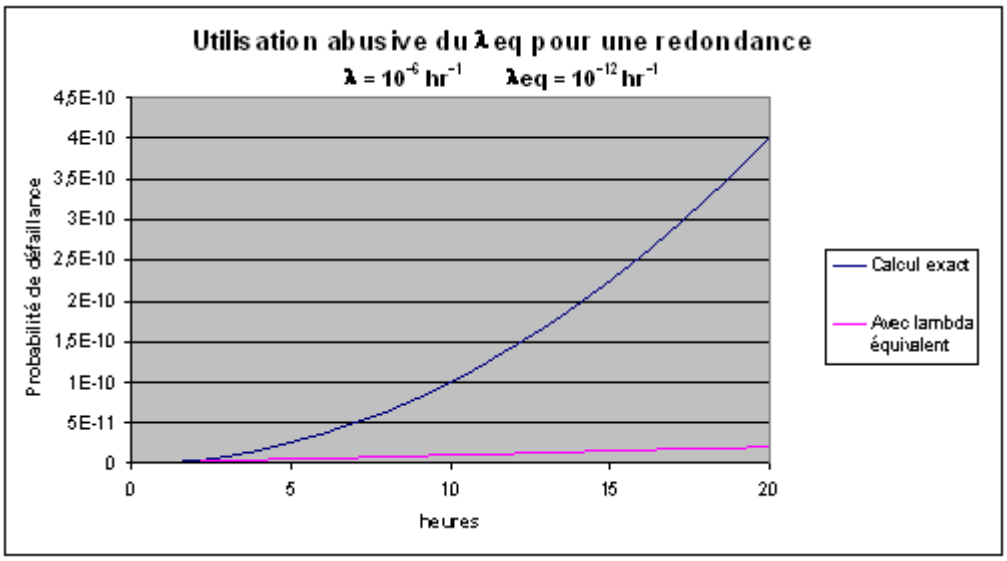
Compilation du bêtisier

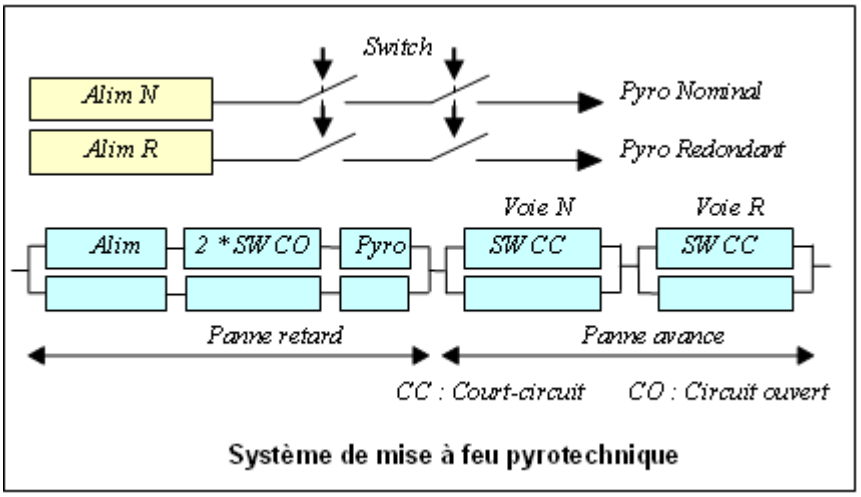
N° 10 – Le « Lambda équivalent »

Le « Lambda équivalent » correspond au taux de panne d'un élément simple dont la fiabilité est la même que celle d'une architecture donnée pour une certaine durée de mission. Ce taux n'a évidemment de sens que pour une seule valeur de temps, mais il est bien tentant de l'utiliser abusivement en remplaçant des parties de modèles complexes par de simples exponentielles. Le graphe ci-dessous montre ainsi l'erreur commise en remplaçant une redondance active par un élément simple de même Lambda équivalent calculé à 1 heure. Une telle erreur peut rapidement conduire à des résultats très optimistes et s'avérer fort gênante notamment dans le cadre d'études de sécurité.



N° 11 – Mode de pannes antagonistes

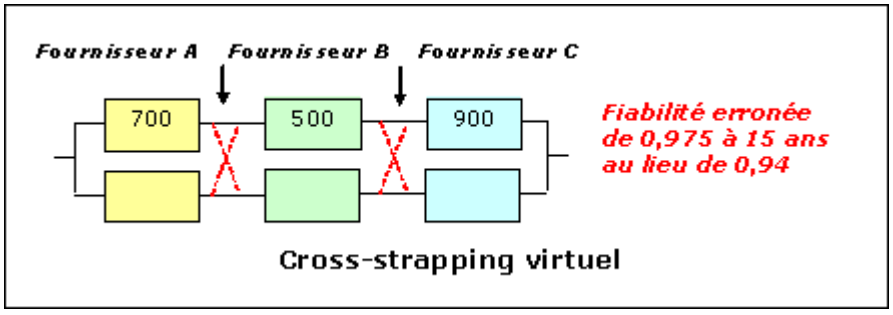
Il est souvent nécessaire de se prémunir de modes de défaillances antagonistes tels que le fonctionnement intempestif (panne avance) et l'absence de fonctionnement (panne retard). Afin de ne pas conduire à des évaluations erronées généralement très optimistes, il importe de bien séparer ces modes dans les modèles de fiabilité car les moyens de protection associés sont également antagonistes. L'exemple ci-dessous concerne un système pyrotechnique dans lequel la protection panne avance est assurée par des relais en série et la protection panne retard par la redondance des chaînes.



Système de mise à feu pyrotechnique

N° 12 – Le cross-strapping virtuel

Erreur d'évaluation particulièrement grossière, le « cross-strapping virtuel » n'en est pas moins fréquent sur des systèmes complexes, pour lesquels différents fournisseurs participent à la réalisation de chaînes fonctionnelles globalement redondées.
Bien que seuls les taux de défaillance des équipements (et éventuellement les paramètres de maintenance associés) sont exploitables au niveau du système, les fournisseurs prennent souvent en compte la redondance dans leur évaluation afin de présenter d'excellents résultats de fiabilités (ou de disponibilité).
Leur simple produit, réalisé abusivement au niveau supérieur, conduit alors à améliorer significativement la performance d'ensemble comme le montre l'exemple ci-dessous (taux de défaillance en fit).



Cross-strapping virtuel

N° 13 - Utilisation erronée des arbres de fautes

Particulièrement facile d'accès, l'arbre de fautes permet de calculer très efficacement la probabilité d'occurrence de diverses combinaisons d'événements. Mais certains utilisateurs oublient parfois que les événements en questions doivent être indépendants.
Or les dépendances peuvent être de multiples natures et concerner tout autant des caractéristiques de fiabilité (stress de composants modifiés dans certaines configurations) que de maintenabilité (phasage d'actions de maintenance périodique, réparateur en nombre limité, etc.).

Des erreurs grossières sont observées dans certaines analyses dont notamment des études de sécurité répondant à la norme **CEI 61508**. Aussi, faut-il rappeler que :

- Un arbre de fautes est un modèle statique permettant de calculer la probabilité d'un événement sommet à partir des probabilités des événements de base (fondé sur le théorème de POINCARE).

- Les résultats obtenus peuvent être erronés si les probabilités des événements de base sont des valeurs moyennes.
- L'approximation "lambda*T/2", proposée par certains outils pour calculer l'indisponibilité d'une unité périodiquement maintenue, peut induire des erreurs très significatives dues à l'effet des redondances.
- L'approximation "mu/(lambda+mu)" ne peut être employée que pour une calcul asymptotique de disponibilité quand les unités sont complètement indépendantes.
- Il est possible de coupler l'arbre de fautes à la simulation de Monte Carlo pour obtenir la distribution de probabilité de l'événement sommet en fonction de celle des événements de base, éventuellement corrélés, sans dégradation de la précision de calcul.

N° 14 – Estimation erronée

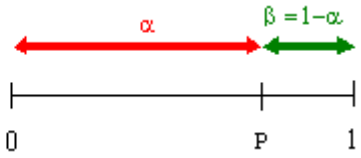
L'intervalle de confiance est une notion délicate qui suscite parfois des erreurs de calcul. Celles-ci concernent notamment des confusions entre les intervalles bilatéral et unilatéral (estimation qui majore le risque) et entre le taux de confiance β ou de risque (= 1 - (que l'on accepte.

A titre d'exemple, la probabilité qu'une pièce soit bonne à 60% de confiance, sachant qu'une pièce a été trouvée défectueuse dans un échantillon de 48 pièces du même lot, est égale à :

48 * P^47 * (1-p) + p^48 = 40 % soit p = 0,9584

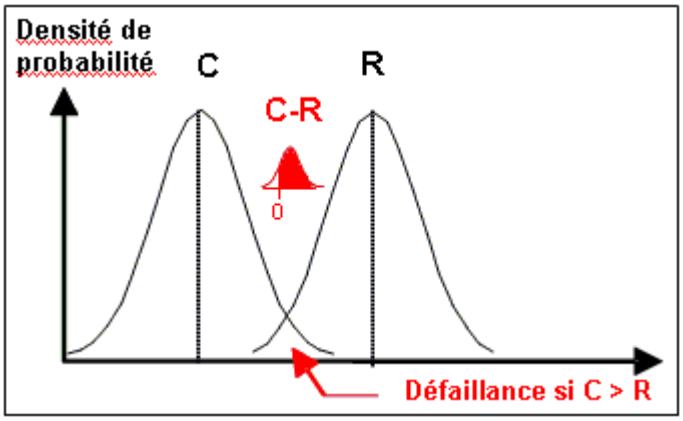
Borne inférieure de l'intervalle unilatéral de la loi binomiale :

$$\sum_{k=m}^{n} C_n^k p^k (1-p)^{n-k} = \alpha$$



N° 15 – Utilisation abusive d'une méthode d'évaluation

L'existence d'une méthode de calcul, aussi rigoureuse soit-elle, ne garantit pas la validité des résultats obtenus qui sont également conditionnés par la justesse des hypothèses et des données d'entrée. La méthode Résistance-Contrainte ne fait pas exception et les évaluations de fiabilité réalisées en mécanique n'ont de sens que si les distributions des contraintes et des résistances sont parfaitement connues.



A supposer que les distributions soient normales, ce qui est déjà discutable, une erreur d'écart type peut avoir un fort impact sur le résultat :

C : moyenne = 8 / écart type = 2 R : moyenne = 16 / **écart type = 2** -> fiabilité = **0,997**

C : moyenne = 8 / écart type = 2 R : moyenne = 16 / **écart type = 3** -> fiabilité = **0,986**

N° 16 – Ambiguïté des termes utilisés en fiabilité

Certains termes sont souvent utilisés en fiabilité de manière ambiguë, ce qui ne manque pas de générer des erreurs d'interprétation dans les évaluations. Ainsi les termes **MTBF** : Mean Time Between Failure (durée moyenne entre deux défaillances consécutives), **MTTF** : Mean Time To Failure (durée moyenne de bon fonctionnement avant la première défaillance) et **MUT** : Mean Up Time (durée moyenne de bon fonctionnement) sont régulièrement confondus.
De même le terme imprécis de « tiède » sera utilisé pour caractériser une redondance (le calculateur d'Ariane 5 par exemple) alors que celle-ci est simplement de type **M parmi N** (M éléments nécessaires parmi N), **active ou passive** (selon que N ou seulement M éléments assurent nominalement la fonction attendue avec un délai de reconfiguration éventuel sur l'un des N-M éléments de rechange), **chaude ou froide** (selon l'état énergétique des éléments en redondance passive : l'hypothèse $\lambda off = \lambda on/10$ pouvant, par exemple, être considérée dans les évaluations). Notre redondance « tiède » est ainsi de type **passive chaude** pour limiter la durée de reconfiguration avec une acquisition éventuelle du contexte de reprise par les éléments en redondance.

N° 17 – Oubli de la « panne avance »

Le fonctionnement intempestif d'un système (panne avance) est souvent aussi critique que la perte ou l'absence de fonctionnement (panne retard). Ainsi, le freinage, l'accélération, le passage de vitesse ou le déclenchement d'airbag intempestifs peuvent être la cause d'accidents mortels en voiture.
Or cette possibilité de panne avance est parfois oubliée dans l'analyse des systèmes ou traitée imparfaitement. En effet, le concepteur cherche d'abord à garantir que son produit assure les fonctions pour lesquelles il a été réalisé et les protections associées à ces deux types de pannes sont généralement antagonistes. Ainsi la redondance fonctionnelle augmente le risque de panne avance et la protection contre cette dernière augmente le risque de non-fonctionnement.
On veillera donc à ne pas « déshabiller » l'un pour « habiller » l'autre, notamment quand on cherche à fiabiliser un « design » existant, comme nous l'observons malheureusement trop souvent.

N° 18 – Le Retour (du manque) d'Expérience

Le REX étant à la mode, combien de fiabilistes se retrouvent dans la situation de devoir exploiter « au mieux » le Retour d'Expérience pour justifier les bonnes caractéristiques d'un produit nouveau. Certes, on peut faire appel aux techniques bayésiennes pour enrichir une expérience limitée (voir l'un des TP de cette publication), mais il est parfois difficile de faire admettre que le génie des statistiques et des probabilités ne peut rien face à une quasi absence de données.
Ainsi, après quelques problèmes de jeunesse, la disponibilité opérationnelle d'un système complexe sera généralement bonne les premières années, mais celle-ci est trompeuse si les lots de rechanges à long délai d'approvisionnement ont été notoirement sous-dimensionnés.

N° 19 - Perte de mémoire dans les systèmes non markoviens

Caractérisés par des taux de transition constants (taux de panne ou de réparation par exemple) les systèmes markoviens présentent la singularité de ne dépendre que de leur état présent pour leurs évolutions futures en faisant table rase de leur histoire passée.
Aussi, ces systèmes à états discrets sont-ils particulièrement simples à simuler puisque que leur état à t+1 est leur état à t modifié par une transition unique correspondant à la plus petite valeur de toutes les durées de transitions tirées aléatoirement dans cet état.
Mais à partir d'un tel simulateur, il devient vite tentant de simuler des lois quelconques (de Weibull par exemple au lieu d'exponentielles) sans se rendre compte que le phénomène d'usure que l'on cherche à modéliser sera bien vite oublié.

