Management des Risques Industriels

Déploiement de la Sûreté de Fonctionnement:

Notions, Méthodes, Cycle de Vie

Pierre DAVID pierre.david@grenoble-inp.fr

Plan

1. Introduction à la cindynique : terminologie, définition
2. Vocabulaire et Grandeurs de la SdF
3. Cycle de réalisation des analyses de SdF : présentation des techniques et des méthodes de SdF et de leurs interactions
    1. Le cycle de gestion des risques
    2. Analyse Préliminaire des Risques
    3. AMDEC
    4. Arbres de défaillances et Diagrammes Bloc de Fiabilité
    5. Modèles avancés d'analyse de SdF
4. IEC 61508 : Exemple de standards de développement de systèmes à fortes contraintes de SdF

INTRODUCTION A LA CINDYNIQUE

Plan

- Historique
- Approche cindynique
- Hyperespace cindynique
- La notion de risque
- Déficits Systémiques Cindynogènes
- Faute erreur défaillance

Cindyniques ?

- Sciences de danger (**Cindyniques**):

Les « Sciences de danger » sont une discipline à part entière. Il s'agit d'un **domaine scientifique horizontal** et non vertical, c'est à dire plongeant ses racines dans toutes les disciplines existantes.

Cindynique vient du grec kindunos ou kindynos, qui signifie " danger ".

Historique

Flixborough (1974)	Explosion nuage de gaz	28 morts, 80 blessés 2450 maisons endommagées
Seveso (1976)	Fuite de dioxine	200 blessés, 700 évacués
Tchernobyl (1986)	Fusion du cœur	31 morts immédiats, 200 irradiés, 135000 évacués 1 M sous contrôle médical 2 M d'hectares de terres agricoles contaminés
Challenger (1984)	Explosion après une fuite de gaz à travers un joint.	7 morts, Traumatisme aux USA Dégradation de l'image de la NASA
Ariane 5 (1996)	Explosion après perte de la centrale inertielle.	Explosion de la fusée et des satellites transportés. Perte de 370 M$

Approche Cindynique

La cindynique peut se définir comme la science visant à maîtriser les dangers en développant et en exploitant les outils, les méthodes et les techniques propres à améliorer et à optimiser la sécurité.

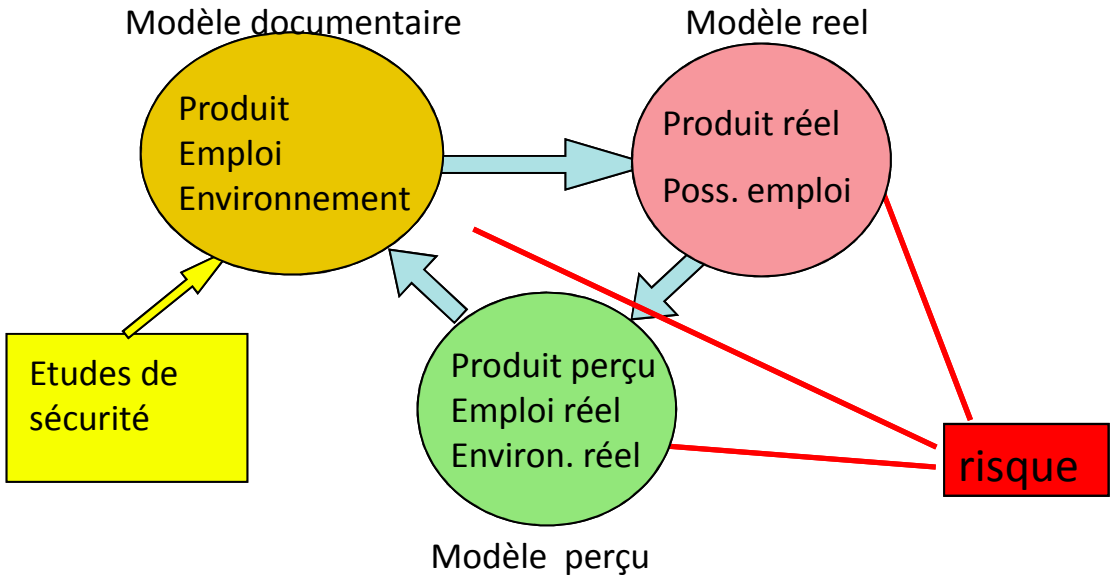
C'est une discipline à part entière qui évalue et tente de prévenir les dangers induits par une activité.

Dans le domaine des risques, ce que l ’on cherche, c ’est bien de les éviter.

Dans cette volonté de maîtrise des risques, une partie traite des activités de Sûreté de Fonctionnement ou FMDS (Fiabilité, Maintenabilité, Disponibilité, Sécurité).

Approche Cindynique / Approche Système

- Prendre une décision c'est prendre un risque
- Le "risque nul" n'est pas atteignable



- Un système est un ensemble d'éléments matériels, humains, logiciels, informatifs en interaction pour remplir une (des) mission(s) dans un environnement de référence.

Approche Cindynique / Approche Système

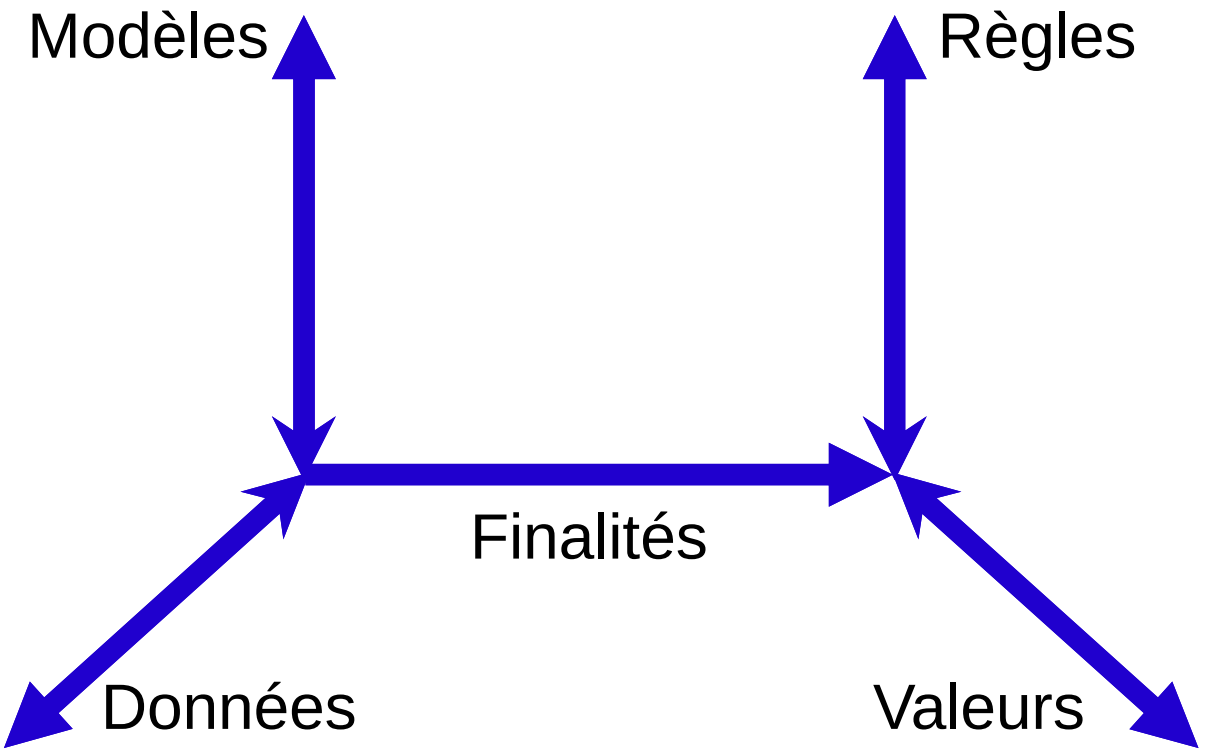
- Pour comprendre et prévenir les accidents et grandes catastrophes la démarche cindynique se développe autour de 2 axes :

  - définir le système le plus global possible rendant compte d'une activité humaine, de la façon dont elle est organisée, conduite et contrôlée ;

    (Système + Environnement + Conception + Management durant et après conception …)
  - identifier dans ce système les déficits expliquant les erreurs commises (ou pouvant être commises) par le système dans son ensemble.

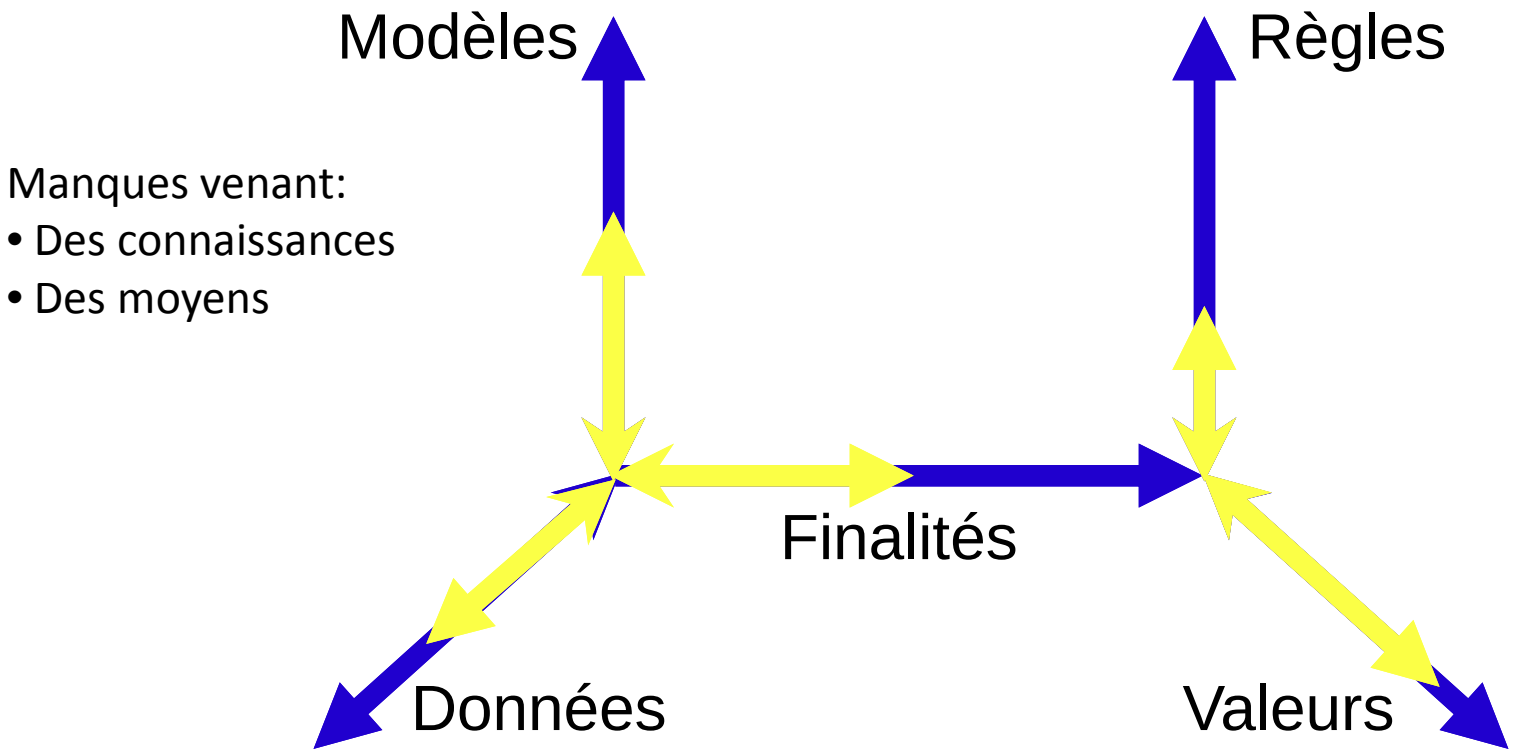
Hyperespace Cindynique

- Hyperespace du danger



Hyperespace Cindynique

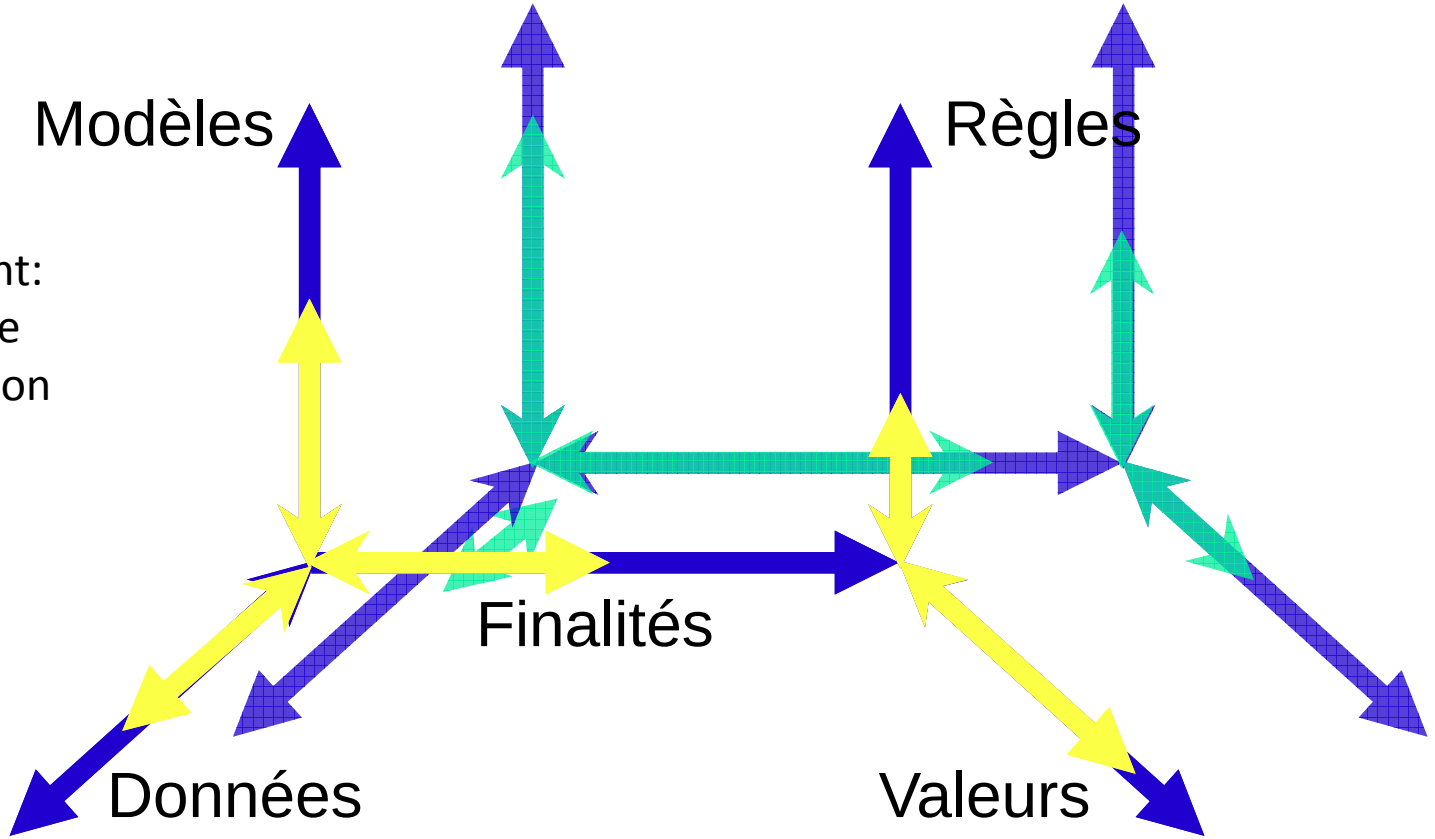
- Recherche des écarts / déficits



Hyperespace Cindynique

- Recherche des dissonances

Manques venant:
- Du vocabulaire
- De la perception



Vocabulaire du Risque

- Danger :

Situation susceptible d'engendrer des évènements indésirables.

- Risque :

Mesure du niveau de danger, fonction de la probabilité d'occurence de l'évènement indésirable et des conséquences (gravité) de cet évènement.

- Sécurité :

- Absence de circonstances susceptibles de conduire à des dégâts humains ou matériel (USA).

- Ensemble des actions destinées à assurer la protection des personnes et des biens contre les dangers, nuisances ou gênes susceptibles d'être provoquées par les installations ou lors du transport de matières dangereuses (UE).

- Protection contre les évènements fortuits (sinistres, catastrophes naturelles) et secours aux personnes et aux biens affectés par ces évènements (sécurité civile) .

- Sûreté :

- L'ensemble des mesures à prendre dans les installations ou lors du transport de matières dangereuse en vue d'éviter les accidents et de minimiser leurs effets (UE)

- Ordre public, protection contre la malveillance (police, gendarmerie) .

Vocabulaire du Risque

- Dans le domaine des systèmes :
  - Sécurité : Aptitude d'une entité à éviter de faire apparaitre, dans des conditions données, des événements critique ou catastrophique [Villemeur].
  - Sûreté « de Fonctionnement »: Aptitude d'une entité à satisfaire à une ou plusieurs fonctions requises dans des conditions données [Villemeur].

Le Risque

- Le risque est la mesure du danger

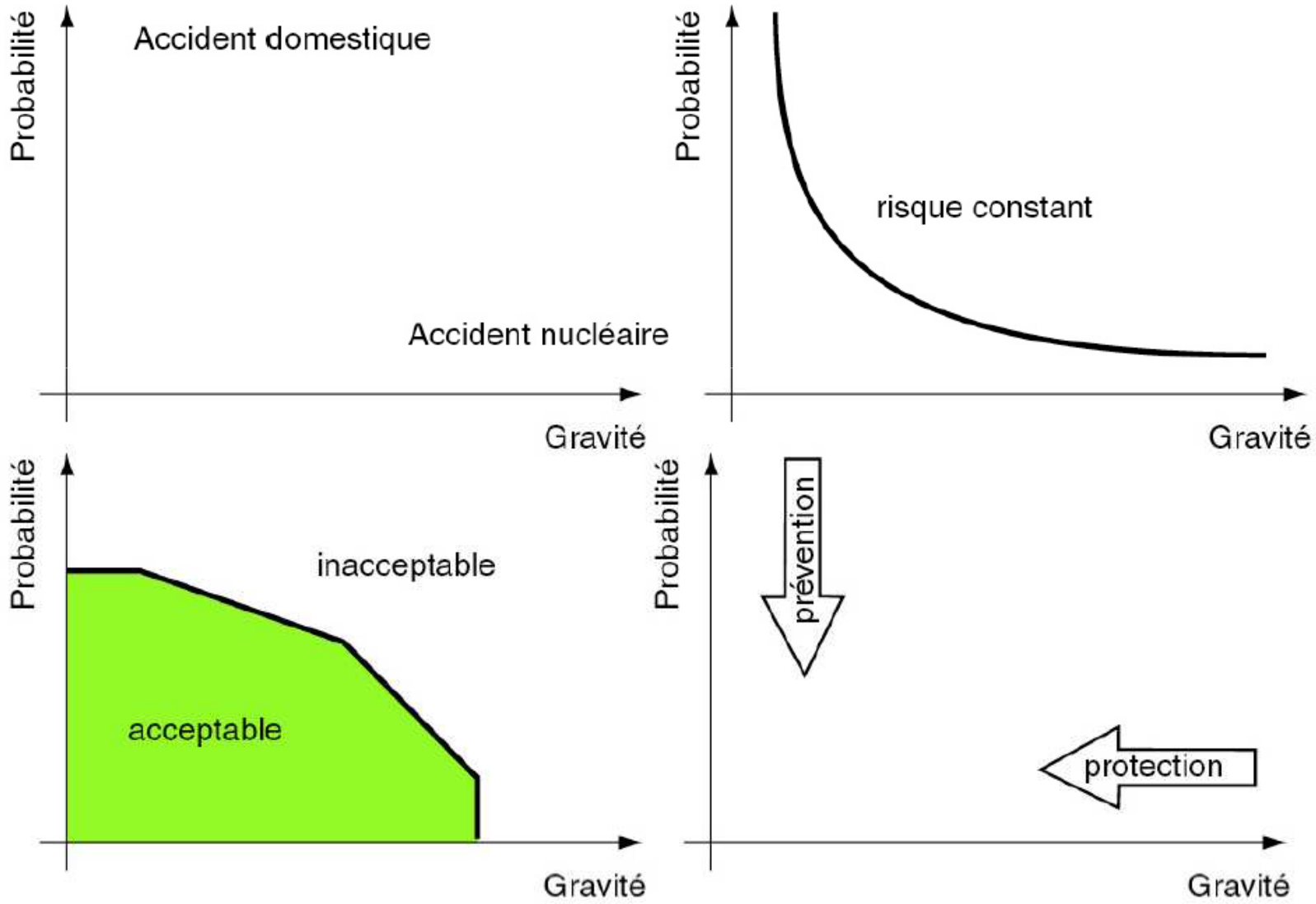
Probabilité d'un événement

Gravité des conséquences potentielles

R = P x G

Mesure du niveau de danger, fonction de la **probabilité** d'occurrence de l'évènement indésirable et des **conséquences** (gravité) de cet évènement.

Espace du danger



Déficits systémiques cindynogènes

Domaine du déficit	Numéro du DSC	Désignation du DSC	Symptômes classiques
CULTUREL	DSC 1	Culture d'infaillibilité	Nous sommes sûrs du succès. Ce système est garanti contre toute défaillance.
	DSC 2	Culture de simplisme	Notre affaire n'est pas complexe. Nous rejetons l'idée de système. Ça marche sans méthodes complexes.
	DSC 3	Culture de non communication	On ne peut vivre en remettant en question certaines vérités évidentes de notre métier. La hiérarchie de notre entreprise supporte mal la remise en question des pratiques techniques. On discute peu entre nous des opérations pratiques. Le personnel parle Hindi, l'équipage le portugais, les passagers le norvégien.
	DSC 4	Culture Nombriliste	Nous sommes les leaders et nous économisons pas mal de temps du fait que nous n'allons pas voir ailleurs ce qui se passe. Nous avons toujours été les premiers à percevoir les problèmes de notre profession. Nous sommes certains du retard de nos concurrents en matière de sécurité.

identifier les déficits culturels, organisationnels ou manageriels pouvant mener (ou contribuer) à une catastrophe.

Déficits systémiques cindynogènes

Domaine du déficit	Numéro du DSC	Désignation du DSC	Symptômes classiques
ORGANISATION	DSC 5	Subordination des fonctions de gestion du risque aux fonctions de production ou a d'autres fonctions de gestion créatrices de risques	Le responsable de la sécurité n'est qu'un collaborateur parmi d'autres du responsable de production. On ne va tout de même pas réduire les prérogatives du chef de production ou lui compliquer la tâche. On crève sous les fonctionnels, ce n'est pas le moment d'en inventer un autre. D'accord, il y a des risques, mais ce n'est pas pour semer le désordre dans nos structures.
	DSC 6	Dilution des responsabilités. Non explicitation des tâches de gestion des risques. Non affectation des tâches à des responsables désignés.	Nous avons rejeté tout formalisme dans notre organisation, chacun peut s'exprimer avec spontanéité. Les gens sont adultes et savent parfaitement ce qu'ils doivent faire sans qu'il soit utile de le leur rappeler.

Déficits systémiques cindynogènes

Domaine du déficit	Numéro du DSC	Désignation du DSC	Symptômes classiques
MANAGEMENT	DSC 7	Absence d'un système de retour d'expérience.	Maintien de pratiques considérées comme dangereuses dans d'autres établissements ou organisations. Pas d'attention aux signes précurseurs apparaissant dans la même profession. Pas d'exploitation systématique des faits concernant les dysfonctionnements survenus mondialement dans le même domaine technique.
	DSC 8	Absence d'une méthode cindynique dans l'organisation.	Dans ce secteur, il faut reconnaître qu'il n'y avait pas de manuel ou d'instruction écrite de la direction.
	DSC 9	Absence d'un programme de formation aux cindyniques adapté à chaque catégorie de personnel.	Les gens des ateliers ont été pris au dépourvu et ont commis des erreurs qui ont aggravé les choses.
	DSC 10	Absence de planification des situations de crise.	Quand on a entendu ce bruit épouvantable, tout le monde s'est mis a courir dans toutes les directions.

Analyse d'accident : Challenger

Chronologie des événements

Dans la nuit du 27 au 28 janvier 1986 : Des ingénieurs s'inquiètent du fait que le mercure est maintenu en dessous du point de congélation et annoncent que Challenger n'est pas prête à endurer un tir dans ces conditions. **Leur avis est ignoré**.

28 janvier 1986 : Il fait deux degrés sur l'aire de départ, alors **qu'aucun décollage n'avait jamais eu lieu en dessous de 9°C**.

28 janvier 1986, 11h38 heure locale (heure H) : Décollage de Challenger

H + 8s : La navette se dirige vers l'Atlantique. « Tout va bien » déclare le commandant Scobee depuis la navette.

H + 21s : Manœuvre de roulis terminée. Challenger s'éloigne normalement de l'aire de lancement.

H + 58s : La navette traverse une cellule orageuse d'une **intensité jamais connue** lors des précédents vols.

Challenger est soumise à une pression énorme (3.5 tonnes de pression par mètre carré). Le joint de la fusée à poudre droite cède. Une flamme d'une température deux fois plus élevée que la température de fusion de l'acier s'en échappe

H + 64.66s : La flamme a percé le réservoir d'hydrogène et s'y alimente.

H + 72.20s : Désintégration de la navette Challenger

A cette époque la Nasa venait de réaliser 24 missions sur une période de 57 mois 7 lancements Columbia, 6 lancements Discovery, 2 Atlantis et 9 Challenger.

La Nasa industrialisait le rythme de ses lancements.

Analyse d'accident : Challenger

- Quels DSC sont mis en évidence dans cet accident?
  - DSC 1 : culture d'infaillibilité,
  - DSC 3 : non communication,
  - DSC 7 : Absence de REX,
  - DSC 5 : Subordination de la sécurité à la production,
  - (DSC 4 : nombrilisme)

Analyse d'accident : Bhopal

Chronologie des événements 3 dec. 1984

A l'usine de Bhopal, située dans l'état du Madhya Pradesh, d'Union Carbide, une fuite se produit dans le réservoir 610 contenant de l'isocyanate de méthyle.

Un nuage de methylisocyanate se répand sur les populations avoisinantes. Les autorités n'étaient absolument pas préparées à ce type d'accident. On dénombre 323 morts et 260 000 blessés dont près de 9 000 sont frappés d'incapacité partielle et permanente. En 1990, soit six ans après cette catastrophe, on enregistre encore un décès par jour parmi les victimes atteintes par l'agression chimique.

En 1975, le gouvernement indien avait autorisé Union Carbide India Ltd à produire le Sevin, insecticide produit a partir du MIC, intermédiaire chimique de cette production. Le nuage de methylisocyanate est du à une réaction entre le MIC et l'eau.

L'absence d'obturateur dans les tuyaux au cours d'une opération de nettoyage, a permis à l'eau de pénétrer dans le réservoir 610.

L'absence d'obturateur est due au fait que personne ne l'a mis en place. Les ouvriers attribuent cela à la suppression du poste de responsable de l'entretien quelques jours avant.

La direction d'Union Carbide avait, en effet, pris une série de mesures d'économie qui affaiblissaient les fonctions d'entretien et de sécurité. On peut y voir une confirmation dans le fait que les tours d'épuration et la torchère vers lesquelles les consignes obligeaient à aiguiller toute fuite d'isocyanate n'étaient pas en état de traiter cette fuite, étant hors service ou arrêtées pour entretien.

Analyse d'accident : Bhopal

Chronologie des événements 3 dec. 1984

Les ouvriers soulignent également les faits suivants :

- les panneaux et les instructions de travail, dans l'usine, étaient écrits en anglais, alors que la majorité des travailleurs ne comprenaient que l'hindi, la formation de ces personnels était insuffisante.
- des accidents précurseurs s'étaient produits dans l'usine
  - en décembre 1981, une fuite de phosgène avait entraîné 1 mort et 2 blessés ;
  - en janvier 1982, une fuite de MIC avait fait 15 victimes ;
  - en août 1982, un technicien avait été brûlé par le MIC ;
  - en octobre 1982, une fuite de MIC et d'acide chlorhydrique, avait touché des personnes à l'intérieur et à l'extérieur de l'usine.

Analyse d'accident : Bhopal

- Quels DSC sont mis en évidence dans cet accident?
  - pas d'analyse des incidents précurseurs : DSC 7, DSC 3
  - pas d'instructions compréhensibles pour le personnel qui parle parfois l'hindi : DSC 8 et DSC 9, DSC 3
  - absence d'un plan de crise : DSC 10.
  - la dilution des responsabilités entre autorité publique et direction d'entreprise : accumulation des bidonvilles à proximité d'installations aussi dangereuses DSC 6,
  - l'absence de personnel d'entretien au moment d'opérations délicates est le fruit d'une mauvaise organisation de la sécurité : DSC 5,
  - le sentiment de quasi-infaillibilité des procédés d'Union Carbide aux Etats-Unis explique la très grande surprise, encore aujourd'hui manifestée, devant ce qui s'est produit en Inde DSC 1 et DSC 4.

LA SÛRETÉ DE FONCTIONNEMENT

Plan

- Définition
- Approche
- Les défaillances : définition, classification
- De la faute aux défaillances
- Les composantes de la sûreté de fonctionnement (SdF)
- Les temps caractéristiques de la SdF
- Réflexion sur le terrain

Définition

Le but de la **sûreté de fonctionnement** (dependability, SdF) est d'**évaluer** les risques potentiels, **prévoir** l'occurrence des défaillances et tenter de **minimiser** les conséquences des situations catastrophiques lorsqu'elles se présentent.

Définition de Laprie 89 : la sûreté de fonctionnement d'un système *informatique* est la propriété qui permet de placer une confiance justifiée dans le service qu'il délivre.

Définition CEI 50(191) : Aptitude d'une entité à assumer une ou plusieurs fonctions requises dans des conditions données.

Approche

- **Identifier** les défaillances de la manière la plus exhaustive possible.
- **Prioriser** l'importance des risques qu'elles impliquent.
- D'un point de vue système il faudra **prévoir** les défaillances.
- Au cours de la vie du système il faudra savoir **mesurer** les défaillances et **capitaliser** ces observations.
- Le but final étant bien sûr de **maîtriser** ces défaillances.

La SdF est ainsi qualifiée parfois de « sciences des **défaillances** ».

Les défaillances

- Définition CEI 50(191) :

  La défaillance est la cessation de l'aptitude d'une entité à accomplir une fonction requise.

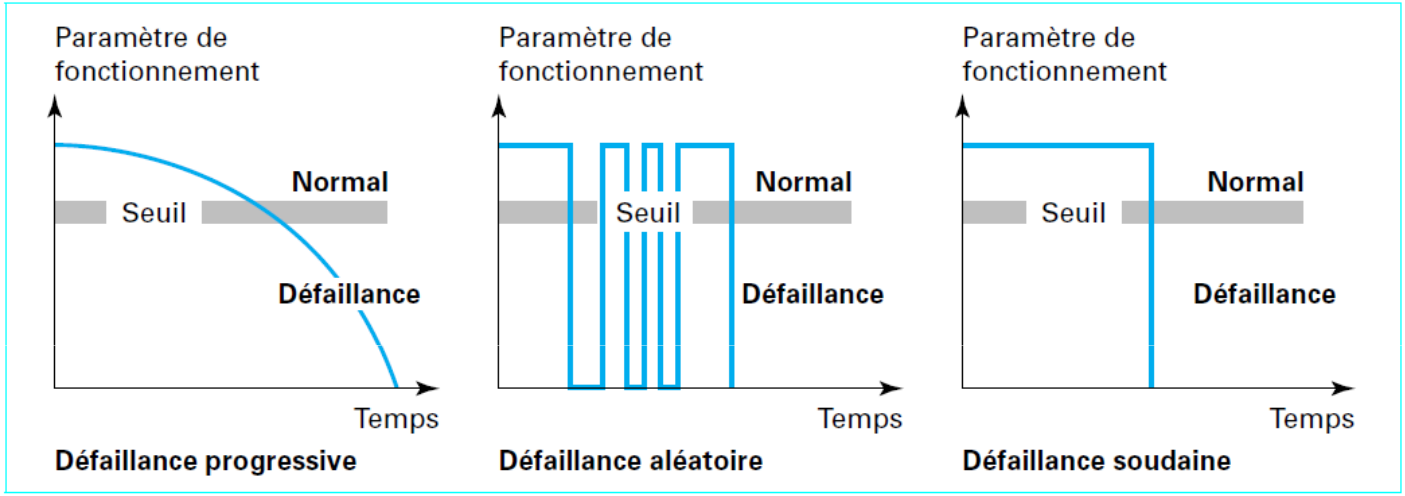
- La défaillance est un **événement**, elles est donc présente ou non et peut se combiner avec un ou plusieurs événements.

- La définition précédente implique la connaissance de la fonction requise et la définition de sa cessation.

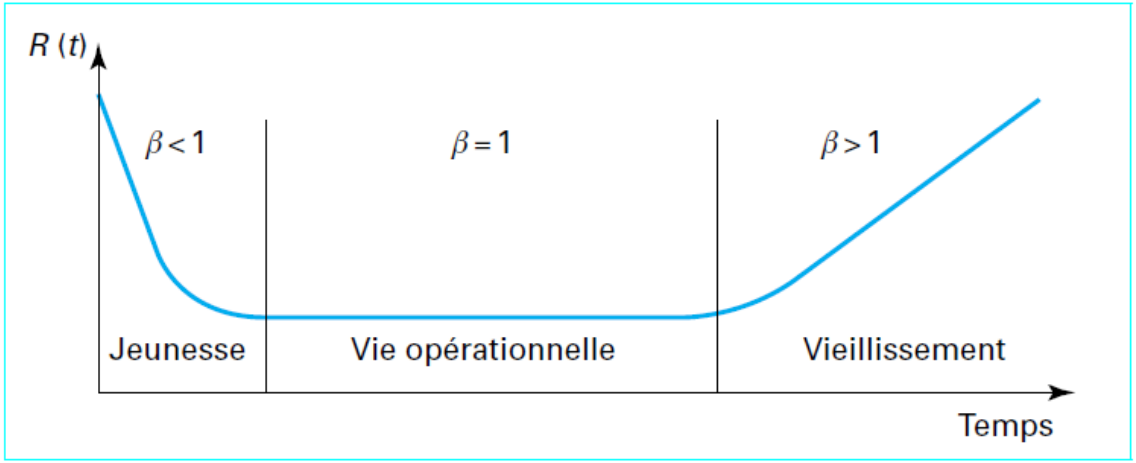
- Plusieurs classifications des défaillances sont alors possibles.

Classification des défaillances

- Par la rapidité d'apparition :



- Par date d'apparition :



Classification des défaillances

- Par les effets :
  - **Défaillance mineure** : nuit au bon fonctionnement en causant un dommage négligeable au système ou à son environnement. Pas de risque humain.
  - **Défaillance significative** : nuit au bon fonctionnement sans dommage notable. Pas de risque humain important.
  - **Défaillance critique** : perte de ou des fonctions essentielles du système. Dégâts important au système ou son environnement. Pas de risque motel ou de blessure pour l'homme.
  - **Défaillance catastrophique** : perte de ou des fonctions essentielles du système. Dégâts important au système ou son environnement. Risque mortel ou de blessures graves pour l'homme.

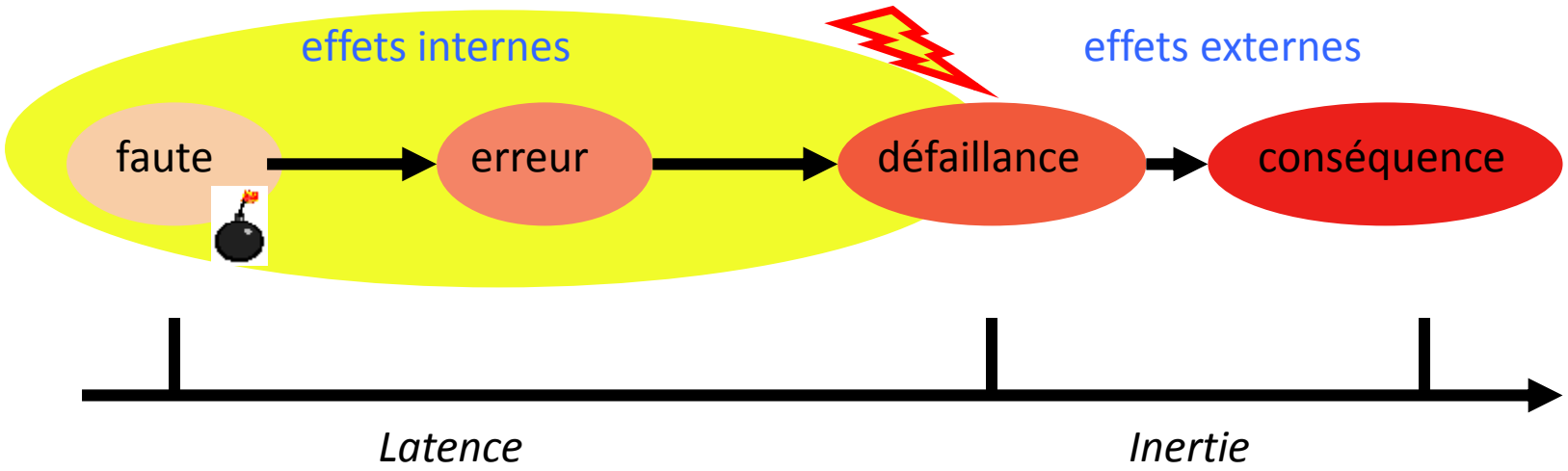
Classification des défaillances

- Par les causes :
  - **défaillance primaire** (ou première) d'une entité: dont la cause directe ou indirecte n'est pas la défaillance d'une autre entité.
  - **défaillance secondaire** (ou seconde) d'une entité : dont la cause directe ou indirecte est la défaillance d'une autre entité. L'entité devenant alors indisponible (nécessité de réparation) après disparition de la cause.
  - **défaillance par (de) commande** d'une entité: dont la cause directe ou indirecte est la défaillance d'une autre entité, mais elle redevient disponible après disparition de la cause.

