

LO22 / AI20

Walter SCHÖN

Rappel des sujets traités

2

- **Sûreté de fonctionnement** : concepts généraux, application aux systèmes informatiques : LO22 et AI20
- Vérification et Validation : LO22 seulement (sujet de AI03 pour les apprentis)
- Méthodes formelles : LO22 et AI20

Plan de la partie Sûreté de Fonctionnement

3

- Sûreté de fonctionnement
 - Terminologie et notions de base
 - Méthodes d'analyse prévisionnelle de la sûreté de fonctionnement (prévision des fautes) : aspect qualitatif
 - Méthodes d'analyse prévisionnelle de la sûreté de fonctionnement (prévision des fautes) : aspect quantitatif
 - Méthodes de conception d'architectures informatiques sûres de fonctionnement (tolérance aux fautes)
 - Élimination des fautes

Sûreté de Fonctionnement des systèmes informatiques

Terminologie et notions de base

Sûreté de fonctionnement : définitions

5

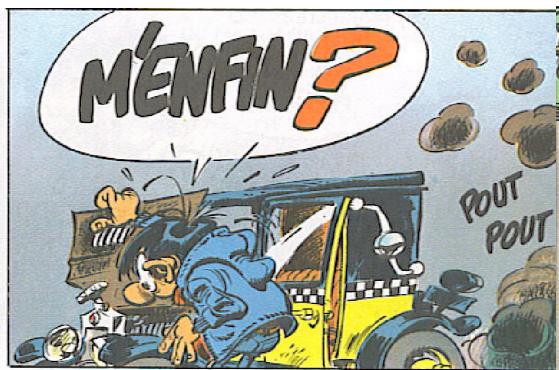
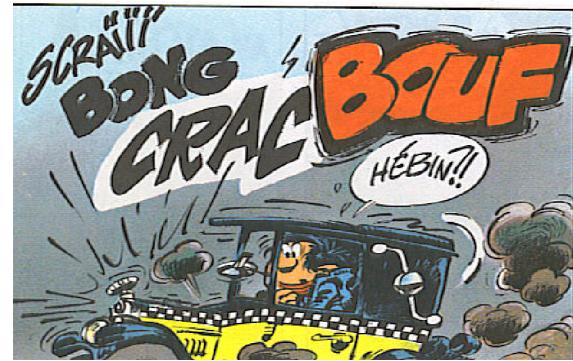
Sûreté de fonctionnement : propriété qui permet à ses utilisateurs de placer une *confiance* justifiée dans le service délivré par un système.

Attributs de la Sûreté de fonctionnement : **FDMS** :

- **Fiabilité** : *Continuité* du service
- **Disponibilité** : Fait d'être *prêt à l'utilisation*
- **Maintenabilité** : Aptitude aux *réparations*
- **Sécurité** : Aptitude à éviter de provoquer des événements *catastrophiques*.

Fiabilité

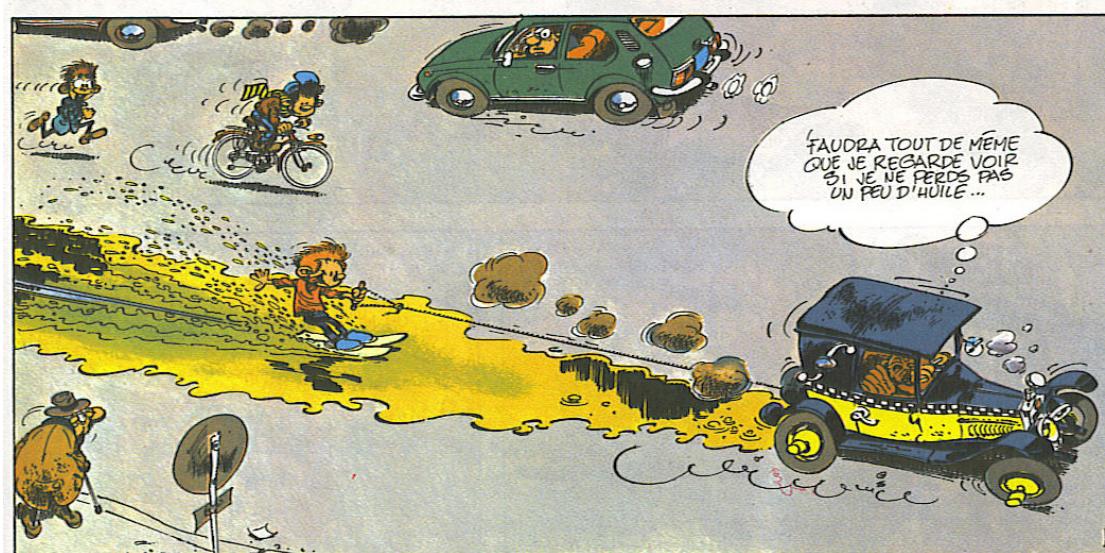
6



Fiabilité

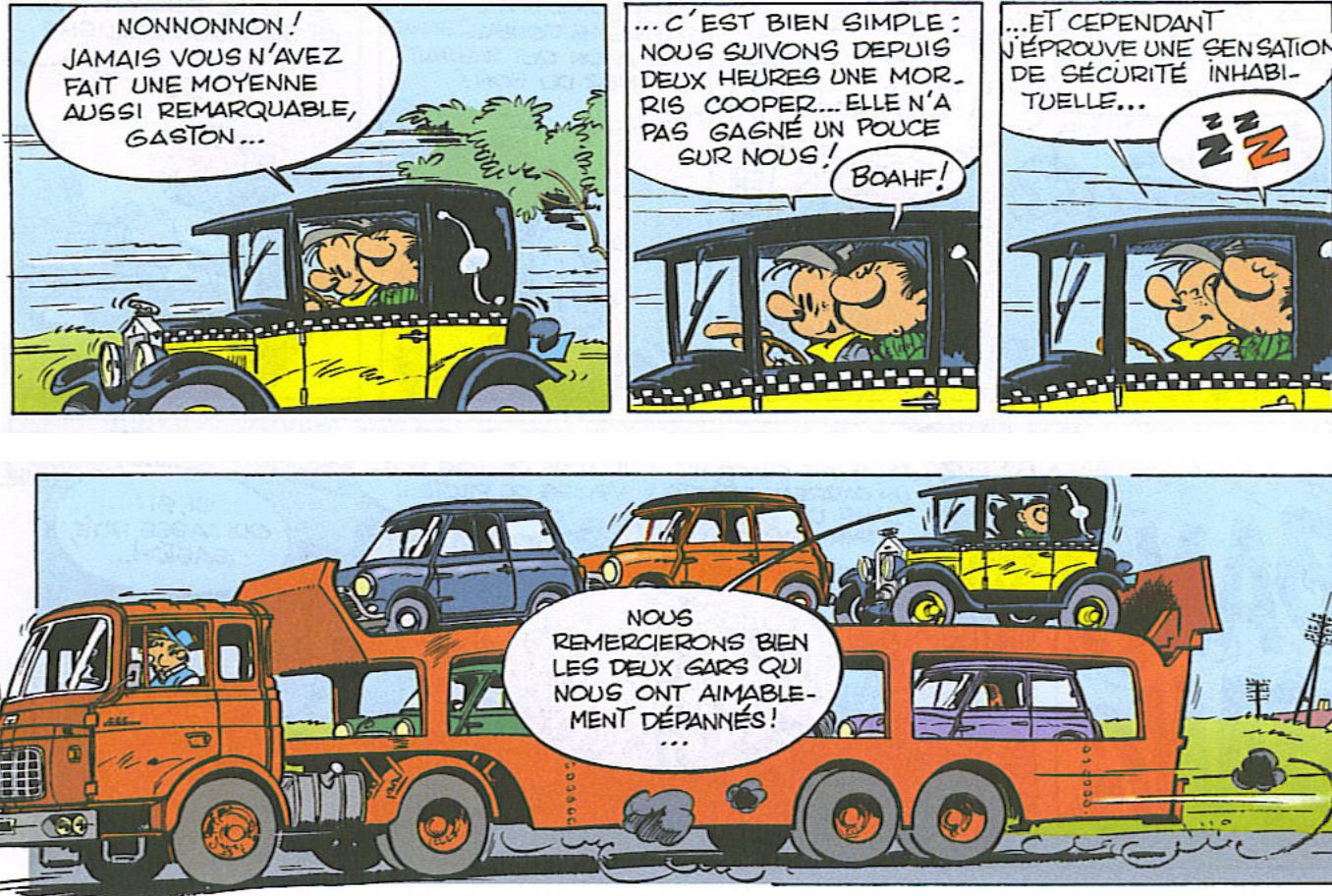
7

Toutes défaillances prises en compte :



Disponibilité

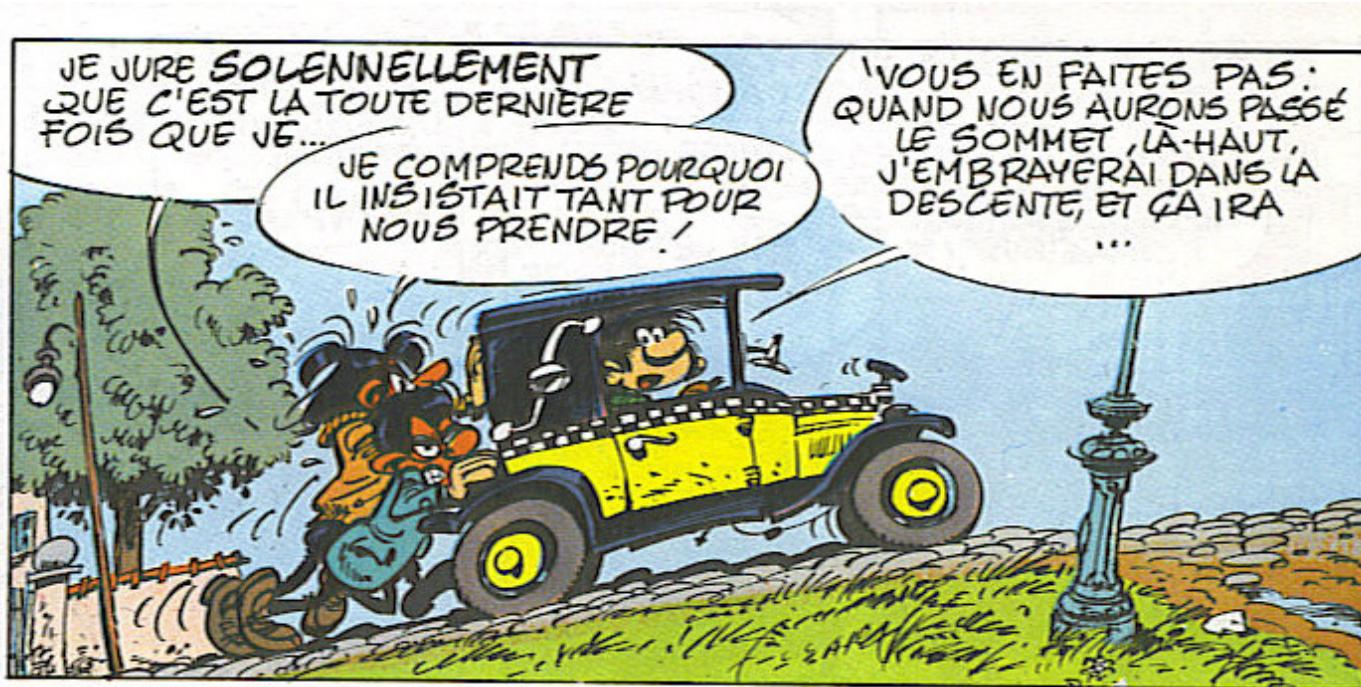
8



Disponibilité

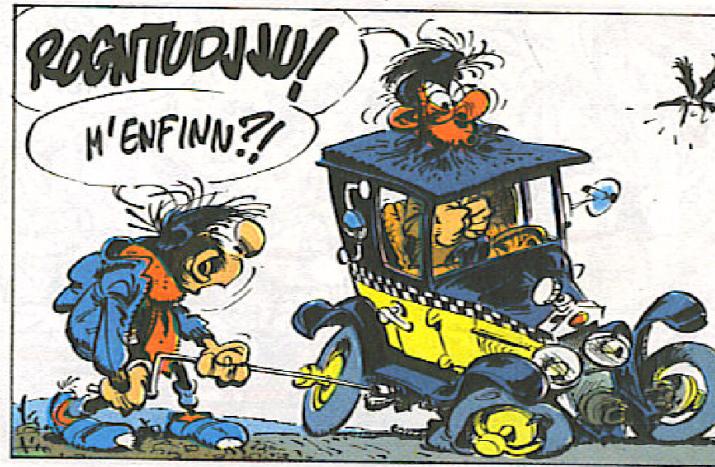
9

- Restriction aux défaillances perturbantes :



