InterSections Novembre 2004
Le magazine Schneider Electric de l'enseignement technologique et professionnel

La Sûreté de Fonctionnement (SdF)

Les préoccupations dites de sécurité sont très présentes dans le monde des machines outils ou dans les procédés continus comme la pétrochimie. Dans les applications de type manufacturier ou batch, les préoccupations sont plutôt liées à la disponibilité. Dès lors que la sécurité ou la disponibilité d'un système est mise en défaut, on incrimine sa fiabilité. Enfin, en cas de dysfonctionnement, il convient de remettre le système en conditions de fonctionnement initial : c'est là qu'intervient la maintenabilité.
Ces quatre caractéristiques constituent la sûreté de fonctionnement d'un dispositif.

p.1
Historique
p.4
Les fondamentaux de la sûreté de fonctionnement
Les études de sûreté de fonctionnement
p.7
Les données de fiabilité
La normalisation
p.9
Lexique

Historique

Jusqu'à la Renaissance et au-delà, on a toujours pensé que la fiabilité d'une chaîne reposait sur celle de son maillon le plus faible. Ainsi, si R était la fonction de fiabilité (ou de survie), alors en fonction du temps, on pensait pouvoir écrire : $R_{chaîne}(t) = Min1 \leq i \leq nRi(t)$, où les items indexent les n maillons de la chaîne.
Or, il s'est avéré que, dans une chaîne, ce n'était pas systématiquement le maillon le plus faible qui se rompait en premier. La fiabilité de la chaîne est alors devenue une certaine fonction de la fiabilité de ses maillons, les plus faibles participant davantage que les plus solides à l'éventualité d'une rupture.

L'époque moderne

Par la suite, des problèmes de fiabilité se sont posés lors de la conquête de l'Ouest. Les composants mécaniques les plus critiques de l'époque étaient les roulements à billes des locomotives à vapeur ! De même, les freins de ces mêmes locomotives, en service entre 1861 et 1883, seront abandonnés pour des problèmes de fiabilité, notamment sur les connexions électriques entre les wagons, et les premiers freins

pneumatiques les remplaceront. Ceux-ci sont toujours d'actualité.
La houille blanche, cette nouvelle énergie électrique, va constituer une formidable source de puissance qu'il va rapidement falloir apprendre à domestiquer et à fiabiliser.
Les premiers appareils construits dans cette optique (transformateurs, lignes de tension, interconnexions de lignes) vont permettre de diffuser l'énergie grâce à la mise en redondance et à l'amélioration des matériels, mais engendreront des problèmes de sûreté dramatiques.
C'est l'absence préalable d'étude de sûreté approfondie qui coûtera au métro parisien ses 84 morts en 1903, puis au Titanic son naufrage en 1912. Durant la 1ère Guerre Mondiale, les bateaux construits rapidement pour amener les soldats américains sur le sol européen ne résisteront que très difficilement aux eaux gelées de l'Atlantique Nord, subissant beaucoup de fissures dans les coques et de multiples naufrages.

Les années 1930

Dès 1930, les transports aériens commencent à collecter des informations statistiques sur les moteurs et les accidents des appareils.
Les premiers objectifs quantifiés sont promus par le capitaine A.F. Pugsley de la 7ème brigade d'infanterie canadienne, entre 1939 et 1942, avec un taux de défaillance évalué à 10^{-5}/h pour les avions, dont 10^{-7}/h pour leur structure.

Les années 1940

Les années 1940 voient le formidable essor des techniques de fiabilité. En Allemagne, W. Von Braun met au point ses V1 et revient sur l'idée que la fiabilité d'une chaîne est celle de son maillon le plus faible, en essayant de prouver que la fiabilité d'une chaîne est la moyenne de la fiabilité de ses constituants. Les essais montreront que cette hypothèse était également erronée.
C'est Eric Pieruschka qui va finalement donner la formule de calcul de la fiabilité d'une chaîne : $R_{chaîne}(t) = P1 \leq i \leq nRi(t)$. La probabilité de survie d'une chaîne à une date t arbitraire est le produit des probabilités de survie de chacun de ses composants à cette date, dans l'hypothèse où lesdits composants sont indépendants les uns des autres.
Aux Etats-Unis, pendant ce temps, les nouvelles techniques permettent de gagner un facteur 4 sur la durée de vie des moteurs de traction des locomotives, pour dépasser le million de miles. Puis naît, en 1949, la loi de Murphy, peut-être mieux connue sous le nom de "loi de l'empoisonnement maximum" ou "loi de la tartine beurrée" : dès qu'il existe une possibilité que les choses tournent mal, elles tournent mal !
E. Murphy, l'ingénieur américain amateur de philosophie qui formula cette loi, ne voulait pas en donner une impression si pessimiste.
Il cherchait simplement à s'assurer que ce qui venait de lui arriver ne se reproduirait jamais. Le capitaine Murphy, alors affecté au projet MX981 de l'armée américaine, venait d'achever une série de tests sur un avion à réaction. Il devait, par ailleurs, étudier les conséquences de la décélération brutale sur les pilotes d'essai. Il avait donc mis au point une combinaison équipée de 16 capteurs de mesure répartis sur le corps du pilote. Murphy savait pouvoir y accorder sa totale confiance, mais ce jour-là aucun des capteurs n'enregistra la moindre information.
Les vérifications permirent de constater que l'appareil de mesure fonctionnait normalement, et que les câbles assurant la liaison avec la combinaison du pilote étaient en parfait état de marche. L'erreur ne pouvait donc résider que dans les capteurs eux-mêmes. Que quelques-uns aient pu connaître une défaillance n'aurait rien eu d'exceptionnel. Mais il semblait très peu probable que tous aient cessé de fonctionner en même temps. En fait, les capteurs ne pouvaient fonctionner qu'à condition d'être branchés dans le bon sens. Or, ce jour-là, le technicien qui avait réalisé les branchements les avait tous effectués à l'envers. Résultat : aucune mesure n'avait été enregistrée.
La probabilité d'une telle erreur est presque nulle. Raison de plus pour prendre toutes les précautions afin d'éviter un tel désastre.
Pour ce faire, on se fonde sur l'hypothèse de travail, raisonnable et à la fois presque paranoïaque, formulée par Murphy lorsqu'il rendit compte de l'échec total de ces expériences : "*S'il existe deux ou plusieurs moyens de réaliser une opération, et si l'un d'eux peut mener à la catastrophe, il est certain que quelqu'un l'emploiera*". Aujourd'hui encore, cette loi résonne dans l'esprit de tout ingénieur responsable d'un système censé être à toute épreuve. La formule connut un succès immédiat. Quelques mois plus tard, on la répétait dans les bases les plus isolées de l'armée de l'air américaine. Le capitaine n'avait fait qu'exprimer une frustration connue de tous les ingénieurs. Neuf ans plus tard, elle passait à la postérité en apparaissant pour la première fois, sous le nom de "Murphy's Law" dans un dictionnaire anglais. Soixante ans plus tard, cette loi est toujours d'actualité : il faut reconnaître qu'elle n'a pas son égale pour expliquer les catastrophes.
Mais une formule populaire n'a pas forcément de fondement. D'ailleurs, la plupart des scientifiques considèrent que la loi de Murphy ne peut être considérée comme une loi au sens physique du terme.

