Présentation de la Sûreté de Fonctionnement Concepts FMDS

Jean Gérard CHEVASSU
Société EADS APSYS

Avancement

- Séances N° 1 et 2 : présentation de l'UE. Introduction et notions fondamentales du métier de chef de projet
- Séance N° 3 :
  - Gestion et maîtrise des risques.
  - La Sûreté de fonctionnement
- Séance N°4 : Mise en place d'un projet en support et maintenance pour une PME, dans le domaine des nouvelles technologies (NTIC)
- Séquence 5 : Analyse de Risque Projet

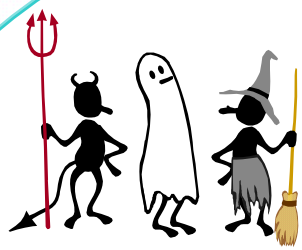
La Sûreté de Fonctionnement

1 Concepts et généralités

2 Méthodes d'analyse

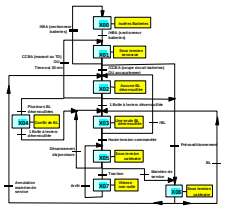
3 Conclusion

Qu'est ce qu'un système ?



Des Hommes

Des Equipements



Des logiciels

Des Techniques

UN SYSTEME

« Ensemble complexe de matériels, logiciels, personnels et processus d'utilisation, organisés de manière à satisfaire les besoins et à remplir les services attendus, dans un environnement donné » (RG AERO 0027 du BNAE)

Sûreté de Fonctionnement

DEFINITION

Définition un peu **excessive**
car la Sûreté de Fonctionnement
est *a priori* loin
d'être une science exacte

HISTORIQUE

La Sûreté de Fonctionnement peut être présentée comme la science des défaillances

Définition un peu **réductrice** car
la Sûreté de Fonctionnement
aborde les systèmes et processus
en considérant d'autres aspects
que leurs défaillances

Sûreté de Fonctionnement

DEFINITION

HISTORIQUE

Vis-à-vis des **défaillances**, la Sûreté de Fonctionnement inclut :

- Leur connaissance
- Leur évaluation
- Leur prévision
- **Leur maîtrise**

DEFINITION : La Sûreté de Fonctionnement est l'aptitude d'un système à satisfaire à une ou plusieurs fonctions requises dans des conditions données

Sûreté de Fonctionnement

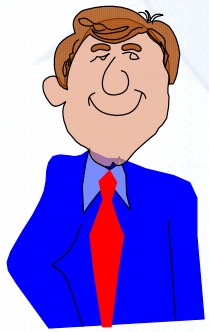
DEFINITION

HISTORIQUE

ANNEES 1950 : Notion de Fiabilité en électronique (Etats-Unis)

ANNEES 1960 : Analyse des défaillances dans l'aéronautique et le spatial

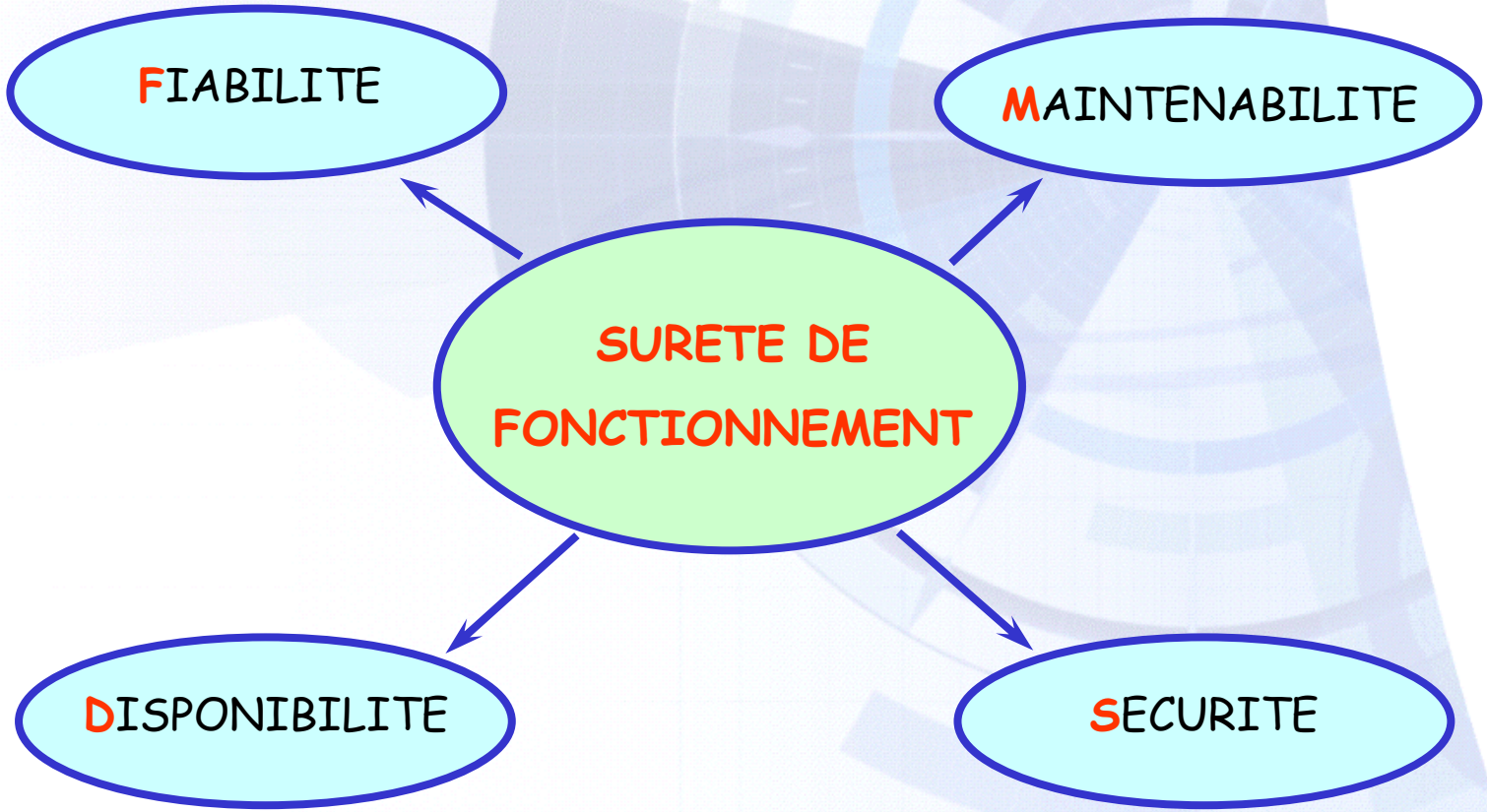
ANNEES 1970 : Evaluation des risques dans le nucléaire



