Société de Calcul Mathématique, S. A.
Outils d'aide à la décision
depuis 1995

Analyse critique des calculs de fiabilité

de systèmes électroniques embarqués

Rapport rédigé par la

Société de Calcul Mathématique SA

novembre 2007

Résumé opérationnel

On s'intéresse ici à des systèmes électroniques qui vont être embarqués sur des avions. La démarche de sûreté doit prendre en compte les différentes phases : au sol, en vol, en essais, etc. On souhaite vérifier que la probabilité globale d'un accident est inférieure à un seuil défini, mais on souhaite aussi identifier les éléments les plus critiques, pour assurer une meilleure surveillance.

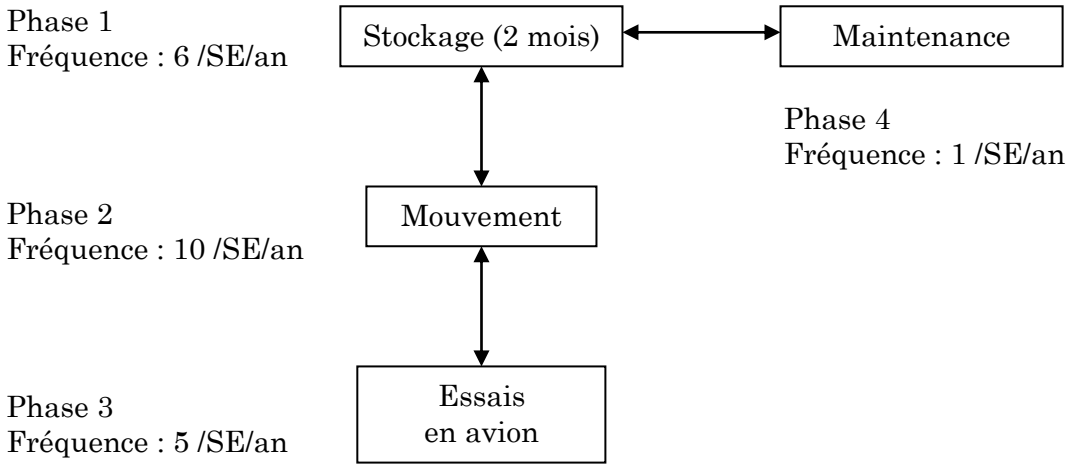
Pour expliquer la méthode d'analyse des risques, nous avons construit un exemple factice de scénario. Il nous permet de mettre en évidence les points, dans la méthode actuelle, qui sont susceptibles d'amélioration. Dans une deuxième partie, nous détaillons le problème lié à la prise en compte de la durée des phases dans le calcul des probabilités.

Enfin, nous donnons nos recommandations pour améliorer la méthode actuelle. Une partie des défauts peut être corrigée via des améliorations portant sur le vocabulaire utilisé et en supprimant les unités fictives employées.

Siège social et bureaux : 111, Faubourg Saint Honoré, 75008 Paris. Tel. : 01 42 89 10 89. Fax : 01 42 89 10 69
Société Anonyme au capital de 56 200 Euros. RCS : Paris B 399 991 041. SIRET : 399 991 041 00035. APE : 731Z

I. Un exemple factice

Voici un exemple simpliste de scénario couvrant une année et comprenant 4 phases répétées un certain nombre de fois :



Le schéma décrit les différentes actions effectuées chaque année pour chaque Système Electronique (SE). Ainsi, pour notre exemple, le SE est déplacé puis fixé dans l'avion pour réaliser différents essais 5 fois par an. Une maintenance est également effectuée une fois par an. On note que les phases n'ont pas la même fréquence.

Pour une phase "Essais en avion", il faut logiquement deux phases "Mouvement" : une dans chaque sens.

Le découpage du scénario par "phases" accompagnées d'une fréquence semble donc le plus approprié. Chaque phase correspond à une unité de lieu, de temps et de matériel.

1. Agressions

L'environnement des opérations, les infrastructures, le matériel utilisé et les opérations elles-mêmes sont la source possible d' "agressions" qui peuvent affecter directement et/ou indirectement le SE. Les agressions sont regroupées par nature et par gammes d'intensité dans des agressions dites "enveloppes" afin d'en limiter le nombre.