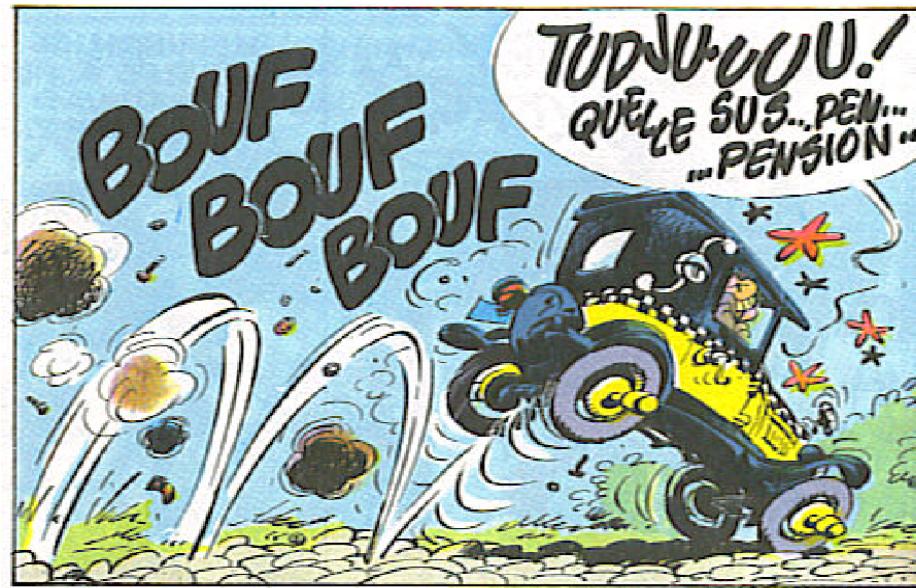
Maintenabilité

10



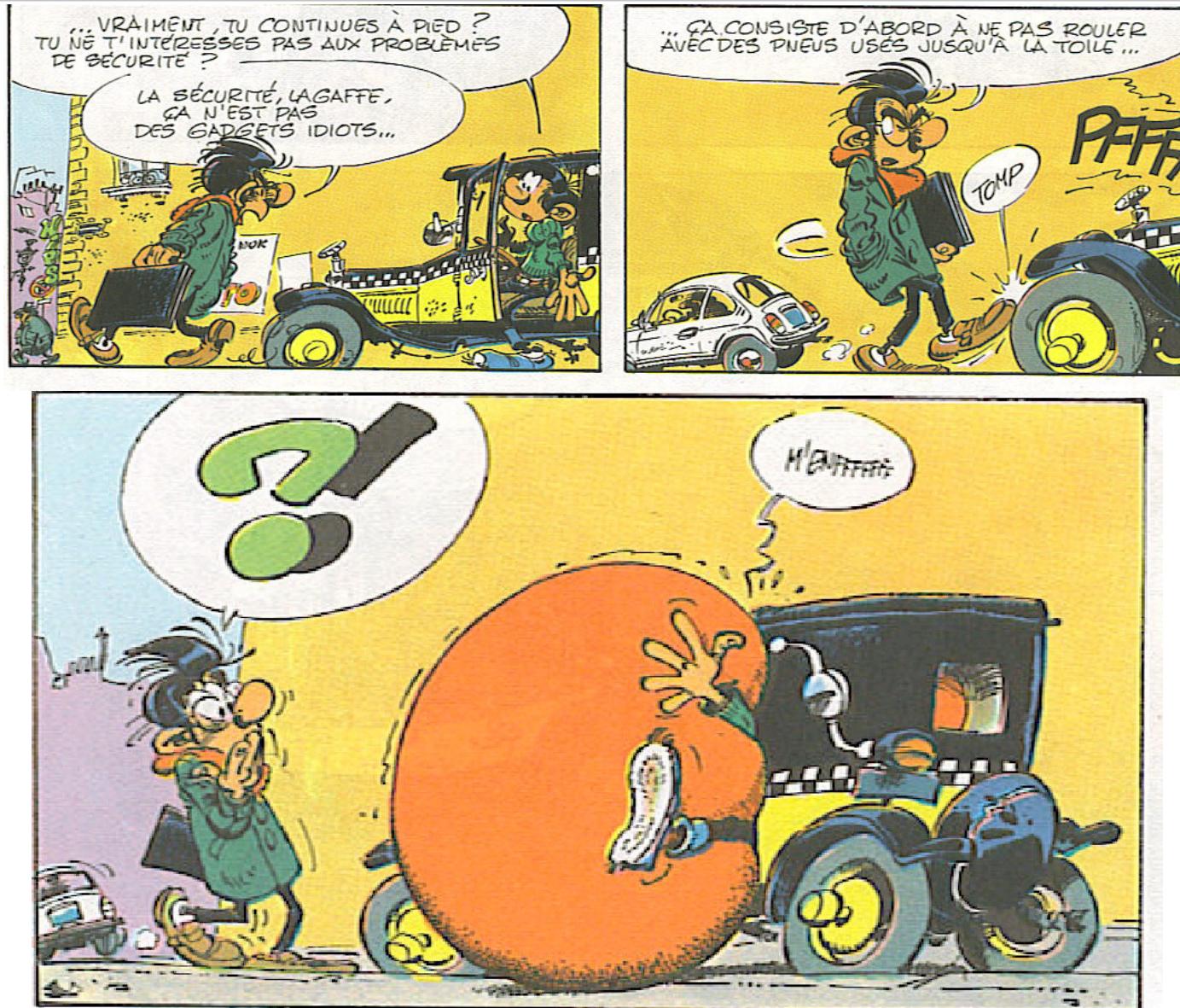
Sécurité

11



Sécurité

12



Terminologie Anglaise et Étymologie

13

- Sûreté de Fonctionnement : **FDMS** : Fiabilité, Disponibilité, Maintenabilité, Sécurité
- Dependability : **RAMSS** : Reliability, Availability, Maintainability, Safety, Security
- Fiabilité : Mot créé en 1962 pour traduire Reliability : du latin Fidare (faire confiance) => Latin médiéval Fiablete (digne de confiance, à qui on peut se fier) => Fiabilité

Sécurité : Safety vs Security

14

Securité traduit deux mots anglais :

- **Safety** : sécurité technique (pas de catastrophes en cas de pannes).
- **Security** : sécurité réglementaire : vis à vis des comportement humains (respect du code du travail, anti-intrusion résistance aux malveillances).

Sécurité : *un des aspects de la Sûreté*

15

Sécurité ⊂ Sûreté (qui contient aussi FDM)

Malgré une même étymologie (latin Securus : Sûr) => fréquentes confusions sûreté / sécurité (security en particulier).

FDMS : mots devenus familiers mais assez récents (fin des années 1960) de la langue Française.

Historique de la SdF : les débuts

16

Début du 20^{ème} siècle : l'âge de l'empirisme

- Recueils de durée de vie : *Fiabilité* (pièces ferroviaires)
- *Disponibilité* de réseaux électriques => redondances, possibilités de reconfigurations pour maintenir le service...
- Sécurité de la signalisation ferroviaire => conception en sécurité, sécurité « intrinsèque » (systèmes sécuritaires en présence de défaillance)
- Domaine aéronautique : premières approches de sécurité probabilistes et objectifs associés (1 accident pour 100000 heures de vol en 1939)

Historique de la SdF : Les débuts

17

Jusqu'en 1940 : Image du maillon faible :

- Identifier les éléments les moins fiables,
- Renforcer ces éléments sans appréhender globalement le système,
- Pécher par orgueil (Exemple : Titanic 1912 revendiqué comme *insubmersible* par ses concepteurs => 1500 morts lors de sa première traversée...)

La prise de conscience (années 1940)

18

- Nombreux problèmes dans des systèmes d'armes de plus en plus complexes (Missiles VII de W. Von Braun...)
- Dus à des éléments réputés « solides » !
- Loi de Murphy (1949) : « If anything can go wrong, it will ! »
- Fin de l'image (fausse) du maillon faible : fiabilité de n éléments de fiabilité r : r^n

Complexité croissante (1950)

19

- Développement de l'électronique à tubes (plusieurs milliers de tubes électroniques dans un navire de guerre)
- Disponibilité alarmante (de l'ordre de 30%)
- Coûts de maintenance astronomiques 2\$/(\$.année d'équipement électronique) !
- Apparition des premiers indicateurs chiffrés de fiabilité (MTBF...)
- Apparition des essais de type de fiabilité
- Premières *clauses contractuelles* FMDS

Dangerosité croissante (1960)

20

- Premiers vols spatiaux habités et développement du nucléaire civil,
- Formalisation de l'essentiel des méthodes d'analyse de la sécurité (AMDEC, Arbres de causes, diagramme de succès...),
- Premières banques de données de fiabilité
- Augmentation des objectifs chiffrés de sécurité (1 accident / 10 millions d'heures de vol)

L'époque contemporaine

21

- Premiers accidents graves dans le nucléaire civil (Three Miles Island, Tchernobyl, Fukushima...) => sensibilité accrue de l'opinion publique
- Apparition de nouvelles méthodes de prévision, spécifiques au nucléaires (arbres de conséquences pour l'analyse des séquences critiques)
- Extension de la FMDS à l'ensemble de l'activité industrielle
- Augmentation des exigences de disponibilité et maintenabilité
- Introduction de l'informatique y compris dans des fonctions de sécurité

Défaillance : définitions

22

La fiabilité est une mesure de l'aptitude à fonctionner sans *défaillance* pendant une durée donnée.

Défaillance :

- Arrêt du fonctionnement *normal* (dictionnaire)
- Cessation de l'aptitude à effectuer une fonction *requise* (normes internationales)
 - ⇒ Nécessité de définir où finit le normal et où commence l'anormal (*frontière nette*).
 - ⇒ La sûreté de fonctionnement classique ne considère que des pannes *soudaines et totales* (« cataleptiques »).
 - ⇒ Il revient à l'analyste de définir la « règle du jeu » qui convient (quitte à en définir plusieurs)

Application aux systèmes informatiques

23

La terminologie usuelle du domaine des systèmes informatiques (adoptée dans pratiquement tous les ouvrages sur le sujet), distingue :

- La **sécurité-innocuité** : sécurité au sens Safety
- La **confidentialité** : aptitude à éviter des divulgations non autorisées de l'information
- L'**intégrité** : aptitude à éviter des altérations inappropriées (intentionnelles malveillantes ou non, ou accidentielles)
- Ces deux notions sont souvent regroupés sous le vocable de **sécurité-confidentialité**

Application aux systèmes informatiques

24

La sûreté de fonctionnement est la propriété qui permet à ses utilisateurs de placer une **confiance** justifiée dans le service rendu par le système.

- FD : Font partie des aspects auxquels les utilisateurs sont les plus sensibles !
- M : Essentielle pour l'évolutivité d'un logiciel
- S (Safety et Security) : Évidemment l'aspect le plus important des logiciels dits "critiques"

Fautes, Erreurs, Défaillances

25

Selon cette même terminologie :

- Une **défaillance** survient lorsque le service délivré par le système dévie de ce à quoi il est destiné (par exemple le non accomplissement d'une fonction requise).
- La cause de la défaillance est une **erreur** affectant une partie de l'état du système (par exemple une variable erronée).
- La cause de l'erreur est une **faute** (par exemple un court-circuit sur un composant, une perturbation électromagnétique, ou une faute de développement d'un logiciel).

Fautes, Erreurs, Défaillances

26

Il est à noter que les définitions qui précèdent sont en fait récursives car la défaillance d'un composant (non accomplissement de la fonction d'un composant) est une faute pour le système que le contient.

