Les Rencontres du CIMI

Sûreté de Fonctionnement des installations industrielles

18 octobre 2011

Quelques essais de définition :

La sûreté de fonctionnement (SdF) traduit la confiance qu'on peut accorder à un système

La sûreté de fonctionnement est la propriété qui permet aux utilisateurs du système de placer une confiance justifiée dans le service qu'il leur délivre

La sûreté de fonctionnement est considérée comme la science des défaillances et des pannes

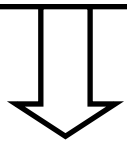
SURETE de FONCTIONNEMENT

Le terme « sûreté de fonctionnement » désigne deux choses :

- l'aptitude d'une entité (système, produit, moyen, …), d'une part, à disposer de ses performances fonctionnelles (fiabilité, maintenabilité, disponibilité) et d'autre part, à ne pas engendrer de risques majeurs (humains, environnementaux, de sécurité,…)
- les activités d'évaluation de cette aptitude (on emploie l'expression : « études de sûreté de fonctionnement »)

FMDS & SdF:

- Fiabilité
- Maintenabilité / Maintenance
- Disponibilité
- Sécurité / Sûreté



Sûreté de Fonctionnement

- évaluée par ses composantes FMDS
- approche probabiliste

FIABILITE

Fiabilité:

- la fiabilité est l'aptitude d'un dispositif à accomplir une fonction requise, dans des conditions d'utilisation et pour une période de temps déterminées

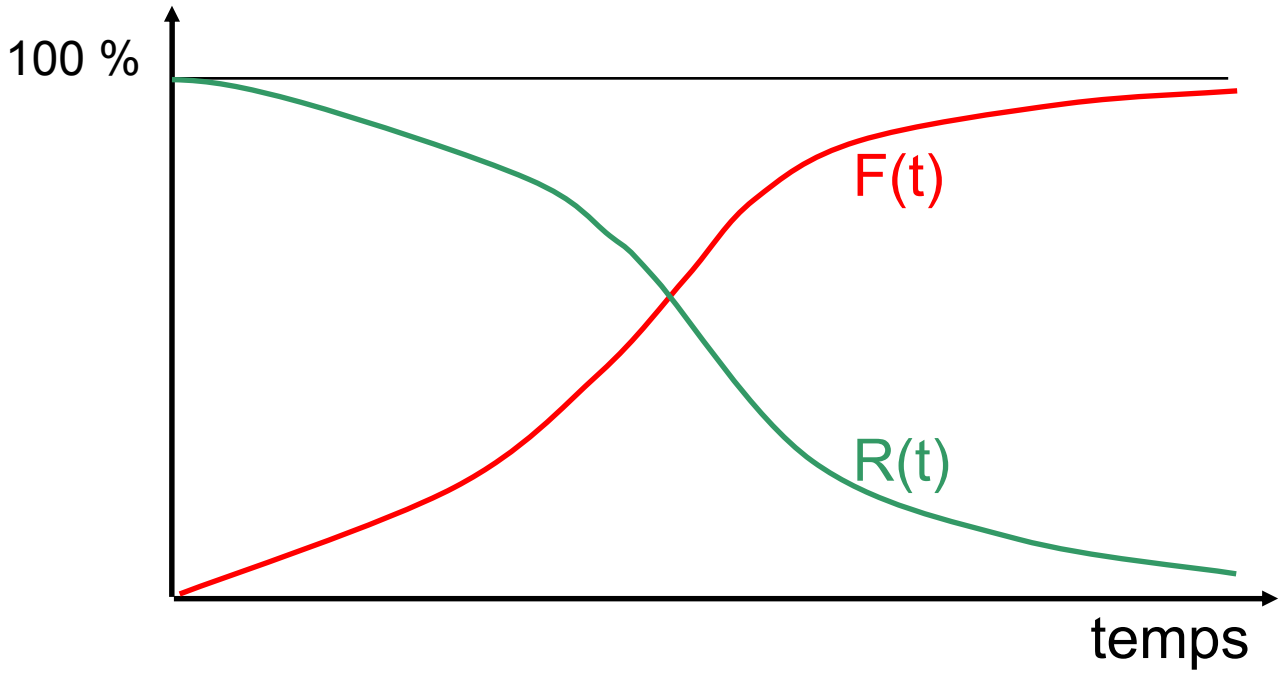
- le terme « fiabilité » est utilisé comme une caractéristique indiquant une probabilité de succès

(Extrait de NF X 06-501)

