Université du 20 août 1955 Skikda

Institut des Sciences et Techniques Appliquées(ISTA)

Méthodes et outils d'analyse des risques

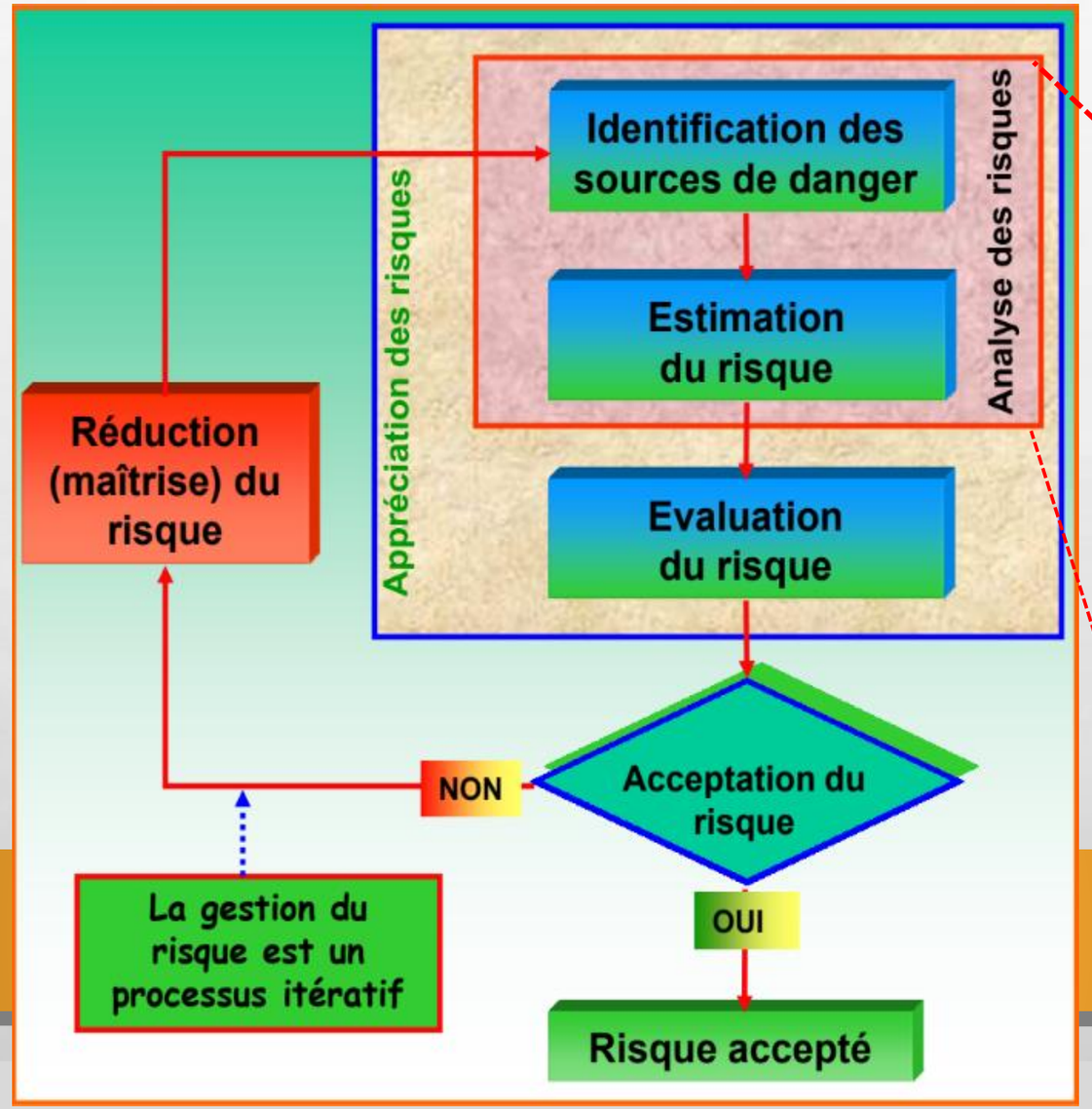
Intervenante : Dr. Chaima Bensaci

Fonction actuelle: *Maitre de conférence classe B à l'Institut des Sciences et Techniques Appliquées (ISTA) – Université du 20 Aout 1955, SKIKDA*

2023 – 2024

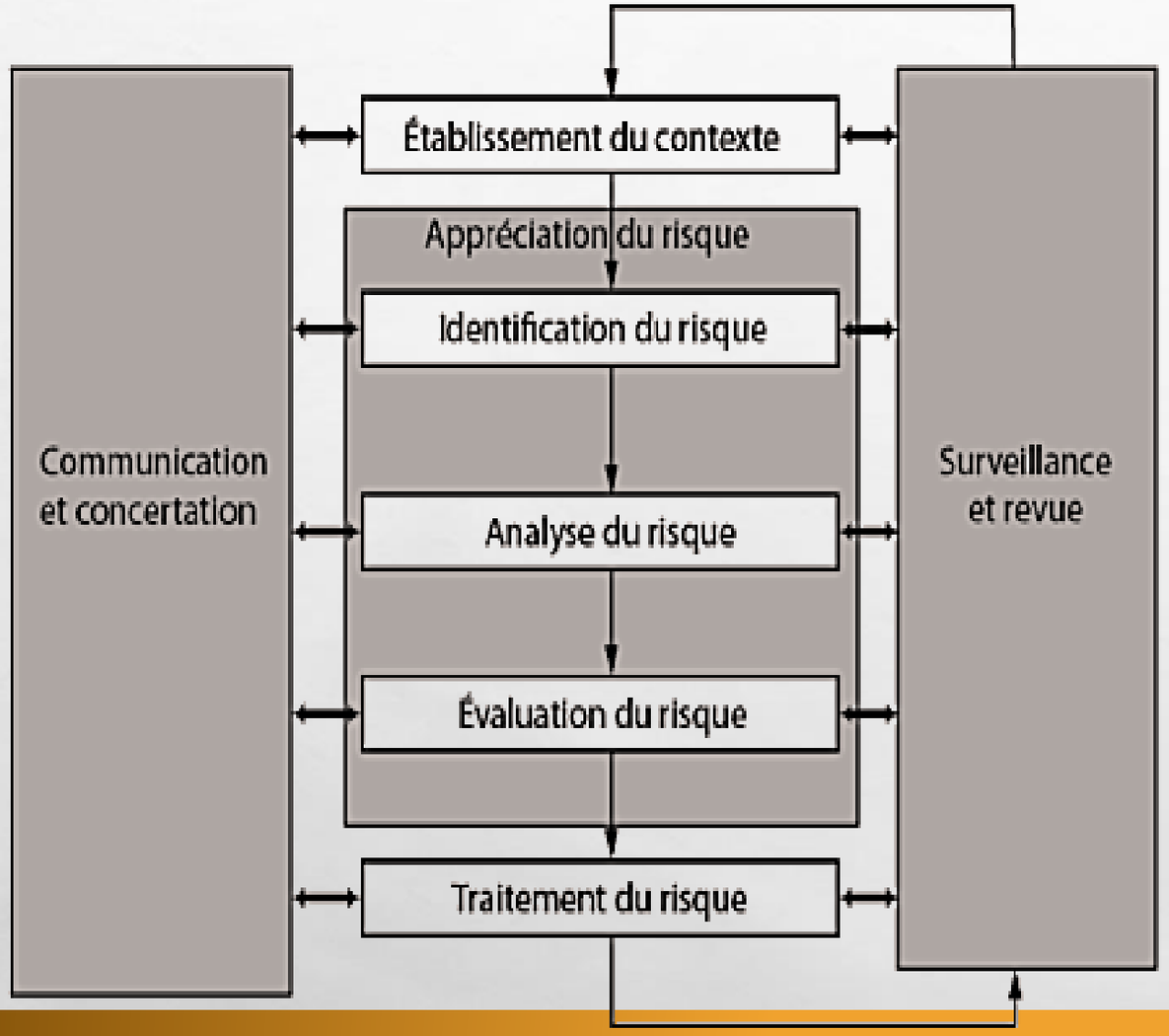
Démarche générale de gestion des risques

Gestion des risques : *ensemble des activités coordonnées en vue de réduire le risque à un niveau jugé tolérable ou acceptable, qui nécessite un usage adapté des méthodes et outils de la SdF.*



- Analyse Fonctionnelle
- AdC
- APR
- AMDEC
- HAZOP
- AdD
- AdE
- MOSAR
- CM
- RdP
- ...

Démarche générale de gestion des risques



Processus de gestion de risque selon l'ISO 31000 v 2018

Afin de gérer les risques, il est important de :

- ***les identifier*** et de ***les analyser qualitativement***.
- ***évaluer leurs degrés de criticité*** : élément important qui va permettre d'estimer *l'importance du risque et ainsi permettre à l'organisme de prioriser ses actions*.
- ***traiter les risques*** en élaborant et en mettant en œuvre un plan d'action.
- Il est important *pendant toute la durée du processus de gestion des risques de veiller à la communication et à l'échange d'informations. La surveillance et le contrôle permanent de ses risques sont également indispensables*

Démarche générale de gestion des risques

L'identification des risques est le processus de recherche, de reconnaissance et d'enregistrement des risques (Nature et emplacement du risque).

BUT: Identifier les raisons pour lesquelles les objectifs du système ou de l'organisation pourraient ne pas être atteints.

L'analyse des risques consiste à déterminer les conséquences et les probabilités pour les risques identifiés en tenant compte de la présence (ou non) et de l'efficacité des contrôles existants, Elle peut être: qualitative, semi-quantitative, quantitative. (Estimer la gravité et la probabilité d'occurrence du risque)

Démarche générale de gestion des risques

Evaluation des risques

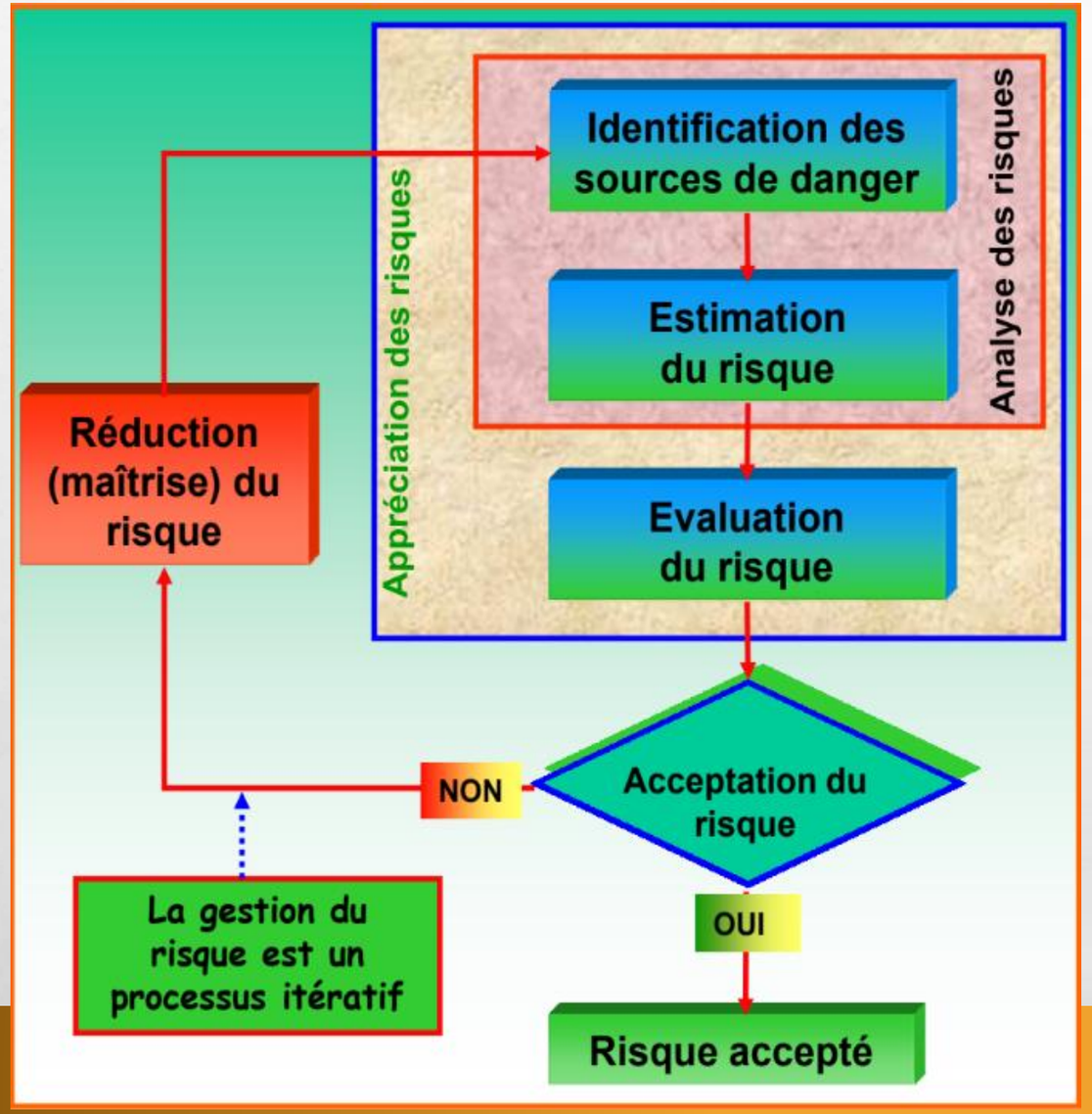
- Evaluer le risque, son niveau de criticité
- Vérifier l'acceptabilité du risque

Traitement des risques

- Sélectionner les mesures nécessaires d'élimination ou d'atténuation de risque et les implémenter

Remarque : Il n'est pas toujours possible d'éliminer ou d'éviter. Mais, il est possible de réduire le risque et de le maitriser

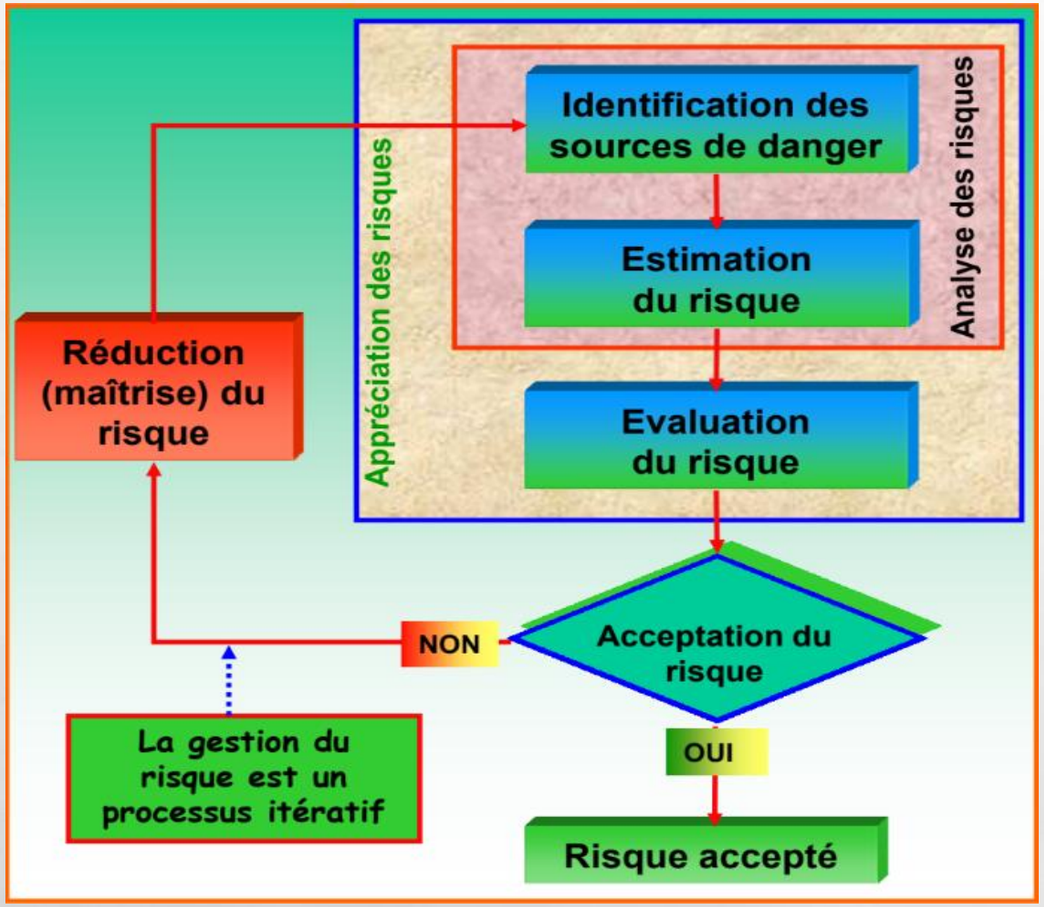
Démarche générale de gestion des risques



- L'analyse des risques s'effectue dans le cadre du processus décisionnel de Gestion des Risques (GR).
- Autrement-dit, ce processus montre que sa finalité est le « traitement des risques » qui dépend de « l'évaluation du risque » et qui dépend, à son tour, de « l'analyse des risques ». D'où la place du choix qu'occupe l'analyse des risques dans ce processus.