D'où le schéma :

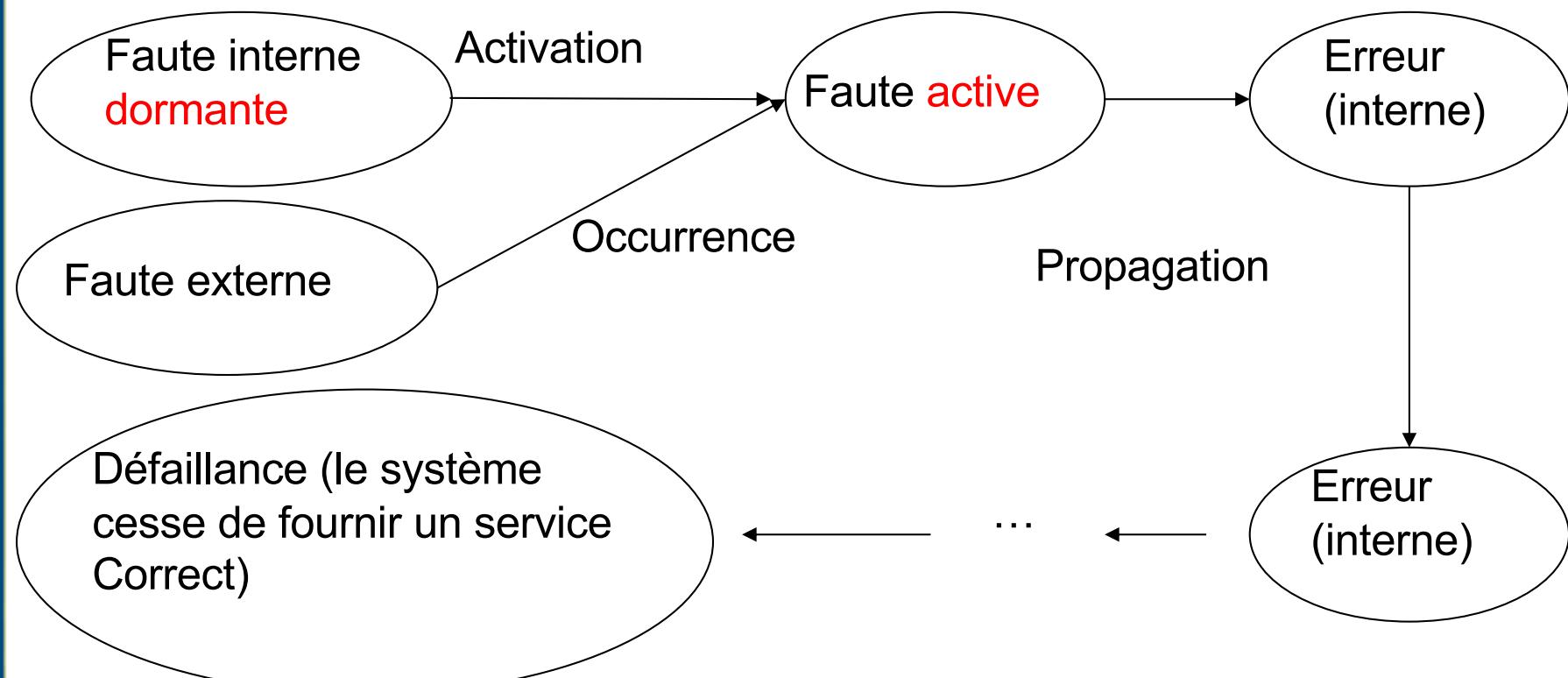


(La structure pouvant être en réalité arborescente par exemple dans le cas d'une faute causant plusieurs erreurs : phénomène appelé **propagation** des erreurs)

Fautes dormantes, fautes actives

27

Une faute peut rester temporairement inactive (instruction boguée non encore exécutée, octet mémoire défaillant non encore utilisé...). Elle est alors dite **dormante** :



Terminologie : Faute, Erreur, Défaillance

28

- Trois notions nécessaires pour les systèmes informatiques, termes consacrés par l'usage :
 - Traitement de **faute**, Tolérance aux **fautes**, diagnostic de **fautes**
 - Détection et correction d'**erreurs**
 - Taux de **défaillance**
- Synonymes :
 - Faute : défaut, bogue
 - Défaillance : dysfonctionnement, rupture de service
- **Panne** est ambigu : tomber en panne (défaillance), chercher la panne (faute). De plus panne humaine, panne de conception ne sont pas en usage.

Attributs, Entraves et Moyens de la SdF

29

- Fiabilité, Disponibilité, Maintenabilité, Confidentialité et Intégrité sont les **attributs** de la Sûreté de Fonctionnement
- Fautes, Erreurs et Défaillances sont les **entraves** à la SdF
- La terminologie des systèmes informatiques définit également les **moyens** pour la SdF qui sont :
 - La **prévention** des fautes
 - La **tolérance** aux fautes
 - L'**élimination** des fautes
 - La **prévision** des fautesPrévention et élimination étant parfois regroupés sous le vocable **éviter** des fautes

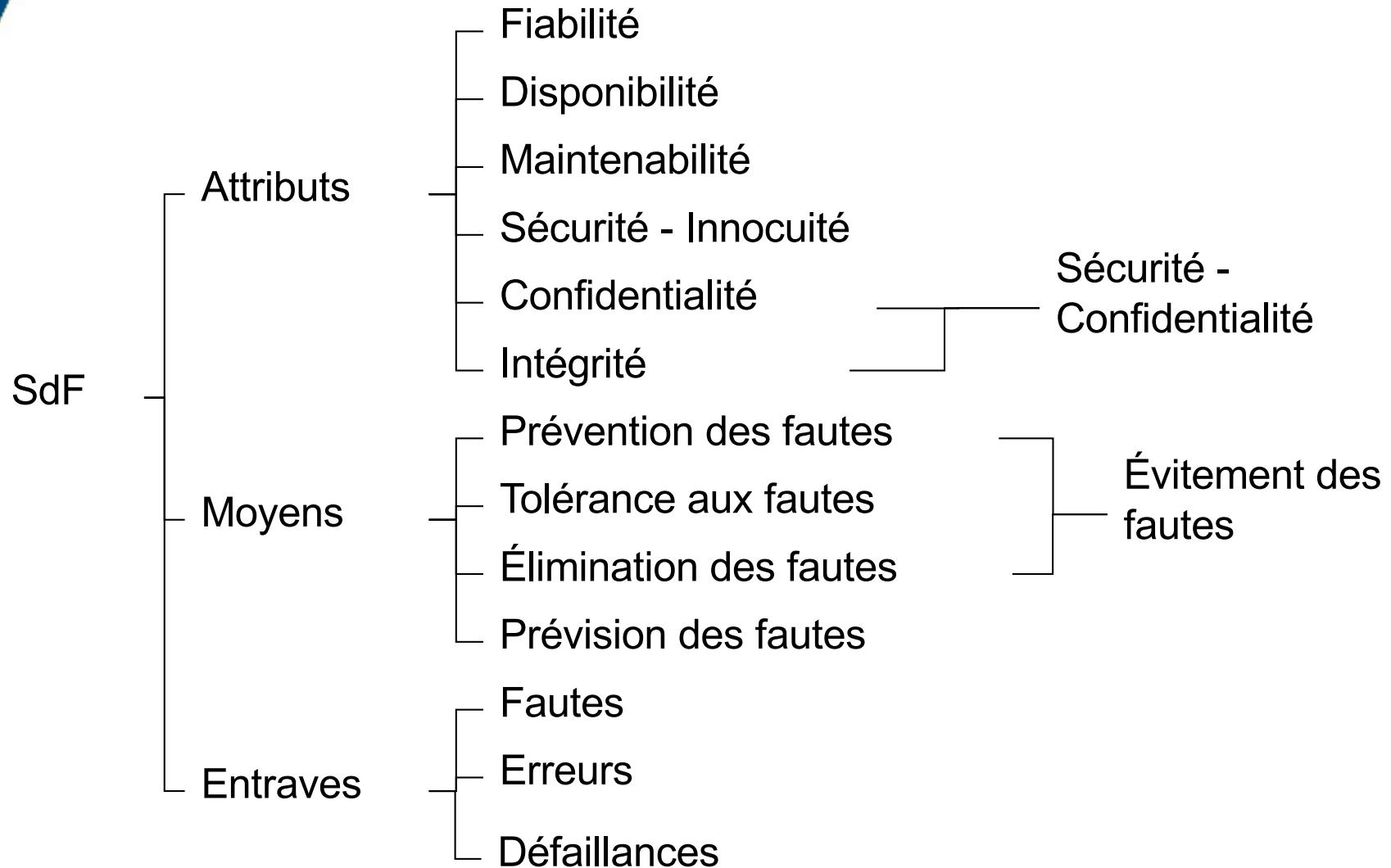
Moyens de la SdF

30

- **Prévention** des fautes : Empêcher l'occurrence ou l'introduction de fautes (rigueur du processus de développement)
- **Tolérance** aux fautes : Permettre la poursuite de la fourniture du service en dépit des fautes (conception adaptée, redondances...)
- **Élimination** des fautes : Réduire le nombre et la sévérité des fautes (vérifications : tests, preuves, modèles...)
- **Prévision** des fautes : Estimer la présence et les conséquences des fautes (Analyses prévisionnelles, AMDEC, AEEL, FTA...)

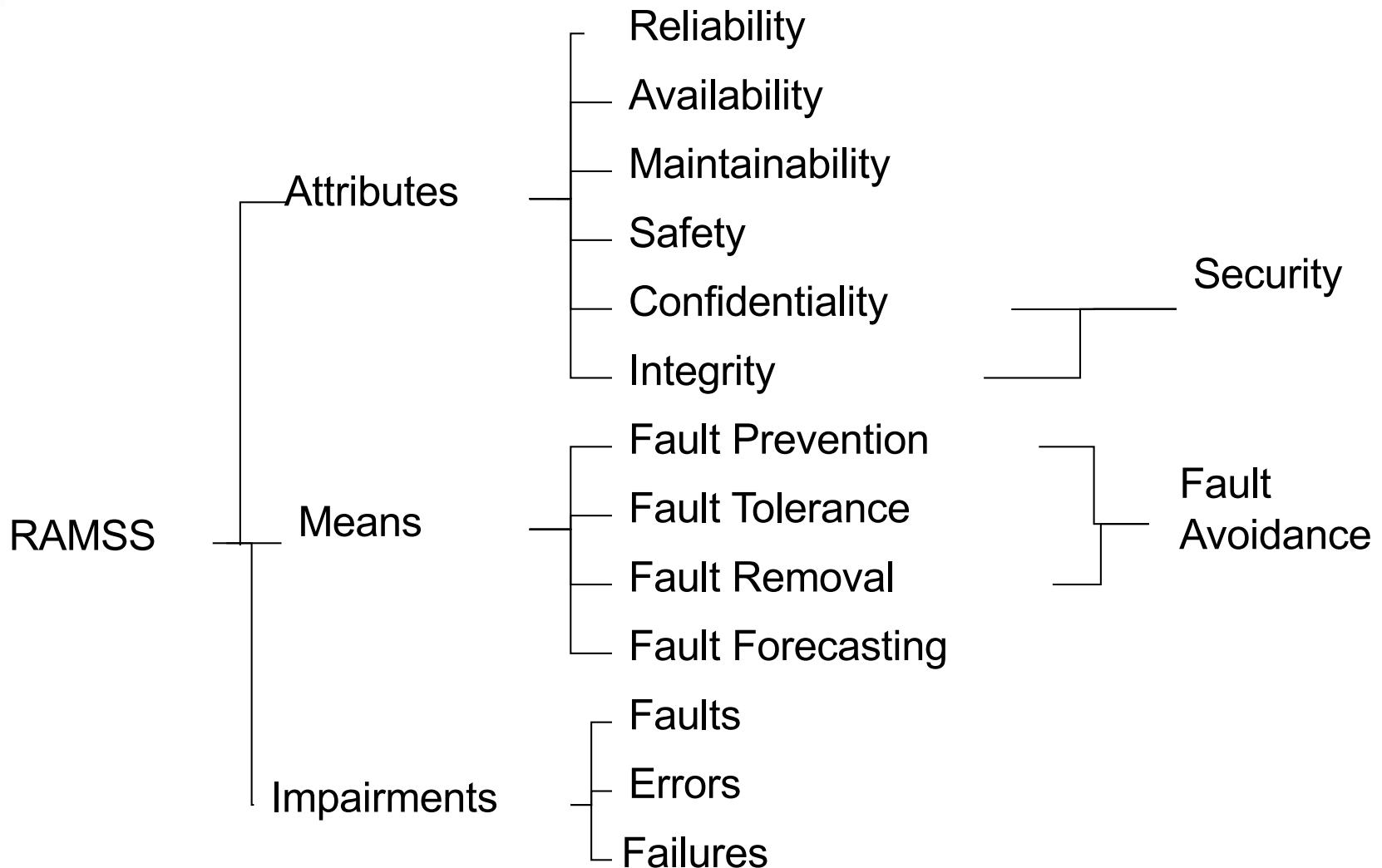
L'arbre de la SdF informatique

31



Computer System Dependability

32



Typologie des défaillances

33

Les défaillances sont souvent classées suivant :