Ceci implique que l'on recherchera la cause de la défaillance

De la faute à la défaillance

- Faute : cause interne de la défaillance
- Erreur : manifestation interne (signal/état incorrect)
- Défaillance : service rendu incorrect
- Conséquence : manifestation externe



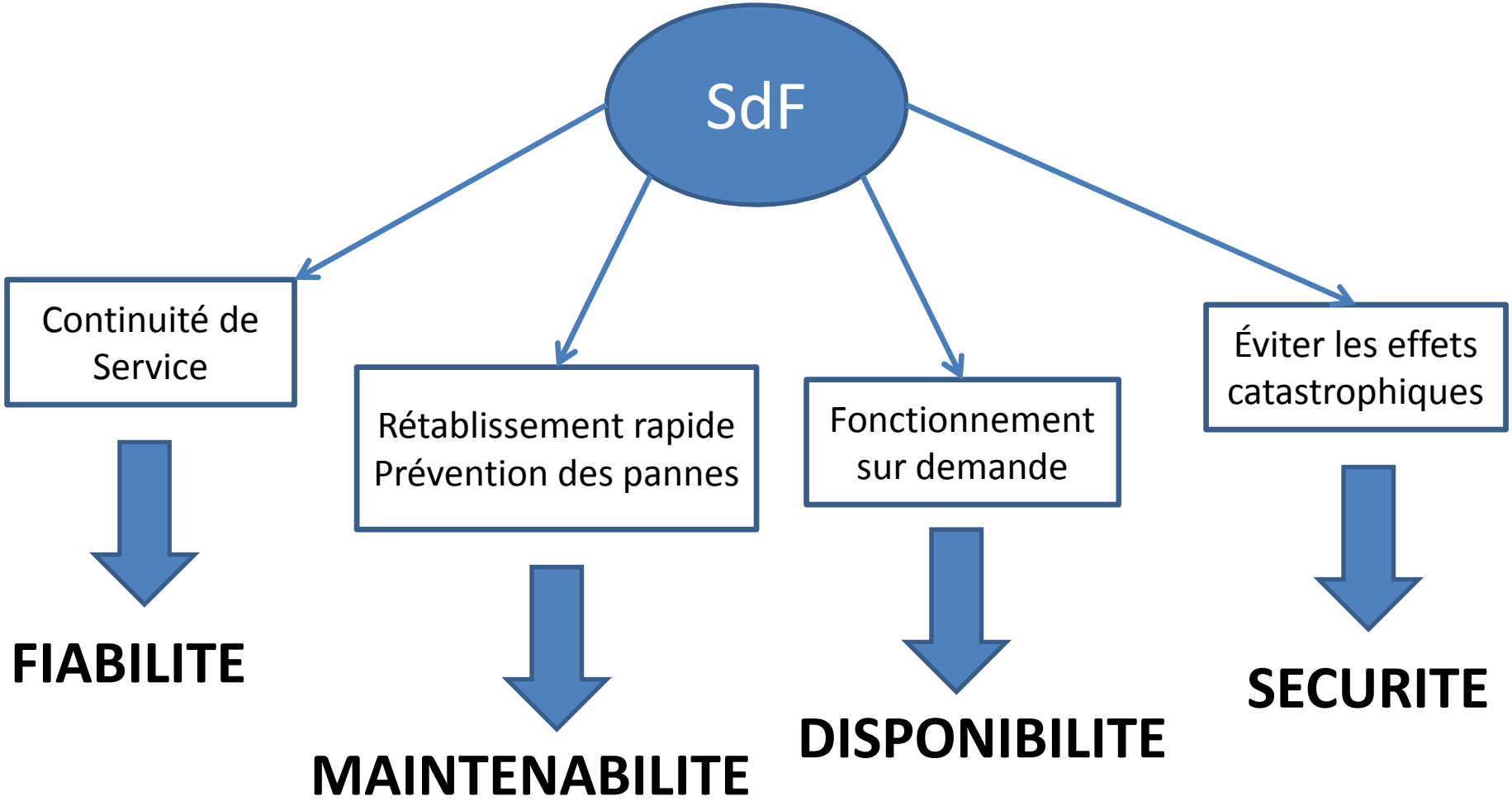
La faute peut être introduite par le concepteur, l'utilisateur ou l'environnement. Elle rend l'entité imparfaite.

Classification des fautes

On peut donner quelques critères de classification des fautes :

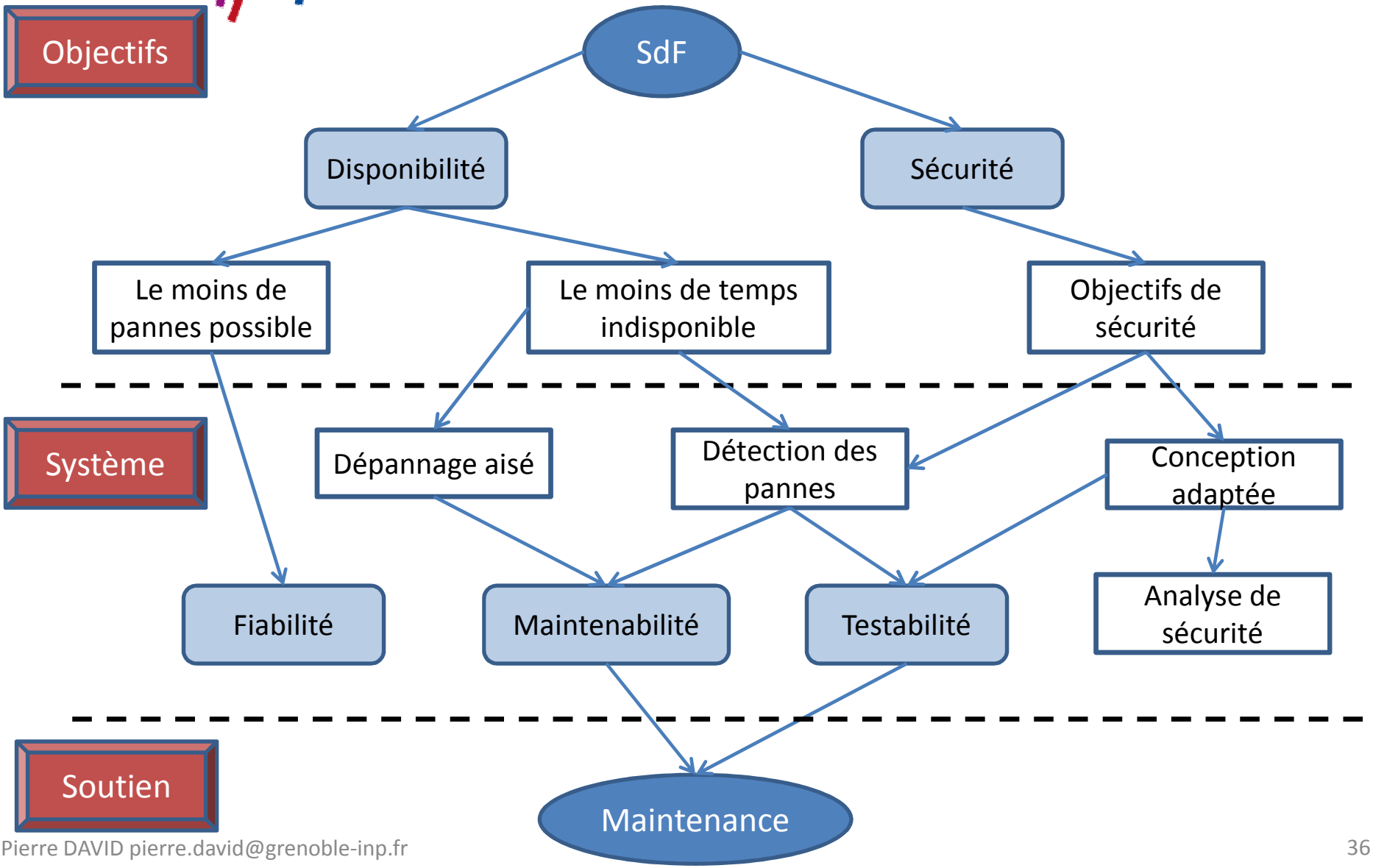
- Accidentelle
- Physique
- Interne
- Active (qui produit une erreur)
- Douce
- Permanente
- Opérationnelle
- Intentionnelle
- Humaine
- Externe
- Dormante
- Dure
- Temporaire / Transitoire
- De conception

Les composantes de la SdF



FMDS

Les composantes de la SdF



La Fiabilité

- **Définition** CEI 50(191) : la fiabilité est l'aptitude d'une entité à accomplir une fonction requise, dans des conditions données, pendant un **intervalle de temps** donné.

- **Mesure** : La fiabilité se mesure par la **probabilité** qu'une entité accomplisse une fonction requise dans les conditions données pendant l'intervalle de temps [o,t].

- **Evaluation(s)** : opérationnelle (observée), extrapolée, prévisionnelle (conception + fiab. Composant), intrinsèque (programme d'essai).

La Fiabilité

Considérons l'instant **T** d'occurrence de la défaillance ; cette variable aléatoire permet de définir la notion de fiabilité qui s'interprète comme la probabilité que l'entité considérée ne tombe pas en panne avant un instant t donné ou bien comme la probabilité qu'elle tombe en panne après l'instant t.

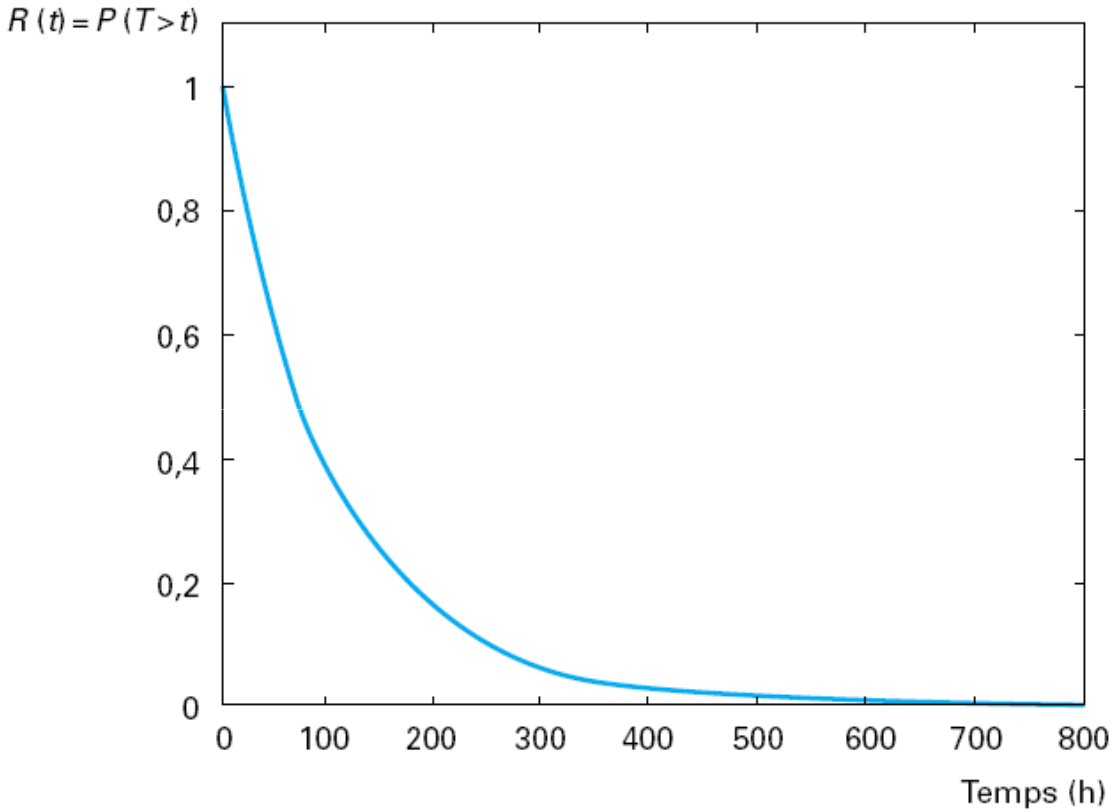
On peut noter : R (t) = P (E non défaillante sur la durée [0, t], en supposant qu'elle n'est pas défaillante à l'instant t = 0).

Ce qui peut s'exprimer par : **R (t) = P (T > t)**

L'aptitude contraire est appelée défiabilité, et est définie par :

$$F(t)= 1 - R\ (t\ ) = P(\ t> T) = F(\ t)$$

La Fiabilité



La figure représente une allure de la fiabilité R (t) en fonction du temps pour une loi exponentielle définie par :

$R(t) = \exp(-\lambda t)$ avec $t \geq 0$ et $\lambda > 0$.

La Fiabilité

Autres expressions de R(t)

R(t) = proportion de systèmes survivants = $\frac{\text{nombre de survivants à l'instant t}}{\text{nombre initial}}$

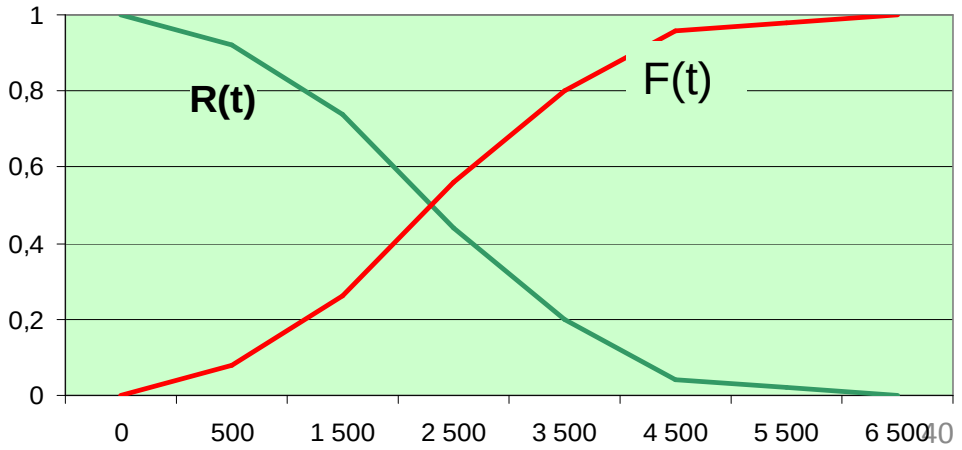
$$R(t) = \frac{N(t)}{N_0}$$

De façon à être concret !

(1) Date (t)	(2) Survivants N(t)	(3) défaillants ΔN(t)	(4) Fiab. R(t)	(5) Défiab. F(t)
0	50	0	1	0
500	46	4	0,92	0,08
1 500	37	9	0,74	0,26
2 500	22	15	0,44	0,56
3 500	10	12	0,2	0,8
4 500	2	8	0,04	0,96
5 500	1	1	0,02	0,98
6 500	0	1	0	1
N0 =		50		

F(t) est une fonction croissante de t, comprise entre 0 et 1

Loi de fiabilité et Loi de défaillance



Fiabilité : Taux de défaillance

Taux de défaillance:

A partir de la connaissance de R (t) on peut définir la notion de **taux de défaillance au temps t** qui est noté universellement par $\lambda(t)$.

Formellement $\lambda(t)\,dt$ représente la **probabilité d'avoir une défaillance entre (t, t + dt)**, sachant qu'il n'y a pas eu défaillance entre sur [0, t]. En appliquant le théorème des probabilités conditionnelles, il vient, si dt est petit :

$$\lambda(t) = -\frac{1}{R(t)}\frac{\mathrm{d}R(t)}{\mathrm{d}t}$$

Fiabilité : Taux de défaillance

Exemple de données

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

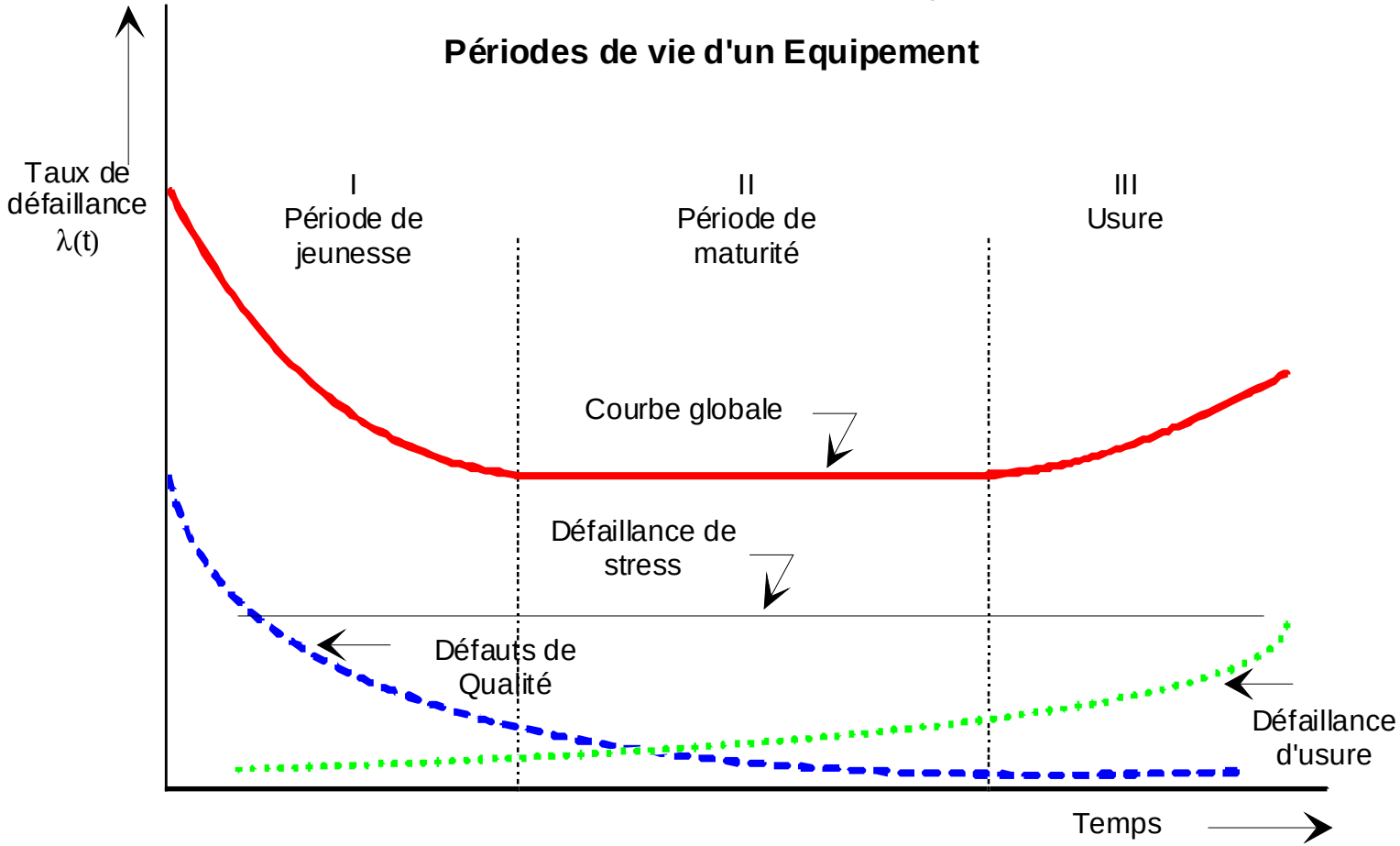
Fiabilité humaine

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

Fiabilité : Taux de défaillance

Taux de défaillance et vie du produit

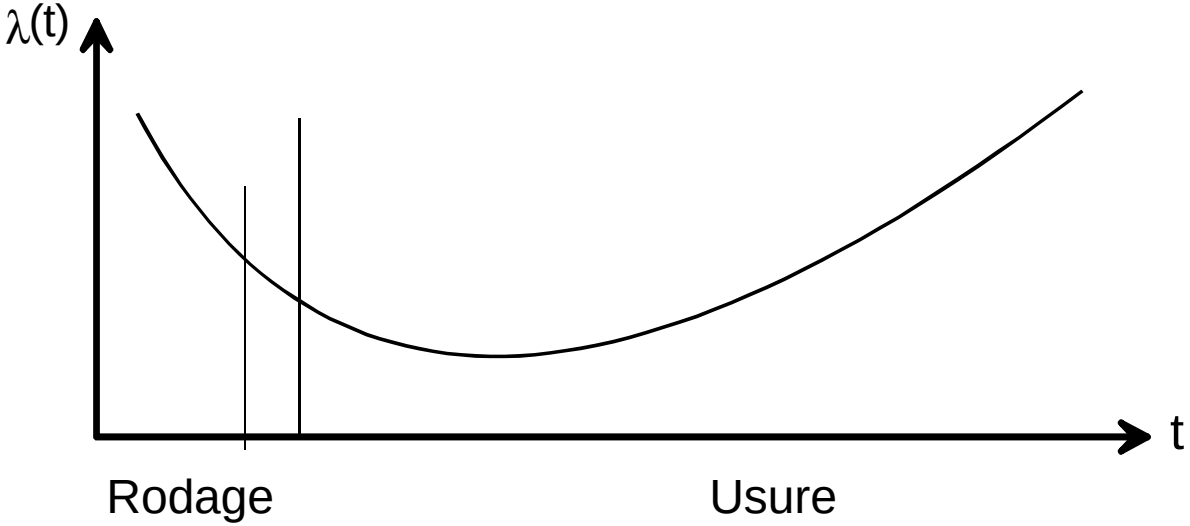


Allure d'un taux de défaillance « en baignoire »

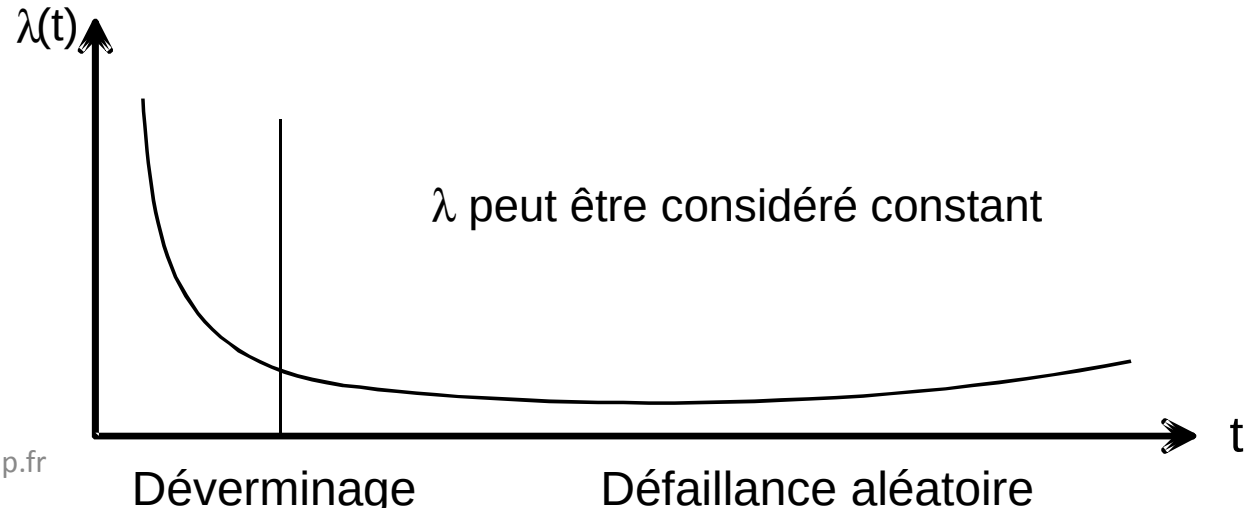
Fiabilité : Taux de défaillance

Taux de défaillance et vie du produit : domaine technologique

Mécanique



Électronique



Fiabilité : Taux de défaillance

Taux de défaillance et vie du produit : cas du λ constant

λ = constante : correspond à des défaillances survenant sans cause systématique, semblant obéir au pur hasard.

La probabilité de défaillance est la même à chaque instant de la période où λ est constant : un équipement a donc la même probabilité de défaillance à t = 0+ε qu'à t élevé.

Illustration : Si une voiture part pour un trajet de 1 000 km, la probabilité de défaillance au cours de ces 1 000 km sera la même, que la voiture ait déjà parcouru 5 000 ou 50 000 km !

Fiabilité : Loi de défaillance

- Pour anticiper les pannes on cherche à modéliser les lois de dégradation des équipements.
- Ces lois sont utilisées pour modéliser la fiabilité.
- Elles sont valables suivant le type de λ utilisé (constant ou non)
- Les principales lois de fiabilité sont :
  - Loi exponentielle : utilisée pour λ=**constante**
  - Loi de Weibull : valable **pour tout** λ (ajustable par trois paramètres)

Fiabilité : Loi de défaillance

La loi exponentielle

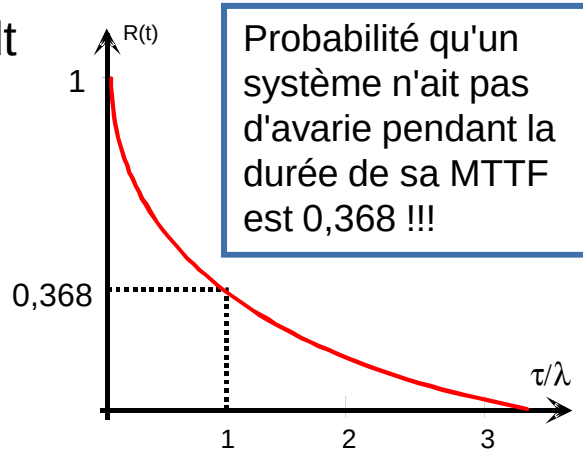
$$R(t) = \exp\left(-\int_0^t \lambda(t)\,dt\right)$$

Si $\lambda(t) = cste = \lambda$

$$R(t) = e^{-\lambda t}$$

$$MTTF = \int_0^\infty R(t)dt$$

➔ $$MTTF = \frac{1}{\lambda}$$



Probabilité qu'un système n'ait pas d'avarie pendant la durée de sa MTTF est 0,368 !!!

Fiabilité : Loi de défaillance

La loi de Weibull

$$R(t) = e^{-\left(\frac{t-\gamma}{\eta}\right)^{\beta}}$$

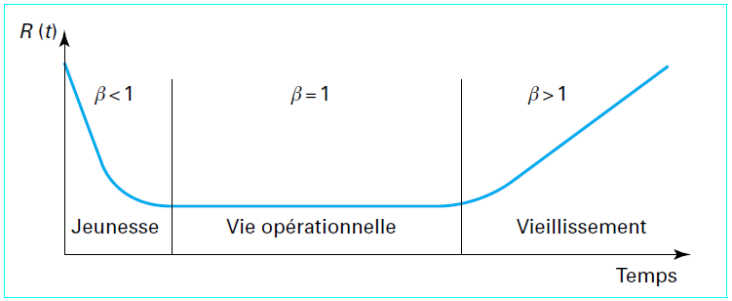
Remarque : Pour β=1 et γ=0, on retrouve la loi exponentielle

Permet d'ajuster la loi de défaillance d'un équipement pour λ constant et λ variable. Car utilise trois paramètres :

- β paramètre de forme $\beta > 0$
- γ paramètre de position $-\infty < \gamma < +\infty$
  (représente la date de début d'observation des équipements)
- η paramètre d'échelle $\eta > 0$

Interprétation selon la valeur de β

- $\beta < 1$ → λ décroît = période de jeunesse
- $\beta = 1$ → λ constant = défaillance indépendante du temps
- $\beta > 1$ → λ croît = phase de vieillesse
  - $1,5 < \beta < 2,5$ phénomène de fatigue
  - $3 < \beta < 4$ phénomène d'usure, corrosion
  - $\beta \approx 3,5$ f(t) est symétrique, loi normale



La Disponibilité

- **Définition** CEI 50(191) : l'aptitude à **être en état d'accomplir** une fonction requise dans des conditions données, à un instant donné ou pendant un intervalle de temps donné.

- **Mesure** : La disponibilité se mesure par la probabilité qu'une entité soit en état d'accomplir une fonction requise dans des conditions données à l'instant t.

  $$A(t) = P[\text{entité non défaillante à l'instant } t].$$

- **Remarques** : La disponibilité ainsi définie **ne fait pas appel à l'histoire** de l'entité, qu'elle ait été ou non réparée une ou plusieurs fois avant l'instant t (c'est en quelque sorte une probabilité non conditionnelle).

  Il est donc évident que pour un système non réparable, la disponibilité est égale à la fiabilité, et que d'une manière générale **A (t) ≥ R (t)**.

La Disponibilité

Comme la fiabilité, plusieurs types de disponibilités peuvent être utilisés :

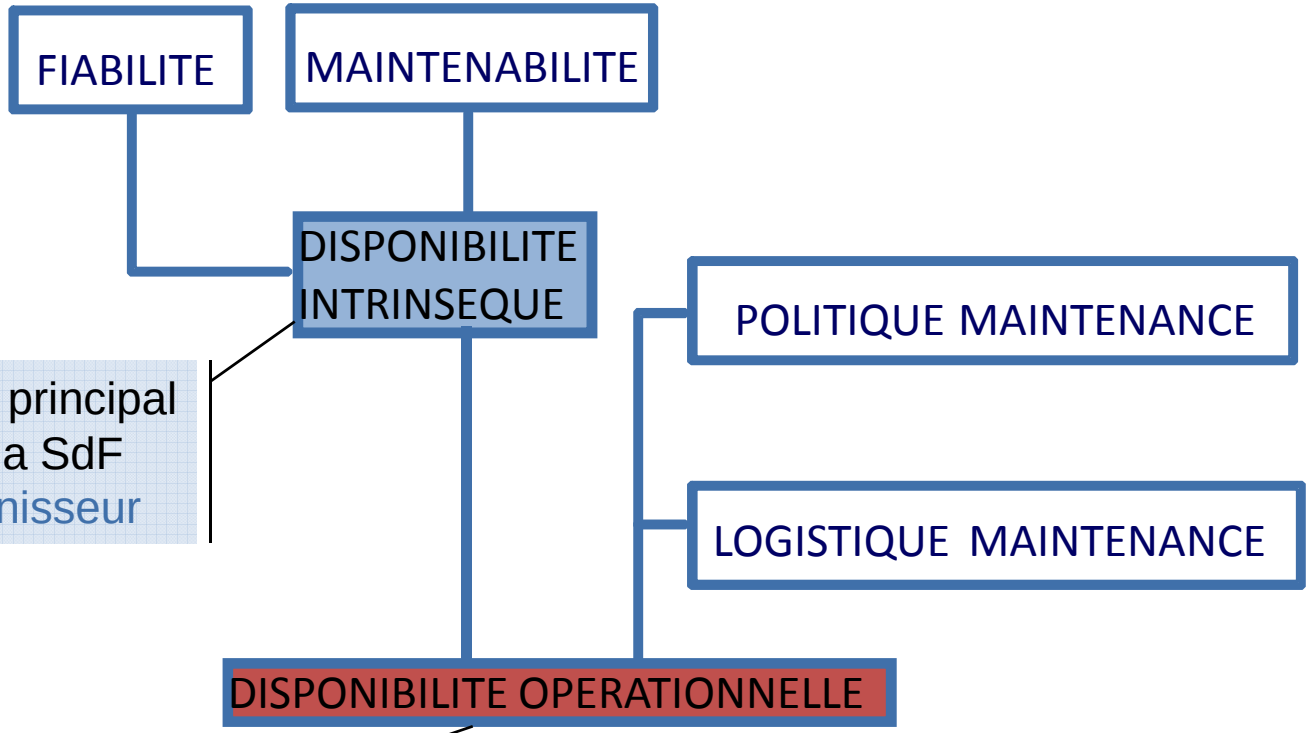
- La disponibilité **instantanée prévisionnelle** (définie précédemment)
- La disponibilité **moyenne** : moyenne sur un intervalle de temps donné [t1, t2] de la disponibilité instantanée prévisionnelle, ou mesurée en phase opérationnelle par la durée de fonctionnement effectif divisée par la durée donnée.

La disponibilité en chiffres :

- A = 99 % -> 4 jours d ’indisponibilité par an
- A = 99,9 % -> 9 heures par an
- A = 99,999 % -> 5 minutes par an

La Disponibilité

Disponibilité et cycle de vie

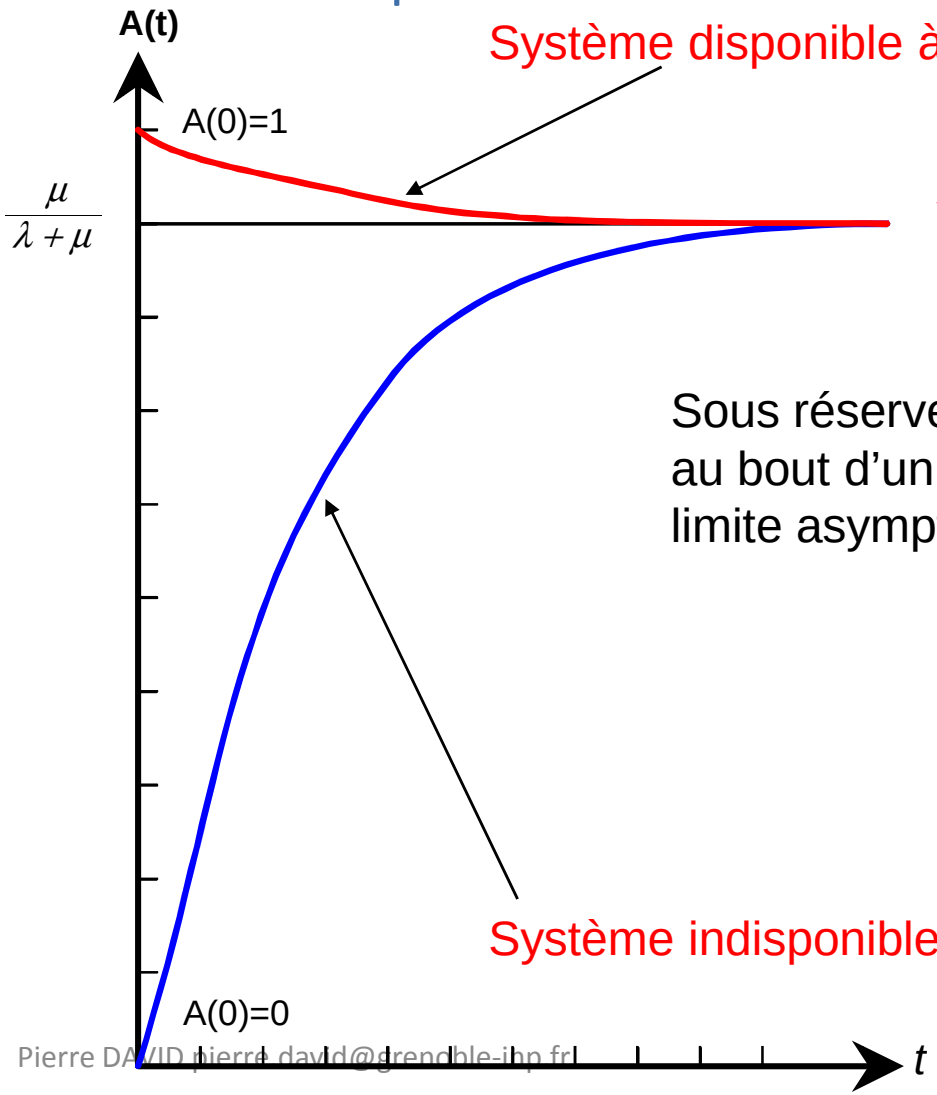


- Imputable au Système principal
- Domaine privilégié de la SdF
- Exigence vis à vis fournisseur

- Imputable au système principal ET à l'organisation du Système de Soutien
- Exigences vis à vis du système en Exploitation

La Disponibilité

Allure de la disponibilité



Système disponible à l'instant t = 0

Valeur asymptotique

Sous réserve d'une politique de maintenance efficace, au bout d'un temps donné, les systèmes ont atteint leur limite asymptotique de disponibilité.

Système indisponible à l'instant t = 0

La Maintenabilité

- **Définition** CEI 50(191) : Aptitude d'une entité à être maintenue ou rétablie dans un état dans lequel elle peut accomplir une fonction requise lorsque la maintenance est accomplie dans des conditions données avec des procédures et des moyens prescrits..