N° 20 - Sous dimensionnement chronique des stocks de rechange

A partir de la disponibilité opérationnelle attendue, le dimensionnement d'un stock de rechange est souvent réalisé au moyen de la formule suivante proposée dans les normes de Soutien Logistique Intégré (SLI) :

$$\text{Disponibilité} = MUT/(MUT + MDT + P_{\text{rupture du stock}} * TAT)$$

avec :
- MUT (Mean Up Time) : Durée moyenne de bon fonctionnement,
- MDT (Mean Down Time) : Durée moyenne d'indisponibilité hors rupture du stock de rechange,
- TAT (Turn Around Time) : durée de réparation en usine ou de réapprovisionnement,
- N : Nombre d'éléments du stock de rechange,
- $P_{\text{rupture du stock}}$: Probabilité d'avoir plus de N pannes pendant le TAT, en considérant un processus de défaillance poissonnien.

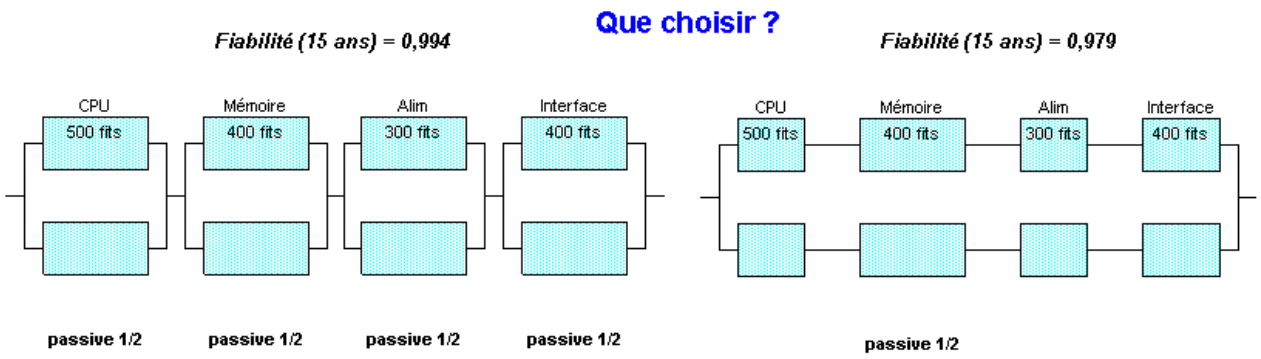
Ce dimensionnement est correct pour un TAT fixe garanti, mais devient notoirement insuffisant si ce TAT est donné en valeur moyenne. La modélisation markovienne, ou la simulation de Monte-Carlo, devient alors incontournable.

N° 21 – Sensibilité du vote aux modes communs

Le vote est un principe de redondance apparemment robuste qui permet de "passiver" une première défaillance. Il consiste à choisir la médiane entre 3 valeurs différentes, telles que les mesures issues de 3 capteurs par exemple, en s'affranchissant, par là même, de la nécessité de localiser la panne. Mais en cas de défaillance affectant 2 entrées, la valeur choisie sera systématiquement la mauvaise. Aussi devra–t-on éviter tout risque de mode commun ou de propagation de panne entre voies en ségrégant correctement les entrées (absence de composants communs, éloignement physique des chemins électriques…) et en fiabilisant les chaînes de mesure, dans le cas de signaux analogiques, si celles-ci ne sont pas différenciées.

N° 22 – Quand le plus fiable s'avère peu sûr

En raison de la nature même d'une quantification incertaine fondée sur des données statistiques toujours sujettes à caution, l'évaluation qualitative et quantitative d'un risque sont indissociables, du moins quand cette dernière peut être réalisée.
Un équipement pourra ainsi inclure de nombreux « cross-stapping » (croisement entre blocs en redondance) afin d'améliorer sa fiabilité, en autorisant diverses combinaisons croisées de fonctionnement, tout en augmentant significativement les risques de propagation de panne qu'il est difficile d'estimer au niveau de ces « cross-stapping » .



N° 23 – Une régression pas toujours linéaire

La régression linéaire consiste à déterminer la droite passant aux mieux à travers un nuage de point et la loi de Student permet de déterminer un intervalle de confiance autour de chacun des points de cette droite. Ainsi peut-on interpoler ou extrapoler à loisir un phénomène physique, à partir d'un recueil de mesures, tout en restant dans les marges rassurantes procurées par un niveau de confiance.
Mais les phénomènes physiques ne sont pas tous linéaires ou leur linéarité est parfois limitée à un domaine restreint. Aussi se méfiera-t-on du « bon sens de l'ingénieur » qui pousse à prolonger dans l'inconnu une connaissance bien souvent limitée.

N° 24 – Un ajustement en manque de points d'appui

Un ajustement consiste à trouver la valeur des paramètres d'une fonction mathématique qui la fait correspondre au mieux à des données expérimentales. La méthode du maximum de vraisemblance est la plus couramment utilisée dans le cas d'une loi de probabilité et différents tests statistiques permettent d'évaluer la qualité de l'ajustement réalisé en comparant la fonction de répartition du modèle théorique avec celle issue des données expérimentales.
Mais un ajustement de qualité ne signifie pas un modèle de qualité surtout quand les données sont rares et les paramètres multiples. Nous avons ainsi rencontré quelques courbes superbes... qui passaient par deux points.

N° 25 – Confusion entre fiabilité et durée de vie

Bien qu'elles évoquent toutes les deux un fonctionnement dans la durée, les notions de fiabilité et de durée de vie correspondent à des performances bien différentes, même quand le produit concerné n'est pas réparable (un satellite par exemple).
La durée de vie caractérise l'aptitude du produit à supporter des dégradations pendant un temps au moins égal à celui de sa mission (consommation d'ergol, usure des mécanismes, dose cumulée des radiations reçues par les composants électroniques, nombre de ON/OFF, nombre de cycles de charge/décharge des batteries d'accumulateurs, dégradation des optiques, etc.) et est validée par des essais de qualification spécifiques et des analyses de dimensionnement en pire cas.
La fiabilité, quant à elle, renvoie à une notion probabiliste de réussite de mission qui dépend de la fiabilité intrinsèque des composants et de l'architecture du produit. Une redondance pourra ainsi améliorer significativement la fiabilité du produit (en début de mission) sans avoir beaucoup d'effet sur sa durée de vie.
A titre d'illustration, la durée moyenne avant défaillance (MTTF) d'un ensemble de n éléments en redondance passive sera au mieux égal à n fois celle de l'élément (MTTFe) et à 2,7 * MTTFe dans le cas d'une redondance active d'une infinité d'éléments.

N° 26 – Quand le virtuel prête à confusion

Proposé à la fin des années 70 par Bradley Efron, le Bootstrap est une méthode de sur-échantillonnage censée améliorer les estimations statistiques. A partir d'un échantillon original, il consiste à générer un grand nombre d'échantillons fictifs, par tirage aléatoire avec remise ; l'objectif étant de mieux exploiter l'information contenue dans l'échantillon original sans créer toutefois aucune information nouvelle.
Ainsi, peut-on estimer des paramètres divers encadrés par un pseudo intervalle de confiance relativement resserré, puisque le nombre d'échantillons générés par tirage aléatoire peut être augmenté à loisir.
Mais les estimations obtenues par cette méthode s'avèrent aussi quelque peu fictives car elles ne correspondent pas à celles de la population mère mais à celles d'une population virtuelle pouvant être générée à partir d'un échantillon. Aussi nous garderons-nous de jouer aux apprentis sorciers.

N° 27 – De si beaux modèles bien mal ajustés

Des modèles paramétriques sont proposés par les théoriciens de la fiabilité pour représenter le comportement des systèmes selon la sévérité de leur environnement ou le type de maintenance dont ils bénéficient.
Ces modèles sont souvent très satisfaisants à l'esprit, tant la logique qui les sous-tend apparaît rationnelle. Mais ils ne peuvent représenter la réalité que si leurs paramètres ont été correctement ajustés à partir de données de retour d'expérience.
A cette fin, la méthode du maximum de vraisemblance est la plus couramment utilisée mais elle ne peut se suffire d'une simple technique d'optimisation locale (gradient, simplexe..) quand les optima sont multiples, ce qui s'avère très souvent le cas pour ces modèles.
Mais cela ne semble guère gêner certains utilisateurs des outils existants qui considèrent le plus souvent ces derniers comme des boîtes noires.

N° 28 – Une indispensable ségrégation

Disposant de composants électroniques toujours plus performants, des concepteurs talentueux imaginent régulièrement d'intégrer des systèmes complets au sein d'une même puce.
Mais les risques de propagation de panne à l'intérieur d'un composant sont difficilement maîtrisables. Aussi, le fiabiliste ne manquera pas de rappeler l'indispensable ségrégation à assurer entre chaînes redondantes ou entre fonction et surveillance ou protection.
Est-ce pour autant freiner l'innovation ? Si ces règles sont prises dès les premières phases de la conception, elles n'engendrent qu'un redécoupage des architectures et n'ont qu'un impact marginal sur les coûts qui se révèlent alors sans commune mesure à celui des justifications peu convaincantes qui devront être fournies a posteriori.

N° 29 – Une réutilisation hasardeuse

Outre son intérêt économique, la réutilisation de composants matériels ou logiciels dont le bon fonctionnement a déjà été « prouvé » en exploitation est un gage de fiabilité des produits.
Encore faut-il que les performances requises, les conditions d'exploitation et l'environnement supporté dans la nouvelle application correspondent rigoureusement à ceux du retour d'expérience.
Aussi apparaît-il bien hasardeux de faire l'économie d'un complément de qualification quand subsiste le moindre écart.

N° 30 – Une propagation de panne quelque peu insidieuse

Pour limiter l'effet d'un éventuel court-circuit, la barre d'alimentation d'un équipement est généralement protégée par un disjoncteur, ou un fusible, souvent associé à un moyen de déconnexion.
Mais un court-circuit partiel peut ne pas pouvoir activer la protection tout en générant une dissipation thermique suffisante pour endommager ou stresser à plus ou moins long terme d'autres équipements à proximité.
Aussi doit-on vérifier l'innocuité d'un tel événement au courant maximal supporté par la protection soit de manière permanente, soit pendant une durée limitée si la déconnexion a été envisagée. Mais la détection de la panne et la coupure de l'alimentation doivent alors s'effectuer dans un délai suffisamment bref pour éviter tout dommage, dont notamment la perte de la fonction de commutation… Après soudure de leurs contacts quelques relais se révèlent parfois inopérants.

N° 31 – Un effort souvent mal dimensionné en Sûreté de Fonctionnement

Une classe est parfois attribuée aux projets par les décideurs, selon leur importance et l'effort consenti à leur développement. Ainsi, les actions d'assurance produit pourront dépendre de cette classe, de même que le niveau de qualité des composants utilisés.
Mais une classe ne recouvre pas forcément le niveau de risque encouru et un projet apparemment anodin peut parfois générer les pires ennuis.
Aussi se méfiera-t-on du volume alloué aux études en Sûreté de Fonctionnement qui ne peut être réellement estimé qu'au terme d'une analyse préliminaire dont l'objet est justement d'identifier les risques encourus.

A titre d'illustration le développement d'une table de radiologie n'a rien à voir avec celui d'un avion… bien qu'elle puisse engendrer bien des dommages parmi ses très nombreux usagers.

N° 32 – Une communication autour du risque bien dévalorisée

Qu'il s'agisse d'accidents sanitaires ou environnementaux, la communication constitue l'un des moyens privilégiés pouvant être mobilisés dans le cadre d'actions préventives ou correctives. Mais à force de chercher à montrer que les situations sont parfaitement maîtrisées par des décideurs d'exception, rassurer des populations « définitivement immatures » qui ne demandent qu'à s'affoler, dégager sa responsabilité sur d'incertains périls, se différentier dans un univers médiatique encombré, …voire en tirer avantage à des fins mercantiles, la communication autour du risque est devenue progressivement inaudible tant sa crédibilité fait aujourd'hui défaut.
Mais les discours improbables, émanant autant de décideurs que d'autorités pseudo scientifiques, ont non seulement pour effet d'aggraver les situations présentes mais également de favoriser l'incohérence des comportements individuels durant les prochaines catastrophes.
Nous pouvons ainsi comparer les effets dévastateurs de certaines affirmations sur le déplacement de nuages radioactifs à l'extérieur de nos frontières ou de certaines mesures à prendre face à l'actuelle pandémie grippale ... à l'incroyable mobilisation crée en son temps par le discours de vérité d'un grand homme d'Etat : « je vous promets du sang et des larmes … » (Winston Churchill).

N° 33 – La maîtrise des incertitudes par une communication maîtrisée

Du théoricien au décideur, la communication est souvent difficile. Aussi, la décision est-elle parfois biaisée par incompréhensions ou manque d'information. Cette difficulté concerne tout particulièrement les analyses statistiques pour lesquelles certaines limitations et hypothèses sous-jacentes font souvent partie d'un « non dit » connu des seuls experts.
Ainsi, un niveau de confiance sera compris par le béotien comme la probabilité que l'information, qui entre dans la prise de risque qu'engage sa décision, soit exacte. Or, c'est souvent beaucoup plus compliqué. Celui-ci concerne, en fait, l'adéquation de données à un modèle, dont la justesse n'est généralement pas garantie, et qui est parfois utilisé dans un domaine d'extrapolation par rapport à toute l'expérience acquise. De plus cet indicateur est souvent évalué de différentes manières pour tenter de le conforter (inversion de la matrice de Fisher, Bootstrap …) qui posent, elles-mêmes, un certain nombre de questions.
Si nous nous en satisfaisons dans bien des domaines, ce flou nous interpelle quand il concerne des études de sécurité. Aussi appelons-nous de nos vœux un dialogue fructueux entre experts et praticiens pour tenter de le dissiper.

N° 34 – Quand la Sûreté de Fonctionnement se moque de la résilience

Se cantonnant aux limites du produit, la sûreté de Fonctionnement se soucie rarement d'interdépendance. Ainsi, par divers apports réglementaires et normatifs, nos moyens de chauffage sont devenus plus sûrs qu'auparavant, mais s'avèrent inopérants sans électricité. De même les relais téléphoniques, fixes ou mobiles, et les répartiteurs Internet présentent aujourd'hui une disponibilité honorable mais sont tous raccordés au réseau électrique. Il est alors facile d'imaginer les conséquences de la succession de deux événements relativement probables : une forte tempête semblable à celle de janvier 2009 dans les Landes (Klaus) immédiatement suivie d'une période de grand froid telle que nous l'avons connue cette année.
De même, les schémas routiers adoptés dans nos villes, où fleurissent ralentisseurs et ronds-points en tout genre, conduiraient immanquablement à une thrombose généralisée en cas de catastrophe urbaine (telle que celle de l'usine AZF de Toulouse en 2001 heureusement sans dégagement de phosgène).
Comment sensibiliser les décideurs à la notion de résilience ?