- La **nature** de leurs conséquences (**en valeur / temporelles** : avance ou retard)
- La **gravité** de leurs conséquences (**bénignes / ... / catastrophiques**, le nombre de niveaux et leur définition dépend de l'application considérée)
- Leur **perception** par plusieurs utilisateurs : **cohérentes** si elles sont perçues de la même manière par tous, **incohérentes** ou **byzantines** sinon)

Typologie des défaillances

34

- Une catégorie particulière de défaillances est constitué des **défaillances par arrêt** avec deux sous-catégories : par **figement** (les sorties conservent leur valeur) ou par **silence** (pas d'envoi de message, sorties mises à zéro)
- La gravité des défaillances (parfois également appelée **sévérité**), permet de définir la **criticité** d'un système comme la gravité la plus importante auquel peuvent conduire ses défaillances.
- **Attention** : cette notion très répandue en informatique (systèmes critiques) est à ne pas confondre avec la criticité de l'AMDEC (le C signifiant Criticité au sens gravité* probabilité)

Systèmes à arrêt sur défaillance

Systèmes sécuritaires sur défaillance

35

- Un système dont toutes les défaillances vraisemblables sont par arrêt est dit à **arrêt sur défaillance (fail stop)**.
- Un système dont toutes défaillances vraisemblables sont bénignes est dit **sécuritaire sur défaillance (fail safe)**, ou parfois « de sécurité intrinsèque ».
- Dans des domaines type transports terrestres ou production d'énergie, un système fail safe est fréquemment réalisé à partir d'une propriété fail stop.
- Le système est alors dit à **défaillances contrôlées** (l'état d'arrêt auquel conduisent toutes les défaillances vraisemblables est dit restrictif).

Typologie des fautes

36

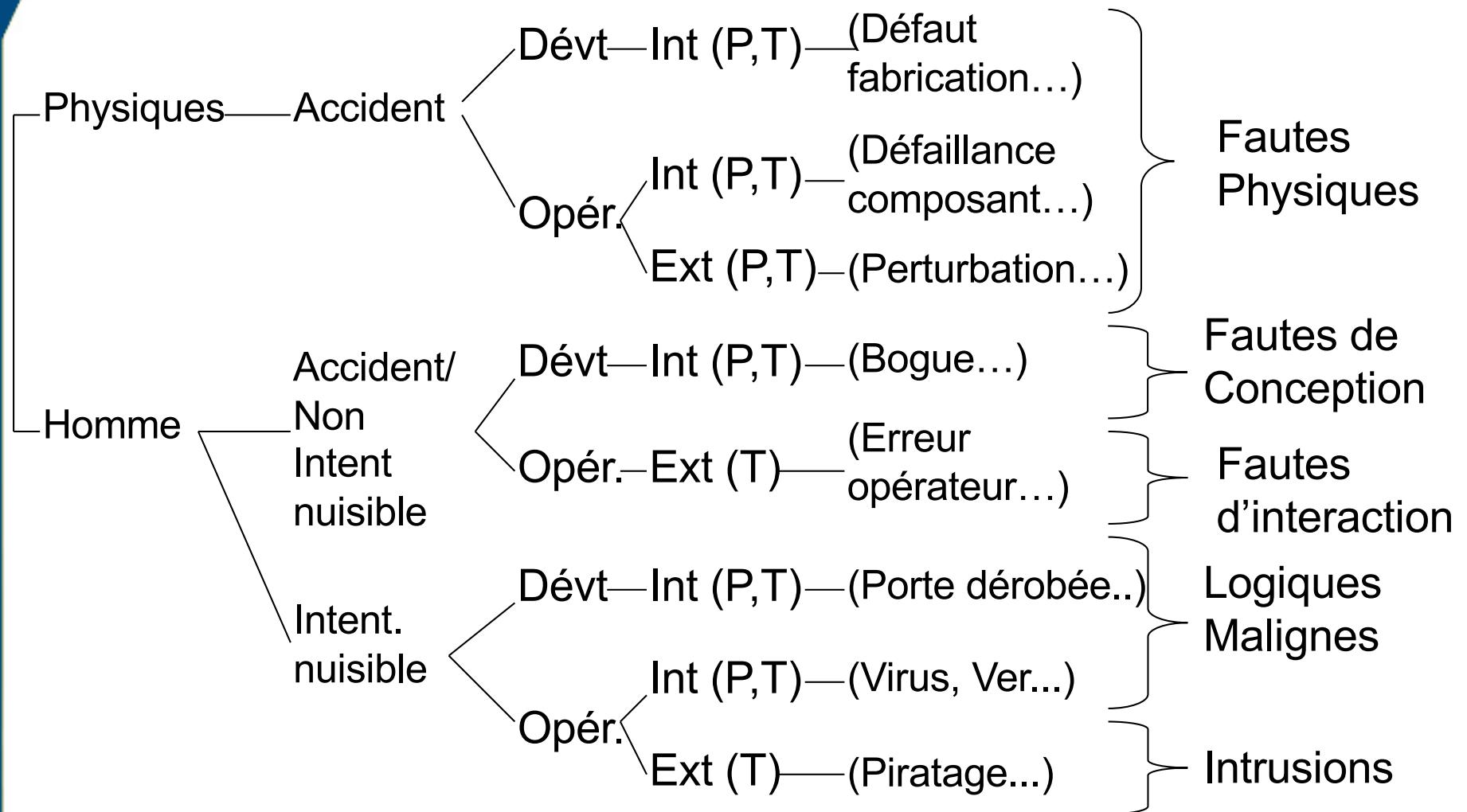
Les fautes sont envisagées suivant 5 points de vue :

- La **cause** phénoménologique : physiques / dues à l'Homme
- La **nature** : accidentelles / intentionnelles malveillantes ou non
- La **phase** de création ou d'occurrence : développement / opérationnelles
- La **situation** par rapport au système : internes / externes
- La **persistante** : permanentes / temporaires

La combinaison exhaustive conduirait à 48 types de fautes, mais certaines combinaisons sont non pertinentes (exemple faute de développement => faute interne)

Typologie des fautes

37



Indépendance des fautes, modes communs

38

- On compte donc 5 grands types de fautes, avec environ 8 grandes catégories différentes.
- Selon la terminologie en usage, une faute temporaire interne est dite **intermittente**, une faute temporaire externe est dite **transitoire**.
- Des fautes dont les causes attribuées sont différentes sont dites indépendantes, elles sont dites dépendantes dans le cas contraire.
- Les fautes dépendantes conduisent à des défaillances dites de mode commun, importantes à rechercher en particulier pour les architectures redondantes.

Fautes humaines intentionnellement nuisibles

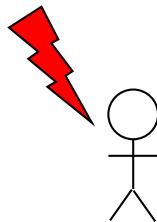
39

- Également appelées malveillances, elles regroupent les intrusions et les **logiques malignes** qui se décomposent en :
 - **Bombe logique** : parties de programmes restant dormantes jusqu'à un événement déclencheur.
 - **Cheval de Troie** : programme qui sous couvert d'une action légitime effectue une action cachée illégitime.
 - **Porte dérobée** : moyen secret (et ici malveillant) de contourner un contrôle d'accès.
 - **Virus** : programme malveillant qui se reproduit en s'adjoignant à un autre programme.
 - **Ver** : Programme autonome qui se propage à l'insu des utilisateurs.

Faute => Erreur => Défaillance : Exemple 1

40

Erreur



Programmeur

Faute
dans le source
du logiciel

Faute dans
l'exécutable
embarqué

Défaillance
compilation ou
claquage PROM

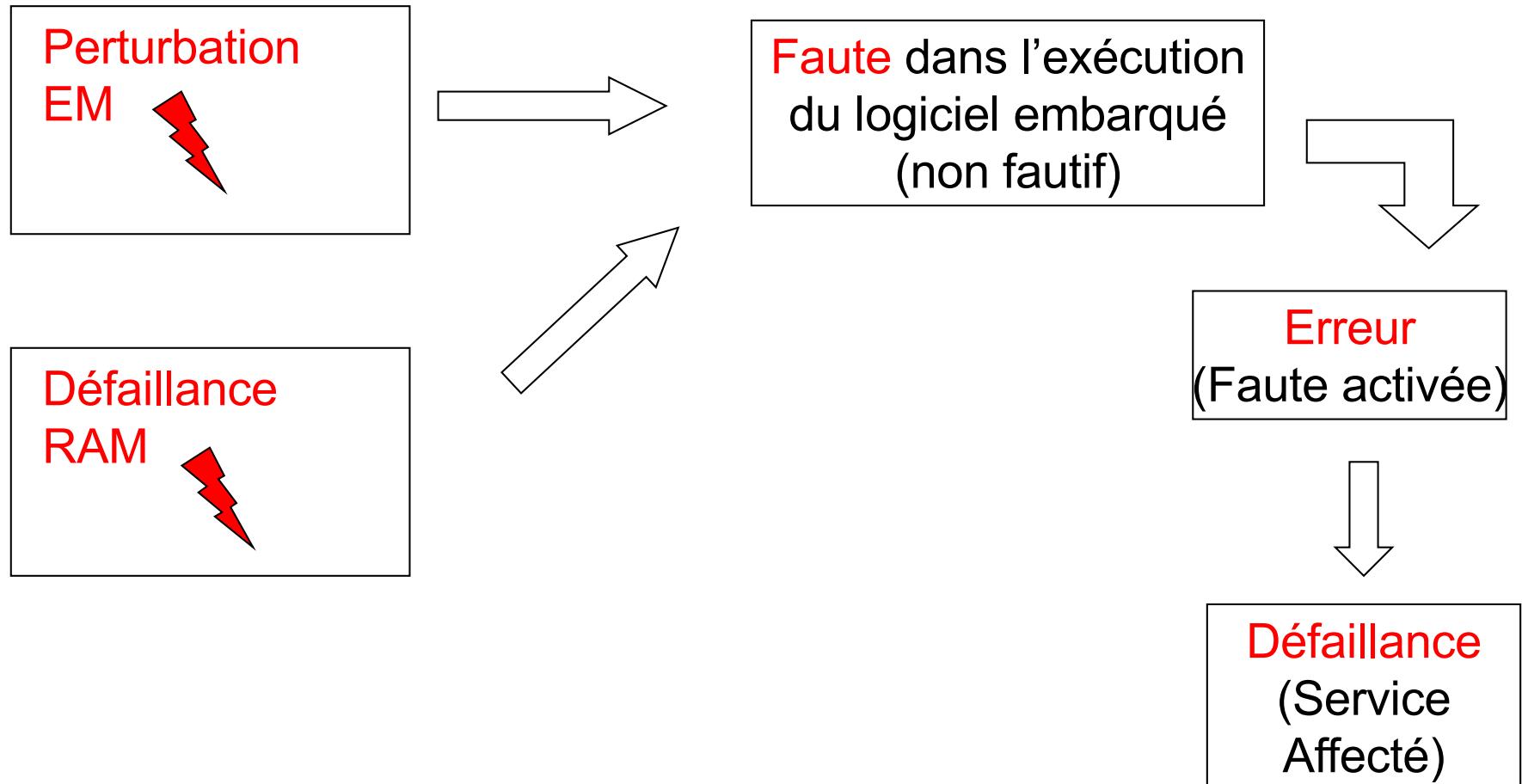
Erreur
(Faute activée)

(peut elle même être due à une
faute du logiciel de compilation
due à une autre erreur de
programmation)

Défaillance
(Service
Affecté)