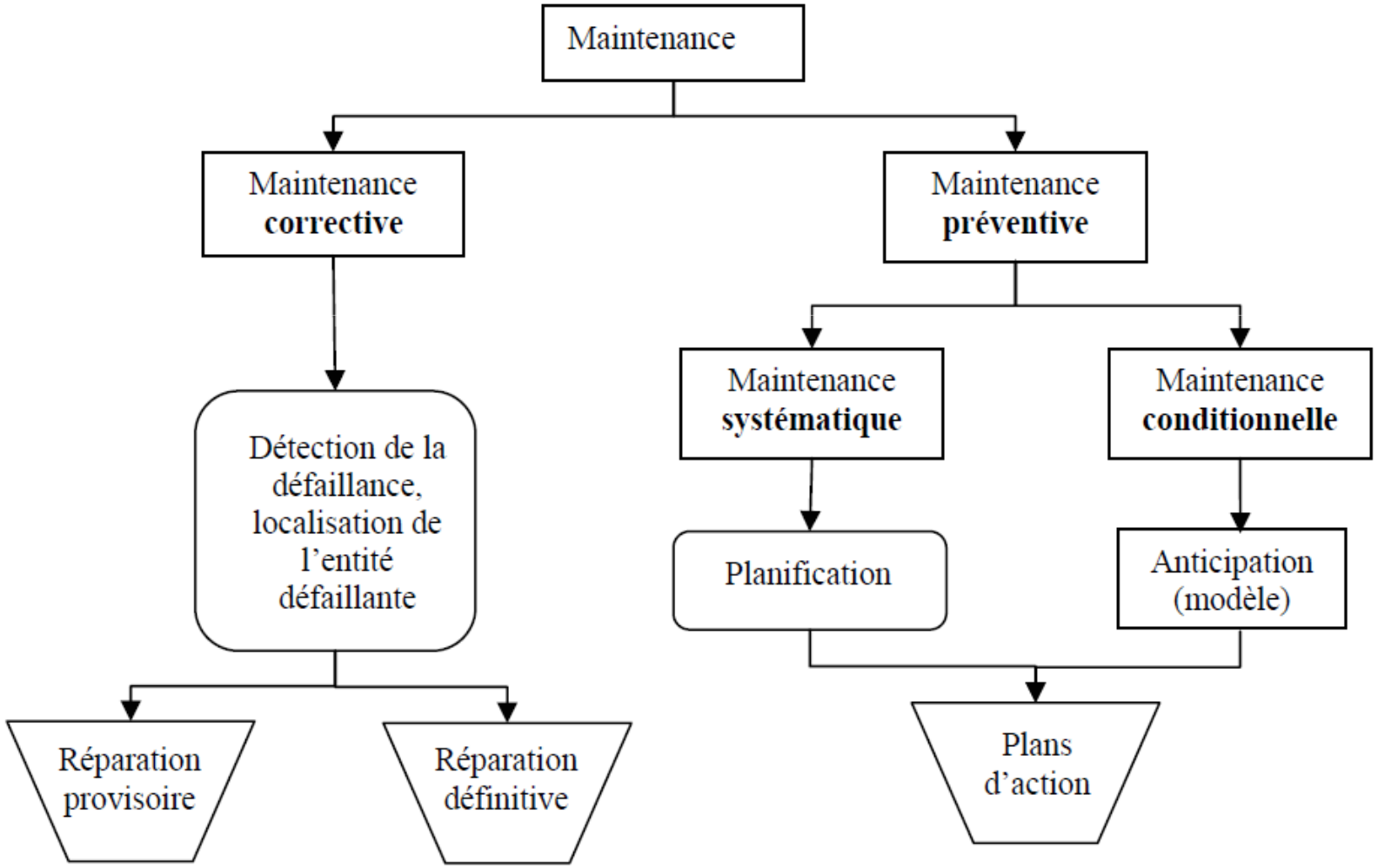
- **Mesure** : La maintenabilité se mesure par la probabilité que la maintenance d'une entité, assurée dans des conditions données et avec des moyens et des procédures présents, s'achève à l'instant t, sachant que l'entité est défaillante à l'instant t = 0

  M (t) = P [E défaillante à l'instant 0 soit réparée à l'instant t]

  ou M (t1,t2) = P [E défaillante à t = t1 soit réparée à t = t2]

La Maintenabilité

Type de maintenance



La Maintenabilité

Analogie de la Fiabilité et la Maintenabilité

Fiabilité

Probabilité "de durée de bon fonctionnement"

v.a. : temps de fonctionnement
$R(t) = Prob(T_p > t)$

Taux de défaillance : $\lambda(t)$

MTTF : Mean Time To Failure

ou MTBF : Mean Time Between Failures

Loi usuelle :
Si λ = constant, loi exponentielle

$$R(t) = e^{-\lambda t} \qquad MTTF = \frac{1}{\lambda}$$

Maintenabilité

Probabilité "de durée de réparation"

v.a. : temps de réparation
$M(T) = Prob(T_R < t)$

Taux de réparation : $\mu(t)$

MTTR : Mean Time To Repair

Loi usuelle :
Si μ = constant, loi exponentielle

$$M(t) = 1 - e^{-\mu t} \qquad \mu = \frac{1}{MTTR}$$

La Sécurité

- **Définition :** Traduit l'aptitude d'une entité à éviter de faire apparaître, dans des conditions données, des événements critiques ou catastrophiques.

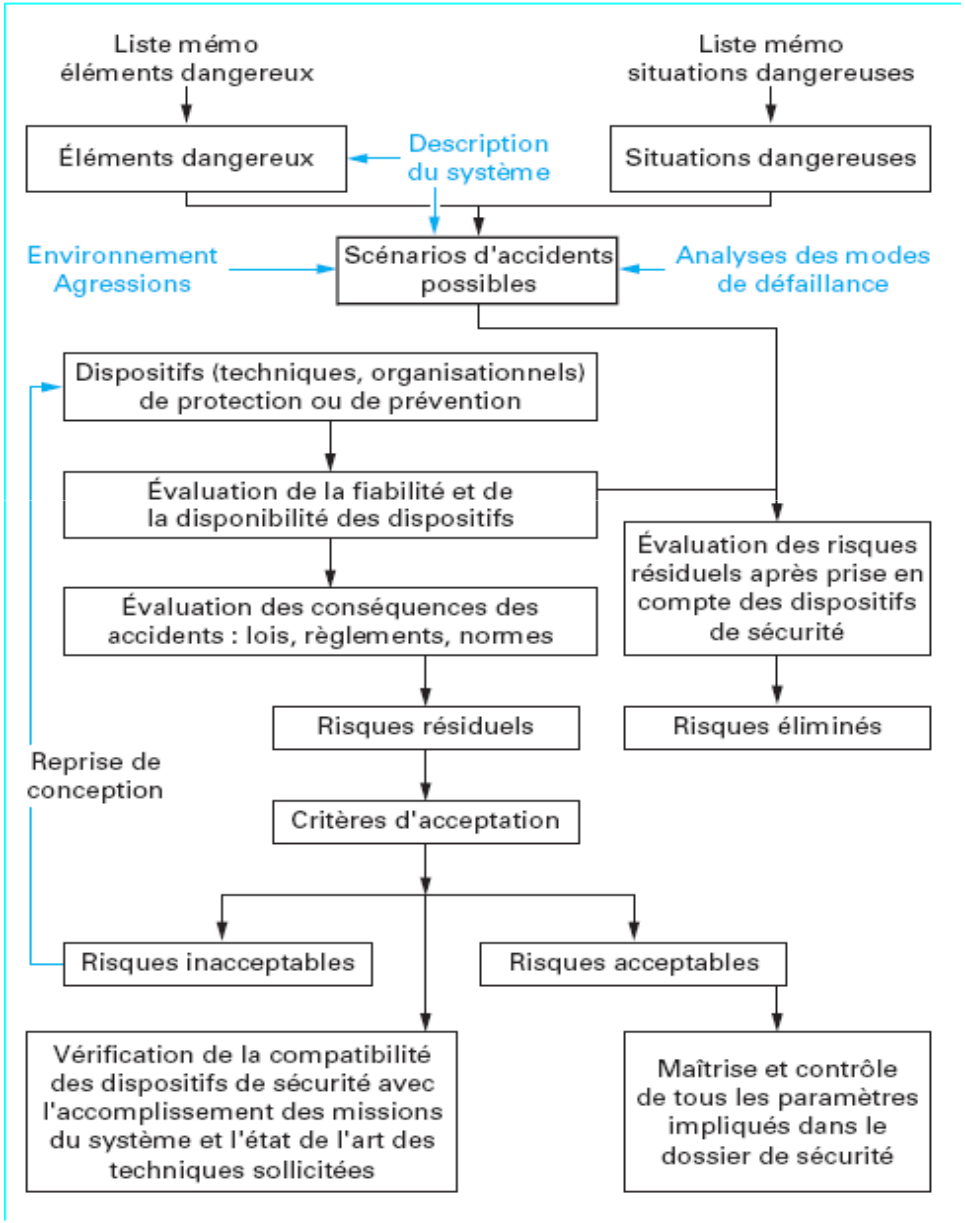
- **Sûreté :** La mesure dans laquelle un système fonctionne ou défaille sans incidence « catastrophique » sur son environnement.

- **Sécurité :** La mesure dans laquelle un système résiste à des fautes intentionnelles.

- **Evaluation(s) :** probabilité de défaillance dangereuse, non atteignabilité d'état dangereux …

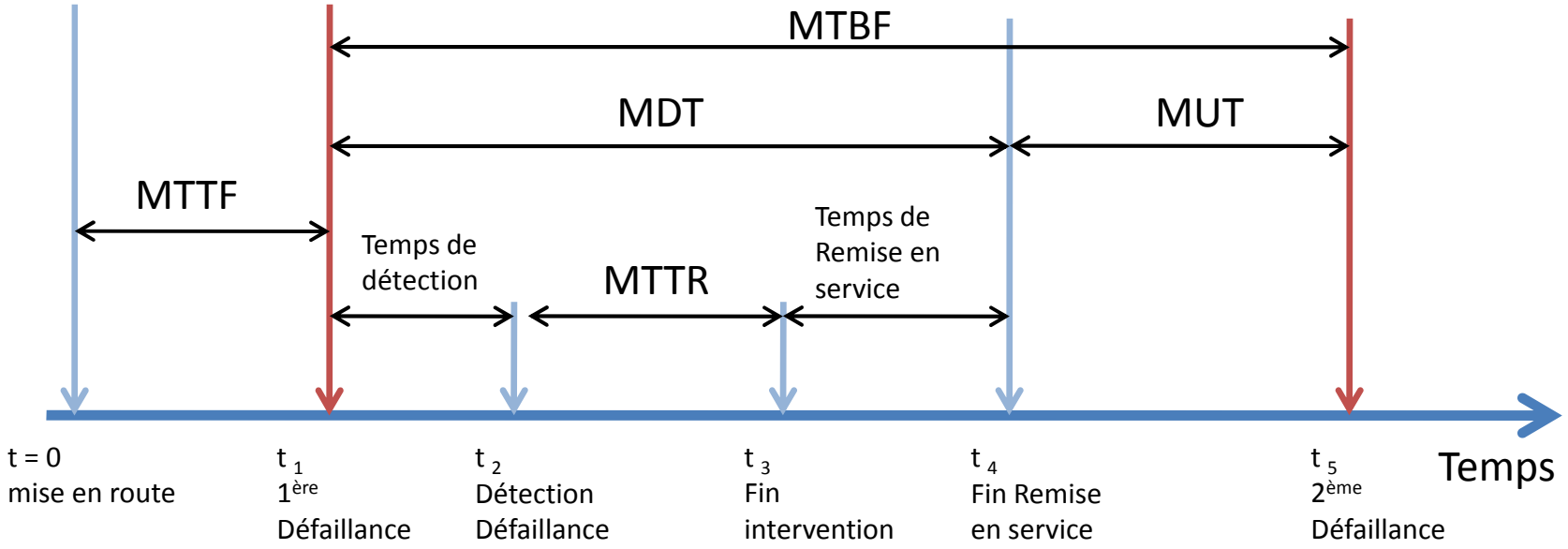
La Sécurité

Analyse de SdF orientée Sécurité

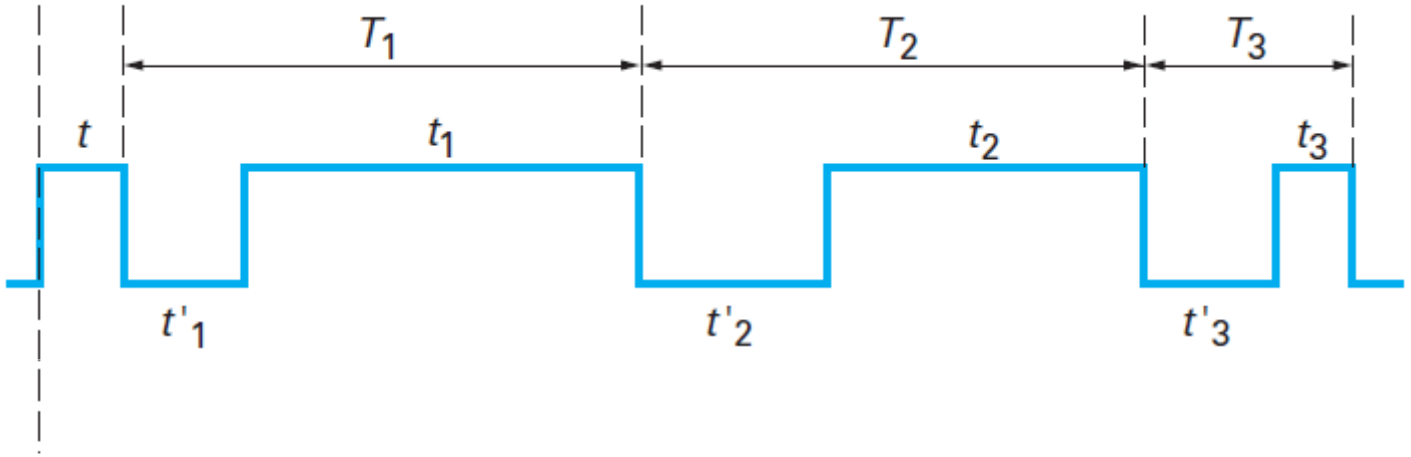


Les temps caractéristiques de la SdF

- MTTF : Mean Time To Failure (parfois MTTFF)
- MTBF : Mean Time Between Failure
- MDT : Mean Down Time
- MTTR : Mean Time To Repair
- MUT : Mean Up Time



Les temps caractéristiques de la SdF



Moyenne des temps de première panne = t

Moyenne des temps entre pannes (MTBF) = $\frac{T_1 + T_2 + T_3}{3}$

Moyenne des temps de bon fonctionnement = $\frac{t + t_1 + t_2 + t_3}{4}$

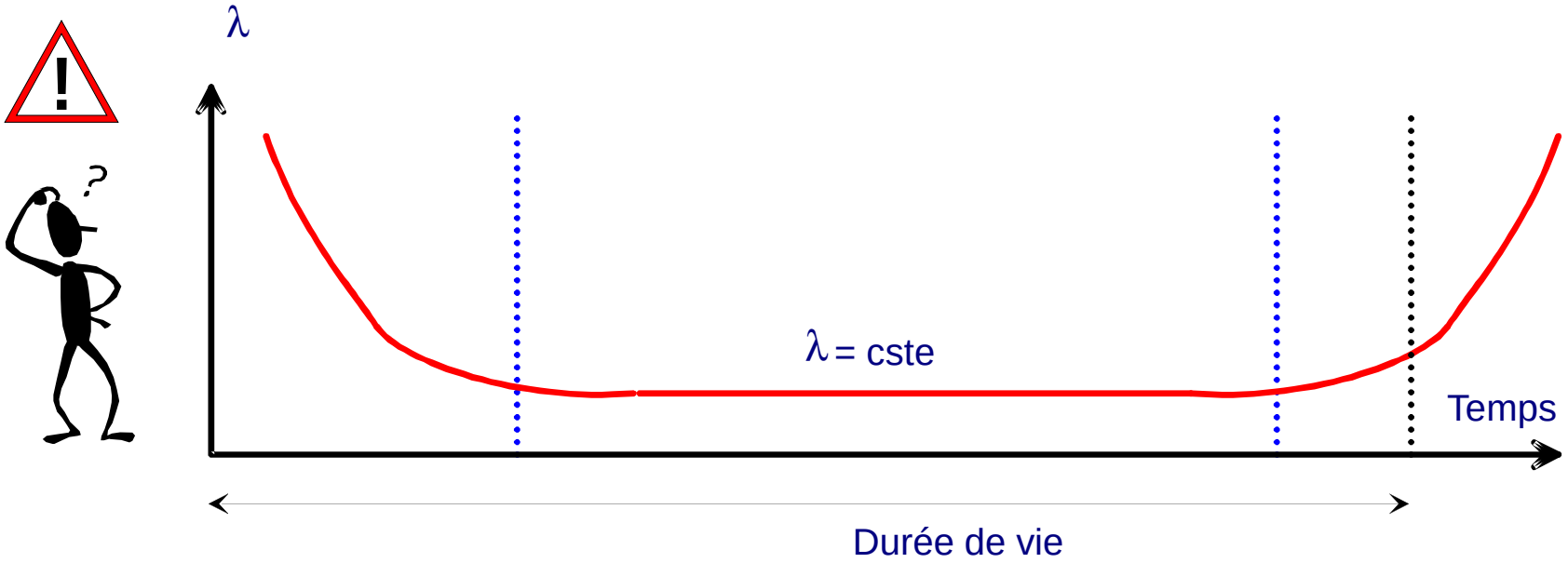
MUT = Mean Up Time = $\frac{t_1 + t_2 + t_3}{3}$

MDT = Mean Down Time = $\frac{t'_1 + t'_2 + t'_3}{3}$

Les temps caractéristiques de la SdF

Notion de Durée de vie

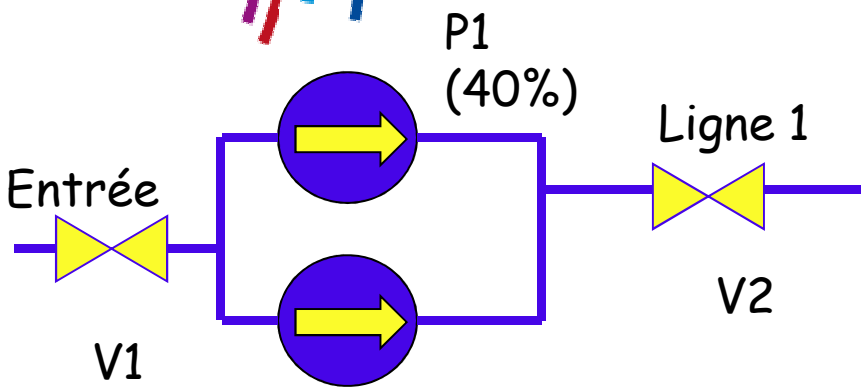
Ne pas confondre Taux de défaillance, MTBF et DUREE DE VIE

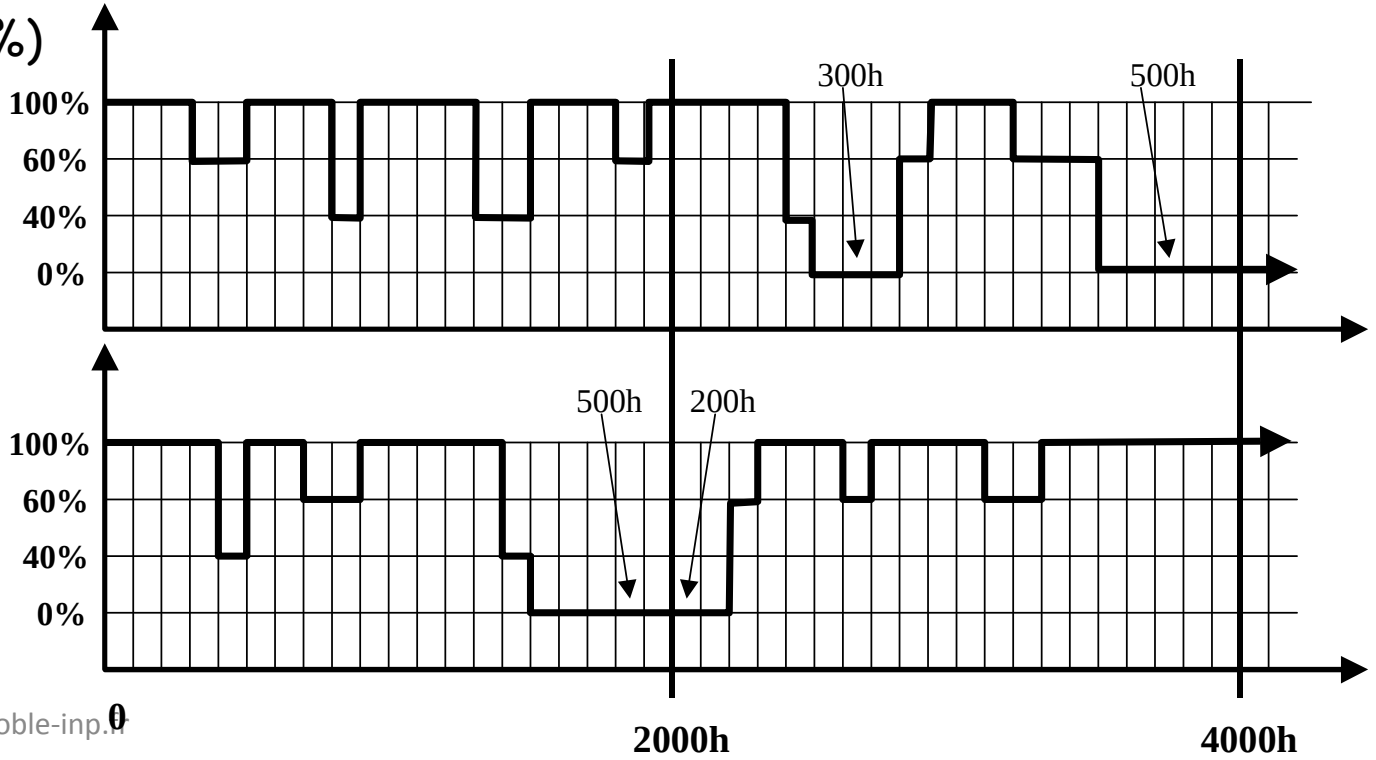


La durée de vie correspond, pour un système réparable, à la durée entre la mise en service et le moment où le taux de défaillance est considéré en augmentation de 10% par rapport λ constant.

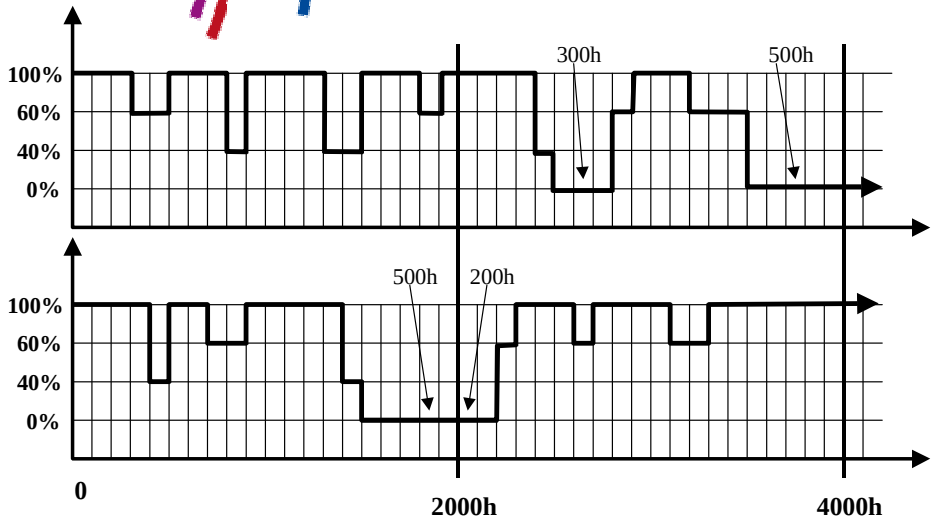
Exemple : Voiture ➔ Durée de vie = 10 ans
MTBF = 2 ans

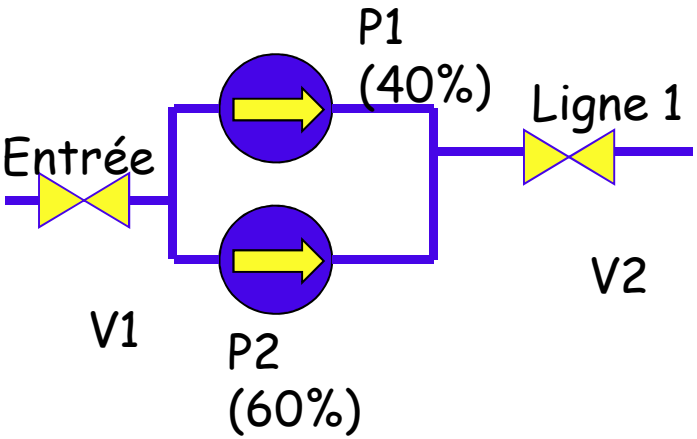
Exemple de réflexion terrain





Exemple de réflexion terrain

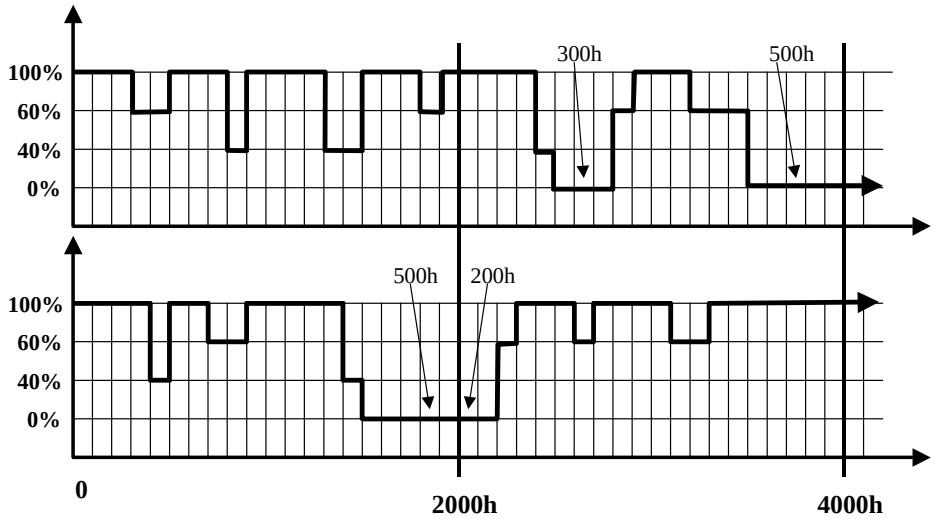




Deux histoires ne constituent pas, bien entendu, un échantillon statistiquement représentatif, mais cela va suffire pour montrer ce qu'on peut tirer de telles simulations.

Plaçons-nous à l'instant t = 2000 (l'abscisse est graduée en pas de 100h pour faciliter la lecture) : au temps 2000 le système est en panne totale 1 fois sur 2, donc son "indisponibilité instantanée" peut être estimée à 1/2 = 0.5

Au temps 2000 le système est resté en panne totale pendant 500h sur 2*2000 = 4000h, donc son "indisponibilité moyenne" peut être estimée à 500/4000= 0.125



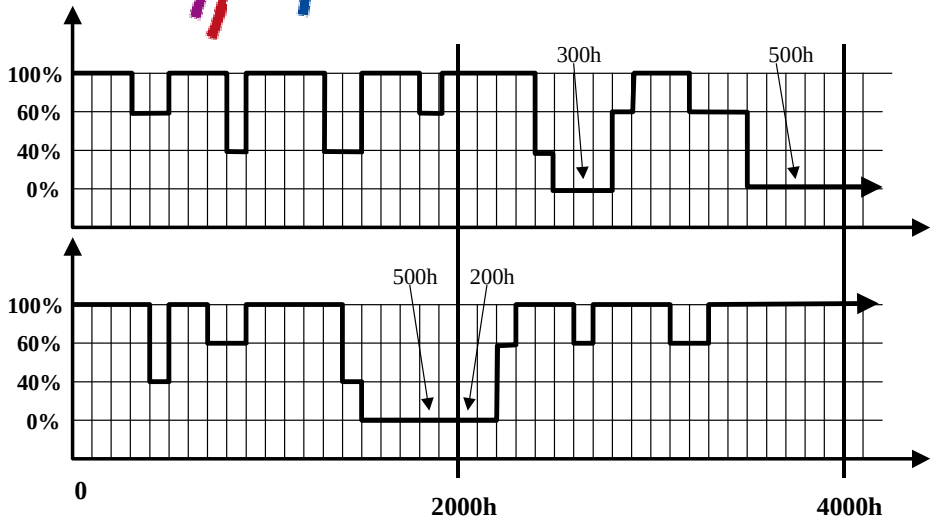
Le système est tombé en panne totale 1 fois sur 2 avant l'instant 2000h, donc sa "défiabilité" (complément à 1 de la fiabilité) peut être estimée à 1/2 = 0.5

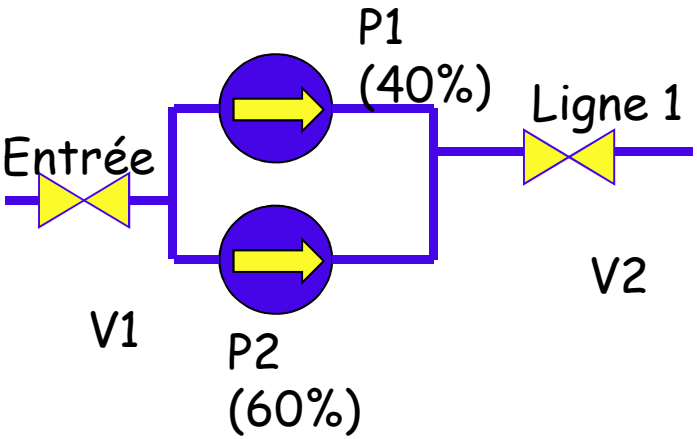
Le système est tombé en panne totale 1 fois sur 2 avant l'instant 2000h, donc son nombre moyen de pannes totales peut être estimé à 1/2 = 0.5

Le système a produit (300+300+400+300+100)+(400+200+500) = 2500h à 100% soit 62.5% du temps

- le système a produit 500h à 60% soit 12.5% du temps
- le système a produit 500h à 40% soit 12.5% du temps
- le système a produit 500h à 0% soit 12.5% du temps
- la "disponibilité de production" (espérance mathématique de la productivité) a été de 62.5 + 12.5*0.6 +12.5*0.4 = 75%

Exemple de réflexion terrain



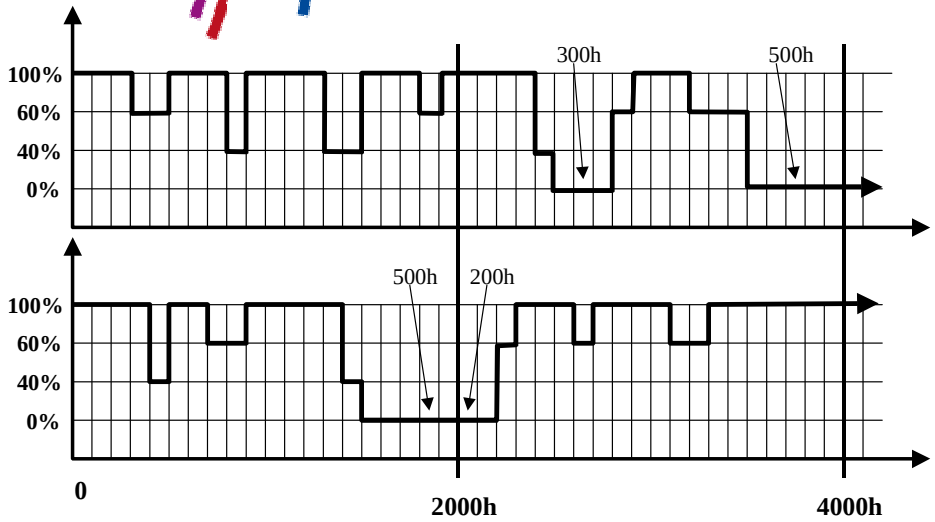


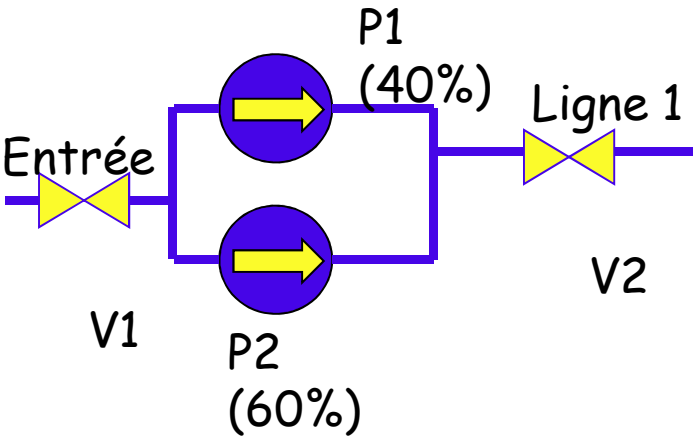
La perte de production ("indisponibilité de production") a été de 1.00-0.75 = 25%
(à comparer avec l'indisponibilité moyenne classique de 12.5%)

L'équipe de réparateurs a été appelée en moyenne 8/2 = 4 fois par histoire

L'équipe de réparateurs à été occupée en moyenne 1500/2 = 750 h par histoire soit 37.5% de son temps

Exemple de réflexion terrain

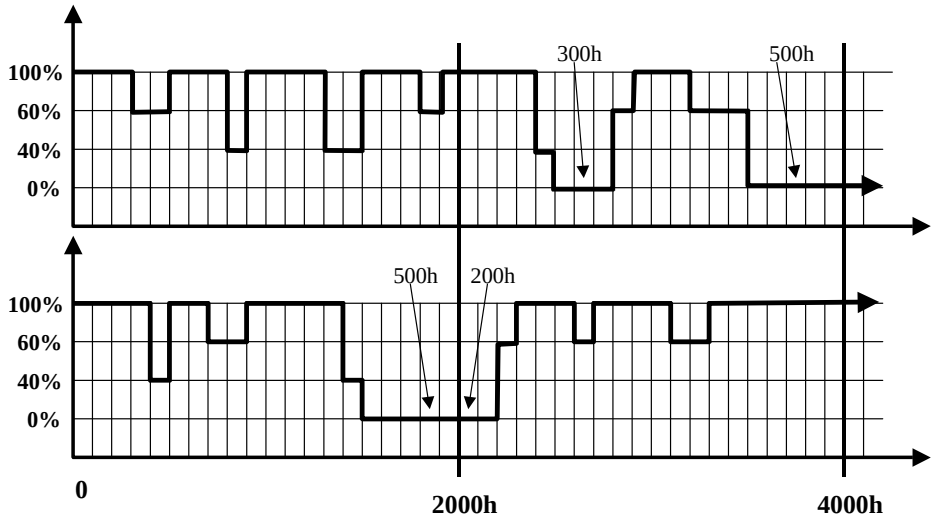




A vous de jouer à 4000h

Plaçons-nous à l'instant t = 4000 : au temps 4000 le système est en panne totale ……fois sur 2, donc son "indisponibilité instantanée" peut être estimée à ……

Au temps 4000 le système est resté en panne totale pendant …… sur ……., donc son "indisponibilité moyenne" peut être estimée à ……



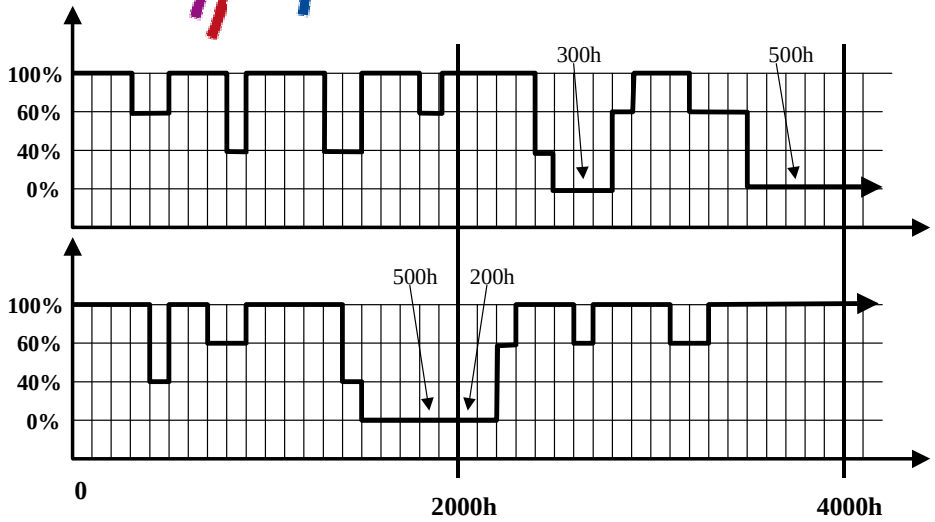
Le système est tombé en panne totale……fois sur 2 avant l'instant 4000h, donc sa "défiabilité" (complément à 1 de la fiabilité) peut être estimée à ……

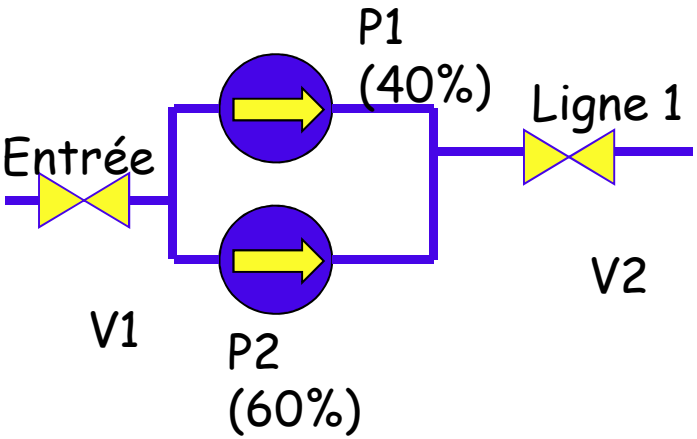
Le système est tombé en panne totale……fois sur 2 avant l'instant 4000h, donc son nombre moyen de pannes totales peut être estimé à ……

Le système a produit …… à 100% soit …….. du temps

- le système a produit…….. à 60% soit …… du temps
- le système a produit …….. à 40% soit ……du temps
- le système a produit ……..à 0% soit ……du temps
- la "disponibilité de production" (espérance mathématique de la productivité) a été de …… = …….

Exemple de réflexion terrain





La perte de production ("indisponibilité de production") a été de …… = ……..%

L'équipe de réparateurs a été appelée en moyenne …….. fois par histoire

L'équipe de réparateurs à été occupée en moyenne …….. par histoire soit …… de son temps

Exercice Fiabilité

Une machine à quatre dispositifs D_1, D_2, D_3, D_4, dont la défaillance peut intervenir de manière indépendante. On observe le fonctionnement de la machine pendant un intervalle de temps T.