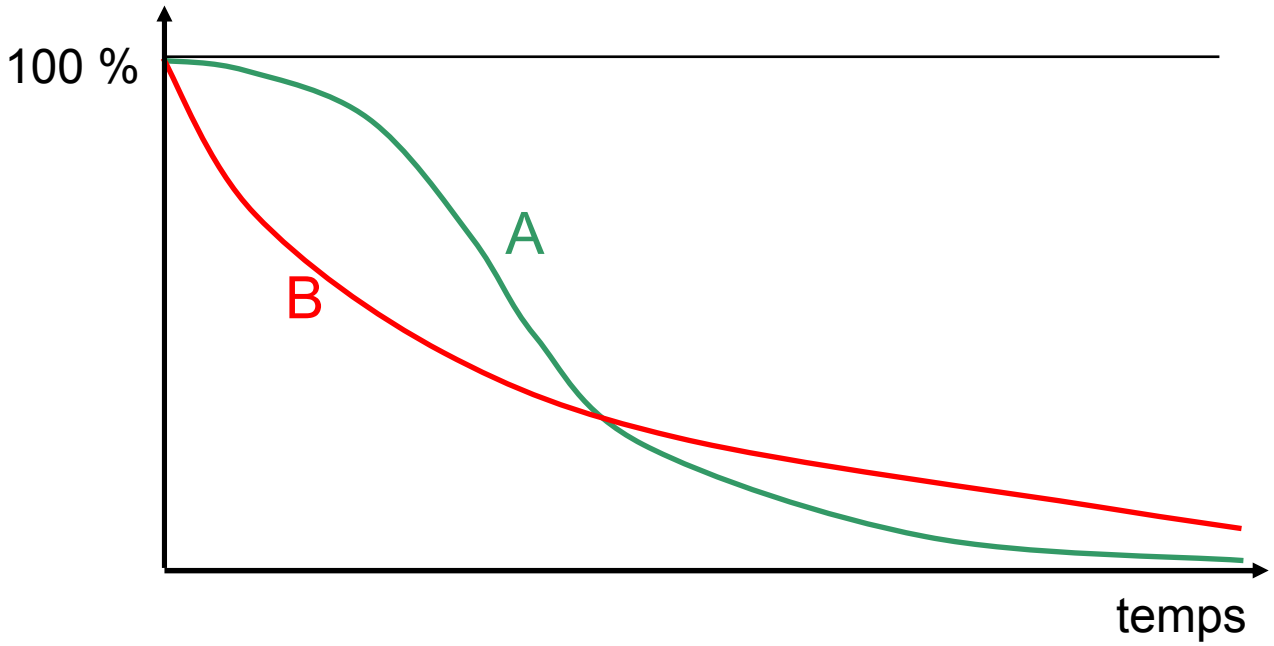
Fonctions Fiabilité / Défiabilité:

- fiabilité à la date t, notée R(t):
  - probabilité d'atteindre la date t sans défaillance

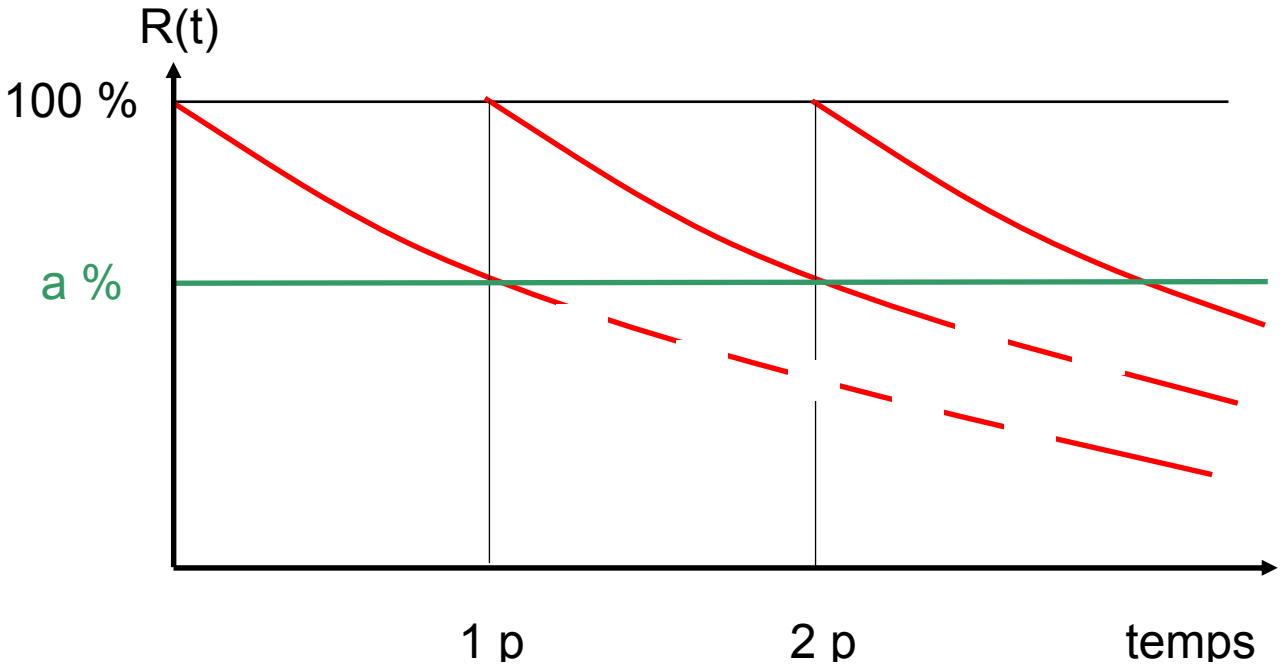
- défiabilité à la date t (notée F(t):
  - probabilité de défaillance avant t



Fonction Fiabilité R(t):



Echange périodique / Fiabilité:



- p = périodicité d'échange
- la fiabilité de la fonction à assurer reste toujours **≥** a %

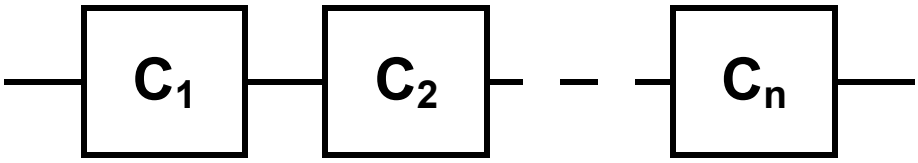
Remarque : sans intérêt pour les composants électroniques