Les années 1950

On assiste à l'avènement du concept de maintenance : $1 en équipement génère $2 en maintenance. C'est à

cette époque que la marine militaire américaine prend conscience que ses tubes électroniques ne sont opérationnels qu'à hauteur de 30 % de leur temps d'utilisation.
Les premières directives en électronique voient le jour, avec des spécifications d'essais de vieillissement accéléré, directives qui seront reprises et adaptées par la NASA. Les toutes nouvelles centrales nucléaires entraînent les premières études sur la fiabilité humaine.
En France, c'est le Centre national d'Etudes sur les Télécommunications qui commence ses travaux sur un recueil de données de fiabilité électronique.

Les années 1960

Les industries aéronautiques et spatiales (Mac-Donnell Douglas) effectuent les premières analyses relatives aux défaillances de composants, pour accompagner les débuts du programme Apollo.
Dans le nucléaire, on assiste aux premiers pas de la méthode du Diagramme de Succès. L'armée américaine (DoD : Department of Defence) promulgue les premières vraies exigences de sûreté de fonctionnement suite à des accidents sur des missiles. Aux Bell Labs, en 1961, le nouveau concept d'arbre des causes est utilisé avec succès sur le projet de missile Minuteman ; cette technique sera reprise par Boeing. En France, la SNIAS (Société nationale des Industries aéronautiques et spatiales) utilise la méthode des combinaisons de pannes sur le projet Concorde, puis sur Airbus. Toutes ces méthodes trouvent un écho favorable dans l'industrie civile, notamment au Japon ; apparaissent alors les premières bases de données et les premiers ouvrages de référence.
Dans un souci d'harmonisation et de standardisation, la Commission électrotechnique internationale crée le Comité technique 56 "Dependability" en octobre 1965 ; les produits de ce groupe deviendront des normes internationales en 1976. L'Académie des Sciences accueille le mot "fiabilité" dans sa terminologie en 1962. En 1965 est introduit le concept de maintenabilité sur lequel le CEA travaillera activement dans les années 67-68.

Les années 1970-80

En 1971 sont publiés les résultats des premiers travaux sur la fiabilité du logiciel. En 1972, EDF et le CEA mènent les premières études exhaustives sur le nucléaire. En 1975, le rapport américain Rasmussen présente une évaluation complète d'un risque nucléaire sur les centrales de Surry 1 et Peach Bottom 2 : en synthèse, le risque calculé pour les populations avoisinant lesdites centrales est inférieur à celui que font courir les chutes de météorites. En 1979, c'est la catastrophe nucléaire de TMI (Three Miles Island) ; une manière inattendue de promouvoir les outils de sûreté de fonctionnement, puisque le scénario qui a mené à la catastrophe était quasiment décrit dans le rapport Rasmussen ! Puis ce sont les industries pétrochimiques qui procèdent à leurs premières études de risque, avant que les techniques de sûreté de fonctionnement ne soient diffusées dans la chimie, le ferroviaire, l'automobile, le traitement et l'épuration d'eau, et l'ensemble des grands secteurs industriels.

Aujourd'hui

La réglementation, et les certifications qu'elle impose, a eu un double effet : le développement de l'utilisation des outils de sûreté de fonctionnement, mais également une certaine idée de la couverture des risques.
N'a-t-on pas oublié que, malgré les études, les précautions, les systèmes de sauvegarde, les protections, le risque existe toujours ?
Dans les procès qui font suite aujourd'hui à la plupart des accidents, il semble que la notion de risque ait été peu à peu effacée pour laisser place à celle de tort ou responsabilité. Comme si tous les risques de notre vie courante pouvaient être prévus et annihilés.
En parallèle, la compétition continue que se livrent les grands groupes les force à disposer d'une productivité la meilleure possible, et donc à réduire les arrêts de production et à maximiser la disponibilité de leurs équipements.
Enfin, la sécurité des biens et des personnes n'a jamais semblé aussi importante qu'aujourd'hui aux yeux de nos concitoyens. En témoignent les actions vigoureuses autour de la notion de malveillance (intrusion par effraction, attaque, vol, piratage).
Dans les deux cas, la pression médiatique et écologique autour des accidents notables (plate-forme Piper Alpha, accident chimique de Bophal et d'AZF, ou catastrophe aérienne de la TWA) est telle qu'elle entraine des conséquences très lourdes pour l'entreprise.

Les fondamentaux de la sûreté de fonctionnement

Quatre composantes

Le terme "sûreté de fonctionnement", inventé voici trente ans pour englober plusieurs concepts, n'a pas d'équivalent exact en langue anglaise.
En France, la sûreté de fonctionnement regroupe quatre notions.

- **La fiabilité :** aptitude d'un système à rester constamment opérationnel pendant une durée donnée.
- **La maintenabilité :** c'est l'aptitude d'un système à être remis rapidement dans un état opérationnel. Ainsi les systèmes dont les composants sont très facilement démontables peuvent bénéficier d'une meilleure maintenabilité que les autres.
- **La disponibilité :** aptitude d'un système à être opérationnel au moment où il est sollicité. C'est une notion importante pour un appareil de sécurité tel qu'un disjoncteur par exemple. Une disponibilité importante est compatible avec une fiabilité faible, pour peu que l'appareil puisse être réparé très rapidement.
- **La sécurité :** c'est l'aptitude d'un système à ne pas connaître de pannes considérées comme catastrophiques pendant une durée donnée.

On trouvera aussi l'acronyme FMDS pour désigner la sûreté de fonctionnement (comme fiabilité, maintenabilité, disponibilité et sécurité).

Les Anglo-Saxons utilisent le terme dependability, qui recouvre la fiabilité (reliability), la disponibilité (availability) et la maintenabilité (maintainability). La sécurité est traitée à part.

Abusivement, on assimile le mot "dependability" à "sûreté de fonctionnement". On préfèrera le terme anglais de RAMS (pour reliability, availability, maintainability and safety).

Le but de la sûreté de fonctionnement

La sûreté de fonctionnement est une notion générique qui mesure la qualité de service délivré par un système, de manière à ce que l'utilisateur ait en lui une confiance justifiée.

