Une synthèse du Bêtisier du Fiabiliste

Groupe SdF Occitanie

28 septembre 2018

Introduction

Le Bêtisier du fiabiliste :

- Rubrique apparue en mars 2006 dans la dixième édition du Journal du Fiabiliste
- Ton humoristique et ironique
- Soixante-quinze chroniques différentes rédigées à ce jour
- Issues de l'observation des pratiques notamment dans le cadre de revues de conception
- Constitue une forme de REX regroupant un certain nombre de leçons apprises.

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.

➢ Synthèse typologique des problèmes soulevés

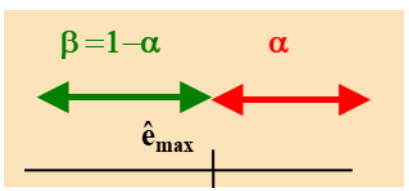
Introduction

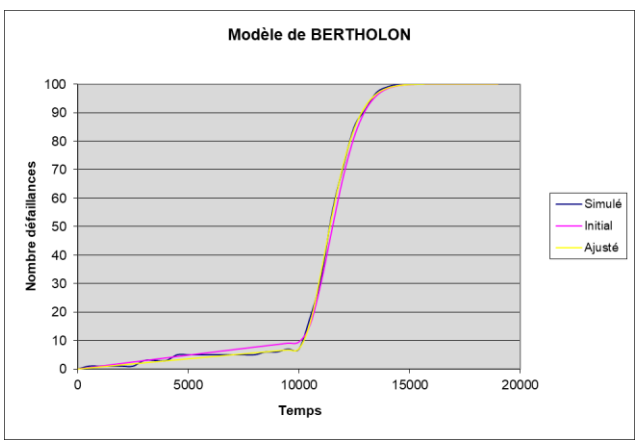
Types de problèmes :

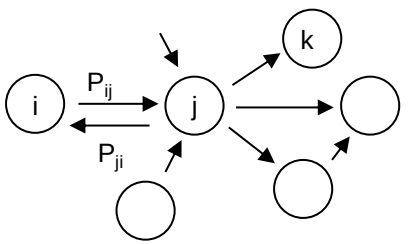
- Erreur de calcul
- Erreur de Modélisation
- Méthode discutable
- Ambiguïté & incompréhension
- Décision erronée
- Mauvaise conception
- Pratique discutable
- Organisation défectueuse

Erreur de calcul

Erreur de calcul	
N° 10 – Le « Lambda équivalent »	Utilisation abusive à différentes valeurs de t
N° 14 – Estimation erronée	Mauvaise utilisation de la notion d'intervalle de confiance
N° 27 – De si beaux modèles bien mal ajustés	Ajustement approximatif par méthode d'optimisation locale
N° 41 - Erreurs dans les modèles markoviens	Démarche de modélisation inappropriée conduisant à erreur
N° 19 - Perte de mémoire dans les systèmes non markoviens	Simulation erronée des systèmes soumis à usure