Système = ensemble de composants

- système série:
  - la défaillance d'un seul composant entraîne la défaillance du système
- système parallèle:
  - il faut que tous les composants soient défaillants pour que le système soit défaillant
- système mixte:
  - constitué de sous-ensembles série, en parallèle
- système complexe:
  - ≠ série, ≠ parallèle, ≠ mixte

Système série:

- la défaillance d'un seul composant entraîne la défaillance du système



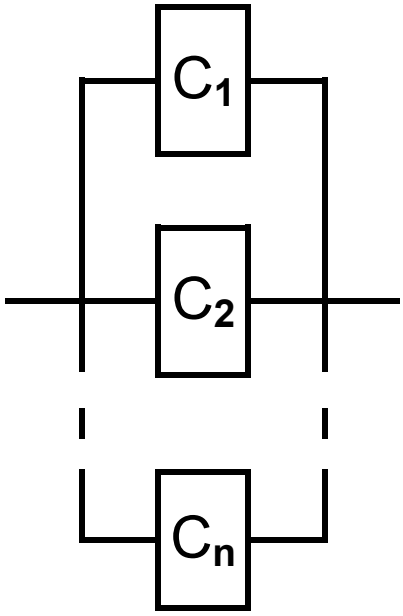
- $R_{système}(t) = \prod_{(1 \text{ à } n)} R_i(t)$

- exemple:
  $R_{C1}(t) = 0,99$ $R_{C2}(t) = 0,97$
  $R_{C3}(t) = 0,96$ $R_{C4}(t) = 0,98$
  $R_{C5}(t) = 0,99$

  ➔ $R_{système}(t) = 0,84$

Système parallèle:

- il faut que tous les composants soient défaillants pour que le système soit défaillant (chacun des composants peut assurer seul la mission)



- $R_{syst.}(t) = 1 - \prod_{(1 \text{ à } n)} [1 - R_i(t)]$
- exemple:
  $R_{C1}(t) = 0,80$
  $R_{C1, C2}(t) = 0,96$
  $R_{C1, C2, C3}(t) = 0,992$

MAINTENABILITE
MAINTENANCE

Maintenabilité:

- dans des conditions données d'utilisation, la maintenabilité est l'aptitude d'un dispositif à être maintenu ou rétabli dans un état dans lequel il peut accomplir sa fonction requise, lorsque la maintenance est effectuée dans des conditions données avec des procédures et des moyens prescrits
- le terme « maintenabilité » est aussi défini comme une caractéristique indiquant une probabilité pour que le dispositif soit réparé dans un intervalle de temps donné

(Extrait de NF X 60-010)

Maintenance:

- ensemble des actions permettant de maintenir ou de rétablir un bien dans un état spécifié ou en mesure d'assurer un service déterminé

(Extrait de NF X 60-010)

DISPONIBILITE

Disponibilité:

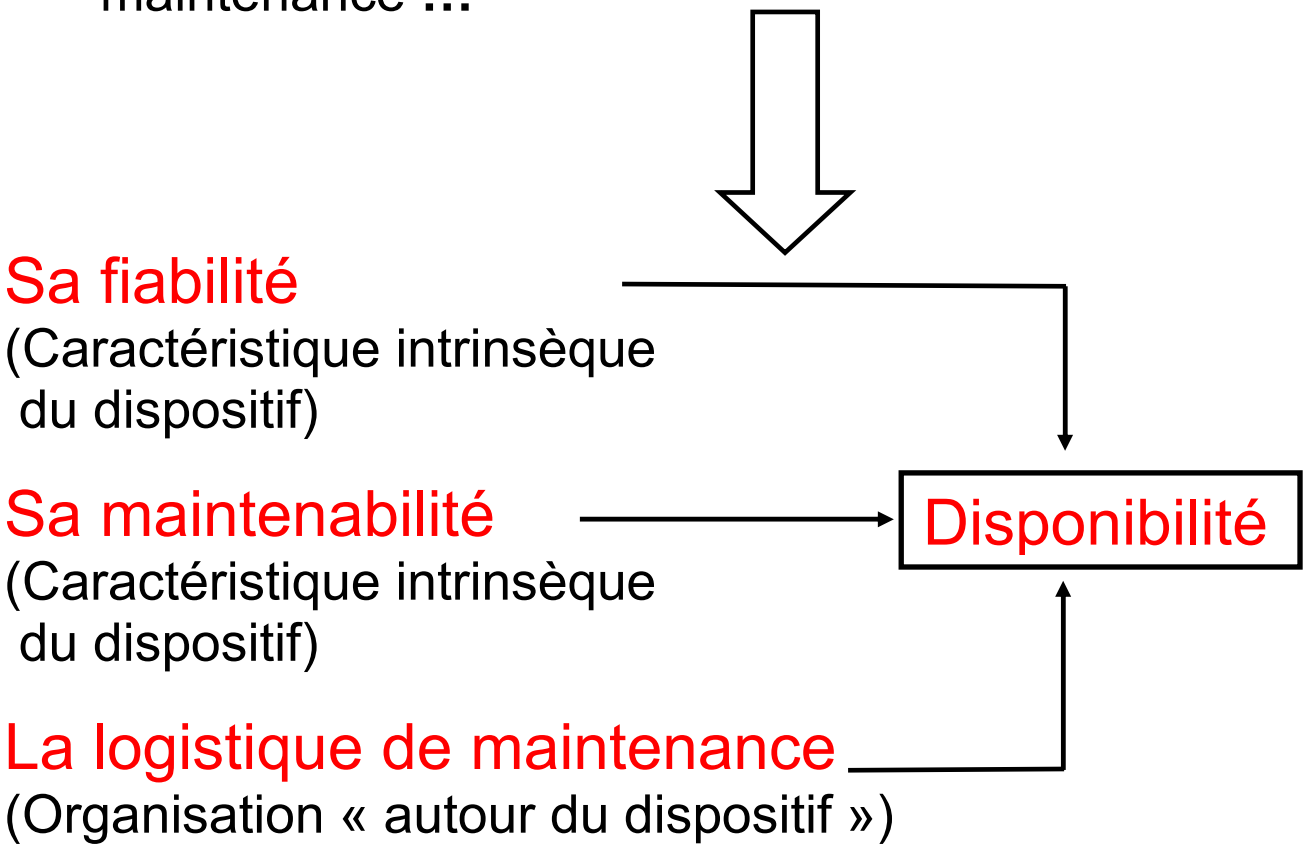
- aptitude d'un dispositif*, sous les aspects combinés de sa fiabilité, de sa maintenabilité et de la logistique de maintenance, à remplir ou à être en état de remplir une fonction à un instant donné ou dans un intervalle de temps donné