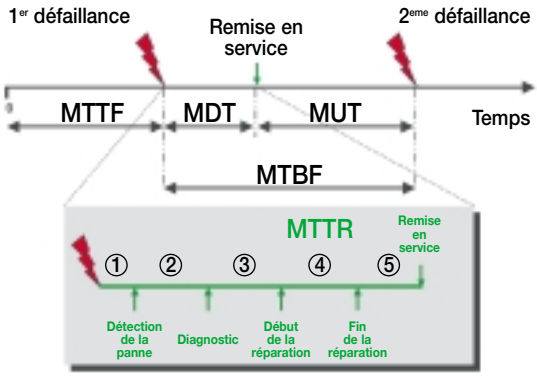
Cette confiance justifiée s'obtient à travers une analyse qualitative et quantitative des différentes propriétés du service délivré par le système, mesurée par les grandeurs probabilistes associées : fiabilité, maintenabilité, disponibilité, sécurité.

Quelques indicateurs

Certains indicateurs vont caractériser le fonctionnement prévu du système, tels que le MTTF, le MDT et le MUT.

- Le MTTF (Mean Time To [first] Failure) est l'estimation de la durée moyenne s'écoulant entre la mise en service du système et la survenance de la première panne.
- Le MDT est le temps moyen séparant la survenance d'une panne et la remise en état opérationnel du système. Il se décompose en plusieurs phases :
  - durée de détection de la panne (1) ;
  - durée de diagnostic de la panne (2) ;
  - durée d'intervention jusqu'au début de la réparation (3) ;
  - durée de la réparation (4) ;
  - durée de remise en service du système (5).
- Le MUT est le temps moyen qui sépare une remise en service opérationnelle du système de la survenance de la panne suivante.

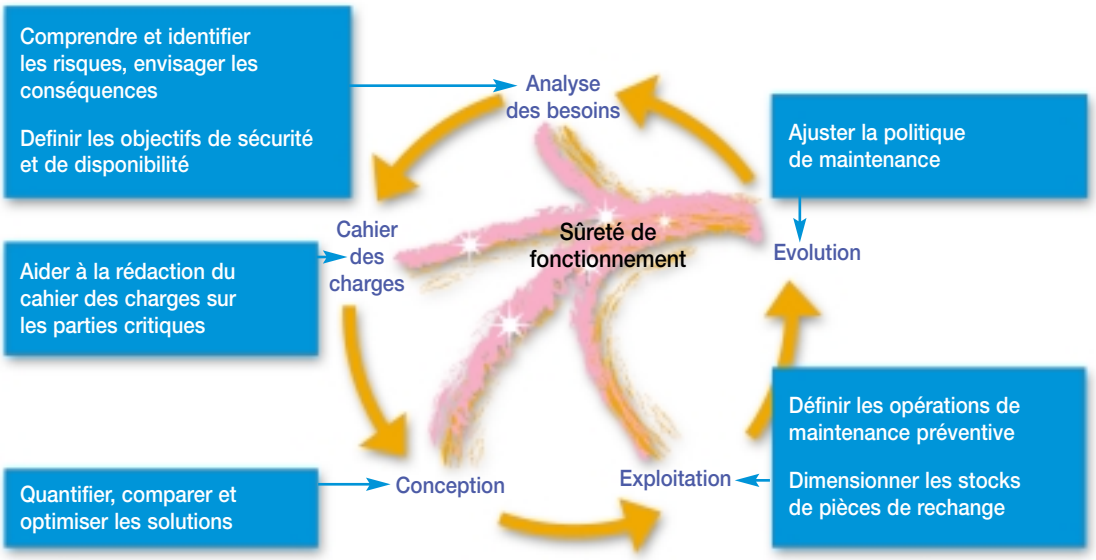
Ces deux derniers indicateurs ne sont pertinents que dans le cas de systèmes réparables. Leur somme MUT+MDT représente le temps moyen qui sépare deux pannes consécutives du système. On le note MTBF, comme Mean Time Between Failures.



Les études de sûreté de fonctionnement

Elles constituent un préalable indispensable à la conception d'un système voulu sûr, et permet d'aider à la décision en :

- comprenant et identifiant les risques ;
- optimisant l'architecture et comparant des solutions différentes ;
- optimisant les moyens de soutien en comparant des solutions ;
- justifiant les choix de façon rationnelle et démontrée ;



■ vérifiant la bonne atteinte des objectifs de sûreté de fonctionnement.

Elle peuvent aussi aider à l'optimisation en :
■ diminuant le nombre de pannes qui seront observées durant la vie du système ;
■ optimisant économiquement la conception par le dimensionnement des équipements et des architectures au "juste nécessaire" ;
■ rendant la maintenance plus ciblée et plus efficace ;
■ dimensionnant au plus juste les moyens de soutien nécessaires (stocks de pièces de rechange).

Etape par étape

La première étape consiste à analyser rigoureusement le besoin pour comprendre et identifier l'ensemble des risques, et envisager leurs conséquences. Ensuite, des niveaux d'acceptabilité sont attribués pour ces risques (on parle d'objectifs de F, M, D et/ou S selon les systèmes).

L'identification précise de ces risques va aider à la rédaction du cahier des charges du système, précisément sur ses parties critiques.
Il faudra alors imaginer des solutions techniques, des architectures adaptées qui, toutes, seront quantifiées d'un point de vue sûreté de fonctionnement, comparées entre elles et, si nécessaire, optimisées.
Une fois la solution retenue, il sera nécessaire de préciser les conditions d'une exploitation la plus efficace possible en :
■ définissant les opérations de maintenance préventive nécessaires pour maintenir les caractéristiques de sûreté de fonctionnement au niveau voulu, sans dégradation des équipements préjudiciable à l'une des quatre composantes ;
■ dimensionnant les stocks de pièces de rechange au plus juste, sans dégrader la disponibilité du système.