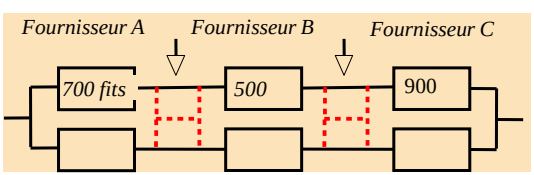


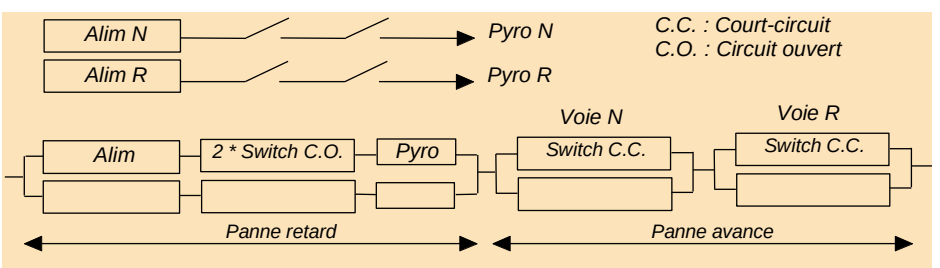




Erreur de Modélisation

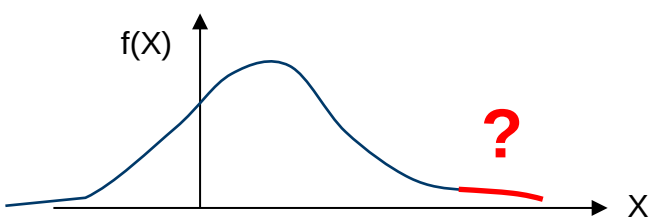
Erreur de Modélisation	
N° 12 – Le cross-strapping virtuel	Redondances mal traitées au niveau des systémiers
N° 13 - Utilisation erronée des arbres de fautes	Dépendances entre les événements de base (réparateur commun, stock de rechange partagée, maintenance synchronisée, etc.)
N° 23 – Une régression pas toujours linéaire	Extrapolation abusive
N° 24 – Un ajustement en manque de points d'appui	Insuffisance de données
N° 11 – Mode de pannes antagonistes	Modélisation erronée de la panne avance et retard
N° 35 – Vote entre 4 capteurs de type min de max (ou max de min)	Modélisation erronée de la panne « trop haut » et « trop bas »
N° 47 - Le mieux est l'ennemi du bien	Raffinement inutile de la modélisation engendrant des risques d'erreur
N° 57 – Complexité physique et exactitude statistique	La complexité d'un modèle ne garantit pas sa justesse (Fides)
N° 80 – Un système n'est pas un composant	La courbe en baignoire n'est pas applicable à un système comprenant des redondances (satellites)





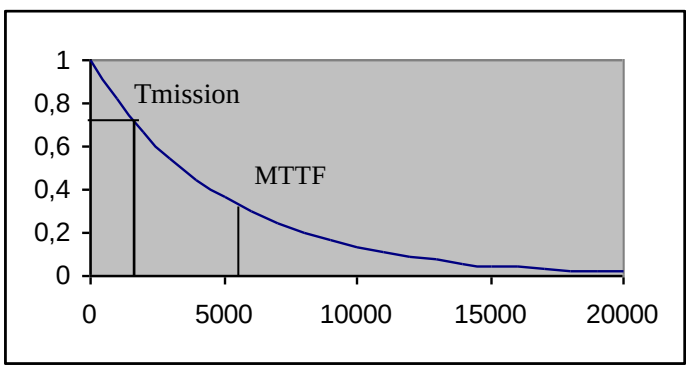
Méthode discutable

Méthode discutable	
N° 26 – Quand le virtuel prête à confusion	La méthode du Bootstrap est totalement erronée dans les queues de distribution (estimation d'un quantile)
N° 50 – Quand la théorie tente de maîtriser les extrêmes	La théorie des valeurs extrêmes ne repose que sur la qualité du retour d'expérience que l'on ne peut pas extrapoler
N° 59 – Ne pas abuser des belles formules	Un modèle explicite (markovien ou autre) vaut bien mieux qu'une suite d'intégrales triples
N° 31 – Un effort souvent mal dimensionné en SdF	La classification des projets selon leur importance n'a rien à voir avec les risques encourus
N° 52 – L'innovation est-elle bien maîtrisée ?	L'indice TRL est devenu un outil simpliste de gestion de l'innovation indépendamment de la complexité des technologies mises en œuvre



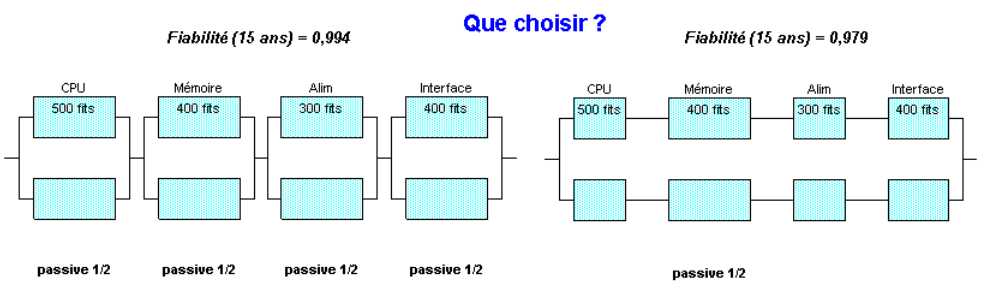
Ambiguïté & incompréhension

Ambiguïté & incompréhension	
N° 16 – Ambiguïté des termes utilisés en fiabilité	Confusion (MTBF / MTTF / MUT, redondance tiède…)
N° 25 – Confusion entre fiabilité et durée de vie	Certains décideurs voudraient que la panne arrive juste à la fin de la mission (confusion entre essais de fiabilité et d'endurance ou durée de vie)
N° 72 – Corrélation n'est pas causalité	Identification infondée de causes d'anomalies
N° 84 – La valeur moyenne à X% de confiance n'est pas le quantile X	Exploitation erronée des résultats de simulation de Monte-Carlo