Soit A_i: « D_i fonctionne sans défaillance pendant l'intervalle T », avec une proba : $P(A_i)$. On sait que $P(A_1)=0.80$ $P(A_2)=0.85$ $P(A_3)=0.90$ $P(A_4)=0.90$

La machine tombe en panne si D_1 est défaillant. La machine continue de fonctionner si un seul des trois dispositifs D_2, D_3, D_4 est défaillant ; mais la défaillance simultanée de deux de ces trois dispositifs met la machine en pane.

Quelle est la probabilité de fonctionnement de cette machine sur l'intervalle de temps T ?


Grenoble INP
génie industriel

Exercice Fiabilité

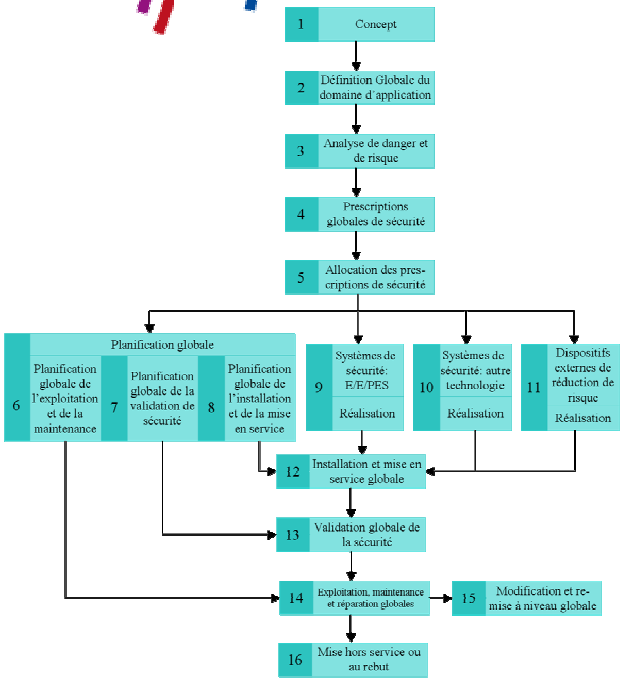
-A- Une machine tombe en panne selon la loi exponentielle avec un facteur $\lambda = 0.5$/heure. Quelle est la probabilité que la machine tombe en panne entre la première et deuxième heure après le démarrage?

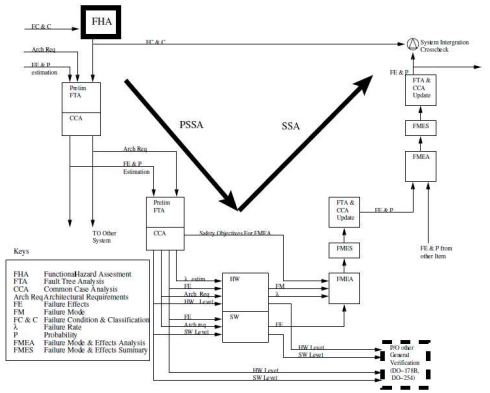
-B- La durée de vie d'un composant d'un système est supposée suivre une loi exponentielle de paramètre λ. Un grand nombre de ces composants sont testés et on a observé que 5% ne durent pas plus de 100 heures.

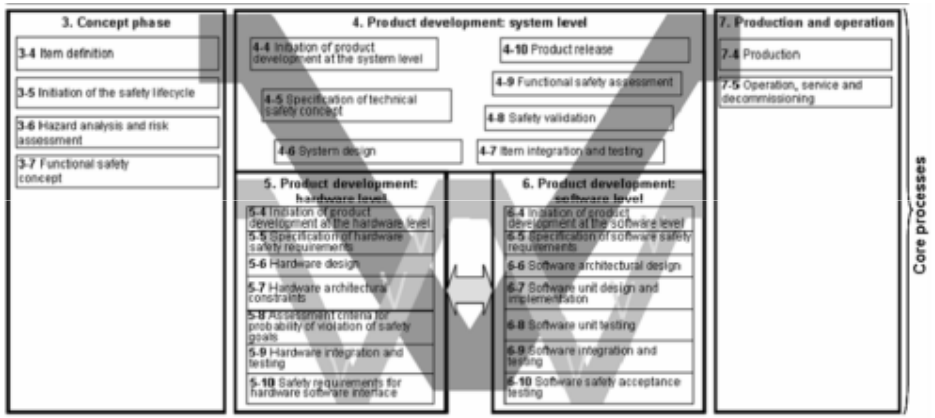
Estimer la probabilité qu'un composant pris au hasard dure plus de 200 heures, ou T est la durée de vie en heures

-C- Quelle est la probabilité qu'un matériel de taux de défaillance en fonctionnement de $\lambda = 8\ 10^{-5}$ / heure tombe en panne durant une année sachant qu'il fonctionne 24 h / 24 h, 6 jours sur 7 ?


Grenoble INP
génie industriel





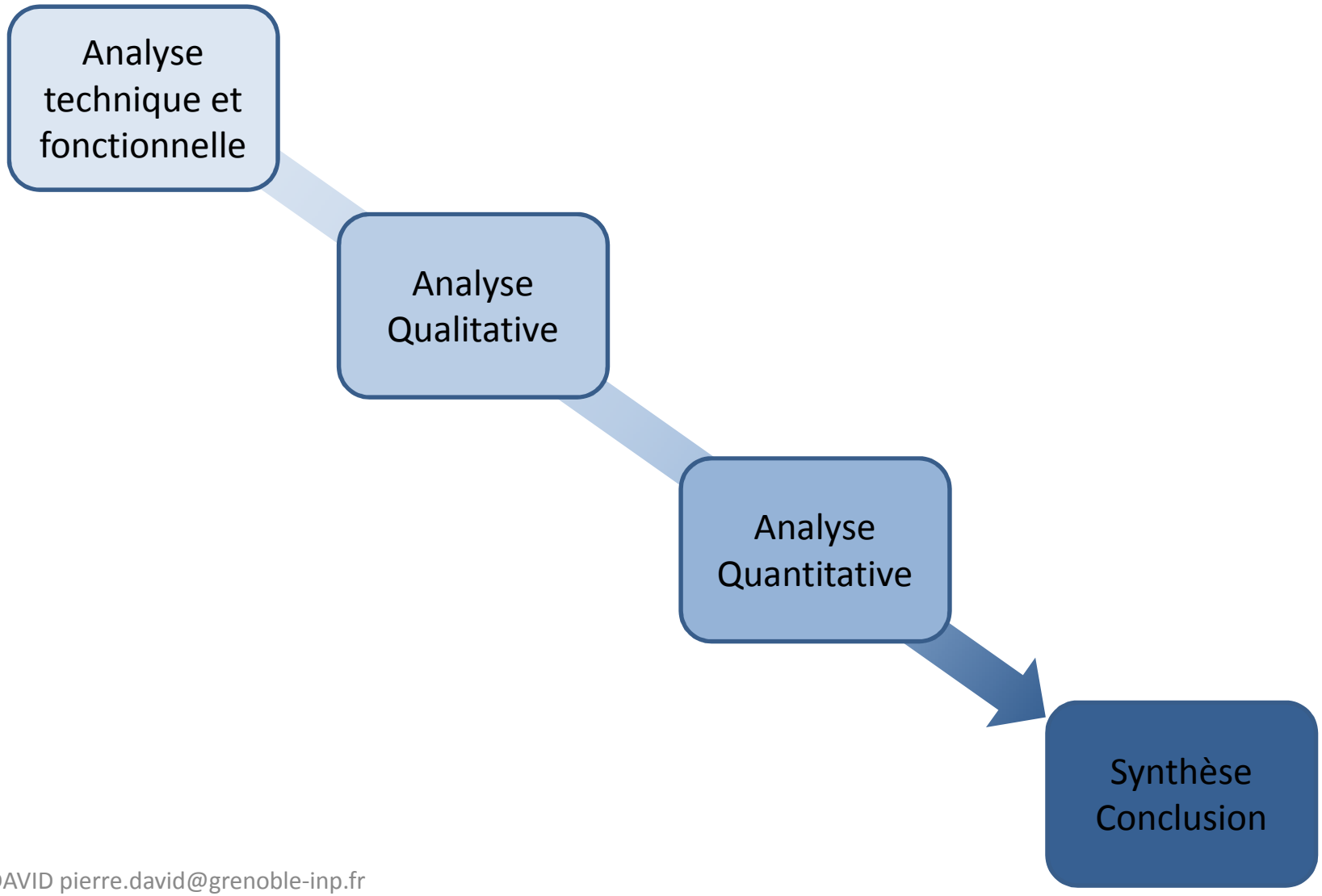


CYCLE DE RÉALISATION DES ANALYSES DE SDF

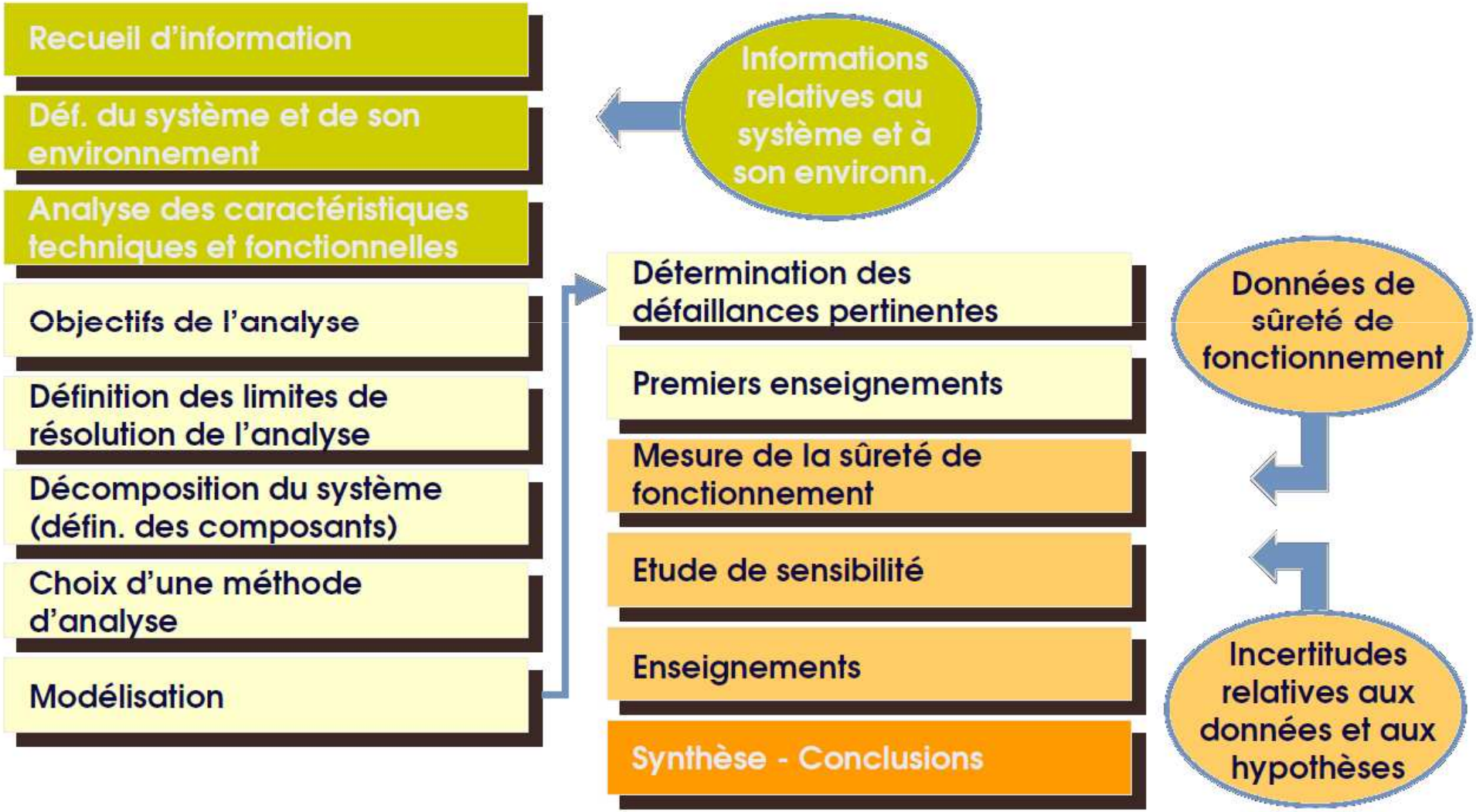
Plan

- Le Cycle traditionnel des analyses de SdF
- La gestion des connaissances dans les cycles SdF
- Les outils et méthodes de la SdF :
  - Analyse Préliminaire des Risques (APR)
  - AMDE / AMDEC
  - Arbres de Défaillance
  - Diagramme Bloc de Fiabilité
  - Modèles à événement discrets

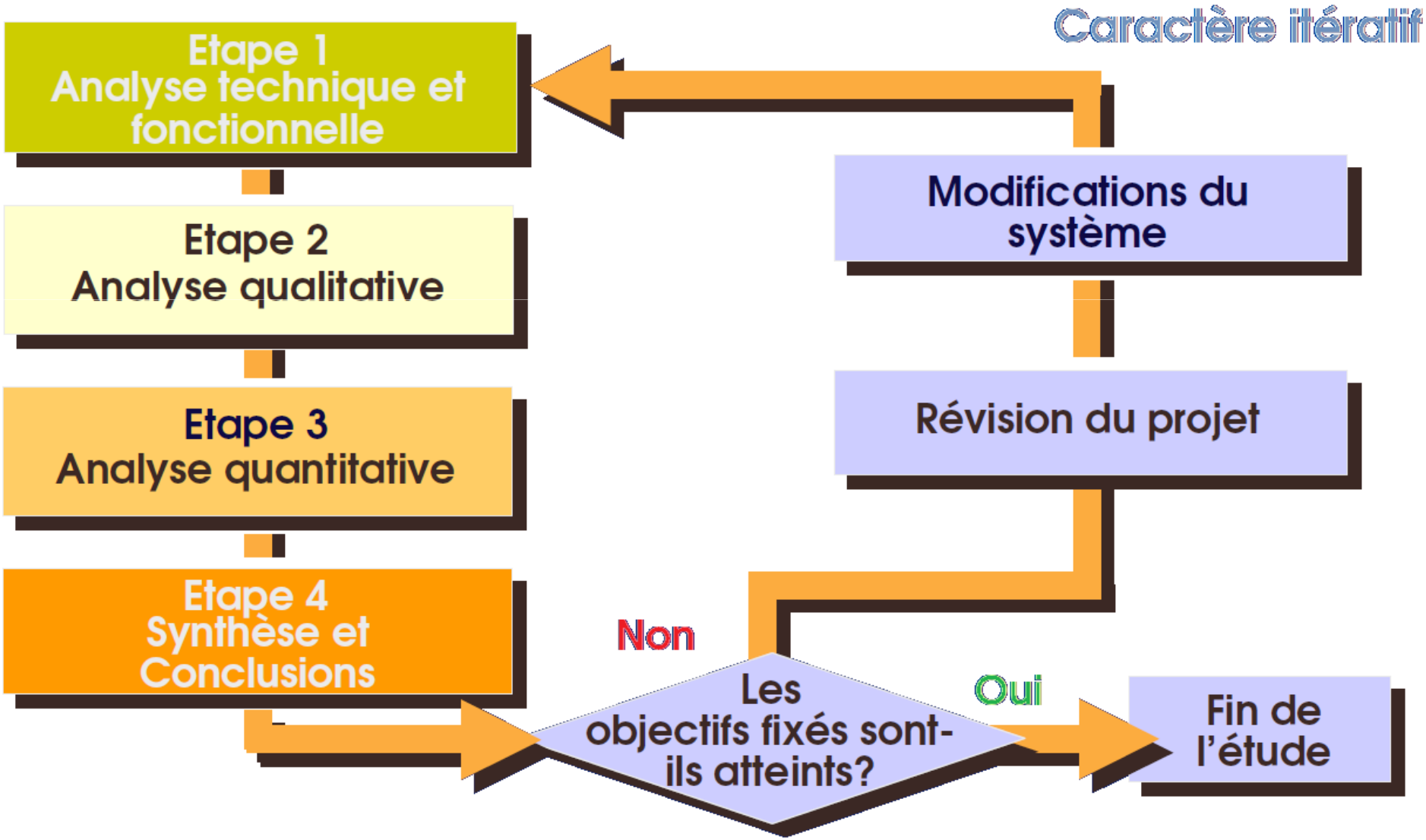
Cycle d'analyse SdF traditionnel



Cycle d'analyse SdF traditionnel



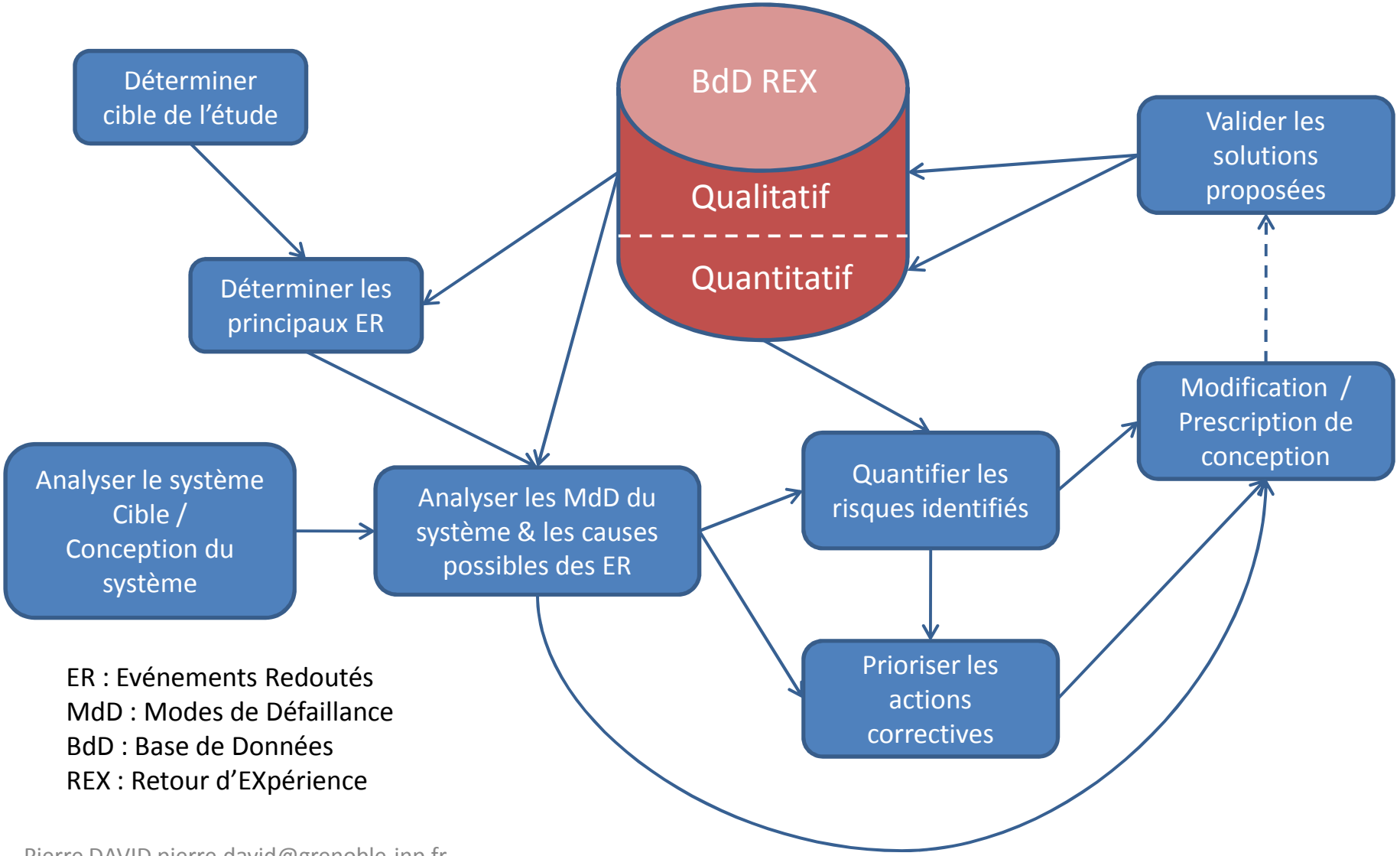
Cycle d'analyse SdF traditionnel



Cycle d'analyse SdF

- A ce cycle traditionnel il convient d'ajouter :
  - La gestion du Retour d'Expérience (REX),
  - Les itérations à travers les niveaux de granularité (système, équipements, composants, composants unitaires)
  - Les itérations entre analyses de SdF (mise à jour d'evt redoutés, de Mode de défaillance …).
- Ce cycle prend aussi des formes différentes suivant s'il est appliqué à un système existant ou en cours de conception.

La gestion des connaissances durant le Cycle d'analyse de SdF

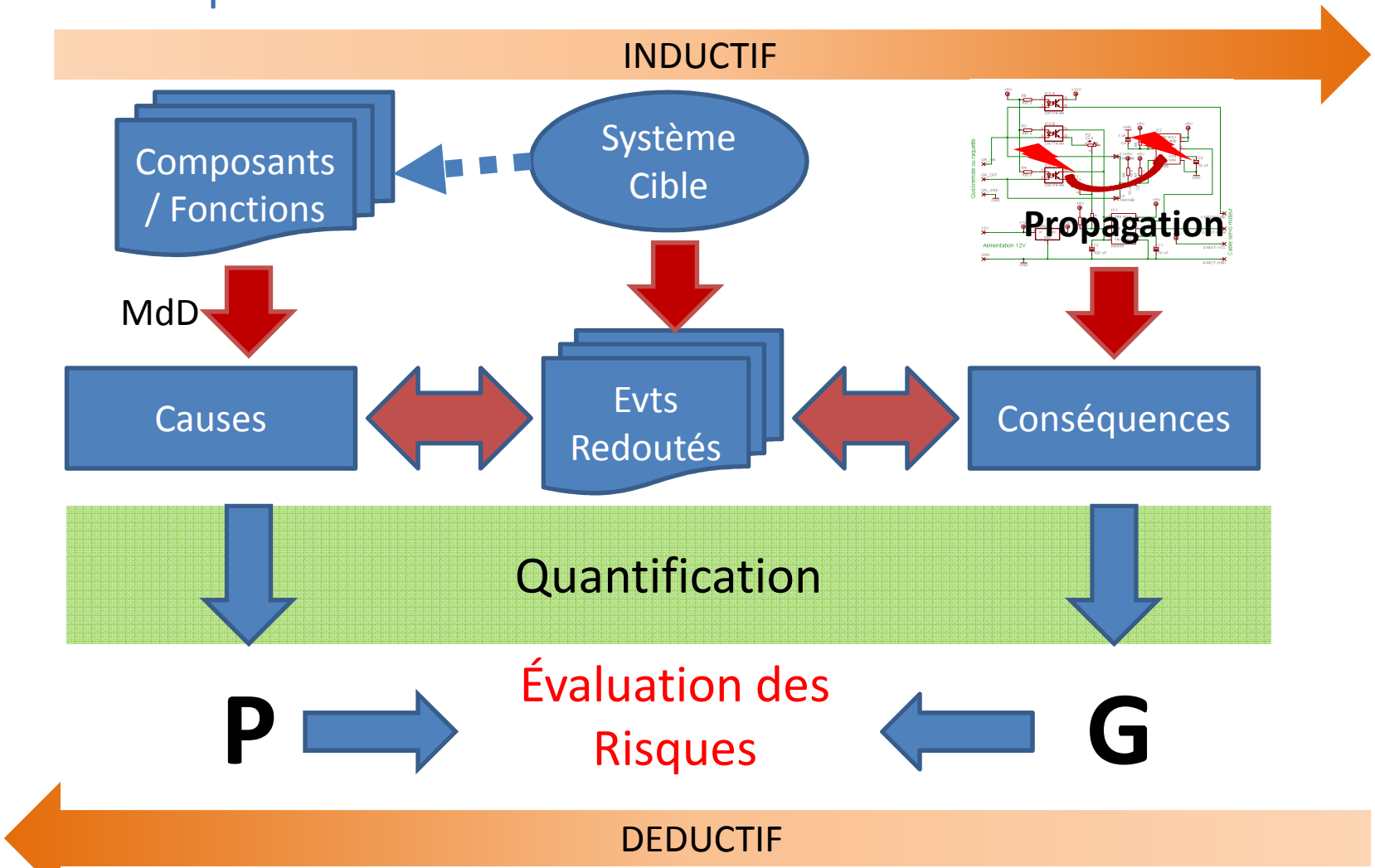


ER : Evénements Redoutés
MdD : Modes de Défaillance
BdD : Base de Données
REX : Retour d'EXpérience

Grenoble INP génie industriel

Schématiquement

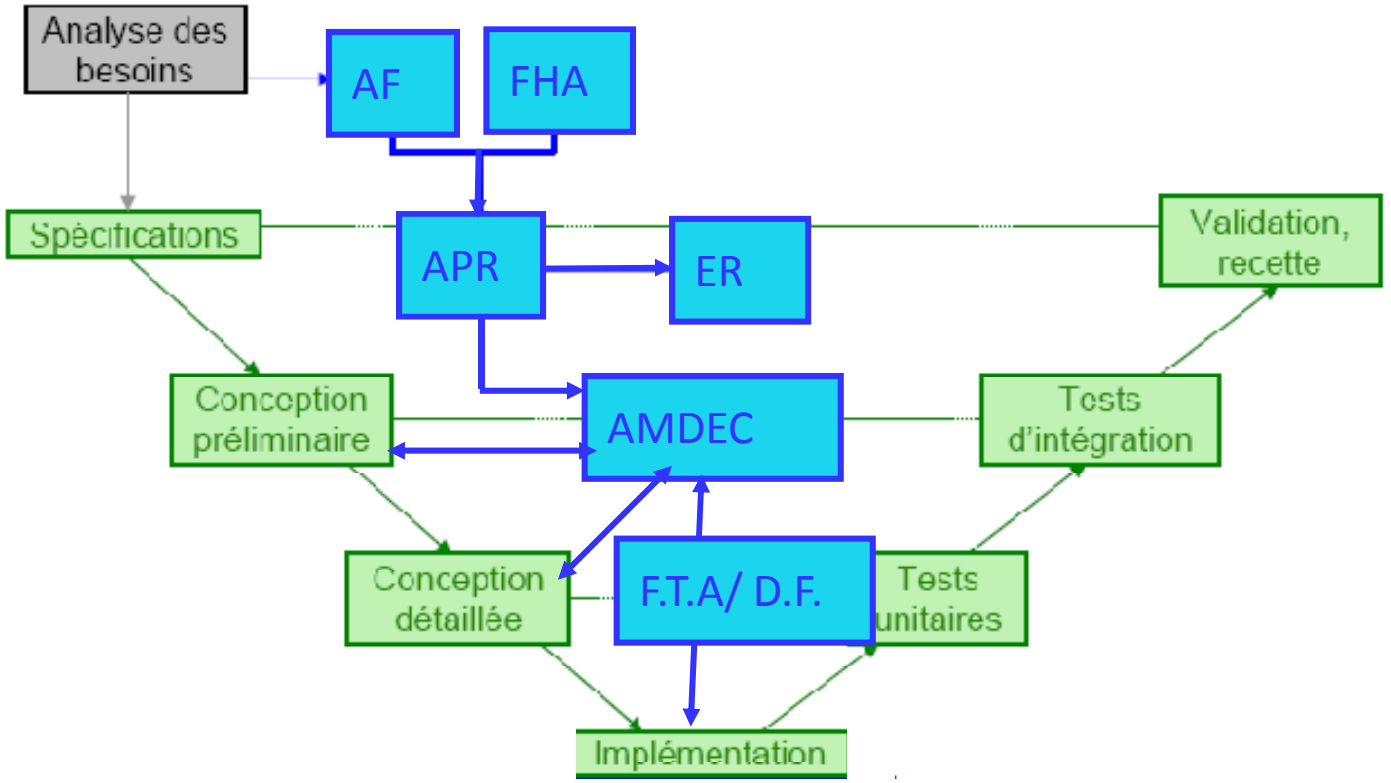
Cycle d'analyse de SdF



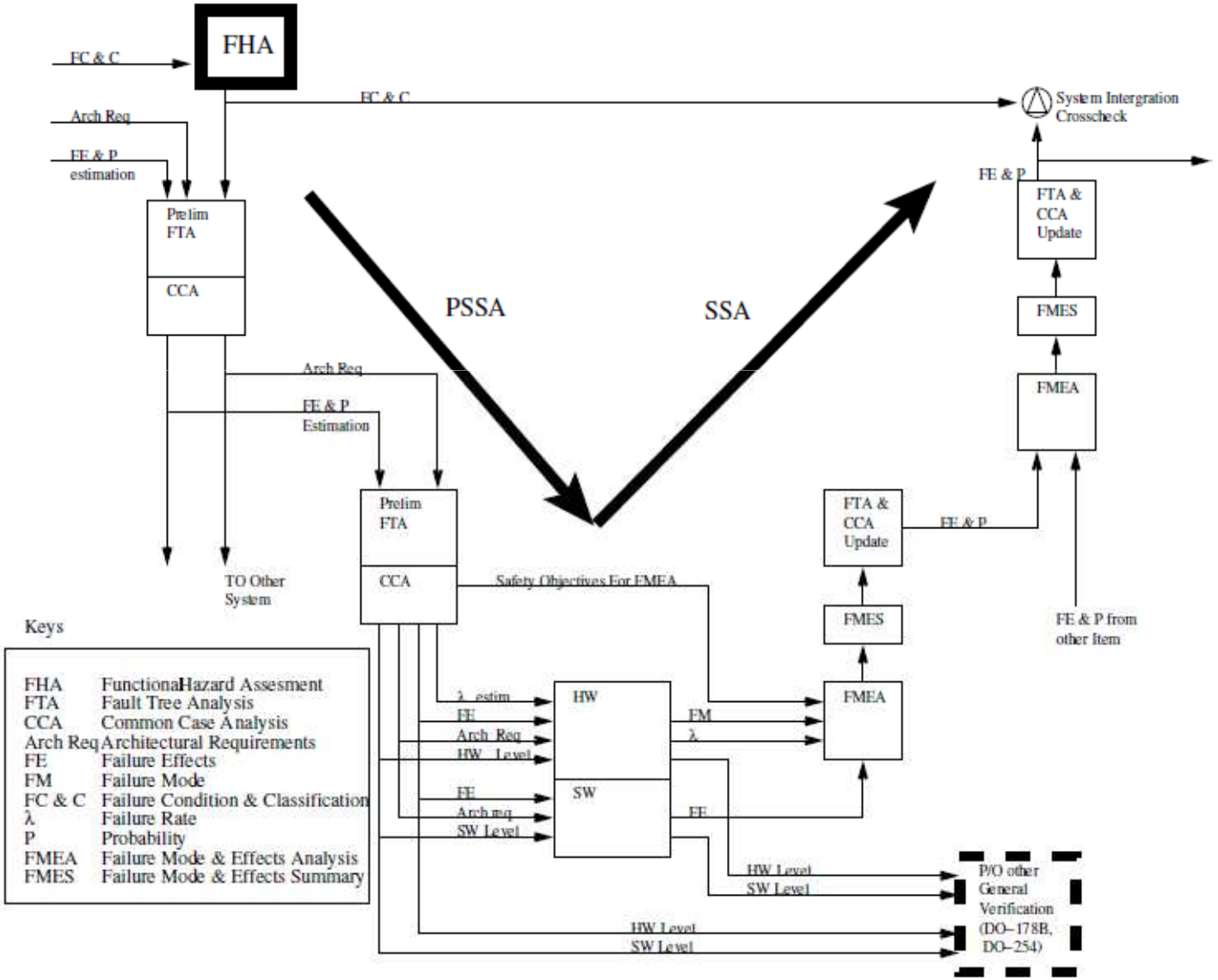
Les outils de la SdF

Démarches/ Méthodes	Inductive/ déductive	Quantitative/ qualitative	Phrase-clef
Retour d'expérience	Déductive	Quantitative	Alimenter sa connaissance du système à la réalité
Analyse préliminaire de risques (APR)	Inductive	Qualitative	Repérer *a priori* les risques à étudier
Analyse des modes de défaillance et de leurs effets (AMDE)	Inductive	Qualitative	Recenser les conséquences des défaillances
Analyse des modes de défaillance, de leurs effets et de leurs criticités (AMDEC)	Inductive	Quantitative	Évaluer les conséquences des défaillances
Arbre de causes	Déductive	Qualitative	Organiser les éléments ayant contribué à un accident
Arbre d'événement	Inductive	Quantitative	Évaluer les conséquences possibles d'un événement
Arbre de défaillances	Déductive	Quantitative	Évaluer les scénarios d'un accident potentiel
Graphes d'état	Inductive	Quantitative	Évaluer les états possibles d'un système réparable

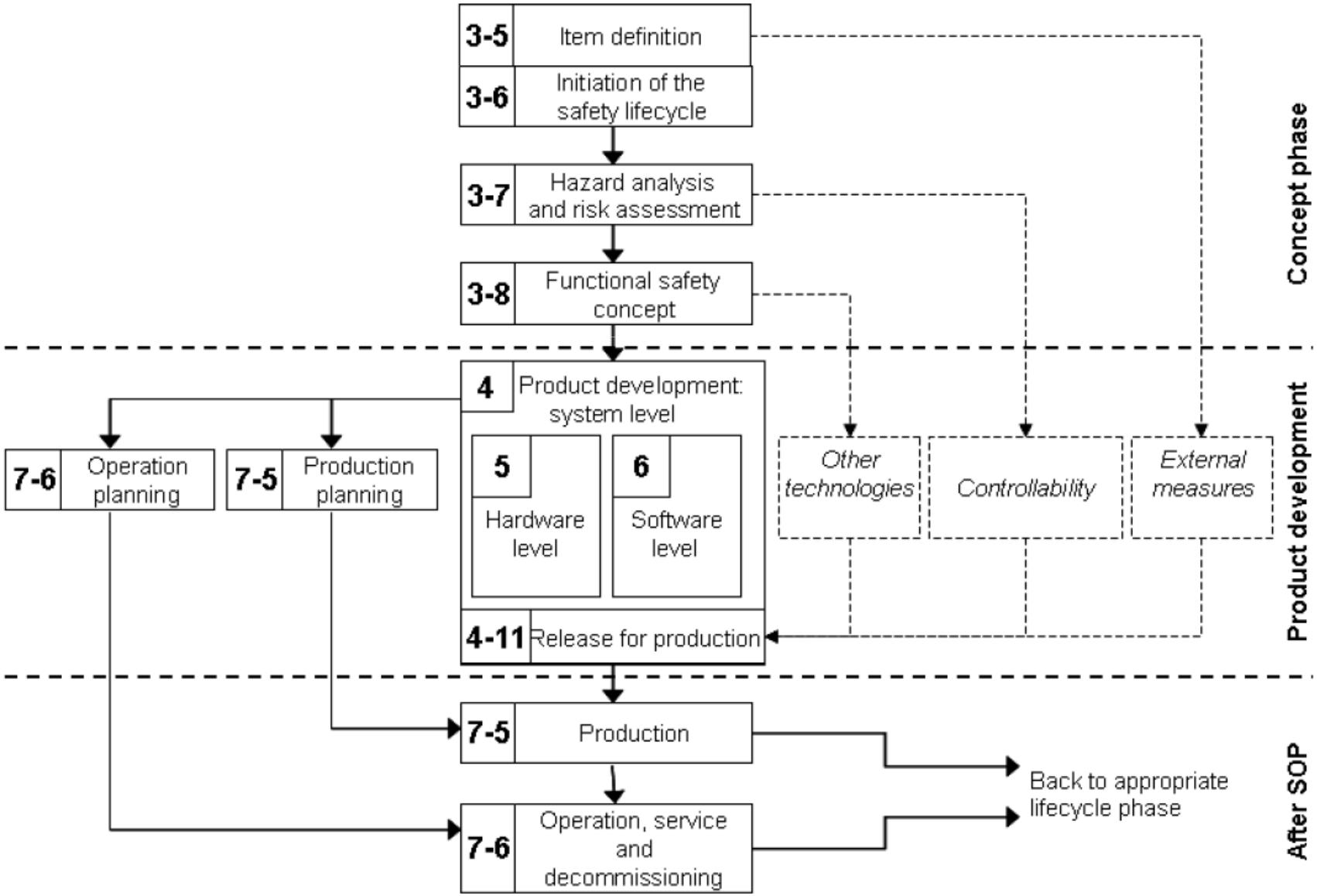
Les outils au cœur du cycle de SdF

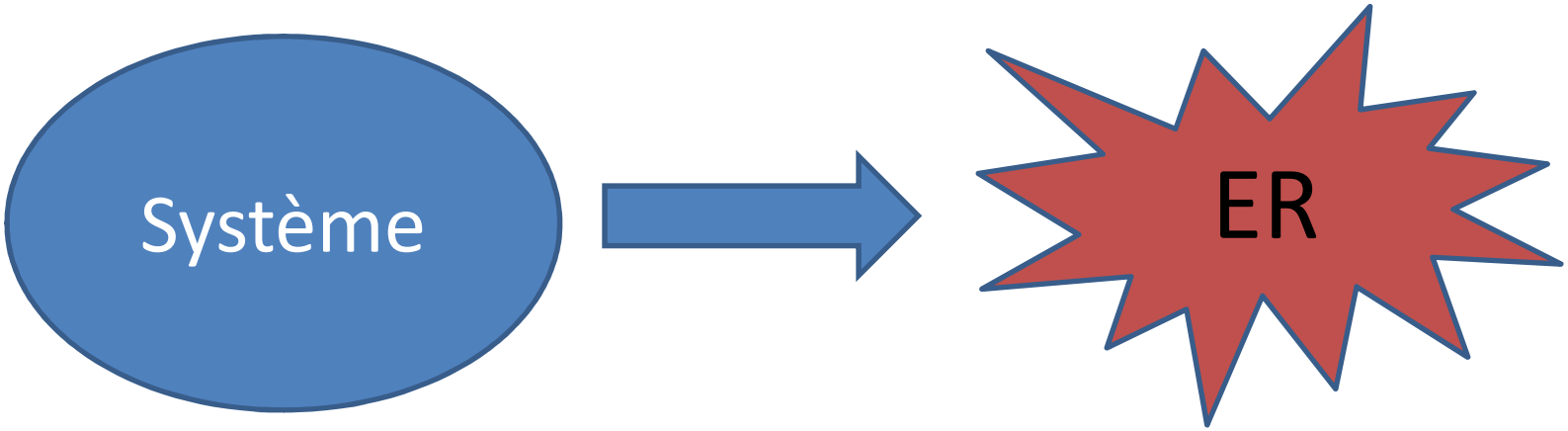


Cycle et domaine industriel



Cycle et domaine industriel





ANALYSE PRÉLIMINAIRE DES RISQUES

Objectifs

- L'objectif général est d'évaluer les problèmes à résoudre en matière de maîtrise des risques :
  - Rendre compte des risques sur le système,
  - Dimensionner les efforts d'études et de réduction des risques,
  - Localiser les points critiques du système.