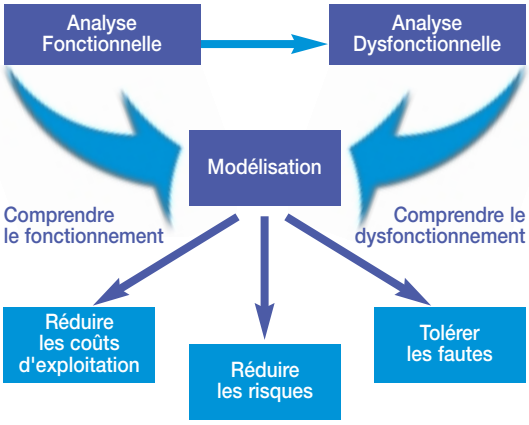
Etudes périphériques

Cette recherche de l'optimisation des tailles de stocks de pièces de rechange (suffisamment de pièces en regard de l'aptitude du système à tomber en panne, mais pas trop de pièces pour éviter des immobilisations financières inutiles) a fait l'objet d'études particulières où ce souci d'optimisation est couplé avec une démarche analogue sur :
■ la maintenance des équipements (pas trop fréquemment pour ne pas gréver la disponibilité du système, mais suffisamment pour ne pas laisser se développer une dérive importante de la fiabilité) ;
■ l'ordonnancement des transports de pièces (par route, mer ou avion).
Il en résulte une méthodologie d'approche globale, appelée soutien logistique intégré, complémentaire aux études de sûreté de fonctionnement dans les milieux industriels.
Ainsi il en est de même de la compatibilité électro-magnétique, science qui s'intéresse aux influences réciproques des équipements susceptibles d'émettre des ondes et ainsi de perturber le fonctionnement d'autres appareils physiquement proches ou reliés.

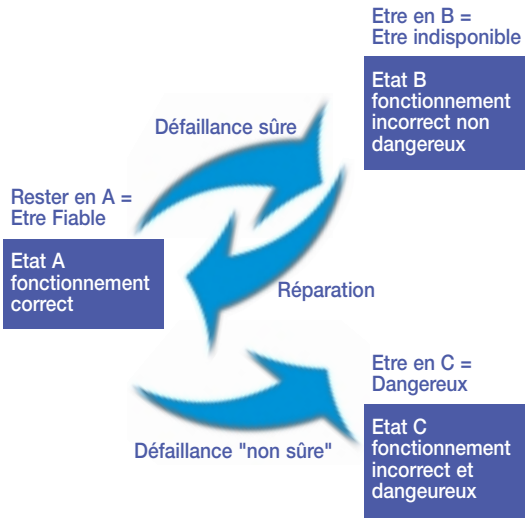
En pratique

L'étude de sûreté de fonctionnement comporte deux volets complémentaires :
■ une analyse fonctionnelle, qui va détailler la manière dont le système va opérer dans toutes ses phases de vie ainsi que les autres systèmes avec lesquels il va pouvoir interagir ;

■ une analyse dysfonctionnelle, qui vise à imaginer l'ensemble des défaillances pouvant survenir n'importe où dans le système, seules ou combinées entre elles, et à analyser l'impact de ces pannes.



Les résultats de ces deux études sont mis en commun dans une modélisation du système qui va représenter virtuellement celui-ci avant sa réalisation, tant dans son fonctionnement attendu que dans les pannes susceptibles de lui arriver.



En étudiant cette modélisation, il devient alors possible de valider ou invalider une solution technique, optimiser des choix architecturaux, remplacer des composants critiques, ceci dans le but de :

■ réduire au maximum les risques ;
■ réduire au maximum les coûts d'exploitation ;
■ tolérer, dans la mesure du possible, certaines fautes en autorisant un fonctionnement en mode dégradé sous certaines conditions.

Les outils utilisés

Pour l'analyse fonctionnelle, les principaux outils utilisés sont les suivants :

■ SADT (system analysis and design technique) : c'est une méthode d'analyse par niveaux successifs d'approche descriptive d'un ensemble, quel qu'il soit. On peut l'appliquer aussi bien à la gestion d'une entreprise qu'à un système automatisé.
■ BDF (blocs diagrammes fonctionnels) : méthode de découpage fonctionnel du système.
■ Méthode MISME : cette méthode considère l'ensemble des composants du système avec leurs interactions, ainsi que les milieux environnants.

Pour l'analyse dysfonctionnelle, on peut recourir à :

■ l'analyse préliminaire des risques (APR), qui fournit l'ensemble des événements redoutés prévisionnels dans toutes les phases de vie du système (de la conception au rebut, en passant par la mise en service, l'exploitation et la maintenance) ;
■ l'AMDEC (analyse des modes de défaillance, de leurs effets et de leur criticité) : cette méthode exhaustive examine les potentialités de dysfonctionnements de chacun des éléments composant le système, à un niveau de détail choisi à l'avance. Elle permet de quantifier la probabilité d'apparition de ladite défaillance et de classer ses effets par ordre de gravité ; la combinaison de ces deux estimations fournissant la criticité de l'élément retenu. A l'issue de cette phase, et pour les éléments les plus critiques, il sera procédé à une fiabilisation, ou bien à l'adjonction d'un dispositif de réduction du risque ;
■ l'AEEL (analyse des effets des erreurs logicielles) : cette méthode est l'adaptation au logiciel de la méthode AMDEC décrite ci-dessus, le programme étant lui-même décomposé en parties élémentaires de taille prédéfinie.

Enfin, pour modéliser le système ainsi analysé, on utilise :

■ Les arbres de défaillance : en partant d'un événement redouté bien identifié (dit "de tête"), on détermine les sous-événements qui peuvent conduire à l'événement de tête
- soit par survenance simultanée (il est nécessaire que tous les sous-événements se réalisent pour que l'événement de tête se réalise (on parle de porte ET),
- soit par survenance d'un quelconque sous-événement (porte OU).
Chacun des sous-événements est lui-même décomposé ensuite de la même manière, jusqu'à obtenir des éléments suffisamment simples pour estimer directement leur probabilité d'apparition (on parle d'événements de base). En recombinant les probabilités d'apparition de tous les événements de base grâce au schéma logique de l'arbre de décomposition (algèbre booléenne/théorème de Poincaré), on en déduit la probabilité d'apparition de l'événement de tête. Pour les calculs correspondants, on peut utiliser les arbres

de décision binaires (binary decision diagrams). Ce formalisme utilise les propriétés de la décomposition de Shannon pour simplifier fortement la structure de l'arbre avant de réaliser les calculs eux-mêmes. Un formalisme qui peut s'avérer utile lorsque le modèle en arbre de défaillances d'un système devient très important.

- Les graphes de Markov : ici, ce sont les différents états du système qui sont représentés. On suppose que le passage d'un état du système à l'autre survient aléatoirement, ou classiquement par la défaillance d'un élément, ou à la fin de la réparation d'un autre élément. Connaissant l'état initial du système, on peut en déduire soit la probabilité d'être dans un état donné après une durée déterminée, soit la probabilité moyenne d'être dans un état donné tout au long de sa durée de vie utile.
- Les réseaux de Petri stochastiques : cette technique s'apparente à celle des graphes de Markov décrite ci-dessus, à la différence que les transitions entre les différents états peuvent suivre des lois de probabilité autres que la loi exponentielle classique. D'autres caractéristiques permettent de synchroniser différentes transitions. Le prix à payer étant la nécessité de simuler le fonctionnement du système par des méthodes de Monte Carlo puisque le calcul analytique n'est quasiment jamais possible. Par ailleurs, pour les systèmes très fiables, les temps de simulation peuvent devenir rédhibitoires lorsqu'on cherche à quantifier leurs différentes probabilités de défaillances. Il existe une abondante littérature sur les diverses techniques actuelles d'accélération des simulations pour ce type de systèmes.
- En complément, les langages formels (LUSTRE, B) permettent de réaliser des études de preuve formelle sur des logiciels embarqués temps réel.

