Sûreté de fonctionnement

Nicolae Brînzei

2022-2023

Sûreté de fonctionnement

Objectifs

- introduction des concepts fondamentaux de la SdF
- montrer à tout ingénieur que la défaillance d'un système n'est pas une fatalité et qu'il est souvent possible d'en évaluer sa probabilité

Prérequis

- probabilités et statistiques
- théories et modèles des systèmes à événements discrets (SED): algèbre de Boole, modèles à états-transitions (automates à états finis, réseaux de Petri)

Programme

- concepts et définitions
- fiabilité des composants
- méthodes qualitatives de la SdF : APR, AMDE, AMDEC, HAZOP, …
- approches d'évaluation combinatoires : diagrammes de fiabilités, arbres des défaillances
- approches d'évaluation basées sur l'espace d'états : processus stochastiques (chaînes de Markov), réseaux de Petri stochastiques
- approches orientées simulation : les SAN (Stochastic Activity Networks)
- sécurité fonctionnelle et systèmes instrumentés de sécurité (SIS) norme IEC 61508, niveau SIL

Savoir-faire et compétences acquises

Savoir analyser et évaluer les paramètres de sûreté de fonctionnement d'un système

Sûreté de fonctionnement

Concepts et définitions.
Fiabilité des composants

Sûreté de fonctionnement. Définitions

- au sens le plus large, **la sûreté de fonctionnement (SdF, dependability)** est

LA « SCIENCE » DES DEFAILLANCES

- étapes :
  - **identifier** les défaillances et de manière aussi exhaustive que possible
  - ensuite pour chacune des défaillances, il conviendra d'en **évaluer** l'importance par rapport aux autres (on parlera de *niveaux de risque*) ou avec une échelle de mesure absolue (en calculant *une probabilité d'apparition*)
  - **prévoir** les défaillances est aussi un objectif essentiel ; ainsi, on doit observer et utiliser des modèles d'évolution
  - à toute observation d'une défaillance, on associera des **mesures** (statistiques - rendement) afin d'enrichir les modèles utilisés pour l'évaluation et la prévision
  - enfin, l'ultime objectif est de **maîtriser** les défaillances par la réduction de leur occurrence, la prévention contre les conséquences ou par leur tolérance

Sûreté de fonctionnement. Définitions

Il existe des définitions plus strictes de la sûreté de fonctionnement, retenons celle-ci assez couramment utilisée et qui est proposée dans la norme du vocabulaire de la sûreté de fonctionnement [CEI 50 (191)]

APTITUDE D'UNE ENTITE A ASSUMER UNE OU PLUSIEURS FONCTIONS REQUISES DANS DES CONDITIONS DONNEES

Cette notion très générale et non quantitative, peut être caractérisée par un certain nombre d'attributs :

- entraves à la sûreté de fonctionnement
- moyens d'obtention de la SdF
- moyens de validation
- mesures de la SdF

Afin de préciser l'extension de la sûreté de fonctionnement, il convient de définir avec précision certains mots apparus dans les définitions précédentes (mots soulignés).

Sûreté de fonctionnement. Définitions

Défaillance (Failure)

- C'est un **événement**. Un événement est présent ou non, il peut se combiner avec d'autres événements pour produire des événements composés. Une partie de l'étude des défaillances relève donc du domaine de l'algèbre des événements et de la théorie des systèmes à événements discrets.

- une défaillance est : **la cessation de l'aptitude d'une entité à accomplir une fonction requise**

Cela amène naturellement à la nécessité de définir la fonction et le critère de cessation de celle-ci et bien sûr à établir une classification des défaillances.

Entité (Item, entity)

- Selon les mêmes références, une entité peut être considérée comme :

  tout élément, composant, sous système, unité fonctionnelle, équipement ou système que l'on peut considérer individuellement

- une entité peut être constituée d'éléments matériels (technologies de toute nature), d'éléments immatériels (logiciels, calculs…), d'éléments vivants (plantes, bactéries…) et bien sûr d'hommes (opérateurs, utilisateurs…) ou de toute combinaison de ces éléments
- la SdF s'applique donc à de nombreux domaines : électricité, électronique, contrôle-commande, thermo-hydraulique, mécanique, informatique, l'organisation des entreprises…
- un ensemble d'entités peut aussi être considéré comme une entité

Exemple de classification à EDF :

pièce $\subset$ composant $\subset$ sous-système $\subset$ système élémentaire $\subset$ système

Entité (Item, entity)

- la frontière permettant de définir l'appartenance à tel ou tel niveau d'entité peut être définie différemment selon la connaissance interne que l'on a ou pas de l'entité
- les relations entre entités seront rigoureusement définies en termes de localisation, de connexions ou d'interdépendance, afin notamment de rechercher les conséquences de leur défaillances les une sur les autres ; chaque entité possède donc une interface qui défini ces relations

Sûreté de fonctionnement. Définitions

Fonction requise

- fonction ou ensemble de fonctions d'une entité dont l'accomplissement est considéré comme nécessaire pour la fourniture d'un service donné
- on parle aussi de mission
- on caractérisera donc les fonctions ou missions d'une entité par leur nombre, leur degré d'importance (principales, secondaires, …) et leurs dépendances

Sûreté de fonctionnement. Définitions

Fonction requise

Relativement à sa (ses) fonction(s), on définit l'état d'une entité :

1. état de fonctionnement (operating state)
2. état de non fonctionnement (non operating state)
3. état de disponibilité (upstate) cf. disponibilité
4. état d'indisponibilité (downstate) (entretien, panne)
5. état d'attente (standby state)
6. état vacant (libre) - idle (free) state
7. état d'incapacité (disabled state - outage) = inaptitude (quelle qu'en soit la raison)

Sûreté de fonctionnement. Définitions

Classification des défaillances

- il existe de nombreux critères de classification, en fonction de leur importance, de la rapidité de leur apparition, de l'instant de leur occurrence, de leurs causes, de leurs effets
- par **la rapidité de manifestation** :
  - défaillance progressive : due à l'évolution dans le temps des caractéristiques (on peut la prévoir)
  - défaillance soudaine : non prévisible.
- par **l'importance** :
  - défaillance partielle : il n'y a pas disparition de toutes les fonctions
  - défaillance complète : inaptitude totale vis à vis de toutes les fonctions
  - défaillance pertinente : interprétation ou calculs
  - défaillance non pertinente : n'entraîne pas d'interprétation ou de calculs

Sûreté de fonctionnement. Définitions

Classification des défaillances

- **par la rapidité et l'importance** :
  - défaillance catalectique : soudaine et complète
  - défaillance par dégradation : progressive et partielle (peut devenir complète)
- **par le type de manifestation** :
  - défaillance systématique : se produisant chaque fois que l'entité est mise dans les mêmes conditions
  - défaillance aléatoire : apparaissant de façon aléatoire lorsque l'entité se trouve dans un état de disponibilité
- **par la date d'apparition** :
  - défaillance précoce (ou de jeunesse) : le taux d'apparition baisse
  - défaillance par vieillissement (usure) : le taux d'apparition augmente

Sûreté de fonctionnement. Définitions

Classification des défaillances

- **par les effets** :
  - défaillance mineure (bénigne) : dommage négligeable au système, pas de risque humain
  - défaillance significative : dommages significatifs au système, pas de risque humain
  - défaillance critique : dommages importants au système mais négligeables aux hommes ou à l'environnement
  - défaillance catastrophique : dommages importants au système, et aux hommes ou à l'environnement

Sûreté de fonctionnement. Définitions

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

➔ Nécessité de rechercher les causes des défaillances.