Une agression enveloppe de départ peut conduire à plusieurs agressions enveloppes résultantes sur le SE. Une agression enveloppe résultante peut donc avoir plusieurs origines. La probabilité d'occurrence de chaque agression résultante dépend donc du "chemin d'agression", c'est à dire de l'enchaînement logique des évènements.

2. Chemins d'agression

Pour notre exemple, nous avons listé les agressions possibles lors de chaque phase. Les agressions possibles choisies sont volontairement simplistes et seulement au nombre de quatre : choc, chute, incendie et explosion.

Pour simplifier, on ne considère qu'un seul intermédiaire possible entre l'agression d'origine et l'agression résultante sur le SE, à savoir le vecteur. La réaction du vecteur aux agressions auxquelles il peut être soumis est connue et est donnée par le tableau suivant :

Agression sur le vecteur	Conséquence	Probabilité
Chute	Incendie	10^{-3}
Incendie	Explosion	10^{-4}

Tableau 1 : Agressions sur le vecteur et conséquences

On considère que l'enchaînement chute > incendie > explosion n'est pas possible pour notre exemple.

Remarques. - En réalité, une agression sur le vecteur peut conduire à quasiment toutes les défaillances possibles avec une probabilité connue. Il faut faire la distinction entre les enchaînements d'évènements qui sont matériellement impossibles et les chemins peu probables ou de probabilité considérée comme négligeable. Dans le premier cas, il n'y a pas de chemin. Dans le second, le chemin existe ; il doit apparaître et être compté dans le nombre total de chemins d'agression. Concernant ce point et les chemins négligeables, cela doit être correctement indiqué.

Le SE est reliée au vecteur seulement lors des phases de mouvement et d'essais, c'est donc seulement lors de ces phases que l'on peut trouver des chemins d'agression indirects à partir de l'agression d'origine.

Dans la représentation des chemins d'agression qui suit, chaque ligne correspond à un chemin. On trouve d'abord le numéro du chemin puis l'agression d'origine, suivie s'il y a lieu de l'agression consécutive à la réaction du vecteur, enfin la dernière colonne indique l'agression résultante sur le SE.

Phase 1 : Stockage (2 mois) – Configuration : SE seul

Chemin	Agression d'origine				Agression résultante sur SE
1	Incendie →			→	Incendie

Phase 2 : Mouvement – Configuration : SE et vecteur

Chemin	Agression d'origine		Intermédiaire : Vecteur		Agression résultante sur SE
1	Chute →			→	Chute
2	Chute →	→	Incendie →	→	Incendie

Phase 3 : Essais sous avion – Configuration : SE et vecteur

Chemin	Agression d'origine		Intermédiaire : Vecteur		Agression résultante sur SE
1	Chute →			→	Chute
2	Chute →		Incendie →		Incendie
3	Incendie →			→	Incendie
4	Incendie →		Explosion →		Explosion

Phase 4 : Maintenance – Configuration : SE seule

Chemin	Agression d'origine				Agression résultante sur SE
1	Choc →			→	Choc
2	Incendie →			→	Incendie

3. Grandeurs caractéristiques d'une phase

Pour chaque phase, on a établi la liste des chemins d'agression possibles. On note n_1, n_2, n_3 et n_4 le nombre de chemins des phases 1, 2, 3 et 4. On a donc $n_1 = 1$, $n_2 = 2$, $n_3 = 4$ et $n_4 = 2$.

Chaque phase est donc caractérisée par sa fréquence (nombre de répétitions de la phase par an) f_i et un nombre de chemins d'agression n_i, avec $1 \le i \le 4$. La suite de la méthode s'intéresse aux chemins d'agression seulement, avant de revenir à un point de vue général. Les probabilités d'accident ne sont pas calculées au niveau des phases.

Nous considérons qu'il faut faire ce calcul pour chaque répétition élémentaire de la phase et il faut le présenter comme tel. Pour la phase i, chaque chemin d'agression est caractérisé par une probabilité d'occurrence $\Pr_{i,j}$, avec $1 \le j \le n_i$. Voyons comment calculer cette valeur.