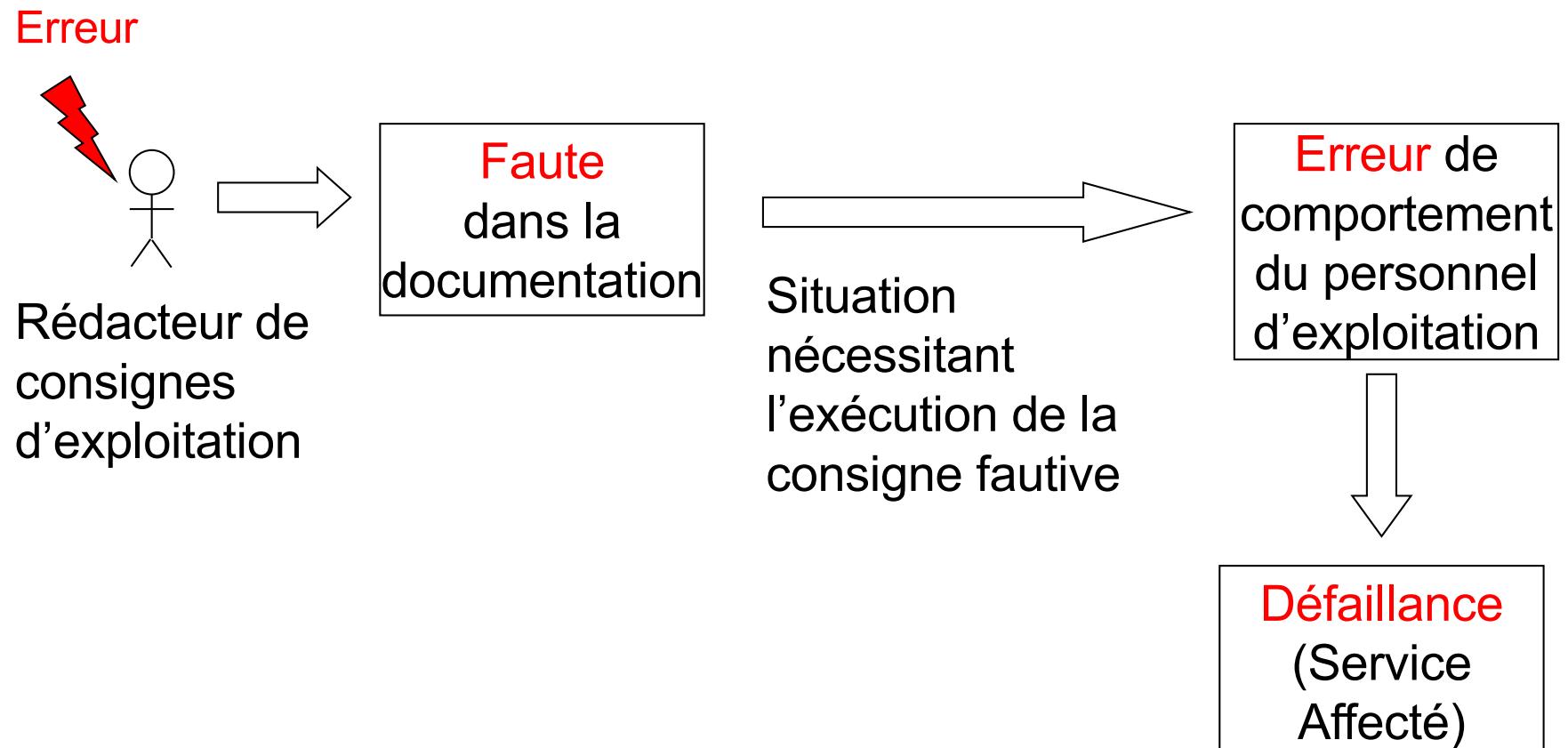
Faute => Erreur => Défaillance : Exemple 2

41



Faute => Erreur => Défaillance : Exemple 3

42



Moyens pour la SdF : Tolérance aux fautes

43

La **Tolérance** aux fautes est classiquement décomposée en :

- **Traitement** d'erreur (élimination d'erreurs avant défaillance)
 - **Détection** d'erreur
 - **Diagnostic** d'erreur
 - **Recouvrement** d'erreur
 - Reprise
 - Poursuite
 - Compensation
- **Traitement** de fautes
 - **Diagnostic** de faute
 - **Passivation** des fautes
 - **Reconfiguration**

Moyens pour la SdF : Élimination des fautes

44

- L'élimination des fautes commence par la vérification suivie si nécessaire de diagnostic et correction et d'une nouvelle vérification dite de non régression.
- La vérification se décompose en :
- Vérification statique (sans activation réelle) :
 - Analyse statique (inspections...)
 - Preuves
 - Analyse du comportement (Model Checking)
- Vérification dynamique (avec activation réelle) :
 - Exécution symbolique
 - Tests (unitaires, intégration, fonctionnels)

Moyens pour la SdF : Prévision des fautes

45

- La **prévision** des fautes comprend toutes les méthodes permettant de prévoir (dès la conception) les attributs de la SdF. Elle se décompose en :
 - Évaluation **qualitative** ou **ordinale** (recherche des scénarios contraires à la SdF sans chiffrage)
 - Évaluation **quantitative** ou **probabiliste** (estimation du taux d'occurrence des scénarios). Le domaine de la SdF informatique distingue de plus :
 - Fiabilité **stabilisée**
 - **Croissance de fiabilité**

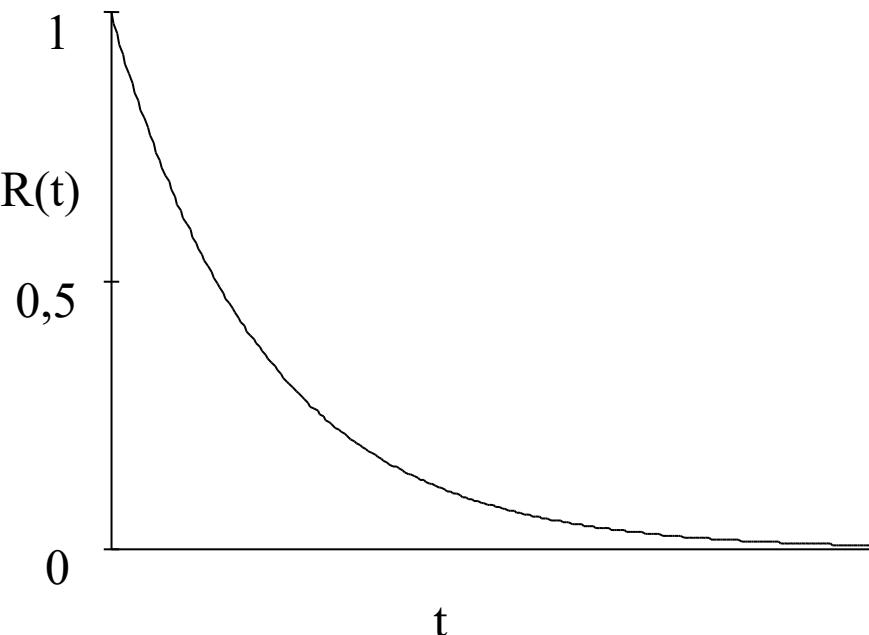
Fiabilité : Reliability $R(t)$

46

- $R(t) = \text{Probabilité(pas de défaillance sur l'intervalle } [0,t]),$ le système étant supposé non défaillant à $t = 0$

Propriétés :

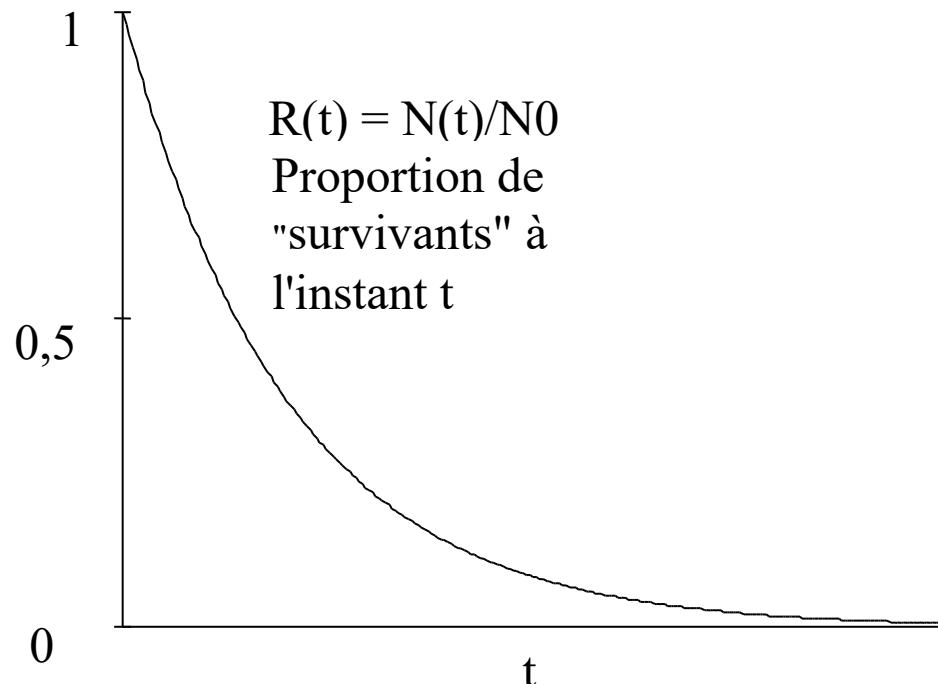
- $R(0)=1$ (Par hypothèse)
- $R' \leq 0$ (Durée augmente \Rightarrow probabilité de défaillance augmente)
- $R(\infty)=0$ (Nul n'est immortel)



Fiabilité : Reliability R(t)

47

- Perception intuitive : Expérience imaginaire :
Population importante de systèmes identiques initialement sans défaillances.

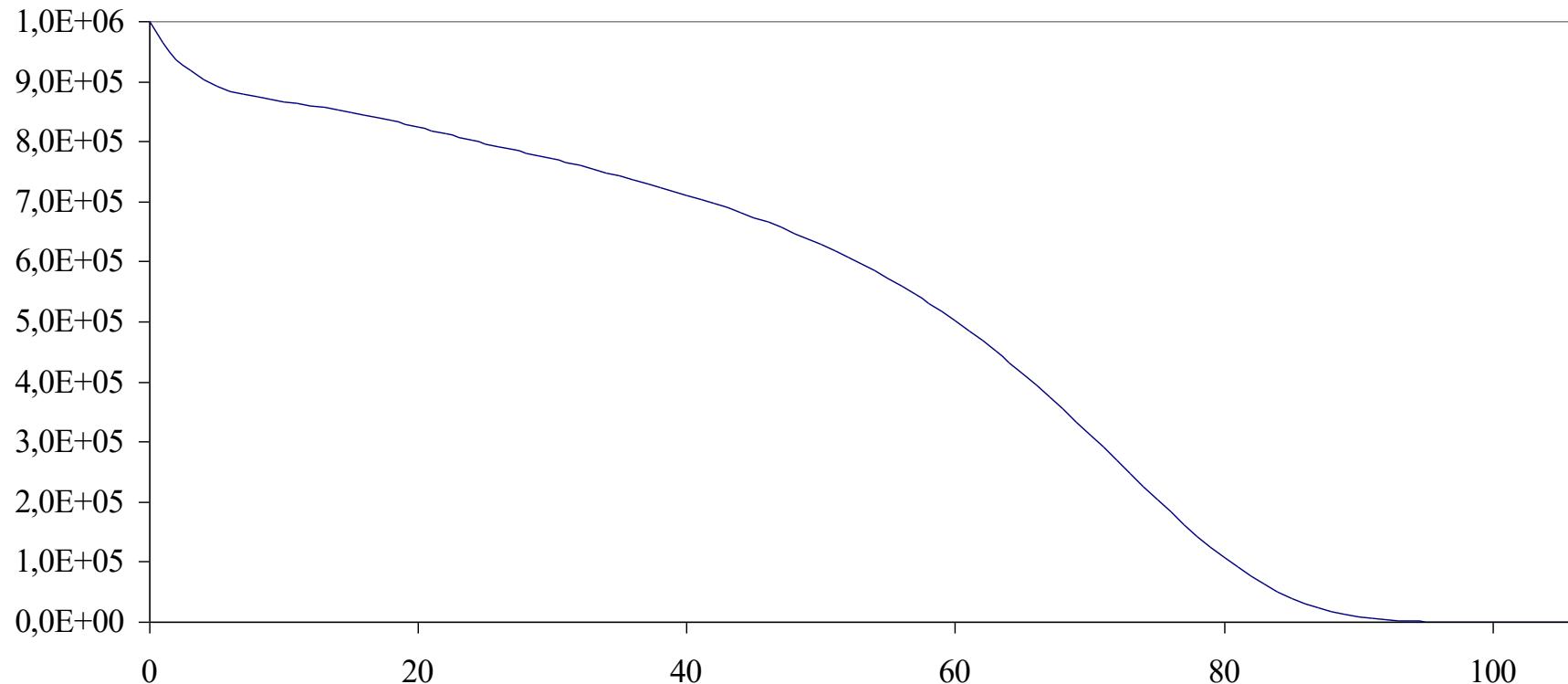


- On laisse la population évoluer sans remplacements.
- La proportion de survivants ramenée à la population initiale est un estimateur de la fiabilité.

