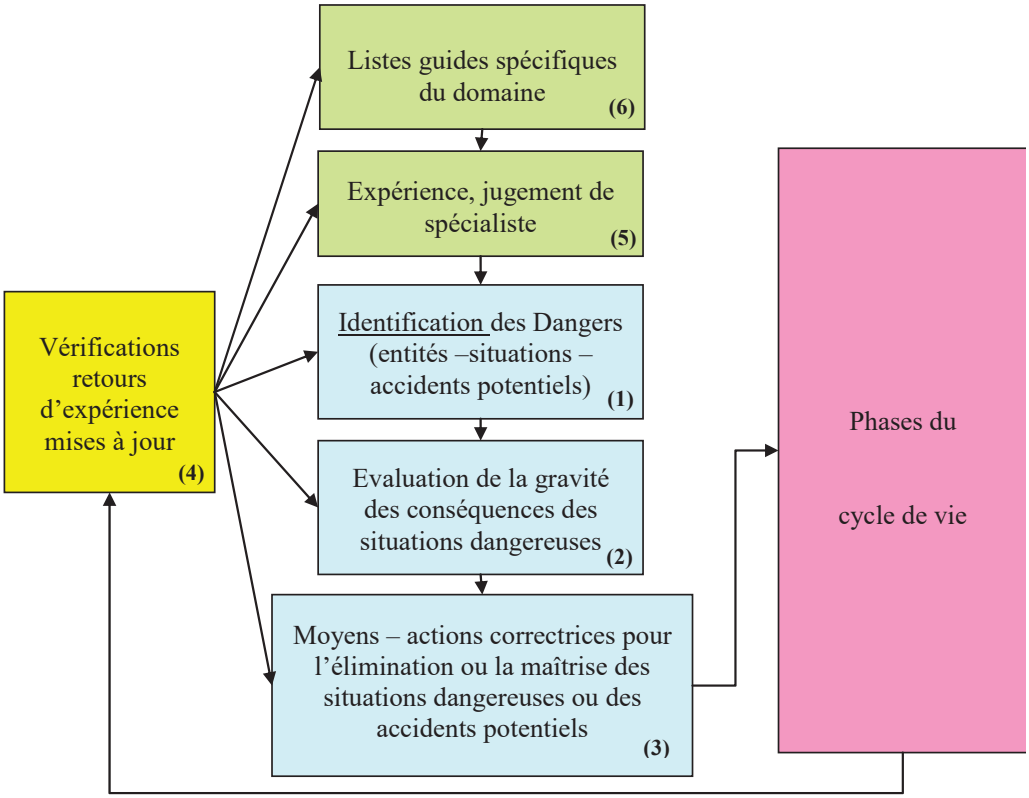
Les méthodes qualitatives apportent une contribution dans la compréhension des phénomènes et la proposition de solutions d'amélioration, que ce soit en phase de conception ou en phase d'exploitation du système. Il en existe un grand nombre, à commencer par l'analyse fonctionnelle qui n'est pas spécifique à la sûreté de fonctionnement. Nous présenterons seulement ici l'analyse préliminaire des risques et l'analyse des modes de défaillances et de leurs effets.

Analyse Préliminaire des Risques (APR)

- est une méthode d'usage très général pour l'identification des risques au stade préliminaire de la conception d'un système ou d'une installation
- cette méthode a été développée à l'origine aux USA dans les années 1960 pour la fabrication de missiles ; elle a ensuite été employée dans l'aéronautique par Boeing, puis dans les industries chimique, nucléaire et aéronautique
- met en évidence des entités d'un système ou des situations nécessitant une attention spécifique pour lesquelles il est nécessaire d'utiliser des méthodes d'analyses de risques plus détaillées
- elle est recommandée en France par l'Union des Industries Chimiques depuis 1980

Analyse Préliminaire des Risques (APR)

Principe



Analyse Préliminaire des Risques (APR)

Principe

L'objectif de la méthode est :

(**1**) d'identifier tous les dangers d'un système, d'une installation, etc., c.à.d. les entités potentiellement dangereuses, les situations à l'origine du danger, les accidents potentiels … Cette identification se fait dès les premières phases de la conception du système, à partir des données disponibles à ce stade.

(**2**) d'évaluer les conséquences de ces situations de danger en terme de gravité

(**3**) d'en déduire une première liste des moyens et actions susceptibles d'éliminer ou de maîtriser les situations dangereuses ou les accidents potentiels

(**4**) au fur et à mesure de la vie du système, l'analyse est vérifiée et complétée

L'identification des dangers repose au départ sur l'expérience et le jugement des experts (**5**), lesquels s'appuient sur des listes guide (**6**) qui sont mises à jour par le retour d'expérience tout au long du cycle de vie du système (voir en utilisant aussi celui d'autres systèmes semblables).