Démarche générale de gestion des risques

De l'analyse des risques aux méthodes d'analyse des risques

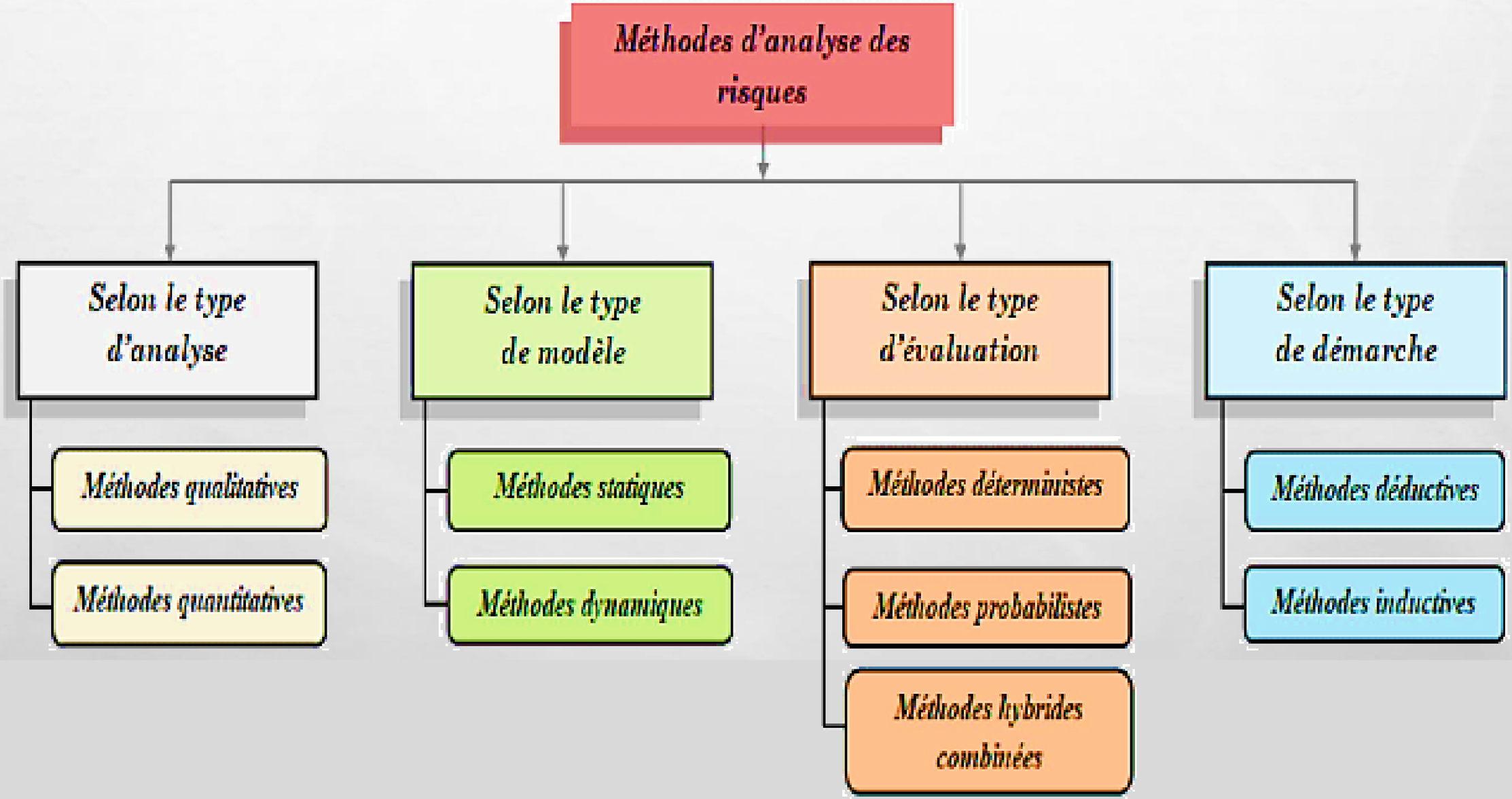


L'analyse des risques s'effectue par le biais de méthodes appropriées « méthodes d'analyse des risques ».

En référence aux systèmes, les méthodes d'analyse des risques se focalisent soit sur la performance des systèmes (paramètres de son fonctionnement.) ou bien sur la contreperformance des systèmes (paramètres de son dysfonctionnement – ENS-).

Chaque méthode d'analyse des risques est caractérisée par son propre formalisme (représentation graphique). Dans ce contexte, une méthode d'analyse des risques peut être représentée sous forme : d'un tableau, d'un arbre ou d'un graphe (ou réseau).

Catégorisation des méthodes d'analyse des risques : une aide au choix de ces méthodes



Démarche générale de gestion des risques

Catégorisation des méthodes d'analyse des risques : une aide au choix de ces méthodes

Selon le type d'analyse Il existe deux principaux types d'analyse, à savoir, qualitative et quantitative.

Selon le type de modèle L'analyse des risques peut être effectuée de deux manières, soit on suit une approche statique, qui permet l'analyse du système d'un point de vue structurel sans avoir à considérer les changements du système au cours du temps, soit une approche dynamique qui tient compte des aspects comportemental et temporel du système.

Selon le type d'évaluation La phase d'évaluation des risques peut être réalisée selon trois approches différentes : évaluation des conséquences des dommages (approche déterministe), évaluation de la probabilité d'accident (approche probabiliste), évaluation combinée des deux approches précédentes (approche hybride combinée).

Selon le type de démarche adoptée par la méthode Généralement, deux catégories de démarches sont considérées : la première, déductive ou descendante ; et la seconde, inductive ou ascendante.

Méthodes inductives : on part du particulier (causes) vers le général (conséquences ou effets)
Méthodes déductives : on part du général vers le particulier.

Catégorisation des méthodes d'analyse des risques : une aide au choix de ces méthodes

Exemples :

- Méthodes inductives (AMDEC, APR, AdE, Hazop…) et déductives (AdD)
- Méthodes dédiées aux systèmes statiques (AdD, …) et méthodes dédiées aux systèmes dynamiques (GE, …)
- Méthodes qualitatives (APR, AMDEC, HAZOP) et quantitatives (AdD, AdE, …)
- Méthodes déterministes (Hazop), probabilistes (ADD, AdE) et combinées (AMDEC..)
- Méthodes dysfonctionnelles (AMDEC, AdD, …), méthodes fonctionnelles (DBF, …) et méthodes combinatoires (GE, …)

APR	Analyse Préliminaires des Risques
AMDEC	Analyse des Modes de Défaillances, de leurs Effets et de leurs Criticités
AdD	Arbres de Défaillances
AdE	Arbres d'Evènements
DBF	Diagramme Blocs Fiabilité
GE	Graphe d'Etats

Démarche générale de gestion des risques

Paramètres évalués par les méthodes quantitatives d'analyse des risques

- *Paramètres instantanés*

  Nous nous intéressons essentiellement à :
  - La fiabilité d'un système et son évolution dans le temps
  - La disponibilité d'un système et son évolution dans le temps
  - La maintenabilité d'un système et son évolution dans le temps

- *Paramètres non-instantanés*

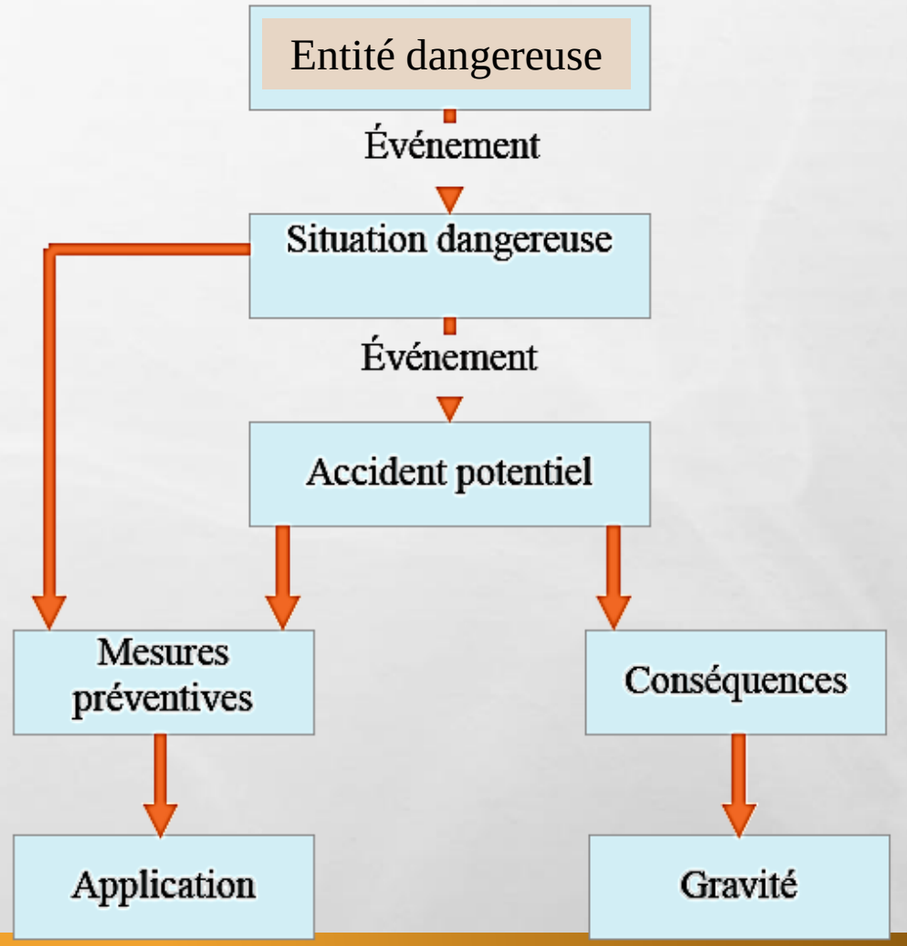
  Nous nous intéressons essentiellement à :
  - La durée moyenne de bon fonctionnement jusqu'à la première défaillance -MTTF -
  - La durée moyenne de bon fonctionnement -MUT -
  - La durée moyenne de défaillance -MDT -
  - La durée moyenne de réparation -MTTR -

APR

Analyse préliminaire des risques

La méthode APR: (Auparavant : Analyse préliminaire des dangers) OU PHA : Primary Hazard Analysis

- Méthode utilisée tout au début d'un projet de maîtrise des risques, avant les méthodes plus fines d'évaluations de risques(Arbres de Défaillance, HAZOP, AMDEC, ...).
- Elle se focalise sur l'analyse « causes-effets » d'une situation dangereuse.
- La méthode a pour objet d'identifier les dangers d'une installation et ses causes (éléments dangereux) et d'évaluer la gravité des conséquences liées aux situations dangereuses et aux accidents potentiels.



Analyse préliminaire des risques APR

Objectifs :

- Identifier les dangers d'une installation et ses causes,
- Evaluer la gravité des conséquences.
- Une Analyse Préliminaire des Risques inclue en plus une estimation de la probabilité d'occurrence des situations dangereuses et des accidents potentiels ainsi que leurs effets et conséquences.
- Proposer des mesures et préparer des procédures pour supprimer les dangers et les accidents potentiels.

Analyse préliminaire des risques APR

Déroulement :

La phase d'identification des dangers consiste à **déterminer les accidents potentiels** que peuvent provoquer **les éléments dangereux** (**entités dangereuses**), ses conséquences, les mesures préventives est ses application,

- Tableau-type synthétisant les résultats de la méthode APR -

Sous-système ou équipement	Phase	Entité dangereuse	Événement causant une situation dangereuse	Situation dangereuse	Événement causant un accident	Accident	Effets ou conséquences	Gravité	Occurrence (fréquence)	Mesures de prévention ou de protection	Application des mesures
.	.	.	.	.	.	.	.	.	.	.	.
.	.	.	.	.	.	.	.	.	.	.	.
.	.	.	.	.	.	.	.	.	.	.	.
.	.	.	.	.	.	.	.	.	.	.	.
.	.	.	.	.	.	.	.	.	.	.	.
.	.	.	.	.	.	.	.	.	.	.	.
.	.	.	.	.	.	.	.	.	.	.	.
.	.	.	.	.	.	.	.	.	.	.	.

Exemple 1 :

Pour chaque élément dangereux identifié: chercher les événements dont l'occurrence pourrait amener à des situations dangereuses.

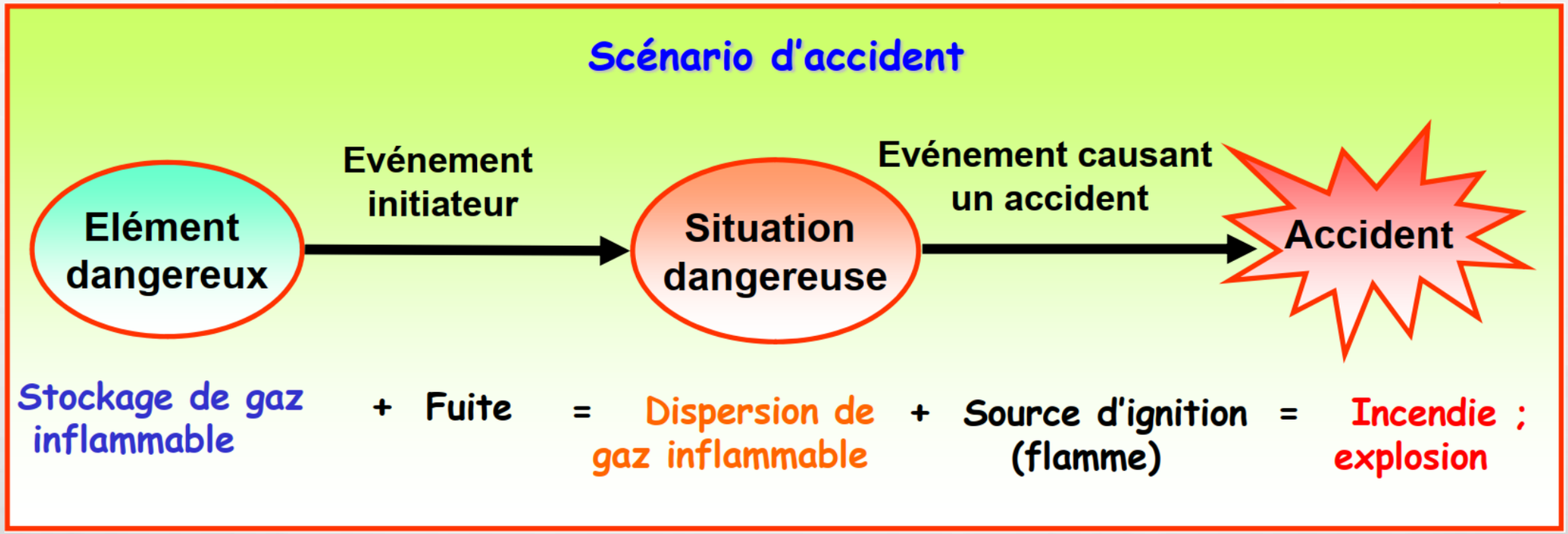
Situation dangereuse = élément dangereux + événement

Fuite de gaz inflammable stockée = Stockage de gaz inflammable + Fuite

Exemple 1 :

Pour chaque situation dangereuse : chercher les événements pouvant provoquer des accidents.