- Attendus :
  - Identifier l'ensemble des ER et leurs scenarii associés,
  - Objectifs de SdF sur les fonctions/architecture,
  - Préconiser des mesures de contrôle du risque.

- Cas d'emploi:
  - Projet multi acteurs,
  - Présence d'exigences de sécurité,
  - Systèmes complexes,
  - Forte influence/interaction avec l'environnement.

L'APR est principalement orientée Sécurité

Piloter la SdF

- Évaluer les risques pour :
  - Entériner les décisions d'approfondir ou clore les investigations de SdF,
  - Fixer les performances de SdF attendues (limites supérieures et inférieures),
  - Canevas du suivi des ER,
  - Préparation de la documentation d'un dossier de sécurité,
  - Justifier certaines décisions techniques (ex. ajout de redondances).

Mise en place

- L'APR adopte une démarche inductive dont la réalisation adopte Trois phases principales :
  - Identification des dangers et événements redoutés,
  - Evaluation et classement des risques associés,
  - Propositions de mesure de couverture des risques.

- L'APR doit être utilisée le plus tôt possible dans le cycle de vie et doit ensuite être mise à jour au fil de l'avancement de la conception et des études de SdF.

- L'APR doit être précédée d'une définition du système et de son environnement :
  - Les fonctions à remplir par le système (analyse fonctionnelle),
  - Comment le système va vivre, être utilisé (profil de mission /phases de vie),
  - La description et la délimitation du système (arborescence technique, organisation industrielle et schéma d'architecture et des interfaces).
- L'APR peut s'effectuer dès la phase exploratoire :
  - Dès que l'on connaît les fonctions à remplir par le système,
  - Dès que l'on connaît les grands choix technologiques

Mise en place

- L'APR peut prendre des formes variées suivant les domaines technologiques et les objectifs de l'études.

- On peut distinguer APR et APD (Analyse Préliminaire de Danger). Dans le second cas seule la gravité est étudiée.

- Elle est effectuée en groupe de travail :
  - Par le responsable Qualité (ou Assurance Produit) du projet en liaison avec le Chef de projet,
  - L'Ingénieur Système,
  - Les responsables techniques des sous-systèmes,
  - Les responsables qualité (ou Assurance Produit) des sous-systèmes le cas échéant.
  - Le document résultant est diffusé à l'ensemble du Projet.

APR méthode

- Méthode inductive : scenarii de dysfonctionnement

  Source -> scénario -> effets -> évaluation -> Action de Réduction du Risque

- Étapes :
  - Identifier les ER
  - Étudier et évaluer les ER (hiérarchiser)
  - Définir les actions de maîtrise.

- Préalables : description fonctionnelle (et matérielle).

APR méthode

- Déploiement de deux approches complémentaires :
  - Une approche fonctionnelle : conséquences des défaillances des fonctions du système,
  - Une approche agression :
    - Conséquences des agressions du système vers l'extérieur (elts potentiellement dangereux),
    - Conséquences des agressions du milieu extérieur vers le système (elts sensibles)

APR méthode

Identification des événements redoutés

- Un événement redoutés :
  - est la conséquence d ’un événement initiateur se traduisant par une situation dangereuse, ou plus généralement, par l’échec de la mission du système.
  - peut se manifester par une gène pour l ’utilisateur (dégradation ou échec de la mission), une dégradation de la sécurité ou des pertes financières.

APR méthode

Identification des événements redoutés

- L'identification des ER s'effectue par :

  - l'identification des sources de dangers
  - la recherche d 'un événement initiateur (défaillance de la fonction ou agression) dont les conséquences provoqueront ou pourront provoquer un événement redouté,
  - la description du cheminement des conséquences de cet événement initiateur à travers un scénario,
  - l 'identification de l 'événement redouté final.

APR méthode

Évaluation/Hiérarchisation des événements redoutés

Classe de Gravité

Classe de Gravité	Signification
Catastrophique	Un ou plusieurs morts et/ou Blessés graves et/ou des dommages majeurs à l'environnement
Critique	Un blessé grave et/ou un dommages significatif à l'environnement et/ou perte du système
Marginal	Un blessé légers et/ou une menace significative de l'environnement et/ou dommages sévères au système
Insignifiant	Dommages mineurs au système

APR méthode

Évaluation/Hiérarchisation des événements redoutés

Classe d'occurrence

Classe d'Occurrence	**Signification**
Invraisemblable	Extrêmement invraisemblable à survenir durant la vie du S/S <= 10 (-9)
Rare	Invraisemblable à survenir mais possible durant la vie du S/ S > 10 (-9)
Occasionnelle	Vraisemblable qu'il survienne Plusieurs fois durant la vie du S/S
Fréquente	Vraisemblable qu'il survienne fréquemment durant la vie du S/S

APR méthode

Évaluation/Hiérarchisation des événements redoutés

Criticité du Risque

	Insignifiante	Marginale	Critique	Catastrophique
Invraisemblable	Négligeable	Négligeable	Négligeable	Négligeable
Rare	Négligeable	Tolérable	Indésirable	Intolérable
Occasionnelle	Tolérable	Indésirable	Intolérable	Intolérable
Fréquente	Indésirable	Intolérable	Intolérable	Intolérable

Traitement de l'ER

APR méthode

	Insignifiante	Marginale	Critique	Catastrophique
Invraisemblable	Négligeable	Négligeable	Négligeable	Négligeable
Rare	Négligeable	Tolérable	Indésirable	Intolérable
Occasionnelle	Tolérable	Indésirable	Intolérable	Intolérable
Fréquente	Indésirable	Intolérable	Intolérable	Intolérable

Hiérarchiser :

- on choisit le juste nécessaire pour traiter les ER en fonction de :

•l'expérience

•la criticité

Définir le type de traitement

- comment s'assure t'on que l'ER est maîtrisé ?

•Utilisation d'outils adéquats : AMDEC, AdD, outils spécifiques, …

•Apport des connaissances du spécialiste.

•Accord du groupe de travail

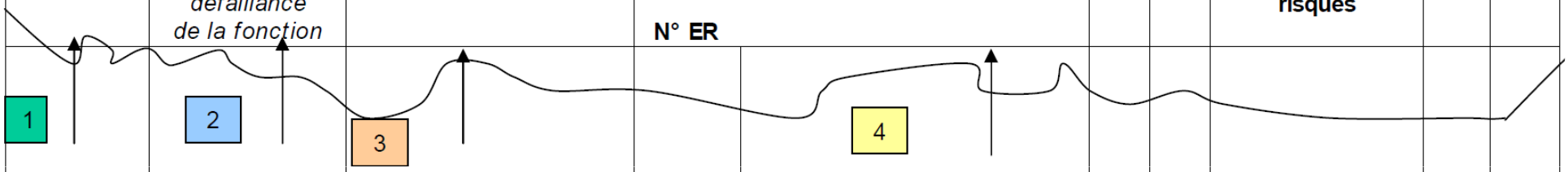
•Diminuer la fréquence ou la gravité

APR méthode

Identification des événements redoutés : Approche fonctionnelle

- Recherche des conséquences des défaillances :
  - de chaque fonction du système,
  - pour chaque situation de vie.
- Formalisée par un tableau

Système :								Page	
Situation de vie :			Pilote :					Date :	
Fonction	**Evénement initiateur** *Mode de défaillance de la fonction*	**Conséquence système et description du scénario**	**N° ER**	**Evènement redouté**	**G**	**F**	**Actions de maîtrise des risques**	**G'**	**F'**
Description de la fonction (service, contrainte, élémentaire …)	- Perte - Dégradation - Absence à la sollicitation - Fonctionnement intempestif	Succession d'évènements provoquant la transformation de l'événement initiateur en événement redouté final (combinaisons de défaillances, des moyens de détection, conditions d'utilisation du système au moment où se produit la défaillance).		Description en termes de gêne pour l'utilisateur, de risque corporel ou de pertes financières.					

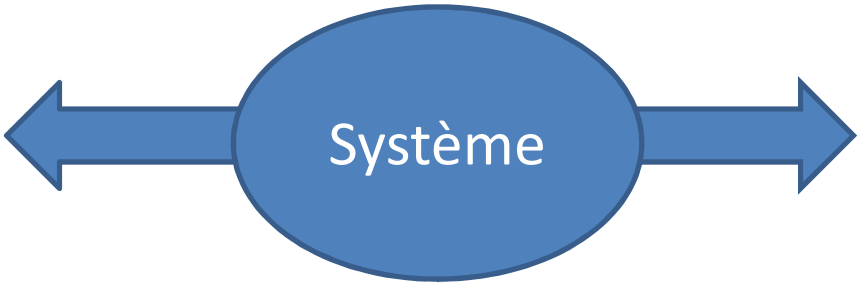


Système : pont roulant									Page 1	
Situation de vie : levage conteneur combustible irradié				Pilote :					Date :	
Fonction	**Evénement initiateur** *Mode de défaillance de la fonction*	**Conséquence système et description du scénario**	**N° ER**	**Evènement redouté**	**G**	**F**	**Actions de maîtrise des risques**		**G'**	**F'**
1 Assurer le maintien de la charge	Lâché de la charge	Chute de la charge sur piscine, rupture des murs, fuite d'eau contaminée, pollution de l'environnement ; risque de fusion des assemblages en piscine.	1	Relâchement de radio-nuclides Fusion possible de combustible	4	?	Si possible : Proposition d'architecture redondante Analyse de risque détaillée (AMDEC, Arbre de Défaillance) Si actions ci-dessus impossibles : dispositions constructives spécifiques		4 2	1

APR méthode

Identification des événements redoutés : Approche agression du système

- L ’identification des ER est réalisée par l ’analyse des conséquences des agressions potentielles que le système peut induire sur le milieu extérieur.
- Formalisée par un tableau

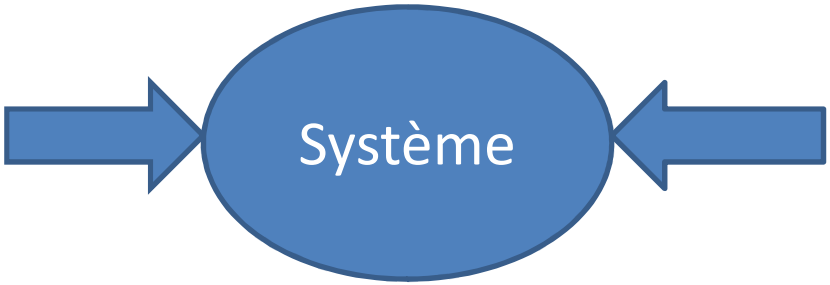


Système									Page	
Situation de vie				Pilote :					Date :	
Elément Potentiellement dangereux	**Evénement initiateur** *Agression système*	**Conséquence système et description du scénario**	**N° ER**	**Evènement redouté**	**G**	**F**	**Actions de maîtrise des risques**		**G'**	**F'**
1 Identification des éléments auxquels on peut associer un danger intrinsèque (possédant une énergie latente capable d'être libérée de manière incontrôlée)	2 Description, correspond à la libération de l'énergie latente d'un élément potentiellement dangereux dont les conséquences provoqueront un événement redouté au niveau système	3 Succession d'évènements provoquant la transformation de l'événement initiateur en événement redouté final (combinaisons de défaillances, des moyens de détection, conditions d'utilisation du système au moment où se produit la défaillance).		4 Description en termes de gêne pour l'utilisateur, de risque corporel, de pertes financières.						

APR méthode

Identification des événements redoutés : Approche agression du système

- Réalisée par l ’analyse des conséquences des agressions Potentielles du Milieu extérieur vers les éléments sensibles du système.
- Formalisée par un tableau



Système								Page	
Situation de vie			Pilote :					Date :	
Elément sensible à agression	**Evénement initiateur** *Agression environnement interface*	**Conséquence système et description du scénario**	**N° ER**	**Evènement redouté**	**G**	**F**	**Actions de maîtrise des risques**	**G'**	**F'**
1	2	3		4					
Identification des éléments du système sensibles à une agression	Description, peut provenir de l'environnement externe ou des autres systèmes interfacés avec le système étudié.	Succession d'évènements provoquant la transformation de l'événement initiateur en évènement redouté final. (combinaisons de défaillances, des moyens de détection, conditions d'utilisation du système au moment où se produit la défaillance).		Description en termes de gêne pour l'utilisateur, de risque corporel, de pertes financières.					

Points sensibles

- Être exhaustif -> travail de groupe
- Constitution d'une donnée d'entrée pour la suite du projet
- Adopter le bon niveau de détails
- Eviter les a priori et fixations

- Attention au syndrome : ça fait X années que l'on fait comme ça!
  - Changement de personnel,
  - Changement de process,
  - Des barrières ont pu disparaître,
  - Évolutions réglementaires ou normatives.

Exemple

- Cycle de vie

ER	PHASE	EVENEMENT	GRAVITE	COMMENTAIRES
1	Exploitation	Vitesse maximale non bridée	Critique	Risque d'accident de la voie publique
2	Mise en service, maintenance	Vitesse maximale bridée de manière intempestive	Significative	Impact sur la disponibilité
3	Maintenance	Non décharge des condensateurs après ouverture de l'appareil	Critique	Danger d'électrocution de l'équipe de maintenance
4	Tests	Résultats des tests utilisateurs incorrects	Significative	Indisponibilité, nécessité d'intervention de la maintenance

Exemple

- Arborescence fonctionnelle

composant	item	situation	Accident Potentiel	compensation	P	G	Remarques
Batteries Cd-Ni	B1	Accélération,chute, vibrations.	Choc, fuite	Bridage, coffre, fixation freinées	4	2	Bac de récupération, évent
	B2	Humidité, corrosion, Oxydation	Oxydation cosse, perte batterie	Maintenance, entretien	4	2	
	B3	Réaction chimique	Explosion	Event,coffre	2	4	
	B4	Chaleur	Pas d'effet	T<70°c	3	1	
	B5	Froid	Baisse des performances	T< -25 °c	3	1	

APR

Checklist de dangers

- Électrique
  - Électrocution, électrisation
  - Brûlure
  - Surchauffe
  - Initiation intempestive de substances en contact ou à proximité
  - Coupure de courant
  - Décharge électrostatique
  - Arc électrique
- Mécanique
  - Équipement tournant
  - Poinçonnement
  - Happement
  - Chute élément lourd
  - Instabilité/basculement
  - Projection d'élément
  - Écrasement
  - Élément coupant
- Incendie (présence de)
  - Carburant
  - Source d'initiation
  - Comburant
  - Produit propulsif
  - Matière inflammable
- Température extrêmes
  - Source de brûlure froide/chaude (surface, immersion, renversement, etc)
  - Élévation de pression
  - Liquide ou gaz confiné
  - Évaporation
  - Réaction
  - Inflammation
  - Gel
  - Dégradation de la fiabilité
  - Dégradation des propriétés mécaniques de la matière

APR

Checklist de dangers

- Équipement sous pression (hydraulique, pneumatique, chimique, etc)
  - Surpression
  - Rupture (canalisation accumulateur, élément, etc)
  - Implosion
  - Défaut de réglage de clapet de surpression
  - Défaut position clapet de surpression
  - Coups de bélier
  - Cavitation

- Accélération, décélération/gravité
  - Impact
  - Perte d'objet en mouvement
  - Chute d'objet
  - Projection d'éclats
  - Ballottement de liquide
  - Chute
  - Glisser/trébucher

APR

Checklist de dangers

- Rayonnement
  - Ionisant
    - Alpha
    - Beta
    - Neutron
    - Gamma
    - X-ray
  - Non ionisant
    - Laser
    - Infrarouge
    - Microonde
    - Ultraviolet
    - Radio
- Explosif
  - Initiation
    - Chaleur
    - Friction
    - Impact, choc
    - Vibration
    - Décharge électrostatique
    - Incompatibilité
    - Foudre
    - Fuite électrique, étincelle
  - Effet
    - Incendie
    - Explosion
    - Surpression
    - Projection d'éclats
    - Onde sismique
- Explosif (suite)
  - Facteur aggravant
    - Chaud, froid
    - Vibration
    - Impact/choc
    - Taux d'humidité
    - Contamination chimique
  - Conditions
    - Poudre propulsive ou explosif
    - Gaz
    - Liquide explosif
    - Poussière explosive
    - Vapeur explosive

APR

Checklist de dangers

- Fuite/épandage (produit)
  - Liquide, produit cryogène
  - Gaz, vapeur
  - Nuage de poussières
  - Sources de radiation
  - Inflammable
  - Toxique
  - Réactif (air, eau, autre produit)
  - Glissant
  - Odorant
  - Pathogène, neurotoxique
  - Asphyxiant
  - Corrosif
- Contamination chimique/eau/sol
  - Fuite
  - Rupture canalisation, réservoir
  - Défaut de distribution/séparation de fluide
- Physiologique (ergonomie)
  - Températures extrêmes
  - Nuisance (odeur, poussière, bruit, vibration, irritant)
  - Variation de pression importante
  - Fatigue
  - Charge portée
  - Allergènes, pathogènes
  - Asphyxiant
  - Radiations
  - Substances toxiques

APR

Checklist de dangers

- Facteur humain
  - Erreur utilisateur
  - Action par inadvertance
  - Action trop tôt/tard
  - Absence d'action
  - Utilisation imprévue
  - Utilisation correct/contrôle incorrect
  - Délai trop long/trop court

- Facteur humain (Cause)
  - Fatigue
  - Inaccessibilité
  - Arrêt d'urgence absent ou inadéquat
  - IHM inadéquate
  - Luminosité trop/pas assez
  - Défaut de conception du poste de travail
  - Procédure de travail/contrôle inadéquate, non présente, mal connue

APR

Checklist de dangers

- Système de contrôle
  - Surtension
  - CEM
  - Humidité
  - Activation intempestive
  - défaillance circuit
  - Défaut de mise à la terre
  - Défaillance logiciel

- Causes communes
  - Perte puissance
  - Humidité
  - Température extrême
  - Mouvement sismique
  - Vibration
  - Poussière, sable
  - Défaut réglage
  - Feu
  - Erreur opérateur
  - Radiation
  - Erreur maintenance
  - Détection
  - Usure
  - Noyage

Grenoble INP génie industriel

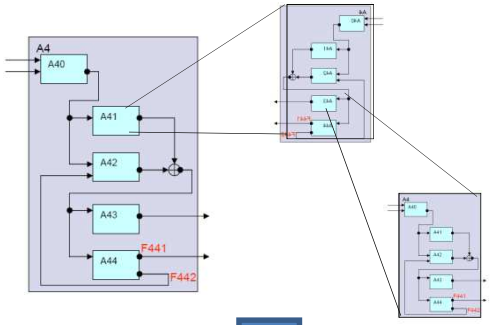
Phases

APR

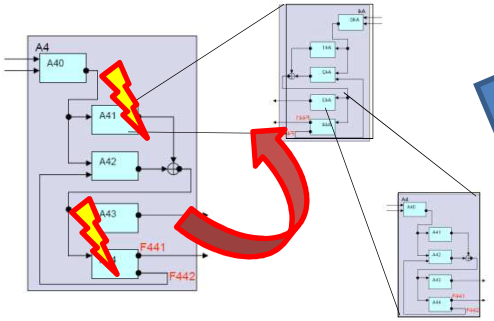
- Transport
- Livraison
- Installation
- Réglage
- Vérification
- Mise en route
- Démarrage standard
- Démarrage d'urgence
- Utilisation normale
- Changement de charge, d'outil
- Accouplement/séparation
- Arrêt standard
- Arrêt d'urgence
- test, diagnostic
- Maintenance
- …

Grenoble INP génie industriel

Système



MdD



ER

Propagation

AMDE/AMDEC

Vocabulaire

AMDE : Analyse des Modes de Défaillance et de leurs Effets

AMDEC : Analyse des Modes de Défaillance, de leurs Effets et de leur Criticité

Equivalences anglaises :

FMEA : Failure Mode and Effects Analysis

FMECA : Failure Mode, Effects and Criticality Analysis

Définition

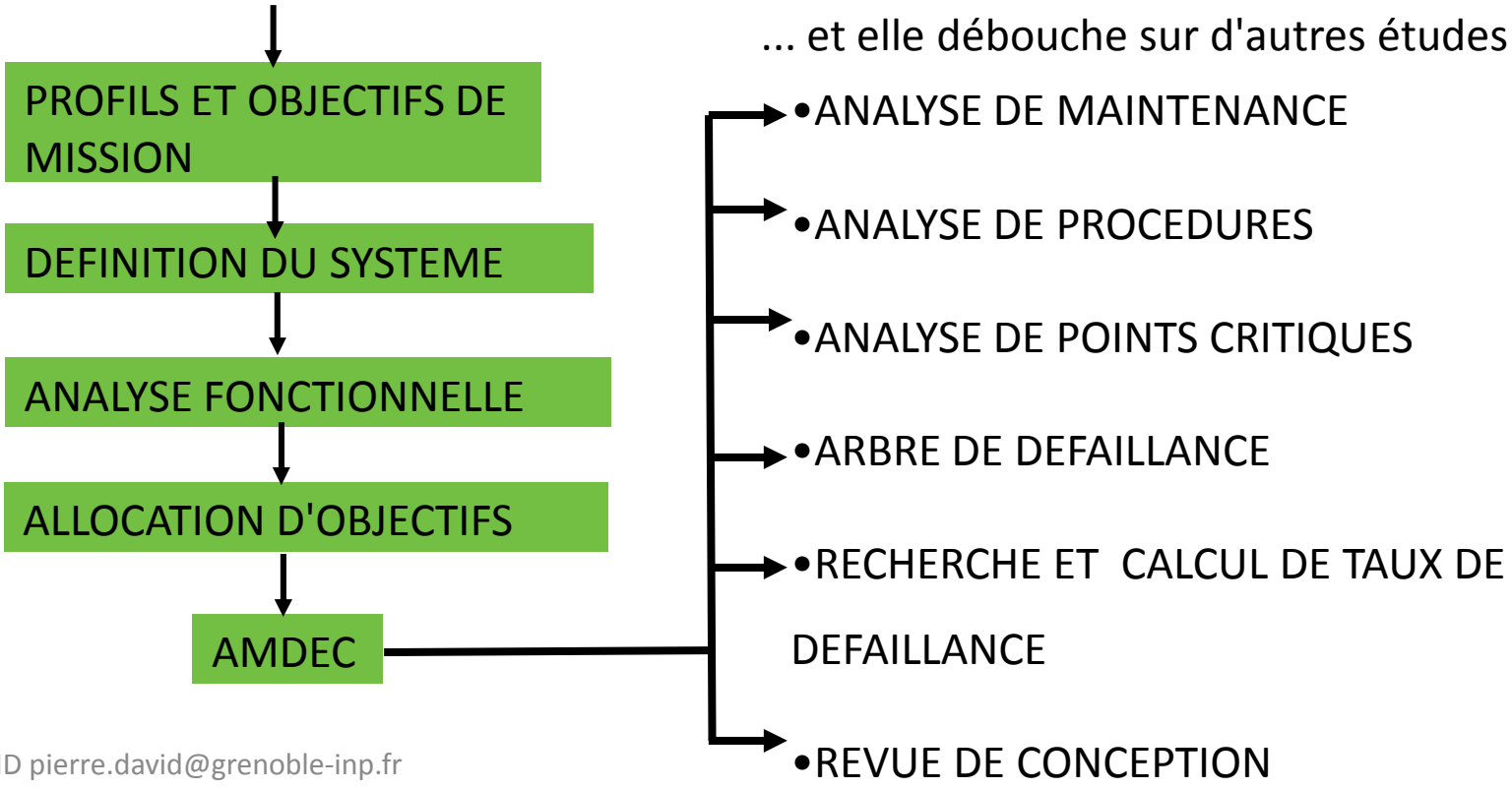
- Technique d'analyse systématique et rigoureuse qui permet :
  - de recenser les modes de défaillances,
  - d'en rechercher les effets,
  - éventuellement d'en identifier les causes,
  - d'évaluer les conséquences et les risques liés à ces défaillances.
- Méthode Inductive
- Analyse de l'influence du dysfonctionnement des composants/fonctions sur le système considéré, dans chacune des phases du profil de mission.
- L'AMDEC est avant tout une méthode d'analyse qualitative.
- Elle peut avoir un aspect quantitatif, lorsqu'elle intègre des notions de taux de défaillance et de probabilités en général

Définition

- L'AMDEC n'est pas une étude isolée

Elle peut venir d'autres études : APR, Arbre de Défaillance

Elle nécessite des étapes de préparation ...



Différents types d'AMDEC

Dans le Temps

- AMDEC "PREVISIONNELLE"

Analyse des modes de défaillance en phase de CONCEPTION,

Développement, d'un système. (Recherche des défaillances potentielles)

- AMDEC "OPERATIONNELLE"

Analyse des modes de défaillance d'un système existant (prototype ou phase exploitation). (Recherche des défaillances potentielles et réelles, démarche d'amélioration)

- L'AMDEC EST EVOLUTIVE ET SUIT LES PHASES D'UN PROJET

  - peu détaillée en phase d'avant-projet,
  - détaillée au cours de la phase de conception,
  - affinée lors des phases de fabrication, assemblage, exploitation ...
  - un lien doit être maintenu au cours du temps entre les AMDEC successives

Différents types d'AMDEC

Par objet d'étude

- AMDEC Produit

  Analyse des défaillances du produit, dues à sa conception, son développement, sa fabrication, son exploitation, ...

- AMDEC Process

  L'AMDEC Process est utilisée pour étudier les défauts potentiels d'un produit nouveau ou non, engendrés par le processus de fabrication.

- AMDEC Moyen de Production (Moyen)

  L'AMDEC - Moyen de production, plus souvent appelée AMDEC-Moyen, permet de réaliser l'étude du moyen de production lors de sa conception ou pendant sa phase d'exploitation.

...

- AMDEC Organisation

Différents types d'AMDEC

Bases de l'analyse

L'AMDEC consiste à étudier les défaillances :

- Des **COMPOSANTS** ou ensemble de composants concourant à la réalisation d'une fonction (ou plusieurs fonctions),

  Parfois appelée « **AMDEC Matériel** » ou « **AMDEC Composants** »

- Des **FONCTIONS**, représentées par des blocs fonctionnels (regroupement d'éléments concourant à la réalisation d'une fonction définie)

  Parfois appelée « **AMDEC Fonctionnelle** »

- Approche "**Matériel**" si les composants peuvent être identifiés individuellement

  composant ➔ sous-système ➔ Effet système

- Approche "**Fonctionnelle**" si les composants ne peuvent être identifiés individuellement ou si la complexité du système impose une définition par blocs fonctionnels

  sous-fonctions des blocs ➔ fonctions du système
  fonctions du système ➔ Effet système

AMDEC fonctionnelle

- **AMDEC fonctionnelle**

  - Réalisable très tôt dès la phase de définition du besoin
  - Utilisation de l'Analyse fonctionnelle système
  - Buts :
    - Rechercher l'implication des fonctions dans les différents domaines (Sécurité, Fiabilité, Maintenance) pour :
      - agir sur la définition fonctionnelle du système
      - minimiser la suite des études
      - rechercher l'implication sur le profil de mission (politique d'exploitation)

AMDEC Composants

- **AMDEC composants**
  - Réalisable dès les phases de conception préliminaire
  - Utilisation de l'Analyse fonctionnelle à un niveau inférieur et utilisation des schémas et plan
  - But :
    - Rechercher l'implication des éléments physiques (limitation de l'étude aux éléments ayant une influence dans les domaines concernés) pour :
      - agir sur la conception
      - éventuellement définir des exigences de maintenance ou d'exploitation
    - Valider une conception en s'assurant de l'absence des effets indésirables

AMDEC Fonctionnelle/Composants

- **AMDEC FONCTIONNELLE :**

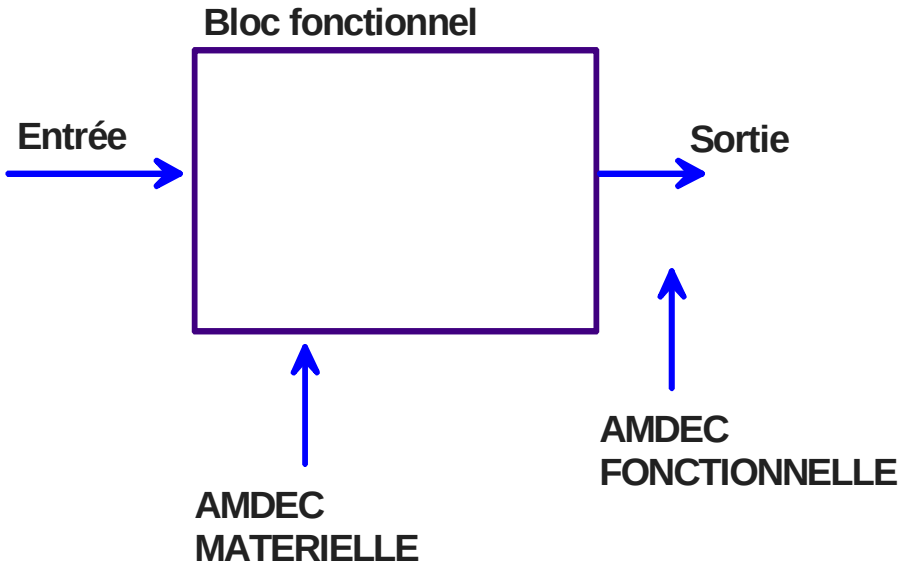
  Mode de défaillance = Défaillance de la fonction ou de la sortie.

  (Correspond à l'effet local)

- **AMDEC MATERIELLE :**

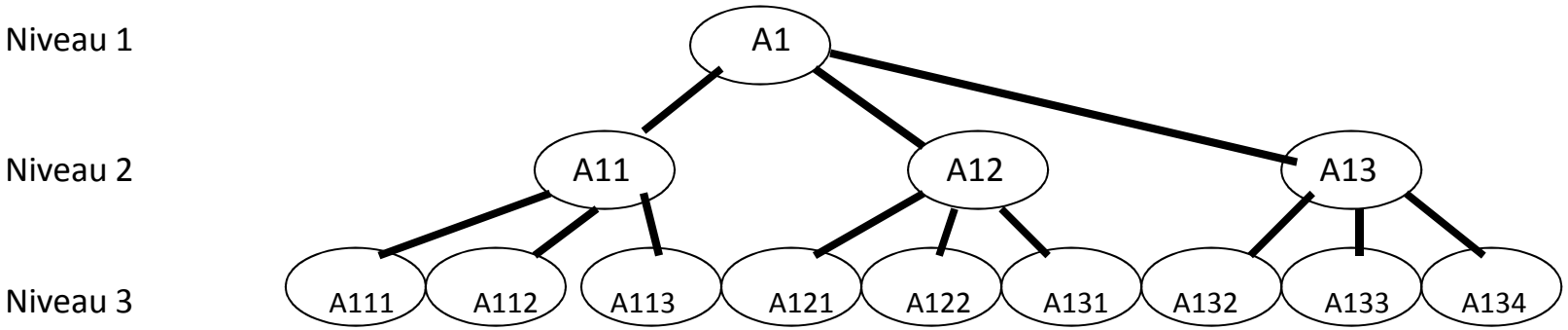
  Mode de défaillance = Défaillance matérielle (interne, entrée, sortie)

  (Effet local = effet sur la fonction ou la sortie attendue)



AMDEC niveau de détails

L'AMDEC SE REALISE A DIFFERENTS NIVEAUX DE DECOUPAGE D'UN SYSTEME



Il est important :

• de bien définir le découpage en niveaux (fonctionnel, matériel),

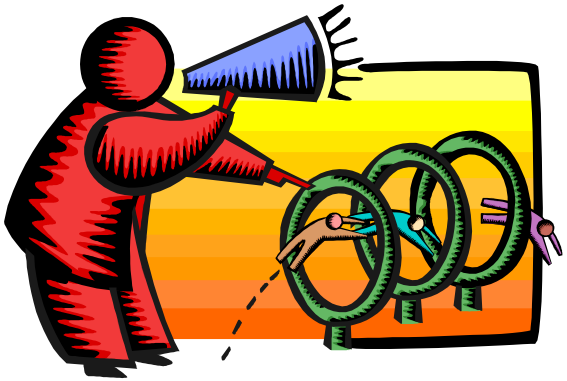
• de choisir comme niveau de base, celui sur lequel on dispose d'informations, ou celui contractuel,

• d'analyser les effets des défaillances sur le ou les niveaux supérieurs
(effet niveau 3 → cause niveau 2)

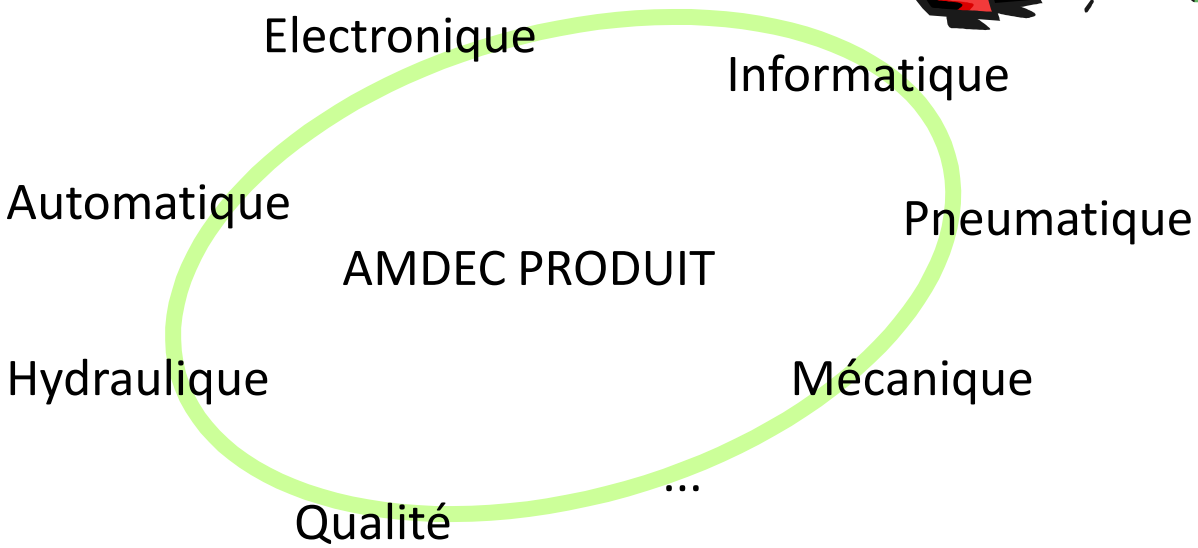
• d'analyser les liaisons entre les différents niveaux.