Analyse Préliminaire des Risques (APR)

Application

Les analyses sont résumées dans des tableaux comme par exemple le tableau de la figure ci-dessous (ex. provenant de l'industrie aéronautique).

1 Système ou fonction	2 Phase	3 Entités danger-euses	4 Evéne-ment causant une situation dange-reuse	5 Situation dange-reuse	6 Evéne-ment causant un accident potentiel	7 Accident potentiel	8 Effets ou consé-quences	9 Clasifi-cation par gravité	10 Mesures préventives	11 Application de ces mesures

Analyse Préliminaire des Risques (APR)

Application

On dispose de listes guide des entités et des situations dangereuses spécifiques à chaque secteur d'application (industrie chimiques, industrie aéronautique, …).

Entités	Situations dangereuses
• Combustible • Propergols • Catalyseurs chimiques • Charges explosives • Capacités • Batteries • Conteneurs sous pression • Ressorts tendus • Systèmes de suspension • Fluides sous pression • Générateurs électriques • Objets susceptibles de tomber • Objets susceptibles de se déplacer, d'être catapultés • Dispositifs de chauffage • Pompes • Ventilateurs, hélices soufflantes • Machines tournantes • Interrupteurs, dispositifs de mise à feu • Eléments nucléaires • Réacteurs • Matériaux favorables à l'électricité statique • Energie sous toutes ses formes	• Accélération • Contamination • Corrosion • Réactions chimiques • Electricité (pannes, chocs, chaleurs, action faite par mégarde • Explosion • Feu • Chaleur, température (y compris variations) • Fuites • Humidité, buée • Oxydation • Pression (trop élevée, trop faible, variations rapides) • Chutes, mouvements, catapultage d'objets • Radiations (thermique, électromagnétique, ultraviolet, nucléaire, ionisation…) • Chocs • Concentration de contraintes • Endommagement structurel • Toxicité • Vibration et bruits…

Liste guide des entités dangereuses et des situations dangereuses utilisées dans l'aéronautique [Villemeur]

Application

Industries chimiques :

Les dangers en industrie chimique sont inhérents :

- aux produits (matières premières - intermédiaires - finis) et à leurs propriétés (corrosion - combustion - toxicité)
- aux procédés utilisés (réactions - opérations) et à leurs équipements (réservoirs, réacteurs …).

Des listes guides sont associées aux deux entités. Elles sont établies et mises à jour à chaque phase du cycle de vie : recherche - développement - conception - réalisation - exploitation.

LORRAINE INP Ensem Analyse Préliminaire des Risques (APR)

Application

Fiche produit

Fiche produit		Formule Brute :	
USINE DE : FABRICATION :		NOM : FORMULE DEVELOPPEE OU COMPOSITION :	
	Annexe ou référence		Annexe ou référence
1. Propriétés 1.1. Etat à 20°C : gazeux, liquide, pâteux, pulvérulent, solide. 1.2. Température de fusion. 1.3. Température d'ébullition. 1.4. Température de vapeur. 1.5. Température critique. 1.6. Pression critique. 1.7. Poids spécifique. 1.8. Densité de vapeur. **2. Solubilités.** 2.1. Insolubilités. **3. Chaleur spécifique.** 3.1. Chaleur de formation. 3.2. Chaleur de fusion. 3.3. Chaleur de vaporisation. 3.4. Chaleur de dissolution. 3.5. Chaleur de combustion. 3.6. Chaleur de polymérisation. **4. Combustion.** 4.1. Point éclair. 4.2. Température d'auto inflammation. 4.3. Limites d'inflammation / air. 4.4. Limites d'inflammation dans les conditions opératoires. 4.5. Energie d'allumage. 4.6. Résistivité. 4.7. Pyrophoricité. 4.8. % O_2 minimum entretenant la combustion. 4.9. Produits de combustion.		**5. Stabilité : risques… de Peroxydation, de Polymérisation.** 5.1. Stabilité thermique. 5.2. Stabilité à la lumière. 5.3. Stabilité au choc. 5.4. Stabilité à la friction. Catalyseur de : 5.5. Polymérisation. 5.6. Décomposition. Inhibiteur de : 5.7. Polymérisation. 5.8. Décomposition. **6. Analyse produit.** Technique ou commercial : Additifs. **7. Effets des impuretés.** 7.1. Par concentration. 7.2. Par réaction avec d'autres produits présents dans le procédé. 7.3. Par formation de sous-produits présentant des risques. **8. Hygiène industrielle.** 8.1. Limite olfactive. 8.2. Valeur M.A.C. **9. Toxicité.** 9.1. DL50. 9.2. CL50. 9.3. Irritations oculaires et cutanée. 9.4. Sensibilité de la peau. 9.5. Toxicité subaiguë. 9.6. Autres effets.	