ANNEES 1980 : Formalisation et généralisation de la SdF dans le cadre de la conception des systèmes complexes

ANNEES 1990 et 2000 : Utilisation de la SdF dans l'industrie

Concepts F.M.D.S.



Concepts F.M.D.S

FIABILITE	MAINTENABILITE	DISPONIBILITE	SECURITE

DEFINITION Aptitude d'un système à accomplir une fonction requise, dans des conditions données, pendant un intervalle de temps déterminé.

MESURE Probabilité qu'un système S accomplisse une fonction requise, dans des conditions données, pendant l'intervalle de temps (0,t).

R(t) = P[S non défaillant sur (0,t)]

Ex : $P = 1\, e^{-\lambda t}$ (λ constant)

Exemples de données

TAUX DE DEFAILLANCE

Composants mécaniques :

Rupture d'un arbre de transmission de puissance :	5.10^{-5} .h^{-1}
Rupture ou dégradation d'un ressort à spirale :	5.10^{-7} .h^{-1}

Composants électriques :

Défaillance totale d'un alternateur d'un groupe :	1.10^{-5} .h^{-1}
Non-fonctionnement d'un fusible :	1.10^{-6} .h^{-1}

Capteurs et instrumentation :

Défaillance d'un capteur de température :	1.10^{-6} .h^{-1}
Obstruction d'une vanne manuelle :	1.10^{-4} .h^{-1}

Fiabilité humaine

Globalement il est admis que la **probabilité d'erreur par action élémentaire** d'un opérateur formé à la tâche qui lui est demandée est de 10^{-3}

Pour les actions « machinales » (ou réflexes) : 5.10^{-5} à 5.10^{-3}

Pour les actions « procédurales » (check-list) : 5.10^{-4} à 5.10^{-2}

Pour les actions « cognitives » (part d'invention) : 5.10^{-3} à 5.10^{-1}

Amélioration de la fiabilité humaine :

- Ergonomie (éviter déconcentration)
- Procédures (vérification)
- Simulateurs (apprentissage)

Concepts F.M.D.S

FIABILITE | **MAINTENABILITE** | DISPONIBILITE | SECURITE

DEFINITION Aptitude d'un système à être maintenu ou rétabli, en un temps donné, dans un état de fonctionnement bien défini lorsque les opérations de maintenance sont accomplies avec des moyens donnés, suivant un programme déterminé.

MESURE Probabilité que la maintenance d'un système S accomplie dans des conditions données, avec des procédures et des moyens prescrits, soit achevée au temps t, sachant que le système est défaillant à t = 0.

$$M(t) = P[S \text{ est réparé sur } (0,t)]$$

Concepts F.M.D.S

FIABILITE | MAINTENABILITE | **DISPONIBILITE** | SECURITE

DEFINITION Aptitude d'un système à être en état d'accomplir une fonction requise, dans des conditions données, à un instant donné, en supposant que la fourniture des moyens extérieurs soit assurée.

MESURE Probabilité qu'un système S soit en état d'accomplir une fonction requise dans des conditions données et à un instant donné.

D(t) = P[S non défaillant à l'instant t]