Décision erronée

Décision erronée	
N° 22 – Quand le plus fiable s'avère peu sûr	Le qualitatif et le quantitatif sont complémentaires en SdF et tous les risques ne sont pas quantifiables
N° 33 – La maîtrise des incertitudes par une communication maîtrisée	Difficulté de communication entre l'analyste et le décideur (confusion entre probabilité d'événement et niveau de confiance, hypothèses non explicites…)
N° 69 – Faut-il baisser la garde quand les pannes se font rares ?	Ne pas supprimer les redondances des satellites même si le MTTF dépasse largement la durée de mission
N° 71 – L'exploitation partisane des données statistiques relatives aux risques	L'argumentaire statistique est parfois volontairement biaisé.
N° 73 – Des impasses malheureuses	Hiérarchiser les problèmes selon leurs conséquences et non pas leur degré de croyance
N° 76 – La finalité de l'action sécuritaire	L'action sécuritaire cherche parfois plus à rassurer ou montrer qu'on agit que résoudre les problèmes
N° 78 – Savoir renoncer à bon escient	Il est souvent difficile d'arrêter un projet quand les risques deviennent déraisonnables

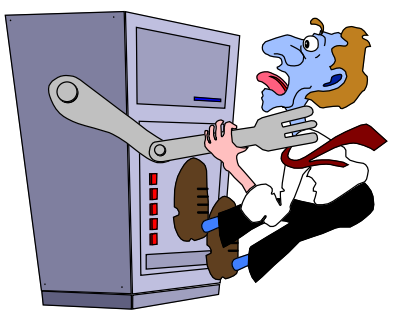


Mauvaise conception

Mauvaise conception	
N° 17 – Oubli de la « panne avance »	Fonctionnement intempestif potentiellement critique
N° 28 – Une indispensable ségrégation	Absence de ségrégation entre redondances ou fonction et protection (illusoire à l'intérieur d'un même composant électronique)
N° 21 – Sensibilité du vote aux modes communs	Absence de ségrégation entre les entrés du vote conduisant à la panne
N° 29 – Une réutilisation hasardeuse	Réutilisation hasardeuse dans des conditions différentes d'exploitation ou d'environnement (Ariane 5 01)
N° 30 – Une propagation de panne quelque peu insidieuse	Mauvais dimensionnement des protections électriques (sensibilité au court-circuit partiel)
N° 68 – Dimensionnement des protections électriques	Surdimensionnement des protections électriques conduisant à la perte d'une chaîne fonctionnelle et de sa redondance
N° 74 – Quand la protection s'avère inopérante	Mauvais dimensionnement des protections électriques (surtension mal passivée)
N° 34 – Quand la Sûreté de Fonctionnement se moque de la résilience	Non prise en compte des interdépendances (énergie électrique…)
N° 37 – De la bonne utilisation des alarmes	Inhibition des alarmes intempestives par les opérateurs (plateforme pétrolière dans le golfe du Mexique)
N° 65 – Quand la barrière de sécurité engendre des catastrophes	Choix malheureux de barrière de sécurité (le blocage des cabines de pilotage contre le terrorisme devient l'arme des pilotes fous)
N° 79 – Choisir un concept robuste ou pallier les faiblesses d'un concept défaillant	Difficulté à fiabiliser un concept intrinsèquement peu fiable (drone quad rotor)

Mauvaise conception

Mauvaise conception	
N° 20 - Sous dimensionnement chronique des stocks de rechange	Dimensionnement diffèrent si TAT garanti ou en valeur moyenne
N° 61 – Des stocks de rechanges mal dimensionnés	Une unité par article n'est pas toujours suffisante
N° 49 – Sur et sous dimensionnement résultant du déterminisme pire cas	L'empilement des marges est très pénalisant et peut être évité par un dimensionnement probabiliste



Pratique discutable

Pratique discutable	
N° 15 – Utilisation abusive d'une méthode d'évaluation	La quantification s'appuie sur la justesse des hypothèses : méthode résistance contrainte applicable que si les distributions sont connues
N° 18 – Le Retour (du manque) d'Expérience	La quantification ne peut pas se fonder sur un REX trop limité
N° 46 - La meilleure raison pour ne rien faire	Un REX met du temps à s'établir.
N° 62 – L'exploitation d'un REX hétérogène	Les données acquises dans des conditions de stress hétérogènes peuvent et doivent être correctement traitées
N° 38 – La preuve par l'outil	Les outils donnent parfois des résultats erronés
N° 39 - Une si jolie boîte noire	La qualité d'un outil de calcul repose d'abord sur les algorithmes avant l'interface utilisateur
N° 40 - Comment générer des catastrophes conformément à la 61508 ?	Les préconisations de la norme 61508 sont parfois discutables
N° 48 – Un bêta qui porte bien son nom	Utiliser pour quantifier grossièrement les modes communs, le β peut paradoxalement conduire à un allègement des analyses qualitatives
N° 45 - Qui trop embrasse mal étreint	L'AMDEC est une analyse de risques et non pas une matrice de conformité
N° 51 – L'anticipation des comportements	Les composants électroniques peuvent s'user
N° 56 – Risque mission et roulette russe	Le prolongement ou la répétition d'une mission augmente d'autant les risques