Application
Fiche produit

Fiche produit		Formule Brute :	
USINE DE : FABRICATION :		NOM : FORMULE DEVELOPPEE OU COMPOSITION :	
	Annexe ou référence		Annexe ou référence
10. Agents extincteurs (eau, eau pulvérisée, mousse, CO_2 halogénés, poudre). 10.1. Agents extincteurs incompatibles. **11. Corrosion.** 11.1. Matériaux préconisés. 11.2. Matériaux prohibés. **12. Incompatibilités.** 12.1. Eau. 12.2. Fluides caloporteurs. 12.3. Métaux. 12.4. Plastiques. 12.5. Autres.		**13. Réglementation.** 13.1. Installations classées. 13.2. Etiquetage. 13.3. Maladies professionnelles. 13.4. Surveillance médicale spéciale. 13.5. Substances vénéneuses. 13.6. Transport: RTMD, RID-ADR, IMCO-IATA. 13.7. Réglementation spécifique. **14. Stockage.** 14.1. Précautions. **15. Destruction.** 15.1. En cas d'épandage. 15.2. Stock inutilisable.	

LORRAINE INP Ensem Analyse Préliminaire des Risques (APR)

Application
Fiche procédé

Fiche procédé	**Produits mis en œuvre : noms et quantités :**
USINE DE : **FABRICATION :** **PHASE :**	- - - -

1. Equation de la réaction principale et des réactions secondaires et chaleurs réactionnelles (préciser en clair : Exothermique ou Endothermique)
2. Conditions opératoires : opérations continue, semi-continue, discontinue.
- 2.1. Mode opératoire résumé.
- 2.2. Schéma de l'appareillage (type schéma de procédé
- 2.3. Solvant
- 2.4. Catalyseur
- 2.5. Température / Pression / pH
- 2.6. Conditions particulières (atmosphère inerte, obscurité…)
- 2.7. T° maxima supportée par le mélange réactionnel sans risque de dégradation

3. Risques.
- 3.1. Potentiel énergétique maximum (P.E.M.).
- 3.2. Volume de gaz émis en cas de décomposition.
- 3.3. Produits chimiques incompatibles dont l'addition provoque une réaction violente.
- 3.4. Risque d'accumulation d'impuretés instables.
- 3.5. Risque de retard au démarrage de la réaction.
- 3.6. Risque de désamorçage de la réaction.
- 3.7. Les mélanges réactionnels sont-ils susceptibles d'évoluer ?
- 3.8. Risques toxique à court et à long termes des matières premières, des intermédiaires, des impuretés et des produits fabriqués par les réactions normales, secondaires ou anormales.
- 3.9. Risque d'incendie ou d'explosion : vapeurs, poussières inflammables, sources d'ignition.

4. Dispositifs prévus pour assurer la maîtrise de la réaction e cas de :
- 4.1. Montée en T°.
- 4.2. Montée en pression (soupape, tampon d'explosion, vidange rapide…).
- 4.3. Emballement (inhibiteurs, dilution…).

5. Moyens de prévention de contamination par mélange intempestif des réactifs :
- 5.1. Retour indésirable par réseau de distribution des réactifs ou des fluides des services généraux (air comprimé, azote, vide…).
- 5.2. Fuite de fluides caloporteurs dans le mélange réactionnel (présence dans le même atelier de produits incompatibles…).

Analyse Préliminaire des Risques (APR)

Application

Fiche procédé

Fiche procédé	Produits mis en œuvre : noms et quantités :
USINE DE : **FABRICATION :** **PHASE :**	- - - -

6. Mesures propres à parer les conséquences d'une panne :
- 6.1. D'énergie électrique.
- 6.2. D'eau.
- 6.3. De fluides caloporteurs (chauffage, refroidissement…).
- 6.4. D'agitation.
- 6.5. De régulation.

7. Mesures propres à éviter les fausses manœuvres :
- 7.1. Oubli de charge d'un réactif.
- 7.2. Double charge d'un réactif.
- 7.3. Confusion de réactif.
- 7.4. Interversion de l'ordre de chargement.
- 7.5. Autres fausses manœuvres possibles.

8. Corrosion (matériaux à proscrire/matériaux à utiliser).
- 8.1. Influence de la température.
- 8.2. Evolution des compositions.
- 8.3. Teneurs en produits secondaires ou impuretés.