Exemple 1 :

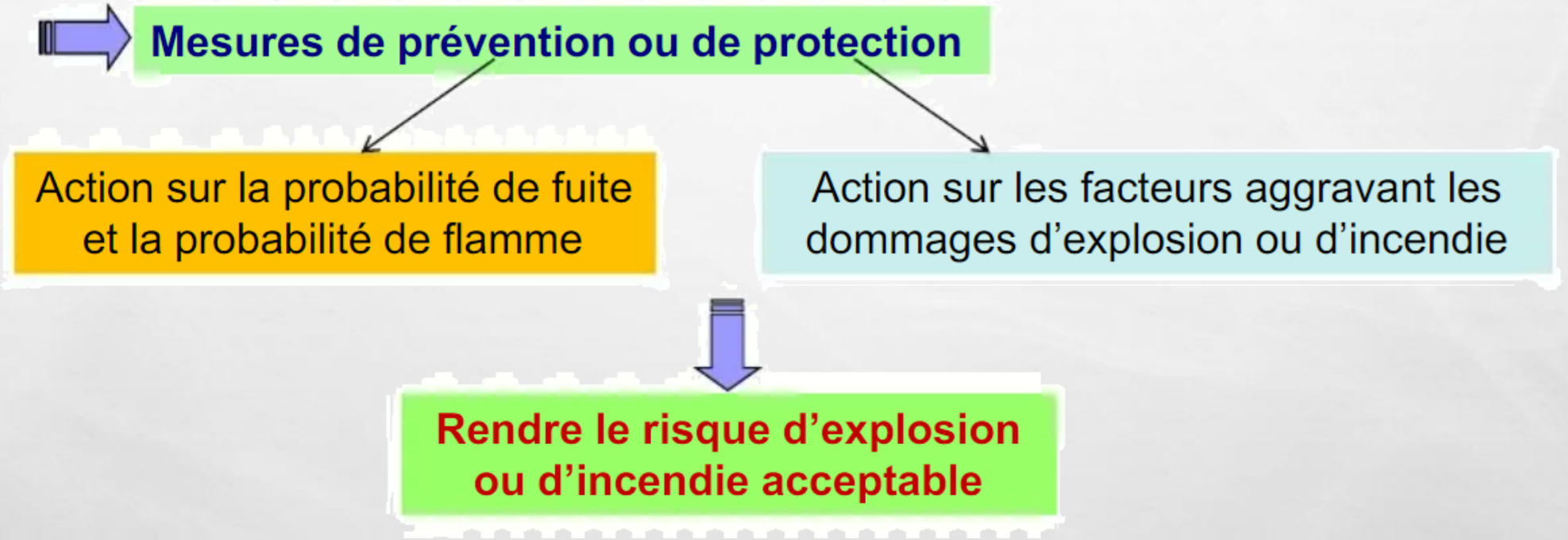

Scénario d'accident
Elément dangereux
Evénement initiateur
Situation dangereuse
Evénement causant un accident
Accident
Stockage de gaz inflammable
+ Fuite
= Dispersion de gaz inflammable
+ Source d'ignition (flamme)
= Incendie ; explosion

Exemple 1 :

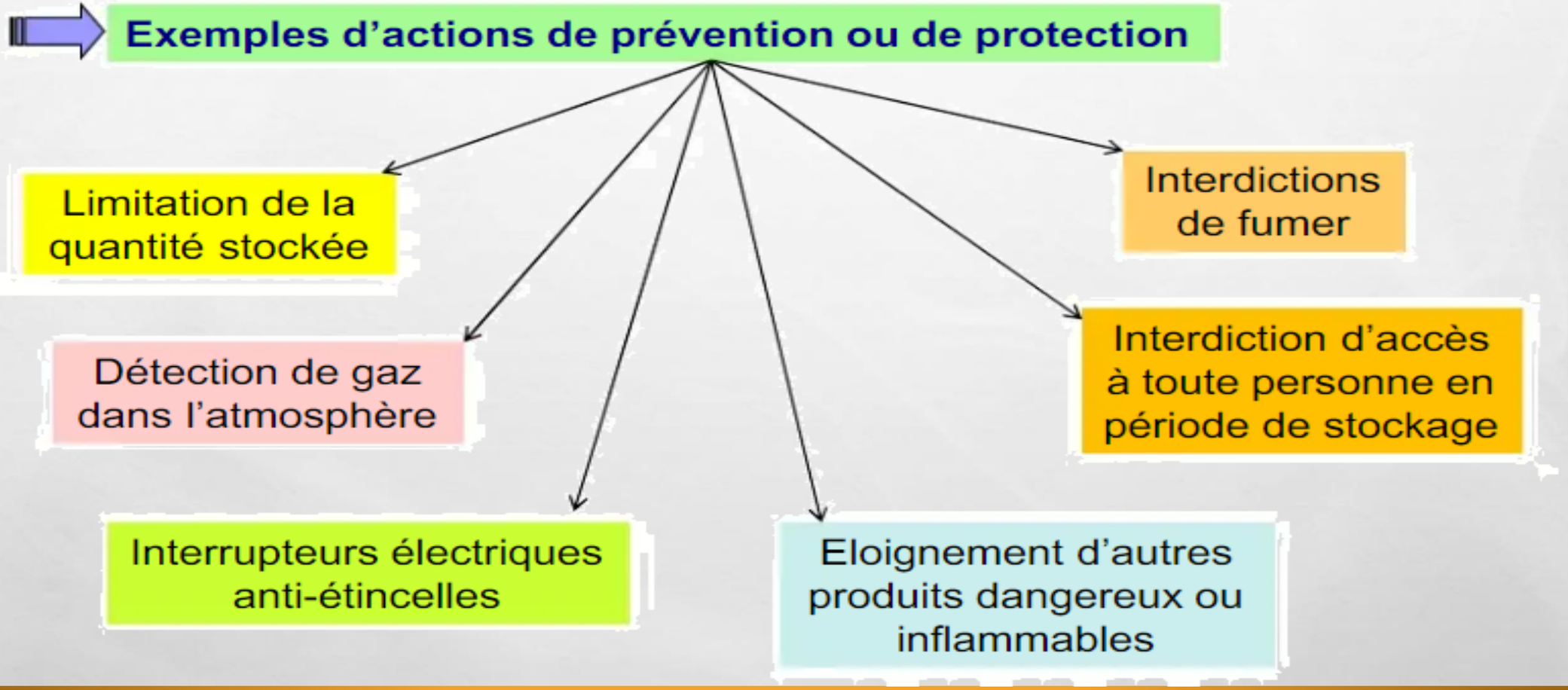
Estimation de la fréquence d'occurrence et de la gravité des conséquences

- Les événements « **fuite** » et « **présence de flammes** » ne peuvent être considérés comme improbables
- La **gravité** de l'**explosion** ou de l'**incendie** dépend de nombreux facteurs : quantité de gaz, confinement, personnes exposées au risque, valeur des biens exposés, …

Exemple 1 :


Mesures de prévention ou de protection
Action sur la probabilité de fuite et la probabilité de flamme
Action sur les facteurs aggravant les dommages d'explosion ou d'incendie
Rendre le risque d'explosion ou d'incendie acceptable

Exemple 1 :


Exemples d'actions de prévention ou de protection
Limitation de la quantité stockée
Détection de gaz dans l'atmosphère
Interrupteurs électriques anti-étincelles
Eloignement d'autres produits dangereux ou inflammables
Interdictions de fumer
Interdiction d'accès à toute personne en période de stockage

Analyse préliminaire des risques APR

Exemple 1 :

1	2	3	4	5	6	7	8	9	10	11	12
Sous-système ou fonction	Phase	Elément dangereux	Evénement Causant une situation dangereuse	Situation dangereuse	Evénement Causant un accident	Accident	Effets	Gravité	Fréqu-ence	Mesures de prévention ou de protection	Application de ces mesures et études complém-entaires
Stockage de gaz inflammable	Rempl-issage Fonct. normal	Réservoir (gaz) Réservoir (gaz)	Surrempl-issage - Fuite - Séisme	Surpressi-on au niveau du réservoir) Dispersion Du gaz	Mauvaise conception - Flamme - Point chaud	Explosion Incendie Explosion Incendie Intoxication		4 4	Ne joue pas un rôle important dans l'APR	-SISs -Limitation de la quantité de gaz -Entretient du réservoir	-Etude des SIS selon la CEI 61508 -Etude des causes de fuite et de surempliss age,…

Autre exemple d'un tableau APR

Fonction ou système :						Date :	
1	2	3	4	5	6	7	8
N°	Produit ou équipement	Situation de danger	Causes	Conséquences	Sécurités existantes	Propositions d'amélioration	Observations
	Réservoir (gaz)	- Surpressi-on au niveau du réservoir) - Dispersion Du gaz	Surrempl-issage - Fuite - Séisme	Explosion Incendie Explosion Incendie Intoxication	- PRV - DR Détecteur de gaz	SIS SIS	-Etude des SIS selon la CEI 61508 -Etude des causes de fuite et de suremplissage,...

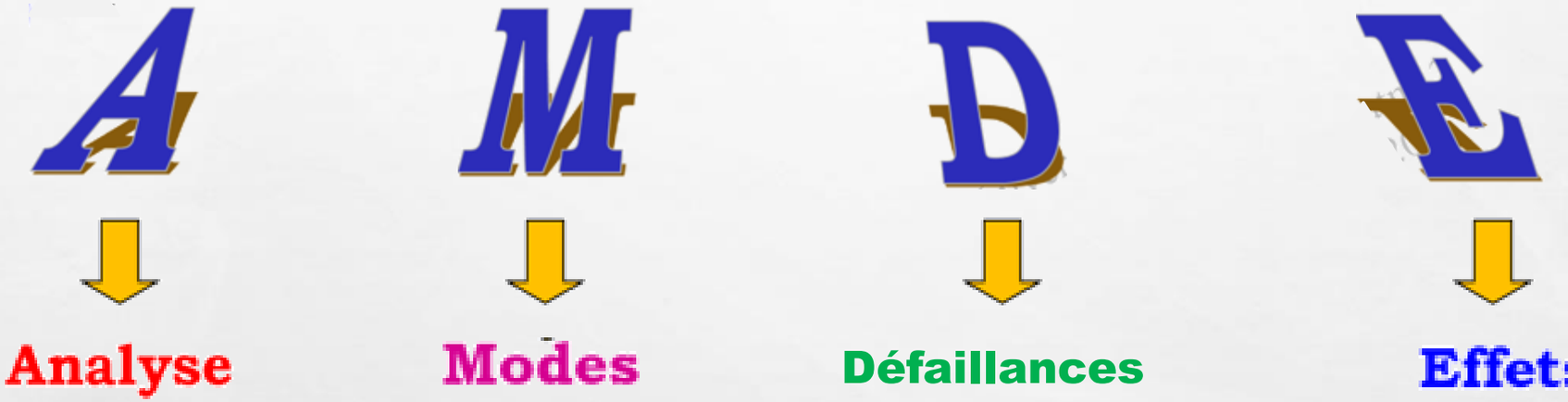
Exemple 2 : Stockage d'hydrocarbures

Phase	Entité dangereuse	Événement causant une situation dangereuse	Situation dangereuse	Événement causant une	Accident potentiel
Stockage	Mare de carburant au voisinage d'un bac de stockage	Source d'inflammation	Feu externe du bac	Feu non maitrisé	Incendie au niveau du bac de stockage

Un accident potentiel

Etude AMDEC

A propos de l'AMDEC

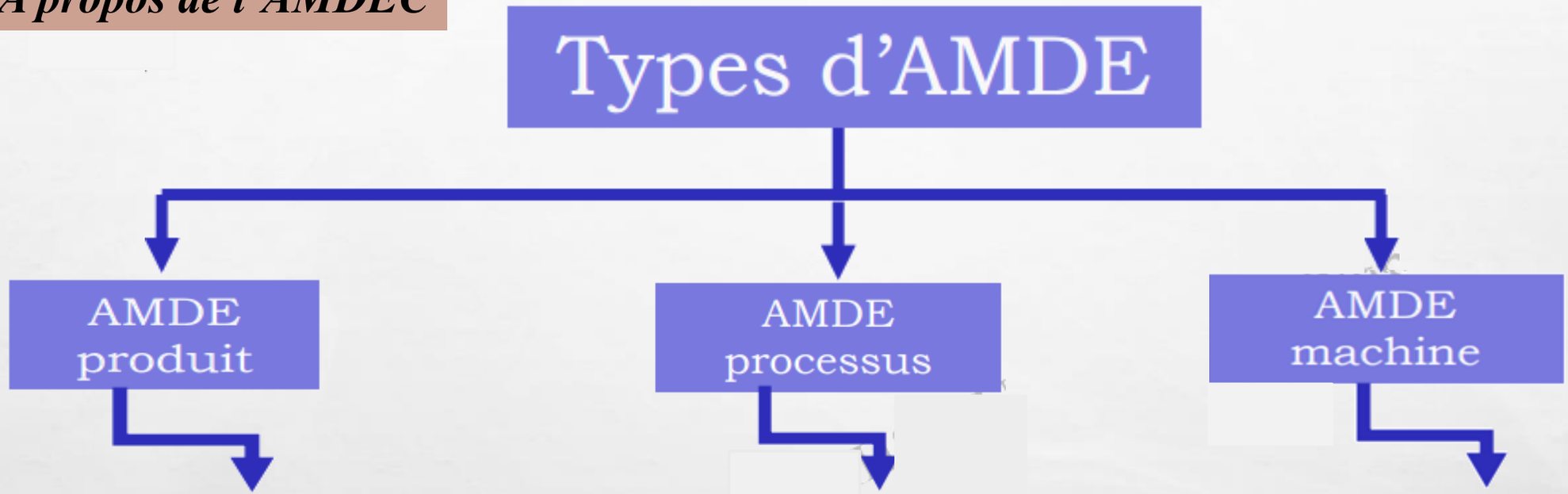


Manière dont se manifeste une défaillance

Cessation de l'aptitude d'une entité à accomplir une fonction donnée dans des conditions données

Conséquences

A propos de l'AMDEC



Analyse de la conception d'un produit pour améliorer la qualité et la fiabilité de celui-ci.

Analyse des opérations de production pour améliorer la qualité de fabrication du produit.

Analyse de la conception et/ ou de l'exploitation d'un moyen ou équipement de production pour optimiser sa sécurité.

RQ: Il à noter que l'AMDEC a été adaptée à l'étude des dysfonctionnements des logiciels, des dérives et violations de l'homme, l'analyse du risque environnemental…

Principe de base et étapes de l'AMDEC

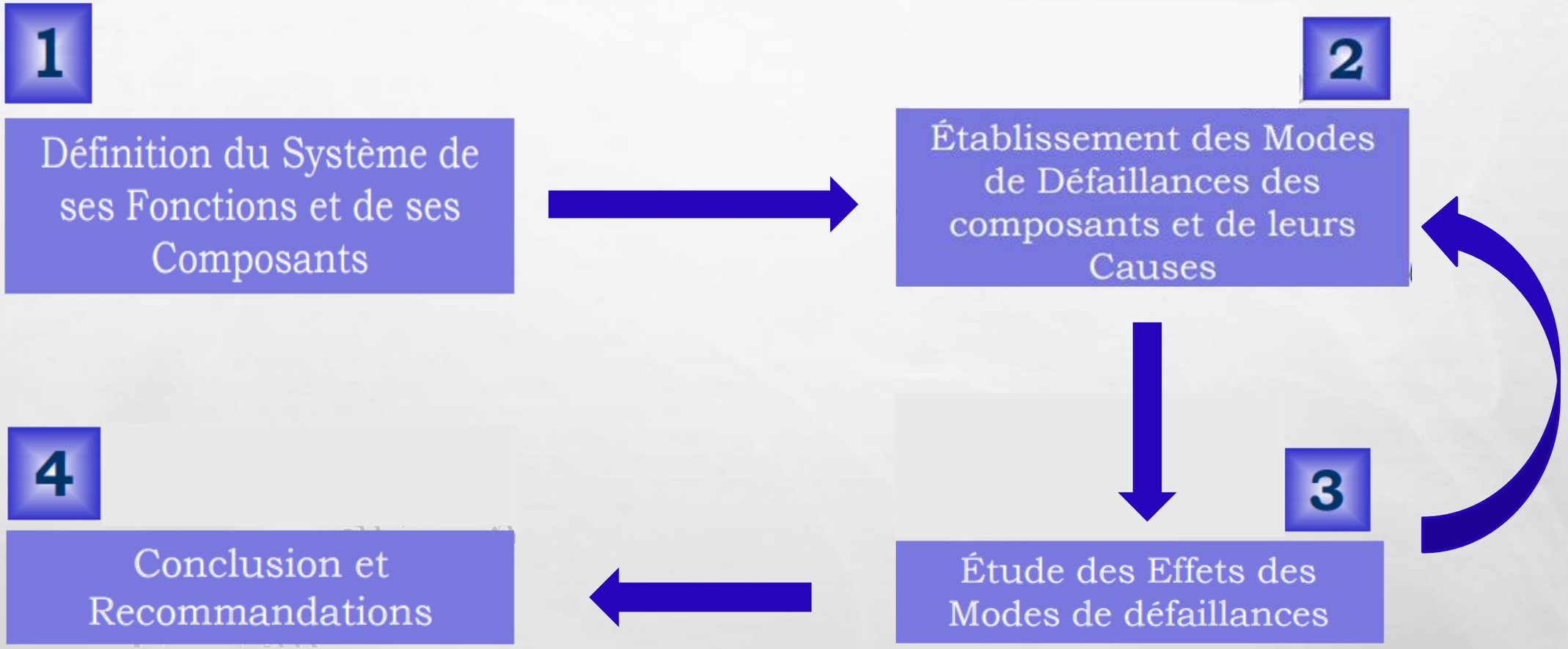
Démarche inductive : causes ⟶ effets

Démarche qualitative : identification des modes de défaillances

Consiste à :

- Identifier les dysfonctionnements potentiels (modes de défaillance),
- Rechercher les origines des dysfonctionnements (causes de défaillances),
- Identifier les conséquences de dysfonctionnement (effets).