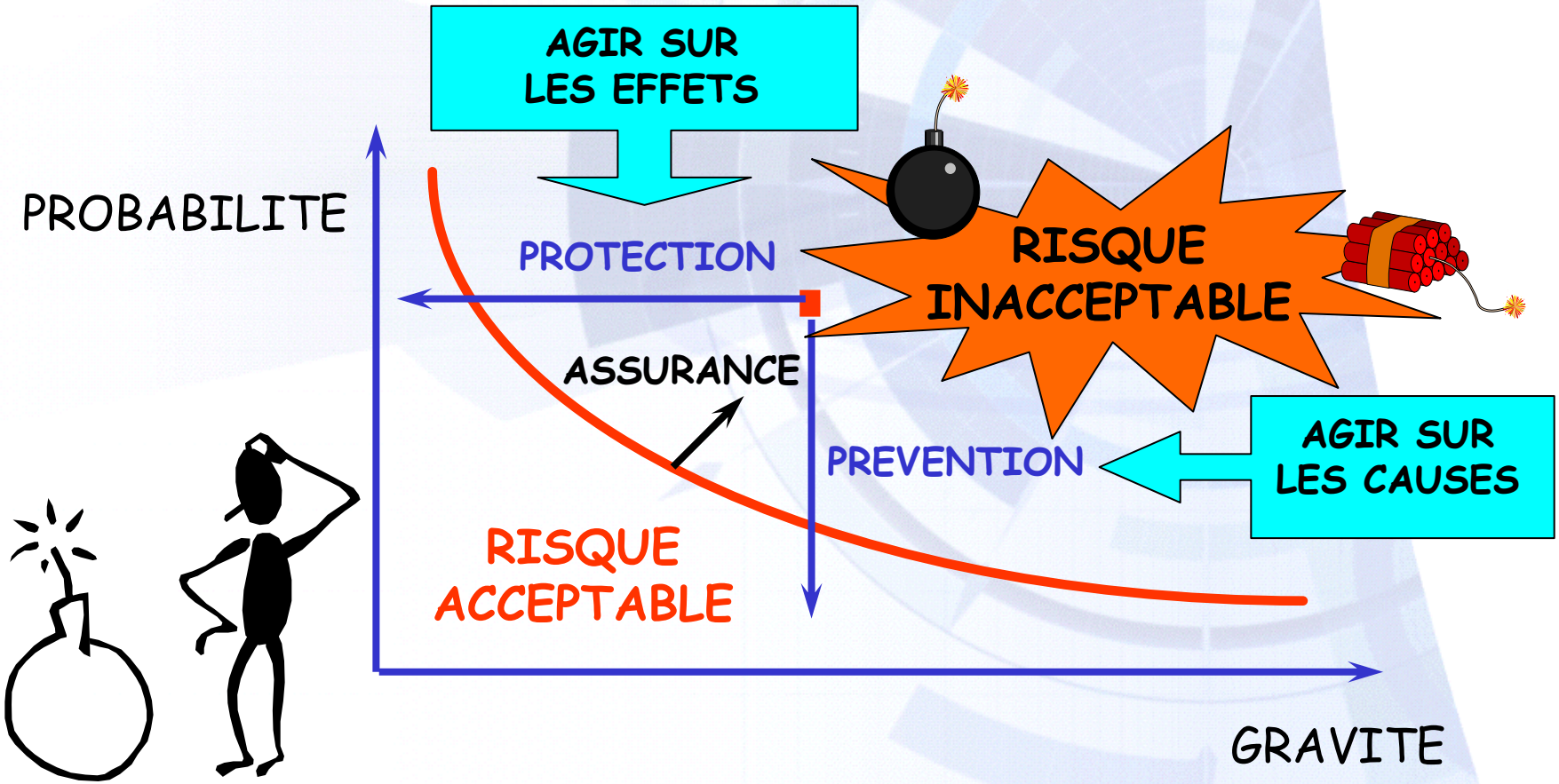
Concepts F.M.D.S

FIABILITE	MAINTENABILITE	DISPONIBILITE	**SECURITE**

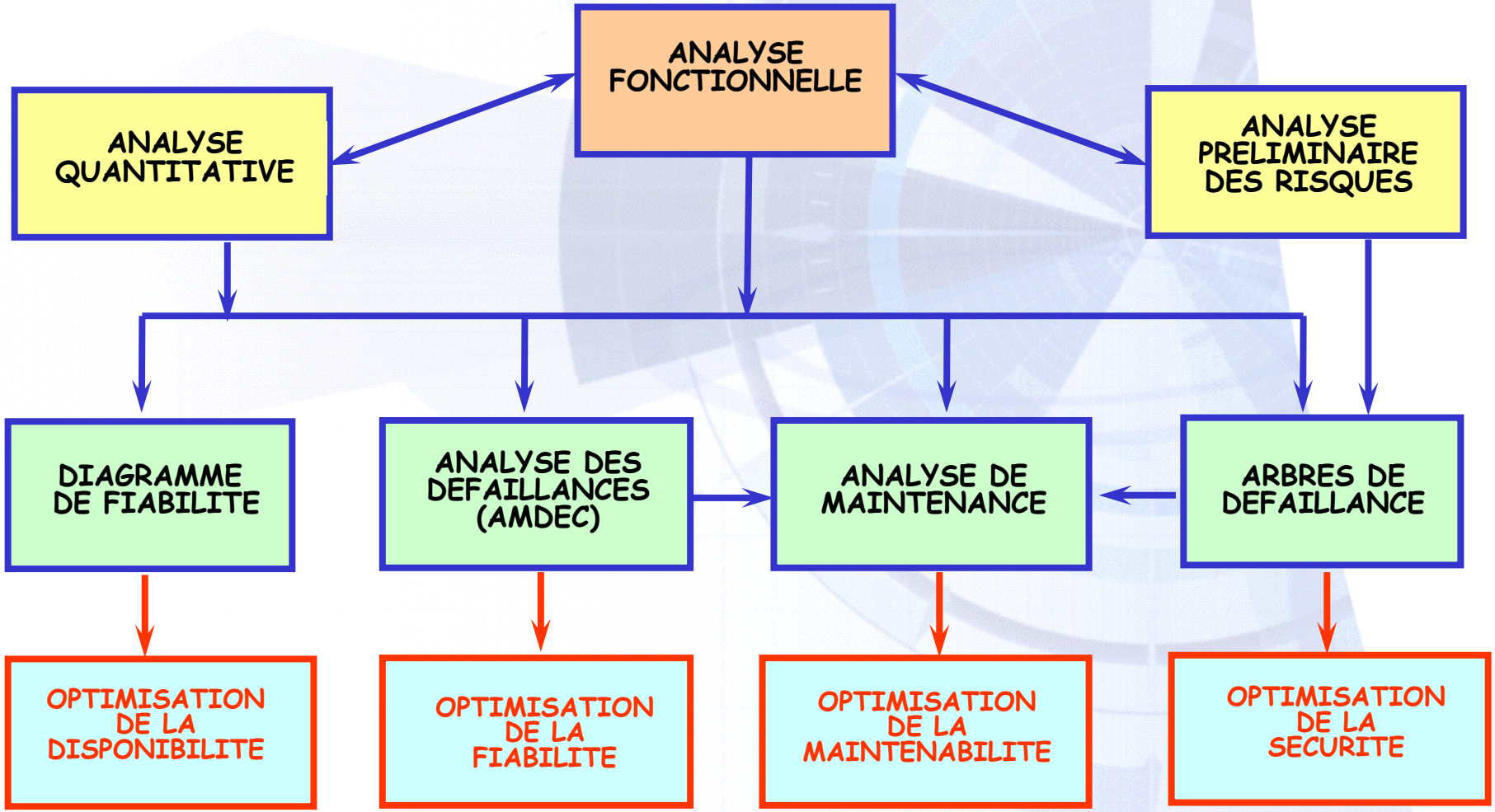
DEFINITION Aptitude d'un système à ne pas générer, dans des conditions données, des événements critiques ou catastrophiques.