Pratique discutable

Pratique discutable	
N° 63 – Savoir passer à la simulation	La méthode d'évaluation doit être adaptée à la problématique (l'arbre de défaillance n'est pas dynamique…)
N° 55 – Risques et inflation des exigences	L'inflation des normes touche la SdF. Les outils de gestion des exigences facilitent la production de spécifications volumineuses.
N° 64 – L'insondable gaspillage engendré par la fonction copier-coller	Chaque exigence d'une spécification à un coût
N° 81 – Du bon usage des normes de sécurité	Les normes prescriptives de sécurité conduisent à ne se conformer qu'aux exigences imposées (drones)
N° 66 – Quand ceinture et bretelles engendrent des risques	Le conservatisme et l'excès de précautions inutiles augmente le risque d'obsolescence des produits
N° 70 – A quoi servent les estimations de fiabilité ?	Les estimations de fiabilité servent au dimensionnement mais ne couvrent pas les erreurs de conception ou de fabrications
N° 82 – Agilité et bricolage	Les méthodes « agiles » facilitent la gestion des interfaces mais peuvent nuire aux fondements même des produits
N° 83 – Sûreté de Fonctionnement et Big data	Le Big data ne peut pas satisfaire des attentes démesurées et ne remplacera pas l'activité de SdF
N° 85 – Quand les essais accélérés s'essoufflent	Si l'accélération des essais est moindre qu'attendue, les résultats sont optimistes
N° 58 – La confiance n'exclut pas le contrôle	Les dossiers de SdF n'offre souvent qu'une visibilité partielle qui ne permet pas la contre-expertise (absence de schéma explicatif, de modèle de calcul, d'hypothèse de travail, etc.)

Organisation défectueuse

Organisation défectueuse	
N° 36 – La qualité des groupes d'experts	Se méfier de certains groupes d'experts
N° 42 - Quand le groupe de travail finit par s'assoupir	Un groupe de travail ne peut être éternel
N° 53 – Le fiabiliste de la 25ème heure	L'analyse en SdF ne sert à rien si elle arrive trop tard
N° 75 – Le fiabiliste n'est pas un décideur	Le rôle du fiabiliste est d'instruire les dossiers sur les risques sans se mettre à la place des décideurs (autocensure)
N° 43 - Les limites du dialogue technique	Le partage des connaissances en SdF est limité dans un cadre contractuel
N° 44 - Les bienfaits de la sous-traitance	La sous-traitance en SdF a parfois des effets pernicieux (contrôle d'un sous-traitant par un sous-traitant)
N° 60 – Une complexité pas si facile à maitriser	La complexité peut difficilement être maîtrisée par des débutants
N° 77 – Peut-on confier l'optimisation d'un système à son fournisseur quand on est opérateur ?	Le fournisseur n'a pas les mêmes objectifs que l'opérateur (maximiser les ventes plutôt qu'optimiser le système)
N° 54 – Langues orientales et fiabilité	Les caractéristiques précises des produits sont de plus en plus difficiles à obtenir
N° 67 – Quand l'organisation faillit	La confiance dans certaines organisations à risques est quelque peu ébranlée (nucléaire…)
N° 32 – Une communication autour du risque bien dévalorisée	La délivrance d'informations douteuses ou approximatives finit par nuire à la crédibilité de toute communication sur les risques

Conclusion

☐ Quelques évidences :

- l'erreur est humaine mais ne doit pas se reproduire (« Errare humanum est, sed perseverare diabolicum est »),
- la complexité se maitrise par la simplicité (ségrégation, etc.),
- la confiance n'exclue par le contrôle et l'analyse doit pouvoir faire l'objet de contre-expertise,
- se méfier de l'intuition dans les calculs de probabilité …. et des erreurs de saisie (Excel),
- garder son sens critique et son intégrité scientifique,
- etc.

➢ Le Bêtisier du fiabiliste devrait survivre à la fin de l'activité au CNES de son auteur, et sera enrichi, si nécessaire, de ses propres erreurs.

☐ La RGPD ne permet plus de vous envoyer des informations sans votre accord et nécessite une demande d'abonnement (gratuit) : http://www.cabinnovation.com/contact