4. Probabilité d'un chemin d'agression

La probabilité d'un chemin d'agression est la probabilité d'occurrence de l'agression résultante sur le SE selon le chemin considéré. Pour la plupart des chemins d'agression, l'agression enveloppe d'origine agit directement sur le SE et la probabilité du chemin correspond alors simplement à la probabilité de l'agression d'origine.

D'autres agressions enveloppes agissent indirectement sur le SE. L'agression frappe d'abord l'avion, l'infrastructure, etc. et provoque une nouvelle agression qui agit à son tour sur le SE. Pour ces situations, la probabilité que l'agression d'origine devienne telle ou telle agression par l'intermédiaire de l'avion, etc. est connue. La probabilité de l'agression résultante sur le SE est donc le produit des différentes probabilités le long du

chemin d'agression. D'autres cas sont plus complexes. Certaines agressions agissent sur le SE à la fois de manière directe et indirecte.

Voyons un exemple avec notre scénario. Lors de la phase 2 – "Mouvement", le SE est reliée au vecteur le tout étant déplacé sur un chariot. En cas de chute sur le sol (probabilité p_0), plusieurs chemins d'agression sont possibles :

Chemin 1 : La chute affecte directement le SE
La probabilité de ce chemin est simplement p_0

Chemin 2 : La chute affecte le vecteur qui s'enflamme
La probabilité que le vecteur s'enflamme en cas de chute est p_1. Il s'agit d'une probabilité conditionnelle. L'agression résultante sur le SE est donc de type thermique.
La probabilité de ce chemin est $p_0 \times p_1$

Remarque. - Les probabilités étant toujours inférieures à 1, et généralement inférieures à 10^{-3} pour notre sujet, il apparaît donc qu'un chemin d'agression indirect est toujours de probabilité inférieure ou égale à celle du chemin d'agression direct d'origine commune. On pourrait donc être tenté de ne pas considérer le chemin indirect.

Il ne faut pas oublier que la probabilité du chemin n'est pas la probabilité d'accident. On doit en effet encore prendre en compte l'insensibilité, dont la valeur dépend de l'agression résultante, comme on va le voir dans le paragraphe suivant. Cette valeur varie beaucoup selon l'agression résultante, ce qui peut compenser la différence de probabilité des chemins direct et indirects. Il ne faut donc à ce stade négliger aucun chemin d'agression.

Dans notre exemple, la même agression enveloppe d'origine peut être présente dans plusieurs phases, c'est le cas pour la chute et l'incendie. Cependant, la probabilité d'occurrence n'a pas de raison d'être la même d'une phase à l'autre. En effet, les agressions considérées ne sont que des enveloppes et l'agression réelle comprise dans l'agression enveloppe varie d'une phase à l'autre selon les opérations effectuées. La probabilité dépend de ces opérations, d'où l'emploi de l'unité [1/opération] dans les tableaux de probabilité des agressions réelles. Cette unité est ambiguë et n'a pas de définition exacte, les opérations étant toutes différentes. Elle doit donc être proscrite.

Les opérations effectuées et les agressions possibles qui en découlent doivent être suffisamment bien définies pour que la probabilité d'agression soit explicite et sans unité.

Certaines agressions sont présentes lors de plusieurs phases de durées différentes ; la durée doit alors être prise en compte pour le calcul de la probabilité de l'agression. En effet, si une phase dure N unités de temps et si on connaît la probabilité p d'une agression sur chaque unité, alors la probabilité d'agression sur l'ensemble de la phase est $P = 1-(1-p)^N$. Nous développons ce point particulier dans la partie II.

Ainsi, pour notre exemple, si la probabilité d'un incendie dans le bâtiment de stockage vaut $10^{-6}/j$, alors la probabilité d'incendie lors de la phase 1 vaut $1-(1-10^{-6})^{60} \approx 6\times10^{-5}$.