Principe de base et étapes de l'AMDEC



RQ: AMDE est réalisée pour un état de fonctionnement donnée

Principe de base et étapes de l'AMDEC - MdD

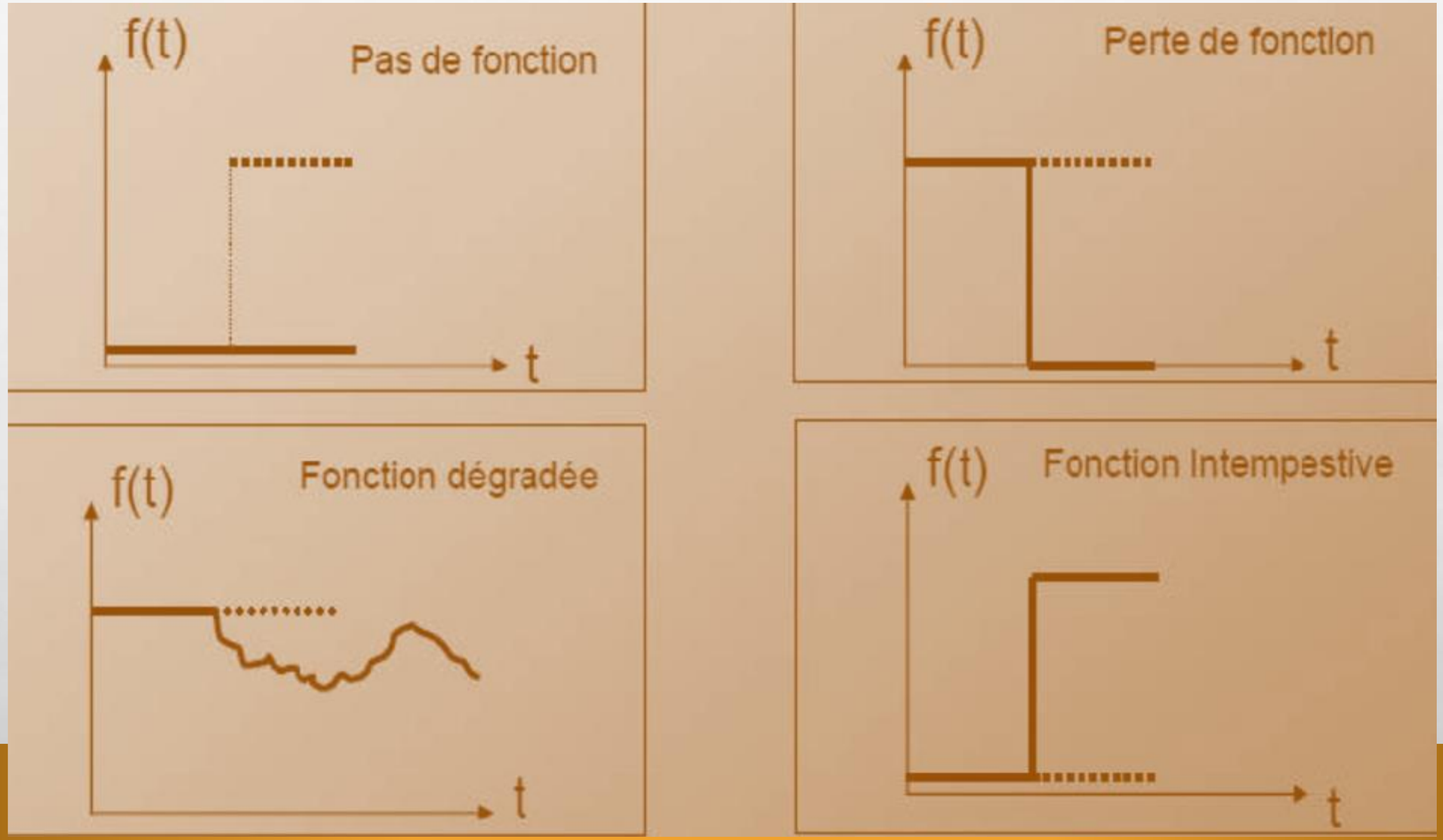
Le ***recensement*** des ***modes de défaillance*** peut s'appuyer sur les éléments suivants :

- Considérer (a priori) tous **les écarts aux fonctionnements attendus**.
- Utiliser **le retour d'expérience** (propre expérience, bases de données (**OREDA**,…)).
- **Avis d'experts**
- **Essais, tests**,…

On classifie les modes de défaillances en général en quatre catégories normalisées : (**norme NF X 60-510**)

- ❑ **Fonctionnement prématuré (ou intempestif).**
- ❑ **Ne fonctionne pas au moment prévu.**
- ❑ **Ne s'arrête pas au moment prévu.**
- ❑ **Défaillance en fonctionnement (fonctionnement dégradé, perte de la fonction…).**

Principe de base et étapes de l'AMDEC - MdD



Principe de base et étapes de l'AMDEC - MdD

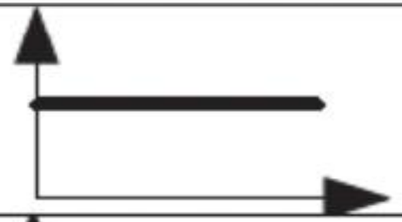
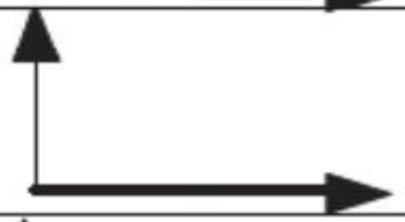
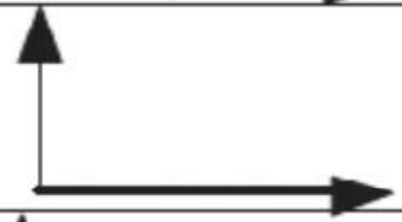
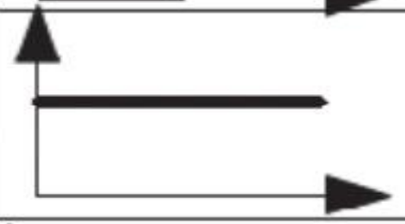
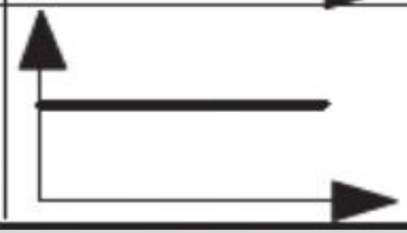
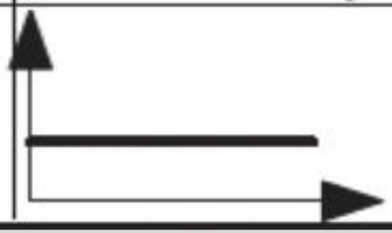
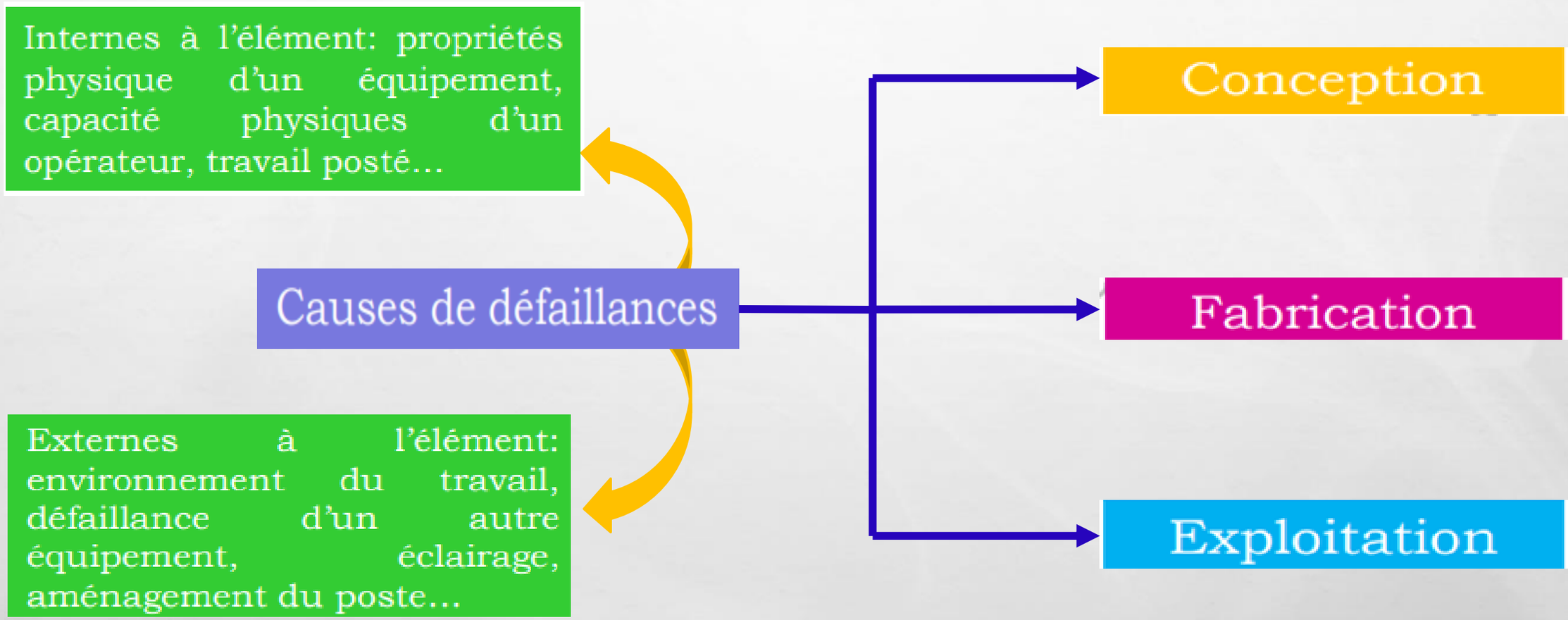
Mode de défaillance génériques	Fonctionnement	
	attendu	réel
Perte soudaine de la fonction (arrêt intempestif)		
Absence de fonction à la sollicitation (refus de démarrer)		
Fonction itempestive (démarrage intempestif)		
Maintien de la fonction sur ordre d'arrêt (refus de s'arrêter)		
Dégradation de la fonction (altération des performances)		

Tableau 4 – Liste de modes de défaillance suivant l'AFNOR	
Modes génériques de défaillance	
1. Défaillance structurelle	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 au-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 fonctionnement et les contraintes opérationnelles
17. Écoulement réduit	

Principe de base et étapes de l'AMDEC – Causes de défaillance



Principe de base et étapes de l'AMDEC – Causes de défaillance

La recherche des ***causes*** se fait ***simultanément*** avec l'identification des ***modes de défaillance***. Il est bien certain qu'un ***même MdD*** peut avoir ***plusieurs causes*** . les ***causes*** peuvent être aussi bien ***internes*** qu'***externes*** :

- ***Causes internes*** : il s'agit des défauts ou défaillances propres au composant.
  - Défaut de conception, de fabrication, …
  - Intrinsèque : usure, grippage, déformation, rupture mécanique, corrosion,…
- ***Causes externes*** : il s'agit des interactions provenant d'autres composants ou de l'environnement du système.

  - Défaillance d'un autre composant : alimentation électrique, air instrument..
  - Mauvaise utilisation : erreur humaine, …
  - Influence de l'environnement : gel, foudre, inondation, neige, vent, …

La recherche des causes peut s'appuyer sur certains outils (ex. ***Ishikawa***)

Principe de base et étapes de l'AMDEC – Causes de défaillance

- Une ***cause de défaillance étant supposée apparue***, le ***mode de détection*** est la ***manière*** par laquelle un ***utilisateur*** (opérateur et/ou mainteneur) ***est susceptible de détecter sa présence avant que le mode de défaillance ne se soit produit complètement***, c'est-à-dire ***bien avant que l'effet de la défaillance ne puisse se produire*** (détection visuelle, température, odeurs, bruits, …).

Principe de base et étapes de l'AMDEC - Effets

Hypothèse : les ***effets*** de chaque mode de défaillance sont ***recherchés*** en ***supposant*** que ***tout le reste du système fonctionne correctement***.

L'AMDEC ne traite que les *défaillances simples (pas de combinaison)*

Les ***effets***, que peut avoir chaque mode de défaillance, doivent être ***recherchés*** par rapport aux ***fonctions attendues du système*** (et de ***ces composants***). Il convient de les rechercher ***le plus loin possible*** (évaluer les effets sur le ou les niveaux supérieurs, jusqu'au niveau le plus haut (système, process, client ...) : il peut exister des ***effets en cascade***. Donc ces effets peuvent concerner :

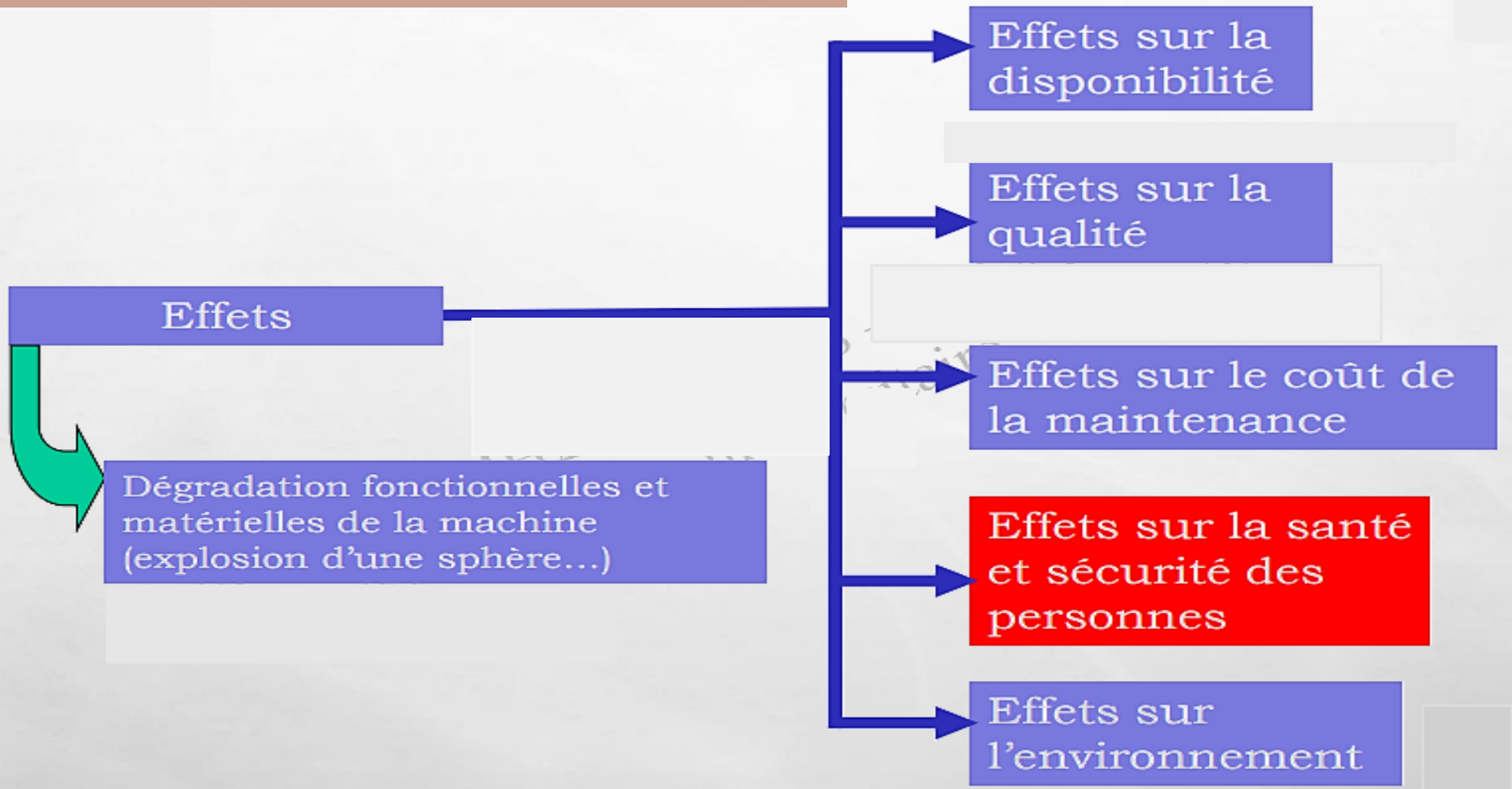
Les fonctions du composant lui-même.
Les fonctions d'autres composants : ***défaillance secondaire***.
Les fonctions du système : arrêt de production, ...

} **Effets locaux**

L'environnement du système : réactions des clients,...
La sécurité du système et de son environnement : accidents,...