Cause des défaillances

- la défaillance d'une entité est la conséquence de l'imperfection de celle-ci (imperfection intrinsèque ou due à celle de ses composants)
- une entité imparfaite est une entité qui contient des erreurs (ou imperfections)
- rechercher les causes de défaillance d'une entité, c'est donc chercher les causes de la présence de ces erreurs
- les erreurs peuvent être dues à de nombreuses causes :
  - faute de conception ou d'utilisation : les défaillances systématiques des logiciels dues à des erreurs de spécification, de conception …
  - action de l'environnement
  - défaillance d'un sous ensemble, composant …
- ces causes peuvent être :
  - accidentelles
  - intentionnelles
  - permanentes
  - temporaires

Cause des défaillances

- l'action de l'environnement, ou d'un sous ensemble est comparable à celle du concepteur ou de l'utilisateur ➔ le terme de **FAUTE** peut donc être généralisé (l'intérêt de cette notion est de mieux correspondre à l'anglais FAULT que le terme français « panne »)
- le schéma suivant caractérise le processus d'apparition des défaillances :

FAUTE ➔ ERREUR ➔ DEFAILLANCE

Un ingénieur commet une faute dans la conception d'un composant. Lorsque le composant est inséré dans un système, il y a alors présence d'une erreur qui produira une défaillance du composant à la sollicitation. Cette défaillance peut alors être considérée comme l'injection d'une faute dans le système qui contient ce composant qui recèle alors lui-même une erreur qui entraînera à son tour le moment venu une défaillance du système.

- faute et défaillance sont des événements, erreur est un état ; on parle généralement de **latence d'erreur** pour la durée de cet état

Sûreté de fonctionnement. Définitions

Cause des défaillances

- la notion de **PANNE** est souvent présentée comme **l'état de l'entité après l'apparition de sa défaillance** ; c'est une conséquence de sa défaillance (à rapprocher plutôt de l'état d'indisponibilité définissant la panne comme l'inaptitude d'une entité à accomplir une fonction requise).

On voit pourquoi il y a souvent assimilation de **faute + erreur** avec **panne**.

Sûreté de fonctionnement. Définitions

Classification des fautes

- on peut classifier les fautes :

-Accidentelle	- Intentionnelle
- Physique	- Humaine
- Interne	- Externe
- Active (qui produit une erreur)	- Dormante (qui ne produit pas d'erreur
- Douce	- Dure
- Permanente	- Temporaire (transitoire)
- Opérationnelle, ou par opposition : de conception	

- certaines de ces classes peuvent être subdivisées, de plus, elles ne s'excluent pas forcément
- par exemple, une erreur humaine peut être de conception, de fabrication ou d'utilisation (mauvais emploi, fausse manœuvre, etc.)

Sûreté de fonctionnement. Définitions

Classification des fautes

Remarque : Lorsque la notion de panne est utilisée de préférence aux notions d'erreur et de fautes, les pannes reçoivent alors les qualificatifs que nous avons attribué aux fautes ou aux défaillances (défaillance complète → panne complète).

Sûreté de fonctionnement. Définitions

En résumé, **la sûreté de fonctionnement** peut être vue comme étant le traitement des fautes (s'attaquer aux sources des défaillances) ; elle regroupe les activités de :

- prévention des fautes : consiste à prévenir le concepteur, le fabricant, l'utilisateur, l'opérateur, le consommateur contre le risque lié aux diverses activités associées à une entité
- tolérance aux fautes : consiste à doter le système des moyens nécessaires à la continuité de la fonction ou du service en présence d'une faute (par la redondance en général)
- élimination des fautes : consiste à détecter la présence d'une faute avant qu'elle ne se manifeste par un danger et à la supprimer (réparation, maintenance, modification, reconception…),
- prévision des fautes : consiste à prévoir l'occurrence de défaillances liées à la présence des fautes dans un système, en particulier par le calcul probabiliste qui permet d'évaluer le risque conséquent

Composantes de la sûreté de fonctionnement

Fiabilité (reliability)

• à l'origine (1960) la fiabilité était à elle seule la sciences des défaillances

• traduction de l'anglais « reliability », ce mot (entré au dictionnaire en 1962) a été construit à partir du mot « fiable » : en qui on peut se fier

Définition

Aptitude d'une entité à accomplir une fonction requise dans des conditions données, pendant une durée donnée.

Mesure

La fiabilité se mesure par la probabilité qu'entité E accomplisse une fonction requise dans les conditions données pendant l'intervalle de temps [0,t] (ou encore [t1,t2] comme dans la norme CEI 50(191)).

R (t) = P [E soit non défaillante sur [0,t]]

ou **R (t1,t2) = P [E soit non défaillante sur [t1,t2]]**

L'aptitude contraire 1 - R(t) est la probabilité de défaillance de l'entité quelquefois appelée **défiabilité.**

Composantes de la sûreté de fonctionnement

Fiabilité (reliability)

Evaluation

L'évaluation de cette probabilité peut être faite différemment selon la nature des entités considérées ou selon les moyens dont on dispose pour le faire.

• la fiabilité **opérationnelle** (observée) résulte de l'observation et de l'analyse du comportement d'entités identiques dans des conditions opérationnelles

• la fiabilité **extrapolée** qui résulte d'une extension (par extrapolation définie ou par interpolation) de la fiabilité opérationnelle à des durées ou des conditions différentes

• la fiabilité **prévisionnelle** (prédite) qui estime une fiabilité future d'une entité à partir de considérations sur la conception de cette entité et la fiabilité de ses composants. La fiabilité prévisionnelle fera l'objet de plusieurs chapitres de ce cours.

• la fiabilité **intrinsèque** est mesurée au cours d'essais spécifiques sur l'entité, effectués dans le cadre d'un programme d'essais entièrement défini

Mainténabilité (maintenability)

Définition

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 E, 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 zéro soit réparée à l'instant t]

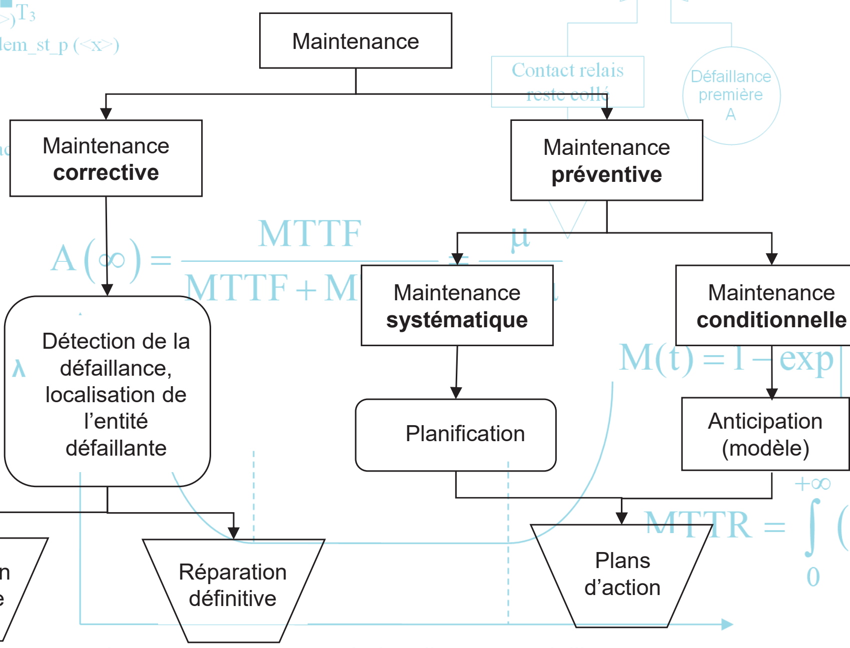
ou **M (t1,t2) = P [E défaillante à t = t1 soit réparée à t = t2]**

Composantes de la sûreté de fonctionnement

Mainténabilité (maintenability)

Evaluation

L'évaluation de cette probabilité est liée à la manière dont est effectuée la remise en état de fonctionnement de l'entité. Il existe différents types de maintenance :



Composantes de la sûreté de fonctionnement

Mainténabilité (maintenability)

Evaluation

- la **maintenance corrective** intervient après la défaillance constatée de l'entité
- la **maintenance différée** consiste à retarder la réparation des entités qui ne mettent pas en jeu le fonctionnement optimal d'un système constitué de multiples entités (pour attendre par exemple le prochain arrêt)
- la **maintenance préventive** programmée ou non programmée des entités les plus critiques consiste à les réparer (voire les remplacer) dès qu'elles manifestent des signes de fatigue, c'est la **maintenance conditionnelle**, ou dès que leur fiabilité estimée devient insuffisante, c'est la **maintenance systématique**

La politique de maintenance adoptée, son éventuelle optimisation selon différents critères (disponibilité, coût, stocks de rechange…), ont un impact direct sur la sûreté de fonctionnement globale d'un système

La terminologie de la maintenance est définie dans différentes normes comme par exemple les normes françaises NF X60-000, NF X60-010, NF X60-011, NF X60-015 et NF X60-020.