Pour les autres phases, nous fixons les probabilités des différentes agressions d'origine comme indiqué dans le tableau suivant :

Phase i	Agression d'origine	Probabilité
1	Incendie	6×10^{-5}
2	Chute	10^{-3}
3	Chute	10^{-4}
	Incendie	5×10^{-4}
4	Choc	10^{-3}
	Incendie	10^{-4}

Tableau 2 : Probabilités des agressions d'origine

En utilisant ces données, les chemins d'agression et les probabilités de défaillance du vecteur suite à une agression (Tableau 1), on peut maintenant calculer la probabilité de chaque chemin d'agression. Le tableau suivant donne les résultats :

Phase i	Chemin d'agression j	Agression résultante sur SE	Probabilité du chemin $\Pr_{i,j}$
1	1	Incendie	6×10^{-5}
2	1	Chute	10^{-3}
	2	Incendie	$10^{-3}\times10^{-3}=10^{-6}$
3	1	Chute	10^{-4}
	2	Incendie	$10^{-4}\times10^{-3}=10^{-7}$
	3	Incendie	5×10^{-4}
	4	Explosion	$5\times10^{-4}\times10^{-4}=5\times10^{-8}$
4	1	Choc	10^{-3}
	2	Incendie	10^{-4}

Tableau 3 : Probabilités des chemins d'agression

5. Risque d'accident lié à chaque chemin d'agression

L'insensibilité est une probabilité conditionnelle : c'est la probabilité d'accident sachant que l'agression a eu lieu. L'utilisation de l'unité [1/agression] est inutile pour les mêmes raisons que celles déjà évoquées.

On considère trois types d'accident, notés A, B, C. Le tableau suivant indique les insensibilités vis à vis de l'accident A pour chaque agression résultante de notre exemple.

Agression résultante sur SE	Insensibilité A I_A
Choc	10^{-10}
Chute	10^{-9}
Incendie	10^{-8}
Explosion	10^{-7}

Tableau 4 : Insensibilités

Pour le cas réel, ce tableau est complété par les insensibilités vis à vis des accidents B et C. Pour notre exemple, nous nous limitons à l'accident A.

Le risque d'accident A lors de la phase i lié au chemin d'agression j est : $\Pr_{i,j} \times I_A$. Pour notre exemple, on a donc :

Phase i	Chemin d'agression j	Agression résultante sur SE	$\Pr_{i,j} \times I_A$
1	1	Incendie	$6\times10^{-5}\times10^{-8}=6\times10^{-13}$
2	1	Chute	$10^{-3}\times10^{-9}=10^{-12}$
	2	Incendie	$10^{-6}\times10^{-8}=10^{-14}$
3	1	Chute	$10^{-4}\times10^{-9}=10^{-13}$
	2	Incendie	$10^{-7}\times10^{-8}=10^{-15}$
	3	Incendie	$5\times10^{-4}\times10^{-8}=5\times10^{-12}$
	4	Explosion	$5\times10^{-8}\times10^{-7}=5\times10^{-15}$
4	1	Choc	$10^{-3}\times10^{-10}=10^{-13}$
	2	Incendie	$10^{-4}\times10^{-8}=10^{-12}$

Tableau 5 : Probabilité d'accident de type A liée à chaque chemin d'agression

Pour savoir si le risque lié à chaque chemin est important ou non par rapport aux autres, on compare cette valeur avec l'objectif de sûreté enveloppe (OSE) de chaque phase. Voyons comment est calculée cette valeur.

6. Répartition des OGS en OSE

Pour chaque type d'accident (A, B, C), l'objectif est que sa probabilité ne dépasse pas une valeur seuil appelée Objectif Global de Sécurité (OGS). Chaque OGS est exprimée par SE et par an : [1/SE/an].

On se pénalise en réduisant l'OGS de 32.5%, ce qui revient à le multiplier par $\frac{67.5}{100}$. La valeur obtenue est ensuite divisée par le nombre total $n = \sum_i n_i$ de chemins d'agression.

La quantité $\frac{67.5}{100} \times \frac{OGS_N}{n}$ est exprimée en [1/SE/an/chemin d'agression]. Cette unité est ambiguë et laisse penser que l'on fait une hypothèse d'équiprobabilité de tous les chemins d'agression.