} **Effets finals**

Principe de base et étapes de l'AMDEC - Effets



Principe de base et étapes de l'AMDEC

Analyse

Modes

Défaillances

Effets

Criticité

Principe de base et étapes de l'AMDEC

- **Criticité (C)** : l'objet principal de l'évaluation de la ***criticité*** est d'***hiérarchiser*** et donc de ***repérer*** les ***modes de défaillances les plus critiques*** (susceptibles d'entraîner un scenario critique), afin de les ***traiter en priorité***.

- La criticité est une évaluation semi-quantitative du risque constitué par le scénario (mode-cause-effet-détection) de défaillance analysé. Elle est généralement établie à partir de l'estimation et la combinaison de trois paramètres : ***C = f(F, G, ND).***

Principe de base et étapes de l'AMDEC

la Criticité (C) = F X ND X G

F — **Fréquence d'apparition de la défaillance**

ND — **Probabilité de non détection de la défaillance**

G — **Gravité des conséquences de la défaillance**

***RQ**: il est à noter que:*

- ✓ *La formule du risque varie d'un domaine à un autre notamment (Risque professionnels « RP » et Risques industriel « RI ») en terme de paramètres d'évaluation, ainsi pour RP on parle de durée d'exposition , de dose d'exposition…;*
- ✓ *Pour le même domaine (RI ou RP) , la formule du risque varie d'une approche à une autre , cependant le paramètre gravité est un facteur déterminant dans l'évaluation.*

Principe de base et étapes de l'AMDEC – Exemple d'échelle

Tableau 1 – Indice de fréquence *F* (1)	
Valeurs de *F*	**Fréquence d'apparition de la défaillance**
1	**Défaillance pratiquement inexistante** sur des installations similaires en exploitation, au plus un défaut sur la durée de vie de l'installation.
2	**Défaillance rarement apparue** sur du matériel similaire existant en exploitation (exemple : un défaut par an) ou **Composant d'une technologie nouvelle** pour lequel toutes les conditions **sont théoriquement réunies** pour prévenir la défaillance, mais il n'y a pas d'expérience sur du matériel similaire.
3	**Défaillance occasionnellement apparue** sur du matériel similaire existant en exploitation (exemple : un défaut par trimestre).
4	**Défaillance fréquemment apparue** sur un composant connu ou sur du matériel similaire existant en exploitation (exemple : un défaut par mois) ou **Composant d'une technologie nouvelle** pour lequel toutes les conditions **ne sont pas réunies** pour prévenir la défaillance, et il n'y a pas d'expérience sur du matériel similaire.
(1) L'indice de fréquence *F* est établi pour chaque association composant, mode, cause.	

Principe de base et étapes de l'AMDEC – Exemple d'échelle

Tableau 2 – Indice de gravité *G*

Valeurs de *G*	Gravité de la défaillance (1)
1	**Défaillance mineure** : aucune dégradation notable du matériel (exemple : *TI* ⩽ 10 min).
2	**Défaillance moyenne** nécessitant une remise en état de courte durée (exemple 10 min < *TI* ⩽ 30 min).
3	**Défaillance majeure** nécessitant une intervention de longue durée (exemple 30 min < *TI* ⩽ 90 min) ou Non-conformité du produit, constatée et corrigée par l'utilisateur du moyen de production.
4	**Défaillance catastrophique** très critique nécessitant une grande intervention (exemple *TI* > 90 min) ou Non-conformité du produit, constatée par un client aval (interne à l'entreprise) ou Dommage matériel important (sécurité des biens).
5	**Sécurité/Qualité** : accident pouvant provoquer des problèmes de sécurité des personnes, lors du dysfonctionnement ou lors de l'intervention ou Non-conformité du produit envoyé en clientèle.

(1) L'effet de la défaillance s'exprime en termes de durée d'arrêt, de non-conformité de pièces produites, de sécurité de l'opérateur.
TI : temps d'interruption.

Principe de base et étapes de l'AMDEC – Exemple d'échelle

Tableau 3 – Indice de non-détection *D* = *ND*	
Valeurs de *D*	**Non-détection de la défaillance (1)**
1	Les dispositions prises assurent une **détection totale** de la cause initiale ou du mode de défaillance, permettant ainsi d'éviter l'effet le plus grave provoqué par la défaillance pendant la production.
2	Il existe un signe avant-coureur de la défaillance mais il y a risque que ce signe ne soit pas perçu par l'opérateur. La **détection est exploitable**.
3	La cause et/ou le mode de défaillance sont difficilement décelables ou les éléments de détection sont peu exploitables. La **détection est faible**.
4	Rien ne permet de détecter la défaillance avant que l'effet ne se produise : il s'agit du cas **sans détection.**
(1) Signes avant-coureurs : bruit, vibration, accélération, jeu anormal, échauffement, visuel...	

Principe de base et étapes de l'AMDEC – Exemple d'echelle

F	FREQUENCE
1	**Très faible taux d'apparition.** **Moins de une défaillance par ans**
2	**Faible taux d'apparition.** **Moins de une défaillance par trimestre**
3	**Taux d'apparition modéré.** **Moins de une défaillance par Semaine.**
4	**Taux d'apparition élevé.** **Plusieurs défaillances par semaine.**

Fréquence d'exposition au danger	Facteur Kinney
Permanent ou continu	10
Fréquent (plusieurs fois par jour)	8
Quotidiennement (1 fois par jour)	6
Régulièrement (quelques fois par semaine)	4
Occasionnellement (1 fois par semaine)	3
Souvent (1 fois par mois ou plusieurs fois par an)	2
Rarement (une ou quelques fois par an)	1
Très rarement (moins qu'une fois par an)	0,5

Principe de base et étapes de l'AMDEC

Gravité / Probabilité	MORTEL (25)	CRITIQUE (20)	GRAVE (15)	IMPORTANTE (10)	MINEURE (5)
TRÈS PROBABLE (5)	125	100	75	50	25
PROBABLE (4)	100	80	60	40	20
POSSIBLE (3)	75	60	45	30	15
PEU PROBABLE (2)	50	40	30	20	10
IMPROBABLE (1)	25	20	15	10	5

1	*Faible*	*Accident ou maladie sans arrêt de travail*
2	*Moyenne*	*Accident ou maladie avec arrêt de travail*
3	*Grave*	*Accident ou maladie avec incapacité permanente partielle*
4	*Très grave*	*Accident ou maladie mortel*

Gravité des dommages potentiels

G	GRAVITE
1	Arrêt de production inférieur à 2 minutes. Aucune dégradation notable du matériel.
2	Arrêt de production de 2 à 20 minutes. Remise en état de courte durée. Déclassement du produit.
3	Arrêt de production de 20 à 60 minutes. Changement du matériel défectueux nécessaire. Retouche du produit nécessaire ou rebut
4	Arrêt de production de 1 à 2 heures. Intervention importante sur sous-ensemble. Production de pièces non conformes non détectées
5	Arrêt de production supérieur à 2 heures. Intervention lourdes nécessitant des moyens coûteux. Problème de sécurité du personnel ou d'environnement

Principe de base et étapes de l'AMDEC - Mesures correctives

La ***valeur de la criticité*** est ensuite ***comparée*** aux ***valeurs des critères d'acceptabilité (seuils)*** définis préalablement par le groupe de travail. Dès lors que la criticité dépasse le ***seuil prédéfini (existence d'un point critique)***, la ***défaillance analysée*** fera l'objet d'une ***action corrective***.
Attention : une criticité égale à 3*2*4 = 24 doit être interprétée et traitée différemment d'une criticité égale à 4*2*3 = 24

Dans la ***définition*** des ***mesures correctives***, on doit ***tenir compte*** des ***valeurs des différents paramètres*** **(F, G, ND) :**

- **Prévention :** visant à diminuer la fréquence d'apparition des modes de défaillance en agissant sur leurs causes : modification de la conception, redondance, entretient,…
- **Détection :** visant à empêcher la réalisation des effets : alarmes, tests périodiques, ..
- **Protection :** visant à limiter l'effet de la défaillance : réduction des MTTR,…

Principe de base et étapes de l'AMDEC - Mesures correctives

la Criticité (C) = F X ND X G

En agissant sur les causes de défaillances: action préventives

En améliorant les moyens de détection

En agissant sur les conséquences: action de protection

la conception

L'exploitation

Le choix de la maintenance

Principe de base et étapes de l'AMDEC – **Représentation**

L'***AMDEC*** est ***formalisée*** par un ***tableau*** dont les ***colonnes représentent les étapes de son déroulement***.

Attention : L'AMDEC n'est pas un ***formulaire (tableau) à remplir***. Le tableau permet seulement de ***formaliser la réflexion*** et de ***présenter les résultats*** de l'analyse.

Il n'existe pas de tableau AMDEC standard. Il doit au minimum avoir la forme suivante :

Tableau 1 – Analyse des modes de défaillance, de leurs effets et de leur criticité

Date : Version : Analyste :

Système étudié :

Composant	Mode de défaillance	Effets	Criticité

Au sens de gravité (G)

Principe de base et étapes de l'AMDEC - Représentation

En fonction des ***objectifs de l'analyse***, ***d'autres colonnes peuvent apparaître***.

Tableau AMDEC selon la norme MIL-STD 1629A

Système .....
Niveau de décomposition .....
Référence du schéma .....
Mission .....

ANALYSE DES MODES DE DÉFAILLANCE ET DE LEURS EFFETS

EXEMPLE N° 2 MIL STD 1629 A

Numéro d'identification de l'équipement	Fonction	Repère	Mode de défaillance	Cause de défaillance	Effet de défaillance		Détection de la défaillance	Dispositifs de remplacement	Probabilité de défaillance	Niveau de criticité	Remarques
					Effet local	Effet final					

Tableau AMDEC selon le CETIM

© AMDEC CETIM	ANALYSE DES MODES DE DÉFAILLANCE DE LEURS EFFETS ET DE LEUR CRITICITÉ										AMDEC MACHINE
	SYSTÈME..... SOUS-SYSTÈME			PHASE DE FONCTIONNEMENT :			DATE DE L'ANALYSE :				.....Page
Élément	Fonction	Mode de défaillance	Cause	Effet	Détection		TI	Criticité				Action corrective
								F	G	N	C	

Principe de base et étapes de l'AMDEC - **Représentation**

Projet	**ANALYSE DES MODES DE DEFAILLANCES DE LEURS EFFETS ET DE LEUR CRITICITE**									Type **AMDEC**
	Système: **Sous-système:**				**Phase de fonctionnement**					
Élément	**Fonction**	**Mode de défaillance**	**Causes de défaillance**		**Effet**		**Détection**	**Criticité**		**Actions correctives**
			Int	**Ext**	**L**	**G**		**F**	**G**	**N**	**C**

Principe de base et étapes de l'AMDEC - Exemple

Exemple d'une analyse AMDEC

D'après la norme CNOMO E41.50.530.N Édition juin 1994	**AMDEC - Moyen de production**													Folio /				
Fournisseur : Bonne machine **Système** : Four **Sous-système** : Mise en position			**Rédacteur** : J. Durand **Service** : Fiabilisation **Date** : 11 sept. 1997 **Réf** :			**Criticité Indices nominaux**					**Actions correctives**			**Criticité Indices finaux**				
Compo-sant	Fonctions	Modes de défaillance	Causes	Effets	Détection	*TI*	*F*	*G*	*D*	*C*		Actions	Resp./ Délai	*TI'*	*F'*	*G'*	*D'*	*C'*
Vérin du four	Fournir l'énergie mécanique à la mise en position du four	Fuite externe	Raccords desserrés	Plus de mouvement	Bruits	10'	1	1	3	3								
			Flexible percé	Plus de mouvement	Bruits	30'	1	2	3	6								
			Joint de tige usé	Plus de mouvement	Bruits	60'	1	3	4	12	CM	Déterminer durée de vie pour changement périodique	Maint	60'	1	3	1	3
			Tige rayée (marquée)	Plus de mouvement	Visuel	60'	1	3	3	9								
		Fuite interne	Mauvaise qualité air	Plus de mouvement	Sans	60'	1	3	4	12	CM	Contrôler groupe de conditionnement d'air 1 fois/mois	Maint	60'	1	3	1	3
			Fin de vie joint intérieur	Plus de mouvement	Sans	60'	1	3	4	12	CM	Déterminer durée de vie pour changement périodique	Maint	60'	1	3	1	3
Rotule avant	Permettre la rotation du levier 1 et permettre l'alignement du vérin	Grippée	Manque graissage	Plus de mouvement	Sans	45'	1	4	3	12	CM	Mettre en place rotule lubrifiée à vie	Maint	45'	1	4	1	1
			Échauffement	Plus de mouvement	Chaleur	45'	2	4	4	32	CM	Empêcher la remontée de chaleur par convection	Maint	45'	1	4	1	4
			Fin de vie	Plus de mouvement	Sans	45'	1	4	4	16	CM	Déterminer durée de vie pour changement périodique	Maint	45'	1	4	1	4
Axe 1		Grippé	Manque graissage	Plus de mouvement	Sans	45'	1	4	3	12	CM	Mettre en place rotule lubrifiée à vie	Maint	45'	1	4	1	1
			Échauffement	Plus de mouvement	Chaleur	45'	2	4	4	32	CM	Empêcher la remontée de chaleur par convection	Maint	45'	1	4	1	4
			Fin de vie	Plus de mouvement	Sans	45'	1	4	4	16	CM	Déterminer durée de vie pour changement périodique	Maint	45'	1	4	1	4

Exemples d'application de l'AMDEC

Causes → **Mode** → **Effet**

Exp 1

La pluie

Mauvaise adhérence

Accident

Exp 2

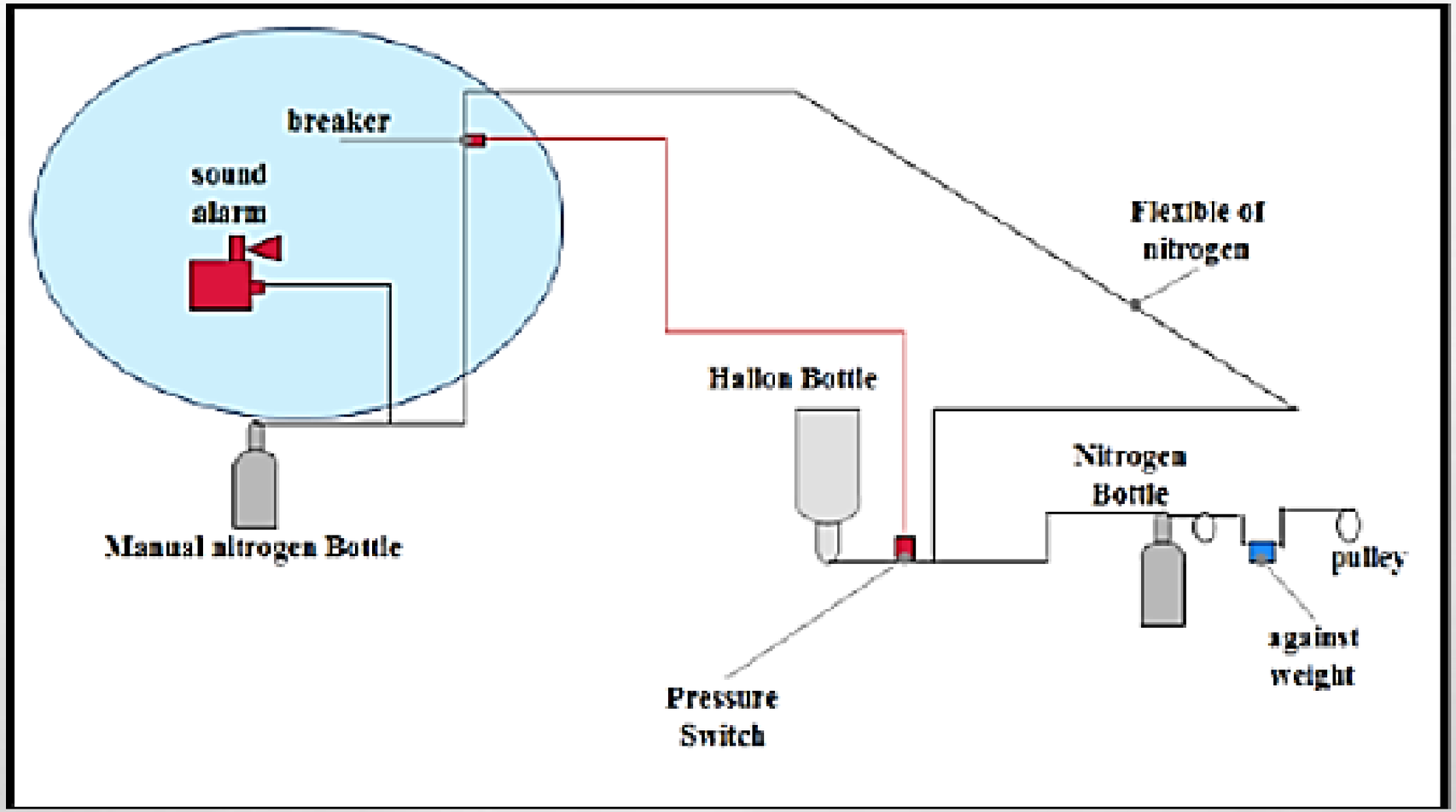
- **Matière première de mauvaise qualité**
- **Production excessive**

- **Mauvaise soudure**
- **Mauvais contrôle**

Exemples d'application de l'AMDEC

Nous considérons dans cette exemple un système d'extinction par HALLON (1211, BCF). Les fusibles sont reliés entre eux par un câble en acier Inoxydable, la rupture des fusibles sous l'effet de la température (90 °C) agira sur les contrepoids suspendus sur poulie et installés sur un support. Ces contrepoids tireront alors sur le câble et agiront sur l'ouverture de la vanne de la bouteille d'azote qui assure le déclenchement de l'ensemble de l'installation, c'est-à-dire l'extinction avec la bouteille d'Halon, le pressostat convertit la pression en énergie électrique, ce système étant relié d'une par au tableau de signalisation et d'autre part à un tableau d'alarme au niveau de la salle de contrôle.