MESURE Probabilité qu'un système S évite de faire apparaître, dans des conditions données, des événements critiques ou catastrophiques.

Notion de Risque

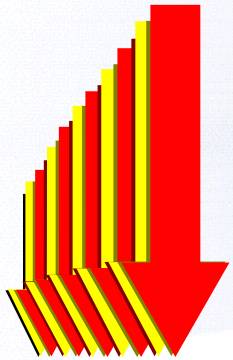


Méthodes d'analyse



Démarche mixte

DEMARCHE INDUCTIVE



On raisonne du plus particulier au plus général :
Face à un système et à une défaillance, on étudie de façon détaillée les effets ou les conséquences de la défaillance sur le système lui-même ou sur son environnement

Exemple : Analyse des défaillances (AMDEC)

DEMARCHE DEDUCTIVE

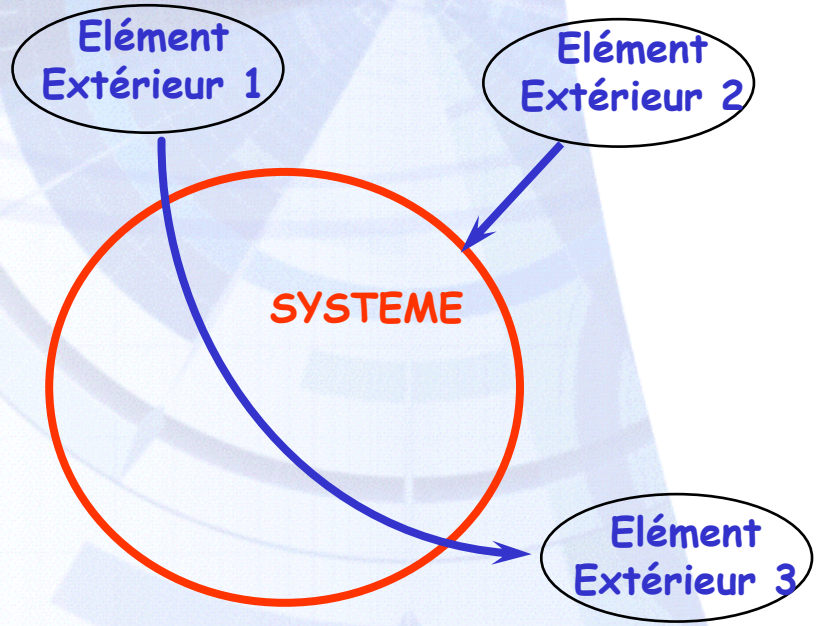
On raisonne du plus général au plus particulier :
Supposant que le système est défaillant, on recherche les causes possibles de la défaillance

Exemple : Arbre de défaillance

Analyse Fonctionnelle

ANALYSE FONCTIONNELLE EXTERNE

ANALYSE FONCTIONNELLE INTERNE



Elle permet de définir avec précision :

- Les **limites fonctionnelles et matérielles** du système
- Les différentes **fonctions** et **missions** réalisées par le système
- Les diverses **configurations d'exploitation**