Dans le nombre de chemins d'agression n, un chemin d'agression donné est compté plusieurs fois s'il apparaît dans plusieurs phases. De plus, les phases n'ont pas la même fréquence, le même chemin d'agression se répète donc avec la fréquence de la phase. Il est donc dangereux d'utiliser l'unité [chemin d'agression] qui ne correspond ici à rien d'établi.

L'objectif de sûreté enveloppe (OSE) se décline pour chaque phase et a pour expression :

$$OSE_N(Phase\ i) = \frac{67.5}{100} \times \frac{OGS_N}{n \times f_i}$$

La valeur précédente a simplement été divisée par la fréquence f_i de la phase. La fréquence s'exprimant en [1/SE/an], l'OSE par phase est exprimé en [1/chemin d'agression]. Cependant, comme on l'a expliqué, cette unité est floue. L'OSE est une probabilité, il n'y a donc pas lieu de lui donner une unité.

Remarques. - Le calcul de l'OSE de chaque phase tel qu'il est présenté n'est pas clair. Il devient plus logique si on remarque que :

$$OSE_N(Phase\ i) = \frac{67.5}{100} \times \frac{OGS_N}{n \times f_i} = \left(\frac{67.5}{100} \times OGS_N \times \frac{n_i}{n} \right) \times \frac{1}{n_i \times f_i}$$

L'OGS est réparti entre les phases au prorata du nombre de chemins d'agression $\frac{n_i}{n}$. Ensuite, pour une phase donnée, la valeur entre parenthèse est divisée par la fréquence f_i et répartie de manière équiprobable entre les n_i chemins d'agression de la phase.

L'expression des OSE par phase laisse à penser que :

– Plus le nombre de chemins d'agression est grand, plus le risque est élevé ;

– Plus la fréquence d'une phase est grande, plus le risque est élevé pour cette phase.

On peut imaginer d'autres formules reposant sur d'autres hypothèses. On pourrait par exemple commencer par attribuer la même part de l'OGS à chaque phase, puis prendre

en compte la fréquence et le nombre de chemins, ou encore considérer une valeur unique pour tous les chemins d'agression.

Le terme utilisé pour désigner la quantité $OSE_N(Phase\,i) = \frac{67.5}{100} \times \frac{OGS_N}{n \times f_i}$ ne semble pas clairement établi. En effet, dans le Catalogue d'Objectifs, les termes "OSE"; "Objectif résultant par ligne" et "OGS résultant par phase" sont utilisés alternativement pour désigner la même chose. Le terme OSE semble avoir été défini dans ce but, tout les autres termes doivent êtres abandonnés pour plus de clarté.

Pour chaque phase, l'OSE représente une probabilité seuil d'accident que chaque chemin d'agression ne doit pas dépasser. De même que pour les OGS, chaque OSE est décliné pour les 3 accidents A, B, C.

Le produit $\Pr_{i,j} \times I_A$ de chaque chemin d'agression est donc comparé à $OSE_N(Phase\,i)$. Lorsque le produit est supérieur, le chemin est considéré comme critique. C'est là la seule fonction des OSE. On ne sait pas, à ce stade, si au niveau global la valeur seuil de l'OGS est respectée.

Revenons à notre exemple. Le nombre total de chemins d'agression est $n = \sum_i n_i = 1+2+4+2 = 9$. L'Objectif Global de Sécurité pour l'accident A vaut : $OGS_N = 10^{-10} / SE / an$. En appliquant la formule citée plus haut, on calcule donc l'OSE de chaque phase :

Phase i	Intitulé	Fréquence f_i	$OSE_N(Phase\,i)$
1	Stockage	1	1.3×10^{-12}
2	Mouvement	10	7.5×10^{-13}
3	Essais en avion	5	1.5×10^{-12}
4	Maintenance	1	7.5×10^{-12}

Tableau 6 : Valeur de l'OSE pour chaque phase

On peut maintenant identifier les chemins critiques de notre exemple. Ils sont au nombre de 2 : le chemin 1 de la phase 2 et le chemin 3 de la phase 3.