Fiabilité des êtres humains...

48

- Une telle courbe (nombre de survivants en fonction de l'âge d'une population initiale de nouveaux nés) sert aux assurances à calculer les primes d'assurance décès...



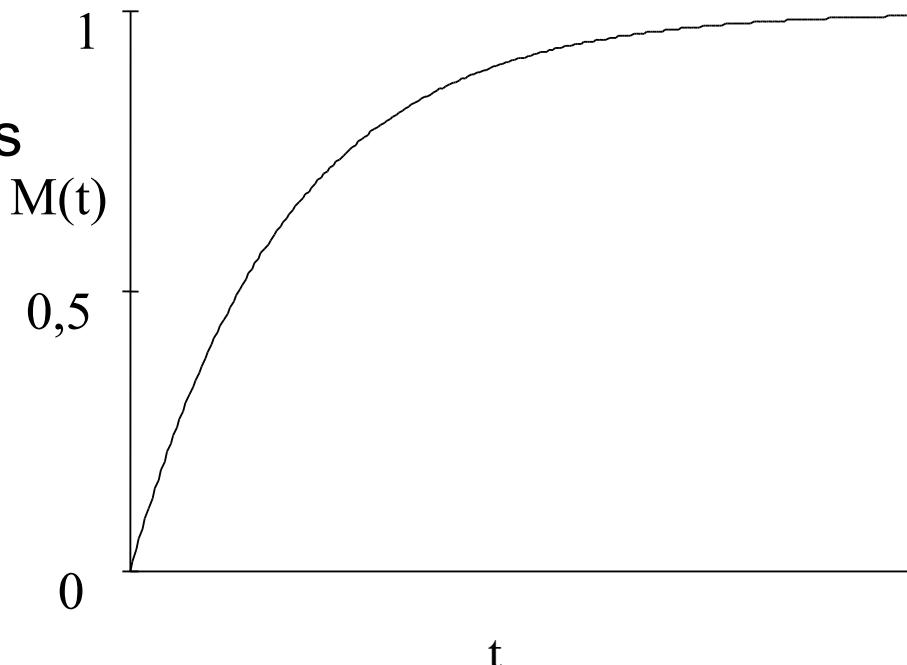
Maintenabilité $M(t)$

49

- $M(t)=$ Probabilité(réparation achevée sur $[0,t]$), le système étant supposé dans un état défaillant donné à $t=0$ et des moyens de maintenance donnés lui étant affectés

Propriétés :

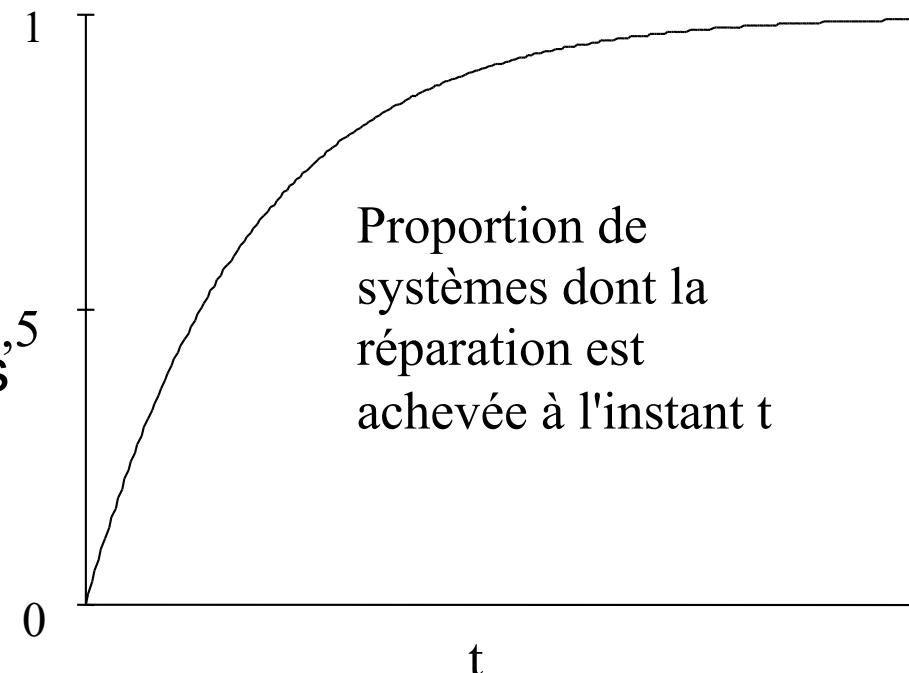
- $M(0)=0$ (Par hypothèse)
- $M' >=0$ (Durée augmente => proba de réparation augmente)
- $M(\infty)=1$ (Rien n'est irréparable dans le domaine technique)
- Il peut y avoir plusieurs $M(t)$: une par état défaillant



Maintenabilité $M(t)$

50

- Perception intuitive :
Expérience imaginaire :
Population importante de systèmes identiques initialement tous dans le *même état défaillant* affectés de moyens de maintenance *identiques*.



- On laisse la population évoluer sans remplacements.
- La proportion de systèmes réparés ramenée à la population initiale est un estimateur de la maintenabilité.

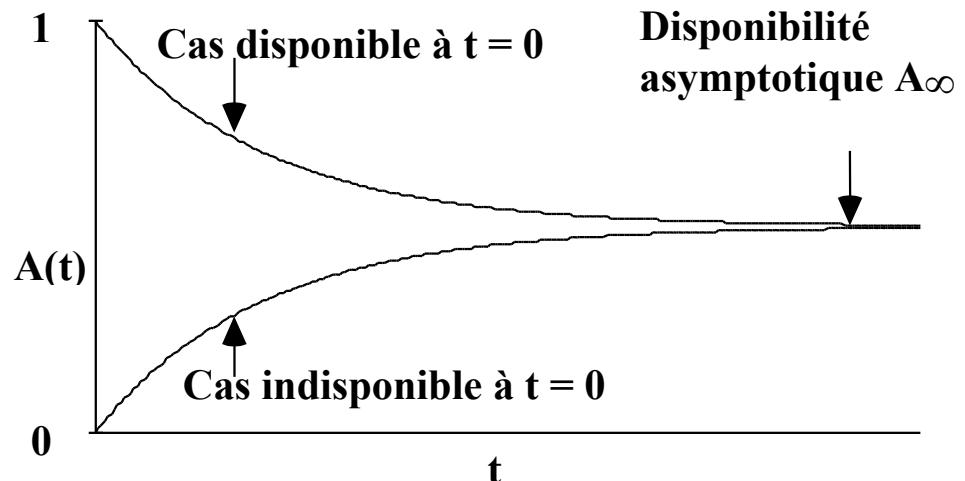
Disponibilité : Availability A(t)

51

- $A(t)$ =Probabilité (système opérationnel à l'instant t)

Propriétés :

- $A(0)$: dépend de l'état initial
- Tend vers une constante "disponibilité asymptotique" (équilibre statistique défaillances / réparations)



Taux de défaillance : $\lambda(t)$

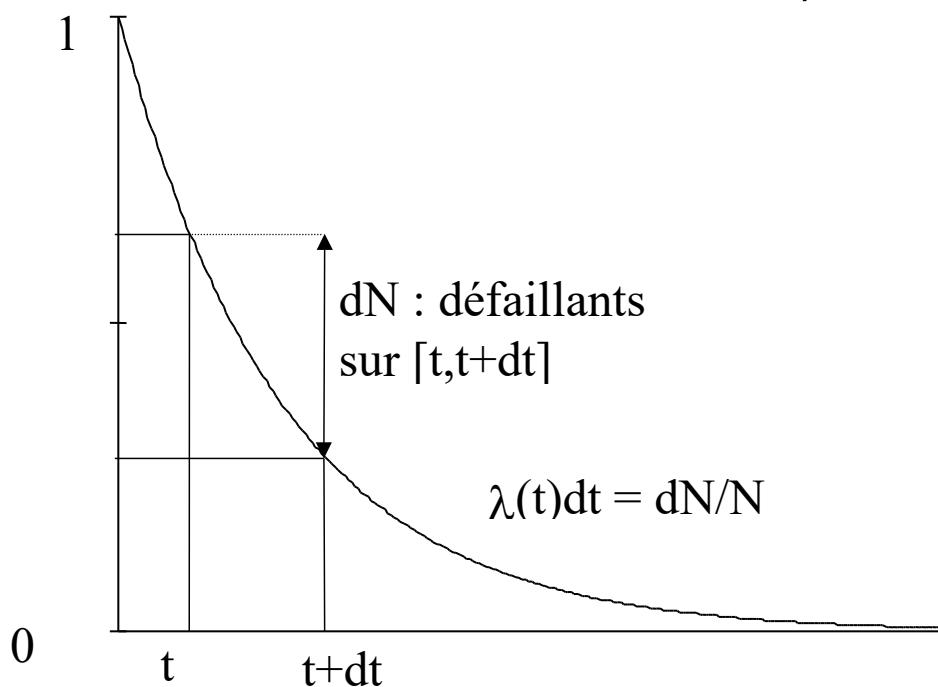
52

$\lambda(t) dt$ = Probabilité(défaillance sur $[t, t+dt]$ sachant qu'il n'y a pas eu de défaillance sur $[0, t]$)

On démontre facilement que :

$$\lambda(t) = -\frac{1}{R} \frac{dR}{dt}$$

$\lambda(t)$: taux de mortalité (ramené à la population des vivants à l'instant t)



Intensité de défaillance $f(t)$

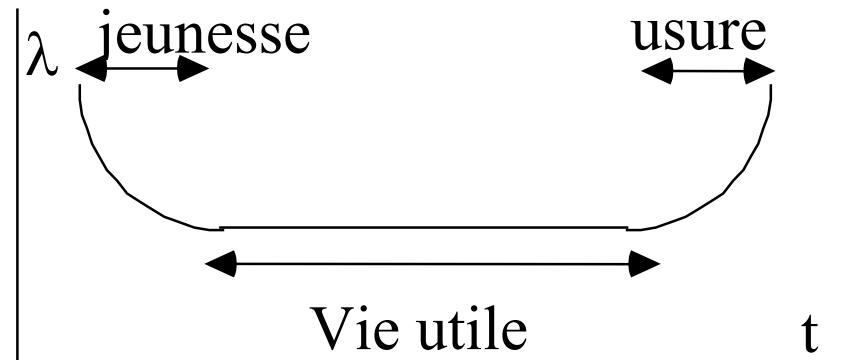
53

- $1-R(t)$ « défiabilité » : probabilité pour que le système connaisse une défaillance sur $[0,t]$ (donc que l'instant de la défaillance soit antérieur à t).
- $1-R(t)$ est donc la fonction de répartition de la variable aléatoire continue « instant de la défaillance ».
- Sa dérivée $f(t)=-dR/dt$ parfois appelée intensité de défaillance est donc la densité de probabilité de cette même variable.
- $f(t)$ est importante car c'est elle qui sera utilisée pour calculer des moyennes (ou espérances mathématiques).
- $f(t)$ ne doit pas être confondue avec $\lambda(t)$: $f(t)dt$ est la probabilité a priori pour que l'instant de la défaillance soit dans $[t,t+dt]$