Les données de fiabilité

Elles sont la base même des études. C'est à partir des données de fiabilité que vont être élaborés les calculs permettant une vision objective des capacités du système en termes de sûreté de fonctionnement.

Les recueils

Il existe de nombreux recueils de données collectées et traitées par des organismes privés ou publics à travers le monde, et mises à jour régulièrement. C'est le cas du domaine électronique notamment, qui bénéficie des nombreux travaux des industriels concernés.

Le retour d'expérience

Est désigné ainsi l'ensemble des dispositions permettant de recueillir des informations sur la fiabilité opérationnelle des produits et systèmes auxquels on s'intéresse : pannes, défaillances détectées préventivement, maintenances diverses. Si le recueil de données est fidèle à la réalité, il est possible, grâce à des techniques statistiques adaptées, de calculer les indicateurs de sûreté de fonctionnement correspondant, spécifiques pour le système considéré. Ainsi ces indicateurs sont plus pertinents aux yeux des clients de ces systèmes.

La normalisation

Au-delà des normes spécifiques à un domaine (comme les relais de protection), il existe des normes génériques pour la sûreté de fonctionnement. Ces normes sont normalement émises par le comité technique 56 "Dependability" de la commission électrotechnique internationale. On trouvera sur le site **http://www.iec.ch/helpline/sitetree/tree_fr.htm** la liste des normes émises par la commission. Le comité technique 65A a également émis une norme générique en sûreté de fonctionnement, la norme 61508 : "Sécurité Fonctionnelle". Une autre norme générique existe, numérotée EN954 "Sécurité des Machines", sous l'égide de l'Union européenne.

Ce guide technique a été rédigé par :
Marcel Chevalier, responsable équipe 6-sigmas ;
Robert Garnier, Master Block Belt 6-sigmas ;
Philippe Chang, expert en sûreté de fonctionnement des systèmes ;
Bruno Lusson, responsable sûreté de fonctionnement des systèmes ;
Equipe Schneider Ingénierie Sûreté, dpt Projects & Engineering Centre.

Bibliographie

■ **Alain Villemeur**
"Sûreté de Fonctionnement des systèmes industriels".
- Collection de la Direction des Etudes et Recherches d'Electricité de France, (Eyrolles, 1988).

■ **Robert Garnier**
"Une méthode efficace d'accélération de la simulation des réseaux de Petri stochastique".
- Thèse de 3ème cycle. Automatique/Productique, Université Bordeaux I, (Juin 1998).

■ **M.A. Boyd**
"What Markov Modeling can do for you : An Introduction".
- Annual Reliability and Maintainability Symposium – (Tutorial notes, 1994).

■ **Michel Prevost & Charles Waroquier**
"L'analyse du soutien logistique et son enregistrement".
- Editions Lavoisier (TEC DOC, 1994).

■ **Alain Leroy & Jean-Pierre Signoret**
"Le risque technologique".
- Collection "Que sais-je ?" (PUF, 1992).

■ **Alain Pagès & Michel Gondran**
"Fiabilité des systèmes".
- Collection de la Direction des Études et Recherches d'Électricité de France, Editions Eyrolles (1980).

■ **CEI / IEC 1025-Norme Internationale**
"Fault Tree Analysis (FTA)".
- Bureau Central de la CEI, Genève, Suisse (1990).

■ **Yves Dutuit, Eric Chatelet, J. Dos Santos & T. Bouhoufani**
"Les diagrammes-blocs fonctionnels : une aide à la construction manuelle des arbres de défaillance. Systèmes sans boucles de régulation"
- Revue Européenne Diagnostic et Sûreté de Fonctionnement (Vol. 5, n° 2, pp. 181-200, 1995).

■ **Christine Bodennec, Robert Garnier, C. Jourdain, C. Mazuet & D. Perez**
"Application of Formal Methods on Safety Assessment and Fault Tolerant Design".
- Colloque ESREL'98, 15-19 juin 1998, Trondheim, Norvège.

■ **Olivier Coudert & J-C Madre**
"Metaprime : An interactive fault-tree analyzer".
- IEEE Transactions on Reliability (Vo. 43, n° 1, pp. 121-127, 1994).

■ **Tadao Murata**
"Petri Nets : Properties, analysis and applications"
- Proceedings of the IEEE transactions on Reliability (Vol. 77, n° 4, 1989).

■ **Carl Adam PETRI**
"Kommunication mit Automaten"
- Bonn: Institut für Instrumentelle Mathematik, Schriften des IIM Nr. 2, 1962, Second Edition, New York : Griffiss Air Force Base (Technical Report RADC-TR-65--377, Vol. 1, 1966).

■ **Antoine Rauzy & Yves Dutuit**
"Exact and Truncated Computations of Prime Implicants of Coherent and Non-Coherent Fault Trees within Aralia".
- Reliability Engineering and System Safety (Vol. 58, n° 2, pp. 127-144, 1997).

■ **Véronique Tieri**
"Traitement des portes "SI" dans les arbres de défaillances".
- Rapport de stage de fin d'études DESS "Ingénierie Mathématique", Qualité & Fiabilité, Université Joseph Fourier (Grenoble 1, 1997).

■ **W.E. Vesely, F.F. Goldberg, N.H. Roberts, D.F. Haasl**
"Fault Tree Handbook".
- U.S. Nuclear Regulatory Commission (Washington, 1981).

■ **Sylvie Logacio**
"Etudes de sûreté des installations électriques".
- Cahier Technique Schneider Electric, n° 184.

■ **Emmanuel Cabau**
"Introduction à la conception de la sûreté".
- Cahier Technique Schneider Electric, n° 144.

Lexique *de la sûreté de fonctionnement*

Voici quelques définitions de termes couramment utilisés en sûreté de fonctionnement [VILLE-88].
Ce lexique n'est pas exhaustif et ne regroupe que des termes ayant un rapport direct avec ce guide technique.