N° 35 – Vote entre 4 capteurs de type min de max (ou max de min)

Voici à nouveau un système à 2 modes de défaillance incompatibles (valeur trop haute ou trop basse) faisant l'objet de protections antagonistes, comme la panne avance et la panne retard vues dans un précédent bêtisier. Il importe de bien séparer ces modes dans les évaluations afin d'éviter une erreur grossière, généralement très optimiste.
Le vote min de max peut se modéliser par une redondance 1 parmi 2 entre blocs de 2 capteurs en série, pour la défaillance de niveau haut, en série avec 2 blocs constitués chacun d'une redondance 1 parmi 2, pour la défaillance de niveau bas (ou inversement pour le vote max de min). Ces pannes de capteurs doivent être complétées par celles éventuelles des comparateurs.

N° 36 – La qualité des groupes d'experts

Des « experts » se rassemblent régulièrement dans divers groupes méthodologiques, comités scientifiques ou instances de normalisation pour orienter la recherche, indiquer les bonnes pratiques ou aider à la prise de décision.
Attendues tel que l'oracle dans la Grèce antique, leurs recommandations avisées engagent toute une communauté…. mais aussi la réputation des organismes qui les mandatent.
Car en dépit de leurs notoriétés et compétences, les experts n'en sont pas moins Homme et leurs motivations ne s'avèrent guère plus élevées que celles de leurs congénères.
Aussi observe-t-on parfois certaines dérives telles que :

- le détournement du groupe par un lobbying actif,
- la privatisation des travaux à des fins personnelles,
- la cooptation et l'absence de renouvellement,
- le mandarinat et ses effets pervers,
- la coupure sur le monde extérieur,
- la fermeture aux idées nouvelles,
- l'obsolescence de l'expertise,
- l'incompétence,
- l'opacité,
- etc.

Plus que dans tout autre domaine, l'erreur en maîtrise des risques n'est pas sans conséquence. Aussi, ne pouvons nous qu'inviter les décideurs des organismes concernés par l'aléa à veiller à l'excellence des travaux d'expertise réalisés en leur nom, afin de ne pas risquer de perdre toute crédibilité telle que l'OMS avec ses recommandations vaccinales ou l'agence américaine de normalisation des installations pétrolières.

N° 37 – De la bonne utilisation des alarmes

La fiabilisation de la majorité des systèmes à risques passe par l'implantation de diverses alarmes censées prévenir l'opérateur que la situation n'est plus totalement sous contrôle et qu'une action est requise de sa part.
Afin d'assurer un bon niveau de sécurité, le concepteur a tendance à limiter, autant que possible, le risque de non détection d'anomalies même si cette approche conduit parfois à quelques fausses alarmes (déclenchements intempestifs).
Mais cette quête de la perfection s'effondre bien vite le jour où l'opérateur excédé finit par débrancher les surveillances, comme cela semble avoir été le cas sur la plateforme pétrolière de British Petroleum qui explosa le 20 avril 2010 dans le Golfe du Mexique.
Aussi, devrions nous autant nous méfier du taux de fausse alarme que de non-détection, bien qu'il soit souvent oublié dans les études de sécurité.

N° 38 – La preuve par l'outil

Pour le fiabiliste prudent (ce qui est un pléonasme) se méfiant des résultats obtenus à partir d'outils informatiques insuffisamment transparents, le bon sens dicte d'effectuer quelques comparaisons entre plusieurs d'entre eux.
Mais outre l'outil, c'est parfois la méthode qui est sujette à caution. Or celle-ci se verra recopier mille fois, sous la caution bienveillante d'une obscure publication, par le simple jeu de la concurrence entre fournisseurs.

N° 39 - Une si jolie boîte noire

Si l'outil informatique rend d'inestimables services, son usage écervelé conduit parfois aux pires excès. L'outil devient alors une boîte noire dont les résultats ne souffrent d'aucune critique mais dont l'apparence se doit d'être parfaite. Aussi, l'essentiel de l'effort de Recherche & Développement porte-t-il sur l'ergonomie et l'interface à un utilisateur passif que l'on ne craint pas d'infantiliser.
Un outil d'ajustement se doit ainsi de proposer la loi de probabilité qui présente le meilleur résultat d'un test statistique (khi-deux, Kolmogorov...), même s'il nous apparaît parfaitement imbécile de procéder à un ajustement sans choisir au préalable la loi susceptible de correspondre, au mieux, à la physique du phénomène étudié.

N° 40 - Comment générer des catastrophes conformément à la 61508 ?

La norme EN 61508 recouvre des préconisations sur la sécurité fonctionnelle de nature qualitative et quantitative.

- Les premières portent notamment sur le niveau de tolérance aux défaillances des architectures pour lequel la proportion de défaillances en sécurité (correspondant au taux de panne conduisant à un état de sécurité ou détectée par un test de diagnostic) constitue le principal critère de dimensionnement. Or pousser un test de diagnostic s'avère souvent beaucoup moins onéreux que de fiabiliser un équipement de piètre qualité. Souvent en réparation, celui-ci présentera un risque non négligeable de panne cachée dangereuse durant son fonctionnement.

- Les secondes portent sur des calculs en valeur moyenne de PFH ou PFD (correspondant à la probabilité de panne dangereuse par heure ou à la sollicitation) qui peuvent être affectées par une maintenance imparfaite ou des dépendances cachées de diverse nature. Ainsi, la synchronisation d'actions de maintenance sur différentes entités du système peut significativement fausser des résultats calculés en valeur moyenne.

N° 41 - Erreurs dans les modèles markoviens

Un modèle markovien décrit à la fois le comportement d'un système et la manière de l'opérer. Sa réalisation est souvent délicate mais le respect de quelques règles simples limite les risques d'erreurs grossières.

1 – Au delà des cas triviaux, le graphe de Markov est à bannir au profit de la matrice de Markov qui permet de visualiser toutes les transitions possibles entre états.

2 – L'identification complète des états du système est facilitée par l'ordonnancement de ces derniers suivant les niveaux de dégradation progressifs.

3 – Dans chaque ligne de la matrice de Markov, la somme des taux de défaillance doit correspondre à celui de l'ensemble des équipements encore en bon fonctionnement dans l'état correspondant.

A titre d'exemple, la norme EN 61508 requiert de considérer les modes communs au moyen d'un pourcentage Bêta du taux de défaillance des éléments en redondance. Une redondance étant constituée d'au moins deux éléments, chacun d'entre eux doit être considéré individuellement dans la matrice de Markov puisqu'il est susceptible de défaillir.

N° 42 - Quand le groupe de travail finit par s'assoupir

Un groupe de travail a pour objet la réalisation d'un travail collectif par un ensemble de personnes qualifiées. Mais cette œuvre commune s'estompe parfois avec le temps sans qu'aucune décision de dissolution ne soit prise. L'absence de production ne nuit nullement à la cohésion d'une instance conviviale qui offre un statut à chacun de ses membres, dont les capacités s'amenuisent peu à peu.
Faut-il s'en offusquer ? Ce groupe occupe une place, que d'autres pourraient prendre, et influence une communauté par diverses prescriptions devenues obsolètes que peu rejetteront. Aussi, nous arrive-il parfois de ressentir imperceptiblement les chaudes effluves d'un vent du sud qui nous susurre à l'oreille : « Dégage !».

N° 43 - Les limites du dialogue technique

La maîtrise d'un système passe par la mise en commun de connaissances partagées entre le Maître d'œuvre et ses divers fournisseurs.
Le Maître d'œuvre ignore certains comportements « exotiques » en fonctionnement ou dysfonctionnement d'équipements comprenant toujours plus de logiciels et de circuits intégrés, dont la visibilité est bien souvent limitée par des clauses de confidentialité.
Le fournisseur méconnaît les conditions réelles d'exploitation du système et les interdépendances entre ses divers constituants.
Seule une solide analyse de risques au niveau du système suivie d'un véritable dialogue entre les intervenants permet de maîtriser cette complexité.
Mais ce processus n'est pas facile à mettre en œuvre dans un cadre contractuel et se limite parfois à une simple gestion de couvertures de documents sous-traités de part et d'autre.

N° 44 - Les bienfaits de la sous-traitance

La quête insatiable de productivité conduit l'entreprise à choisir systématiquement les acteurs moins disants en terme de coût horaire.
Les métiers subalternes sortent rapidement de son activité, puis des spécialités, telle que la Sûreté de Fonctionnement, sont progressivement externalisées. Elles sont, dans un premier temps, sous-traitées à des cabinets d'experts, puis à des généralistes capables de fournir, du moins sur le papier, à peu près toutes les compétences, à n'importe quel prix, dans les plus brefs délais.
Le savoir-faire de l'organisation se transforme alors en un savoir faire-faire puis en un s'avoir faire-faire-faire afin que l'activité et le suivi de celle-ci puisse vraiment s'opérer au minimum de coût…
… Au moindre coût horaire, bien sûr, car l'objectif n'est plus alors de résoudre efficacement les problèmes de l'entreprise mais de faire perdurer les contrats de part et d'autre.

N° 45 - Qui trop embrasse mal étreint

L'AMDEC (Analyse des Modes de Défaillance, des Effets et des Criticités) est une analyse des dysfonctionnements qui fait appel à une démarche déductive pour en imaginer les causes ou inductive pour en évaluer les effets.
Son principal objet est l'identification des risques (inconnus a priori), mais elle se transforme parfois en une sorte de matrice de conformité au CDCF (Cahier Des Charges Fonctionnel) au risque de faire perdre au fiabiliste une bonne part de son acuité.

N° 46 - La meilleure raison pour ne rien faire

La Sûreté de Fonctionnement se nourrit de Retour d'Expérience mais bien peu d'entreprises exploitent les données opérationnelles de leurs produits.
Certes, la collecte des données est parfois difficile, mais la principale raison invoquée pour ne rien faire est que la statistique impose trop d'heures de fonctionnement cumulées avant que les estimations atteignent les objectifs attendus. Un simple traitement bayésien permet pourtant de s'affranchir de cette difficulté. Il suffit d'initialiser l'estimation par un a priori, tel qu'une estimation prévisionnelle issue d'une base de données ou obtenue par analogies, puis d'attendre patiemment que cette donnée se consolide d'un réel vécu.
Cette base d'information devient alors un véritable puit de connaissances… du moins si l'on se donne la peine de l'exploiter.

N° 47 - Le mieux est l'ennemi du bien

L'estimation de fiabilité se nourrit de modèles. Selon les spécificités du système et des caractéristiques à évaluer, celui-ci sera statique ou dynamique, limité à des angles de vue particuliers et entrera plus ou moins profondément dans le fonctionnement intime des divers constituants.
Mais qui n'a pas rêvé d'une modélisation parfaite, tant sur les aspects fonctionnels que dysfonctionnels, permettant de réaliser automatiquement toutes les analyses de sûreté de Fonctionnement d'un simple clic d'ordinateur ?
Lancée depuis déjà quelques décennies, cette quête à la modélisation globale resurgit périodiquement selon les progrès de l'informatique. Mais outre l'assemblage d'éléments simples au comportement parfaitement connu, celle-ci apparaît utopique et présente même des risques si la complexité n'est pas bien maîtrisée. Aussi, vaut-il mieux éviter de complexifier la modélisation au-delà du juste nécessaire par rapport au besoin.

N° 48 – Un bêta qui porte bien son nom

Introduit par la norme 61508, le bêta permet de considérer les modes communs dans les estimations de fiabilité.
Si l'intention parait louable de ne pas oublier ce type de risque et de chercher à promouvoir tout ce qui peut le limiter, sa quantification pose un certain nombre de questions.
- Le risque de mode commun dépend avant tout des choix de ségrégation et de diversification des chaînes en redondance et n'est pas directement proportionnel à leur taux de défaillance.
- L'existence même d'une quantification, qui est ici largement « pifométrique » en dépit des diverses communications dont elle fait l'objet, peut libérer des consciences et autoriser parfois des conceptions invraisemblables, telles que l'intégration complète de fonctions critiques et de leurs surveillances au sein d'un même composant électronique, par exemple.
La normalisation et la standardisation simplifient les études de sûreté de fonctionnement qui sont dorénavant le plus souvent confiées à des non-spécialistes dans un contexte forcené de diminution des coûts…. Souhaitons qu'elles ne deviennent pas l'œuvre de simples d'esprit !

N° 49 – Sur et sous dimensionnement résultant du déterminisme pire cas

Si la maîtrise des risques est censée apporter de la robustesse en conception, elle peut paradoxalement favoriser un risque particulièrement redouté du décideur mais parfois oublié du fiabiliste : le surdimensionnement ou l'obsolescence du produit par rapport à la concurrence.
Le produit est traditionnellement dimensionné pour assurer une mission de référence dans les pires cas de fonctionnement combinant toutes les conditions extrêmes (tolérance de composant, vieillissement, température, état énergétique, etc.)
Cette approche, qui simplifie la validation en limitant les vérifications à un cas de référence unique, peut conduire à un surdimensionnement général et à l'impossibilité de bénéficier de certains effets de seuil (utilisation de composants disponibles notamment). Par ailleurs, l'utilisation fréquente de coefficients de sécurité n'assure qu'une maîtrise partielle des dispersions.
Aussi existe-t-il une autre approche qui considère les aléas de toute nature, dont notamment ceux relatifs à la mission, et autorise occasionnellement des interruptions du service en raison d'un manque transitoire de performances ou de ressources (une mission plus contraignante que la mission de référence étant en revanche tolérée tant que les conditions le permettent).
Ce dimensionnement probabiliste impose l'emploi généralisé de la simulation ainsi qu'une méthode de validation à partir des résultats de celle-ci. La méthode d'estimation de quantiles proposée par Wilks répond à cette nécessité mais le poids des habitudes et le conservatisme ambiant freinent l'émergence de cette approche radicalement nouvelle dans notre monde industriel.