Principe de base et étapes de l'AMDEC - Exemple



Principe de base et étapes de l'AMDEC - Exemple

METHODE AMDE SUR LE SOUS SYSTEME S3 (SYSTEME DE SIGNALISATION)

Identification du composant	Fonction	Mode de défaillance	Cause possible d'une défaillance	Effet sur le système
pressostat	Transformation de la pression d'azote en un signal électrique	Fonction intempestif	DM (défaut interne) Usure Dépôts de poussiers	Pas de signal Signal en retard
Vérin du coffret d'alarme	tourne pour donner le signale a la sirène	Blocage en position	DM (Défaut mécanique)	Pas de signal
Sirène	Alarme sonore	Pas d'alarme	DM (Défaut mécanique) Pas de signal d'arrivée	Signalisation incomplète Pas d'alerte
		Fonctionnement intempestif	DM (défaut mécanique) usure	

LES ARBRES DES DÉFAILLANCES TRAITÉS À L'AIDE DU LOGICIEL GRIF

2016 – 2017

1. Introduction
2. Construction d'un AdD
3. Exploitation qualitative d'un AdD
4. Exploitation quantitative d'un AdD

Dénominations

- Arbre des Défaillances (AdD)
- Arbre des pannes
- Arbre des fautes
- Fault Tree (FT) Analysis (FTA)

CEI 61025

Introduction

Bref historique

- L'**AdD** a été à l'origine développée en **1962** aux **BELL Laboratories** par **H.A. Watson**, pour évaluer le Système de commande de Lancement du missile intercontinental **Minuteman**.

- **Boeing** a commencé à utiliser les AdD pour la conception **d'avions civils** vers **1966**.

- **1981** (suite a l'accident de **Three Mile Island**): publication du manuel sur les AdD intitulé ***NRC Fault Tree Handbook* (NUREG-0492).**

- Bases de l'évaluation quantitative (Vesely, 1970) : Kinetic Tree Theory (KITT).

- Diagrammes de décision binaires ou DDB (Coudert, Madre, ***Rauzy*** ; 1992).

Introduction

Définition et principe

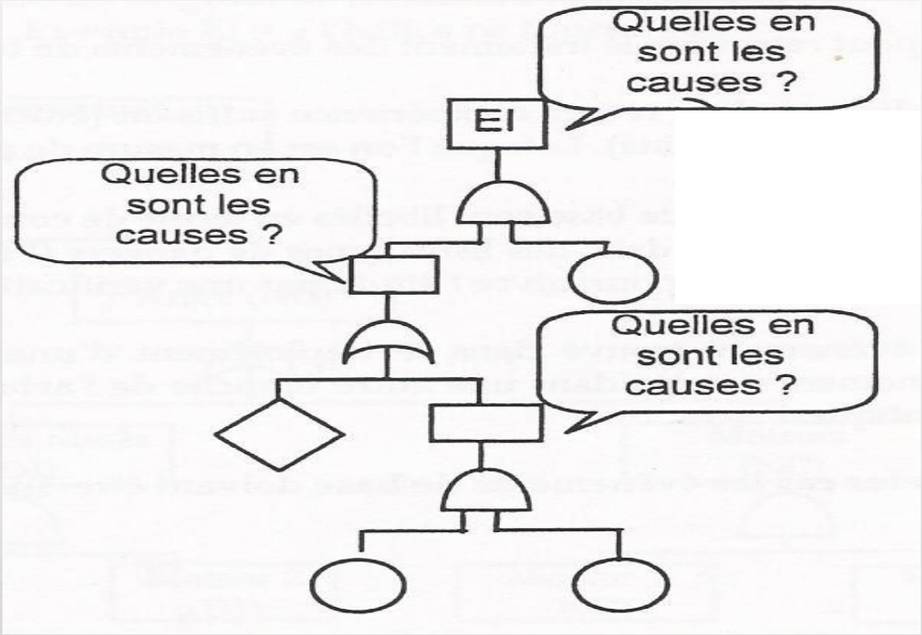
- Méthode de *représentation graphique de la logique de dysfonctionnement* d'un système. Elle utilise une *symbolique graphique* particulière qui permet de présenter les résultats dans une *structure arborescente*.

- Méthode *déductive* (Top-Down) : considère un *événement redouté (indésirable, sommet)* (**ER**) ou (*conséquences, effets*) (ex.: arrêt de production, explosion…) dont elle cherche à expliquer les *causes* possibles: e_i *(événements élémentaires).*

Introduction

Définition et principe

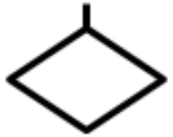
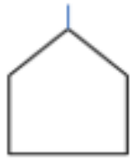
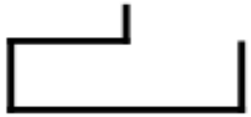
- Méthode de détermination des ***scénarios*** (combinaisons d'événements «élémentaires») conduisant à la réalisation d'un **ER** engendré par le système étudié. Les liens entre les différents évènements identifiés sont réalisés grâce à des ***portes logiques*** (de type « ET » et « OU » par exemple).



- Méthode de ***quantification de l'occurrence*** de l'ER considéré.

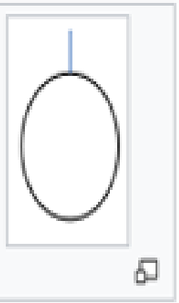
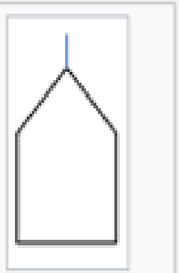
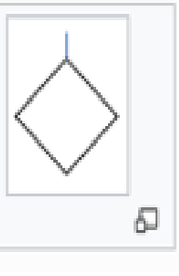
Introduction

Conventions graphiques

Evénement / report	Dénomination	Portes	Dénomination
	Evénement de base		Porte « ET »
	Pseudo-événement de base		Porte « OU »
	Evénement maison		Porte « OU exclusif »
	Evénement-sommet ou événement intermédiaire		Porte « combinaison »
	Report (sortie) Le sous-arbre situé sous ce « drapeau » est à dupliquer …		Porte « NON-OU »
	Report (entrée) … à l'endroit indiqué par ce second drapeau		Porte « NON-ET »

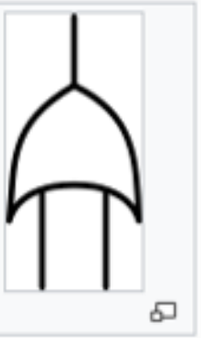
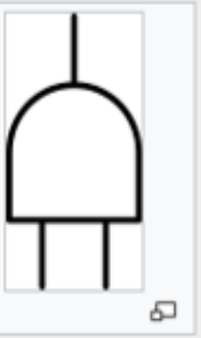
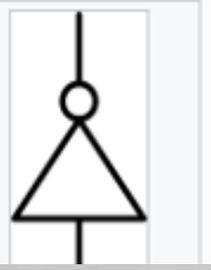
Introduction

Conventions graphiques

Symbole	Nom	Description
	Événement de Base	Événement du plus bas niveau pour lequel la probabilité d'apparition ou d'information de fiabilité est disponible
	Événement maison	Événement qui doit se produire avec certitude lors de la production ou de la maintenance. On peut aussi le définir comme un événement non-probabilisé, que l'on doit choisir de mettre à 1 ou à 0 avant tout traitement de l'arbre. Ce type d'événement permet d'avoir plusieurs variantes d'un arbre sur un seul dessin, en modifiant la logique de l'arbre selon la valeur choisie par l'utilisateur.
	Événement non développé	Le développement de cet événement n'est pas terminé, soit parce que ses conséquences sont négligeables, soit par manque d'information

Introduction

Conventions graphiques

Symbole	Nom	Description
	OU (OR)	L'événement de sortie apparaît si au moins un des événements d'entrées apparaît
	ET (AND)	L'événement de sortie apparaît si tous les événements d'entrées apparaissent
	NON (NOT)	L'événement de sortie apparaît si l'événement d'entrée n'apparaît pas. L'état logique de la sortie est l'inverse de celui d'entrée

Introduction

Conventions graphiques

	OU Exclusif (XOR)	L'événement de sortie apparaît si un seul événement d'entrée apparaît
	VOTE MAJORITAIRE	L'événement de sortie apparaît si au moins k événements d'entrées apparaissent

Champ d'application

❑ ***Pas de véritables contraintes limitant :***

- ✓ son pouvoir de ***modélisation*** (logique de dysfonctionnement),
- ✓ son aptitude à être exploité ***qualitativement*** :
  - portes séquentielles, libellé étendu des événements, …
  - allocation d'objectifs qualitatifs.

❑ Mais, une ***limitation drastique*** de sa capacité ***d'évaluation quantitative*** due au respect de la condition ***d'indépendance des événements de base.*** Cette indépendance doit se vérifier au niveau :

- ✓ des ***défaillances*** (redondance passive),
- ✓ des ***réparations*** (nombre de réparateurs disponibles),
- ✓ de ***la mission*** (fiabilité).

Construction de l'ADD

Types de construction

- Procédure *manuelle directe*
- Procédure *manuelle indirecte*
- Procédure *automatique*

Règles de base

❑**Règle1** : ***Libellé explicite*** : écrire explicitement le libellé de tous les événements (notamment celui de l'événement sommet).

▪**Remarque** : l'utilisation préalable de méthodes inductives (APR, AMDEC, HAZOP) permet d'identifier les évènements qui méritent d'être retenus pour une analyse par arbre des défaillances.

Exemples:

- Rejet à l'atmosphère de produits toxiques ou inflammables
- Incendie
- Explosion
- échec d'une mission (défaillance d'un système de sécurité ou d'un système de production, …)

Construction de l'ADD

Règles de base

❑ **Régle 2** : ***Cause (s) immédiate(s)*** : rechercher systématiquement les causes immédiates, nécessaires et suffisantes de chaque événement à développer.

1. Evénement intermédiaire type-composant : la vanne reste ouverte,
2. Evénement intermédiaire type-système : le système d'alimentation ne s'arrête pas (alimentation continue), …

❑ **Régle 3** :

- **Composant** ⇒ Evénement du type-composant ⇒ 

Associer automatiquement à chaque événement intermédiaire de type-composant une porte **OU** doté au plus de trois entrées:

1. défaillance primaire du composant : vanne bloquée ouverte, …
2. défaillance secondaire : agression extérieure, erreur humaine, …
3. défaut de commande : la vanne n'a pas reçu de signal de fermeture, pas d'alimentation électrique, …

Construction de l'ADD

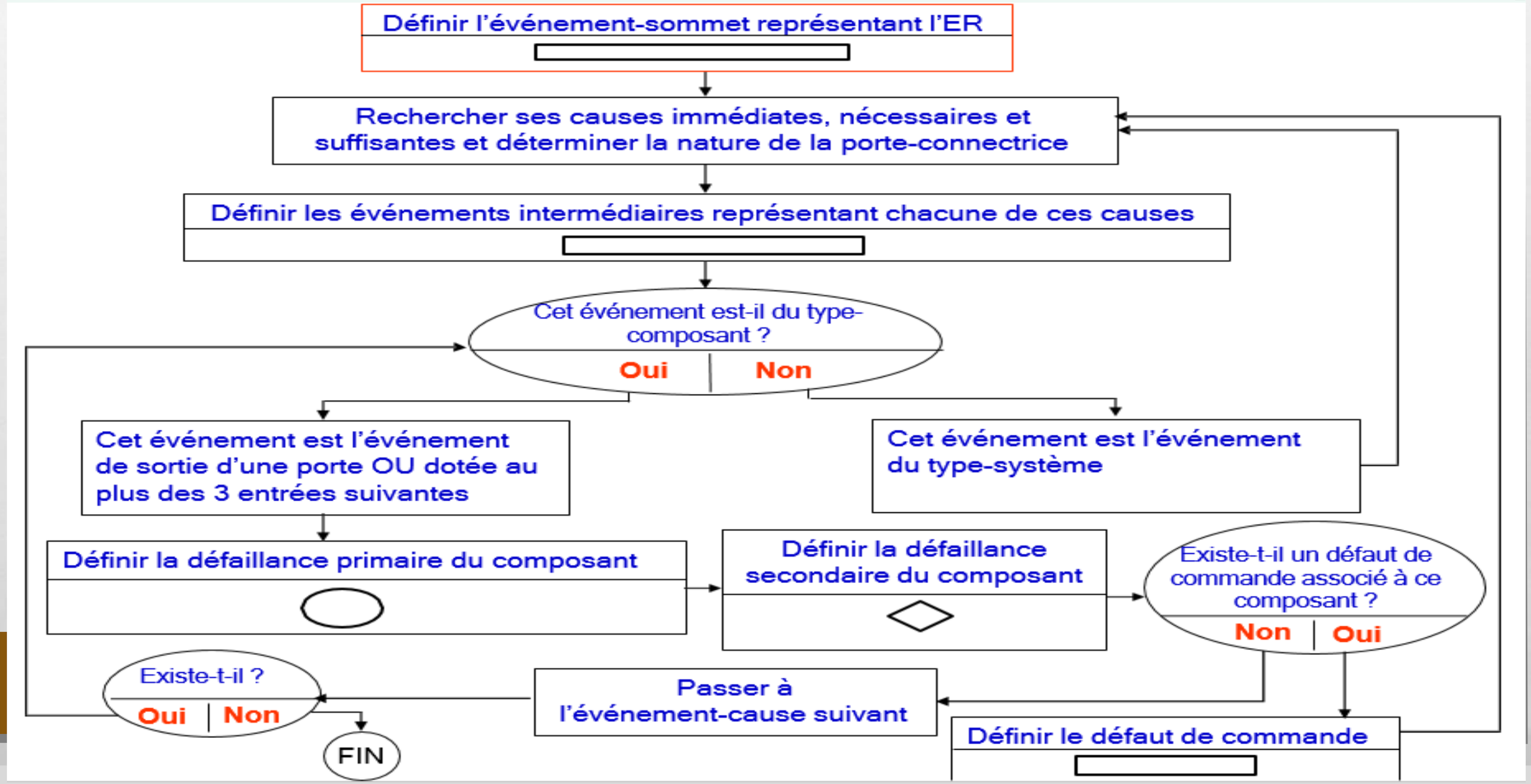
Règles de base

- **Système** → Evénement du type-système → Type de porte

❑ **Règle 4** : ***Pas de porte à porte*** : ne pas oublier d'associer à chaque porte un événement de sortie.