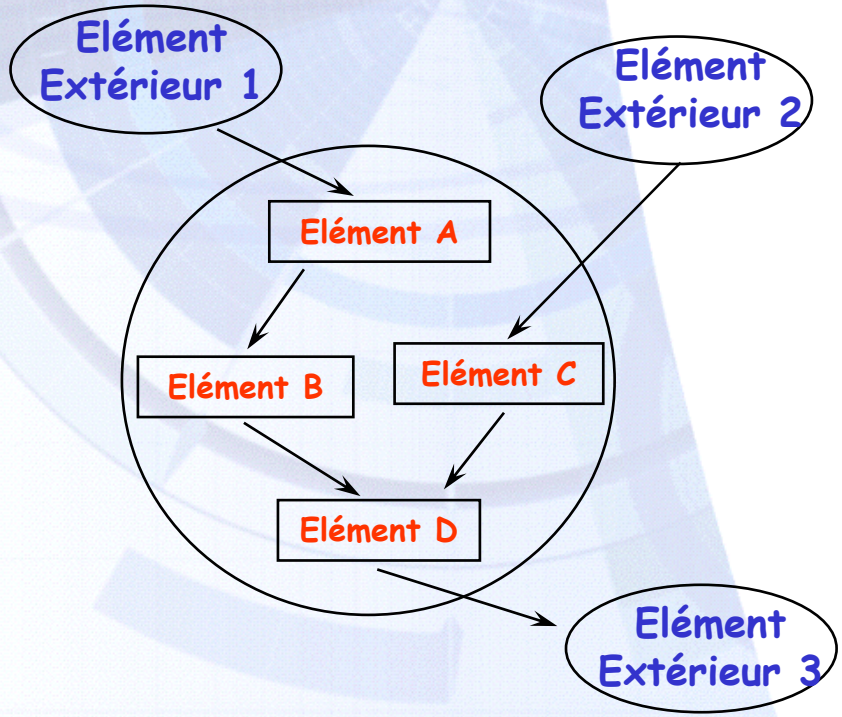
Analyse Fonctionnelle

ANALYSE FONCTIONNELLE EXTERNE

ANALYSE FONCTIONNELLE INTERNE

Elle permet :

- de réaliser une **décomposition arborescente et hiérarchique** du système en éléments fonctionnels et/ou matériels
- de lister le **cheminement des fonctions** définies au niveau système au travers des différents éléments



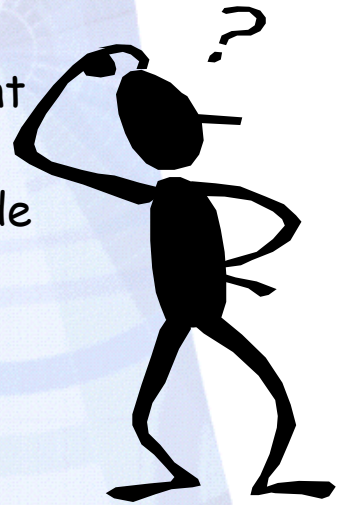
Analyse quantitative

PRINCIPALE NOTIONS | COURBE EN BAIGNOIRE

MTTF : Mean Time To Failure (durée moyenne de fonctionnement d'un équipement avant la 1ère défaillance)

MTTR : Mean Time To Repair (durée moyenne de réparation et de remise en service d'un équipement)

MTBF : Mean Time Between Failure (durée moyenne entre deux défaillances consécutives d'un équipement réparé)



En utilisant la loi exponentielle (taux de défaillance constant), on obtient :

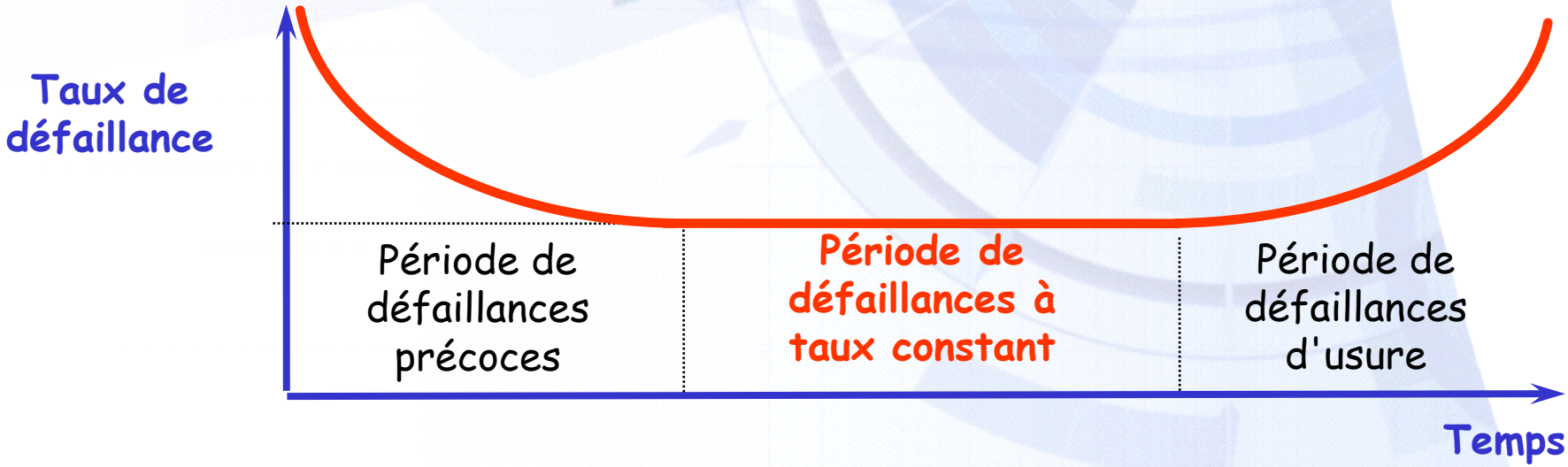
Taux de défaillance : $\lambda = 1 / MTTF$ si $MTTR \ll MTTF$ alors $MTTF \approx MTBF$
alors $\lambda = 1 / MTBF$