N° 50 – Quand la théorie tente de maîtriser les extrêmes

Fondée sur le retour d'expérience, la théorie des valeurs extrêmes propose un cadre méthodologique pour estimer la probabilité d'événements rares dont notamment celles utilisées pour dimensionner les systèmes à risques susceptibles d'être confrontés à des conditions naturelles hors norme. Son principe consiste à modéliser une queue de distribution au moyen d'une loi de probabilité que l'on ajuste à partir de données maximales périodiques ou de données dépassant une valeur de seuil (voir TP n° 26). Une confiance asymptotique sur la valeur d'un quantile peut être alors obtenue à partir de la matrice de Fisher par les méthodes delta et de Wald.
Mais ces brillants calculs supposent évidemment que les données exploitées soient parfaitement représentatives du phénomène considéré et en nombre suffisant sur des durées parfois très longues. C'est la raison pour laquelle la hauteur de la vague dépasse parfois celle de la digue, que la crue emporte quelques ouvrages d'art, que le niveau du fleuve se révèle insuffisant pour refroidir la centrale, que le tremblement de Terre occasionne des dégâts inimaginables jusqu'alors, etc.

N° 51 – L'anticipation des comportements

De multiples modèles de fiabilité d'architecture de système sont développés en conception pour prévoir les comportements futurs et garantir l'adéquation au besoin durant la mission.
Ces modèles reposent sur des hypothèses sous-jacentes implicites telles que le taux de défaillance constant pour la majorité des composants électroniques ou des lois d'usure progressive pour certains mécanismes (Weibull).
Mais, ces hypothèses peuvent être remises en cause, notamment ce taux de panne constant qui aurait une fâcheuse tendance à ne plus l'être après une durée plus ou moins longue d'utilisation de composants électroniques toujours plus intégrés (loi de Bertholon).
Faut-il s'en alarmer ?
Certes les tenants de l'obsolescence programmée y trouveront là leur compte mais le fiabiliste peut d'ores et déjà s'y préparer en suivant au mieux le retour d'expérience sur les technologies nouvelles et en mettant à jour les modèles dépassés.

N° 52 – L'innovation est-elle bien maîtrisée ?

Créé par la NASA en 1989, l'indice TRL (Technological Readiness Level) permet de mesurer le degré de maturité technologique d'une innovation pour mieux en évaluer les risques d'emploi.

TRL 1 - Principes généraux
TRL 2 - Concept technologique
TRL 3 - Expérimentation et preuve du concept
TRL 4 - Composants basiques produits à échelle de laboratoire
TRL 5 - Composants basiques produits en environnement simulé
TRL 6 - Production de prototype de démonstration
TRL 7 - Prototype opérationnel dans son environnement final
TRL 8 - Qualification complète
TRL 9 - Utilisation validée dans plusieurs configurations

Bien que les risques encourus et l'effort à supporter pour monter en niveau de TRL dépendent fondamentalement des technologies mises en oeuvre, cet indice est devenu aujourd'hui un outil de management quelque peu simpliste qui élimine sans discernement tout niveau supérieur à 3 dans le domaine de la Recherche & Développement et tout niveau inférieur à 7 dans le cadre des nouveaux développements.
Or si l'absence d'audace offre une certaine quiétude aux décideurs, elle engendre surtout un risque bien réel d'obsolescence par rapport à la concurrence et d'exclusion à terme des différents marchés.
Certes, la surchauffe inopinée des batteries au lithium du Boeing 787 fait cruellement souffrir son constructeur mais craignons que d'autres ne les choisissent en plomb.

N° 53 – Le fiabiliste de la 25ème heure

Rattaché à un service qualité afin de bénéficier d'une indépendance théorique, ou par le hasard des chicaneries de prérogatives dans les organisations, le fiabiliste se retrouve parfois fort éloigné de l'activité d'ingénierie.
Sorte de super contrôleur de produits quasiment finalisés, il effectue (ou sous traite) des analyses parfois volumineuses sur les dysfonctionnements possibles d'une conception détaillée afin de répondre, avant tout, à une demande contractuelle.
Ses recommandations arrivent alors bien tard et conduisent au mieux à quelques palliatifs, au pire au sourire gêné d'un chef de projet alors tout autant à cours de budget que de planning.
Sa valeur ajoutée serait probablement tout autre s'il intervenait très en amont au sein de l'équipe de conception afin d'identifier les risques quand tout n'est encore que papier et qu'ils peuvent être maîtrisés à un coût raisonnable. Il participerait alors avec le gestionnaire des coûts à l'optimisation d'un produit contraint par des exigences de performances et de Sûreté de Fonctionnement, du moins si le choc des cultures l'autorise dans l'entreprise.

N° 54 – Langues orientales et fiabilité

A force de délocalisations et de renoncements multiples, notre expertise dans la technologie se limitera bientôt à savoir choisir « le bon chinois » susceptible de nous fournir « le bon produit ».
Mais, outre l'achat de ce dernier que l'on sait encore à peu près spécifier, sa maîtrise impose d'appréhender ses comportements nominaux et dégradés afin de pouvoir l'intégrer correctement dans un système.
Or cette connaissance stratégique devient de plus en plus difficile à acquérir, telle que celle concernant la batterie au lithium et phosphate de fer (LiFePO4) et son BMS (Batterie Management System) qui nous a fait particulièrement défaut lors de la mise au point de notre lampadaire solaire autonome.
Aussi, conseillerions-nous d'intégrer une solide connaissance des langues orientales dans le cursus universitaire des futurs fiabilistes.

N° 55 – Risques et inflation des exigences

La normalisation (ou standardisation) cherche moins à diffuser de bonnes pratiques que d'imposer celles des organisations représentées dans les comités normatifs afin de renforcer leur position dominante ou concurrentielle.
Ce processus, hors contrôle, touche notamment la Sûreté de Fonctionnement qui s'enrichit régulièrement de documents divers dont chacune des phrases, qu'elle soit pertinente, discutable, redondante ou superflue, constitue autant d'exigence nouvelle susceptible de s'imposer à tous.
Certes, de nouveaux outils de gestions permettent de gérer automatiquement ces exigences et génèrent sans effort des spécifications diverses qui grossissent à vue d'œil.
Mais outre les notables surcoûts engendrés par cette inflation des exigences, la vérification formelle de leur tenue devient vite impossible et le risque s'accroit à force de faire semblant de bien le contenir.

N° 56 – Risque mission et roulette russe

Les systèmes engendrant des risques pour les personnes ou les biens doivent respecter des exigences sécuritaires qui limitent la probabilité d'occurrence des évènements redoutés durant leur mission à un seuil acceptable ou du moins tolérable. L'architecture et la mise en œuvre de ces systèmes font alors l'objet de diverses analyses et essais dont les résultats sont regroupés dans un dossier de sécurité justifiant la tenue de ces exigences.
Mais pour toutes sortes de raisons, économiques, scientifiques, techniques... il est souvent tentant de prolonger la mission, surtout quand celle-ci s'est déroulée jusqu'alors sans incident majeur. Certes, un complément du dossier de sécurité est alors établi pour assurer à nouveau la tenue des exigences… mais le risque pris est alors accepté autant de fois que la mission est prolongée à la manière du révolver dans le jeu de la roulette russe.

N° 57 – Complexité physique et exactitude statistique

L'estimation de fiabilité se nourrit de modèles plus ou moins complexes qui cherchent à mettre en équation des durées de fonctionnement ou des processus de vieillissement.
Ces modèles se fondent sur des données statistiques opérationnelles ou d'essais ou tentent de se raccrocher à la physique des phénomènes de défaillance.
Portant sur le dimensionnement des architectures en conception puis sur l'optimisation de la maintenance en exploitation, leur utilisation requiert d'autant moins de précision que les systèmes mettent en jeux des redondances multiples.
Aussi, apparait-il bien souvent illusoire de copier la nature dans ses moindres détails quand la complexité nous éloigne de l'exactitude, qui ne se juge que dans la durée face à la réalité des faits.

N° 58 – La confiance n'exclut pas le contrôle

Les évaluations de disponibilité ou de fiabilité opérationnelle font appel à des techniques de modélisation plus ou moins complexes supportées par des outils de calcul ou de simulation. La méthode employée doit être en adéquation avec la problématique, c'est-à-dire suffisamment riche pour décrire au bon niveau les comportements du système mais aussi la plus simple possible pour limiter les efforts d'analyse et surtout les risques d'erreur de modélisation.
Or la lecture de certains dossiers justificatifs, souvent volumineux et disparates, révèle des modélisations peu lisibles ainsi que des hypothèses mal explicitées.
Quelle que soit la compétence du fiabiliste, son travail doit pouvoir donner lieu à une contre-expertise, au-delà de la simple gestion des couvertures de document, notamment quand la disponibilité interagit avec certains aspects sécuritaires.

N° 59 – Ne pas abuser des belles formules

Certaines de nos universités et grandes écoles s'évertuent à donner une importance démesurée au calcul mathématique, parfois au détriment même de leurs enseignements. Il ne serait pas sérieux d'envisager un cours sans équations multiples et intégrales diverses pour l'agrémenter.
Cette approche présente cependant quelques inconvénients :
- elle rend obscure des choses relativement simples, freine leur acquisition et limite leur diffusion,
- elle tend à simplifier les phénomènes qui ne se laissent pas toujours mettre en équation,
- elle ralentit la diffusion de techniques de modélisation et simulation beaucoup plus efficaces
- elle glorifie les aspects théoriques en oubliant parfois le sens commun,
- elle fatigue le vérificateur des travaux réalisés qui perd un temps précieux à tout redémontrer

Ainsi, trouvons-nous parfois de très jolies formules analytiques pour exprimer la fiabilité d'architectures diverses dont nous vérifions la validité en quelques minutes par comparaison des résultats avec ceux d'un simple modèle markovien.

P.S. Nous ne résistons pas à vous conter la savoureuse mésaventure d'élèves de l'une de nos brillantes écoles d'aéronautique qui optimisèrent très finement les performances d'un drone en croisière en oubliant, jusqu'aux essais, qu'un avion... ça décolle !

N° 60 – Une complexité pas si facile à maitriser

Si la lecture de certaines publications académiques peut donner l'impression qu'appréhender la complexité ne résulte que du choix judicieux de quelques méthodes et outils, les prédispositions propres à l'analyste ne doivent pas être négligées. Celui-ci doit savoir notamment dissocier l'essentiel de l'accessoire, traiter le global avant de s'intéresser au local, et démêler l'interdépendance de l'indépendance, source de simplification et traitements différenciés.
Aussi, apparait-il quelque peu hasardeux de confier l'évaluation d'un système complexe à une personne sans expérience comme le proposent parfois certains généralistes dans le domaine de la fiabilité.

N° 61 – Des stocks de rechanges mal dimensionnés

La constitution de stocks de rechanges s'avère indispensable au maintien opérationnel d'un service, tant les durées de retour en usine ou de réapprovisionnement des matériels (Turn Around Time) se révèlent parfois très longues.
Ces stocks étant évidemment onéreux, on peut chercher à les dimensionner en procédant à une optimisation sous contrainte de la disponibilité du service attendu, à partir du modèle complet du système et de son soutien logistique ou du moins à partir d'un modèle analytique simplifié utilisant la loi de Poisson.
On peut également prévoir une unité pour chaque élément du stock, comme le propose certains programmes de soutien, en priant pour que la disponibilité opérationnelle ne s'éloigne pas trop de la disponibilité intrinsèque à stock infini.

N° 62 – L'exploitation d'un REX hétérogène

L'exploitation de données opérationnelles peut être riche d'enseignement, mais celles-ci sont souvent acquises dans des conditions d'utilisation et d'environnement très différents. Le véhicule conduit par une brute hors des chemins balisés risque fort de vieillir bien plus vite que celui du conducteur ordinaire.
Aussi, peut-on aisément mitonner une soupe statistique en mélangeant des choux et des carottes. On peut également faire appel à des experts pour pondérer les données en fonction de leur provenance, selon une approche qui s'assimile parfois au doigt mouillé teinté de techniques bayésiennes.

On peut enfin relever les conditions d'acquisition des données sous forme de covariables (température, niveau vibratoire, humidité…) et traiter les données avec ces dernières afin d'acquérir simultanément les paramètres des modèles de fiabilité ou de dégradation et ceux des modèles d'accélérations qui rendent compte de l'hétérogénéité.

N° 63 – Savoir passer à la simulation

L'expertise d'un analyste porte avant tout sur sa capacité à choisir une méthode face à une problématique. Elle recouvre la connaissance des domaines et limites de chacune d'elles et l'appropriation de critères décisionnels pertinents. La simplicité constitue le premier qui conduit à éviter d'utiliser le marteau pilon pour écraser une mouche. La lisibilité en est un second qui nous rappelle que tout travail d'analyse doit pouvoir faire l'objet d'une contre-expertise et que les premières erreurs proviennent d'incompréhensions entre les acteurs. La précision et la rapidité de calcul en est un troisième. Les habitudes organisationnelles peuvent en constituer un autre …
L'emploi de méthodes pseudo analytiques (arbre de défaillance dynamique par exemple) apparait vite hasardeux au-delà du raisonnable. La complexité et l'interdépendance engendrent rapidement une explosion combinatoire qui ne laisse plus le choix et impose la simulation de Monte-Carlo. Le traitement est alors sensiblement plus long mais rarement rédhibitoire. En effet sa durée dépend peu de la taille du système considéré mais surtout du nombre moyen d'évènements aléatoires qui se produisent au cours de sa mission. A titre d'exemple, un avion est un objet relativement complexe mais si sa disponibilité opérationnelle n'était pas accessible par la simulation, nous pourrions craindre qu'il reste éternellement bloqué sur son aéroport.

N° 64 – L'insondable gaspillage engendré par la fonction copier-coller

Si chaque exigence d'une spécification répond, peut-être, à un besoin, elle est toujours génératrice de coûts. Ce fait, fréquemment oublié par les donneurs d'ordres, concerne notamment la Sûreté de Fonctionnement dont les exigences, recopiées parfois de programme en programme et formulées souvent de manière ambiguë, peuvent se révéler ruineuses. Ainsi, une exigence de durée de vie ou de fiabilité conditionne directement la durée d'amortissement d'un matériel et il est inutile de se situer en-deçà de l'état de l'art si le service attendu est pérenne. De même une exigence de disponibilité caractérise le niveau de tolérance à la perte momentanée du service mais dimensionne aussi les architectures (redondance), les opérations (en heures ouvrables ou au-delà), les contrats de maintenance et de réapprovisionnement des matériels, les lots de rechanges, etc. Or, de telles exigences résultent souvent de la subjectivité d'un décideur sans réelle analyse d'impact ni identification d'éventuelles dégradations de service tolérées par les usagers. Certes, il existe de beaux outils de gestion des exigences mais nous craignons que leur emploi conduise plutôt à l'inflation qu'à un usage plus raisonné.