Acceptable : Qualifie un événement jugé acceptable au regard d'objectifs de sûreté de fonctionnement.
Terme anglais : "Acceptable"

Accident : Evénement ayant des conséquences catastrophiques ou susceptible d'en avoir. Dans le nucléaire, l'accident est défini comme l'événement pouvant entraîner l'endommagement d'une ou plusieurs barrières et donc conduire à un relâchement de produits radioactifs et demandant la mise en service de systèmes de protection.
Terme anglais : "Accident"

Amélioration de la sûreté de fonctionnement : Procédé intentionnellement destiné à produire une croissance d'une caractéristique de la sûreté de fonctionnement (disponibilité, fiabilité, maintenabilité, sécurité, etc.) en vue d'atteindre des objectifs spécifiés par élimination de défaillance ou réduction de leur probabilité d'occurrence.
Terme anglais : "Dependability Improvement"

Analyse d'un système : Processus orienté vers l'acquisition, l'investigation et le traitement ordonnés d'informations spécifiques au système et pertinentes vis-à-vis d'une décision ou d'un objectif donné.
Ce processus conduit à l'obtention d'un modèle et, éventuellement, à son évaluation quantitative.
Terme anglais : "System Analysis"

Analyse de criticité de défaillance : Analyse ayant pour objet d'évaluer le couple gravité/probabilité associé à une défaillance.
Terme anglais : "Criticality Analysis"

Analyse des modes de défaillance et de leurs effets (AMDE) : Méthode d'analyse quantitative d'un système ayant pour objet d'identifier les modes de défaillance des composants du système, leurs causes et leurs effets.
Terme anglais : "Failure Modes and Effects Analysis" (FMEA)

Analyse des modes de défaillance, de leurs effets et de leur criticité (AMDEC) : Méthode d'analyse d'un système qui comprend une analyse des modes de défaillance et de leurs effets, complétée par une analyse de criticité des modes de défaillance.
Terme anglais : "Failure Modes, Effects and Criticality Analysis" (FMECA)

Analyse préliminaire des risques : Analyse ayant pour objet d'identifier et d'évaluer des risques (économiques, humains...) liés à l'utilisation d'un système, et ce de manière préliminaire à l'utilisation de méthodes d'analyse plus précises.
Terme anglais : "Preliminary Hazard Analysis (PHA)" ; "Preliminary Risks Analysis"

A sûreté intégrée : Qualifie une entité qui est conçue en vue d'éviter que ses défaillances n'entraînent des conséquences critiques ou catastrophiques. On parle aussi de "sécurité intrinsèque".
Terme anglais : "Fail safe"

Composant : C'est la plus petite partie d'un système qu'il est nécessaire et suffisant de considérer pour l'analyse d'un système.
Terme anglais : "Component"

Composant actif : Composant qui comporte des pièces mobiles dont la position est modifiée ou qui nécessite pour remplir sa fonction une variation de sa configuration ou de ses propriétés à l'aide d'une source d'énergie extérieure.
Terme anglais : "Active component"

Composant critique : Composant dont la défaillance, dans un état de fonctionnement donné d'un système, entraîne la défaillance de ce système.
Terme anglais : "Critical component"

Composant passif : Composant n'entrant pas dans la définition des composants actifs et qui n'est soumis, par exemple, qu'à des variations de pression, de température, de débit de fluide ou de courant électrique lorsqu'il remplit sa fonction. Cette définition est utilisée dans le nucléaire.
Terme anglais : "Passive component"

Danger : Situation pouvant nuire à l'homme, à la société ou à l'environnement.
Terme anglais : "Hazard" ; "Danger"

Défaillance : Cessation de l'aptitude d'une entité à accomplir une fonction requise (Norme CEI-271-1974).
Terme anglais : "Failure"

Défaillance à taux constant : Défaillance qui apparaît avec un taux sensiblement constant pendant la durée de vie utile de l'entité. Cette défaillance est généralement catalectique. Elle est encore appelée "défaillance aléatoire".
Terme anglais : "Random Failure"

Défaillance catalectique : Défaillance qui est à la fois soudaine et complète (Norme CEI-271-1974).
Terme anglais : "Catastrophic Failure"

Défaillance complète : Défaillance résultant de déviation d'une ou des caractéristiques au-delà des limites spécifiées, telle qu'elle entraîne une disparition complète de la fonction requise (Norme CEI-271-1974).
Terme anglais : "Complete Failure"

Défaillance de commande : Défaillance d'une entité dont la cause directe ou indirecte est la défaillance d'une autre entité et pour laquelle cette entité a été qualifiée et dimensionnée.
Terme anglais : "Command Failure"

Défaillance d'usure : Défaillance qui apparaît avec un taux rapidement croissant par suite de processus inhérents à l'entité.
Terme anglais : "Wearout Failure"

Défaillance non pertinente : Défaillance à exclure pour l'interprétation ou l'évaluation d'une mesure de la sûreté de fonctionnement. On parle aussi de "défaillance à ne pas prendre en compte" (Norme CEI-271A-1978).
Terme anglais : "Non-relevant Failure"

Défaillance par dégradation : Défaillance qui est à la fois

progressive et partielle (Norme CEI-271-1974). A la longue, une telle défaillance peut devenir une défaillance complète (Norme CEI-271-1974).
Terme anglais : "Degradation Failure"

Défaillance partielle : Défaillance résultant de déviation d'une ou des caractéristiques au-delà des limites spécifiées, mais telle qu'elle n'entraîne pas une disparition complète de la fonction requise (Norme CEI-271-1974).
Les limites sont des limites spéciales spécifiées à cette fin (CEI-271-1974).
Terme anglais : "Partial Failure"

Défaillance pertinente : Défaillance à prendre en compte pour interpréter ou évaluer une mesure de la sûreté de fonctionnement. On parle aussi de "défaillance à prendre en compte" (CEI-271A-1978).
Terme anglais : "Relevant Failure"

Défaillance progressive : Défaillance due à une évolution dans le temps des caractéristiques d'une entité. En général, une défaillance progressive peut être prévue par un examen ou une surveillance antérieur.
Terme anglais : "Gradual Failure" ; "Drift Failure"

Défaillance de cause commune : Défaillances dépendantes ayant pour origine la même cause directe.
Terme anglais : "Common cause Failures"

Défaillance de mode commun : Défaillances de cause commune se manifestant par le même mode de défaillance des entités.
Terme anglais : "Commun mode Failures"

Défaut : Ecart entre une caractéristique d'une entité et la caractéristique voulue, cet écart dépassant les limites d'acceptabilité.
Terme anglais : "Defect"

Démarche déductive : Démarche dans laquelle on raisonne du plus général au plus particulier.
Terme anglais : "Deductive approach"

Démarche inductive : Démarche dans laquelle on raisonne du plus particulier au plus général.
Terme anglais : "Inductive approach"

Densité de défaillance : C'est la limite, si elle existe, du quotient de la probabilité conditionnelle pour que l'instant T de la première défaillance d'une entité soit compris dans un intervalle de temps donné $[t;t+\Delta t]$, par la durée de l'intervalle de temps, lorsque Δt tend vers zéro, sachant que l'entité est en fonctionnement au temps t=0. Elle est notée U(t).
Terme anglais : "Failure density"