AMDEC équipe projet

Une AMDEC peut permettre de regrouper toutes les spécialités intervenant sur un système



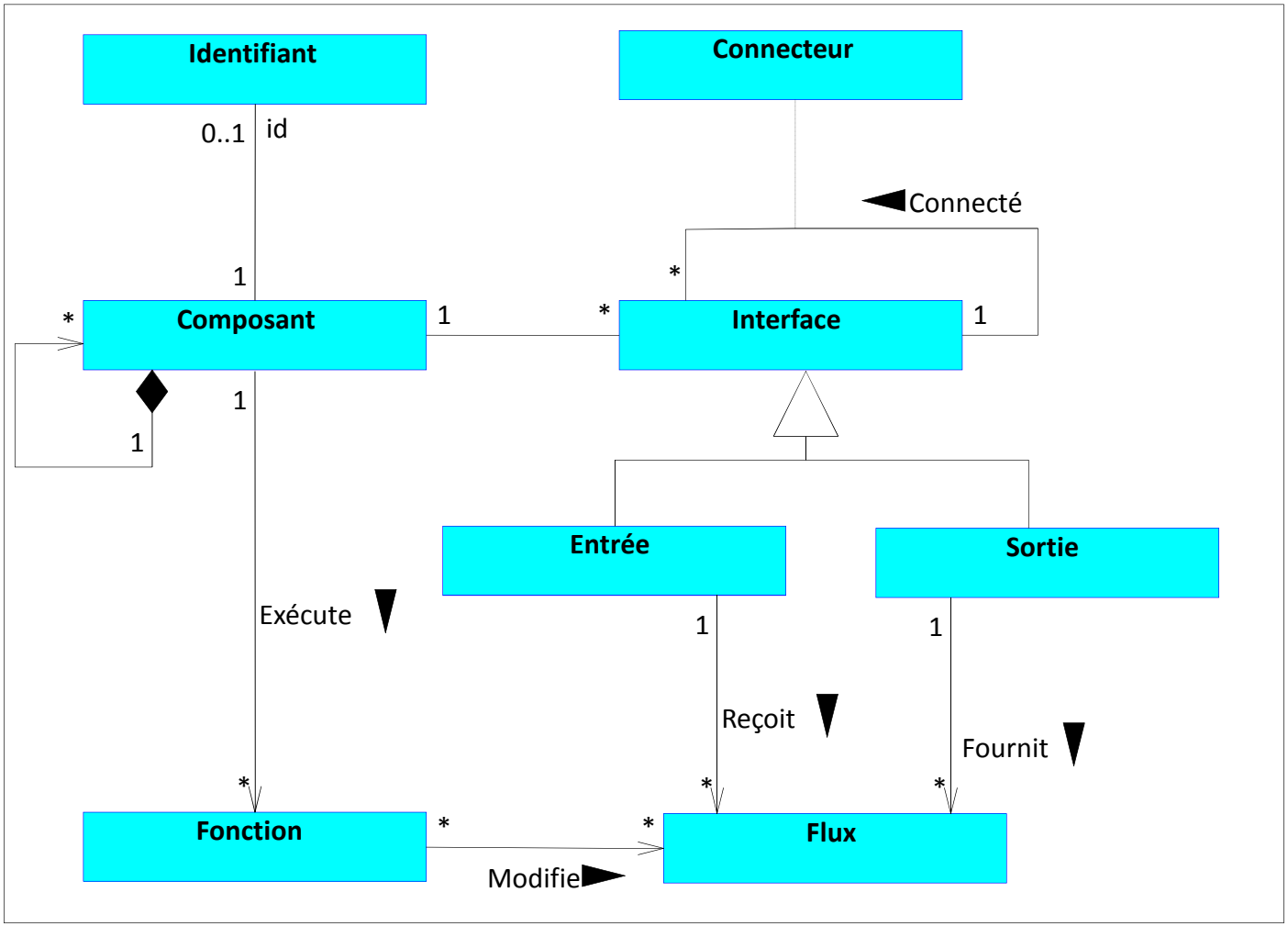
GROUPE DE TRAVAIL



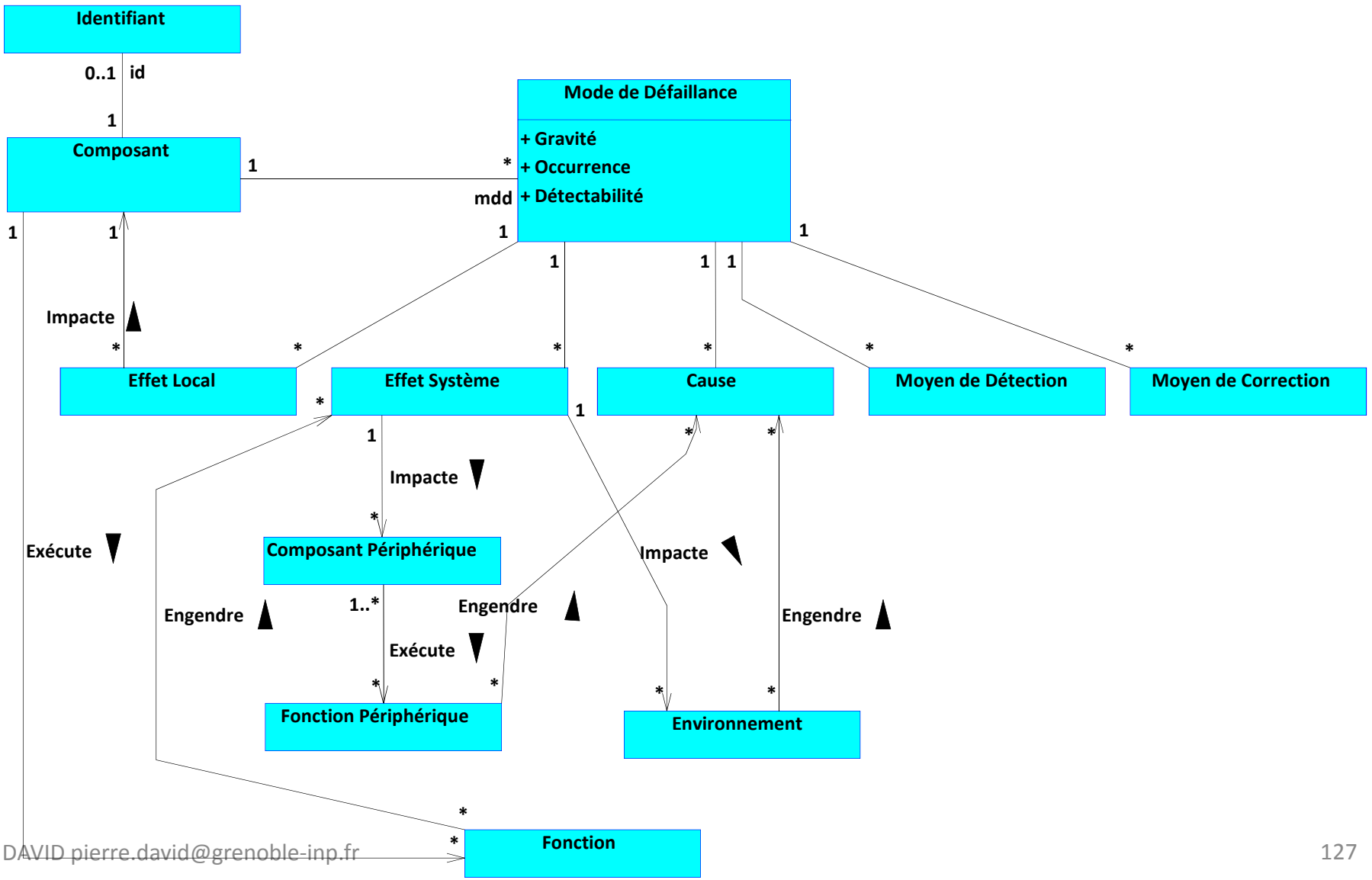
AMDEC : méthode

- Composition
- Connexion

- Exécution
- Diffusion



AMDEC : méthode



Grenoble INP génie industriel

Phase 1 :

AMDEC : méthode

-1- IDENTIFICATION

Préparation de l'AMDEC :

- Caractérisation des limites et des phases d 'utilisation
- Recensement des fonctions et des éléments qui définissent le système,
- Définition des niveaux de découpage,
- Expression des objectifs précis de l'analyse.

-2- DESCRIPTION

L'AMDEC est formalisée par un tableau dont les colonnes représentent les étapes de la procédure AMDEC.

Ces colonnes sont définies selon les objectifs de l'étude.

Certaines néanmoins sont obligatoires :

- désignation et description de l'élément de base considéré (fonction ou matériel),
- modes de défaillance,
- effets des défaillances,
- criticité.

AMDEC : méthode

Phase 1 :

-3- RECENSEMENT DES MODES DE DEFAILLANCE

Un mode de défaillance décrit la façon dont se manifeste une défaillance.

Tout élément est caractérisé par une ou plusieurs fonctions à réaliser, valorisées par des performances.

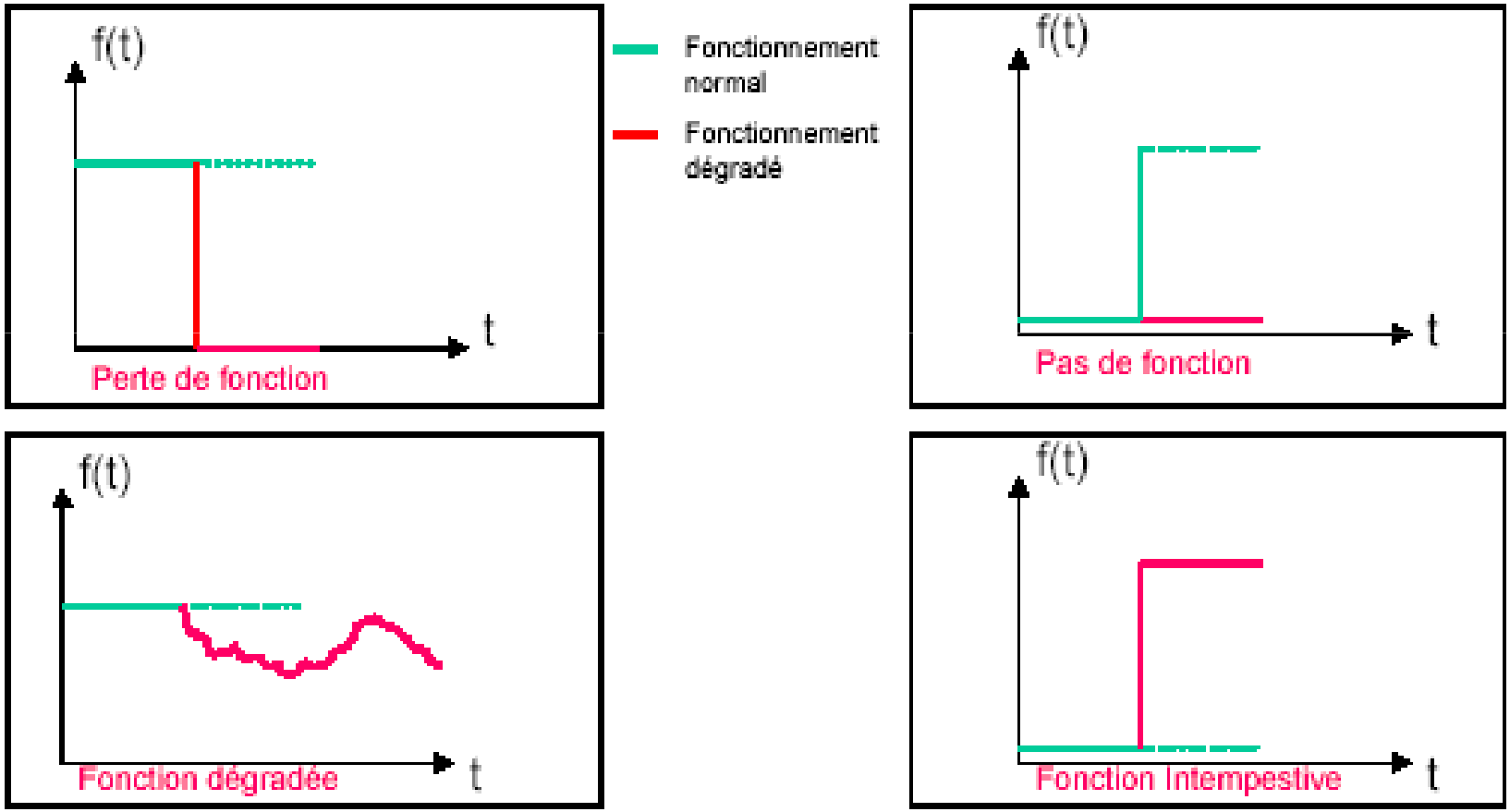
Un mode de défaillance est l'altération de cette ou de ces fonctions.

- PAS de fonction ?
- PERTE de la fonction ?
- DEGRADATION de la fonction ?
- Fonction INTEMPESTIVE ?

On recense tous les modes de défaillances possibles. Heureusement il existe des référentiels.

AMDEC : méthode

Modes de Défaillance générique des fonctions



… Ajout possible des contraintes temporelles

AMDEC : méthode

Modes de Défaillance AFNOR

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

AMDEC : méthode

Phase 1 :

-4-. RECHERCHE DES CAUSES

Suivant les besoins de l'étude, on peut rechercher les causes attribuables à chaque mode de défaillance :

- CAUSES INTERNES
  - défaut de conception, de fabrication,
  - défaut de matériau,
  - intrinsèque (usure ...), ...
- CAUSES EXTERNES
  - mauvaise utilisation,
  - influence de l'environnement (agression, pollution ...)
  - défaillance d'un élément environnant,

On recherche souvent la cause la plus élémentaire (cause des causes).

AMDEC : méthode

Phase 1 :

-5-. RECHERCHE DES EFFETS

On recense les conséquences que peut avoir chaque mode de défaillance.

Il convient de les évaluer sur le ou les niveaux supérieurs, jusqu'au niveau le plus haut (système, process, client ...).

AMDEC : méthode

Phase 2 :

-6-. ANALYSE DE CRITICITE

• Définition :

La criticité est l'expression de l'importance globale d'une défaillance donnée.

Elle permet de hiérarchiser les défaillances selon leur influence globale sur le système, le process, le client ..., vis-à-vis de la fiabilité, la maintenance, la sécurité.

Expression (criticité) :

Elle peut être exprimée par un paramètre ou une combinaison de paramètres tels que :

- gravité : classe ou degré sur les effets des défaillances
- occurrence : taux de défaillance, fréquence d'apparition
- détection : probabilité ou niveau
- paramètres spécifiques aux particularités de l'étude (durée de fonctionnement...)

AMDEC : méthode

$$C = F^{\alpha} G^{\beta} N^{\gamma}$$

Calcul de la criticité

F: Fréquence d'occurrence (taux de défaillance si disponible 1/MTBF)

G: Gravité

N : Probabilité de non détection (signe avant coureur, temps mis pour détecter la défaillance)

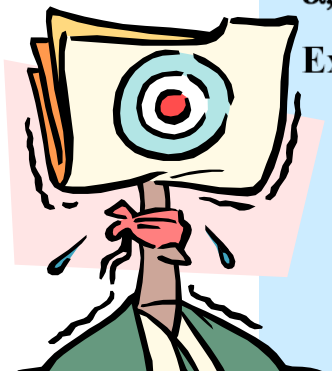
F,G,N : Valeurs numériques si étude prélable de FMD

F,G,N : Valeurs entières (Echelle pour chacune 1-10, 1-4, 1-6)
Valable pour étude AMDEC au sein de l'entreprise

Ne change selon le système

α,β,γ : A définir avec justification et précaution (sinon 1 par défaut)

Exemple



	F	G	N	C α=1β=3 γ=1	C α=3 β=1γ=1
Defail 1	1	4	1	64	4
Défail 2	4	1	1	4	64

15

AMDEC : méthode

Gravité	CONSEQUENCES				PROBABILITE				
	Personnes	Biens	Environnement		A	B	C	D	E
					Pas connu dans votre industrie	S'est produit dans votre industrie	Arrivé dans votre Compagnie	Arrivé plusieurs fois par an dans votre compagnie	Arrivé plusieurs fois par an sur votre site
0	Pas de blessé	Pas de dommage	Pas d'effet (ni environement ni coût)						
1	Blessures légères (Soin infirmerie ou ASA)	Dommages légers.	Faibles effets (interne au site et coût négligeable)						
2	blessures mineures (AAA)	Dommages mineurs.	Effets mineurs						
3	Blessures graves (Arrêt de travail prolongé)	dommages localisés.	effets localisés						
4	Un à trois décès	Dommages importants	effets importants						
5	Plusieurs décès	dommages énormes	effets énormes						

AMDEC : méthode

Phase 2 :

-7-. MODE DE DETECTION

Dans cette colonne sont décrits les différents moyens envisagés, permettant de détecter l'apparition du Mode de Défaillance ou de l'effet.

-8-. ACTIONS CORRECTIVES OU DE MAINTENANCE

Afin de concrétiser les résultats de l'analyse, on décrit les actions à engager suite à la définition des priorités.

Domaines possibles d'actions :

modifications de conception, portant par exemple sur la fréquence et la détectabilité des défaillances,

actions de maintenance, portant sur la gravité des modes de défaillances

Exemple de Tableau

Objet :
Système : Atelier A (fabrication)
Sous-système : Alimentation par pompe X

ANALYSE DES MODES DE DEFAILLANCES DES COMPOSANTS ET DE LEURS EFFETS SUR LE SYSTEME

Documents :

Identification du composant	Fonction états	Modes de défaillance	Causes possibles de défaillance	Conséquences		Classe de gravité	Moyen de détection des défaillances	Actions correctrices	Remarques
				Locales	Sur le système				

Observations

- Les remarques suivantes sont issues d'expériences d'applications d'AMDEC.
  - L'AMDEC est souvent engagée trop tard par rapport au développement d'un produit.
  - La formation du personnel à la méthode est souvent insuffisante.
  - La création d'un groupe de travail pour l'application de l'AMDEC est préférable pour son efficacité.
  - L'Analyse Fonctionnelle du système préalablement à l'application de l'AMDEC n'est pas systématique, alors qu'elle sert à définir les fonctions et niveaux du système étudié.

AMDEC Points faibles

- Lourdeur de gestion pour des systèmes complexes
  - Beaucoup de composants
  - Multiples fonctions
  - Différentes politiques de réparation et d'entretien
  - Plusieurs modes opérationnels

Recommandations ➔ Bien délimiter le cadre de l'étude

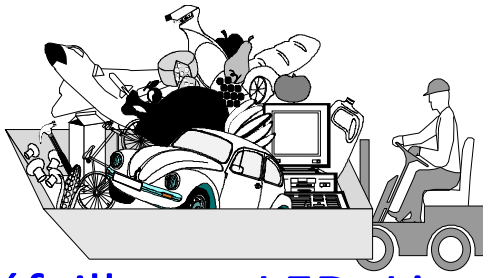
- L'AMDEC ne met pas en évidence les combinaisons éventuelles de défaillances, entraînant la défaillance globale du système.

Recommandations ➔ Compléter l'AMDEC, si possible, par des arbres de défaillances pour les événements les plus critiques

AMDEC Points faibles

- Volume d'informations très important et souvent non homogène

- Risque de perte d'information par synthèse



=> Recommandations

- Ne pas se perdre dans les détails
- Traiter les AMDEC (Liste des Effets de Défaillance LED, Liste de Articles Critiques LAC,...)

AMDEC Points faibles

- Certains points durs dans la réalisation :
  - Analyse du contexte et déterminer le périmètre de l'étude
  - Métrique du risque (définition des échelles de cotation)
  - Explicitation des risques
  - Obsolescence des connaissances contenue dans les analyses
  - Cohérence intra et inter-analyses
  - Maîtrise du vocabulaire (recommandations: création de dictionnaire)

AMDEC Points forts

- Outil très **performant** lorsqu'il est utilisé dès la phase de conception.
- Connaissance des **états dégradés** du système.
- L'AMDEC permet la constitution de **bases de données** sur les **connaissances** relatives aux produits, aux procédés et à l'organisation, en particulier utiles pour d'autres AMDEC.
- Outil de base pour la **construction** de la **maintenance.**

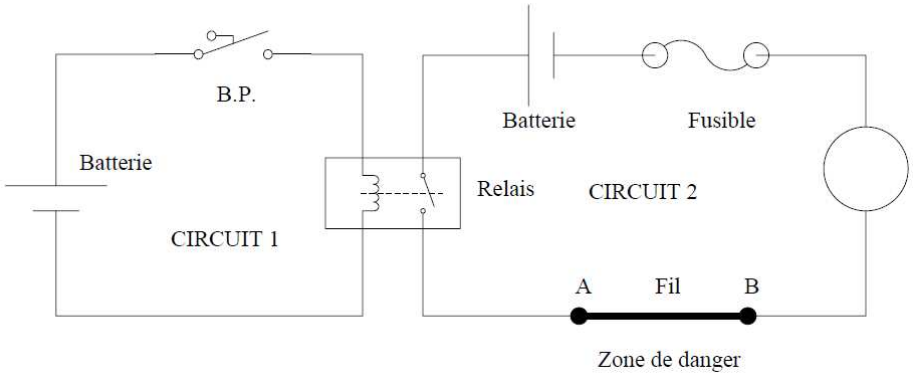
AMDEC Points forts

- Établissement d'une liste de points critiques. (LAC) ; Synthèse pour des revues de conception

- Mise en évidence de priorités : contrôle, vérification, fabrication, points de tests, pièces de rechange de premier niveau,...

- La mise en place d'un groupe de travail facilite les relations :
  - entre les différents services, vis à vis du système,
  - entre les différents spécialistes techniques.

Exemple relations internes



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

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

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

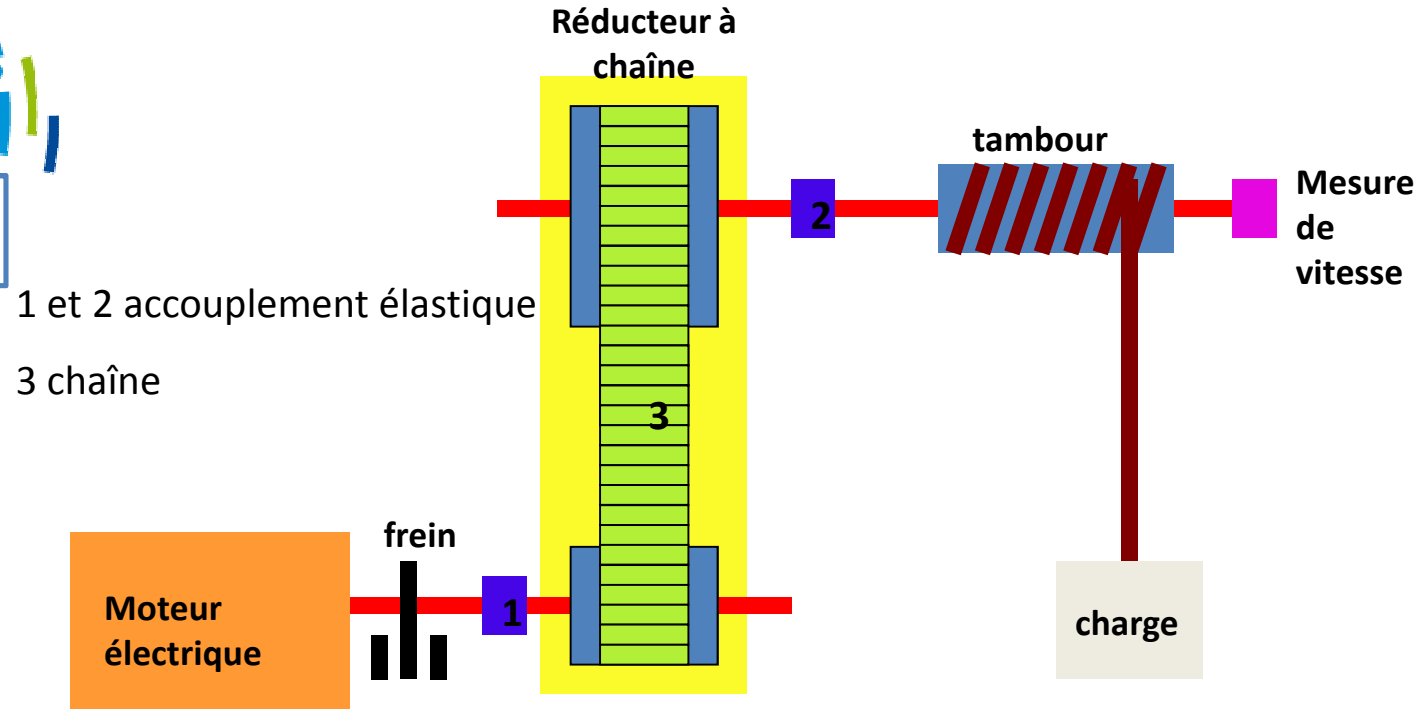
L'analyse portera seulement sur les composants suivants :

- Bouton poussoir – Relais – Fusible – Moteur.

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

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

EXEMPLE 2



1 et 2 accouplement élastique

3 chaîne

-- Le moteur électrique entraîne le réducteur;
-- Le réducteur est constitué par une chaîne et deux pignons à dents ;
-- le frein hydraulique assure le maintien de la charge en position dès qu'il y a commande de l'arrêt du moteur;
-- pour palier aux défauts d'alignements et amortir une partie des efforts de torsion, les liaisons entre le moteur, le réducteur et le tambour sont réalisées par des accouplements élastiques;
-- Un dispositif, lié au tambour, mesure sa vitesse de rotation; en cas de vitesse excessive, il commande l'arrêt du moteur et le freinage;
-- l'alimentation électrique du moteur, la centrale hydraulique et son alimentation électrique, le circuit de contrôle/commande ne sont pas représentés.

Grenoble INP génie industriel

composant	fonction	Modes de défaillance	Causes	Effet sur le système	Effets/sécurité	Moyen de détection
Moteur électrique	Assure l'entraînement du réducteur					
Frein	Assure le maintien de la charge en position et le freinage d'urgence					

Grenoble INP

composant	fonction	Modes de défaillance	Causes	Effet sur le système	Effets/sécurité	Moyen de détection
Accouplement élastique 1	Assure la liaison entre le moteur et le réducteur					
Réducteur	Entraîne le tambour par rotation					
Accouplement élastique 2	Assure la liaison entre le réducteur et le tambour					
Dispositif de mesure de vitesse	Commande l'arrêt du moteur et le freinage lorsque la vitesse de rotation du tambour dépasse un seuil					

Grenoble INP génie industriel

composant	fonction	Modes de défaillance	Causes	Effet sur le système	Effets/sécurité	Moyen de détection
Moteur électrique	Assure l'entraînement du réducteur	Non démarrage				
		Arrêt intempestif				
		Pas d'arrêt				
		Démarrage intempestif				
Frein	Assure le maintien de la charge en position et le freinage d'urgence	Absence de freinage				
		Freinage intempestif				

Grenoble INP

composant	fonction	Modes de défaillance	Causes	Effet sur le système	Effets/sécurité	Moyen de détection
Accouplement élastique 1	Assure la liaison entre le moteur et le réducteur	rupture				
Réducteur	Entraîne le tambour par rotation	Blocage				
		Rupture de la chaîne				
Accouplement élastique 2	Assure la liaison entre le réducteur et le tambour	rupture				
Dispositif de mesure de vitesse	Commande l'arrêt du moteur et le freinage lorsque la vitesse de rotation du tambour dépasse un seuil	Commande intempestive				
		Absence de commande d'arrêt (en cas de vitesse excessive)				

Grenoble INP génie industriel

composant	fonction	Modes de défaillance	Causes	Effet sur le système	Effets/sécurité	Moyen de détection
Moteur électrique	Assure l'entraînement du réducteur	Non démarrage	Défauts internes Défauts d'alimentation électrique Défauts de la commande			
		Arrêt intempestif	Défauts internes Défauts d'alimentation électrique Défauts de la commande Erreur humaine (commande intempestive)			
		Pas d'arrêt	Défauts de la commande Erreur humaine (commande intempestive)			
		Démarrage intempestif	Erreur humaine (commande intempestive)			
Frein	Assure le maintien de la charge en position et le freinage d'urgence	Absence de freinage	Défauts internes Défauts de la commande Défauts de la centrale hydraulique Usure des garnitures			
		Freinage intempestif	Défauts internes Défauts de la commande			

Grenoble INP

composant	fonction	Modes de défaillance	Causes	Effet sur le système	Effets/sécurité	Moyen de détection
Accouplement élastique 1	Assure la liaison entre le moteur et le réducteur	rupture	Défauts internes Absence de graissage			
Réducteur	Entraîne le tambour par rotation	Blocage	Défauts propres Efforts anormaux			
		Rupture de la chaîne				
Accouplement élastique 2	Assure la liaison entre le réducteur et le tambour	rupture	Défauts propres Vieillissements			
Dispositif de mesure de vitesse	Commande l'arrêt du moteur et le freinage lorsque la vitesse de rotation du tambour dépasse un seuil	Commande intempestive	Défauts propres			
		Absence de commande d'arrêt (en cas de vitesse excessive)	Défauts propres			

Grenoble INP génie industriel

composant	fonction	Modes de défaillance	Causes	Effet sur le système	Effets/sécurité	Moyen de détection
Moteur électrique	Assure l'entraînement du réducteur	Non démarrage	Défauts internes Défauts d'alimentation électrique Défauts de la commande	Perte de la fonction levage		
		Arrêt intempestif	Défauts internes Défauts d'alimentation électrique Défauts de la commande Erreur humaine (commande intempestive)	Perte de la fonction levage		
		Pas d'arrêt	Défauts de la commande Erreur humaine (commande intempestive)	Risque de chute de la charge	Danger pour les personnels	
		Démarrage intempestif	Erreur humaine (commande intempestive)		Danger pour les personnels	
Frein	Assure le maintien de la charge en position et le freinage d'urgence	Absence de freinage	Défauts internes Défauts de la commande Défauts de la centrale hydraulique Usure des garnitures	Non-maintien de la charge en position descente par gravité jusqu'au sol	Danger pour les personnels	
		Freinage intempestif	Défauts internes Défauts de la commande	Perte de la fonction levage		

composant	fonction	Modes de défaillance	Causes	Effet sur le système	Effets/sécurité	Moyen de détection
Accouplement élastique 1	Assure la liaison entre le moteur et le réducteur	rupture	Défauts internes Absence de graissage	descente de la charge par gravité, augmentation de la vitesse du tambour, freinage sans effet	Danger pour les personnels	
Réducteur	Entraîne le tambour par rotation	Blocage	Défauts propres Efforts anormaux	Perte de la fonction levage		
		Rupture de la chaîne		descente de la charge par gravité, augmentation de la vitesse du tambour, freinage sans effet	Danger pour les personnels	
Accouplement élastique 2	Assure la liaison entre le réducteur et le tambour	rupture	Défauts propres Vieillissements	descente de la charge par gravité, augmentation de la vitesse du tambour, freinage sans effet	Danger pour les personnels	
Dispositif de mesure de vitesse	Commande l'arrêt du moteur et le freinage lorsque la vitesse de rotation du tambour dépasse un seuil	Commande intempestive	Défauts propres	Perte de fonction levage		
		Absence de commande d'arrêt (en cas de vitesse excessive)	Défauts propres	descente de la charge par gravité jusqu'au sol	Danger pour les personnels	

Grenoble INP génie industriel

composant	fonction	Modes de défaillance	Causes	Effet sur le système	Effets/sécurité	Moyen de détection
Moteur électrique	Assure l'entraînement du réducteur	Non démarrage	Défauts internes Défauts d'alimentation électrique Défauts de la commande	Perte de la fonction levage		
		Arrêt intempestif	Défauts internes Défauts d'alimentation électrique Défauts de la commande Erreur humaine (commande intempestive)	Perte de la fonction levage		
		Pas d'arrêt	Défauts de la commande Erreur humaine (commande intempestive)	Risque de chute de la charge	Danger pour les personnels	
		Démarrage intempestif	Erreur humaine (commande intempestive)		Danger pour les personnels	
Frein	Assure le maintien de la charge en position et le freinage d'urgence	Absence de freinage	Défauts internes Défauts de la commande Défauts de la centrale hydraulique Usure des garnitures	Non-maintien de la charge en position descente par gravité jusqu'au sol	Danger pour les personnels	
		Freinage intempestif	Défauts internes Défauts de la commande	Perte de la fonction levage		Par thermique du moteur

composant	fonction	Modes de défaillance	Causes	Effet sur le système	Effets/sécurité	Moyen de détection
Accouplement élastique 1	Assure la liaison entre le moteur et le réducteur	rupture	Défauts internes Absence de graissage	descente de la charge par gravité, augmentation de la vitesse du tambour, freinage sans effet	Danger pour les personnels	Par dispositif de mesure de vitesse
Réducteur	Entraîne le tambour par rotation	Blocage	Défauts propres Efforts anormaux	Perte de la fonction levage		Par thermique du moteur
		Rupture de la chaîne		descente de la charge par gravité, augmentation de la vitesse du tambour, freinage sans effet	Danger pour les personnels	Par dispositif de mesure de vitesse
Accouplement élastique 2	Assure la liaison entre le réducteur et le tambour	rupture	Défauts propres Vieillissements	descente de la charge par gravité, augmentation de la vitesse du tambour, freinage sans effet	Danger pour les personnels	Par dispositif de mesure de vitesse
Dispositif de mesure de vitesse	Commande l'arrêt du moteur et le freinage lorsque la vitesse de rotation du tambour dépasse un seuil	Commande intempestive	Défauts propres	Perte de fonction levage		
		Absence de commande d'arrêt (en cas de vitesse excessive)	Défauts propres	descente de la charge par gravité jusqu'au sol	Danger pour les personnels	

Memento Gestion AMDEC

① PRÉSENTATION	② ANIMATION DE L'AMDEC
1.1 Bien définir le problème à traiter : — formaliser les objets recherchés ; — déterminer les limites de l'étude. **1.2 Constituer le groupe de travail :** — sélectionner les participants ; — établir les convocations aux réunions en précisant les objectifs et les limites de l'étude. **1.3 Déterminer le planning de travail :** — prévoir le nombre de réunions ; — intégrer les séquences de synthèse et le bilan. **1.4 Réunir les documents nécessaires :** — relevé des incidents sur le moyen de production étudié ; — plans, schémas, notes de calcul, etc. **1.5 Faire le découpage fonctionnel du moyen de production étudié** **1.6 Réserver les moyens logistiques des réunions :** — réserver les salles de réunion avec le matériel nécessaire.	**2.1 Présenter les participants et rappeler les objectifs de l'analyse** **2.2 Présenter les principes de l'AMDEC** **2.3 Présenter l'installation à l'aide de son découpage fonctionnel** **2.4 Mettre au point et valider les tables de cotation de la criticité** **2.5 Réaliser l'analyse AMDE (documentation des grilles d'analyse)** **2.6 Déterminer la criticité (documentation des grilles d'analyse)** **2.7 Déterminer les actions correctives le cas échéant (documentation des grilles d'analyse)** **2.8 Déterminer la nouvelle criticité le cas échéant (documentation des grilles d'analyse)**

Memento Gestion AMDEC

③ SYNTHÈSE

3.1 Mettre au propre les documents d'analyse :
- — mise au propre du découpage fonctionnel ;
- — mise au propre des grilles AMDEC avec vérifications.

3.2 Établir le bilan des indices de criticité avec classement par tableaux et graphiques :
- — pourquoi ?
  - • pour faire l'analyse par sous-système ;
- — comment ?
  - • par pondération des actions correctives,
  - • par hiérarchisation par sous-système et par types d'action ;
- — dans quel but ?
  - • faire une synthèse des indices de criticité.

3.3 Éditer la liste des préconisations avec l'approche d'un plan d'action global :
- — pourquoi ?
  - • analyser par types d'action et par sous-système ;
- — comment ?
  - • par extraction des actions correctives depuis les grilles AMDEC ;
- — dans quel but ?
  - • élaborer un plan d'action à mettre en place rapidement.

3.4 Présenter le rapport en 5 parties :
- — 1re partie : synthèse de l'AMDEC
  - • feuille de synthèse
  - • schémas de l'installation
  - • découpage de l'AMDEC
  - • statistiques sur les criticités
  - • liste des actions par défaut
- — 2e partie : tableaux AMDEC
  - • suivant la décomposition de l'installation
- — 3e partie : liste des points critiques
  - • Criticité $\geqslant$ 16 ou $G \geqslant 4$ ou $F = 4$ après 2e cotation
- — 4e partie : actions correctives fournisseur
  - • qualité du produit fabriqué
  - • fiabilité de l'installation
  - • maintenabilité de l'installation
  - • sécurité
  - • remarques
- — 5e partie : actions correctives client
  - • dispositions de maintenance
  - • formation à l'exploitant
  - • organisation logistique

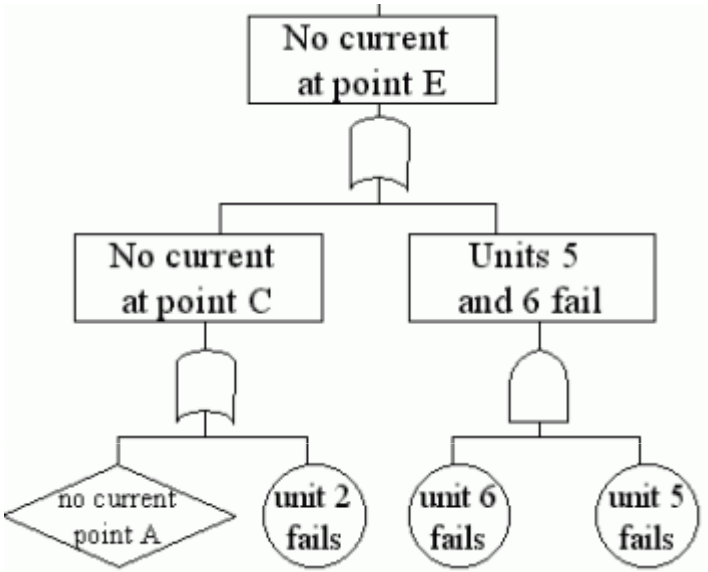
④ SUIVI

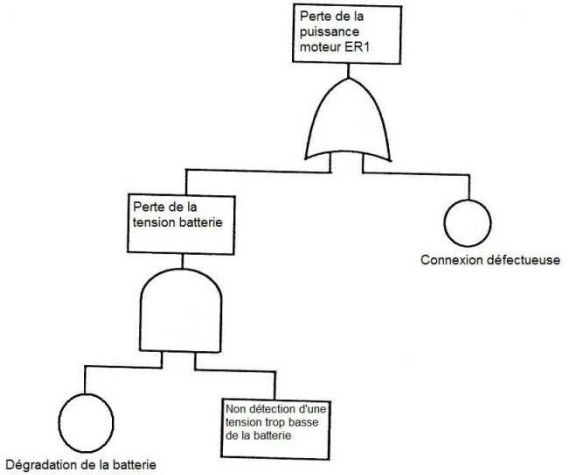
4.1 Établir un planning pour mener les actions

4.2 Veiller à la bonne application des mesures préconisées

4.3 Approvisionner les moyens et ressources nécessaires à la réalisation des actions correctives

4.4 Prendre en compte les mises à jour :
- — de la documentation ;
- — des gammes de maintenance préventives ;
- — des listes de pièces de rechange ;
- — etc.