9. Moyens d'élimination et de destruction des effluents (gazeux, liquides, solides).

10. Anomalies observées et incidents divers :
Consigner toute observation d'un phénomène inattendu ou d'incident survenant au cours de la recherche, du développement ou de l'exploitation du procédé, tels que : émission de gaz, fumées, flammes…, apparition de mousses, émulsion, débordement…, formation de goudron, dépôts, précipité, polymère…

Analyse Préliminaire des Risques (APR)

Avantages de l'APR :

- permet un examen rapide des situations dangereuses,
- économique en termes de temps passé
- ne nécessite pas un niveau de description détaillé du système

Limites de l'APR :

- ne permet pas de décrire finement les enchaînements (causes-conséquences) qui conduisent à un accident majeur (système complexe),
- nécessite l'utilisation ultérieure d'une AMDEC ou d'un Arbre de défaillances

Analyse des modes de défaillance et de leurs effets (AMDE, FMEA)

Historique

- 1960 Aéronautique Sécurité des avions
  Concorde, Airbus, LEM (Lunar Excursion Module)
- Recommandée aux USA après l'accident nucléaire de TMI (Three Mile Island) dans lequel le cœur d'un réacteur nucléaire a partiellement fondu et des substances radioactives sont échappées dans l'environnement.
- Etendue au spatial, nucléaire (EDF), chimie puis à l'automobile.
- Normes : CEI 812 - 1985
  MIL-STD 1629 A
  ANSI, N41-4 1976, IEEE Std 352 1975

Extensions :

•Analyse des modes de défaillances, de leurs effets et de leur criticité (AMDEC)

•Hazard and Operability Study (HAZOP)

Analyse des modes de défaillance et de leurs effets (AMDE, FMEA)

Introduction

Soit un **système** constitué de **composants**. Etant donné **un état de fonctionnement** de ce système dans lequel il doit assumer un certain nombre de **fonctions**, l'objectif de l'AMDE est :

• d'identifier les modes de défaillance des composants ayant des effets significatifs sur la disponibilité ou la fiabilité ou la maintenabilité ou la sécurité …

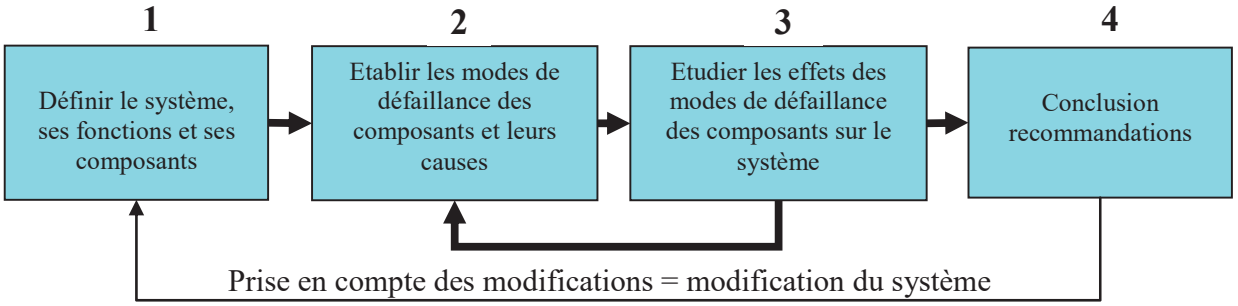
• d'évaluer les effets de chaque mode de défaillance des composants sur les fonctions du système

⇒ **c'est une méthode inductive**

Un **mode de défaillance** d'un composant est l'effet par lequel une défaillance de ce composant se manifeste.

Analyse des modes de défaillance et de leurs effets (AMDE, FMEA)

Etapes de l'élaboration d'une AMDE



• on rappelle que l'étude est relative à un état de fonctionnement du système (en attente, en secours, en test, en marche opérationnelle, en maintenance …).

• les états de fonctionnement peuvent être nombreux dans certains systèmes ; choisir quelques états judicieux (après une APR par exemple).

Analyse des modes de défaillance et de leurs effets (AMDE, FMEA)