N° 65 – Quand la barrière de sécurité engendre des catastrophes

La possibilité de bloquer de l'intérieur la porte des cabines de pilotage des avions de ligne résulte d'une recommandation prise peu après les attentats du 11 septembre 2001. Cette barrière s'avère une protection efficace pour contrer la menace engendrée par la présence de terroristes à bord mais renforce dramatiquement celle du pilote fou.
Ces deux risques contradictoires, tels que la panne avance (fonctionnement intempestif) et la panne retard (absence de fonctionnement), étaient connus avant cette prise de décision funeste, mais le choix de protection aux risques antagonistes conduit à un dilemme.
Aussi, importe-t-il de soupeser chacune des menaces et de ne pas privilégier exagérément l'une d'elles afin de calmer les angoisses générées par la dernière catastrophe.

N° 66 – Quand ceinture et bretelles engendrent des risques

L'activité du fiabiliste consiste à identifier les risques et à les évaluer au mieux afin d'aider à la

prise de décision. Bien que l'évaluation recouvre toujours une part de subjectivité, celle-ci est au service d'une action collective et ne doit pas être biaisée afin d'exonérer son auteur de tous les problèmes à venir. En effet, l'excès de précautions inutiles expose le groupe de travail au risque bien réel de perdre son activité, du jour au lendemain, au profit d'acteurs moins timorés et/ou plus innovants. On se méfiera donc du conservatisme de certains « experts » rétifs à tout changement et des enragés de la normalisation qui multiplient les exigences superflues dans les spécifications.

N° 67 – Quand l'organisation faillit

Loin d'être un adepte de la politique du risque zéro, qui nous engage souvent à ne rien faire, nous estimions jusqu'alors qu'un risque connu était maîtrisable si les préceptes de notre discipline étaient correctement appliqués. Des technologies à haut risque sociétal étaient alors envisageables dans la mesure où le sérieux des équipes de conception et le niveau adéquat des moyens engagés ne faisaient aucun doute.
Mais notre opinion a été quelque peu ébranlée par l'accumulation de révélations concernant des manquements graves à l'éthique au sein d'organisations apparemment irréprochables. Ici, ce sont les résultats d'essais infructueux sur la tenue de matériaux essentiels à la sécurité nucléaire qui sont délibérément cachés, là c'est le ferraillage du béton qui est oublié par d'obscurs sous-traitants...
Quand l'ingénieur laisse sa place au financier, il est temps d'arrêter de jouer dans les domaines techniques à risques… La crise économique que nous a fait subir le système bancaire ne demande qu'à s'y propager.

N° 68 – Dimensionnement des protections électriques

Qu'il s'agisse d'un simple fusible ou d'un disjoncteur plus élaboré, une protection électrique a pour objet de se prémunir des conséquences d'une surconsommation transitoire (courant d'appel…) ou permanente (court-circuit...).
Cette protection est dimensionnée, par analyse et/ou essais, pour supprimer tout risque de propagation de panne (écroulement de l'alimentation, échauffement critique, etc.), sans inhiber cependant les pires cas de fonctionnement nominaux. Il est, en effet, ballot de perdre une chaîne fonctionnelle ainsi que sa redondance en raison d'une protection surdimensionnée, notamment sur un système non réparable tel qu'un satellite.

N° 69 – Faut-il baisser la garde quand les pannes se font rares ?

Outre l'obsolescence intentionnelle programmée par certains à des fins mercantiles, on peut s'interroger, de bonne foi, sur une éventuelle surfiabilisation d'équipements qui ne tombent pas en panne avec pour objectif d'en réduire le coût. Ainsi, la durée de vie des satellites spatiaux dépasse très souvent, et parfois largement, celle qui était prévue et les équipements embarqués sont pour la plupart redondés car leur réparation en orbite n'est pas envisagée. Les fiabilistes seraient-ils incapables de répondre au juste besoin et faut-il incriminer leurs méthodes d'estimation par trop conservatives ?
Les spécifications des clients exigent, pour la plupart, une fiabilité d'environ 70 % en fin de mission, soit 30 % de risque de perte du satellite durant celle-ci, dans un mode nominal ou faiblement dégradé. Ce dimensionnement de bon sens pour un investisseur se traduit par une durée de vie moyenne de 2,8 fois la durée de mission pour un satellite sans redondances (et un peu moins avec), en dehors des limitations en ergol : $T_{mission} / MTTF = -\ln(0,7)$.
Aussi, ne faut-il pas s'étonner que les satellites ne meurent pas comme des mouches, mais il pourrait en être autrement si un pseudo bon sens paysan conduisait à supprimer toute redondance dans la conception des satellites des futures constellations.

N° 70 – A quoi servent les estimations de fiabilité ?

Trop de dysfonctionnements sont observés sur les satellites spatiaux dès leur première année en orbite (perte moyenne de 5 % de la capacité mission) en totale contradiction avec les

estimations prévisionnelles de fiabilité souvent beaucoup plus optimistes (>0,995 à 1 an).
Faut-il remettre en cause les méthodes d'analyse, ajuster à nouveau les recueils de fiabilité de composants, voire rejeter toute quantification ?
Fondée sur le retour d'expérience, l'estimation ne porte évidemment que sur ce qui est quantifiable et exclue donc toute erreur de conception, défaut de fabrication ou stress subi en intégration, dont les effets se manifestent généralement en début de vie.
En revanche, les estimations aident à rendre les architectures cohérentes et susceptibles de répondre à l'exigence de fiabilité exprimée par le client pour toute la durée de la mission, qui apparait alors beaucoup plus en phase avec la réalité observée.
Aussi, n'apparait-il pas judicieux d'ajuster les primes d'assurance aux estimations prévisionnelles, mais peut-être moins encore de se priver de ces dernières.

N° 71 – L'exploitation partisane des données statistiques relatives aux risques

Nous prenons chaque mois connaissance des résultats du baromètre de l'Observatoire National Interministériel de la Sécurité Routière (ONISR) concernant les accidents de la route en France. Pour diverses raisons (amélioration de la voirie, sécurisation des véhicules, actions de prévention, pénalisation des comportements à risques....), le nombre d'accidents a été réduit drastiquement depuis l'année 1972 (18 000 morts) pour atteindre un seuil difficile à franchir (moins de 4 000 morts depuis 2014), avec des dispersions inhérentes à toutes les statistiques que renforcent les variations des conditions météorologiques, du nombre de jours de congé dans le mois et de quelques accidents majeurs (autocars). Mais nos décideurs trouvent une explication à tout : la baisse de février résultera de l'excellence de l'action gouvernementale, l'hécatombe en juillet (de quelques % en sus par rapport à l'année précédente) d'une incompétence de cette dernière dénoncée avec force par les partis d'opposition ou d'un relâchement des comportements qu'il faudrait immédiatement corriger par un renforcement accru des dispositifs de surveillance (radars), des limitations de vitesse et de la sévérité des peines délictueuses (42% des condamnations pour délits en 2012 sont liées à la route engendrant 5,4% de la population carcérale). Ces statistiques routières mériteraient cependant d'être mises en perspective en regard d'autres causes de mortalité qui ne semblent pas bénéficier d'une telle frénésie sécuritaire. Selon l'INSERM, la pollution atmosphérique est la cause de 20 000 à 40 000 décès annuels en France. 11 000 personnes environ s'y suicident soit un taux 40 % supérieur au taux européen, etc.

N° 72 – Corrélation n'est pas causalité

La confusion entre corrélation et causalité conduit à de multiples sophismes dans la recherche des causes d'anomalies et des décisions qui en résultent.
Les gens habitant près des pylônes à haute tension sont plus souvent malades que le reste de la population. Est-ce la faute du courant électrique ou le fait que les habitants sont plus pauvres à proximité des pylônes et qu'un fort lien existe entre santé et pauvreté ?
Plus de la moitié des accidents automobiles ont lieu sur un trajet de moins de 30 km. Les conducteurs sont-ils moins vigilants sur le chemin du travail ou ce dernier présente-il plus d'obstacles aux heures de pointes et les courts trajets ne sont-ils pas largement majoritaires ?
Les joggeurs soixantenaires ont plus de chance de se trouver en bonne santé à l'âge de 70 ans. Est-ce la pratique du jogging qui maintient en forme ou la population déjà en bonne santé qui reste sportive à 60 ans ?
Exploitée par les théoriciens du complot et à la base de très nombreuses campagnes de communication plus ou moins déguisées, ce raisonnement fallacieux devrait tous nous conduire à suivre la célèbre recommandation de Coluche d'éviter l'hôpital quand on est malade où la probabilité de mourir est dix fois plus grande que dans son lit.

N° 73 – Des impasses malheureuses

Edward Aloysius Murphy (1918-1990), ingénieur aérospatial américain, énonça de la manière suivante la loi empirique qui porte dorénavant son nom : « Tout ce qui est susceptible de mal tourner, tournera nécessairement mal », exprimé par la suite en « le pire est toujours certain » ou plus familièrement par la « loi de l'emmerdement maximum ».

Cette loi a pour corollaire, dans la gestion de projet, qu'une impasse n'est pas à décider selon le degré de croyance en l'absence ou la maitrise de problèmes éventuels, mais plutôt à l'aune des conséquences des problèmes rencontrés.
Quelques essais biens sentis, malheureusement tardifs, ont pu ainsi doucher les certitudes de brillants ingénieurs durant le développement de produits innovants.

N° 74 – Quand la protection s'avère inopérante

L'importance de la ségrégation a été rappelée à plusieurs reprises dans cette rubrique, que cela soit entre des chaînes en redondance ou entre une fonction, sa surveillance ou sa protection. Mais cette règle de bon sens semble souvent oubliée dans le cas de la protection des convertisseurs d'alimentation aux surtensions (OVP : overvoltage protection) par des concepteurs soucieux de performance et d'intégration toujours plus poussée.
Une surtension mal passivée génère pourtant de gros dégâts parmi l'ensemble des équipements alimentés, dès que la tension d'entrée de ces derniers dépasse la valeur admissible (rating).
Et ces destructions se propagent, immédiatement ou après commutation, aux équipements en redondance, si l'alimentation de ces derniers est commune avec les équipements nominaux (CV en redondance).

N° 75 – Le fiabiliste n'est pas un décideur

Le fiabiliste diffère du concepteur par le fait qu'il voit le mal partout sans se laisser éblouir par les performances attendues d'un produit ou service. Son travail consiste à instruire un dossier sur les risques associés sans aucun a priori pour les identifier, puis un minimum de subjectivité pour les hiérarchiser. Il recommande alors des actions pour les maîtriser qu'une entité supérieure décidera de mener ou pas selon des critères et contraintes qui lui sont propres (impositions légales, ressources, planning, etc.).
Mais son esprit critique est parfois défaillant voire souffre de pusillanimité, craignant de se voir coller une image fantasque ou de se faire anéantir comme le messager porteur de mauvaises nouvelles dans la Grèce antique.
Il peut également s'autocensurer en jouant au décideur, recherchant plus ou moins consciemment à satisfaire l'organisation dont il fait partie.
Certaines analyses de Sûreté de Fonctionnement apparaissent bien faibles au cours des enquêtes après incidents. Aussi, n'est-il pas inutile de rappeler que la responsabilité (éventuellement pénale) d'un agent réside dans la bonne exécution du rôle qui lui est dévolu et non pas dans la prise de décisions qui n'est pas de son ressort.

N° 76 – La finalité de l'action sécuritaire

Pour un fiabiliste dont le métier est d'instruire les situations dangereuses dans le but d'aider à la prise de décision, l'irrationalité des actions sécuritaires apparait souvent incompréhensible :
- dans les établissements à l'hygiène irréprochable, une pince est imposée pour se servir du produit en vrac, même si celle-ci constitue un vecteur de contamination de tous les usagers,
- à chaque variation défavorable des statistiques d'accidents routiers, de nouvelles mesures coercitives sont prises à l'encontre des automobilistes, même si le seuil d'environ 3000 morts annuels apparait infranchissable en France, et ce depuis bien longtemps,
- la route focalise l'essentiel de l'action sécuritaire alors que les 60.000 morts annuels liés à la pollution de l'air semblent brusquement découverts après l'ignorance feinte des effets de l'amiante,
- la lutte enfin menée contre les particules polluantes favorise paradoxalement les plus fines beaucoup plus nocives,
- refusée dans les déchetteries par application du principe de précaution, une grande partie des déchets amiantés finissent dans des décharges sauvages plutôt que dans les onéreux centres spécialisés,
- en dépit d'un coût prohibitif et d'une efficacité douteuse, la lutte contre le terrorisme conduit à multiplier les patrouilles de forces armées dans les lieux publics et à annuler des manifestations festives ou commerciales, plutôt que de renforcer les actions secrètes…

Faut-il sacrifier notre économie et nos modes de vie afin de préserver les victimes du terrorisme sensiblement moins nombreuses que celles de la route ? De même, la réglementation vis-à-vis des stupéfiants peut-elle résulter d'une véritable analyse des coûts et bénéfices ? Mais la volonté est-elle de réduire les risques ou bien de diminuer le sentiment d'insécurité ?
Quand le décideur cherche à rassurer les populations et montrer qu'il agit plutôt que de résoudre les problèmes, l'action menée se révèle souvent inutile voire contreproductive.

N° 77 – Peut-on confier l'optimisation d'un système à son fournisseur quand on est opérateur ?

L'optimisation d'un système recouvre de multiples aspects dont les caractéristiques des moyens employés. Qui d'autre que le fournisseur est à même d'améliorer ces derniers et n'est-il pas naturel de lui confier l'optimisation du système dans sa globalité ?
Mais, outre la satisfaction de diverses contraintes, une optimisation porte sur des critères qui n'ont aucune raison d'être partagés.
Ainsi, l'opérateur cherche-il à maximiser son retour d'investissement, ce qui va généralement à l'encontre des objectifs du fournisseur dont les gains dépendent directement de la quantité de matériels fournis.
Le premier a intérêt à valoriser le service offert dans la durée en utilisant des matériels fiables, pérennes et souples pour répondre aux aléas de la demande, alors que le second tire bénéfice de toute consolidation ou renouvellement des moyens utilisés.
Si l'on peut concevoir qu'un train de voyageur frise l'obsolescence après vingt-cinq ans d'utilisation, est-il vraiment raisonnable de vouloir optimiser des services spatiaux en réduisant la durée de vie des satellites à moins d'une dizaine d'années ?