Taux de réparation : $\mu = 1 / MTTR$

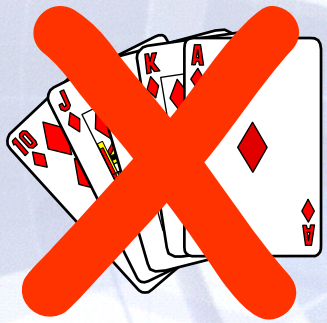
Analyse quantitative

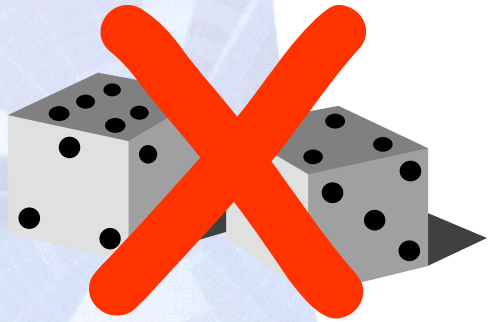
PRINCIPALES NOTIONS

COURBE EN BAIGNOIRE



Recherche des données quantitatives élémentaires de Fiabilité et Maintenabilité





- Retours d'expériences
- Fournisseurs
- Bases de données

Diagramme de fiabilité

PRINCIPE ET REPRESENTATION

CALCULS

OBJECTIF : Représentation de la structure du système (série, redondance, secours...) et calculs de la fiabilité, de la maintenabilité et de la disponibilité du système.

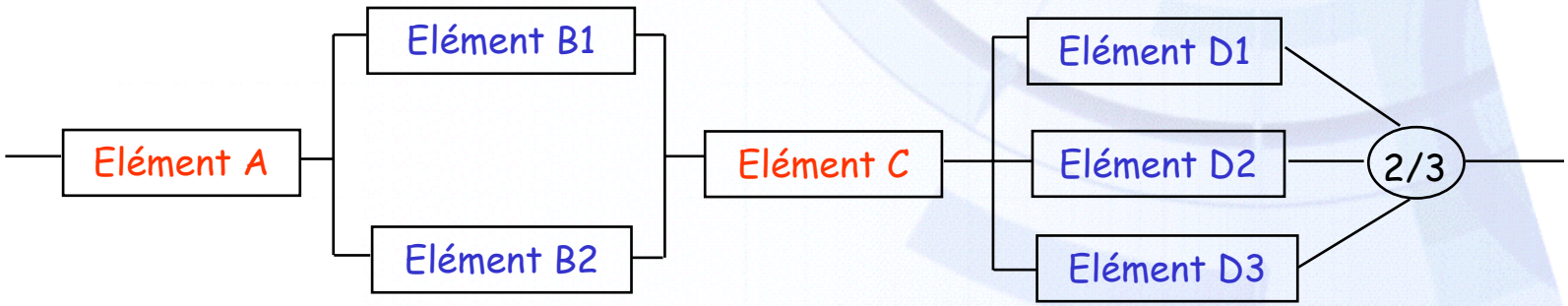


Diagramme de fiabilité

PRINCIPE ET REPRESENTATION

CALCULS

En introduisant les données quantitatives de chaque élément (taux de défaillance et taux de réparation), il est possible de déterminer :

LA FIABILITE DU SYSTEME

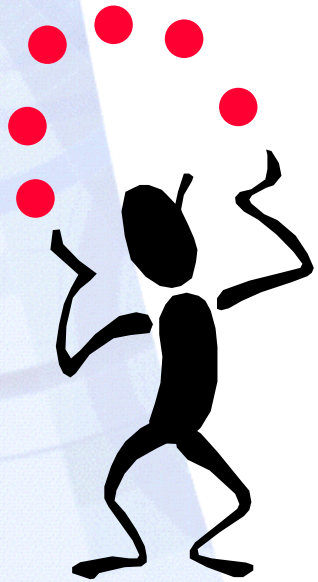
- Courbe de fiabilité du système en fonction du temps
- **MUT :** Mean Up Time (Temps de disponibilité du système)

LA MAINTENABILITE DU SYSTEME

- Courbe de la maintenabilité du système en fonction du temps
- **MDT :** Mean Down Time (Temps d'indisponibilité du système)

LA DISPONIBILITE DU SYSTEME

- Courbe de disponibilité du système en fonction du temps
- **Disponibilité Moyenne = MUT / (MUT + MDT)**



Analyse des défaillances (AMDEC)

PRINCIPE | TABLEAU | AMELIORATIONS

Analyse des Modes de Défaillance, de leurs Effets et de leurs Criticités (AMDEC)

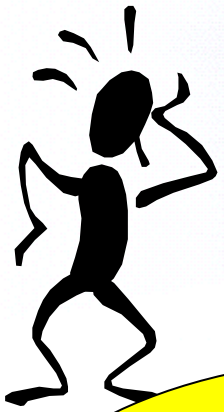
OBJECTIF L'AMDEC, précédée d'une analyse fonctionnelle et d'une analyse quantitative, a pour objet l'obtention de la fiabilité optimale d'un système ou d'un moyen de production. Elle permet de lister et classifier les défaillances des équipements du système.