Composantes de la sûreté de fonctionnement

Disponibilité (Availability)

Définition

C'est l'aptitude d'une entité à être en état d'accomplir une fonction requise dans des conditions données et à un instant donné.

Mesure

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

A (t) = P [entité non défaillante à l'instant t]

- cette caractéristique est appelée disponibilité instantanée
- la notion contraire est appelée **indisponibilité (unavailability)** notée U(t)
- 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)
- 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)

Composantes de la sûreté de fonctionnement

Sécurité (safety)

Définition

La norme CEI 50 (191) n'intègre pas la sécurité comme composante de la sûreté de fonctionnement qu'elle restreint aux seules fiabilité, maintenabilité et disponibilité (FMD ou en anglais RAM).

La norme EN 292 sur la sécurité des machines donne cette définition :

« Aptitude d'une machine à accomplir sa fonction, à être transportée, installée, mise au point, entretenue, démontée et mise au rebut dans les conditions d'utilisation normales spécifiées dans la notice d'instructions, sans causer de lésions ou d'atteinte à la santé. »

Selon les lois, la sécurité s'applique aux risques d'atteinte physique aux personnes et plus récemment aux atteintes à l'environnement. Selon l'IEC 61508, la sécurité est définie par l'absence de risque inacceptable.

C'est la sécurité des personnes, en anglais **« safety »**.

On constate une certaine ambiguïté entre les mots sécurité et sûreté en français d'une part et les mots safety et security en anglais d'autre part.

Composantes de la sûreté de fonctionnement

Sécurité (safety)

C'est pourquoi en français, on parle de **« Sécurité innocuité » (safety)** : aptitude d'une entité à éviter de faire apparaître des événements critiques ou catastrophiques c.à.d. pouvant affecter les personnels et les équipements. Une telle entité est dite à **sûreté intégrée** ou de **sécurité intrinsèque** (**fail safe**).

Définition

Le terme anglais **« security »** correspond pour [Laprie] à la **« sécurité confidentialité »** : aptitude d'une entité à la préservation de la confidentialité et de l'intégrité des informations.

Composantes de la sûreté de fonctionnement

Sécurité (safety)

Mesure

La sécurité-innocuité :

- doit vérifier que le comportement du système respecte toutes les exigences de sécurité (empêcher des comportements dangereux ou illégaux, *e.g.* une sollicitation du système de commande ne peut pas avoir lieu dans un état incompatible avec cette commande)
- peut également s'exprimer sous forme d'une probabilité d'évitement d'une situation dangereuse ou catastrophique (la sécurité fonctionnelle par exemple doit être évaluée quantitativement par la probabilité de défaillance dangereuse d'un système chargé d'assurer une fonction de sécurité sur une installation)

Evaluation

- les exigences de sécurité sont évaluées qualitativement par des méthodes formelles
- la probabilité d'évitement d'une situation dangereuse est évaluée quantitativement par des approches stochastiques

Composantes de la sûreté de fonctionnement

Sécurité (safety)

Par rapport à la sécurité-innocuité les défaillances peuvent être classifiées en :

- **défaillances sûres (safe failures)** qui n'entraînent pas des dommages critiques pour l'homme ou pour l'environnement
- **défaillances dangereuses (dangerous failures)** qui entraînent des dommages critiques ou catastrophiques pour l'homme ou pour l'environnement

D.p.d.v. du diagnostic les défaillances peuvent être classifiées en :

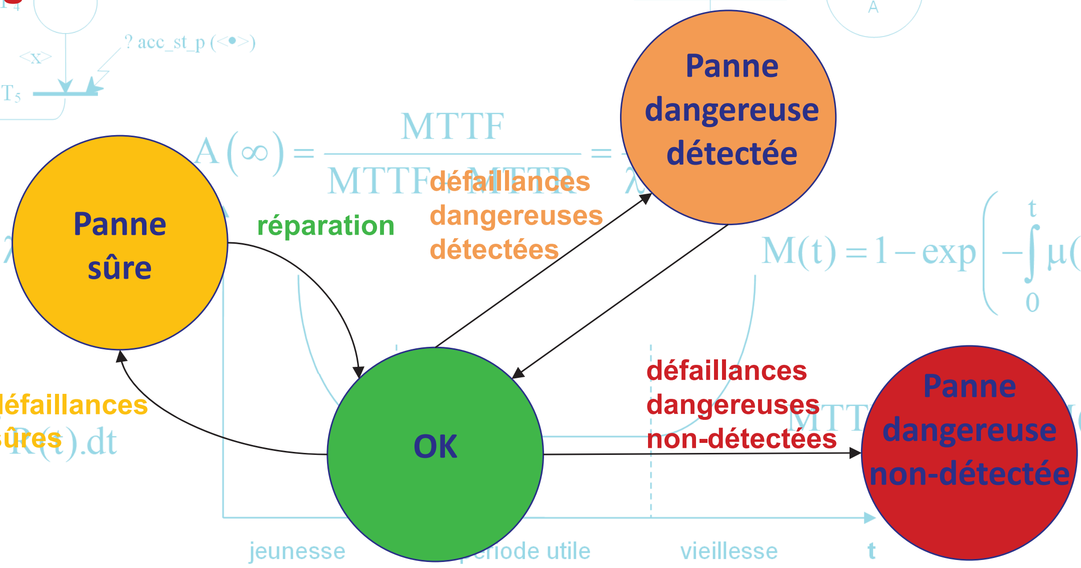
- **défaillances détectées** qui peuvent être détectées par un système de diagnostic
- **défaillances non-détectées** qui ne peuvent pas être détectées (absence d'un système de diagnostic ou impossibilité physique ou technique de détection)

Composantes de la sûreté de fonctionnement

Sécurité (safety)

4 classes d'états du système :

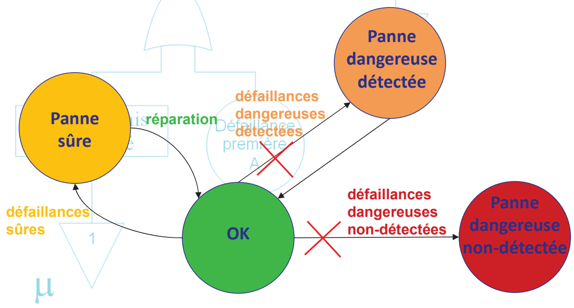
- **états sûrs et système disponible**
- **états sûrs et système non disponible**
- **états dangereux détectés, système non-disponible**
- **états dangereux non-détectés**



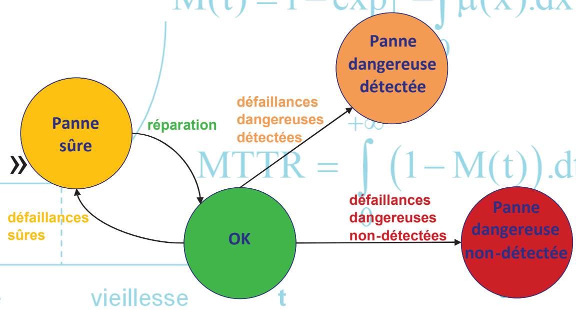
Composantes de la sûreté de fonctionnement

Sécurité (safety)

- les exigences de sécurité doivent montrer formellement qu'***aucun état de panne dangereuse n'est atteignable*** (les croix rouges traduisent les transitions dont il est nécessaire de prouver l'inexistence) soit par l'action d'un système instrumenté de sécurité (SIS - Safety Instrumented System) après détection d'une défaillance dangereuse, soit par rendre impossible des défaillances dangereuses non-détectées (par ré-conception, par exemple)



- la probabilité de ne pas attendre un état dangereux s'évalue comme ***la probabilité de rester dans les états sûrs*** (états « OK » ou de panne sûre)