Etapes de l'élaboration d'une AMDE

1. Définir le système, ses fonctions, ses composants

• les principales fonctions du système dans l'état de fonctionnement choisi

• les limites fonctionnelles du système et de ses composants

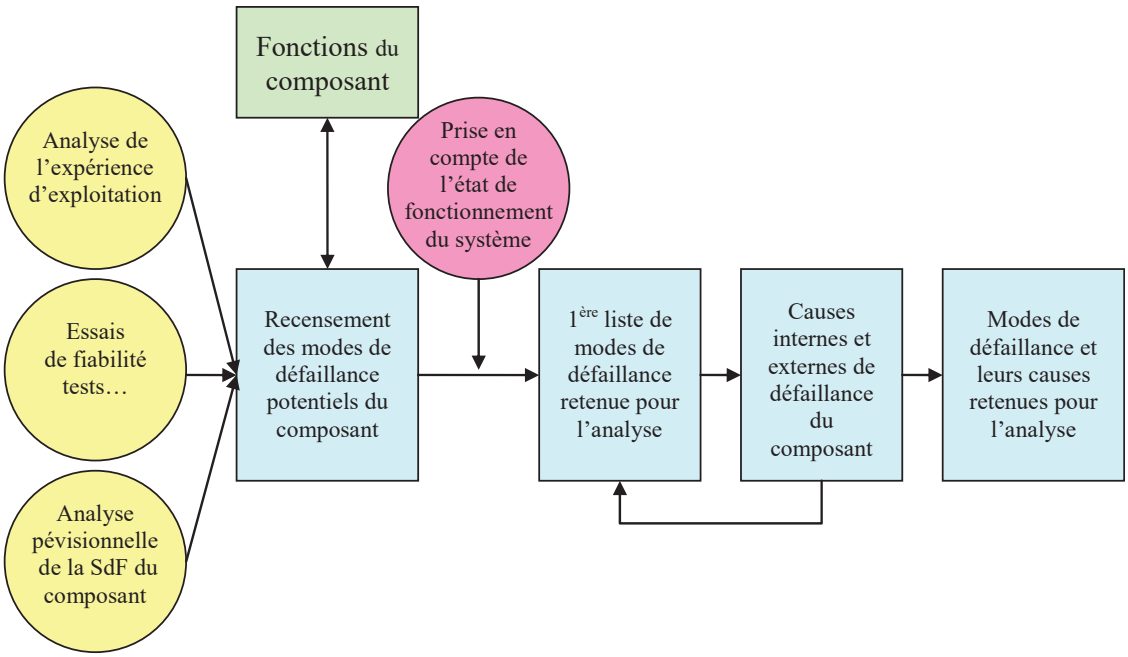
• les spécifications de fonctionnement et d'environnement du système et des composants

• le niveau de décomposition en fonction des connaissances dont on dispose

Analyse des modes de défaillance et de leurs effets (AMDE, FMEA)

Etapes de l'élaboration d'une AMDE

2. Etablir les modes de défaillance des composants et leurs causes



Analyse des modes de défaillance et de leurs effets (AMDE, FMEA)

Etapes de l'élaboration d'une AMDE

2. Etablir les modes de défaillance des composants et leurs causes

a) Recenser de manière aussi complète que possible les modes de défaillance des composants (plausibles - potentiels).

Attention à ne pas confondre cause et mode de défaillance !

La recherche s'appuie sur :
- le retour d'expérience en exploitation des composants
- le retour d'essais et de tests
- pour un composant nouveau, on cherche une expérience dans des composants similaires, ou on fait des études prévisionnelles (fiabilité)
- une classification préétablie et des listes guide de modes de défaillance génériques

Analyse des modes de défaillance et de leurs effets (AMDE, FMEA)

Etapes de l'élaboration d'une AMDE

2. Etablir les modes de défaillance des composants et leurs causes

Une liste guide des modes de défaillance génériques est données ci-dessous :

Modes de défaillance génériques	
1. Défaillance structurelle (rupture).	18. Mise en marche erronée.
2. Blocage physique au 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. Es 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.	Autres condition de défaillances exceptionnelles suivant les caractéristiques du système, les conditions de fonctionnement et les contraintes opérationnelles.
17. Ecoulement réduit.	

Remarque.

On élimine bien sûr les modes de défaillance n'ayant pas de rapport avec l'état de fonctionnement étudié.

ex : dans un système contenant une vanne qui doit être ouverte en permanence dans l'état de fonctionnement choisi, il est inutile d'envisager les modes de défaillance "refus de fermeture de la vanne".

Analyse des modes de défaillance et de leurs effets (AMDE, FMEA)

Etapes de l'élaboration d'une AMDE

2. Etablir les modes de défaillance des composants et leurs causes

b) Etablir les causes possibles des défaillances manifestées.

• il est souvent difficile d'élaborer une liste complète des causes possibles. On peut recourir par exemple à une méthode de type arbre des causes en considérant le composant comme étant lui-même un système.

• on distingue généralement les causes internes et externes

Mode de défaillance	Causes internes	Causes externes
Refus de démarrer	- Blocage mécanique	- Perte de l'alimentation électrique. - Erreur humaine (exemple : les opérateurs ont trop resserré les garnitures lors d'une précédente intervention).
Débit de la pompe inférieur au débit requis	- Défaillance mécanique - Vibrations	- Perte de l'alimentation électrique - Cavitation - Perte de charge importante en amont

Exemple des causes de modes de défaillance dans le cas d'une pompe

Analyse des modes de défaillance et de leurs effets (AMDE, FMEA)

Etapes de l'élaboration d'une AMDE

2. Etablir les modes de défaillance des composants et leurs causes

• on peut décomposer le composant en parties distinctes : mécanique - électrique - alimentation …

• certains modes de défaillance peuvent être cachés car confondus avec des causes

Ex : les vibrations d'une pompe peuvent être considérées comme la cause interne d'une baisse du rendement (débit) de la pompe (mode de défaillance), mais peuvent être considérées comme un mode de défaillance à part entière car ayant des effets (rupture de tuyauterie) sur le système.
En considérant simplement la vibration comme cause de la baisse du rendement, on oubliera l'effet qu'elle peut avoir sur le système. Il n'y a que le mode de défaillance dont on étudie les effets, pas les causes.