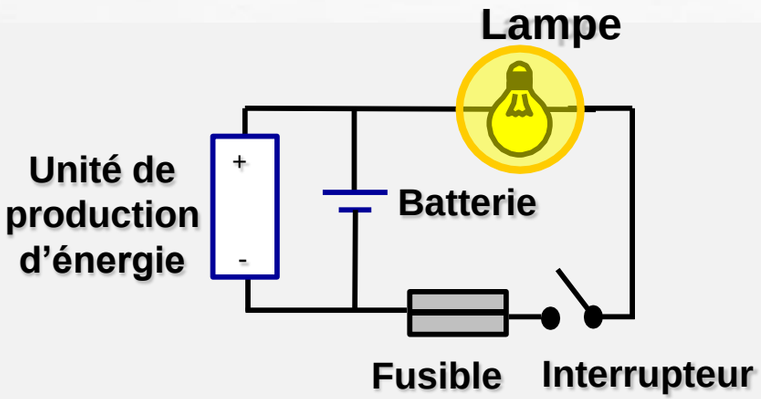
Construction de l'ADD

Construction manuelle



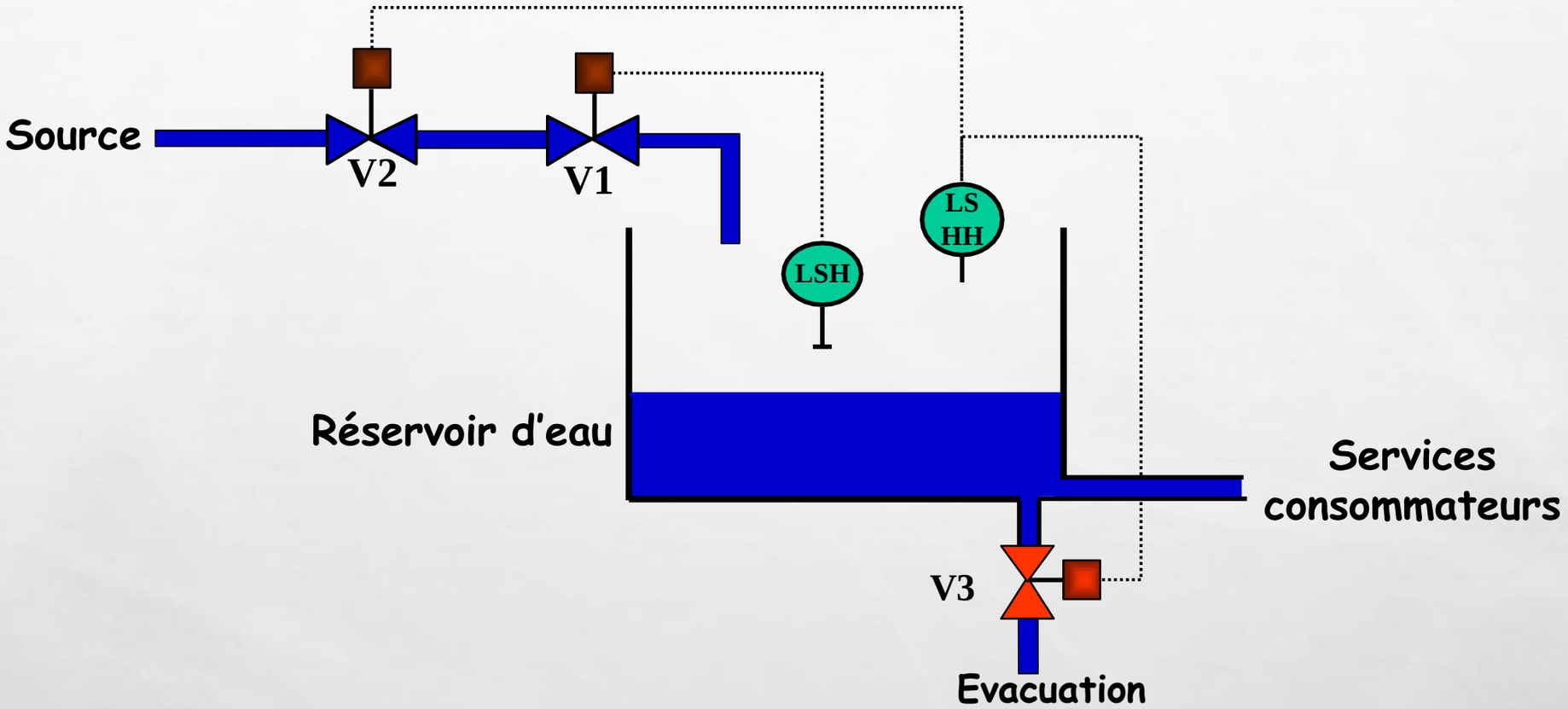
Construction de l'ADD

Construction manuelle : Exemple 1 (circuit électrique)



Construction de l'ADD

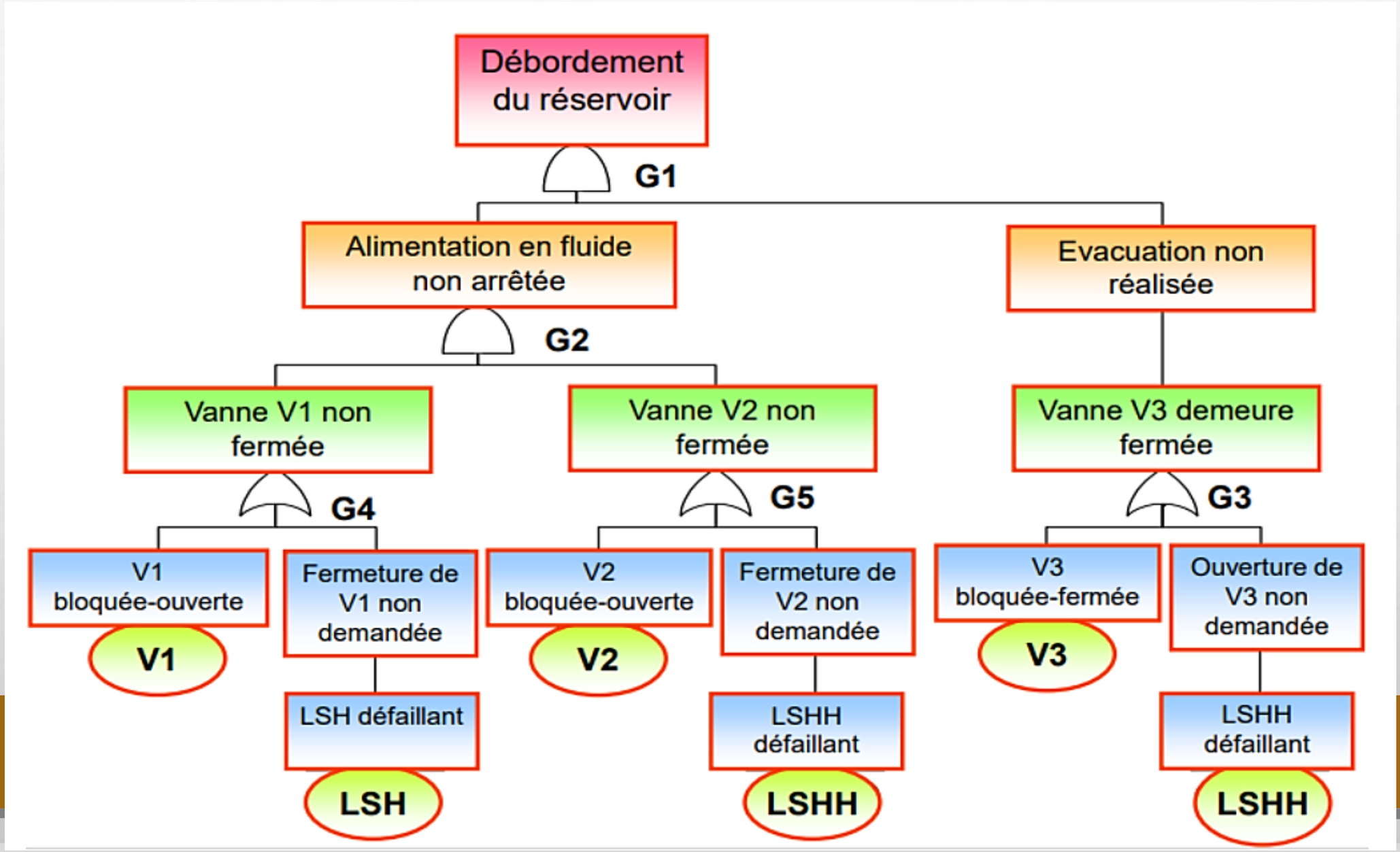
Construction manuelle : Exemple 2 (Réservoir d'eau)



L' alimentation du réservoir en eau est assurée par une source supposée inépuisable et une canalisation dont le débit est commandé par l'ouverture ou la fermeture des vannes automatiques V1 et V2. Durant le remplissage, la vanne automatique V3 demeure fermée. Le débit qu'elle autorise est supérieur à celui des vannes V1 et V2. Lorsque le niveau haut est atteint, il est détecté par le capteur LSH (Level Switch High) qui commande alors la fermeture de V1. Si cete séquence venait à échouer, le niveau d'eau continuerait de monter dans le réservoir jusqu'à atteindre sa valeur limite qui serait détecée par le second capteur LSHH (Level Switch High High). Celui-ci commanderait aussitôt la fermeture de V2 et, par mesure de sécurité, l'ouverture de V3 qui permettrait l'évacuation du trop-plein vers un bassin de rétention de grande capacité.

Construction de l'ADD

Construction manuelle : Exemple 2 (Réservoir d'eau)



Construction de l'ADD

Construction manuelle indirecte : Etapes

- Cette procédure est basée sur l'analyse fonctionnelle du système étudié. Elle se décompose en trois étapes :

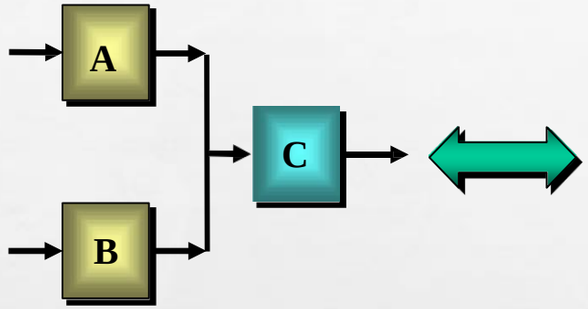
  - ✓ Modélisation du ***fonctionnement attendu*** du système étudié. Cette modélisation privilégie la représentation des ***liaisons fonctionnelles*** entre composants sous la forme de ***diagrammes-blocs fonctionnels***.

  - ✓ ***Affinement du diagramme fonctionnel*** obtenu afin de n'en conserver que les éléments pertinents.

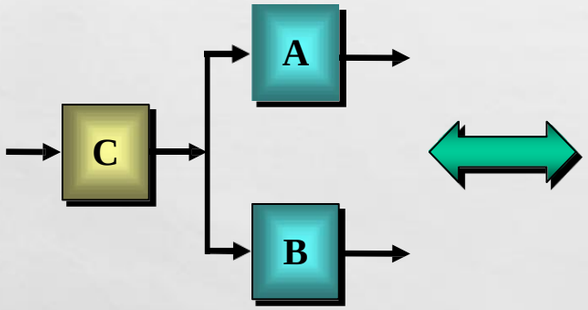
  - ✓ Déductuion d'un ***arbre de succès***, dont la ***forme duale*** n'est autre que l'***AdD recherché***.

Construction manuelle indirecte : Diagramme bloc fonctionnel

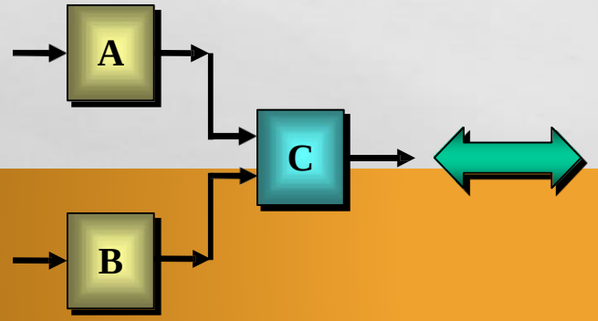
Règles de combinaison



Il est nécessaire et suffisant *que* ***A et B*** *remplissent leurs fonctions pour que* ***C puisse*** *remplir la sienne.*



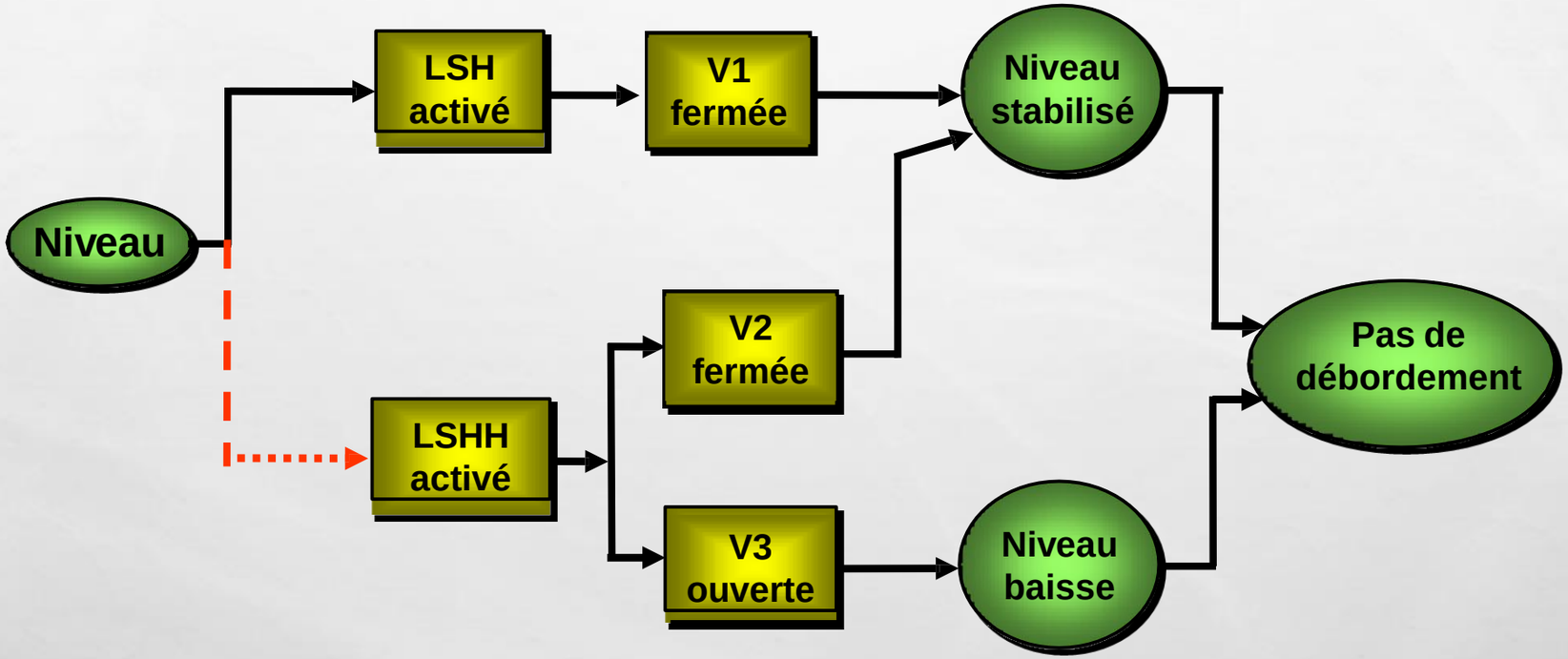
Il est nécessaire et suffisant *que* ***C*** *remplisse sa fonction pour que* ***A*** *et* ***B puissent*** *remplir les leurs.*



Il est nécessaire et suffisant que ***A ou B*** remplissent leurs fonctions pour que ***C puisse*** remplir la sienne.

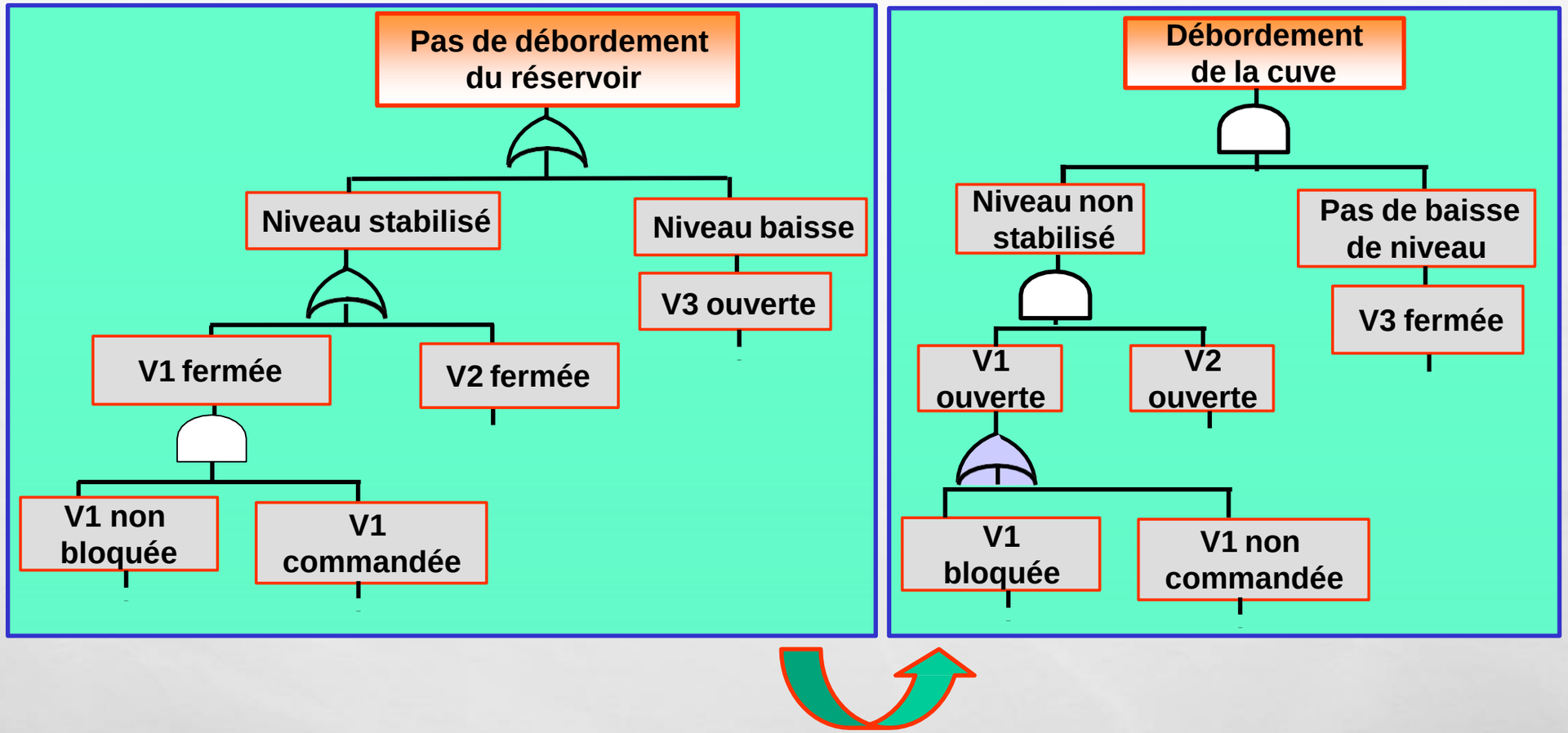
Construction manuelle indirecte : Diagramme bloc fonctionnel

Diagramme bloc fonctionnel relatif au réservoir d'eau



Construction de l'ADD

Construction manuelle indirecte : Arbre de succès et AdD



- Porte **ET** devient porte **OU**
- Porte **OU** devient porte **ET**
- Porte **KooN** devient porte **N-K+1ooN**

Exploitation qualitative d'un ADD

Coupes minimales

❑ ***Coupe minimale*** : une ***combinaison nécessaire et suffisante d'événements de base*** dont la conjonction des occurrences conduit à celle de l'ER.