* équipement, système, service,…

(Extrait de NF X 60-503)

Disponibilité:

- … sous les aspects combinés de sa fiabilité, de sa maintenabilité et de la logistique de maintenance …



Sur une base de **1000** heures :

	nb de pannes	pour une panne		temps d'arrêt de prod. total (en h)	temps de prod. restant (en h)	dispo (en %)
		temps de rép. (en h)	temps logist. (en h)			
situation de réf.	5	10	12	110	890	89,00
A	5	**5**	12	85	915	91,50
B	5	10	**6**	80	920	92,00
C	5	**5**	**6**	55	945	94,50
D	**3**	10	12	66	934	93,40

Par rapport à la situation de référence :

A = amélioration de la maintenabilité ➔ **gain de 2,5 % de dispo**

B = amélioration de la logistique ➔ **gain de 3 % de dispo**

C = amél. maintenabilité et logistique ➔ **gain de 5,5 % de dispo**

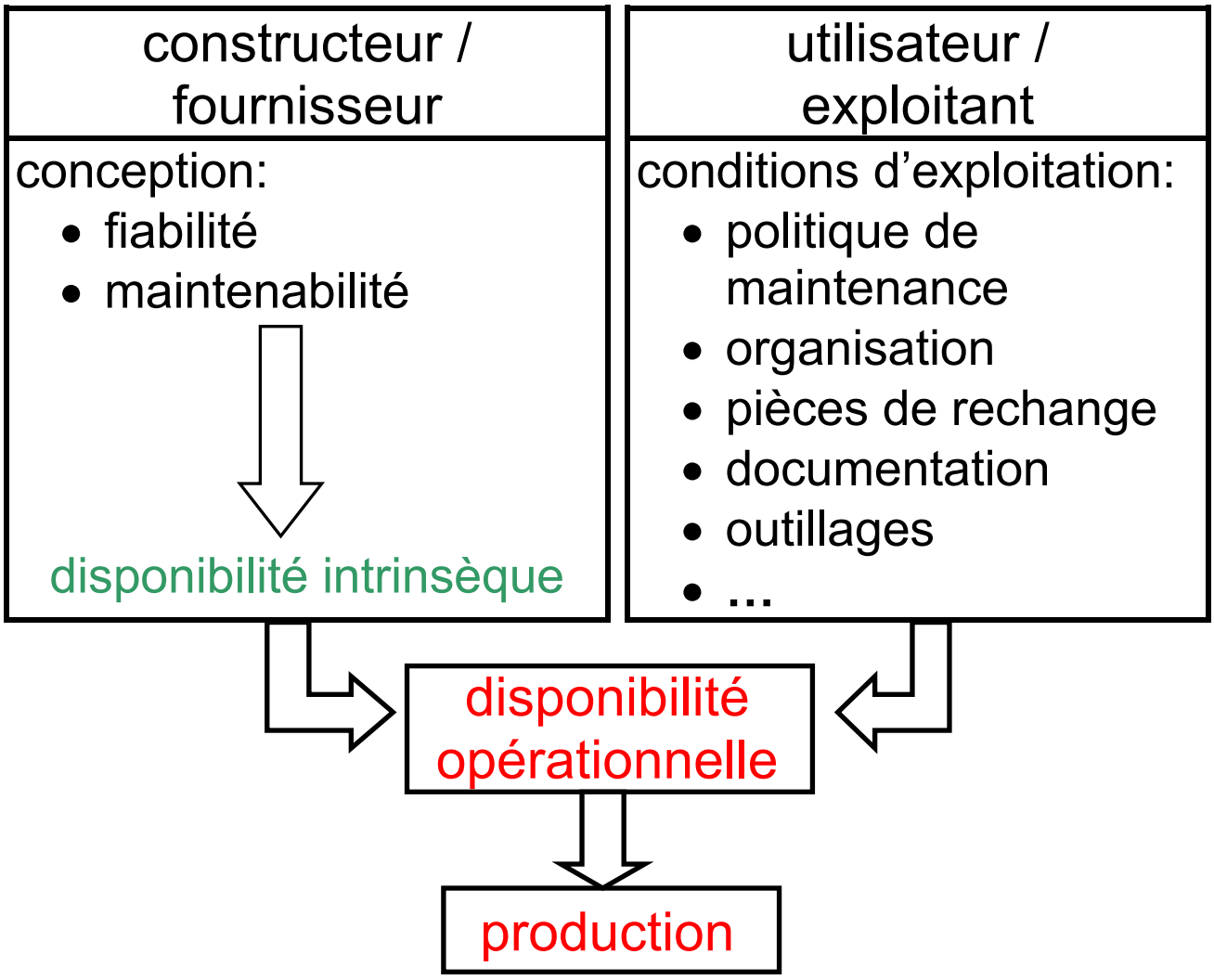
D = amélioration de la fiabilité ➔ **gain de 4,4 % de dispo**