LORRAINE INP Ensem

Analyse des modes de défaillance et de leurs effets (AMDE, FMEA)

Etapes de l'élaboration d'une AMDE

3. Etudier les effets des modes de défaillance des composants

On étudie les effets pour chaque mode de défaillance défini pour un composant sur les fonctions du système et sur les autres composants. Etude complète (autant que possible) limitée à une défaillance unique dans le système.

La considération des variables importantes du système et de leur comportement peut aider dans l'étude des effets. Dans certains cas, des études et la recherche de modèles sont nécessaires. Elles peuvent impliquer le recours au spécialiste du système.

L'objectif de l'étude peut être limité au système lui-même ou aux autres systèmes faisant partie de son environnement ou en interaction avec lui.

On notera bien sûr les effets qui font déjà l'objet de surveillance par les systèmes d'alarme et de contrôle et ceux qui ne le font pas.

Analyse des modes de défaillance et de leurs effets (AMDE, FMEA)

Etapes de l'élaboration d'une AMDE

4. Conclusions recommandations

L'AMDE conduit à :

- l'assurance que tous les modes de défaillance importants et leurs effets sur le système ont été pris en compte dès la conception
- l'identification des défaillances simples, critère de conception consistant à empêcher le dysfonctionnement du système sur simple défaillance d'un composant (nécessite dont une double défaillance)
- le classement des modes de défaillance selon l'ampleur de leurs effets et les besoins en redondances
- l'identification des défaillances secondes (défaillance entrainée par la défaillance d'un autre composant)
- la prévision des moyens de détection des modes de défaillances ou la vérification de l'adéquation de ceux prévus à priori
- l'aide à la définition de procédures de maintenance

LORRAINE INP Ensem

Analyse des modes de défaillance et de leurs effets (AMDE, FMEA)

Présentation

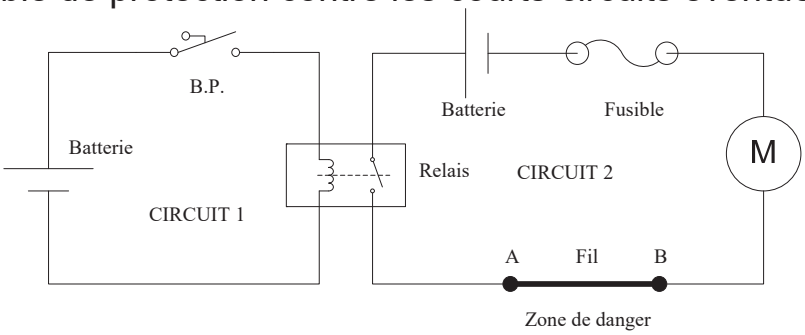
Exemple de tableaux utilisés par EDF [Villemeur]

Identification du composant (repères, désignation, type, lieu)	Fonctions Etats	Mode de défaillance	Causes possibles d'une défaillance (internes-externes)	Effets sur le système élémentaire	Moyens de détection	Actions de l'opérateur	Observations
Repère : 031 VD *Désignation :* Vanne de réglage du débit d'alimentation du GV n°1 par la MPS 021 PO *Type :* Vanne réglante *Lieu :* KA 0524	*Fonction :* Réglage du débit d'alimentation du GV n°1 par la MPS 021 PO *Etats :* Vanne normalement ouverte Les signaux de démarrage de l'ASG confirment l'ouverture en grand de la vanne	1. Vanne bloquée en position grande ouverture	• Défaut mécanique interne • Défaut du circuit pneumatique de commande •Manque d'air moteur (SAR) • Manque de tension de commande 125 V (Voie A)	• Réglage du débit d'alimentation du GV n°1 par la MPS 021 PO impossible depuis la salle de commande • En cas de RTE, de RTV ou de RTVG, l'isolement du GV n°1 est impossible depuis la salle de commande	• Dispositif de fin de course • Débit d'alimentation du GV n°1 Mesures de débit anormalement élevées (101 et 102 MD). Eventuellement alarme de haut débit (101 et 102 MD) ; seuil fixé à 120 t/h	• L'opérateur devra venir positionner la vanne en local •L'opérateur devra soit arrêter la MPS 021 PO, soit venir fermer en local la vanne 051 VD	• Les vannes réglantes associées aux MPS sont alimentées par la même voie que la MPS ; les vannes réglantes associées aux TPS sont alimentées en voies A et B