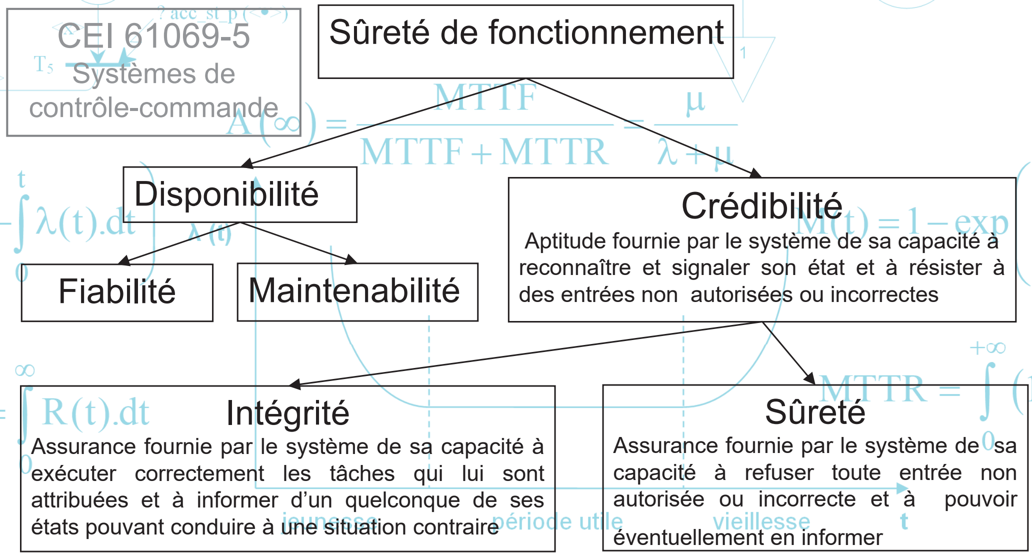


Composantes de la sûreté de fonctionnement

Intégrité, crédibilité

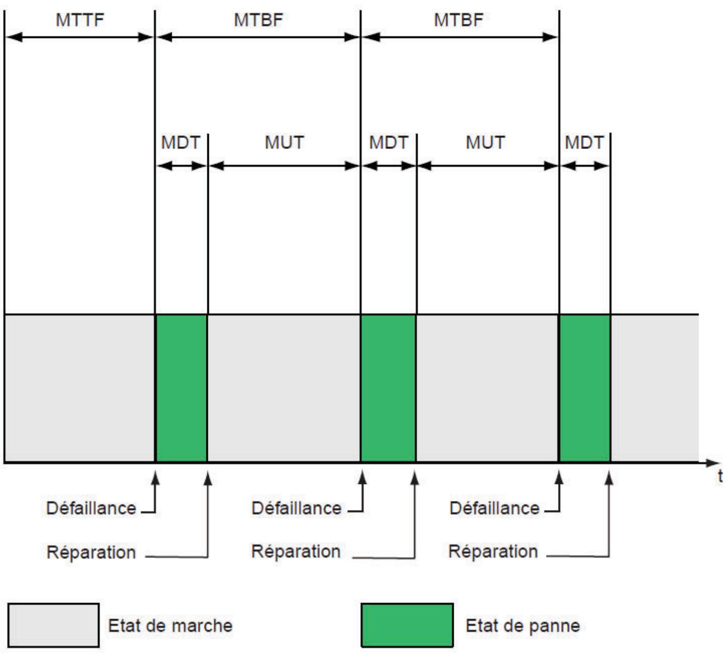
Définition

La norme 61069-1 partie 5 relative aux systèmes de contrôle-commande des installations industrielles, donne les mêmes définitions de la FMD, mais considère que la sûreté de fonctionnement dépend aussi de la crédibilité, elle-même décomposée en intégrité et sûreté, cette dernière se rapprochant de la notion de sécurité confidentialité précédemment évoquée.



Les temps caractéristiques pour la SdF

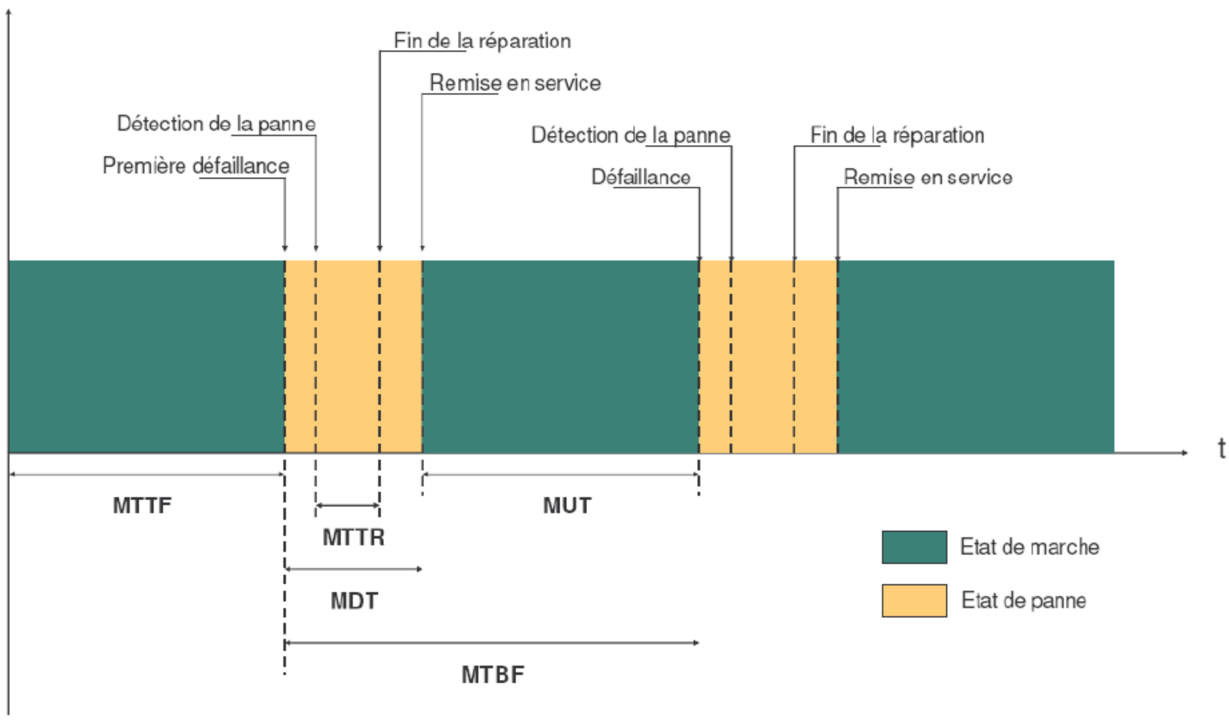
- les grandeurs caractérisant la SdF sont d'abord les durées de fonctionnement: avant défaillance, entre défaillances, entre défaillance et réparation, etc...
- ces temps dépendent des probabilités d'occurrences des divers événements défaillances, réparations, ce sont des variables aléatoires que l'on cherche à caractériser par leur espérance mathématique



Les temps caractéristiques pour la SdF

- **MTTFF (mean time to first failure) ou MTTF (mean time to failure) :** durée moyenne de fonctionnement avant la première défaillance, espérance mathématique de la durée de fonctionnement avant la première défaillance
- **MTBF (mean time between failures) :** durée moyenne entre deux défaillances consécutives d'une entité réparable
- **MUT (mean up time)** ou TMD (temps moyen de disponibilité) : durée moyenne de bon fonctionnement après réparation, espérance mathématique de la durée de disponibilité
- **MDT (mean down time)** ou TMI (temps moyen d'indisponibilité) : durée moyenne de défaillance comprenant la détection de la panne, la durée d'intervention, la durée de la réparation et la durée de la remise en service, espérance mathématique de la durée d'indisponibilité
- **MTTR (mean time to repair) :** durée moyenne de la panne ou moyenne des temps pour la remise en état de fonctionnement, espérance mathématique de la durée de panne

Les temps caractéristiques pour la SdF



Grandeurs caractéristiques de la fiabilité

Fonction de répartition

Soit T la variable aléatoire mesurant **la durée de fonctionnement de l'entité avant défaillance** (on dit parfois durée de vie mais cela ne s'applique qu'aux entités non réparables).