Dans les clauses FMDS:

- identifier ce qui est recherché:
  - un fonctionnement «sans défaillance» pendant la durée d'une mission = pb. de fiabilité (production en lots, systèmes de télécomm. embarqués, transport aérien ou ferroviaire, …)
  - un taux de fonctionnement sur une longue période de temps = pb. de disponibilité stationnaire (disponibilité des équipements de production sur une année, …)
  - un dispositif qui doit être disponible à un instant donné (pas en maintenance préventive, ni corrective) = pb. de disponibilité instantanée (disponibilité d'un dispositif de secours, …)

Dans les clauses FMDS (suite):

- préciser ce qui est « imputable » au constructeur et à l'utilisateur



SECURITE

Sécurité:

- aptitude d'un système à ne pas générer, dans des conditions données, des évènements critiques ou catastrophiques
- probabilité que le système évite de faire apparaître, dans des conditions données, des évènements critiques ou catastrophiques

Sécurité d'une machine:

- aptitude d'une machine à accomplir sa fonction, à être transportée, installée, mise au point, entretenue et mise au rebut dans les conditions d'utilisation normale spécifiées dans la notice d'instructions, sans causer de lésion ou d'atteinte à la santé

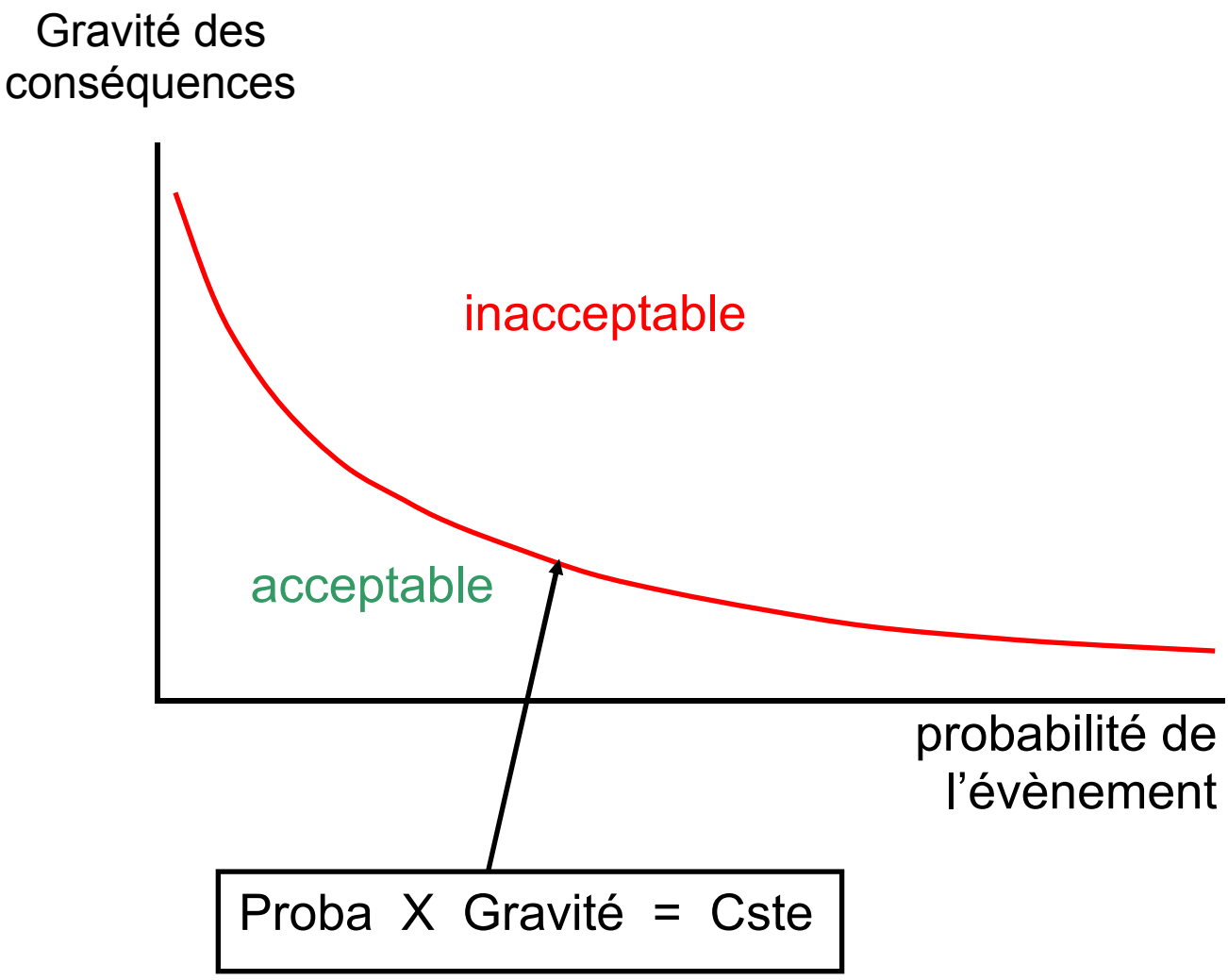
(Extrait de EN 292-1)

Risque :

- le risque relatif au phénomène dangereux considéré est une fonction de la gravité du dommage possible pouvant résulter du phénomène dangereux considéré et de la probabilité d'occurrence du dommage