Densité de probabilité : C'est la dérivée, si elle existe, de la fonction de répartition d'une variable aléatoire.
Elle est notée f(x).
Terme anglais : "Probability density function"

Densité de réparation : C'est la limite, si elle existe, du quotient de la probabilité conditionnelle pour que l'instant T d'achèvement de la réparation d'une entité soit compris dans un intervalle de temps donné $[t;t+\Delta t]$, par la durée de l'intervalle de temps, lorsque Δt tend vers zéro, sachant que l'entité est défaillante au temps t=0. Elle est notée G(t).
Terme anglais : "Repair density"

Densité de transition : C'est la dérivée, si elle existe, de la probabilité de transition.
Terme anglais : "Transition density"

Disponibilité : Aptitude d'une entité à être en état d'accomplir une fonction requise dans des conditions données et à un instant donné. Le terme de "disponibilité" est aussi employé pour désigner la mesure de la disponibilité.
Terme anglais : "Availability"

Disponibilité (mesure de la) : Probabilité pour qu'une entité soit en état d'accomplir une fonction requise dans des conditions données et à un instant donné. Elle est généralement notée A(t) et est aussi dénommée "disponibilité instantanée".
Terme anglais : "Availability"

Disponibilité asymptotique : C'est la limite, si elle existe, de la disponibilité instantanée représentée par un modèle mathématique, quand on fait tendre le temps vers l'infini. Elle est notée $A(\infty)$.
Terme anglais : "Steady-state availability" ; "Asymptotic availbility"

Disponibilité moyenne : C'est la moyenne de la disponibilité instantanée sur un intervalle de temps donné [t1;t2]. Elle est notée $A^m(t1,t2)$.
Terme anglais : "Mean availability"

Durée de disponibilité : Période pendant laquelle une entité est en état d'accomplir sa fonction requise (Norme CEI-271A-1978).
Terme anglais : "Up time"

Durée de fonctionnement : Période pendant laquelle une entité accomplit sa fonction requise (Norme CEI-271A-1978).
Terme anglais : "Operating time"

Durée de vie utile : Période commençant à un instant donné, pendant laquelle, dans des conditions données, une entité a un taux de défaillance acceptable, ou période précédant l'apparition d'une défaillance non réparable (Norme CEI-271-1978).
Terme anglais : "Useful life"

Durée d'indisponibilité : Période pendant laquelle une entité n'est pas en état d'accomplir sa fonction requise (Norme CEI-271A-1978).
Terme anglais : "Down time"

Entité : Tout élément, composant, sous-système, dispositif, équipement, unité fonctionnelle que l'on peut considérer individuellement.
Terme anglais : "Entity" ; "Item"

Etat d'attente : Etat d'une entité disponible et en état de non-fonctionnement pendant une période requise.
Terme anglais : "Standby state"

Etat de disponibilité : Etat d'une entité caractérisée par son aptitude à accomplir une fonction requise.
Terme anglais : "Availability state"

Etat de fonctionnement : Etat d'une entité dans lequel cette entité accomplit correctement une fonction requise.
Terme anglais : "Operating state"

Etat de panne : Etat d'une entité caractérisée par une inaptitude à accomplir une fonction requise.
Terme anglais : "Fault state"

Evénement catastrophique : Evénement qui occasionne la perte d'une (ou des) fonction(s) essentielle(s) d'un système en causant des dommages importants au dit système ou à son environnement et/ou entraîne pour l'homme la mort ou des dommages corporels.
Terme anglais : "Catastrophic event"

Evénement critique : Evénement qui occasionne la perte d'une (ou des) fonction(s) essentielle(s) d'un système en causant des dommages importants au dit système ou à son environnement en ne présentant toutefois qu'un risque négligeable de mort ou de blessure.
Terme anglais : "Critical event"

Evénement indésirable : Evénement (de la vie d'une entité) ne devant pas se produire ou devant se produire avec une probabilité moins élevée au regard d'objectifs de sûreté de fonctionnement.
Terme anglais : "Undesirable event"

Evénement majeur : Evénement critique ou significatif.
Terme anglais : "Major event"

Fiabilité : Aptitude d'une entité à accomplir une fonction requise, dans des conditions données, pendant une durée donnée (Norme CEI-271-1974).
Terme anglais : "Reliability"

Fiabilité (mesure de la) : Probabilité qu'une entité accomplisse une fonction requise dans des conditions données, pendant une durée donnée (Norme CEI-271-1974). Elle est notée R(t). On suppose en général que l'entité est en état d'accomplir la fonction requise au début de l'intervalle de temps donné.
Terme anglais : "Reliability"

Graphe d'états : Diagramme logique montrant les états de fonctionnement et de pannes d'un système, ainsi que leurs transitions.
Terme anglais : "States graph"

Immaintenabilité : Inaptitude 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.
Terme anglais : "Unmaintainability"

Inacceptable : Qualifie un événement jugé inacceptable au regard d'objectifs de sûreté de fonctionnement.
Terme anglais : "Unacceptable"

Incident : Evénement ayant des effets ou des conséquences critiques ou susceptible d'en avoir.
Terme anglais : "Incident"

Indisponibilité : Inaptitude d'une entité à accomplir une fonction requise, dans des conditions données et à un instant donné.
Terme anglais : "Unavailability"

Indisponibilité (mesure de l') : Probabilité qu'une entité ne soit pas en état d'accomplir une fonction requise, dans des conditions données et à un instant donné. Elle est notée $\overline{A}$ (t). Elle est aussi dénommée "indisponibilité instantanée".
Terme anglais : "Unavailability" ; "Instantaneous unavailability"

Indisponibilité asymptotique : C'est la limite, si elle existe, de l'indisponibilité instantanée représentée par un modèle mathématique, quand on fait tendre le temps vers l'infini. Elle est notée $\overline{A}$ (∞).
Terme anglais : "Steady-state unavailability" ; "Asymptotic unavailability"

Indisponibilité moyenne : C'est la moyenne de l'indisponibilité instantanée sur un intervalle de temps donné [t1;t2]. Elle est notée $\overline{A}^{m}$ (t1, t2).
Terme anglais : "Mean unavailability"

Insécurité : Aptitude d'une entité à faire apparaître, dans des conditions données, des événements critiques ou catastrophiques.
Terme anglais : "Unsafety"

Maintenabilité : Aptitude d'une entité à être maintenue ou rétablie dans un état dans lequel elle peut accomplir une fonction requise lorsque la maintenance est effectuée dans des conditions données avec des procédures et des moyens prescrits.
Terme anglais : "Maintainability"