La fonction de répartition de T s'écrit : F(t) = P(T ≤ t)

avec $\lim_{t \to 0} F(t) = 0$ et $\lim_{t \to \infty} F(t) = 1$

Or par définition :

R(t) = P(T > t) (rappel : probabilité pour que l'entité soit non défaillante sur [0,t])

➔ F(t) = 1- R(t) = $\bar{R}(t)$ et R(0)=1, R(∞)=0

La fonction de répartition de T est égale à la probabilité de défaillance ou la défiabilité de l'entité.

Grandeurs caractéristiques de la fiabilité

Densité de probabilité ou fonction de distribution

La densité de probabilité f(t) de la variable continue T ou encore fonction de distribution est définie par la relation :

$$F(t) = \int_{-\infty}^{t} f(u).du$$ où F(t) est sa fonction de répartition

D'après la norme, d'une manière générale :

$$f(t) = \lim_{\Delta t \to 0} \frac{F(t+\Delta t) - F(t)}{\Delta t}$$

La densité de probabilité de défaillance de l'entité (plus exactement de la variable T) est la dérivée de la fonction de répartition F(t) dans les domaines où elle est continue :

$$f(t) = \frac{dF(t)}{dt} = \frac{d\bar{R}(t)}{dt} = -\frac{dR(t)}{dt} \qquad \int_{-\infty}^{\infty} f(u).du = 1$$

f(t) dt est la probabilité que la défaillance de l'entité intervienne entre t et t + dt

f(t) dt = P [t < T ≤ t+dt]

LORRAINE INP Ensem

Grandeurs caractéristiques de la fiabilité

Taux instantané de défaillance

Contrairement à la densité de probabilité de défaillance (qui correspond à une probabilité à priori), le taux de défaillance s'apparente à la probabilité conditionnelle de défaillance sur]t, t+ dt] sachant que l'entité n'a pas de défaillance sur [0,t].

Définition (selon [CEI 50 (191)])

On appelle taux instantané de défaillance la limite, si elle existe, du quotient de la probabilité conditionnelle pour que l'instant T de défaillance d'une entité, soit compris dans l'intervalle de temps [t, t+Δt], par la durée Δt de l'intervalle de temps lorsque celui-ci tend vers zéro, en supposant que l'entité n'a pas eu de défaillance sur [0,t].

$$\lambda(t) = \lim_{\Delta t \to 0} \frac{1}{\Delta t}.P[t < T \leq t + \Delta t / T > t]$$

Conséquence

Cela signifie que $\lambda(t)$ dt est la probabilité conditionnelle de défaillance sur]t, t + dt] sachant que l'entité n'a pas eu de défaillance sur [0,t].

LORRAINE INP Ensem

Grandeurs caractéristiques de la fiabilité

Taux instantané de défaillance

Démonstration

Etablissons les relations entre $\lambda(t)$, R(t) et f(t) :

D'après le théorème des probabilités conditionnelles, on a donc :

$$\lambda(t).dt = \frac{P[(t < T \leq t + dt) \cap (T > t)]}{P[T > t]}$$

T > t étant inclut dans l'événement t < T < t + dt, et P[T > t] étant la définition de R(t), on a :

$$\lambda(t).dt = \frac{P[t < T \leq t + dt]}{R(t)}$$

or : P[t < T ≤ t+dt] = f(t) dt

f(t) étant la fonction de distribution ou densité de probabilité

d'où : $\lambda(t) = \dfrac{f(t)}{R(t)} = \dfrac{-\dfrac{dR(t)}{dt}}{R(t)}$ $\lambda(t) \geq 0$ car $f(t) \geq 0$

Grandeurs caractéristiques de la fiabilité

Taux instantané de défaillance

$$\lambda(t) = -\frac{d}{dt}\left(\log\left(R(t)\right)\right)$$

En intégrant les deux membres de 0 à t, sachant que R(0) = 1 :

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

Grandeurs caractéristiques de la fiabilité

Evaluation statistique de R (t), f(t) et λ(t)

- considérons maintenant une population de N_0 entités ayant la même fonction de distribution des instants de défaillance
- la variable aléatoire discrète N(t), nombre d'entités non défaillantes à l'instant t, possède une distribution binomiale. (N_0 est le nombre d'épreuves, une épreuve est la non-apparition de la défaillance d'une entité à l'instant t avec la probabilité R(t) ou l'apparition d'une défaillance à ce même instant avec la probabilité 1-R(t))

$$P\left[N(t) = n\right] = C_{N_0}^{n}\left(R(t)\right)^{n} - \left(1 - R(t)\right)^{N_0 - n}$$

Soit :
$$P\left[N(t) = n\right] = \frac{N_0!}{n!(N_0 - n)!}\left(R(t)\right)^{n} - \left(1 - R(t)\right)^{N_0 - n}$$

N(t) a pour espérance mathématique (moyenne) que nous noterons n(t)

$$E(N(t)) = n(t) = N_0 R(t)$$

on a donc :
$$R(t) = \frac{n(t)}{N_0}$$

On montre ainsi que **la fiabilité est le rapport du nombre moyen d'entités non défaillantes au temps t sur le nombre initial d'entités**.

MTTF et fiabilité

T étant défini comme la durée de fonctionnement avant défaillance, le MTTFF de l'entité correspondante est donc son espérance mathématique :

$$\mathrm{MTTFF} = \int_{-\infty}^{+\infty} t.f(t).dt$$

la variable t étant toujours positive, l'intervalle d'intégration est réduit à [0, +∞(

$$\mathrm{MTTFF} = \int_{0}^{+\infty} t.\frac{dR(t)}{dt}.dt$$

que l'on peut intégrer par parties :

$$\mathrm{MTTFF} = \int_{0}^{+\infty} R(t).dt - \left[t.R(t)\right]_0^{\infty}$$

pour t = 0 : R (t) = 1 et t R (t) = 0

pour t = ∞ : $\lim_{t\to\infty} t.\exp\left(-\int_0^t \lambda(x).dx\right) = 0$ si $\lambda(t) \neq 0$

$$\mathrm{MTTFF} = \int_{0}^{\infty} R(t).dt$$

MTTF et fiabilité

Si on sait calculer la transformée de Laplace R(s) de R(t), alors :

$$L\left[\int_0^t R(x).dx\right] = \frac{R(s)}{s}$$

d'après le théorème de la valeur finale :

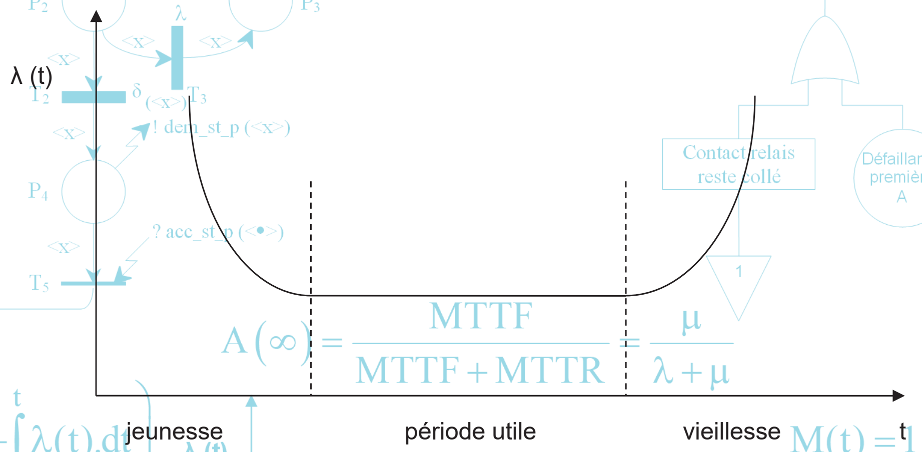
$$\mathrm{MTTF} = \lim_{t\to\infty}\int_0^t R(x).dx = \lim_{s\to 0} s.L\left[\int_0^t R(x).dx\right] = \lim_{s\to 0} s.\frac{R(s)}{s}$$

$$\mathrm{MTTF} = \lim_{s\to 0} R(s)$$

Grandeurs caractéristiques de la fiabilité

Application aux principales lois de probabilité

Généralement, la loi de variation du taux de défaillance λ(t) évolue dans le temps suivant trois périodes :



Courbe en baignoire

Grandeurs caractéristiques de la fiabilité

Application aux principales lois de probabilité

- **La période de jeunesse où λ(t) diminue très rapidement avec t.** Pour garantir un niveau de fiabilité suffisant, un fabriquant de matériels est souvent amené à vieillir artificiellement ses matériels avant de les livrer. C'est par exemple le « déverminage » (ou « burn-in ») des produits électroniques (fonctionnement accéléré aux limites des grandeurs d'influence : température, hygrométrie, vibrations…).