Si on retire à une coupe minimale un seul de ses éléments, n'importe lequel, le reste ne suffit plus à produire l'ER.

Scénario critique

Réduction de l'AdD

❑ Exploitation qualitative :

- ✓ Nombre de coupes minimales.
- ✓ Ordre (longueur) de ces coupes.

Exploitation qualitative d'un ADD

Coupes minimales : procédure classique

❑ La recherche des coupes minimales se fait traditionnellement à partir de l'AdD en appliquant ***les règles classiques de simplification des expressions booléennes à la fonction logique sous-jacente*** qu'il représente.

❑ **Règles de simplification**

- **Idempotence** :
  - ✓ **A . A = A**
  - ✓ **A + A = A**
- **Absorption** :
  - ✓ **A + A . B = A**

❑ **Procédure classique appliquée au réservoir d'eau**

ER = G1 = G2 . G3
G2 = G4 . G5
G4 = V1 + LSH
G5 = V2 + LSHH
G3 = V3 + LSHH

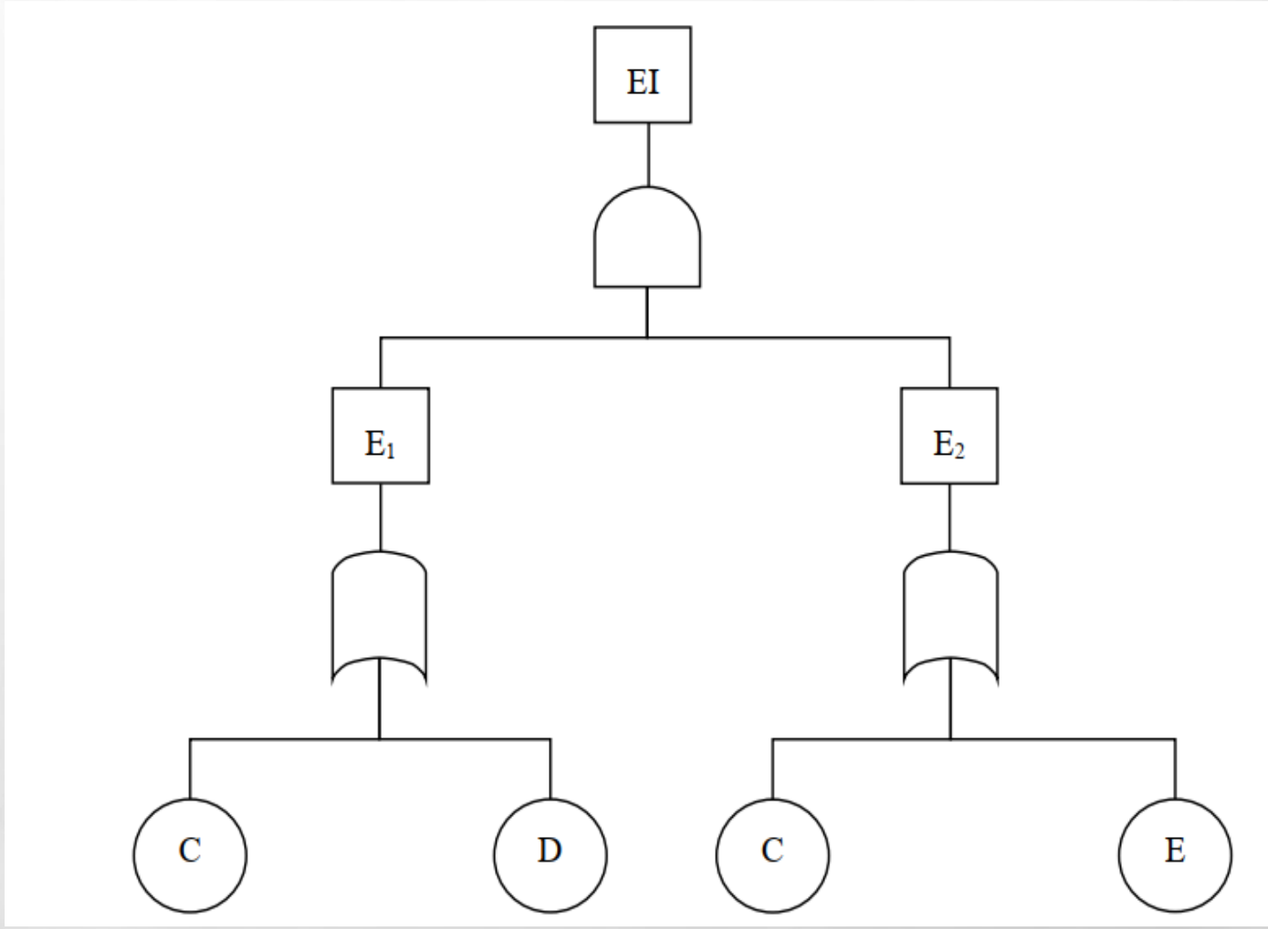
ER = G2 . G3 = G4 . G5 . G3
ER = (V1 + LSH) . (V2 + LSHH) . (V3 + LSHH)
ER = V1.V2.V3 + V1.V2.LSHH + V1.LSHH.V3 + V1.LSHH.LSHH + LSH.V2.V3 + LSH.V2.LSHH + LSH.LSHH.V3 + LSH.LSHH.LSHH.

- **Coupes minimales = { V1.V2.V3 ; V1.LSHH ; LSH.LSHH ; LSH.V2.V3 }**

Exploitation qualitative d'un ADD

Coupes minimales : procédure classique

1. Ecrire la fonction de structure réduite relative à cet arbre
2. Dessiner l'ADD réduit



Exploitation qualitative d'un ADD

Coupes minimales : procédure classique

L'équation booléenne :

$$E_1 = C + D$$

$$E_2 = C + E$$

$$EI = E_1 \times E_2 = (C + D) \times (C + E) = C.C + C.E + C.D + D.E$$

Réduction de l'équation :

Après avoir utilisé les propriétés de réduction, on trouve :

$$EI = C + C.E + C.D + D.E = C + C.D + D.E = C + DE$$

Donc : $\boxed{EI = C + DE}$

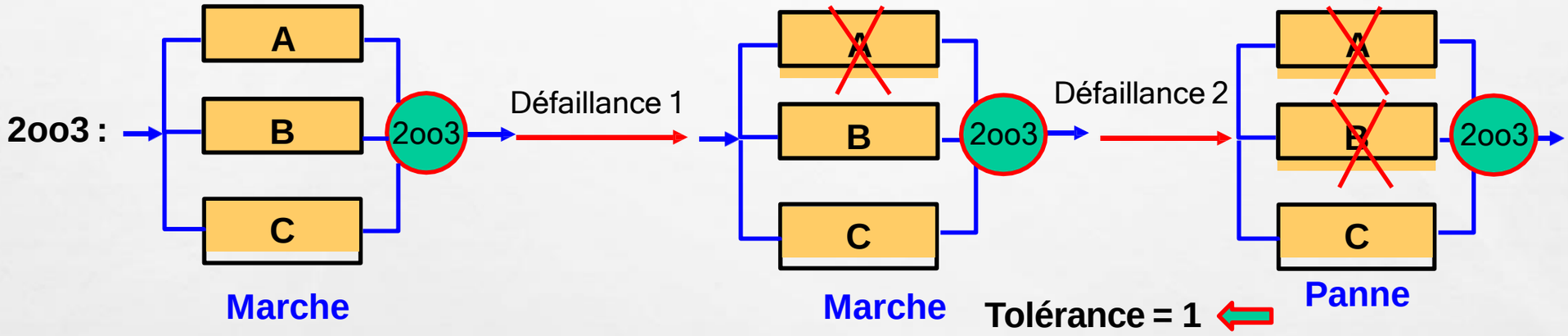
Exploitation quantitative d'un ADD

L'***exploitation quantitative*** d'un AdD consiste principalement à calculer la ***probabilité d'occurrence de son événement sommet*** (ER). Cette exploitation n'est possible que si l'on ***dispose de données numériques relatives aux probabilité d'occurrence de tous les événements de base*** de l'AdD.

Exploitation quantitative d'un ADD

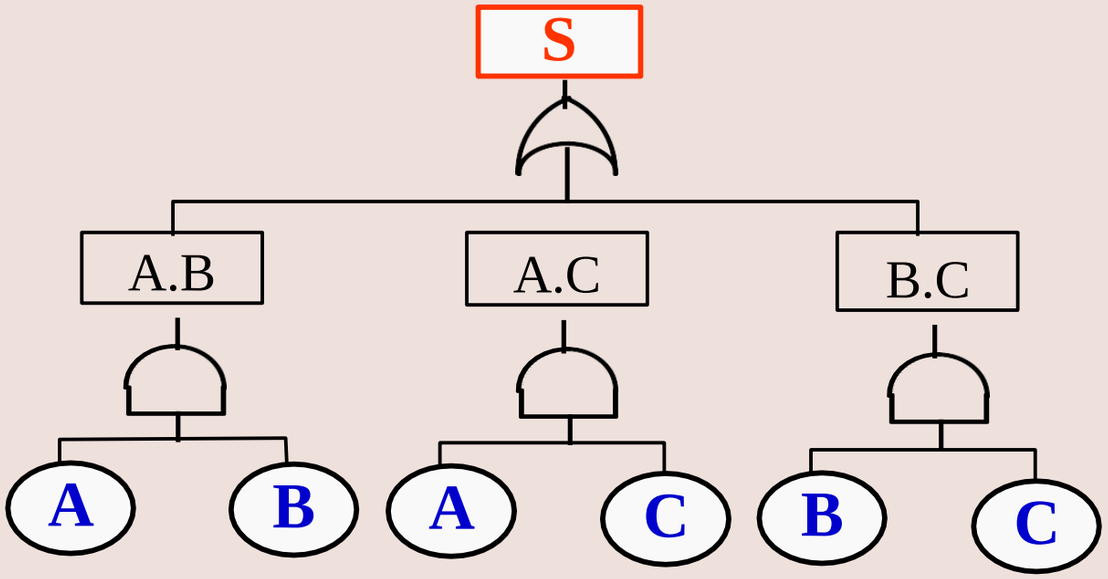
Architecture 2003

- DBF relatif à l'architecture 2oo3



Tolérance aux défaillances M = N – K

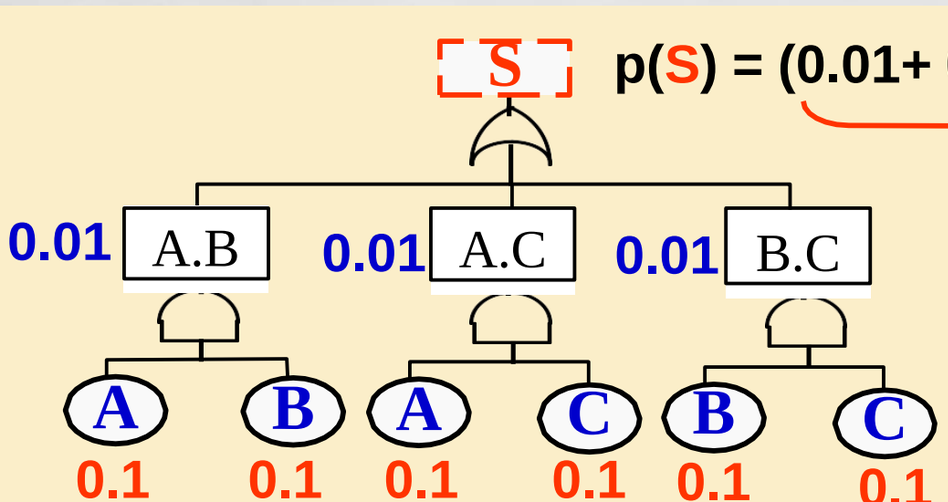
- AdD relatif à l'architecture 2oo3



Exploitation quantitative d'un ADD

Techniques de calcul classiques : (1) Méthode directe

- Cette méthode consiste à ***calculer la probabilité de tout événement intermédiaire*** (événement de sortie d'une porte) ***à partir de celles de ses événements-causes*** (événements d'entrée) en appliquant, d'une manière ascendante, ***les deux règles de base suivantes*** :
  - ✓ **Porte ET :** $P(e_i \cap e_j) = P(e_i) \times P(e_j)$
  - ✓ **Porte OU :** $P(e_i \cup e_j) = P(e_i) + P(e_j) - P(e_i) \times P(e_j)$
- ***Méthode élémentaire*** mais ***rarement applicable*** dans la pratique : ***AdD sans événement répété***.
- **Application :** p(*A*) = p(*B*) = p(*C*) = *q* = 0.1



p(S) = (0.01+ 0.01- 0.01 x 0.01) + 0.01- 0.0199 x 0.01

p(S) = 0.029701

Ce résultat est erroné car cet AdD contient des événements répétés.

Techniques de calcul classiques : (2) Méthode d'inclusion-exclusion (Sylvester-Poincaré)

- Cette méthode est ***implantée dans la majorité des logiciels de traitement des AdD*** actuellement comercialisés. Elle permet de s'***affranchir de la contrainte pesant sur la méthode directe***, mais ***requiert*** cependant la ***détermination préalable des coupes minimales C_i***.

- Le calcul de la ***probabilité de l'événement sommet (redouté) p(ER)*** se réalise à partir des ***probabilités des C_i, $p(C_i)$,*** selon la formule suivante :

$$p(ER) = \sum_{i=1}^{n} p(C_i) - \sum_{i=1}^{n-1} \sum_{j=i+1}^{n} p(C_i . C_j) + \sum_{i=1}^{n-2} \sum_{j=i+1}^{n-1} \sum_{k=j+1}^{n} p(C_i . C_j . C_k) \ldots$$

- Cependant, cette méthode présente à son tour certains inconvénients :
  - ✓Elle nécessite de calculer $2^n - 1$ termes pour l'obtention de la valeur exacte de *p*(ER), **n** étant le nombre des C_i : ***le plus gros handicap de cette méthode.***
  - ✓Elle doit tenir compte, pour chaque conjonction de C_i , de leur dépendance ou indépendance mutuelle.

Techniques de calcul classiques : (2) Méthode d'inclusion-exclusion (Sylvester-Poincaré)

❑ Application au système 2oo3

S = A.B + A.C + B.C
On en déduit :

$$p(S) = p(A.B + A.C + B.C)$$

$$= p(A.B) + p(A.C) + p(B.C) – p[(A.B) . (A.C)] – p[(A.B) . (B.C)] - p[(A.C) . (B.C)] + p[(A.B) . (A.C) . (B.C)]$$

$$= p(A.B) + p(A.C) + p(B.C) – 2\, p(A.B.C)$$

$$p(S) = 3p(A.B) – 2\, p(A.B.C) = 3\, p(A) . p(B) – 2\, p(A) . p(B)\, p(C)$$

$$= 3\, q^2 – 2\, q^3 = \mathbf{0.028}$$

Ce résultat est exact et donc différent de celui obtenu par la méthode directe.