METHODE

- Recherche des **défaillances** des éléments du système
- Identification des **causes** possibles
- Evaluation des **effets** des défaillances
- Estimation du **risque** (**Criticité**)
- Recherches d'**améliorations**
- Mise en œuvre des améliorations

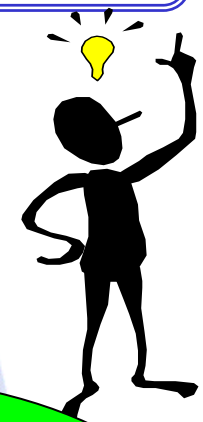
Analyse des défaillances (AMDEC)

PRINCIPE | TABLEAU | **AMELIORATIONS**



INDICE DE CRITICITE :

$C = P \times G$



C > Seuil

AMELIORATIONS

Diminution de la probabilité d'apparition des dysfonctionnements

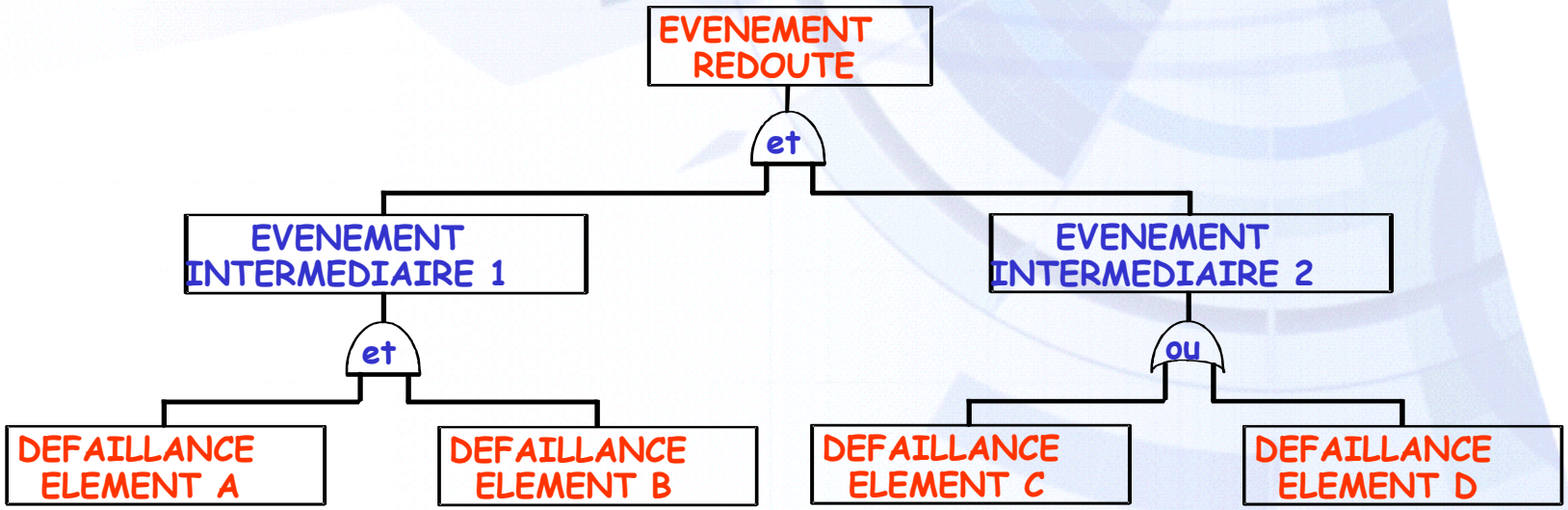
Diminution de la gravité des effets des dysfonctionnements

Arbre de défaillances

PRINCIPE ET REPRESENTATION

ANALYSES

OBJECTIF Mise en évidence des diverses combinaisons possibles d'événements qui entraînent la réalisation d'événements redoutés. Représentation des combinaisons au moyen d'une structure arborescente



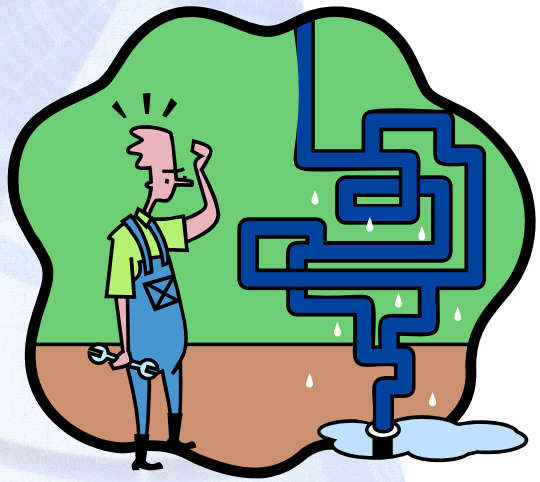
Arbre de défaillances

PRINCIPE ET REPRESENTATION

ANALYSES

ANALYSE QUALITATIVE :

- Détermination des **coupes minimales (chemins critiques)**
- Une coupe minimale est une combinaison d'événements élémentaires entraînant l'événement redouté, tel qu'aucun sous-ensemble de cette combinaison ne produise cet événement redouté



ANALYSE QUANTITATIVE :

- Calcul de la **probabilité d'occurrence** des événements redoutés pour un temps de mission donné à partir des probabilités d'occurrence de chaque événement élémentaire

La SdF dans un programme

- L'ensemble des dispositions prévues dans le Plan SdF et leur management visent à :
  - – définir les objectifs de Sûreté de Fonctionnement et les tâches nécessaires pour les atteindre,
  - – gérer le déroulement de ces travaux,
  - – identifier et corriger les éventuels écarts par rapport aux objectifs,
  - – justifier l'atteinte des objectifs.

- Ces actions sont conduites sous la responsabilité du fournisseur et se réalisent selon la logique de déroulement du programme.