- **La période utile où λ(t) varie peu.**

- **La période de vieillesse où λ(t) augmente de plus en plus vite avec t** avant ou au début de laquelle il convient de remplacer le composant âgé par un composant neuf (maintenance préventive).

Le problème posé aux fiabilistes est donc d'abord de modéliser chacune de ces phases par des lois de probabilité connues. La plupart des lois de probabilité sont utilisées en fiabilité pour modéliser λ(t) et calculer les MTTF.

Grandeurs caractéristiques de la fiabilité

Application aux principales lois de probabilité

La loi exponentielle

La loi exponentielle représente correctement la distribution des durées de vie lorsque :

- les défaillances sont indépendantes et imprévisibles, et dont la génération obéit à un processus de Poisson
- le taux de défaillance est constant et égal à λ.

C'est le cas des composants électroniques en période utile de fonctionnement.

Cette loi est caractérisée par les relations suivantes :

$$\lambda(t) = \lambda = \text{constante}$$

$$f(t) = \frac{-dR(t)}{dt} = \lambda e^{-\lambda t}$$

$$F(t) = 1 - e^{-\lambda t}$$

$$\text{MTTF} = \int_0^\infty R(t)\,dt = \int_0^\infty e^{-\lambda t}\,dt = \frac{1}{\lambda}$$

$$R(t) = 1 - F(t) = e^{-\lambda t}$$

Ce modèle est le plus utilisé car il permet une simplification pour le calcul de la fiabilité de systèmes composés de nombreuses entités différentes.

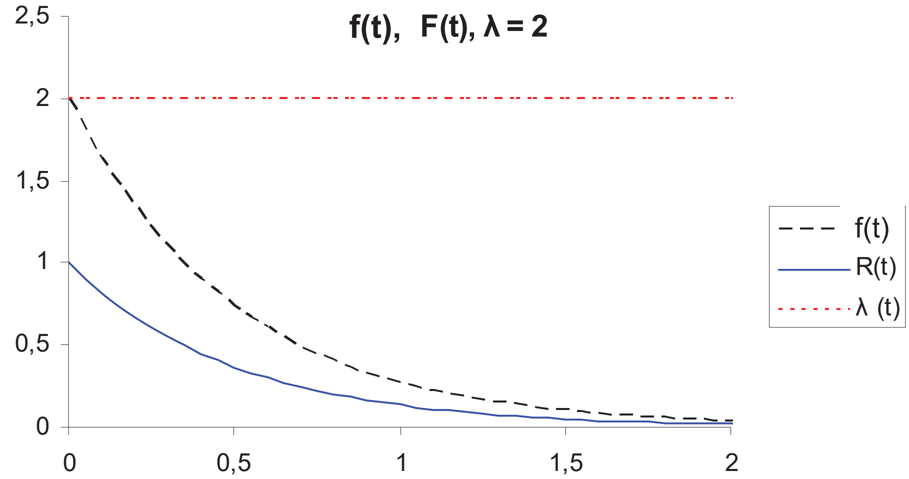
En outre, **le passé de tels systèmes n'affecte pas leur évolution future**.

Grandeurs caractéristiques de la fiabilité

Application aux principales lois de probabilité

La loi exponentielle

Exemple



Grandeurs caractéristiques de la fiabilité

Application aux principales lois de probabilité

La loi normale

Elle convient aux composants usés dont le taux de défaillance augmente avec t.

En effet, cette loi s’applique pour des systèmes dont les caractéristiques fonctionnelles sont altérées par un nombre important de causes indépendantes agissant de manière additive.

C’est le cas par exemple pour les durées de vie liées à l’usure de matériels mécaniques, nombre de charges/décharges supportables par des accumulateurs…

Cette loi est caractérisée par les relations suivantes :

$$f(t) = \frac{1}{\sigma\sqrt{2\pi}} \exp\left(-\frac{1}{2}\left(\frac{t-\mu}{\sigma}\right)^2\right)$$

$$\lambda(t) = \frac{\exp\left(-\frac{1}{2}\left(\frac{t-\mu}{\sigma}\right)^2\right)}{\int_t^{\infty} \exp\left(-\frac{1}{2}\left(\frac{x-\mu}{\sigma}\right)^2\right)dx}$$

$$R(t) = 1 - F(t) = 1 - \frac{1}{\sigma\sqrt{2\pi}} \int_{-\infty}^{t} \exp\left(\frac{-(t-\mu)^2}{2\sigma^2}\right)dt$$

$$MTTF = \mu$$

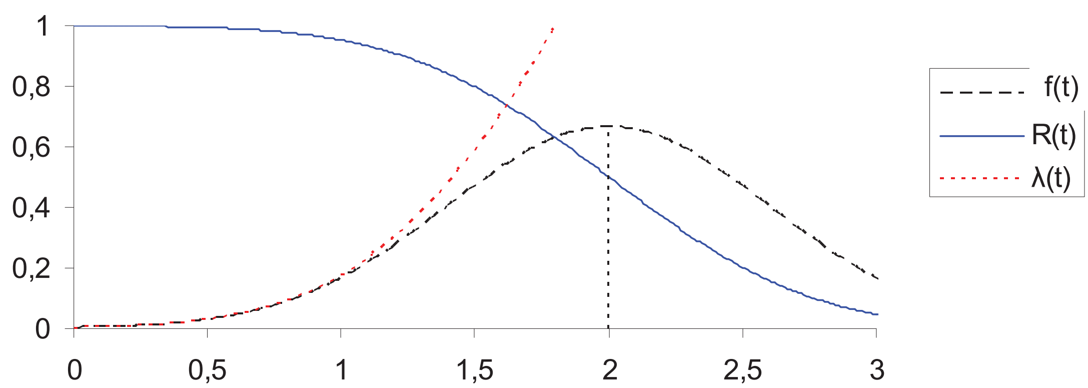
Grandeurs caractéristiques de la fiabilité

Application aux principales lois de probabilité

La loi normale

Exemple

f(t), F(t), λ(t) pour μ = 2 et σ = 0,6



Grandeurs caractéristiques de la fiabilité

Application aux principales lois de probabilité

La loi log-normale

Elle s'applique pour des systèmes dont les caractéristiques fonctionnelles sont influencées par un nombre important de facteurs indépendants agissant de manière multiplicative.

Cette loi s'applique particulièrement au cas de la durée de vie des matériaux travaillant en fatigue sous l'action répétée de contraintes mécaniques ou à la durée de vie de composants optoélectroniques tels que les diodes laser (en rapport avec la réduction progressive du pouvoir émissif).

Cette loi est caractérisée par les relations suivantes :

$$f(t) = \frac{1}{\sigma t\sqrt{2\pi}} \exp\left(-\frac{1}{2}\frac{(\log t-\mu)^2}{\sigma^2}\right) \qquad MTTF = \exp\left(\mu + \frac{\sigma^2}{2}\right)$$

$$R(t) = 1 - F(t) = 1 - \frac{1}{\sigma\sqrt{2\pi}}\int_0^t \frac{1}{t}\exp\left(-\frac{1}{2}\frac{(\log t-\mu)^2}{\sigma^2}\right)dt$$

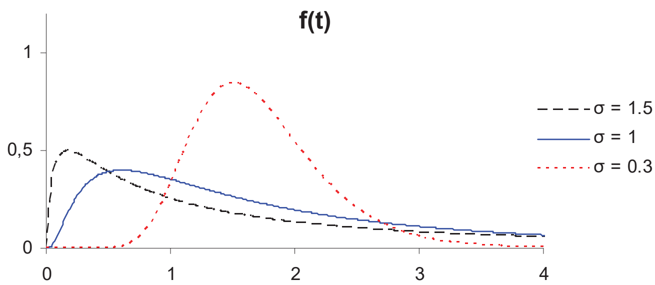
Grandeurs caractéristiques de la fiabilité