Taux de défaillance des composants électroniques

54

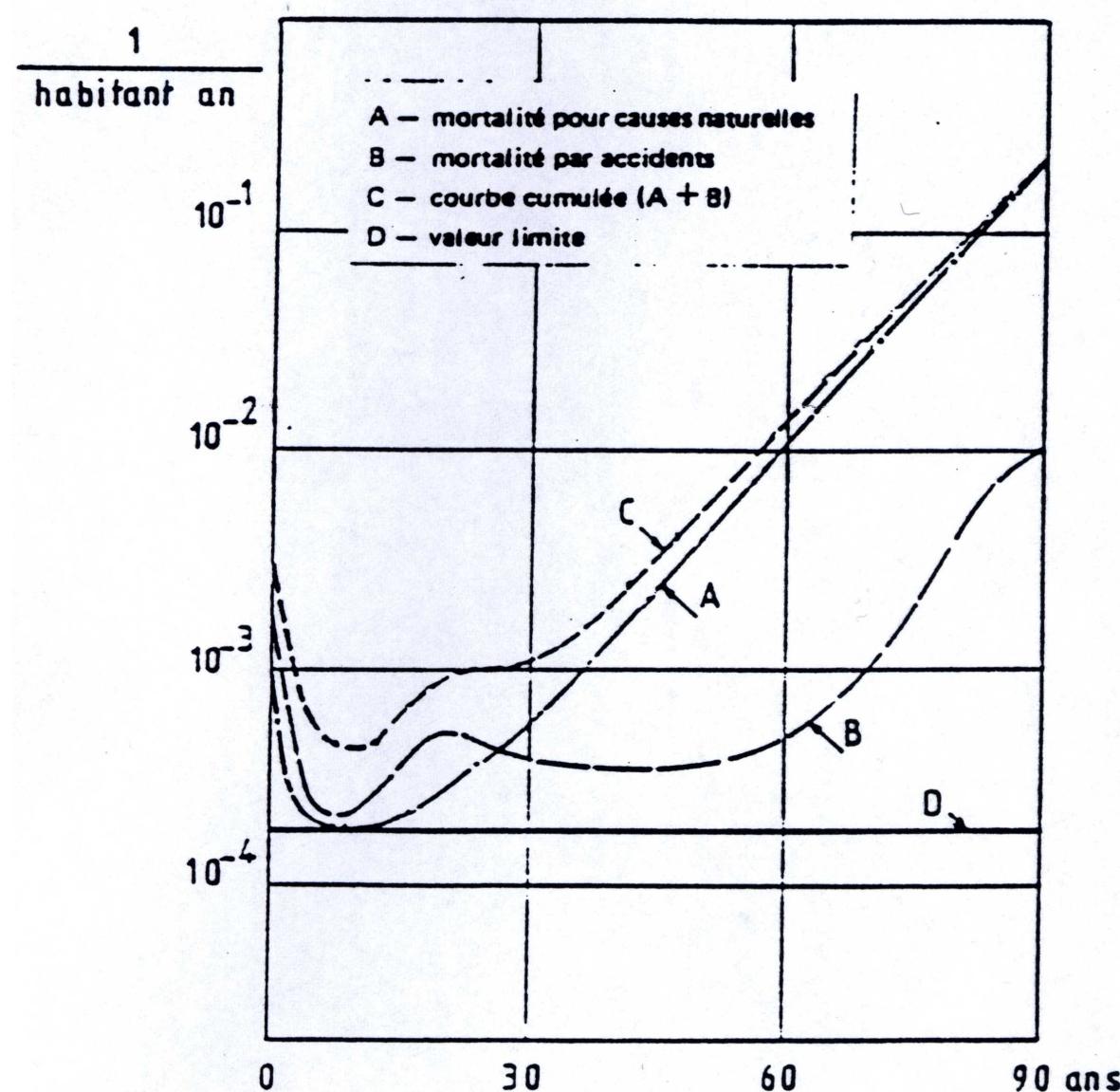
- Allure caractéristique courbe "en baignoire"
- Jeunesse : mortalité infantile (défauts de fabrication)
- Usure : mortalité par vieillesse
- Vie utile : taux de défaillance constant mais non nul
- Se ramener dans cette zone => déverminage et remplacement préventif avant usure



Défaillances à taux constant
"purement aléatoires" : l'âge du
composant n'a pas d'importance :
"il ne vieillit pas"

Taux de défaillance des êtres humains...

55



Mean Time To Failure : MTTF

56

- MTTF : Mean Time To (First) Failure ou Durée moyenne jusqu'à défaillance est la moyenne du temps de vie ou espérance (mathématique) de vie.

Intégration par parties immédiates (R rapidement décroissante à l'infini) :

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

Taux de réparation μ , Mean Time To Repair MTTR

57

- On définit de manière tout à fait analogue le taux de réparation μ :

$$\mu = \frac{1}{1 - M} \frac{dM}{dt}$$

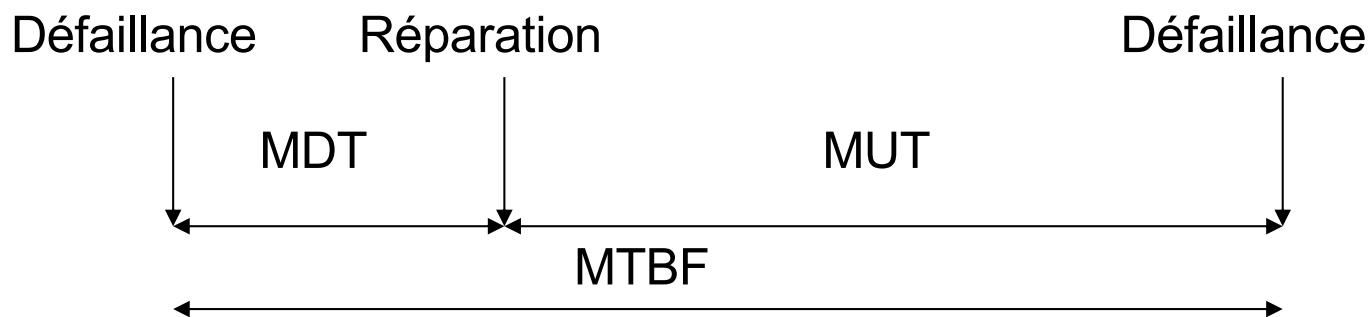
et la durée moyenne jusqu'à réparation Mean Time To Repair MTTR, dont il est facile de démontrer (également par intégration par parties) qu'elle vaut :

$$MTTR = \int_0^\infty (1 - M(t)) dt$$

MDT, MUT, MTBF

58

- Pour un système réparable : cycle défaillance réparation défaillance séparés en moyenne de :



- MUT : Mean Up Time ou durée moyenne de bon fonctionnement après réparation
- MDT : Mean Down Time ou durée moyenne de réparation après une défaillance
- MTBF : Mean Time Between Failures ou durée moyenne entre défaillances (et pas Moyenne des Temps de Bon Fonctionnement !)

Grandeurs dépendantes ou non de l'état initial

59

- Un système a en général plusieurs états défaillants dits **modes de défaillance**.
- $M(t)$ et donc MTTR dépend des moyens de maintenance et du mode de défaillance de départ => plusieurs $M(t)$ et MTTR pour un même système.
- Pour un système avec redondance : plusieurs états (« modes ») de bon fonctionnement (certains avec fautes tolérées grâce à la redondance) => En principe plusieurs $R(t)$ et MTTF.
- Par convention toutefois l'état initial pour la fiabilité est l'état où le système ne comporte aucune faute.

Grandeurs dépendantes ou non de l'état initial

60

- MUT, MDT et MTBF envisagent par contre un cycle moyen tous modes de défaillance et de bon fonctionnement pris en compte.
- Ces grandeurs ne dépendent donc pas de l'état initial
- MUT doit être vu comme la durée moyenne où le système demeure dans un mode de bon fonctionnement moyen
- MDT comme la durée moyenne où le système demeure dans un état défaillant moyen
- MDT et donc MTBF dépend par contre toujours des moyens de maintenance
- Pour un système industriel « raisonnable »
 $MDT \ll MUT$

Taux de défaillance constant

61

- Hypothèse très souvent utilisée : valeurs données par les bases de données, calculs simples.
 - Réaliste pour systèmes électroniques avec déverminage et remplacement de composants avant vieillissement.
 - Dans ce cas : $R(t) = e^{-\lambda t}$ $MTTF = \frac{1}{\lambda}$
- Se souvenir de la signification : la défaillance est à taux constant est un phénomène « accidentel » pour lequel l'âge n'a pas d'importance. Le composant « ne vieillit pas » : il est inutile de changer un composant contre un autre ayant fonctionné moins longtemps (dès lors que l'on reste à λ constant).
- Un exemple très caractéristique de λ constant est l'atome radioactif dont la désintégration suit exactement cette loi...

Taux de défaillance constant

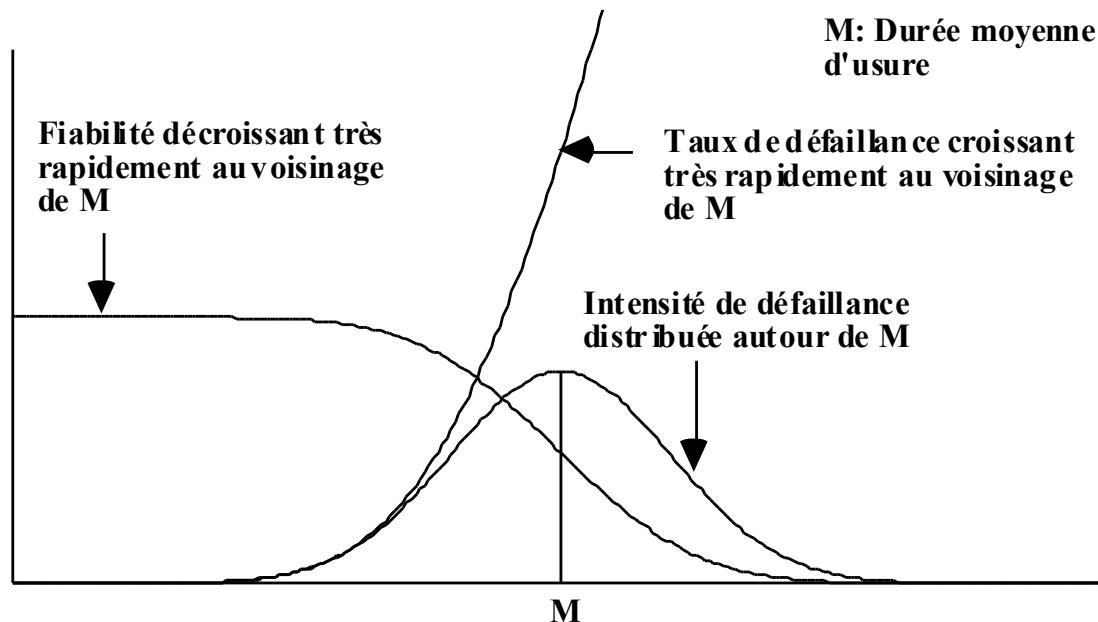
62

- On démontre facilement dans ce cas les résultats suivants :
- L'instant de la défaillance est distribué suivant une loi exponentielle,
- Si le composant est immédiatement remplacé par un composant identique à chaque défaillance, la probabilité d'avoir n défaillances sur $[0,t]$ suit une loi de Poisson (l'instant de la n ième défaillance est alors distribué suivant une loi d'Erlang),
- La probabilité d'avoir n défaillances sur $[0,t]$ sur un parc de N équipements suit une loi binômiale qui tend vers la loi de Poisson si le parc est important et la probabilité de défaillance faible.