Analyse des modes de défaillance et de leurs effets (AMDE, FMEA)

Exemple [Villemeur]

Soit le système de commande à distance d'un moteur à courant continu par l'appui sur un bouton poussoir (B.P.). Cela provoque l'excitation de la bobine d'un relais et la fermeture du contact associé qui permet l'alimentation du moteur à partir d'une source d'énergie électrique (batterie par exemple). Le circuit d'alimentation du moteur comprend un fusible de protection contre les courts-circuits éventuels du moteur.



Le système est conçu pour fonctionner pendant un temps court (la classe du moteur ne permet pas le fonctionnement permanent) et on admet que le fonctionnement prolongé du moteur entraîne un échauffement qui se traduit par une destruction du moteur qui se met en court-circuit.

On admet aussi que le contact du relais peut rester collé après le passage d'un courant excessif comme celui correspondant au court-circuit du moteur.

L'analyse portera seulement sur les composants suivants :

- Bouton poussoir – Relais – Fusible – Moteur

Analyse des modes de défaillance et de leurs effets (AMDE, FMEA)

Exemple [Villemeur]

On retiendra pour ces composants que les modes de défaillance essentiels (un ou deux par composant). Le tableau suivant résume l'analyse.

Composant	Modes de défaillance	Causes possibles	Effets sur le système
Bouton poussoir (B.P.)	- le B.P. est bloqué	- défaillance première (mécanique)	- perte de la fonction du système : le moteur ne tourne pas
	- le contact du B.P. reste fermé	- défaillance première (mécanique) - l'opérateur ne relâche pas le B.P. (erreur humaine)	- le moteur tourne pendant un temps trop long : d'où un court-circuit du moteur, puis l'apparition d'un courant élevé et la fusion du fusible.
Relais	- le contact du relais reste ouvert	- défaillance première (mécanique)	- perte de la fonction du système : le moteur ne tourne pas
	- le contact du relais reste collé	- un courant élevé traverse le contact	- le moteur tourne pendant un temps trop long : d'où un court-circuit du moteur, puis l'apparition d'un courant élevé et la fusion du fusible.
Fusible	- le fusible ne fond pas	- défaillance première - l'opérateur a surdimensionné le fusible (erreur humaine)	
Moteur	- le moteur ne tourne pas	- défaillance première le B.P. est bloqué - le contact du relais reste ouvert	- perte de la fonction du système : le moteur ne tourne pas
	- court-circuit	- défaillance première - le moteur tourne pendant un temps trop long	le court-circuit du moteur entraîne l'apparition d'un courant élevé puis la fusion du fusible ; le contact du relais reste collé

Analyse des modes de défaillance et de leurs effets (AMDE, FMEA)

Exemple [Villemeur]

La détermination des modes de défaillances de chaque composant ne pose pas de problème particulier, ils sont courants et leur utilisation traditionnelle.

Pour la recherche des causes de ces modes de défaillances, on doit commencer par les causes internes au composant (défaillances premières) puis continuer par les causes externes en recherchant les éventuelles causes de commande (exemple le contact du bouton poussoir reste collé parce que l'opérateur ne l'a pas relâché).

Pour les causes dues à d'autres composants, on attendra d'avoir énuméré les conséquences des modes de défaillances de ces composants, ceci de manière à garantir une certaine exhaustivité. Ainsi (flèches rouges), dans les causes du mode de défaillance « le moteur ne tourne pas », la cause « le B.P. est bloqué » n'est introduite qu'après avoir énoncé la conséquence « perte de la fonction du système : le moteur ne tourne pas » du mode de défaillance « le B.P. est bloqué ». Il en va de même pour la cause « le contact du relais reste ouvert ».

LORRAINE INP Ensem

Analyse des modes de défaillance et de leurs effets (AMDE, FMEA)

L'étude des effets de chacun des modes de défaillances des composants est une phase importante de la méthode car elle **peut apporter une meilleure connaissance du système** et **induire une recherche de modifications du système pour annihiler ces conséquences**. C'est pourquoi le tableau comporte souvent des colonnes supplémentaires pour proposer ces modifications.

Lorsqu'on ne cherche pas à améliorer la structure du système mais simplement à réagir sur lui en phase d'exploitation, il conviendra d'introduire une colonne décrivant les moyens de détection de la défaillance ainsi que les moyens d'intervention (alarme puis intervention d'un opérateur par exemple).