L'utilité des OSE s'arrête ici ; ils n'ont pas d'autre fonction que l'identification des chemins critiques.

7. Risque global d'accident – "consommation de l'OGS"

La probabilité d'accident pour l'ensemble des phases sur une année et pour une SE correspond à la somme des probabilités d'accident dues à chaque chemin d'agression pondérée par la fréquence des phases. On parle alors d'OGS "consommé" :

$$\text{OGS consommé} = \sum_{i=1}^{4}\left(f_i \times \sum_{j=1}^{n_i} \text{Pr}_{i,j} \times I_A \right)$$

Pour notre exemple, cela donne :

$$\text{OGS consommé} = \begin{bmatrix} 1\times\left(6\times10^{-13}\right) \\ +10\times\left(10^{-12}+10^{-14}\right) \\ +5\times\left(10^{-13}+10^{-15}+5\times10^{-12}+5\times10^{-15}\right) \\ +1\times\left(10^{-13}+10^{-12}\right) \end{bmatrix} = 4\times10^{-11} / SE / an$$

L'objectif de $10^{-10} / SE / an$ est respecté ; seuls 60% des 67.5% de l'OGS_A attribués sont effectivement consommés.

II. Probabilité d'agression et durée des phases

La probabilité de certaines agressions est mal exprimée. C'est particulièrement le cas pour les probabilités exprimées par "opération".

En effet, une même agression peut se produire lors de différentes phases qui n'ont a priori pas la même durée. Or il paraît logique que lors d'une phase longue, le risque soit plus important que lors d'une phase courte. Une probabilité par "opération" ne permet pas de traduire cela.

Pour les agressions caractérisées par des unités ambiguës, l'origine de la valeur doit être précisée afin de l'exprimer dans une unité conventionnelle. Il est ensuite simple de calculer la probabilité en fonction de la durée.

En effet, si une phase dure N unités de temps (ou bien concerne N unités de distance) et si on connaît la probabilité p d'une agression sur chaque unité de temps, alors la probabilité d'agression sur l'ensemble de la phase est $P=1-\left(1-p\right)^N$, à condition que les étapes soient indépendantes.

On notera que $P=1-\left(1-p\right)^N \approx N\times p$ si $N\times p \ll 1$, ce qui est souvent le cas ici. Le calcul des probabilités tel qu'il est présenté reste donc correct pour la grande majorité des cas.

IV. Nos recommandations

Comme on l'a vu à plusieurs reprises, les défauts de la méthode employée proviennent en grande partie de l'utilisation d'un vocabulaire mal adapté ou mal défini. L'attribution d'unités fictives aux différentes grandeurs ne facilite ni la compréhension, ni les calculs.

Nous rappelons qu'en dehors du cas particulier des valeurs temporelles (par heure, jour ou année), une probabilité est sans unité. Pour résoudre le problème de la prise en compte de la durée des phases, il faut commencer par exprimer convenablement les probabilités des agressions d'origine. L'étude de l'origine de chaque valeur doit permettre de savoir s'il s'agit d'une valeur temporelle ou bien si elle dépend uniquement des opérations effectuées et est donc sans dimension.

Le calcul des probabilités se fait actuellement au niveau élémentaire des chemins d'agression puis au niveau global. Nous recommandons de calculer les probabilités d'accident pour chaque répétition élémentaire de chacune des phases afin d'introduire un niveau intermédiaire plus accessible, ni trop ni trop peu détaillé.

La représentation des chemins d'agression doit être refaite à partir de nouvelles bases qui permettront d'une part une lecture plus facile, mais aussi de n'oublier aucun chemin. Chaque chemin doit être représenté de manière plus linéaire par une suite logique d'événements placés côte à côte.

Enfin, nous suggérons l'abandon du terme "phase" pour celui d' "opération globale". Chaque "opération globale" serait composée d' "opérations élémentaires" et caractérisée par une probabilité d'accident (probabilité d'un accident quelconque pendant l'opération globale) et une fréquence (nombre de fois où l'opération globale est répétée dans l'année).