Maintenabilité (mesure de la) : Pour une entité donnée, probabilité qu'une maintenance accomplie dans des conditions données, avec des procédures et des moyens prescrits, soit achevée au temps t sachant que l'entité est défaillante au temps t = 0. Elle est notée M(t).
Terme anglais : "Maintainability"

Maintenance : Combinaison de toutes les actions techniques et des actions administratives correspondantes, y compris les opérations de surveillance et de contrôle, destinées à maintenir ou à remettre une entité dans un état lui permettant d'accomplir une fonction requise.
Terme anglais : "Maintenance"

Maintenance corrective : Maintenance effectuée après la détection de panne et destinée à remettre une entité dans un état lui permettant d'accomplir une fonction requise.
Terme anglais : "Corrective maintenance"

Maintenance préventive : Maintenance effectuée à intervalles prédéterminés ou selon des critères prescrits et destinée à réduire la probabilité de défaillance ou la dégradation du fonctionnement d'une entité.
Terme anglais : "Preventive maintenance"

MDT : Durée moyenne d'indisponibilité.
Terme anglais : "Mean down time"

Mode de défaillance : Effet par lequel une défaillance est observée (Norme CEI-271-1974).
Terme anglais : "Failure mode"

Mode de fonctionnement : Effet par lequel un fonctionnement est observé.
Terme anglais : "Functional mode"

MTBF : Durée moyenne entre deux défaillances consécutives d'une entité réparée.

Terme anglais : "Mean time between failure"

MTTF : Durée moyenne de fonctionnement d'une entité avant la première défaillance.
Terme anglais : "Mean time to failure" ; "Mean Time To First Failure" (MTTFF)

MTTR : Durée moyenne de réparation. Ce terme est parfois utilisé pour désigner la durée moyenne de maintenance corrective.
Terme anglais : "Mean time to repair"

MUT : Durée moyenne de fonctionnement après réparation.
Terme anglais : "Mean up time"

Panne : Inaptitude d'une entité à accomplir une fonction requise.
Terme anglais : "Fault"

Panne intermittente : Panne d'une entité subsistant pendant une durée limitée après laquelle l'entité redevient apte à accomplir une fonction requise sans avoir été soumise à une opération de maintenance corrective.
Terme anglais : "Intermittent fault"

Panne latente : Panne qui existe, mais qui n'a pas encore été détectée.
Terme anglais : "Latent fault"

Panne permanente : Panne d'une entité qui persiste tant que n'ont pas eu lieu les opérations de maintenance corrective.
Terme anglais : "Permanent fault"

Probabilité de transition : Probabilité de quitter un état du système dans l'intervalle de temps [0;t] et de passer dans un autre état en une seule transition, sachant que l'on est entré dans le premier état à l'instant t=0.
Terme anglais : "Transition probability" ; "Transition distribution"

Processus stochastique : Ensemble de variables aléatoires dépendant du temps, dont les valeurs sont régies par un ensemble donné de lois de probabilité multidimensionnelles qui correspondent à toutes les combinaisons des variables aléatoires. Le terme de "processus aléatoire" est aussi utilisé.
Terme anglais : "Random process"

Qualité : Aptitude d'un produit ou d'un service à satisfaire les besoins des utilisateurs.
Terme anglais : "Quality"

Redondance : Existence, dans une entité, de plus d'un moyen pour accomplir une fonction requise (Norme CEI-271-1974).
Terme anglais : "Redundancy"

Redondance active : Redondance selon laquelle tous les moyens d'accomplir une fonction requise sont mis en œuvre simultanément (Norme CEI-271-1974).
Terme anglais : "Active redundancy"

Redondance passive : Redondance où les différents moyens d'accomplir une fonction donnée ne sont pas mis en oeuvre avant que ce ne soit nécessaire (Norme CEI-271-194).
Terme anglais : "Standby redundancy"

Réparation : Partie de la maintenance corrective pendant laquelle des opérations sont effectuées sur l'entité.
Terme anglais : "Repair"

Risque : Mesure du danger associant une mesure de l'occurrence d'un événement indésirable et une mesure de ses effets ou conséquences.
Terme anglais : "Risk"

Sécurité : Aptitude d'une entité à éviter de faire apparaître, dans des conditions données, des événements critiques ou catastrophiques.
Terme anglais : "Safety"

Sûreté de fonctionnement : Aptitude d'une entité à satisfaire à une ou plusieurs fonctions requises dans des conditions données. Ce concept peut englober la fiabilité, la disponibilité, la maintenabilité, la sécurité... ou des combinaisons de ces aptitudes. Au sens large, on considère la sûreté de fonctionnement comme la Science des Défaillances et des Pannes.
Terme anglais : "Dependability"

Taux de défaillance : C'est la limite, si elle existe, du quotient de la probabilité conditionnelle pour que l'instant T d'une défaillance soit compris dans un intervalle de temps donné $[t;t+\Delta t]$, par la durée de l'intervalle de temps, lorsque Δt tend vers zéro, en sachant que l'entité n'a pas eu de défaillance sur [0;t]. Ce taux est noté $\Lambda(t)$.
Terme anglais : "(Instantaneous) Failure rate"

Taux de défaillance asymptotique : C'est la limite, si elle existe, du taux de défaillance représenté par un modèle mathématique lorsqu'on fait tendre le temps vers l'infini. Il est noté $\Lambda(\infty)$.
Terme anglais : "Steady-state failure rate"

Taux de réparation : C'est la limite, si elle existe, du quotient de la probabilité conditionnelle pour que l'instant T d'achèvement de la réparation (ou d'une opération de maintenance) d'une entité soit compris dans un intervalle de temps donné $[t;+\Delta t]$, par la durée de l'intervalle de temps, lorsque Δt tend vers zéro, sachant que l'entité a été en panne sur tout l'intervalle de temps [0;t]. Ce taux est noté M(t).
Terme anglais : "Repair rate (instantaneous)"

Taux de réparation asymptotique : C'est la limite, si elle existe, du taux de réparation représenté par un modèle mathématique lorsqu'on fait tendre le temps vers l'infini. Il est noté $M(\infty)$.
Terme anglais : "Steady-state repair rate"

Taux de transition : C'est la limite, si elle existe, du quotient de la probabilité de quitter un état du système pour un autre état du système dans l'intervalle de temps $[t;t+\Delta t]$, par la durée de l'intervalle de temps, lorsque Δt tend vers zéro.
Terme anglais : "Transition rate"

Tolérance aux fautes : Propriété d'un système qui le rend capable d'accomplir une fonction requise en présence de certaines défaillances ou pannes de ses composants.
Terme anglais : "Fault tolerance"