(Extraits de EN 1050)

Acceptation du risque:



Exemple (aéronautique):

On définit des objectifs limites en terme de probabilité d'occurrence des événements :

pour une classe de conséquence :	la probabilité d'occurrence devra être inférieure à :	on parle alors d'évènement :
catastrophique	10^{-9} / h de vol	extrêmement improbable
critique	10^{-7} / h de vol	extrêmement rare
majeure	10^{-5} / h de vol	rare
mineure	pas d'objectif	probable

ETUDES de SURETE de FONCTIONNEMENT

Les études de sûreté de fonctionnement:

- regroupent l'évaluation prévisionnelle de la FMDS d'une organisation, d'un système, d'un produit ou d'un moyen
- permettent, par comparaison aux objectifs, d'identifier les actions de conception ou d'amélioration de l'entité
- peuvent également concerner le suivi des performances d'un système en exploitation
- utilisent un ensemble d'outils et de méthodes qui consistent généralement à analyser les effets des pannes, dysfonctionnements, erreurs d'utilisation, ,…, de l'entité étudiée

Quelques méthodes et outils de la SdF:

- diagrammes de fiabilité
- analyses préliminaires de risques
- AMDE(C)
- arbres de défaillance (ou de défauts)
- graphes de Markov
- ...

Analyse préliminaire des risques (APR):

- a pour but:
  - de déceler les risques et leurs causes, c'est à dire de déterminer les éléments dangereux, les situations dangereuses, les accidents potentiels
  - de déterminer la gravité de leurs conséquences
  - de définir des règles de conception et des procédures permettant d'éliminer ou de maîtriser les situations dangereuses et les accidents potentiels ainsi mis en évidence
- qualitative
- considérée comme inductive, mais en pratique fait appel conjointement aux démarches inductive et déductive

Analyse des Modes de Défaillances et de leurs Effets (AMDE / AMDEC):

- permet de recenser les défaillances des composants dont les conséquences affectent le fonctionnement du système
- qualitative
- inductive:

  défaillance du composant → effet(s) sur le système ?

- exhaustive: analyse de tous les modes de défaillance de tous les composants du système
- avec une limite: ne traite que les défaillances simples ou uniques (ne traite pas les combinaisons de défaillances)

Introduction de la notion de criticité:

- à l'AMDE, on « ajoute » une évaluation de la criticité de chacun des modes de défaillance
- cette évaluation de la criticité impose de définir préalablement un «système de jugement», généralement constitué par:
  - des critères (fréquence, gravité, …)
  - des échelles ou des barèmes de notation
  - des seuils ou des repères à partir desquels un mode de défaillance sera considéré comme « critique »
- on peut alors « extraire » de l'AMDEC la liste des points critiques qui devront faire l'objet de modifications de conception, de contrôles périodiques, …

Méthode des arbres de défaillances:

- permet de rechercher les défaillances uniques et les combinaisons de défaillances qui conduisent à la réalisation d'un événement «indésirable»
- qualitative (dans un premier temps)
- déductive:

  défaillance(s) de quel(s) composant(s) ? ← événement ou situation du système

- permet de calculer la probabilité de l'événement «indésirable» (≈ défiabilité)
- l'événement «indésirable» doit être identifié à priori et il existe un arbre de défaillance associé à chaque événement indésirable

Méthode des graphes de Markov:

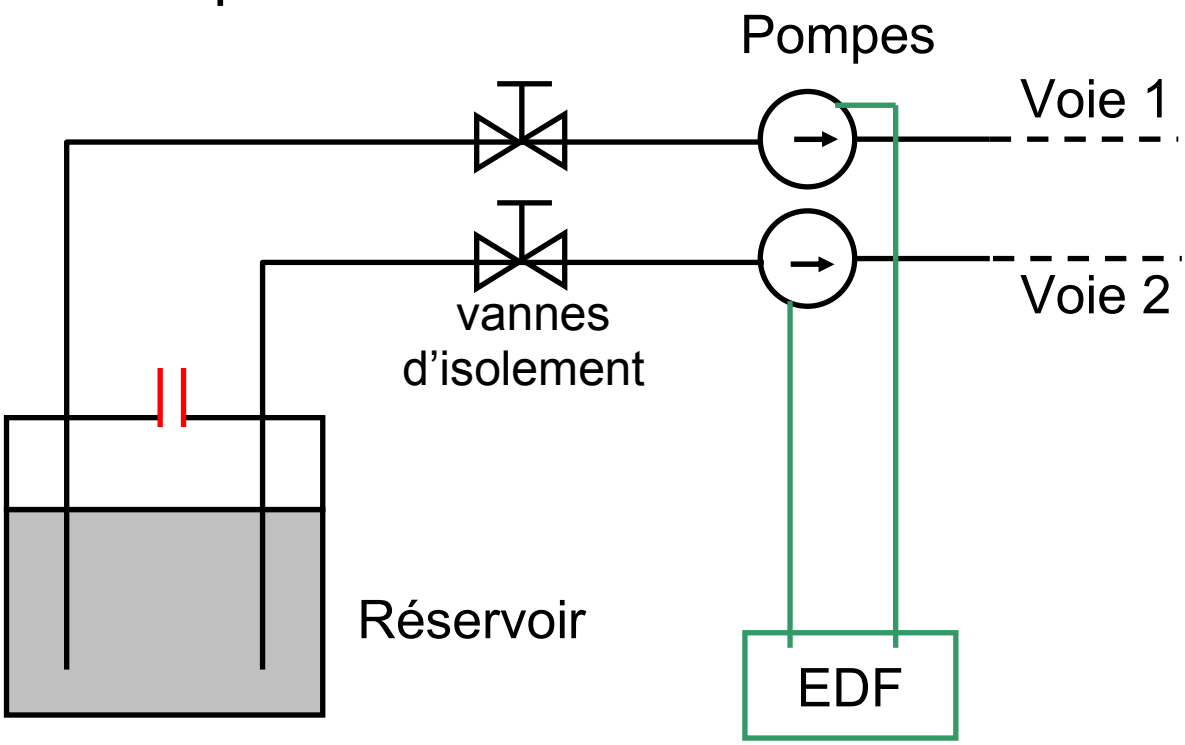
- permet d'évaluer la fiabilité et/ou la disponibilité d'un système
- on recense les différents états possibles de chacun des composants du système (en marche, en stand by, en panne, …)
- on recense les différents états possibles du système (chacun des états du système est une combinaison des états possibles des composants)
- on considère que les changements d'état du système résultent du changement d'état de ses composants (par exemple, le système passera de l'état de panne à l'état de marche par la réparation d'un composant)