La SdF dans un programme

- **Relations avec l'assurance de la qualité**
  - Les actions d'assurance qualité relatives aux tâches de Sûreté de Fonctionnement consistent à s'assurer :
  - – que l'examen critique des exigences de Sûreté de Fonctionnement a été effectué,
  - – que le plan de Sûreté de Fonctionnement définit des moyens capables d'apporter une réponse adaptée aux exigences spécifiées,
  - – de la pertinence des méthodes d'analyse et de la validité des données d'entrée utilisées,
  - – de la conformité des travaux SdF par rapport au plan de SdF et de leurs résultats (indicateurs SdF),
  - – de la gestion des risques intrinsèques au produit identifiés par les études SdF.

faisabilité La SdF dans un programme

Type de tâche	Désignation	MOA	MOI	Utilisateur
C	Réaliser l'AF su système attendu	X	X	X
C	Définir le profil de vie et les conditions d'environnement	X	X	X
M	Mettre en place structure management SdF et liaison	R	P	-
C	Définir les exigences Soutien logistique : concept de maintenance	X	X	X
C	Identifier les exigences SdF et recueillir données nécessaires à rédaction STB	R	P	P
M	Elaborer le § SdF de la Spécification de management et des STB et participer aux évolutions du CdCF	R	P	P
M	Identifier les ressources et les délais nécessaires aux tâches SdF	P	R	-
M	Etablir la logique de construction de la SdF par sélection des tâches au long du programme	P	R	-
M	Elaborer le Plan de SdF	-	R	-
M	Accepter le Plan de SdF	R	-	-

faisabilité La SdF dans un programme

Type de tâche	Désignation	MOA	MOI	Utilisateur
C	Analyser le profil de vie et les facteurs d'environnement et déterminer les contraintes associées pour la SdF	P	R	-
C	Réaliser l'analyse comparative des différents concepts envisagés	X	X	X
C	participer aux activités relatives au soutien logistique	X	X	X

M	C	R	P	-	X
Management	Construction	responsable	Participant	non concerné	concerné SdF

La SdF dans un programme

définition et développement

Type de tâche	Désignation	MOA	MOI	Utilisateur
C	Réaliser l'analyse comparative, d'un point de vue SdF, des différentes solutions techniques envisagées	-	R	-
C	Effectuer les allocations de SdF	P	R	-
M	Exprimer les règles de conception en matière de SdF	P	R	-
M	Compléter les exigences par les règles de l'art	P	R	-
M	Définir et mettre en place le processus de Logique de traitement des incidents	P	R	P
M	Consolider le Plan de SdF	-	R	-
M	Accepter la consolidation du Plan de SdF	R	-	-
C	Définir les éléments du soutien	X	X	X
C	Réaliser les analyses de SdF retenues	-	R	-
C	Réaliser les essais spécifiques prévus	-	R	-
C	Mettre en œuvre la démarche de croissance de la SdF	-	R	-

La SdF dans un programme

définition et développement

Type de tâche	Désignation	MOA	MOI	Utilisateur
M	Qualifier la définition du produit	X	X	-
M	Gérer les points critiques de SdF			
M	Participer aux revues du projet	X	X	-
M	S'assurer de l'application du Plan de SdF	P	R	-
M	Préparer er organiser le recueil des faits techniques en utilisation	X	X	X
M	Définir les indicateurs de SdF pour le système en utilisation	X	X	X
M	Capitaliser l'expérience du programme	X	X	X

La SdF dans un programme

production

Type de tâche	Désignation	MOA	MOI	Utilisateur
C	Réaliser les essais spécifiques retenus ou nécessaires	-	R	-
M	Gérer évolutions des moyens et des processus de production	X	X	-
C	Définir les évolutions du produit pour satisfaire les objectifs de SdF non atteints	X	X	X
M	Instruire les évolutions du produit pour s'assurer du maintien des performances SdF	X	X	X
C	Maîtriser les processus de production	-	R	-
C	réaliser les opérations de déverminage	-	R	-
M	Poursuivre le processus de logique de traitement des incidents	-	R	-
M	Gérer les points critiques de SdF	P	R	-
M	S'assurer de l'application du Plan de SdF	P	R	-
M	Finaliser le dispositif de recueil des faits techniques en utilisation	X	X	X
M	Recueillir et exploiter les faits techniques liés à la production	X	X	-
M	Capitaliser l'expérience du programme	X	X	X

La SdF dans un programme

utilisation et retrait du service

Type de tâche	Désignation	MOA	MOI	Utilisateur
M	Mettre en place le dispositif de recueil et d'exploitation des faits techniques	X	X	X
C	Recueillir les faits techniques et alimenter le dispositif d'exploitation	X	X	X
M	Poursuivre le processus de logique de traitement des incidents	P	R	P
C	Définir les évolutions du produit pour satisfaire les objectifs de SdF non atteints	X	X	X
M	Instruire les évolutions du produit pour s'assurer du maintien des performances SdF	X	X	X
M	Gérer les points critiques de SdF	P	R	-
C	Renseigner les indicateurs de SdF en utilisation	X	X	X
M	Finaliser les études de SdF relatives au retrait du service et au démantèlement du système	P	R	P
M	Capitaliser l'expérience du programme	X	X	X

Approche Sûreté de Fonctionnement

- Prise en compte :
  - De l'architecture des systèmes (Série, Redondance)
  - Du retour d'expérience (Fréquences, Probabilités)
  - Des effets des défaillances (Gravité, Criticité)
  - Des coûts (Conception, Exploitation, Maintenance)
- La Sûreté de Fonctionnement est utilisable pour **tous les systèmes et moyens de production**
- Les méthodes et outils de la Sûreté de Fonctionnement sont **faciles à mettre en place**
- Les études de Sûreté de Fonctionnement facilitent **le dialogue entre la conception, l'exploitation et la maintenance**