Extensions : Analyse des modes de défaillance, de leurs effets et de leur criticité (AMDEC)

•c'est une extension de l'AMDE à laquelle on associe la criticité du mode de défaillance

• la criticité est assimilable au niveau du risque associé à cette défaillance

• elle se mesure par le produit de la probabilité (ou fréquence) d'occurrence du mode de défaillance par la gravité de ses effets et parfois il peut-être complété par la probabilité de non détection du mode de défaillance

• ces paramètres sont estimés par les experts chargés de l'étude en fonction de leur connaissance et du retour d'expérience

Criticité **C = G x F x ND**

G - gravité
F - fréquence
ND - non-détection

Extensions : Analyse des modes de défaillance, de leurs effets et de leur criticité (AMDEC)

Indicateurs qualitatifs

• la gravité, la fréquence et la non-détection sont évalués sur une échelle qualitative (1 à 10, 1 à 4, etc., où 1 signifie un impact très faible et en allant de manière ascendante vers les impacts les plus forts, catastrophiques)

Fréquence / Gravité	Très faible	Faible	Moyenne	Forte
Classe I ou Effets mineurs				
Classe II ou Effets significatifs				
Classe III ou Effets critiques				
Classe IV ou Effets catastrophiques				

• pour la non-détection l'échelle suivante pourra être utilisée :
  • présence d'un signe avant-coureur qui permettra à l'opérateur d'éviter le mode de défaillance par une action préventive
  • le signe avant-coureur existe, mais il y un risque que l'opérateur ne le perçoit pas
  • le signe avant-coureur n'est pas facilement détectable
  • aucun signe avant-coureur n'existe ou n'est détectable

Extensions : Analyse des modes de défaillance, de leurs effets et de leur criticité (AMDEC)

Indicateurs qualitatifs

L'objectif de cette évaluation est de s'attaquer en priorité aux défaillances aux conséquences les plus critiques.

On cherchera à ramener cette criticité en dessous d'un niveau acceptable en réduisant la fréquence (prévention), la gravité (protection) ou la non-détection.

L'approche reste cependant très subjective car la quantification se fait par estimation d'appartenance à un niveau de probabilité ou de criticité.

		Prévu/Existant								Actions			Résultat			
N°	Fonction	Défaillance	Cause	Effet	Détection	F	G	D	C	Responsable	Délai	Modification	F'	G'	D'	C'

Extensions : Méthode HAZOP (Hazard and Opérability Study)

• c'est une méthode non basée sur la notion de composant, car la difficulté de décomposer un système complexe est grande et pour pallier à celle-ci on part de la notion de défaillance constatée au niveau système

• la méthode HAZOP (Hazard and operability Study) est normalisée par la norme [CEI 61882]

• la méthode HAZOP s'apparente à l'AMDE par la démarche et à une méthode de type cause-conséquence ; elle utilise des mots guides comme point de départ des modes de défaillance (voir tableau ci-dessous)

Guide word	Deviation	Possible causes	Consequences	Action required
NONE	No flow			
MORE	More flow			
	More pressure			
	More temperature			
LESS OF	Less flow			
	Less temperature			
PART OF	High water concentration or stream			
MORE THAN	Organic acids presence			
OTHER	Maintenance			

Extensions : Méthode HAZOP (Hazard and Opérability Study)

- à la différence de l'AMDE, les deux premières colonnes constituent une recherche déductive des modes de défaillance
- la méthode HAZOP s'apparente à la méthode AMDEC mais s'intéresse aux flux échangés entre les fonctions ou composants tandis que l' AMDEC s' intéresse aux fonctions
- HAZOP permet de recenser l'ensemble des **déviations d'un flux** en se basant sur des déviations génériques puis d'analyser les causes et les effets de ces déviations sur le système. La déviation représente une variation anormale d'un flux entrant ou sortant d'une fonction ou des propriétés des objets formant ce flux (équivalent aux modes de défaillance).
- cette méthode peut être, par conséquent, moins fastidieuse pour des systèmes complexes mais peut poser un problème d'exhaustivité (extension du système vis-à-vis des causes possibles)

Conclusions

L'AMDE et ses extensions :

- peuvent être utilisée pour les composants, les systèmes, les systèmes de sûreté proprement-dits
- présentent un intérêt pour l'aide à la conception surtout au début ; elles peuvent être employées aux différentes étapes de conception, réalisation, exploitation, maintenance et démantèlement
- apportent des modèles de modes de défaillance et compte tenu de leur relative universalité elles nécessitent l'utilisation de documents standard pour communiquer entre les différents spécialistes
- améliorent le dialogue entre analyste et spécialiste, concepteur et exploitant
- génèrent cependant un travail souvent très fastidieux et assez coûteux (en temps surtout)
- l'AMDE tend à s'étendre à d'autres domaines (électronique, numérique, logiciel)