COMPLEMENTS

Défaillances de mode commun:

- attention à la conception de certaines installations

- exemple:



Défaillances de mode commun (suite):

- principales «familles » de causes communes »:
  - erreurs de conception, de fabrication, d'exploitation, …
  - fautes logicielles
  - agressions de l'environnement

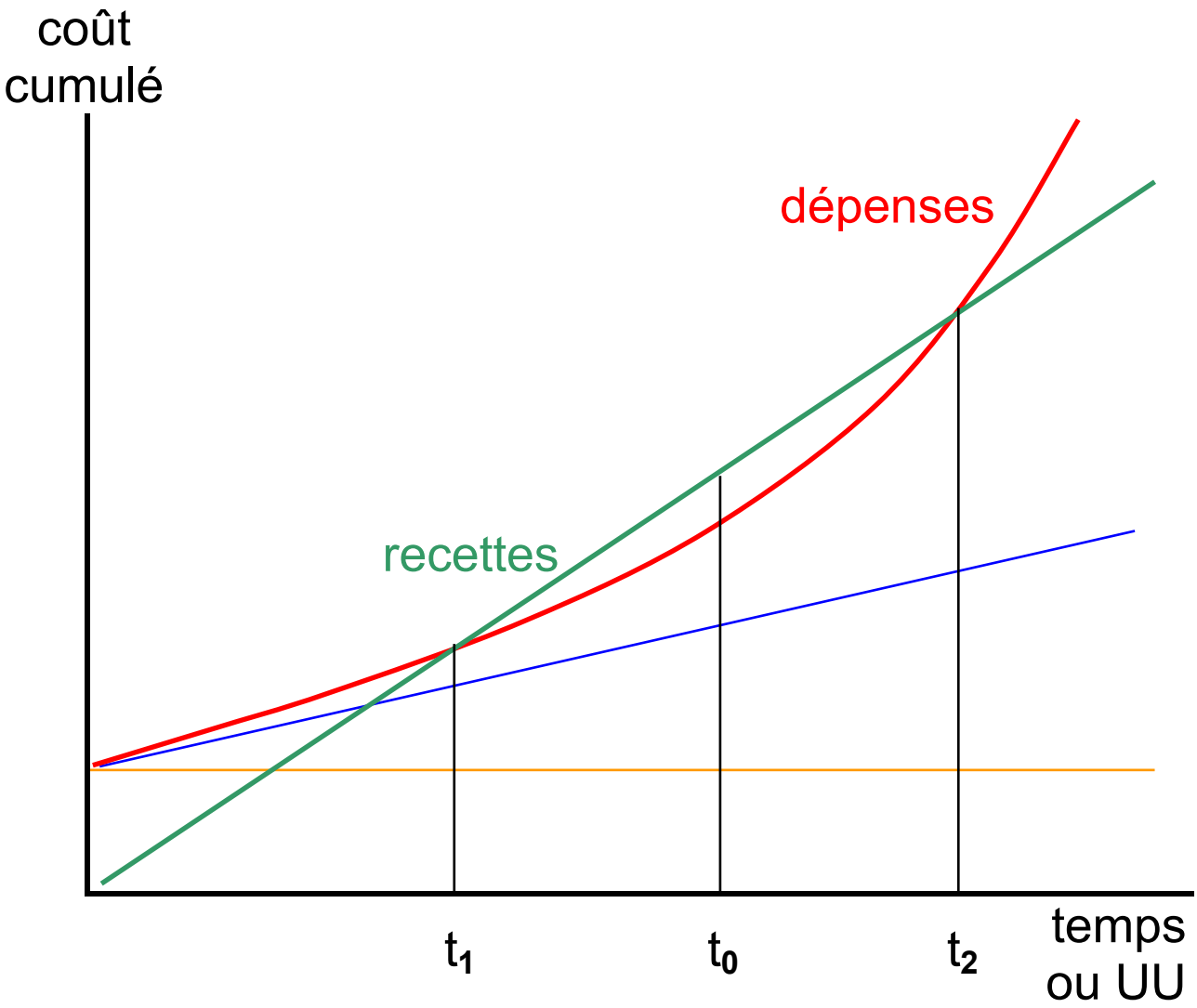
- réponse :
  - séparation: séparation physique, séparation des alimentations, affectation de composants à une seule fonction, …
  - diversité : fonctionnelle, matérielle, logicielle, humaine

Fiabilité humaine:

- la fiabilité globale d'un système est la résultante de:
  - la fiabilité des composants techniques
  - la fiabilité des composants humains
- l'erreur humaine est considérée comme un équivalent fonctionnel des défaillances techniques qui affectent le système
- à ce titre, on peut identifier des « modes d'erreur » (équivalents aux modes de défaillance): oubli, fausse manœuvre, action intempestive, …
- on cherchera à évaluer l'effet du mode d'erreur sur le système (et / ou sur son taux de défaillance)

ASPECTS ECONOMIQUES

Remplacement des matériels:

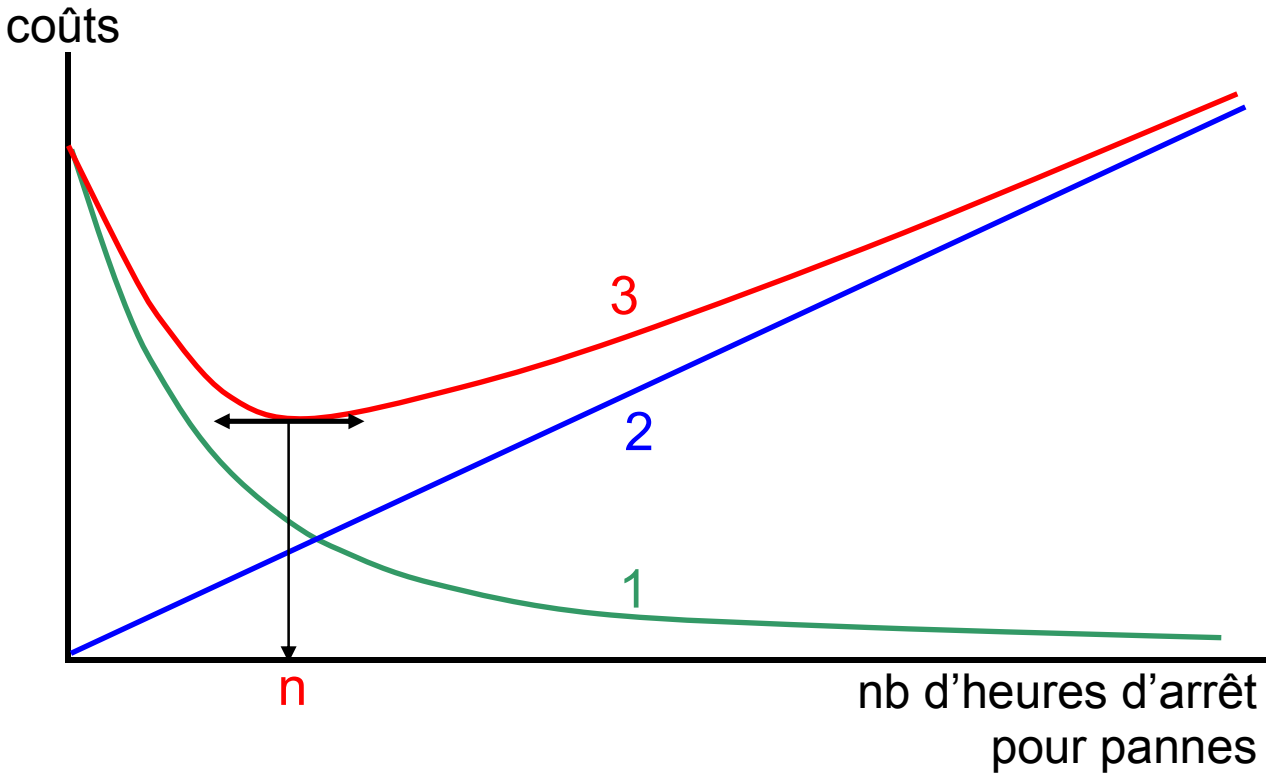


t_1 = « point mort bas » ou retour d'investissement

t_2 = « point mort haut »

t_0 ⟷ bénéfice maxi

Coûts de maintenance:



1 = coût de maintenance préventive
2 = coût des arrêts de production
3 = coût total = 1 + 2

- si l'on recherche le coût total minimal, il faut « admettre » n heures d'arrêt pour pannes

SYNTHESE

Synthèse :

- la SdF, un concept global, qui ne peut pas être caractérisé par une grandeur unique, mais par plusieurs paramètres
- l'utilisateur ou l'exploitant devra exprimer ses besoins par référence à ces paramètres : fiabilité ou disponibilité recherchées, temps d'arrêt maximum, niveau de risque acceptable,…
- le concepteur devra vérifier que les solutions retenues satisfont à ces besoins, en mettant en œuvre les méthodes et outils de la sûreté de fonctionnement

Synthèse (suite) :

- l'approche probabiliste et l'acceptation du risque peuvent s'avérer quelque peu « dérangeantes » lorsque les conséquences sont du type arrêt total de la production, atteinte à la sécurité des personnes ou de l'environnement,….
- ces conséquences graves ne peuvent être acceptables que si la probabilité de leur occurrence est faible (voire infime), mais elle ne sera jamais nulle

Synthèse (suite) :

- les équipements actuels comportent des milliers de composants constituant autant de sources de pannes potentielles, dont les conséquences peuvent être graves et/ou coûteuses
- la réparation des pertes d'exploitation, ou des atteintes à la santé des personnes ou à l'environnement, … résultant de ces dysfonctionnements font aujourd'hui souvent l'objet de procédures judiciaires
- il n'est alors plus possible de faire l'impasse sur une réflexion structurée débouchant sur des choix raisonnés
- tels sont les enjeux de la sûreté de fonctionnement