N° 78 – Savoir renoncer à bon escient

Renoncer, c'est baisser les bras, se résigner, mais c'est aussi l'action à prendre dès que nous avons conscience de faire fausse route. Cette capacité de détachement, qui représente une forme de sagesse individuelle, semble toutefois difficilement transposable au plan collectif. D'une part, la conscience collective a beaucoup plus d'inertie que les consciences individuelles, qui recouvrent une part de non-dit. D'autre part, les leaders (prescripteurs ou décideurs de projets) n'aiment pas perdre la face et se trouvent souvent acculés dans des organisations qui peinent à offrir des portes de sortie aux sages qui abandonnent. C'est ainsi que certains projets d'envergure sont conduits dans l'impasse alors que leur finalité même a depuis longtemps disparu dans un contexte évolutif ou que leur complexité et les risques associés ne sont plus maîtrisables. Paradoxalement, d'autres mènent à l'obsolescence, faute d'innovation, par exclusion du risque pour éviter l'échec.

N° 79 – Choisir un concept robuste ou pallier les faiblesses d'un concept défaillant

Un système peut être fiabilisé par divers moyens plus ou moins sophistiqués de détection et de passivation de panne mais bénéficie également de la robustesse intrinsèque de son concept originel qui offre des modes de fonctionnement plus ou moins dégradés en cas de défaillance ou faiblesse de ses constituants.
Ainsi, l'hélice d'un hélicoptère permet la descente à vitesse réduite en autorotation, en cas de panne de motorisation, contrairement au concept de drone multi rotor dont la stabilité est mise à mal dès la perte de l'un de ses rotors (panne de moteur ou de sa commande, désolidarisation de l'hélice, collisions diverses, etc.).
Certes, un bon automaticien peut trouver des lois de contrôle pour maintenir en vol une telle machine après défaillance, même avec un seul de ses rotors (alors très largement sur-motorisés), mais évitons cependant de faire voler des « fers à repasser » s'ils doivent un jour passer l'épreuve de la certification.

N° 80 – Un système n'est pas un composant

Cherchant à répondre à une question à quelques millions de dollars sur la durée de vie résiduelle (RUL) de satellites en orbites, des statisticiens, inspirés par la courbe en baignoire, ont récemment proposé un modèle à taux de défaillance constant jusqu'à la fin de leur durée de mission prévisionnelle, suivi d'une simple pente.

Il faut cependant rappeler que :

- le choix de la loi exponentielle crée un lien entre la fiabilité et la durée de vie moyenne comme le montre l'exemple suivant :

$$R(T\ mission) = 0,7 = \exp(-(T\ mission\ /MTTF)$$

$$MTTF/\ T\ mission = -1/LN(0,7) = 2,8$$

- cette hypothèse de taux de panne constant est fausse dans le cas d'un satellite en raison de la présence des redondances qui font que le facteur multiplicatif serait plutôt de l'ordre de 1,5 dans cet exemple et dépend de l'architecture considérée,
- les phénomènes d'usure, qui ne sont pas pris en compte dans les estimations de fiabilité prévisionnelle en raison des essais d'endurance réalisés, sont très dépendants des satellites (reliquats d'ergol notamment) et ne peuvent pas se modéliser par une augmentation linéaire du taux de panne.

P.S. Construit sur des fondements plus solides (bayésiens), un modèle de RUL de satellite est proposé dans le livre « De la quantification du risque à l'optimisation des systèmes».

N° 81 – Du bon usage des normes de sécurité

Avant l'émergence de la «Sécurité Fonctionnelle» introduite dans la 61508, les normes de sécurité étaient de nature prescriptive avec l'imposition d'exigences diverses essentiellement fondées sur le retour d'expérience, sans objectif quantitatif (probabilité d'événement catastrophique) ou qualitatif (nombre de barrières de sécurité).
Paradoxalement, ces normes «traditionnelles» ne favorisent pas vraiment la sécurité car elles poussent les concepteurs à ne se conformer strictement qu'aux exigences imposées, sans chercher à fiabiliser les nouveaux systèmes ou se préoccuper des manques éventuels du législateur. Elles freinent par ailleurs l'innovation en interdisant a priori des pans entiers de recherches nouvelles. L'autonomie du contrôle des drones est ainsi interdite dans la réglementation française même si celle-ci s'avère indispensable à la réalisation de certains services ou à leur développement dans des conditions économiques viables. Mais d'autres produisent ailleurs et développent actuellement les nouveaux usages qui arriveront bientôt ici.

N° 82 – Agilité et bricolage

Les méthodes agiles sont devenues le must du management de projets. Elles se veulent pragmatiques, réactives et à l'écoute permanente du client. Elles prônent :
- les individus et leurs interactions plus que les processus et les outils,
- le fonctionnement opérationnel plus que la documentation exhaustive,
- la collaboration plutôt que la contractualisation des relations,
- l'acceptation du changement plutôt que la conformité aux plans.

En outre, elles donnent aux décideurs l'impression d'un suivi efficace des travaux et d'une parfaite maîtrise des risques associés (techniques, calendaires et financiers).
Mais si ces méthodes se révèlent efficaces pour gérer les interfaces et parfaire l'ergonomie des produits (un site web par exemple), nous doutons qu'elles permettent de bâtir et structurer proprement un projet d'envergure ou d'élaborer des algorithmes sortant de l'ordinaire.
Certains développeurs avaient certes tendance à bâtir des cathédrales mais nous craignons de voir autour de nous se multiplier les favélas.

N° 83 – Sûreté de Fonctionnement et Big data

Même si bien peu de personnes en connaissent le sens, et moins encore les capacités réelles des outils qui lui sont associés, le Big data est devenu une sorte de Graal susceptible de résoudre tous les problèmes via la fusion de données ou l'apprentissage profond (deep learning). Véritable sésame parmi les décideurs, il est devenu un objet à la mode que l'on finance sans compter. Sa capacité à transformer le moindre traitement statistique en projet innovant favorise la gabegie et peut engendrer des effets pervers quand il accapare des domaines où son apport est limité. Ainsi la Sûreté de Fonctionnement utilise certains outils statistiques innovants dans le cadre de la maintenance prédictive ou de la reconnaissance des situations (voiture autonome), mais d'aucun serait prêt à remplacer cette science de l'ingénieur par quelques algorithmes hypothétiques pour résoudre des problèmes de disponibilité opérationnelle, fautes de les avoir correctement traités.

N° 84 – La valeur moyenne à X% de confiance n'est pas le quantile X

La simulation de Monte-Carlo permet d'évaluer des risques relatifs à des dysfonctionnements (pire cas) ou au franchissement de seuils critiques. Les outils produisent des résultats avec des niveaux de confiance. Mais faut-il encore comprendre leur nature qui n'est pas toujours bien explicitée. Ainsi, le résultat n'a pas 90% de chance d'être inférieur (ou supérieur) à la valeur moyenne à 90% de confiance, mais au quantile 90. Ce quantile peut, lui-même, être estimé avec un niveau de confiance, tel que le quantile 90/95 qui a 95 % de chance d'être supérieur à la valeur du quantile 90. Ce quantile peut être estimé par la méthode de Wilks en choisissant l'une des plus grandes valeurs (ou plus petites) simulées parmi N, mais surtout pas par la méthode du bootstrap, préconisée par certains dans le domaine nucléaire, qui donne des résultats totalement erronés en queue de distribution.

N° 85 – Quand les essais accélérés s'essoufflent

Menés pour estimer la fiabilité ou démontrer l'endurance des produits, ces essais sont réalisés dans des conditions de stress (température, vibration, etc.) plus sévères qu'en utilisation pour accélérer l'apparition des défaillances et réduire par la-même la durée des essais. Des facteurs d'accélération permettent alors de passer des conditions nominales aux conditions d'essai et inversement. Mais ces facteurs intègrent des paramètres influents, rarement testés (l'énergie d'activation du modèle de température d'Arrhenius par exemple), et sont parfois appliqués globalement à l'ensemble du produit (en multipliant les différents facteurs) bien que les stress n'agissent que sur certains modes de défaillance. La Ferrari escomptée peut alors se changer en 2CV et les résultats devenir très optimistes.

N° 86 – Quand la fiabilité échappe au fiabiliste

Si la boîte à outils du fiabiliste n'apparait pas bien lourde, dotée de quelques démarches de bon sens et d'un vernis généraliste, certains spécialistes métier se font fort de fiabiliser les systèmes dans leur domaine de compétences : l'électronicien préconise une intégration fonctionnelle toujours plus poussée sans trop se préoccuper des risques de propagation de panne et de modes communs, l'automaticien multiplie les mécanismes de reprise et de contrôle sophistiqués difficiles à maîtriser, l'informaticien développe des logiciels critiques très onéreux même s'ils peuvent être évités par quelques surveillances additionnelles, le mécanicien dimensionne en pire cas au prix de lourdes marges cachées… enfin le jeune « data scientist » multiplie les capteurs et remplace les mécanismes de détection, passivation et reconfiguration (FDIR) par quelques réseaux de neurones aux capacités incertaines d'apprentissage. L'absence d'esprit critique et de synthèse n'est pas sans conséquence sur les performances et la sécurité des nouveaux systèmes.

N° 87 – Quand on veut trop en faire et qu'on a peur de tout

S'il faut toujours retirer les leçons des échecs passés, l'impréparation de l'aviation française en septembre 1939 est des plus édifiante. Face à une Luftwaffe en mesure d'aligner 4000

avions de guerre moderne, dont 1300 à nos frontières, moins de 400 sur les 1235 répertoriés dans le dernier plan d'armement sont alors véritablement opérationnels. Où sont les 800 avions manquants ? Disséminés dans des hangars d'usines et entrepôts de l'armée de l'air, ceux-ci constitueront de très belles cibles dont se moquera la propagande allemande à la radio. La raison de cette déroute : écartelée entre des doctrines contradictoires, l'élite de notre armée fut incapable d'exprimer correctement son besoin qui se concrétisa par de multiples prototypes jamais totalement aboutis, la discontinuité des financements entrava les développements avant de se transformer en véritable gabegie quand il était déjà trop tard, la planification approximative des équipements et des moteurs cloua au sol bon nombre de machines, la peur exagérée du sabotage conduisit à armer les avions dans la seule base de Châteaudun où la désorganisation régnait en maître (cf. dernier numéro du « Fana de l'aviation » que nous remercions ici). Qu'en est-il aujourd'hui ? La disponibilité opérationnelle des aéronefs militaires stagne autour de 44% dont 30% en métropole (d'après le rapport de Christian Chabbert) et bien d'autres programmes civils ou militaires s'engagent avec des spécifications pas véritablement matures, dues à un engourdissement intellectuel ou une incapacité à décider, non sans « ceintures et bretelles » pour se protéger de quelques risques incertains.

N° 88 – Un fiabiliste souvent absent en R&D

Les projets de Recherche & Développement sont généralement contraints en terme de financement. Aussi, la présence d'un fiabiliste n'y est souvent pas jugée prioritaire, tant la réflexion sur les aspects dysfonctionnels apparait prématurée par rapport à l'activité à mener pour atteindre les performances fonctionnelles attendues. L'application opérationnelle semble alors bien lointaine, mais finit par se rapprocher. En dépit des budgets consommés, certains projets de R&D sont alors arrêtés, soit en raison de l'incapacité des produits développés à répondre aux exigences d'une mission véritablement opérationnelle, soit de leur dangerosité quand les équipes de développement ignorent toute notion sécuritaire. La consultation, même ponctuelle, d'un spécialiste de la maîtrise des risques est-elle vraiment un luxe ?

N° 89 –Avion d'Ingénieur ou avion de bricoleur

Les deux derniers crashs de Boeing 737 Max n'ont pas manqué de rouvrir l'éternel conflit entre pilotes et ingénieurs sur le rôle de l'opérateur face à la machine. Doit-on faire reposer la sécurité d'un avion sur un individu d'exception, éliminer ce dernier jugé trop faillible bien qu'il puisse réagir efficacement dans des situations imprévues (1 tâche mal exécutée sur 1000 par une personne entrainée) ou rechercher le meilleur compromis entre l'homme et la machine ? En réduisant considérablement le risque d'accident pris par des passagers toujours plus nombreux (division par 10 des morts par km/passager entre 1996 et 2004 avec une diminution régulière depuis, soit moins d'un centième qu'en voiture), l'ingénieur a manifestement su trouver de bons compromis en dépit de la réduction progressive du nombre de navigants techniques présents dans les cockpits, de cinq (pilote, copilote, mécanicien navigant, navigateur, radio) avant-guerre à deux et peut-être un demain.
Mais a-t-on affaire à des ingénieurs quand toutes les règles élémentaires de la Sûreté de Fonctionnement sont bafouées ?
- un avion au comportement différent (moteurs plus gros déplacés plus avant sous les ailes) présenté comme quasiment identique sans modification de la formation des pilotes,
- un automatisme anti-décrochage MCAS (nécessaire en raison de la différence de comportement) difficilement débrayable et très mal documenté (renvoie l'appareil en piqué),
- une redondance des capteurs d'angle d'attaque vis-à-vis de la panne retard (non fonctionnement du MCAS) multipliant par là même les points de panne unique vis-à-vis de la panne avance (fonctionnement intempestif),
- une auto certification du MCAS délégué au constructeur par l'organisme de certification (FAA).
L'ingénieur peut se sentir légitimement trahi.

N° 90 – Peut-on faire confiance aux architectes ?