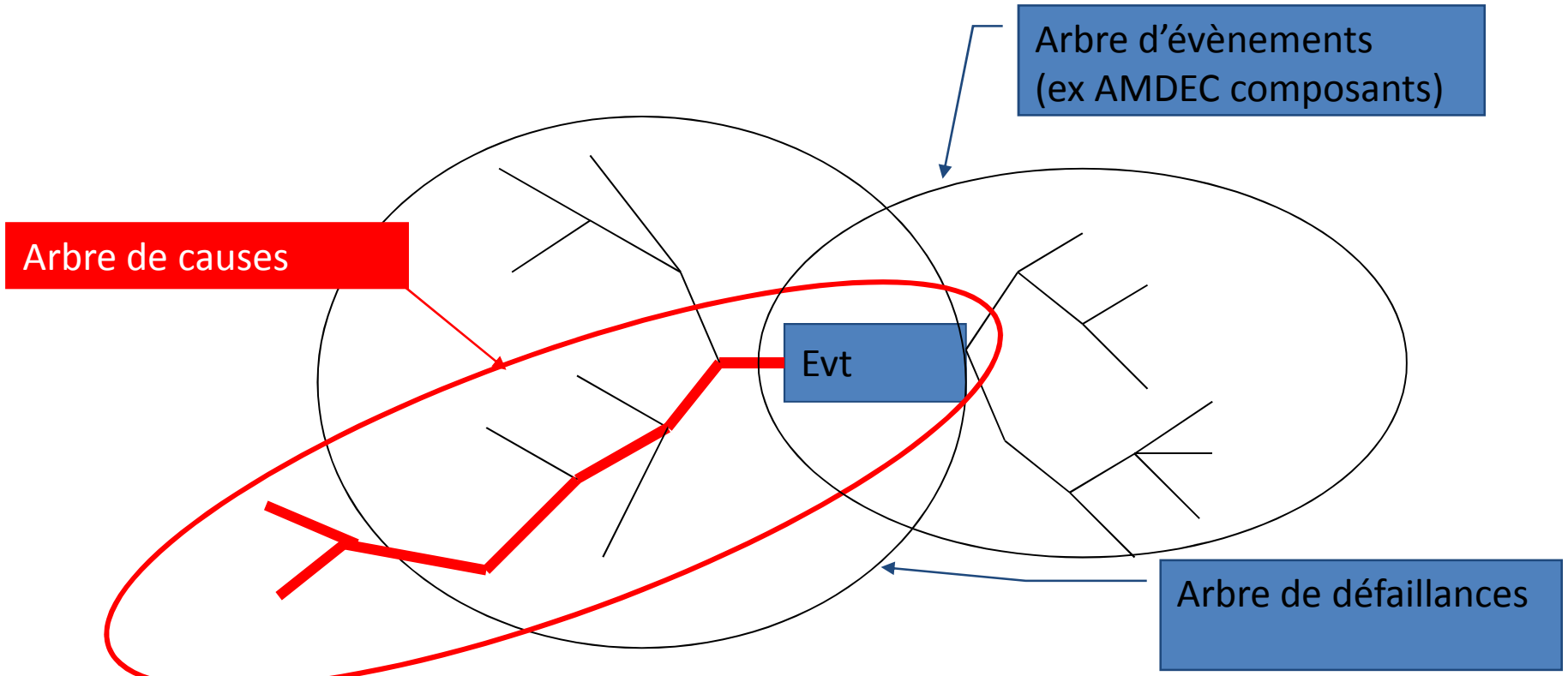




ARBRES DE DÉFAILLANCES

Généralités

- Méthodes **déductives** qui permet d'investiguer les causes d'un événement redouté et représente **tous** les scénarios redoutés,
- Permet d'accéder rapidement à des caractérisations quantitatives.



Définition et objectifs

- Représenter **graphiquement** les relations causes/effets, à l'aide d'une structure de type arbre logique (portes logiques, et, ou, …).
- Résultats attendus :
  - qualitatifs : scénarios possibles conduisant à l'ER
  - quantitatifs : probabilité d 'apparition de l'ER.
- Évaluer l'importance des différents scénarios dans l 'apparition d'un ER.
- Orienter les actions d'étude et d'amélioration de la conception.
- Éventuellement, aider à l 'allocation d 'objectifs de SdF.
- L'objectif est de suivre une logique déductive en partant d'un Événement Redouté (noté ER) pour déterminer **de manière exhaustive** l'ensemble de ses causes jusqu'aux plus élémentaires

AdD Démarche

-1-. Définition des événements

•<u>Événement redouté</u> :

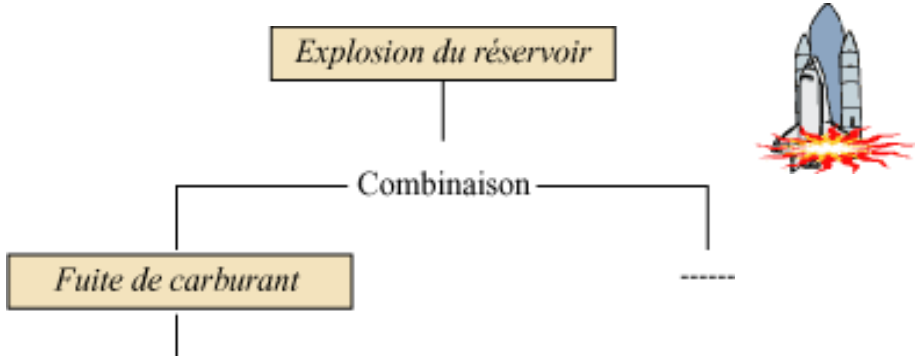
•L'événement redouté est l'événement indésirable pour lequel nous faisons l'étude de toutes les causes qui y conduisent. Cet événement est unique pour un arbre de défaillance et se trouve au "sommet" de l'arbre.

•Avant de commencer la décomposition qui permet d'explorer toutes les combinaisons d'événements conduisant à l'événement redouté, il faut définir avec précision cet événement ainsi que le contexte de son apparition.

•L'événement redouté est représenté par un rectangle au sommet de l'arbre comme par exemple l'explosion du réservoir de carburant de Challenger.

AdD Démarche

-2-. Définition des événements



•<u>Événements intermédiaires</u> :

•Les événements intermédiaires sont des événements à définir comme l'événement redouté. La différence avec l'événement redouté est qu'ils sont des causes pour d'autres événements. Par exemple c'est la combinaison d'événements intermédiaires qui conduit à l'événement redouté.

•Un événement intermédiaire est représentés par un rectangle comme l'événement redouté. Dans notre exemple, c'est la combinaison d'une fuite de carburant avec d'autres événements qui est susceptible de provoquer l'explosion du réservoir.

AdD Démarche

-3-. Définition des événements

- Événements élémentaires :
- Les événements élémentaires sont des événements correspondants au niveau le plus détaillé de l'analyse du système. Dans un arbre de défaillance ils représentent les défaillances des composants qui constituent le système étudié.

- Pour fixer le niveau de détails de notre étude, nous considérons en général que les événements élémentaires coïncident avec la défaillance des composants qui sont réparables ou interchangeables.

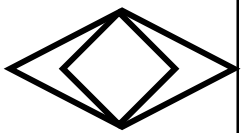
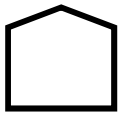
- Les événements élémentaires sont représentés par des cercles. Dans notre exemple, c'est la combinaison de la défaillance Joint percé et Vanne bloquée ouverte qui provoque une fuite de carburant.

AdD Démarche

-4-. Définition des événements

Résumé de la symbolique des événements :

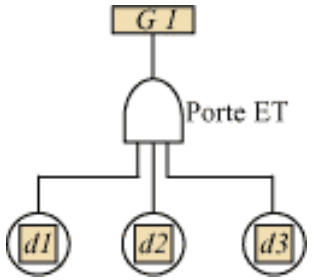
- Il existe d'autres types d'événements définis par la norme leurs symboles ainsi que leurs significations sont répertoriés dans le tableau suivant.

Symbole	Nom	Signification
	Rectangle	Événement redouté ou événement intermédiaire
	Cercle	Événement élémentaire
	Losange	Événement élémentaire non développé
	Double losange	Événement élémentaire dont le développement est à faire ultérieurement
	Maison	Événement de base survenant normalement pour le fonctionnement du système

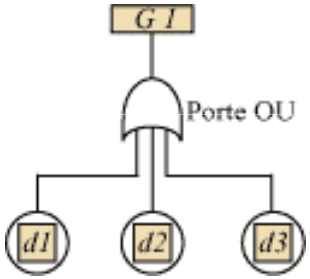
AdD Démarche

-5-. Portes logiques de base

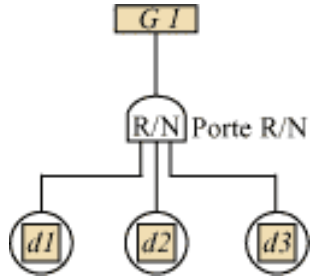
Porte ET :
L'événement G1 ne se produit que si les événements élémentaires d1, d2 et d3 existent simultanément.



Porte OU :
L 'événement G1 se produit de manière indépendante si l'un ou l'autre des événements élémentaires d1, d2 ou d3 existe.



Porte R/N :
Si R=2 et N=3 alors il suffit que deux des événements élémentaires d1, d2, d3 soient présents pour que l'événement G1 se réalise.



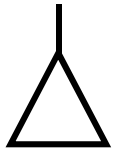
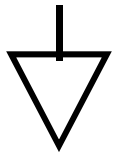
AdD Démarche

-6-. Transfert de sous-arbres

Il existe pour les arbres de défaillances une symbolique normalisée qui permet de faire référence à des parties de l'arbre qui se répètent de manière *identique** ou de manière *semblable* [+] pour éviter de les redéfinir.
L'objectif est de réduire la taille du graphique. Le tableau suivant présente les symboles ainsi que les significations qui sont utilisés.

* Identique : même structure, même événements.

[+] Semblable : Même structure mais avec des événements différents.

Symbole	Nom	Signification
	Triangle	La partie de l'arbre qui suit le premier symbole se retrouve identique, sans être répétée, à l'endroit indiqué par le second symbole.
	Triangle inversé	La partie de l'arbre qui suit le premier symbole se retrouve semblable mais non identique à l'endroit indiqué par le second symbole.

AdD Démarche

Règles de construction

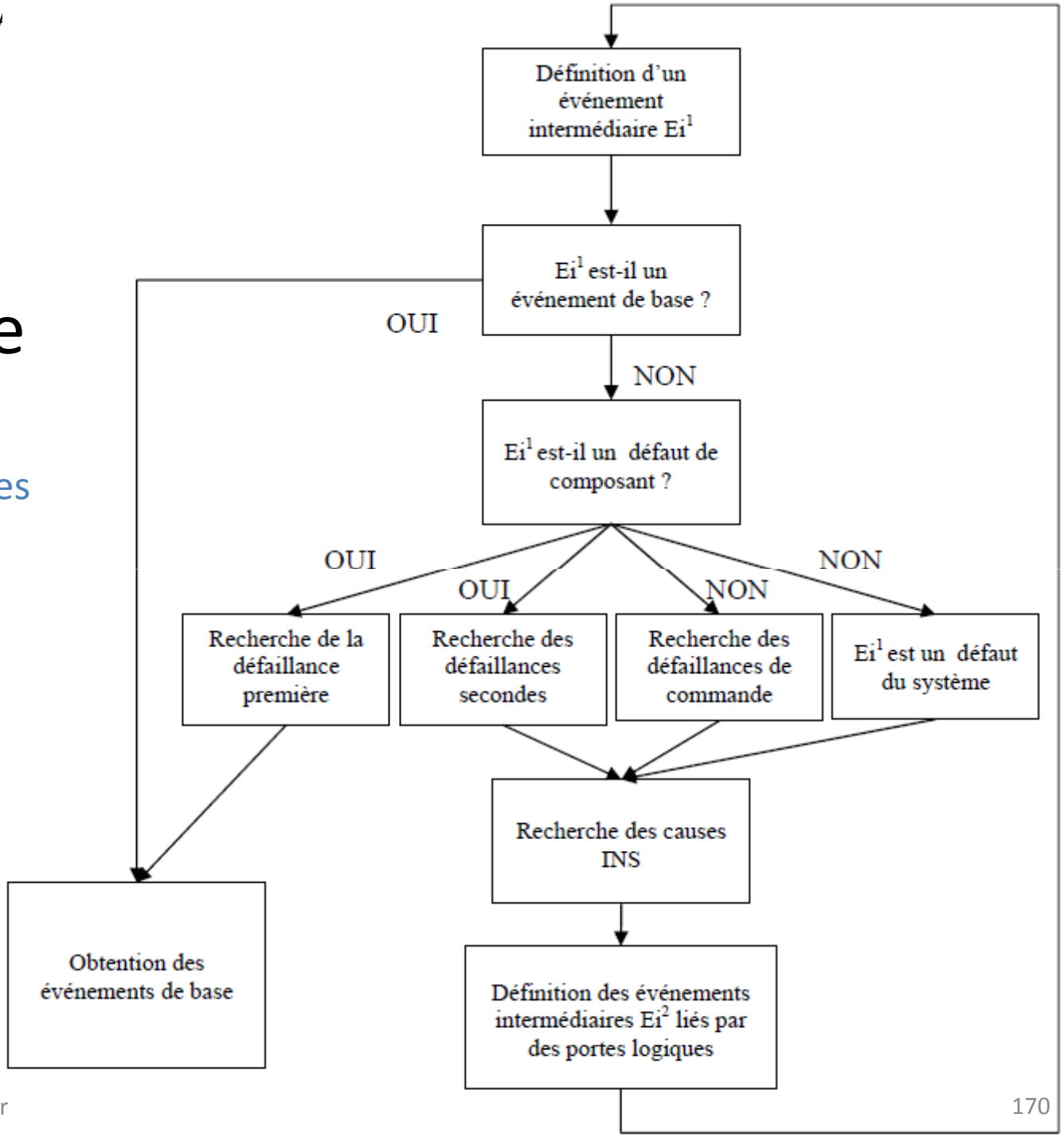
- Expliciter les faits et noter comment et quand ils se produisent
  - pour l'événement redouté
  - pour les événements intermédiaires
- Effectuer un classement des événements :
  - événement élémentaire représentant la défaillance d'un composant: défaillance première,
  - événements intermédiaires provenant d'une défaillance de composant. C'est par exemple un mode de défaillance !
  - événements intermédiaires provenant du système indépendamment du composant. C'est par exemple une configuration particulière.
- Rechercher les " causes immédiates " de l'apparition de chaque événement intermédiaire afin d'éviter l'oubli d'une branche
- Éviter les connexions directes entre portes

  elles sont en générale dues à une mauvaise compréhension du système ou une analyse trop superficielle.
- Supprimer les incohérences

  comme par exemple : un événement qui est à la fois cause et conséquence d'un autre événement.

AdD Démarche

Classification des événements intermédiaires



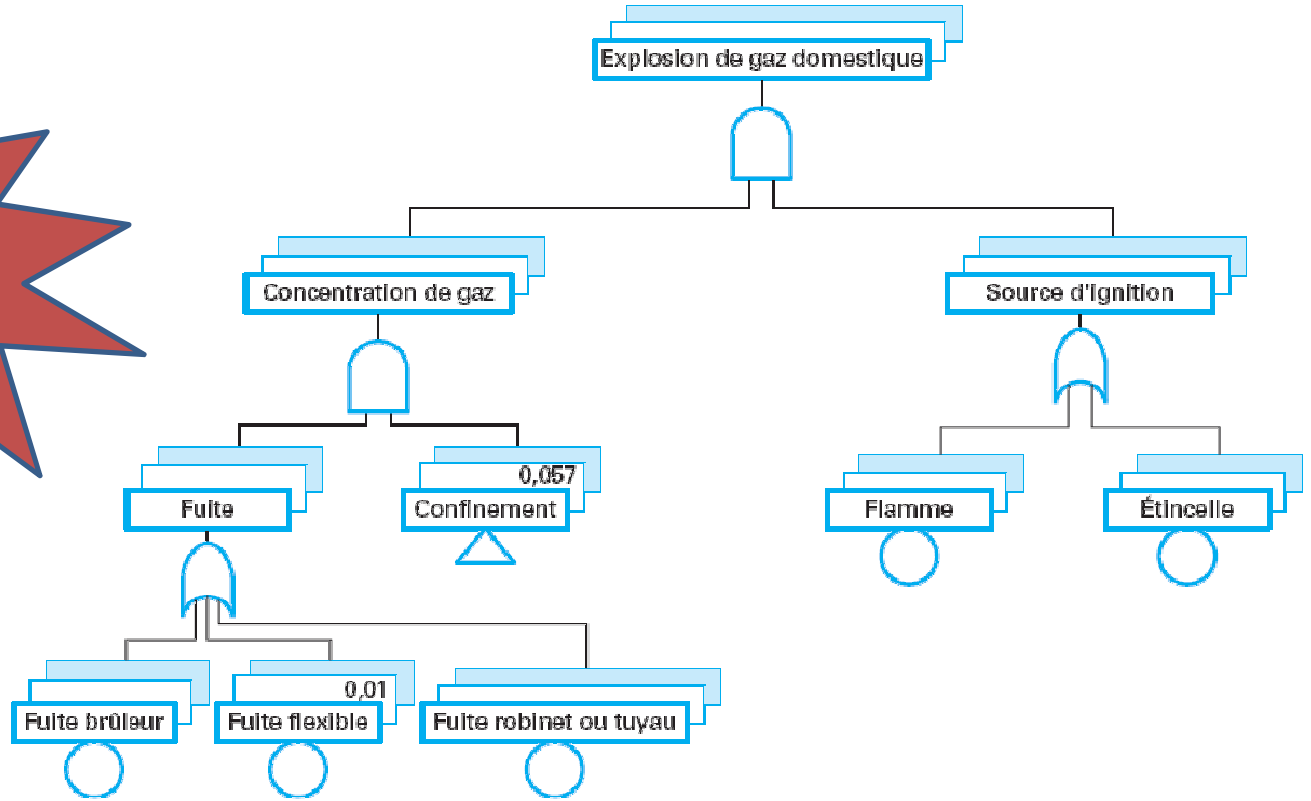
INS : Immédiat
Nécessaire et Suffisant

AdD Calcul de fiabilité

Si E résulte de A « ET » B indépendants, sa probabilité est le produit des probabilités de A et de B : $P(E) = P(A) \times P(B)$

Si E résulte de A « ou » B indépendants, sa probabilité est définie comme :
$P(E) = P(A \text{ ou } B) = P(A) + P(B) - P(A) \times P(B)$

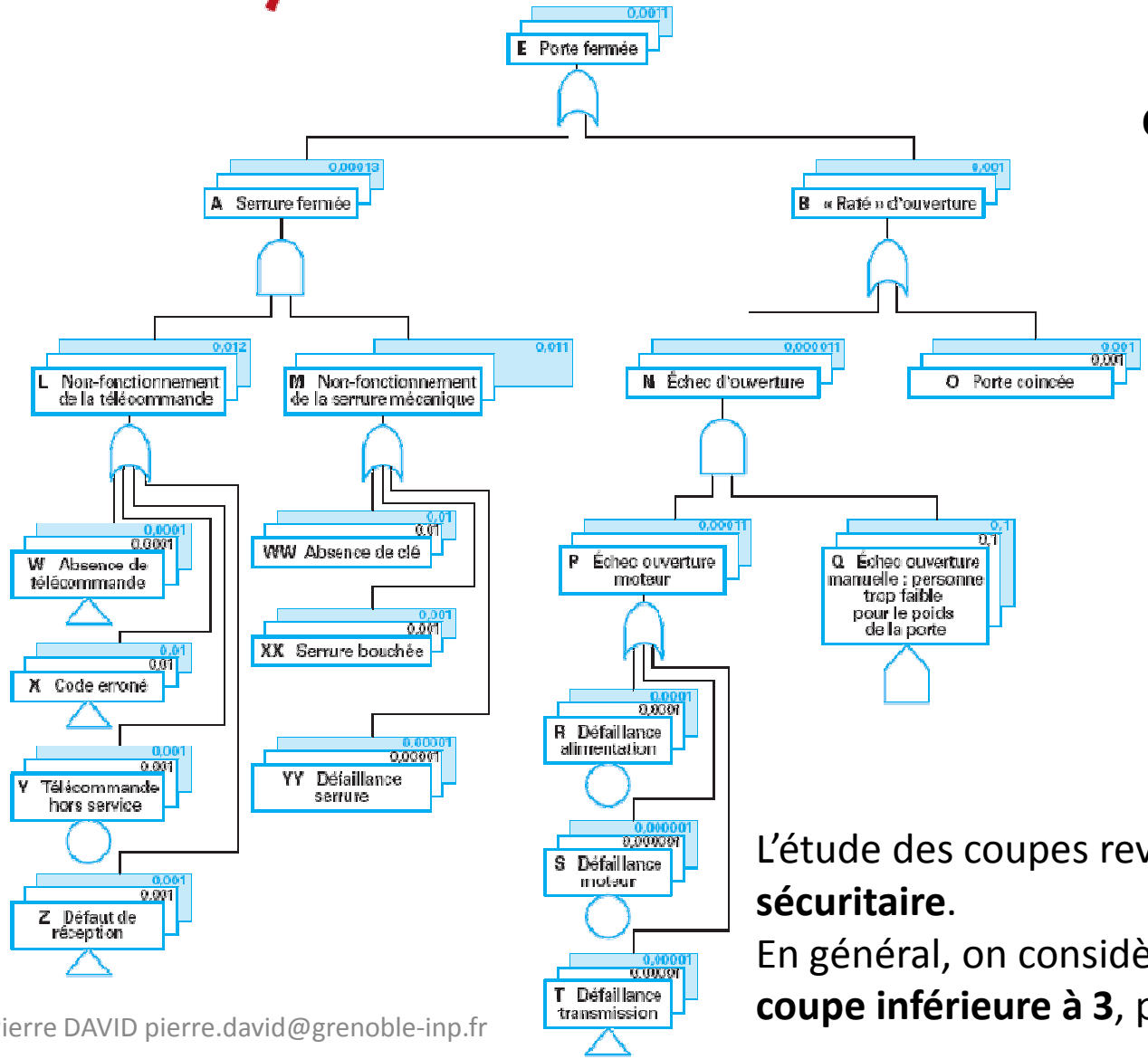
Les évts élémentaires doivent être indépendants



AdD Coupes

On appelle **coupe** d'un arbre un ensemble d'événements de base et de conditions suffisant pour produire l'événement-sommet.
Parmi ces coupes on appelle **coupe minimale** un ensemble d'événements de base ou conditions nécessaire et suffisant à produire l'événement-sommet. Si on retire à une coupe minimale un seul de ses éléments le reste ne suffit plus à produire l'événement-sommet.
On les trouve en descendant l'arbre, étape par étape de la manière suivante : la première étape donne un seul ensemble : {l'événement sommet}. C'est la coupe minimale triviale ;
une porte « ET » remplace dans un ensemble un événement par les événements dont il est la conjonction;
une porte « OU » divise l'ensemble en autant d'ensembles que la porte en introduit.
D'étape en étape, on arrive à des ensembles qui ne contiennent que des événements de base ou conditions
— éliminer les redondances d'événements dans une même coupe (il est inutile de citer plusieurs fois le même événement dans une coupe)
— éliminer les redondances de coupes (quand le même ensemble d'événements a été produit par plusieurs voies, il est inutile de le conserver en plusieurs exemplaires) ;
— éliminer les « super-coupes » qui en contiennent d'autres (quand un ensemble est strictement contenu dans un autre, il n'est utile de garder que le plus petit).

AdD Coupes exemple



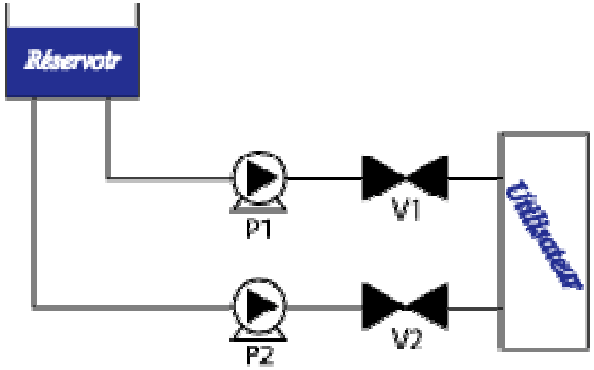
Coupes minimales :

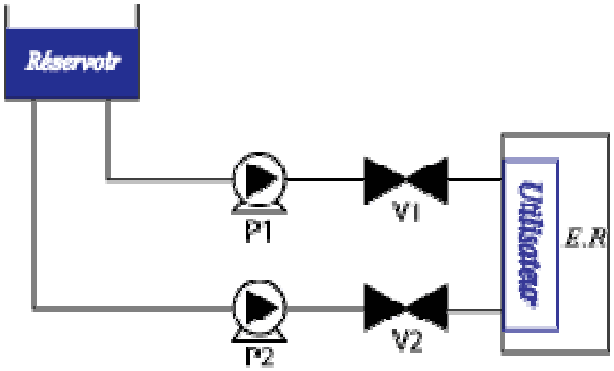
O
R, Q
S, Q
T, Q
W, WW
W, XX
W, YY
X, WW
X, XX
Y, WW
Y, XX
Y, YY
Z, WW
Z, XX
Z, YY

L'étude des coupes revêt un grand **intérêt sécuritaire**.

En général, on considère qu'il ne doit **pas** y avoir **de coupe inférieure à 3**, pour un système sécuritaire.

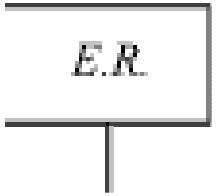
AdD exemple





L'événement redouté

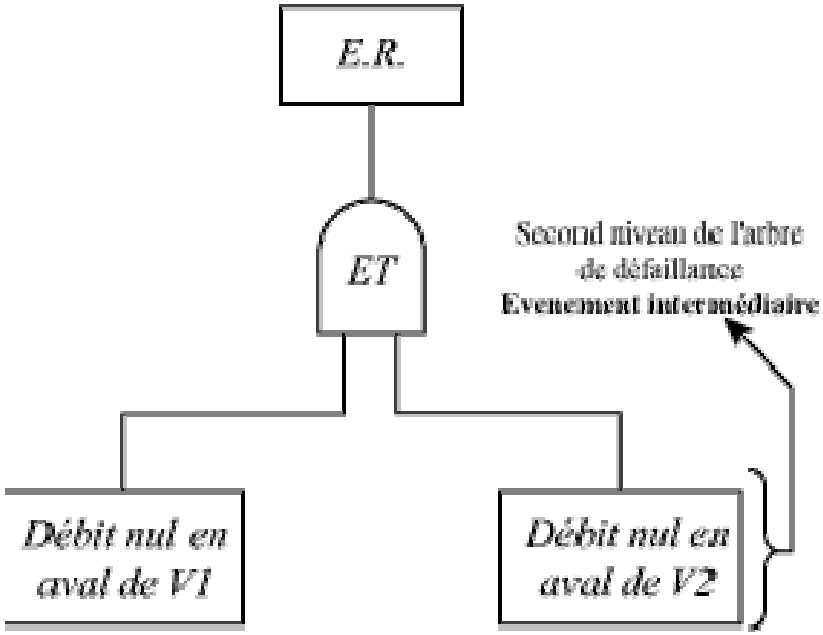
"Le système utilisateur est non alimenté" que l'on nomera ***ER***

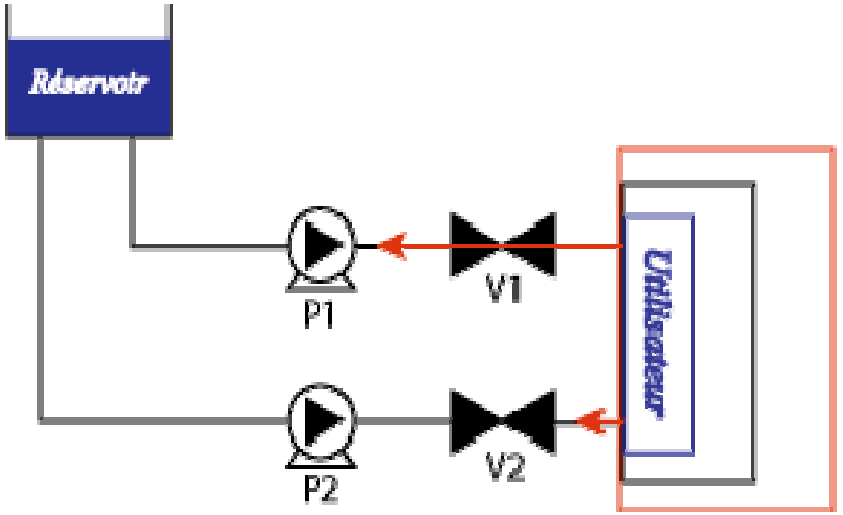


AdD exemple

cela se produit si :

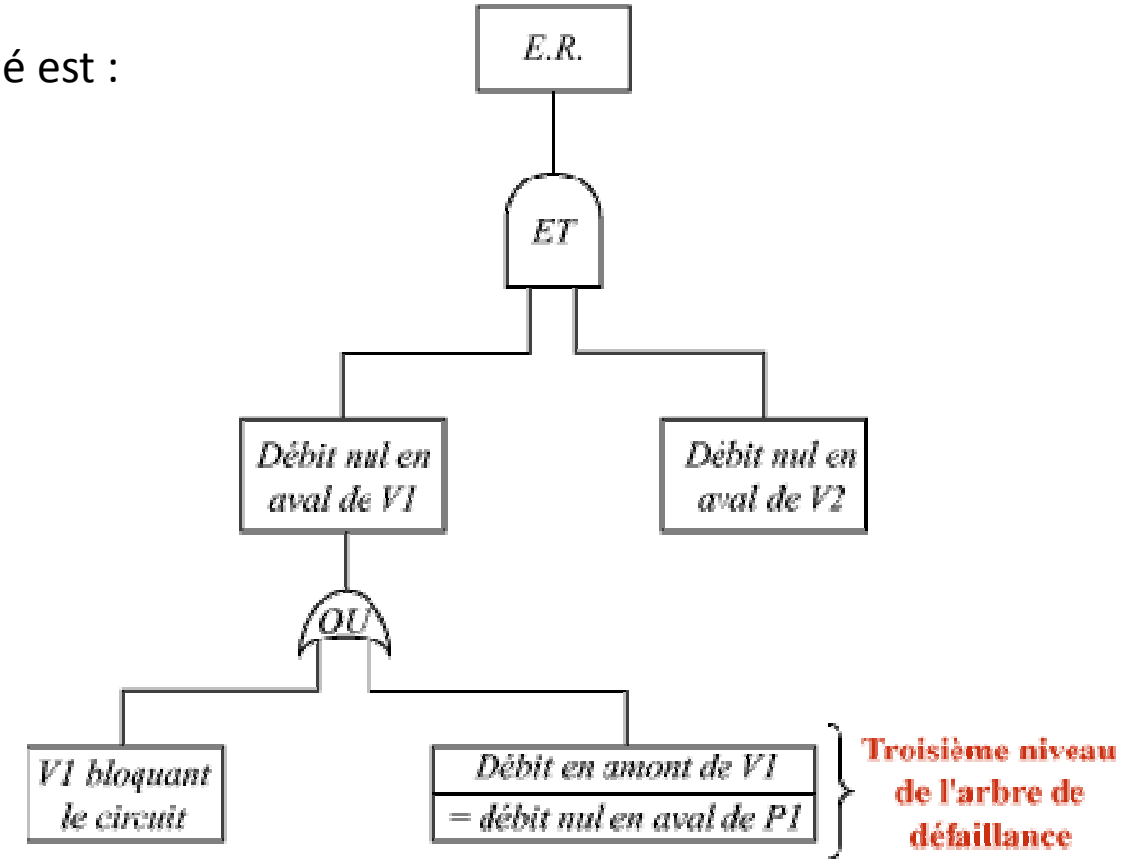
"Débit nul en aval de V1" ***ET*** *"Débit nul en aval de V2"*





AdD exemple

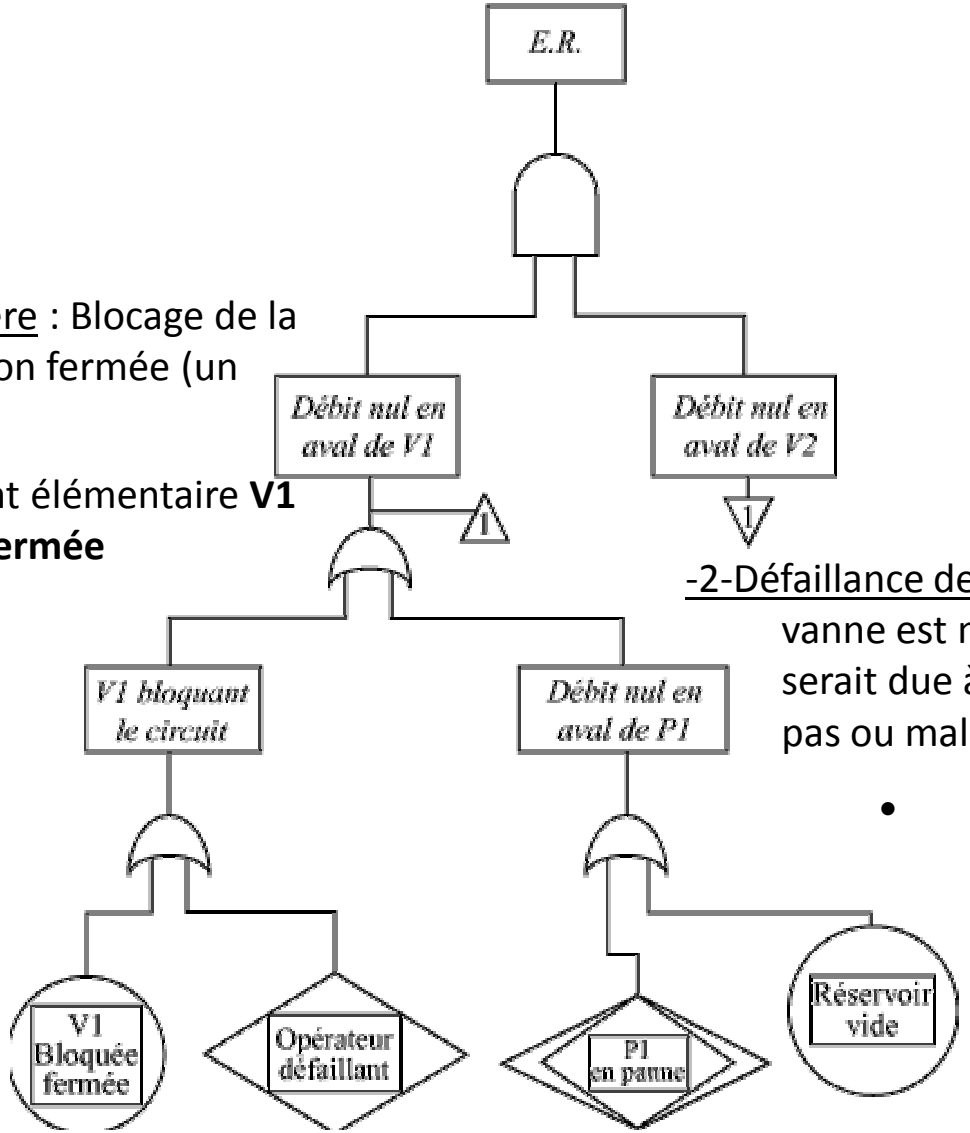
L'arbre associé est :



AdD exemple

-1-Défaillance première : Blocage de la vanne en position fermée (un vieillissement).

- événement élémentaire **V1 bloquée fermée**



-2-Défaillance de commande : Puisque la vanne est manuelle, cette défaillance serait due à l'opérateur qui n'aurait pas ou mal effectué l'ouverture de V1.