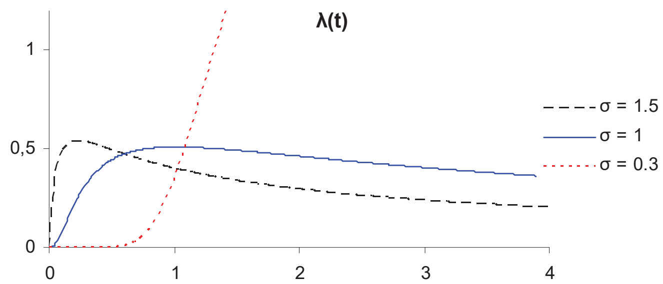
Application aux principales lois de probabilité

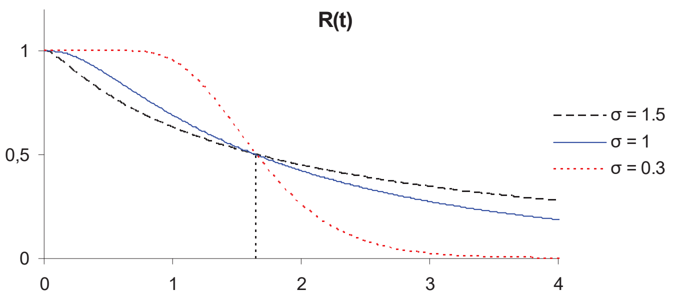
La loi log-normale

Exemple

loi lognormale pour μ=0.5 et plusieurs valeurs de σ.







Grandeurs caractéristiques de la fiabilité

Application aux principales lois de probabilité

La loi de Weibull

Elle est très utilisée pour les composants dont les taux de défaillance varient beaucoup (ex : mécanique).

Cette loi est caractérisée par la relation suivante :

$$f(t) = \frac{\beta(t-\gamma)^{\beta-1}}{\eta^{\beta}} \exp\left(-\left(\frac{t-\gamma}{\eta}\right)^{\beta}\right)$$

- pour $\beta < 1$, le taux de défaillance est décroissant avec le temps (rodage, pannes de jeunesse)
- pour $\beta = 1$, le taux de défaillance est constant et indépendant du temps (défauts aléatoires, loi exponentielle)
- pour $\beta > 1$, le taux de défaillance est croissant avec le temps (phénomène d'usure, par exemple pour des roulements, moteurs…)

Grandeurs caractéristiques de la fiabilité

Application aux principales lois de probabilité

La loi de Weibull

$$R(t) = 1 - F(t) = 1 - \left(1 - \exp\left(-\left(\frac{t-\gamma}{\eta}\right)^{\beta}\right)\right) = \exp\left(-\left(\frac{t-\gamma}{\eta}\right)^{\beta}\right)$$

$$MTTF = \gamma + \eta\Gamma\left(1 + \frac{1}{\beta}\right) \qquad \Gamma(a) = \int_0^{\infty} t^{(a-1)} e^{-t}\,dt$$

$$\lambda(t) = \frac{\beta(t-\gamma)^{\beta-1}}{\eta^{\beta}}$$

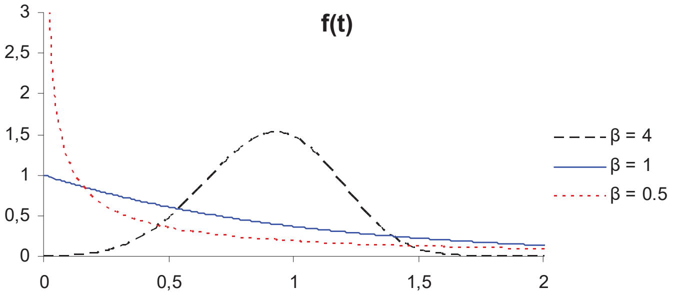
Grandeurs caractéristiques de la fiabilité

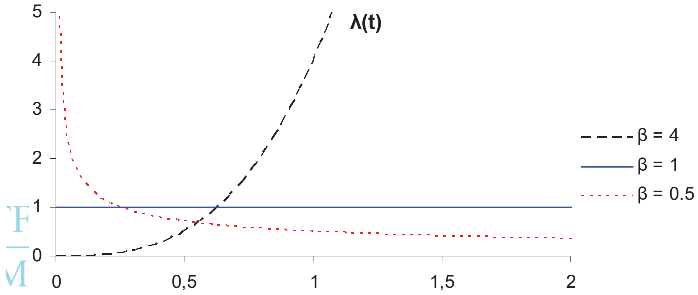
Application aux principales lois de probabilité

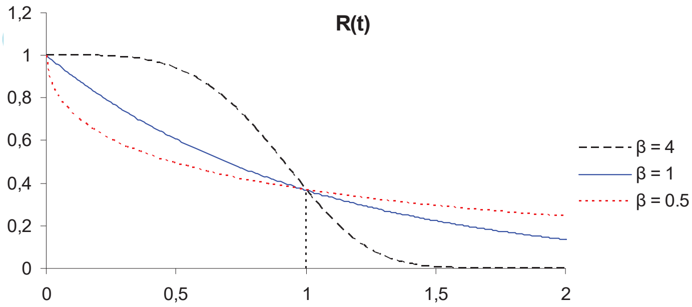
La loi de Weibull

Exemple

loi de Weibull η=1, γ=0 et μ=0.5 et plusieurs valeurs de β







Grandeurs caractéristiques de la fiabilité

Exercice

Soit un composant dont sa durée de vie (durée de fonctionnement avant la défaillance) est distribuée suivant une loi exponentielle de taux de défaillance $\lambda = 10^{-6}\ h^{-1}$.

Calculer le MTTF de ce composant et la valeur de la fiabilité R(MTTF). Qu'en concluez-vous ?

Un autre composant ayant la même fonctionnalité à son taux de défaillance $\lambda' = 10^{-7}\ h^{-1}$. Comparez les valeurs de la fiabilité de ces composants aux instants $t_1 = 10^4$ h et $t_2 = 10^6$ h.

Quelle est la probabilité de défaillance de ces composants à l'instant $t = 10^4$ h?

Grandeurs caractéristiques de la fiabilité

Exercice

Soit un composant dont sa durée de vie (durée de fonctionnement avant la défaillance) est distribuée suivant une loi de Weibull de paramètres $\eta=1.5*10^4$h, $\gamma=0$ et $\beta=2$.

1. Déterminer et représenter graphiquement l'évolution de la fiabilité et du taux de défaillance de ce composant. Déterminer et représenter graphiquement l'évolution de la probabilité de défaillance de ce composant.

2. Le processus de réparation mis en place par l'entreprise est caractérisé par un taux de réparation $\mu = 4*10^{-2}$ h^{-1}. Déterminer son MTTR. Calculer sa maintenabilité M_{10} et M_{500}. Représenter graphiquement l'évolution de la maintenabilité de ce composant.

3. Le processus de réparation est externalisé par l'entreprise, et dans ce cas il est caractérisé par une loi de Weibull de paramètres $\eta= 6.0*10^3$h, $\gamma=0$ et $\beta=1.8$. Déterminer et représenter graphiquement l'évolution de la maintenabilité et du taux de réparation du composant dans ce cas.

Comparer les deux politiques de maintenance.

Grandeurs caractéristiques de la maintenabilité

Fonction de répartition

La variable aléatoire est, dans le cas de la maintenabilité, **le temps T total de réparation** si l'entité est défaillante à t = 0.

$$F(t) = P[T \leq t] = M(t)$$

Il y a identité entre la fonction de répartition et la maintenabilité.

$$\lim_{t\to 0} F(t) = 0 \;\Rightarrow\; M(0) = 0$$

$$\lim_{t\to \infty} F(t) = 1 \;\Rightarrow\; M(+\infty) = 1$$

Grandeurs caractéristiques de la maintenabilité

Densité de probabilité ou fonction de distribution

D'après la norme CEI 50 (191) :

$$w(t) = \lim_{\Delta t \to 0} \frac{F(t+\Delta t) - F(t)}{\Delta t}$$

soit pour une fonction de répartition continue :

$$w(t) = \frac{dF(t)}{dt} = \frac{dM(t)}{dt}$$

$$w(t) = \frac{dM(t)}{dt}$$

w(t)dt est la probabilité pour que l'entité soit réparée entre t et t + dt

$$w(t)dt = P[t < T \leq t+dt]$$

Grandeurs caractéristiques de la maintenabilité

Taux de réparation

$\mu(t)$dt est la probabilité pour que l'entité soit réparée entre t et t + dt sachant qu'elle est encore en panne à l'instant t.