L'incendie de Notre-Dame suscite bien des polémiques entre partisans d'une reconstruction à l'identique et adeptes d'une architecture contemporaine. Sans chercher à nous immiscer dans ce débat (ni analyser les causes très instructives de l'incendie), nous constatons que quelques architectes triés sur le volet (des bâtiments de France, du Ministère de la culture, des services d'urbanisme départementaux ou municipaux) s'érigent en dépositaires du bon goût et nous imposent leur subjectivité. Mais l'esthétique est rarement contrainte par des considérations sécuritaires, environnementales, ou simplement pécuniaires. Stocker 210 tonnes de plomb dans une toiture et environ mille chênes dans une charpente ne semblent pas trop émouvoir, en dépit des carences manifestes de la protection des monuments historiques (une dizaine d'églises auraient brûlé depuis un an). Dans le même ordre d'idées, l'imposition de l'intégration au bâti des panneaux photovoltaïques, plutôt que leur simple installation au-dessus des toitures, a conduit à une multiplication de problèmes d'étanchéité, une aggravation du risque d'incendie et une explosion des coûts d'acquisition. De même, Toulouse pourrait accueillir des colonies d'enfants, en raison de la limitation longtemps imposée aux surélévations d'immeuble à des demi-étages, et passe aujourd'hui au gris, voire au noir anthracite, couleurs très à la mode parmi nos architectes qui ne manqueront pas de réchauffer le cœur de la ville rose dans cette période de réchauffement climatique.

N° 91 – Perseverare diabolicum

Les canicules de cet été ont contraint le réseau ferré français à tourner parfois au ralenti et un rapport confidentiel de l'Établissement public de sécurité ferroviaire (EPSF) indiquerait que les problèmes de maintenance, ayant conduit à des accidents comme celui de Brétigny-sur-Orge en 2013, persistent (C.F Le Parisien du 20 août 2019).
Jalousement cachées aux yeux d'éventuels concurrents, des tonnes de données de retour d'expérience sur l'état du réseau semblent avoir été conservées depuis des décennies, sans que cette mine d'information ne soit apparemment exploitée. Sans attendre que des réseaux de neurones réfléchissent à notre place, une politique de maintenance cohérente pourrait être alors suivie :

- établir des modèles de dégradation des tronçons de voie (ballaste, rail, caténaire..) à partir d'observables représentatifs (défauts constatés, vibration, consommation, etc.) en fonction des stress subis (température, sollicitations, charge à l'essieu, etc.).
- définir des seuils d'intervention pour faciliter le pronostic à partir d'un diagnostic,
- traiter les tronçons les plus dégradés en priorité,
- communiquer du REX aux fournisseurs afin d'améliorer les maillons faibles.

Ainsi éviterions-nous qu'une « honte de prendre l'avion » ne s'accompagne demain d'une « peur de prendre le train ».

N° 92 – Un fiabiliste mal voyant

Si un bon fiabiliste est capable de garantir un niveau de disponibilité opérationnelle à minimum de coût, encore faut-il pour cela, qu'il ait la visibilité sur l'ensemble des coûts des constituants du système et des opérations menées sur ce dernier. Or les coûts sont souvent peu accessibles dans les organisations, disséminés au sein des diverses entités ou constituent une véritable chasse gardée de l'une d'entre elles (contrôle des coûts rattaché à la direction financière par exemple).
La conception optimale exige une collaboration de toutes les parties prenantes. Aussi, resterons-nous à la traine de nos amis anglo-saxons, si notre culture d'entreprise n'évolue par sur le sujet.

N° 93 – Fiabiliser par l'IA ou fiabiliser l'IA

L'Intelligence Artificielle (IA) suscite bien des interprétations, fantasmes et inquiétudes dans les récits et films de science-fiction, qui sévissent également parmi les concepteurs.
Certains se la représentent comme la solution à tous les problèmes mal traités à ce jour, dont la faible disponibilité opérationnelle de certains systèmes. Ils bardent alors ces derniers de capteurs multiples et stockent à tout va des montagnes de données au cas où l'IA pourrait un jour les résoudre.
Afin de pallier les étincelles d'intelligence sur le plan sécuritaire, d'autres cherchent à créer une IA fiable et explicable en rendant compréhensible son processus de décision.
Sans douter des apports (limités) de l'IA, dont on aurait tort de se priver pour trier des données en grand nombre ou identifier des signaux faibles, pouvons-nous suggérer de tenter de résoudre correctement les problèmes avec notre propre intelligence avant de la délocaliser à de simples machines.

N° 94 – Communication et gestion de crise

Objet de préconisations diverses dans tous les manuels de management, la communication de crise est activée quand une suite de dysfonctionnements met en péril la stabilité et la réputation d'une organisation. Elle regroupe la communication utile à la gestion de la crise (alerte des personnes concernées, communication de coordination des opérations, etc.) et celle qui se destine à préserver l'image de l'organisation en crise et la réputation de ses dirigeants. Mais ces deux branches sont rarement indépendantes, voire antagonistes, quand la préservation de la réputation de l'organisation nuit à la gestion de la crise. L'épidémie du coronavirus en est un triste exemple avec des responsables locaux de la province de Hubei cherchant à étouffer les révélations des premiers lanceurs d'alerte (dont le regretté Li

Wenliang) pendant près de trois semaines… et la majorité des responsables de la santé des pays occidentaux jurant que les frontières étaient alors infranchissables, sans envisager de mesure préventive telle que l'achat de masques de protection. Cette mauvaise gestion de la crise nuit alors en retour à l'image de l'organisation et à la crédibilité des dirigeants. La communication ne prend-telle pas trop de place dans nos sociétés ?

N° 95 – Expertise et décision

L'expert peut instruire une problématique pour aider le décideur mais ne peut pas décider à sa place :

- sa connaissance a des limites et les experts ne sont pas toujours d'accords entre eux,
- son domaine d'expertise ne couvre généralement qu'une partie de la problématique,
- il en ignore les contraintes financières, logistiques et programmatiques,
- son jugement est biaisé quand il sort de son rôle.

Le décideur consulte l'expert mais la décision n'engage que lui.
Ainsi, face à la pandémie du coronavirus, qui pilote la lutte et quel est l'objectif ? Préserver la santé, est-ce :

- éviter l'engorgement des centres d'urgences ?
- diminuer la mortalité globale à l'hôpital, dans les EHPAD et à la maison ?
- réduire les conséquences directes et indirectes de la pandémie qui abrège aujourd'hui la vie des anciens, accapare les moyens au détriment des autres malades et dont les conséquences économiques fragiliseront demain les jeunes et les plus faibles ?

A un objectif clairement énoncé répondrait une stratégie propre, adaptée au terrain et aux ressources disponibles.

N° 96 – L'illusion de la modélisation physique

Un modèle physique est une représentation explicative d'un phénomène (mécanique, électrique, chimique, etc.) qui permet d'en prédire certains aspects.
Mais ce modèle est généralement simplifié quand la réalité est complexe et recouvre une part d'aléa.
Il n'en reste cependant pas moins prisé de l'analyste, parfois grisé par l'illusion de comprendre le Monde, même s'il se révèle souvent moins juste qu'un modèle descriptif exclusivement fondé sur l'observation.
Ainsi, les modèles prédictifs conduisent à une grande variété de résultats selon la manière d'appréhender le hasard et l'imprécision, notamment quand celle-ci est purement académique et résulte d'un nombre d'observations limité.
Aussi, nous nous méfierons tout particulièrement de ces experts capables de juger "au doigt mouillé" la valeur des paramètres de modèles probabilistes complexes.

N° 97 – Les pièges de l'accélération des essais

Les essais de durabilité ou de fiabilité permettent de démontrer la capacité des produits à assurer leur mission opérationnelle ou de tenir, a minima, leur période de garantie. Pour obtenir des résultats au plus tôt et réduire les coûts, ils peuvent être accélérés de diverses manières, sous réserve de pouvoir justifier la correspondance entre le profil de vie opérationnelle et celui de la séquence d'essais. Une surestimation de l'accélération se traduit par une évaluation optimiste de la fiabilité du produit, alors qu'une sous-évaluation engendre des dégradations prématurées ou des défaillances précoces en essais qui compromettent la démonstration des objectifs fixés. Certains produits tiennent alors mieux que d'autres leurs promesses en opération.

N° 98 – L'excès de précaution est parfois mortifère

L'instruction des situations à risques est souvent biaisée par le poids des décisions résultant de ses conclusions. L'analyste sort alors de ses attributions en jouant au décideur ou surestime le risque en s'appuyant notamment sur le « principe de précaution ». Reposant sur des données

erronées, la décision peut se révéler catastrophique comme l'atteste la gestion des masques durant la première vague de la COVID-19. Selon les organismes de normalisation, les masques chirurgicaux devaient être impérativement jetés au bout de quatre heures d'utilisation alors qu'ils filtrent encore 95 % des particules de moins de trois microns après plusieurs lavages, soit plus que les 90 % des masques en tissu grand public. Un simple test d'efficacité des masques après lavage aurait alors permis de conserver un objet essentiel à notre protection collective, en dehors du personnel médical.

N° 99 – Choisir le bon modèle

Une évaluation « réaliste » de la fiabilité des composants au moyen d'un modèle fondé sur la « physique » de défaillance n'a pas beaucoup de sens, si ce n'est que l'estimation (statistique) est juste ou erronée dans des conditions précises d'utilisation et d'environnement. Ainsi, tout phénomène d'usure interdit l'emploi d'un taux de défaillance constant si on cherche à prédire la maintenance au-delà de la période de garantie. De même, l'estimation de la durée de vie restante (RUL) au moyen d'un modèle de dégradation implique que ce dernier soit capable de représenter le comportement des matériels dans la durée. Mais si l'évaluation n'est que contractuelle, qu'importe sa validité !

N° 100 – Le meilleur des ajustements

La maintenance prédictive fait de plus en plus d'adeptes, mais sa mise en œuvre effective peine à se concrétiser. Elle implique l'emploi d'un modèle prédictif, capable de décrire le vieillissement des matériels, et son ajustement à partir de données observées. La qualité des prédictions peut être mesurée par des indicateurs de biais (MAE) ou de variance (RMSE) des estimations par rapport à des observations non employées pour l'ajustement (20%). Réalisé par la méthode du maximum de vraisemblance, ce dernier peut à la fois porter sur des paramètres du modèle prédictif et de facteurs d'accélération utilisés pour traduire la variabilité des conditions d'utilisation et d'environnement. Le meilleur ajustement est alors celui qui donne la plus grande vraisemblance aux observations, comme le fait régulièrement notre outil Gencab d'optimisation hybride, capable de s'affranchir d'éventuels optima locaux. Mais si la comparaison est facile, faut-il encore que la vraisemblance (densité de probabilité) qui caractérise les modèles soit explicitée et que ces derniers ne se réduisent pas à de simples boîtes noires aux résultats incertains.

N° 101 – Quand la précaution brouille la réflexion

Le principe de précaution impose de se prémunir des risques susceptibles d'engendrer des dommages aux personnes ou à l'environnement, en l'absence de certitudes techniques ou scientifiques. Intégrée dans la constitution française à travers une charte de l'environnement, ce principe est évoqué lors de divers jugements (démontage d'antenne-relais…) mais est aussi critiqué pour son encouragement à l'immobilisme et son opposition au progrès scientifique (il expliquerait la diminution des autorisations de mise sur le marché de nouveaux médicaments de 39 à 19 entre 1998 et 2007 par la Food and Drug Administration). Mais la précaution devient carrément mortifère quand l'incertitude juridique qui l'accompagne entrave les capacités de jugement des décideurs en situation de crise, qui semblent alors avoir du mal à choisir entre des actions à risques hypothétiques ou négligeables et celles à risques avérés. Ce jugement est de plus altéré par des notions dévoyées d'égalité, consistant à traiter chacun de la même manière indépendamment des risques encourus, ou de liberté que l'on peut restreindre considérablement à tous sans imposer de mesures particulière à chacun, notamment aux personnes les plus concernées. Doit-on s'assurer de l'homologation des bouées de sauvetage avant de les lancer aux naufragés !

N° 102 – Il y a drone et drone

Peut-on sécuriser les opérations de drones sans en dissocier les usages ?
Le taxi volant sans chauffeur accapare des énergies, même s'il risque de rester longtemps une chimère à l'instar du véhicule sur route totalement autonome.
Son poids, sa taille et la présence de personnes à bord en fait un objet à risque de complexité sans rapport avec celui d'un drone de moins de 25 kg susceptible de rendre des services beaucoup plus profitables à la communauté.
Aussi, serait-il dommage que l'apport sociétal des drones soit freiné par des considérations sécuritaires qui ne concernent qu'une partie marginale de ses possibles usages.

N° 103 – Sachons rester simple

La prévision repose sur des modèles plus ou moins complexes fondés sur l'expertise et l'observation de données. Ces modèles ont une tendance naturelle à se sophistiquer pour représenter au mieux les phénomènes au fur et à mesure du développement de leur compréhension. Mais sont-ils pour autant meilleurs pour établir un pronostic ? Le mieux étant souvent l'ennemi du bien (Montesquieu), l'analyste doit savoir s'incliner quand des indicateurs statistiques de qualité des prévisions donnent l'avantage à la simplicité, notamment quand les données disponibles se révèlent insuffisantes pour ajuster ou procéder au recalage des modèles.

N° 104 – Un drone n'est ni un jouet, ni un aéronef ordinaire !

L'absence de personne à bord et la possibilité d'interrompre la mission (par une chaîne indépendante) permettent de sécuriser et de fiabiliser les opérations de drones (de moins de 25 kg) aussi bien, mais beaucoup plus simplement, que celles réalisées par des avions ou hélicoptères. De même que les techniques classiques de fabrication aéronautique se révèlent inappropriées, en termes de performance des machines, la multiplication des redondances alourdit inutilement les architectures, consomme de l'énergie et diminue la disponibilité opérationnelle en augmentant d'autant les risques de défaillance. Certes la chute d'un drone au sol ne doit pas occasionner de dommage aux personnes et aux biens et toute collision avec un autre usager de l'espace aérien ne doit jamais se produire. Mais des solutions existent pour chaque type d'opération et la méthode SORA constitue un excellent cadre d'analyse et de justification de la maîtrise des risques, au même niveau que l'aérien piloté, mais sans complexification inutile. En se trompant d'objet, l'essor des opérations de drone, entrant dans la catégorie spécifique de l'EASA, risque de prendre du retard dans notre pays.