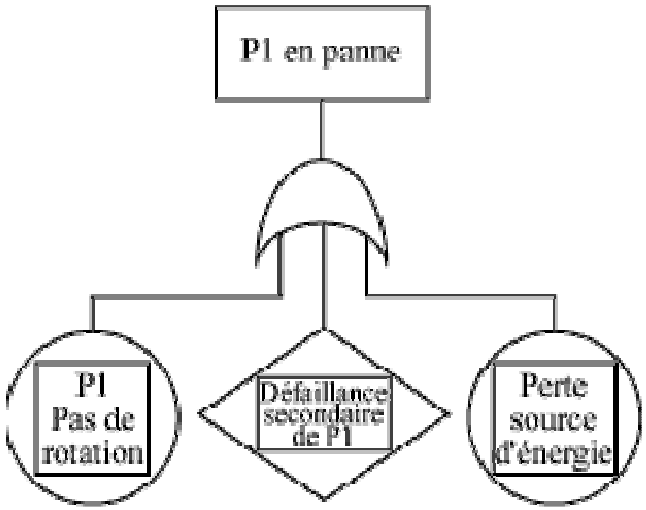
- événement élémentaire non développé **opérateur défaillant**

AdD exemple

1. <u>Défaillance première</u> : pas de rotation de la pompe.
   - événement élémentaire "P1 - Pas de rotation"

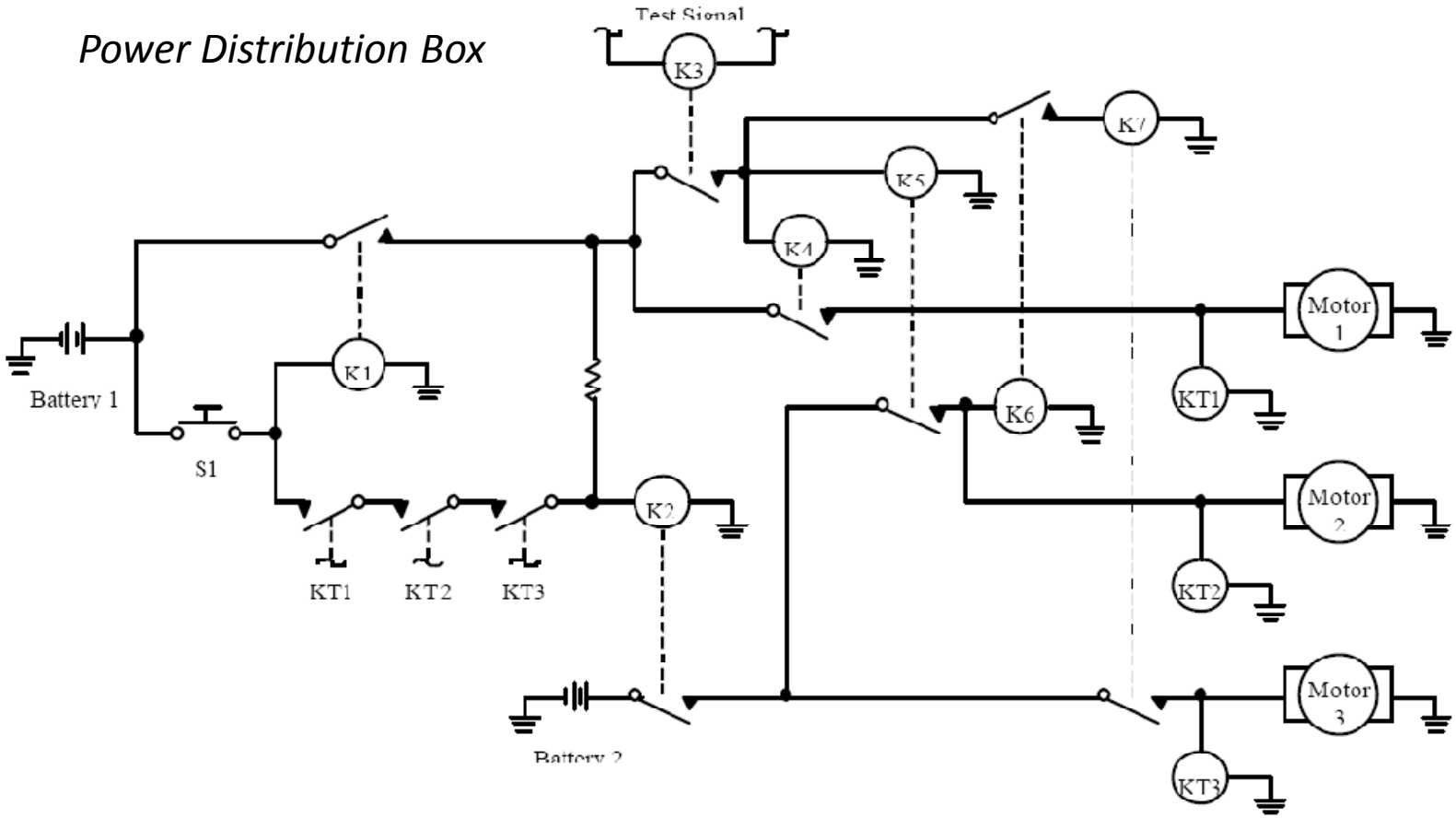
2. <u>Défaillance secondaire</u> : défaillance due à une cause extérieure ou à une utilisation particulière. Ici un corps étranger qui obstrue la pompe.
   - événement élémentaire non développé "Défaillance secondaire de P1"

3. <u>Défaillance de commande</u> : puisque la pompe est électrique, cette défaillance serait due à la perte de la source d'énergie.
   - événement élémentaire "Perte source d'énergie“



Exemple de déduction

Power Distribution Box



Order 2:

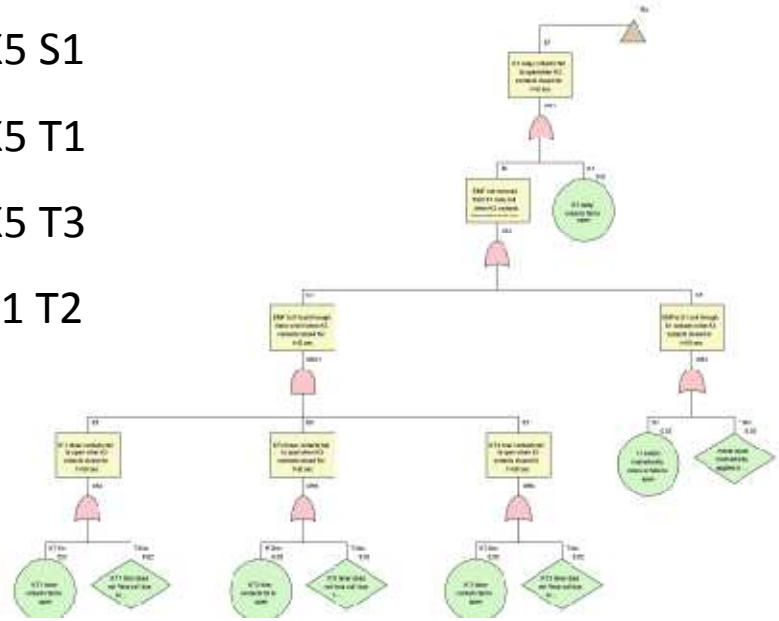
1) K1 K5
2) K1 T2
3) K2 K5
4) K5 S1
5) K5 T1
6) K5 T3
7) S1 T2

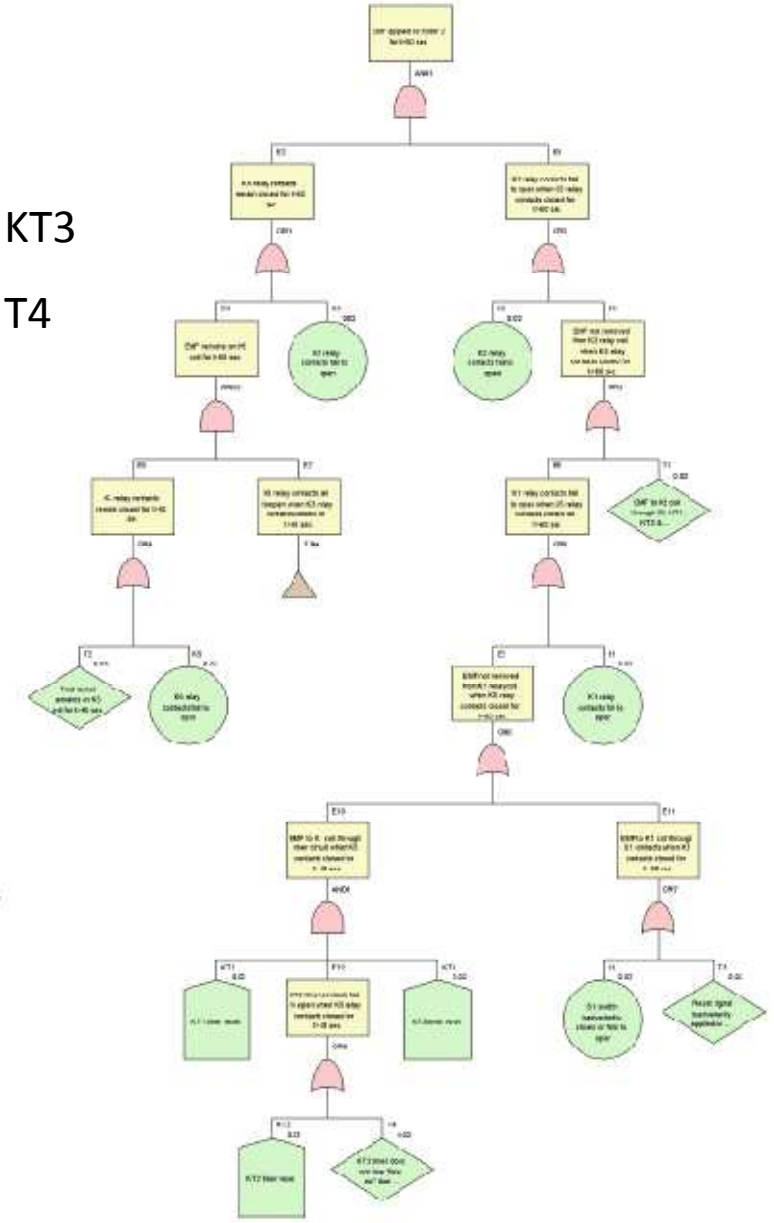
Order 3:

1) K2 T1inc T2
2) T1 T1inc T2
3) T1inc T2 T3

Order 4:

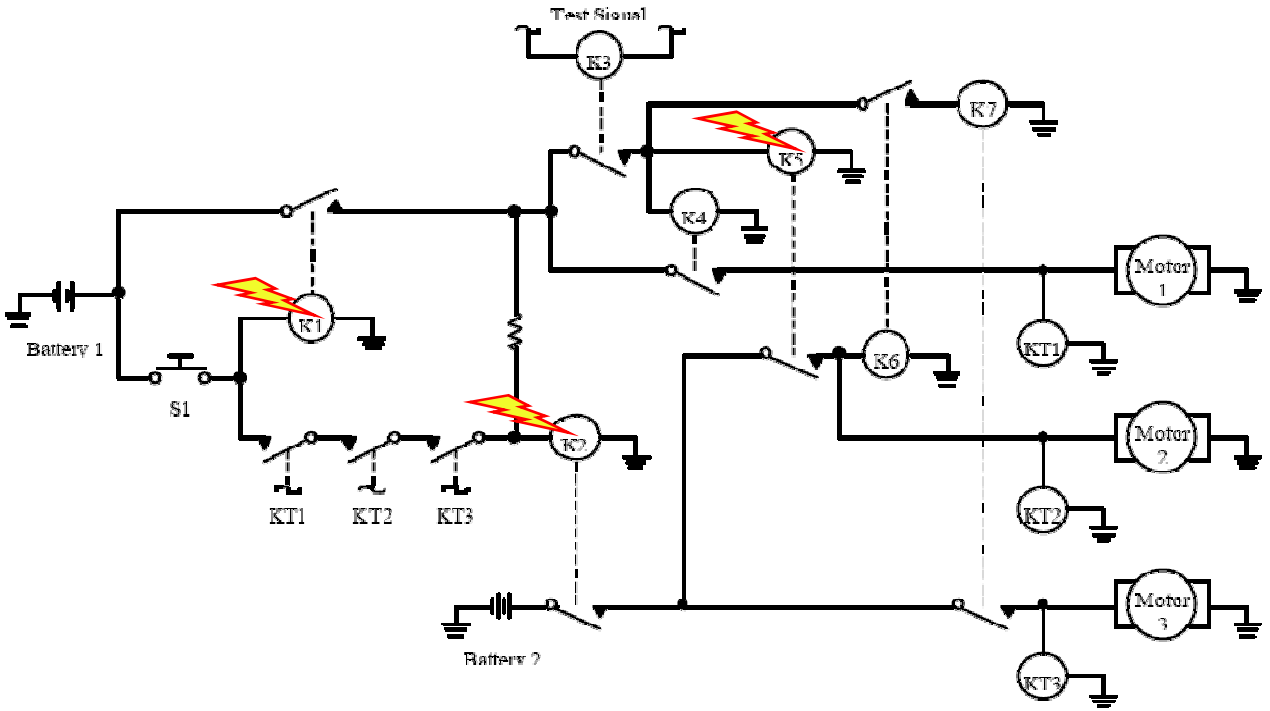
1) K5 KT1 KT2 KT3
2) K5 KT1 KT3 T4





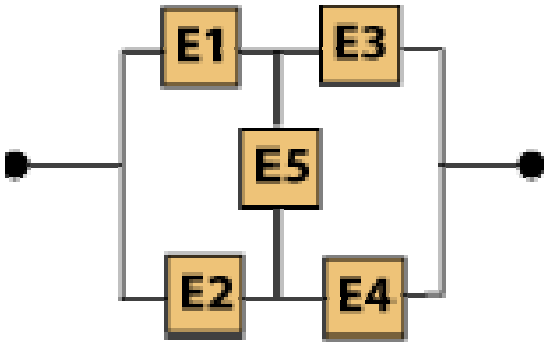
1 K1 K5	4.000000E-004
2 K1 T2	4.000000E-004
3 K2 K5	4.000000E-004
4 K5 S1	4.000000E-004
5 K5 T1	4.000000E-004
6 K5 T3	4.000000E-004
7 S1 T2	4.000000E-004
8 K2 T1inc T2	8.000000E-006
9 T1 T1inc T2	8.000000E-006
10 T1inc T2 T3	8.000000E-006
11 K5 KT1 KT2 KT3	1.600000E-007
12 K5 KT1 KT3 T4	1.600000E-007
13 K2 KT1inc KT2inc KT3inc T2	3.200000E-009

Event	Failure contrib.	Importance
K1	8.000000E-004	29.41%
K2	4.080256E-004	15.00%
K5	2.000320E-003	73.53%
KT1	3.264205E-007	0.01%
KT1inc	3.841023E-008	0.00%
KT2	1.632102E-007	0.01%
KT2inc	3.841023E-008	0.00%
KT3	3.264205E-007	0.01%



Exercice

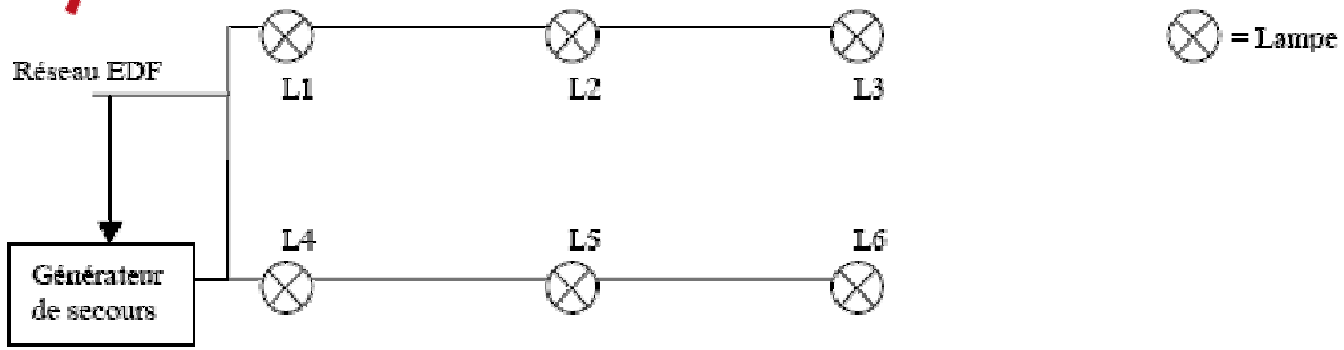
1) Établir l'arbre de défaillance du système suivant :



2) Rechercher les coupes minimales.

Exercice

Exercice



Soit une salle de sport dont le schéma de câblage de l'éclairage peut être représenté par le schéma ci-dessus. La salle de sport est éclairée par 2 rampes de lampe. Chaque rampe possède 3 lampes montées en série.

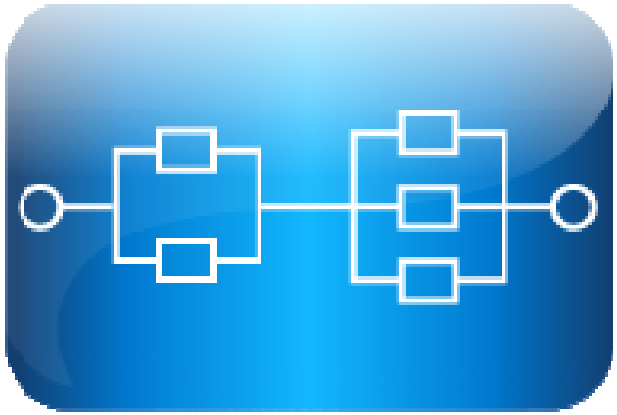
L'événement redouté est « Salle de sport plongée dans le noir », sachant qu'il faut au minimum 3 lampes pour que la salle ne soit pas plongée dans le noir.

Voici les données dont vous disposez :
Le réseau EDF tombe en panne en moyenne 1 fois par mois.
Le taux de défaillance d'une lampe est de 4 10^{-4} /heure (Loi expo.)
La probabilité de défaillance à la sollicitation du générateur de secours est de 10^{-2}.

Vous devez :
- Réaliser l'analyse qualitative de cet événement redouté en utilisant la méthode des arbres de défaillance.
- Écrire l'équation de l'arbre régissant l'événement redouté
- Déterminer les coupes minimales de l'arbre
- Calculer la probabilité de l'événement redouté pour une séance de sport d'une durée de 2 heures (on suppose qu'au début de la séance, toutes les lampes sont allumées et que le réseau EDF n'est pas défaillant).

Exercice

Exercice



BLOC DIAGRAMME DE FIABILITÉ

Objectifs

- Disposer d'une modélisation simple pour analyser et calculer la fiabilité d'un système.
- Mise en évidence des chemins de succès et coupes minimales.
- Calculer la fiabilité d'un équipement.
- Connus sous les noms de: Bloc Diagramme de Fiabilité (BDF), diagramme de fiabilité, Reliability Block Diagram (RDB).
- Mais quelques limitations : systèmes non réparables, pas de défaillances simultanées.

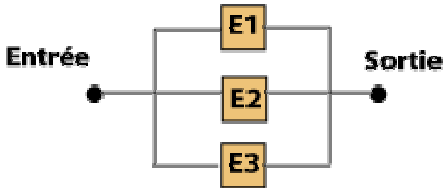
BDF

Un diagramme de fiabilité est un modèle qui permet de représenter le comportement d'un système sous une vue fonctionnelle.

La méthode d'analyse par diagramme de fiabilité repose sur :
- Une décomposition du système en sous-systèmes, chaque entité est modélisée par des blocs : Les sous-systèmes, Les fonctions, Les composants.
- Ces blocs modélisent leur participation au succès de la mission.

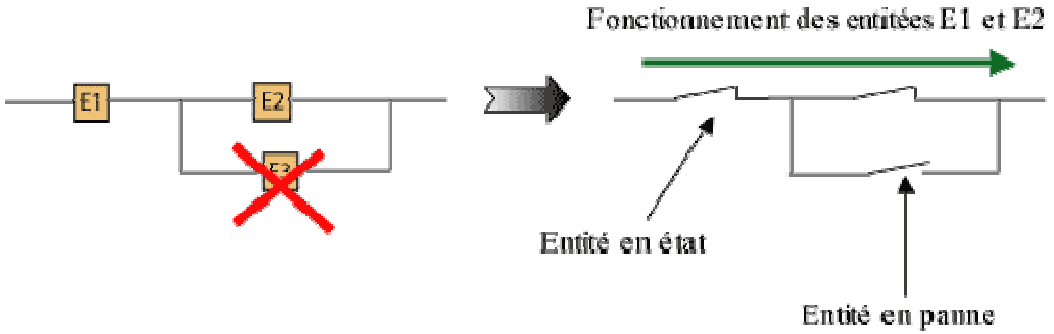
On décompose le système en composant reliés en série,

ou en parallèle .



BDF: chemin de succès

Un bloc est considéré comme un interrupteur fermé lorsque l'entité est en état de fonctionnement ou un interrupteur ouvert lorsque l'entité est en état de panne.
Si le "signal" qui entre dans le diagramme en ressort, le système est déclaré en état de fonctionnement et la mission est réussie, sinon le système est en panne.



Un Lien ou chemin de succès est un ensemble d'entités dont le fonctionnement assure le succès de la mission du système.

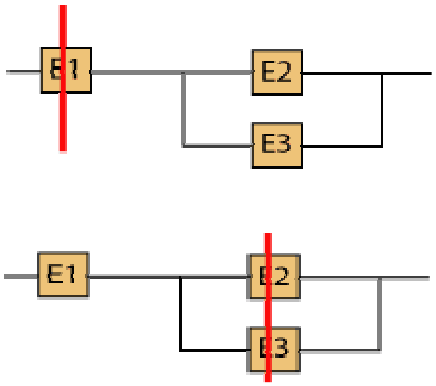
Un chemin de succès minimal est une des plus petites combinaisons d'entités qui lorsqu'elles sont en fonction permettent d'assurer la fonction requise pour le système.

BDF: coupes

Une coupe est un ensemble de blocs ou d ’entités qui conduit à la panne ou la non réussite de la mission du système si ces blocs ne peuvent plus réaliser leurs fonctions (ex : défaillance de composant).

Une coupe est un ensemble d ’entités qui apparaissent dans tous les chemins de succès. Si l ’ensemble des entités d ’une coupe est en panne alors aucun chemin de succès ne permet de conduire à la réussite de la mission du système.

Une coupe minimale est la plus petite combinaison d ’entités entraînant l ’échec de la mission du système (elle ne contient aucune autre coupe).



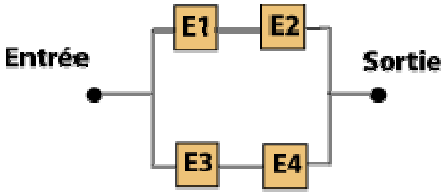
Motifs élémentaires

Le diagramme série :
La panne de l ’un ou de l ’autre des éléments entraîne la panne du système
Chemins de succès ou liens minimaux :
E1, E2

Coupes minimales :
E1
E2

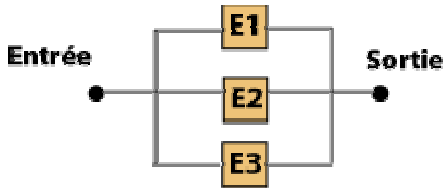
Le diagramme série-parallèle
Chemins de succès ou liens minimaux :
E1, E2
E3, E4

Coupes minimales :
E1, E3
E1, E4 E2, E3
E2, E4



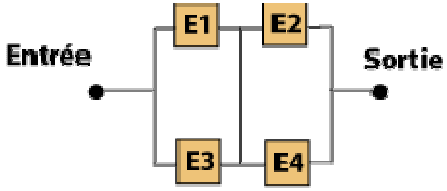
Le diagramme parallèle (ou redondance active)
La panne de tous les éléments entraîne la panne du système. Si un seul
des éléments fonctionne alors il conduit au fonctionnement du système.
Chemins de succès ou liens minimaux :
E1
E2
E3

Coupes minimales :
E1, E2, E3



Le diagramme parallèle-série
Chemins de succès ou liens minimaux :
E1, E2
E1, E4 E2, E3
E3, E4

Coupes minimales :
E1, E3
E2, E4



Calculs de probabilité

Blocs en Série

n composants indépendants en série.

E_i le composant i fonctionne.

$R_s = P(E_1 \cap E_2 \cap \ldots \cap E_n)$

A cause de l'indépendance :

$$P(E_1 \cap E_2 \cap \ldots \cap E_n) = \prod_{i=1}^{n} P(E_i)$$

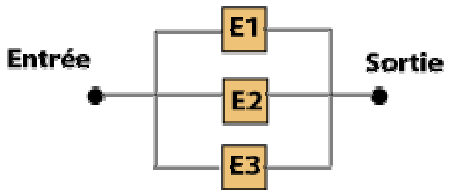
En notant $R_i = P(E_i)$, on obtient :

$$R_s = \prod_{i=1}^{n} R_i$$

On remarque que $R_s < min(R_i)$. Le système est moins fiable que sa composante la moins fiable.

Calculs de probabilité

Blocs en Parallèle



n composants indépendants en prallèle.

E_i le composant i fonctionne.

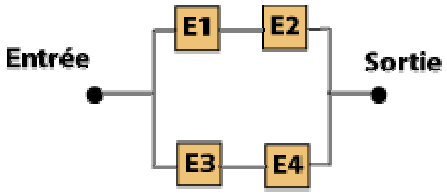
$R_s = P(E_1 \cup E_2 \cup \ldots \cup E_n)$

Le système est en panne si tous les composants sont en panne :

$$1 - R_p = \prod_{i=1}^{n} (1 - R_i)$$

Calculs de probabilité

Système Série-Parallèle



Décomposition récursive : un système série-parallèle (SP) est soit :

- un bloc isolé
- plusieurs sous-systèmes SP en série
- plusieurs sous-systèmes SP en parallèle

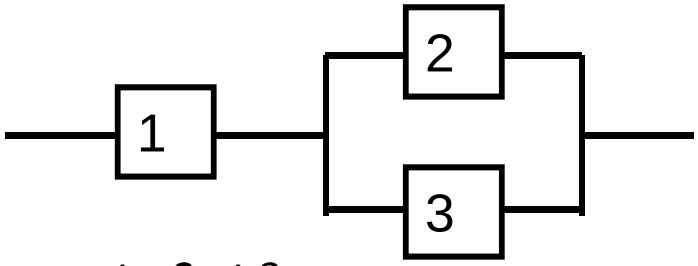
Utilise la décomposition récursive de la construction pour obtenir la fiabilité.

Exemple simple : n étages en série, chaque étage composé de m composants en parallèle tous identiques :

$$R_{sp} = (1 - (1 - R)^m)^n$$

Exemple

Exemple: Calculer la fiabilité et la probabilité de défaillance du système suivant.
Supposons les probabilités de défaillance suivantes
$Q_1 = 0.01$, $Q_2 = 0.02$ and $Q_3 = 0.03$.



Solution:

- Combinons en parallèle les composants 2 et 3
- La probabilité de défaillance est

$$Q_{2,3} = Q_2 \cap Q_3 = Q_2 \cdot Q_3$$

- La fiabilité est

$$R_{2,3} = R_2 \cup R_3$$
$$= R_2 + R_3 - R_2 \cdot R_3$$

Exemple

Puis combinons le composant 1 et le sous système(2,3) en série.

La probabilité de défaillance pour le système est :

$$\begin{aligned} Q_{SYS} &= Q_1 \cup Q_{2,3} \\ &= Q_1 + Q_{2,3} - Q_1 \cdot Q_{2,3} \\ &= Q_1 + Q_2 \cdot Q_3 - Q_1 \cdot Q_2 \cdot Q_3 \end{aligned}$$

$$Q_{SYS} = (0.01) + (0.02)(0.03) - (0.01)(0.02)(0.03) = 0.010594$$

Sa fiabilité est :

$$\begin{aligned} R_{SYS} &= R_1 \cap R_{2,3} \\ &= R_1 \cdot R_{2,3} \\ &= R_1(R_2 + R_3 - R_2 \cdot R_3) \\ &= R_1 \cdot R_2 + R_1 \cdot R_3 - R_1 \cdot R_2 \cdot R_3 \end{aligned}$$

$$R_{SYS} = (1-0.01)(1-0.02) + (1-0.01)(1-0.03) - (1-0.01)(1-0.02)(1-0.03)$$

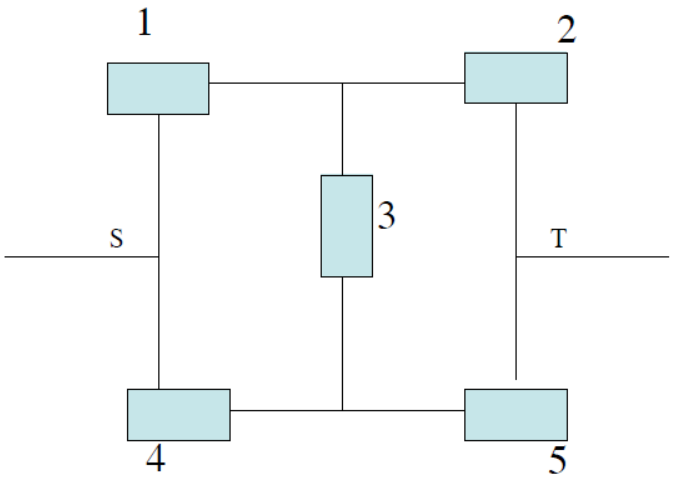
Ce qui est cohérent avec $R_{SYS} = 1 - Q_{SYS}$ $= 0.989406$

Calculs de probabilité

Systèmes NON Série-Parallèles

- Si on ne peut plus utiliser la décomposition SP, on peut enumérer et construire la table Booléenne.

réseau avec bridge :



Calculs de probabilité

Ex: Bridge

Examiner tous les cas UP et DOWN pour tous les composants

Dans chaque cas, évaluer si le système est UP ou DOWN

Calculer les probabilités de chaque cas (facile, c'est le produit des probas élémentaires à cause de l'hypothèse d'indépendance).

Exemple : Si $E1 = E2 = E4 = 1$ et $E3 = E5 = 0$ le système est UP et la probabilité de cette configuration est $R_1 R_2 R_4 (1 - R_3)(1 - R_5)$.

Sommer les probabilités que le système soit UP

Calculs de probabilité

Ex: Bridge

1	2	3	4	5	Bridge	Probability
0	0	0	0	0	0	
0	0	0	0	1	0	
0	0	0	1	0	0	
0	0	0	1	1	1	(1-R1)(1-R2)(1-R3)R4R5
0	0	1	0	0	0	
0	0	1	0	1	0	
0	0	1	1	0	0	
0	0	1	1	1	1	(1-R1)(1-R2)R3R4R5
0	1	0	0	0	0	
0	1	0	0	1	0	
0	1	0	1	0	0	
0	1	0	1	1	1	(1-R1)R2(1-R3)R4R5
0	1	1	0	0	0	
0	1	1	0	1	0	
0	1	1	1	0	1	(1-R1)R2R3R4(1-R5)
0	1	1	1	1	1	(1-R1)R2R3R4R5

Calculs de probabilité

1	0	0	0	0	0	
1	0	0	0	1	0	
1	0	0	1	0	0	
1	0	0	1	1	1	R1(1-R2)(1-R3)R4R5
1	0	1	0	0	0	
1	0	1	0	1	1	R1(1-R2)R3(1-R4)R5
1	0	1	1	0	0	
1	0	1	1	1	1	R1(1-R2)R3R4R5
1	1	0	0	0	1	R1R2(1-R3)(1-R4)(1-R5)
1	1	0	0	1	1	R1R2(1-R3)(1-R4)R5
1	1	0	1	0	1	R1R2(1-R3)R4(1-R5)
1	1	0	1	1	1	R1R2(1-R3)R4R5
1	1	1	0	0	1	R1R2R3(1-R4)(1-R5)
1	1	1	0	1	1	R1R2R3(1-R4)R5
1	1	1	1	0	1	R1R2R3R4(1-R5)
1	1	1	1	1	1	R1R2R3R4R5

En agrégeant la table précédente et en factorisant on trouve que :

$$\begin{aligned} R_{bridge} &= R_1 R_2 \\ &+ R_1(1-R_2)(R_4R_5 + R_3(1-R_4)R_5) \\ &+ (1-R_1)R_4(R_5 + (1-R_5)R_2R_3) \end{aligned}$$

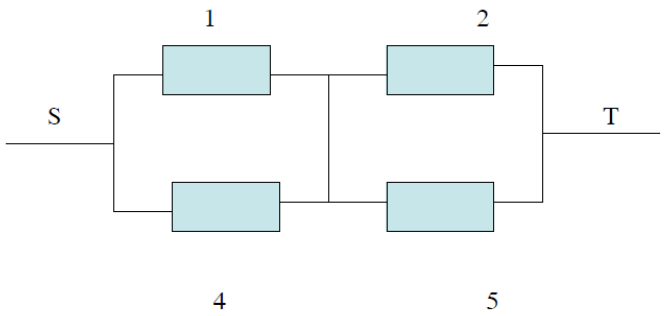
Calculs de probabilité

Mais il faut considérer les 2^n configurations si il y a n objets.

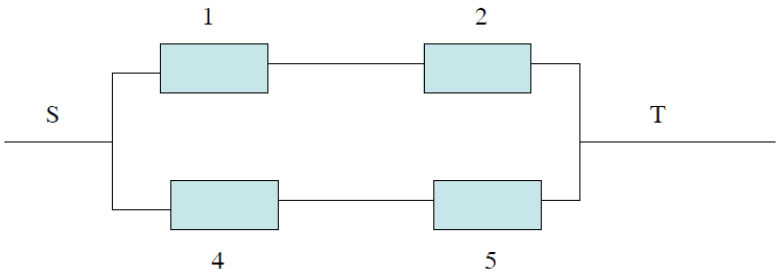
On conditionne sur le l'état d'un composant (ou de plusieurs composants) pour se ramener à des structures déjà étudiées ou faciles (SP)

Sur l'exemple du bridge, on conditionne sur l'état du bloc 3.

3 fonctionne



3 ne fonctionne pas



Calculs de probabilité

Si le composant 3 est DOWN, on obtient un modèle SP

Si le composant 3 est UP, on obtient également un modèle SP

On applique le théorème de conditionnement et les formules pour les modèles série-parallèles.

$$R_{3down} = 1 - (1 - R_1 R_2)(1 - R_4 R_5)$$

$$R_{3up} = (1 - (1 - R_1)(1 - R_2))(1 - (1 - R_4)(1 - R_5))$$

On applique le théorème de conditionnement

$$R_{bridge} = R_3 R_{3up} + (1 - R_3) R_{3down}$$

Calculs de probabilité

Systèmes K parmi N

Système consistant en N composants indépendants.

Le système est UP quand K ou plus de ces composants sont UP.

Cas Identique : tous les composants ont le même taux de panne et de réparation.

Cas Non Identique : Les composants ont des taux de panne et de réparation distincts par composant.

Avec sous composants identiques

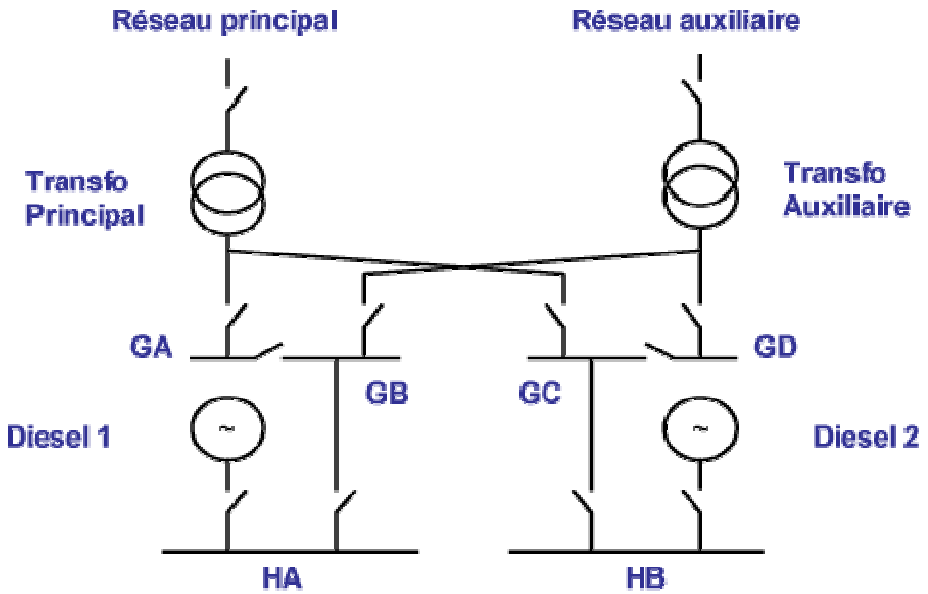
Soit R la fiabilité d'un composant.

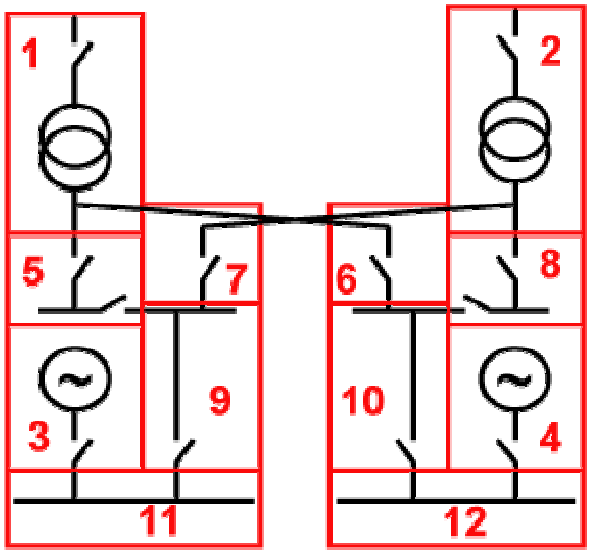
On additionne les probabilités de toutes les configurations avec au moins K composants opérationnels.

$$R(K,N) = \sum_{j=K}^{N} R^j (1-R)^{N-j} \frac{N!}{j!(N-j)!}$$

Exercice

Une alimentation électrique fonctionne selon le schéma suivant :
L'alimentation électrique fonctionne correctement si l'un des deux jeux de barre HA ou HB est sous tension.
Le système peut être décomposé en 12 macro-éléments représentés sur le schéma ci-joint.





1) Déterminer le diagramme de fiabilité de l'alimentation électrique. Puis en déduire les chemins de succès et les coupes minimales.

2) Les deux réseaux (principal et auxiliaire) peuvent tomber en panne ensemble par suite d'un orage par exemple.
Ceci est une panne de mode commun qui nécessite la représentation d'un élément fictif n°13.
Comment sont modifiés le diagramme de fiabilité, les chemins de succès et les coupes minimales ?

Exercice

Exercice

Bibliographie

- Cours académiques :
  - Vincent IDASIAK – ENSI de Bourges
  - David DELAHAYE – CNAM
  - Claire PAGETTI – CERT/ONERA
  - Jean-François AUBRY – INP Nancy Lorraine
  - Thierry VERDEL – Mines de Nancy
  - Samuel BASSETTO – INP Grenoble
  - Franck DECOBECQ – DGA/ENSI de Bourges
- Techniques de l'Ingénieur :
  - Yves MORTUREUX – Analyse Préliminaire des Risques
  - Marc GIRAUD – Sûreté de Fonctionnement des systèmes
  - Gilles ZWINGELSTEIN – Sûreté de Fonctionnement des systèmes Industriels complexes
- Ouvrages :
  - Alain VILLEMEUR – Sûreté de Fonctionnement des systèmes industriels – 1988
  - Jean-Claude LAPRIE – Sûreté de fonctionnement des systèmes informatiques – 1989
  - Georges-Yves KERVERN – Eléments fondamentaux des cyndiniques – 1995
- Normes :
  - CEI 50191
  - IEC 61508