C'est la limite si elle existe, du quotient de la probabilité conditionnelle pour que l'instant T de réparation d'une entité soit compris entre t et t + Δt, par la durée de l'intervalle Δt lorsque celui-ci tend vers zéro, sachant que l'entité est restée en panne sur l'intervalle [0,t] (cf. à la norme CEI 50(191)).

$$\mu(t) = \lim_{\Delta t \to 0} \frac{1}{\Delta t} P\left[t < T \leq t+\Delta t / T > t\right]$$

par une démonstration identique à celle du taux de défaillance :

$$\mu(t) = \frac{\frac{dM(t)}{dt}}{1 - M(t)} \qquad \mu(t) \geq 0$$

et par conséquent :

$$M(t) = 1 - \exp\left(-\int_0^t \mu(x).dx\right) \qquad w(t) = \mu(t).\exp\left(-\int_0^t \mu(x).dx\right)$$

Grandeurs caractéristiques de la maintenabilité

MTTR et maintenabilité

Le MTTR étant l'espérance mathématique de la variable aléatoire T de densité de probabilité w, on a donc :

$$\mathrm{MTTR} = \int_0^{+\infty} t.w(t).dt$$

Soit :

$$\mathrm{MTTR} = \int_0^{+\infty} t.\frac{dM(t)}{dt}.dt$$

L'intégration par partie et les conditions aux limites donnent :

$$\mathrm{MTTR} = \int_0^{+\infty} \left(1 - M(t)\right).dt$$

Dans le cas d'une distribution exponentielle, le taux de réparation μ est constant et le MTTR est égal à l'inverse de μ.

$$\mathrm{MTTR} = \frac{1}{\mu}$$

Disponibilité d'une entité

Disponibilité asymptotique

- lorsque l'entité n'est pas réparable, sa disponibilité est égale à sa fiabilité
- lorsque l'entité est réparable, on peut écrire que la disponibilité d'une entité à l'instant t + dt est égale à la probabilité pour que l'entité soit disponible à t et qu'elle ne retombe pas en panne entre t et t + dt ou que l'entité, étant en panne à l'instant t, soit réparée à l'instant t + dt :

A (t + dt) = P[(E disponible à t et non défaillance sur]t, t + dt])
<u>OU</u> (E en panne à t et réparée sur]t, t + dt])]

Les deux cas étant complètements indépendants, cette probabilité est la somme des probabilités de chaque cas :

A (t + dt) = P[E disponible à t et non défaillante sur [t, t + dt]]
+ P [E en panne à t et réparée sur [t, t + dt]]

Disponibilité d'une entité

Disponibilité asymptotique

La disponibilité étant une probabilité à priori :

P[E disponible à t et non défaillante sur]t, t + dt]]

= P[E disponible à t] . P[E non défaillante sur [t, t + dt]].

On écrit la même chose pour le deuxième terme.

Si on se place dans le cas de distributions exponentielles où les taux de défaillance et de réparation sont constants (respectivement λ et μ) :

P[E disponible à t] = A(t) P[non défaillante sur [t, t+dt]] = 1-λ.dt

P[E non disponible à t] = 1-A(t) P[défaillante sur [t, t+dt]] = λ.dt

Disponibilité d'une entité

Disponibilité asymptotique

A (t + dt) = A (t).(1 - λdt) + (1 - A (t)).μdt

A (t + dt) = A (t) - (λ + μ) A (t) dt + μdt

$$\frac{dA(t)}{dt} = \mu - (\lambda + \mu).A(t)$$ équation différentielle dont la solution est :

$$A(t) = \frac{\mu}{\lambda+\mu} + \frac{\lambda A(0) - \mu(1 - A(0))}{\lambda+\mu}.e^{-(\lambda+\mu)t}$$

Supposons que A(0) = 1 (l'entité est disponible à l'instant t = 0) :

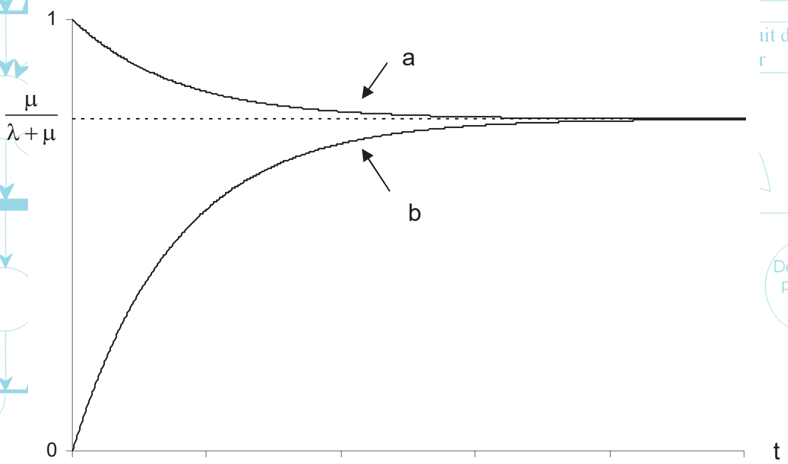
$$A(t) = \frac{\mu}{\lambda+\mu} + \frac{\lambda}{\lambda+\mu}.e^{-(\lambda+\mu)t}$$

Supposons que A (0) = 0 (l'entité est en panne à l'instant t = 0) :

$$A(t) = \frac{\mu}{\lambda+\mu} - \frac{\mu}{\lambda+\mu}.e^{-(\lambda+\mu)t}$$

Disponibilité d'une entité

Disponibilité asymptotique



Disponibilité d'une entité réparable
(a : démarrage en état de marche, b : démarrage en en état de panne)

Disponibilité d'une entité

Disponibilité asymptotique

Lorsque t→∞, les deux équations tendent vers $\frac{\mu}{\lambda+\mu}$

$$A(\infty)=\frac{\mu}{\lambda+\mu}=\frac{\frac{1}{MTTR}}{\frac{1}{MTTF}+\frac{1}{MTTR}}=\frac{MTTF}{MTTF+MTTR}$$

La disponibilité asymptotique est égale à la proportion du temps pendant lequel l'entité est en état de fonctionnement.

On a de même : $1-A(\infty)=\frac{\lambda}{\lambda+\mu}=\frac{MTTR}{MTTF+MTTR}$

Remarque

Généralement, MTTF >> MTTR

Grandeurs caractéristiques de la fiabilité

Exercice

Soit un composant dont sa durée de vie (durée de fonctionnement avant la défaillance est distribuée suivant une loi exponentielle de taux de défaillance $\lambda = 10^{-6}\ h^{-1}$.

Le processus de réparation mis en place par l'entreprise est caractérisé par un taux de réparation $\mu = 4*10^{-2}\ h^{-1}$.

1. Déterminer la disponibilité asymptotique de ce composant.
2. Représenter graphiquement l'évolution de sa disponibilité en fonction du temps sous l'hypothèse suivante.
   a. Le composant est disponible à l'instant initial.
   b. Le composant est indisponible à l'instant initial.

Sûreté de fonctionnement des systèmes

Analyse qualitative

- analyse préliminaire des risques, APR
- analyse des modes de défaillance, de leurs effets (et de leur criticité) AMDE(C)
- méthode HAZOP (hazard and operability study)

Analyse (évaluation) quantitative

Systèmes statiques*

Méthodes combinatoires

- diagrammes de fiabilité, RBD
- arbres des défaillances
- arbres d'événements
- fonction de structure
- réseaux de fiabilité

Systèmes dynamiques*

Méthodes de l'espace d'états

- chaînes de Markov et leurs extensions
- Statecharts stochastiques
- réseaux de Petri stochastiques et leurs extensions
- Boolean Driven Markov Processes (BDMP)
- automates stochastiques hybrides (ASH)

***D.p.d.v. fiabiliste, c.à.d. la structure fiabiliste du système ne change pas (statique) ou elle évolue pendant sa durée de vie (dynamique).**