Défaillances d'usure

63

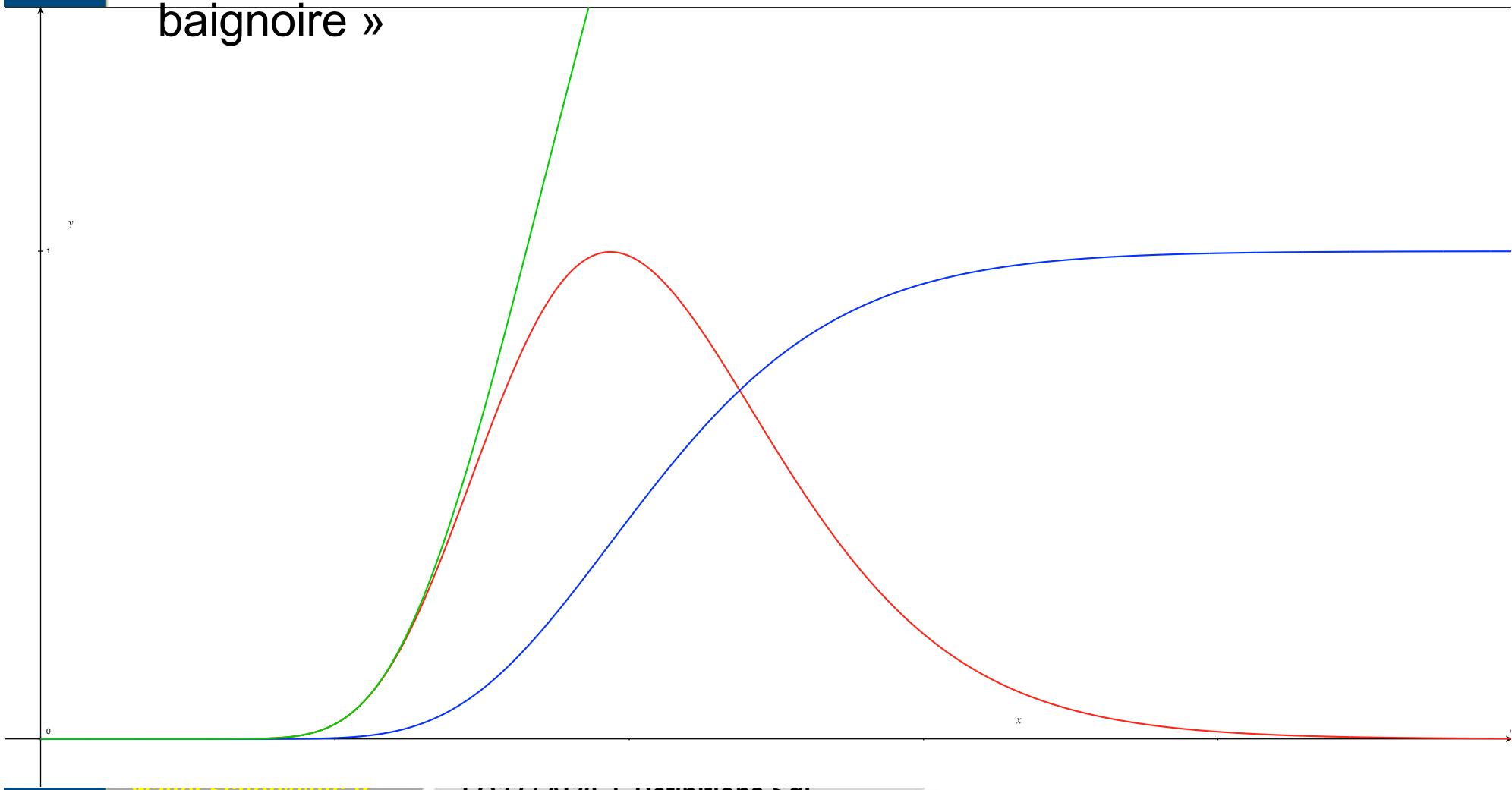
- Pour les défaillances d'usure, l'instant de la défaillance est réparti autour d'une valeur dite « durée moyenne d'usure » (notée M) avec un certain écart type.
- La fiabilité et le taux de défaillance que l'on peut recalculer par intégration de cette densité de probabilité ont alors l'allure suivante



Défaillances d'usure

64

Tout est donc dans le modèle d'usure (ici un exemple utilisant une loi log-normale) qui revient à modéliser le « bord droit de baignoire »



Défaillance à taux constant vs défaillances d'usure

65

Ne surtout pas s'imaginer que l'on peut utiliser un composant électronique sur une durée voisine de MTTF en effet :

- La probabilité de survie d'un composant de λ constant à $t=MTTF$ n'est que de 37% (e^{-1}). Elle n'est que de 90% à $MTTF/10$
- La durée moyenne d'usure est en général très petite devant MTTF (ordre de grandeurs typiques 10^4 h contre 10^6 h). Pour garder l'hypothèse du λ constant, le composant sera donc remplacé bien avant d'atteindre MTTF.

Taux de réparation constant

66

- Bien que moins réaliste (revient à dire que le composant « tombe en marche » accidentellement), l'hypothèse est toutefois parfois utilisée car donne lieu à des calculs simples qui fournissent de bons ordres de grandeurs.
- Dans ce cas :

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

$$MTTR = 1/\mu$$

- L'instant de la réparation est également réparti suivant une loi exponentielle

Taux de défaillance et de réparation constants

67

- Dans le cas λ et μ constant on peut obtenir une expression analytique de la disponibilité par :

$$A(t+dt) = A(t) (1-\lambda dt) + (1-A(t)) \mu dt$$

Système disponible à
t+dt dans deux cas
mutuellement
exclusifs

1) Le système était
disponible à t et ne
défiaille pas sur
[t, t+dt]

2) Le système était
indisponible à t et est
réparé sur [t, t+dt]

➤ D'où :

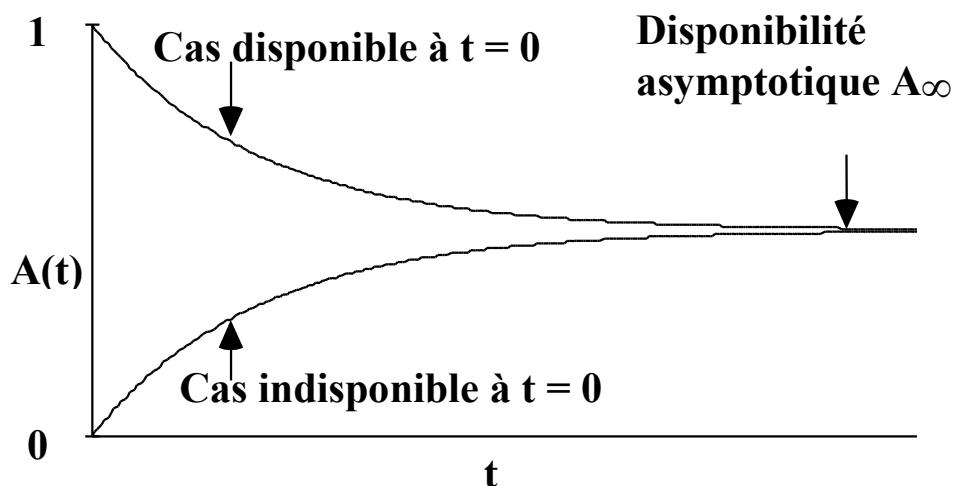
$$\frac{dA}{dt} = \mu - (\lambda + \mu)A(t)$$

Taux de défaillance et de réparation constants

68

- Par intégration immédiate
- $A(t) = \mu/(\lambda+\mu) + \lambda/(\lambda+\mu)e^{-(\lambda+\mu)t}$ (cas disponible à $t=0$)
- $A(t) = \mu/(\lambda+\mu) - \mu/(\lambda+\mu)e^{-(\lambda+\mu)t}$ (cas indisponible à $t=0$)

- La disponibilité asymptotique vaut donc $\mu/(\lambda+\mu)$.
- En considérant le cycle moyen on voit également aisément qu'elle vaut : **MUT/MTBF**



Sécurité des systèmes

69

L'approche sécurité repose sur la répartition des événements indésirables par :

- Classes de **gravité** : conséquences en termes de dommages aux biens et aux personnes
- Classes de **fréquence** (taux d'occurrence par heure de fonctionnement du système)
- L'acceptabilité est déterminée par des zones acceptables ou non dans la "**matrice de criticité**" (ou occurrence - gravité)
- La sécurité prévisionnelle utilise donc les même indicateurs que la fiabilité (taux de défaillances **catastrophiques** focalisé sur les événements à conséquences graves).

Exemple de classes de gravité (D'après Norme ferroviaire EN 50126)

70

Niveau de gravité	Conséquence pour les Personnes ou l'environnement	Conséquence pour le service
Catastrophique (4)	Des morts et/ou plusieurs personnes gravement blessées et/ou dommages majeurs pour l'environnement	
Critique (3)	Un mort et/ou une personne grièvement blessée et/ou des dommages graves pour l'environnement	Perte d'un système important
Marginal (2)	Blessures légères et/ou menaces graves pour l'environnement	Dommage grave pour un (ou plusieurs) système(s)
Insignifiant (1)	Éventuellement une personne légèrement blessée	Dommages mineurs pour un système

Classes de fréquence selon EN 50126

71

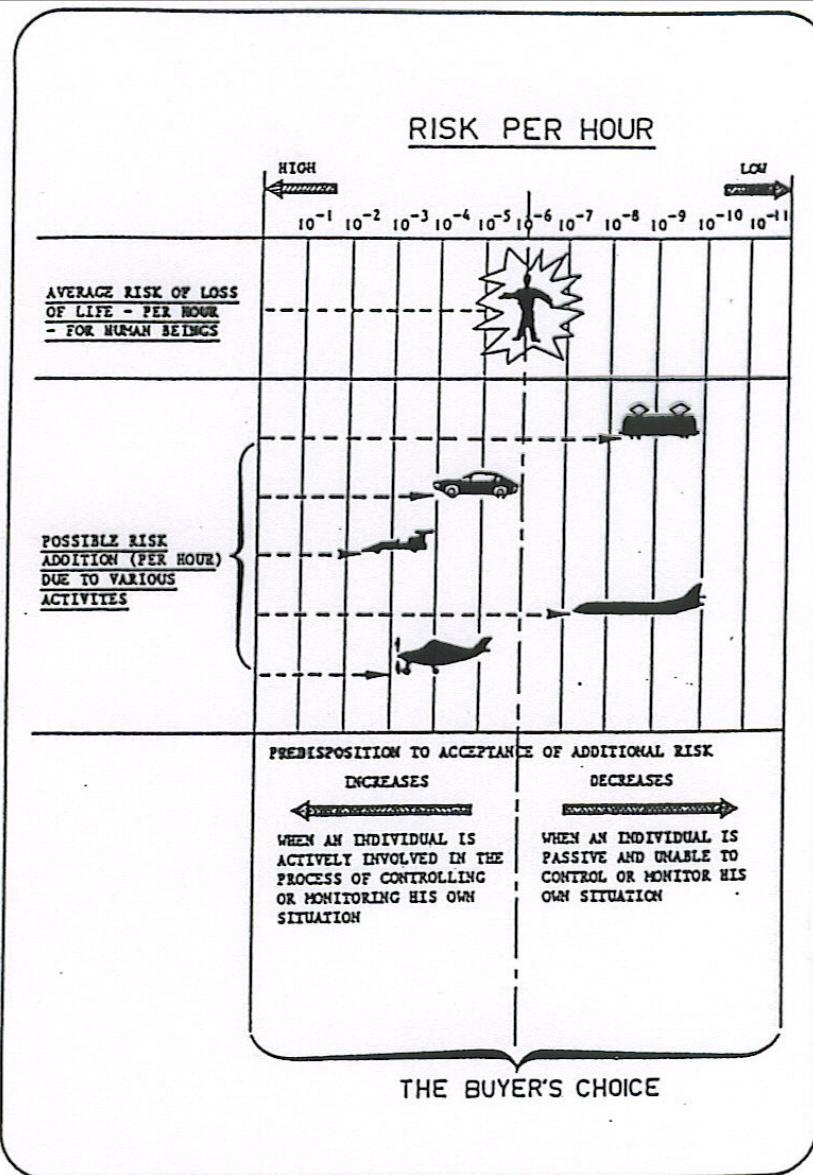
Catégorie	Description	Taux
Fréquente (A)	Susceptible de se produire fréquemment. Situation dangereuse continuellement présente.	$<10^{-4}/h$
Probable (B)	Peut survenir à plusieurs reprises. Situation dangereuse survenant souvent.	$<10^{-5}/h$
Occasionnelle (C)	Susceptible de survenir à plusieurs reprises.	$<10^{-6}/h$
Rare (D)	Susceptible de se produire à un moment donné du cycle de vie du système. La situation dangereuse se produira vraisemblablement.	$<10^{-7}/h$
Improbable (E)	Peu susceptible de se produire mais possible. Peut exceptionnellement se produire.	$<10^{-8}/h$
Invraisemblable (F)	Extrêmement improbable. On peut supposer que la situation dangereuse ne se produira pas.	$<10^{-9}/h$

Matrice de criticité (en rouge zone inacceptable)

Gravité Fréquence	Catastrophique (4)	Critique (3)	Marginal (2)	Insignifiant (1)
Fréquent (A)				
Probable (B)				
Occasionnel (C)				
Rare (D)				
Improbable (E)				
Invraisemblable (F)				

Niveaux de sécurité comparés des transports

73



Niveaux de sécurité comparés des transports

74