N° 105 – L'anti-fiabilité

L'obsolescence programmée est définie dans la loi française comme « l'ensemble des techniques par lesquelles un metteur sur le marché vise à réduire délibérément la durée de vie d'un produit pour en augmenter le taux de remplacement ». Elle concerne, par exemple, des condensateurs électrolytiques sous- dimensionnés, des pièces de fatigue non renforcées, une taille mémoire réduite pour empêcher les évolutions, etc. Elle entre également dans la politique de renouvellement de certains produits dont la finalité est davantage de déprécier les modèles précédents que de les améliorer, en flattant le désir de différentiation ou de suivi des modes d'une partie des consommateurs. Mise en œuvre pour accroître les bénéfices des entreprises, au risque de ternir leur image, cette stratégie remporte la palme du bêtisier du fiabiliste par ses conséquences au niveau social et environnemental : outre les surcoûts engendrés, la surconsommation inutile génère de la pollution, un surplus de déchets et un gaspillage de ressources.

N° 106 – Ne construisons plus sur du sable !

Désignant la capacité des matériaux à retrouver leur état initial à la suite d'un choc (métallurgie), l'aptitude d'un écosystème à se régénérer après une catastrophe (écologie) ou celle d'un individu à supporter un traumatisme (psychologie), la résilience est un concept nomade qui exprime la capacité d'un système (ou organisation) à survivre à un événement imprévu. Certes, il est difficile de maîtriser l'imprévisible mais peut-on continuer à concevoir des systèmes toujours plus imbriqués, sans se préoccuper de robustesse ? Il est pourtant facile d'imaginer la perte ou la saturation de certains constituants, quelle qu'en soit la cause. La chaîne de fournisseurs se brise, la logistique se grippe, le service s'arrête dès qu'un organe s'enrhume... Outre les organisations, l'absence de résilience nous affecte directement : le chauffage (gaz ou fioul) ne fonctionne plus sans électricité, le photovoltaïque ne fournit plus d'énergie en cas de panne de réseau (même en auto consommation), des services essentiels (banque, transport, localisation, santé…) ne sont délivrés qu'avec l'utilisation d'un téléphone mobile, etc. La succession de crises que nous subissons actuellement (réchauffement climatique, pandémie, guerre entre pays voisins…) révèle combien nos choix de conception peuvent se révéler funestes en l'absence de réflexion sur les risques encourus (environnemental, systémique, géopolitique, médical, etc.).

N° 107 – Les centrales ne sont pas éternelles

Les centrales du parc nucléaire français ont été dimensionnées pour une durée de vie de 40 ans car elles comprennent des éléments non réparables, dont notamment la cuve qui subit un vieillissement mécanique sous l'effet de l'irradiation.
Elles rencontrent aujourd'hui des problèmes génériques :

- des fissures, liées à un phénomène de corrosion sous contrainte, affectent les tuyauteries des systèmes de sécurité,
- la teneur en carbone de l'acier employé lors de la fabrication des couvercles et fonds de cuve présente des anomalies,
- le retour d'expérience dans le domaine nucléaire impose de revoir certaines règles de sécurité dont notamment la protection des moyens de secours après la catastrophe de Fukushima,
- l'obsolescence des matériels renchérit significativement les coûts de maintenance.

Même si certains semblent croire à la poule aux œufs d'or, nos centrales ne fourniront pas vingt ans d'énergie gratuite supplémentaires après leurs quarante ans d'amortissement.

N° 108 – Peut-on encore concevoir un produit sans se préoccuper de bonne santé ?

Le Health Monitoring (suivi de bonne santé) et la maintenance prédictive (prévisionnelle) n'améliorent pas seulement la disponibilité opérationnelle et la sécurité des produits, tout en réduisant leurs coûts de possession, mais ils les modifient en profondeur par des simplifications multiples, tant au niveau du système que des équipements.
Les redondances systématiques (dont la triplication chère au domaine de l'aéronautique) ne s'avèrent plus toujours nécessaires quand l'occurrence des défaillances est très fortement diminuée par l'observation précoce des dégradations (notamment dans le cas des aéronefs sans pilote).
De même, le coût des différents essais est grandement diminué quand les observables existent, sans nécessité de démontage et de matériels de test spécifiques.
Ces observables ne nécessitent pas autant de capteurs, qui complexifierait inutilement les architectures de système, mais surtout d'une exploitation intelligente de l'information disponible jusque alors ignorée.
Par ailleurs, la sécurité d'un système est globale et ne repose pas plus particulièrement sur les algorithmes de surveillance qui n'en constituent que des maillons.
Les concepteurs qui ignorent encore l'importance du suivi de bonne santé développent d'ors et déjà des produits obsolètes, alors qu'ils sont pourtant les mieux placés pour s'en préoccuper.

N° 109 – Quand la fiabilité rend moins sûr

L'idée qu'une meilleure efficacité conduit à une moindre consommation d'énergie est fausse car elle est alors plus accessible et donc plus demandée, comme l'expliquait l'économiste W. S. Jevons à propos du charbon au XIXe siècle pendant que James Watt perfectionnait la machine à vapeur. Cet effet rebond joue également dans le domaine de la fiabilité où l'amélioration de la la Sûreté de Fonctionnement invite à se rapprocher des limites. Ainsi l'introduction des équipements de sécurité active (système de freinage ABS par exemple) ou l'amélioration des virages routiers ne réduisent pas vraiment le nombre d'accidents et engendrent même parfois des accidents plus graves car les conducteurs ont alors tendance à rouler plus vite. De même la multiplication des alarmes fait qu'elles ne sont plus perçues, voire débranchées pour ne plus les entendre.
Aussi gardons-nous des impressions toutes faites dans le domaine de la sécurité et fions nous au seul retour d'expérience.

N° 110 – Peut-on garder des taux de défaillance constants dans les recueils de fiabilité ?

Outre les composants mécaniques soumis à des phénomènes d'usure dès leur première heure de fonctionnement, les composants électroniques vieillissent de plus en plus vite, au fur et à mesure que leur intégration progresse. Leur fiabilité ne peut plus alors se modéliser par une simple exponentielle mais par une loi de probabilité capable de traduire ce vieillissement, telle que Weibull ou lognormale. Aussi, les recueils devront bientôt s'enrichir d'un second paramètre et la simple sommation des taux de défaillance devra être remplacée par le produit des fiabilités dans les analyses. Mais si l'estimation de fiabilité n'a pour finalité que de répondre à une demande contractuelle… on peut évidemment ne rien changer.

N° 111 – Comment réaliser un essai de fiabilité au prix d'un essai d'endurance ?

Contrairement aux essais de fiabilité, les essais d'endurance permettent de démontrer la capacité d'un produit à réaliser une mission, dans des conditions données, sans estimer sa probabilité de réussite. Ces essais portent sur un nombre réduit de pièces à tester et sont généralement accélérés afin d'en réduire la durée et les coûts, en augmentant le niveau des stress subis (température, vibration...). L'ajustement d'un modèle de fiabilité à partir de durées de fonctionnement nécessite beaucoup plus de données pour atteindre une certaine précision. Mais, si le produit est sujet à des phénomènes d'usure, et non à des pannes aléatoires, l'observation de son état durant les essais permet d'obtenir un très grand nombre de données à partir de quelques pièces. Il est alors possible d'ajuster précisément un modèle de dégradation, à partir des trajectoires de niveau d'usure, puis une loi de fiabilité équivalente (Weibull ou lognormale) pour un seuil de fonctionnement donné. Les essais ne sont-ils pas suffisamment couteux pour en tirer le maximum d'information avec un peu d'intelligence ?

N° 112 - Du bon usage des techniques bayésiennes

L'inférence bayésienne consiste à réviser la probabilité d'une hypothèse par l'observation de faits. Elle permet notamment d'estimer un risque d'échec ou un taux de défaillance à partir d'une connaissance a priori (jugement d'expert) et d'observations statistiques (retour d'expériences ou résultats d'essais). L'approche est solide sur le plan des mathématiques (théorème de Bayes) mais sa validité ne repose que sur la qualité de la connaissance a priori. Or que vaut un jugement d'expert élaboré en dehors de toute démonstration scientifique ou retour d'expériences similaires ? Des méthodes ont bien été développées pour consolider les jugements entre différents experts mais moyenner l'absence de réelle connaissance apparaît vain. S'il est dommage de se passer des techniques bayésiennes pour consolider les résultats d'observations, quand on dispose d'un tant soit peu de véritable connaissance (pour dimensionner un essai de fiabilité par exemple), il est en revanche malhonnête de vouloir infléchir par des pseudos experts ce que ne peuvent pas démontrer les observations.

N° 113 - Quand le décideur casse le thermomètre

Si le rôle du fiabiliste est d'instruire les analyses de risques indépendamment de la prise de décisions (voir bêtisier N° 75), certains décideurs œuvrent manifestement en se voilant la face. Deux événements récents paraissent emblématiques :
- le projet de fusion de l'Institut de radioprotection et sûreté nucléaire (IRSN) au sein de l'Autorité de sûreté nucléaire (ASN) limite l'indépendance et la capacité d'expression des experts, au moment où la France veut lancer un nouveau programme de réacteurs, en dépit des multiples dysfonctionnements observés dans la filière,
- le ministère de l'agriculture tente d'infléchir la décision de l'Anses (Agence nationale de sécurité sanitaire de l'alimentation, de l'environnement et du travail) sur le S-métolachlore, un herbicide responsable de la contamination de nappes phréatiques.
Comment un décideur peut-il inspirer confiance et ne pas engendrer des angoisses justifiées ou des fantasmées au sein des populations concernées, s'il refuse tout éclairage scientifique dans son processus de décision ?

N° 114 - La norme : un ouvrage méthodologique pour les nuls… qui veulent bien le rester

La norme industrielle cherche à unifier les conditions de réalisation des opérations ou d'élaboration des produits. Elle facilite ainsi le travail des donneurs d'ordres en réduisant le cahier des charges à une expression de besoin et une liste de documents applicables. Mais le processus de normalisation n'est pas régulé et produit toujours plus de documents, souvent volumineux, par des groupes informels, au profit d'organisations diverses, selon leur intérêt, et d'organismes de normalisation qui vivent de leur vente. La norme engendre un coût d'acquisition et de formation significatif pour un très grand nombre d'acteurs. Elle impose parfois des règles discutables ou obsolètes sans trop donner d'explication sur les méthodologies sous-jacentes. Elle recouvre généralement des recettes simplistes dont l'acquisition peut donner à certains l'illusion de maîtriser tout un domaine d'ingénierie. Dans notre domaine de prédilection, l'inflation des normes ne semble pas avoir freiné les pertes de compétence observées dans l'industrie. Car si la norme prospère, il n'en n'est pas de même pour les ouvrages de références ou les formations scientifiques et techniques.

N° 115 - La durée de vie, une notion mal comprise

La durée de vie est une notion quelque peu ambiguë qui désigne indifféremment l'espérance de la durée de fonctionnement d'un système ou la durée initialement choisie pour dimensionner sa conception. Cette durée peut être éventuellement allongée quand le matériel se comporte mieux que prévu ou si des améliorations sont réalisées durant sa vie opérationnelle par rapport aux actions de maintenance envisagées au départ. Mais des limitations existent cependant quand le système n'est pas entièrement réparable ou que l'usure, l'obsolescence des matériels ou la perte de certaines compétences, finissent par générer des coûts insurmontables de remise à niveau. Un investissement n'est donc pas infini et il est illusoire de faire perdurer gratuitement des systèmes largement amortis, tels que nos véhicules, nos habitations, notre réseau ferroviaire ou nos centrales nucléaires. Un mur d'indisponibilité se présente face à nous quand des actions de remplacement des matériels n'ont pas été mises en œuvre suffisamment tôt. L'inaction devient alors extrêmement coûteuse (voire dangereuse) par l'arrêt prolongé du service ou sa réintroduction menée dans l'urgence.

N° 116 - Quelle confiance accorder aux recueils de fiabilité ?

Les recueils de fiabilité prévisionnelle donnent une estimation du taux de défaillance des composants électroniques en fonction des conditions d'environnement d'utilisation ou d'approvisionnement.
Mais ces normes (MIL-HDBK-217F, FIDES, TR 62380 IEC, Bellcore SR-332, etc.) donnent des résultats variables, pour un même type de composant, car leurs modèles diffèrent.
Le taux de défaillance reste constant, même pour des composants soumis à usure.
Il regroupe un ou plusieurs taux élémentaires (puce, boîtier, connectique, etc.), chacun multiplié par divers facteurs correctifs (température, environnement, qualité, approvisionnement, etc.).
Outre le nombre de taux élémentaire et de facteurs correctifs, les modèles se distinguent par la valeur des paramètres des facteurs d'accélération (ex. énergie d'activation) et celle des conditions de référence (ex. température).
La complexité de certains modèles rend très difficile, voire impossible, l'estimation de leurs paramètres à partir de données de retour d'expérience et on peut alors s'interroger sur la validité des valeurs qui ont été choisies.
Aussi, faut-il privilégier l'exploitation de données opérationnelles ou d'essais, quand cela est possible, et ne pas accorder trop d'importance à des modèles prévisionnels dont la complexité et le raffinement peuvent s'avérer l'ennemi du bien.

N° 117 - Un bêtisier pas si bête !

Cette rubrique humoristique, qui n'a pour ambition que d'amuser le lecteur en l'interrogeant sur certaines pratiques dans notre domaine de prédilection, ne semble pas totalement décalée comme l'illustrent les articles suivants portant sur une « bagarre » en cours entre différents organismes de normalisation et des interrogations sur les recueils de fiabilité, deux sujets abordés ici à plusieurs reprises.

- NASA awards CALCE grant for assessment of FIDES Reliability Prediction Tool | Center for Advanced Life Cycle Engineering (umd.edu)
- Assessment of the FIDES Guide 2022 electrical, electronic, and electromechanical reliability prediction methodology - ScienceDirect

Toutefois, si le ton, voire le fond, de cette rubrique apparaît discutable, n'hésitez pas à nous faire parvenir votre bêtisier du bêtisier.

N° 118 - Déverminer mais pas trop !

Les essais de déverminage (screnning or burn-in test) permettent de révéler des défauts de jeunesse de composants avant leur utilisation. Leur fiabilité opérationnelle devient alors la fiabilité conditionnelle à t+T, sachant qu'ils ont fonctionné correctement pendant une durée d'essai T, soit :

$$R(t+T/T) = R(t+T)/R(T) = e^{-([(T+t-\gamma)/\eta)]^{\beta}+[(T-\gamma)/\eta)]^{\beta})}$$ dans le cas d'une loi de Weibull.

Cette fiabilité s'améliore si β est inférieur à 1 mais diminue dans le cas contraire. Aussi évitera-t-on d'entamer le potentiel de vieillissement des produits en cherchant à les améliorer.