Limites d'utilisation des normes EN 61508 - EN 61511. Retour d'expérience d'un organisme de certification

Brice Lanternier, Jean-Michel Dranguet, Dominique Charpentier

LIMITES D'UTILISATION DES NORMES EN 61508-EN 61511
RETOUR D'EXPERIENCE D'UN ORGANISME DE CERTIFICATION

OPERATIONAL LIMIT OF EN 61508- EN 61511
EXPERIENCE FEEDBACK OF A CERTIFICATION ORGANIZATION

LANTERNIER B., – DRANGUET J.-M., CHARPENTIER D.

INERIS
Parc ALATA
60550 Verneuil en Halatte- France

Résumé : Les normes de sécurité fonctionnelle et notamment les normes EN 61508/61511 introduisent une évaluation de la probabilité de défaillances dangereuses en complément de l'analyse déterministe traditionnelle.

L'application de ces normes sur différents matériels et systèmes a permis de mettre en évidence des difficultés relatives à la nature des grandeurs calculées ainsi qu'aux outils mathématiques associés. La comparaison des différents modèles mathématiques met en évidence que l'utilisation de graphes de Markov peut conduire à des résultats approximatifs pour des matériels partiellement réparables.

L'article tentera d'apporter des éléments de réponse à ces difficultés en s'appuyant sur l'expérience de l'INERIS dans l'évaluation et la certification de matériel et de systèmes instrumentés de sécurité.

Summary : Safety functional standards and in particular the standards IEC 61508/61511 introduce an assessment of the dangerous failure probability on demand in complement of the traditional deterministic analysis. The application of these standards on various equipments and systems made it possible to highlight difficulties relating to the concepts calculated thus to the associated mathematical tools. Comparison of various mathematical models highlights that the use of Markov graphs can lead to approximate results for partially reparable equipments.

The article will try to bring brief replies to these difficulties while being based on the experiment of INERIS in the assessment and the certification of instrumented safety material and systems.

Mots-clefs : SIL, graphes de Markov, blocs diagrammes, PFD.

Domaine : Réglementation - normalisation

---

1 INTRODUCTION

La norme EN 61508 [1] devient la norme de référence pour la spécification et la conception des systèmes instrumentés de sécurité (SIS). Cette norme générique est destinée plus particulièrement aux fabricants et fournisseurs de systèmes électriques, électroniques et électroniques programmables de sécurité (EEPS). La norme EN 61511 [2] est elle, plutôt destinée aux concepteurs, intégrateurs et utilisateurs dans le domaine du process industriel.

Ces normes de sécurité fonctionnelle introduisent une approche probabiliste qui vient compléter l'approche déterministe classique. L'introduction de probabilité dans la mesure du niveau de sécurité a entraîné la mise en place de nouveaux concepts tels que les notions de calculs de probabilité de défaillance à la sollicitation ou de défaillance par unité de temps.

Elles n'imposent cependant pas l'utilisation de modèles particuliers mais fournissent des formules approchées pour les architectures courantes. Les limites d'application de ces formules aux architectures les plus simples contraignent les utilisateurs de ces normes à maintenir les éléments intervenant dans les formules d'une part, et à entreprendre des modélisations sur des systèmes complexes d'autre part.

Différentes techniques sont néanmoins préconisées. Parmi celle-ci, on peut citer les arbres de défaillances, les blocs diagramme fiabilité ainsi que les graphes de Markov. Les deux premières permettant une modélisation statique des systèmes à la différence des graphes de Markov qui permettent de mener des études de fiabilité dynamique. Nous montrons par la suite les difficultés qu'entraîne l'application de la quantification probabiliste des défaillances telles que préconisée par les normes EN 61508 et EN 61511.

2 MODELISATION PAR LES FORMULES APPROCHEES DE LA NORME EN 61508

2.1 Introduction

Certains principes et hypothèses de base de la norme EN 61508 doivent être rappelés :

- Tout d'abord, l'évaluation probabiliste des boucles de sécurité s'applique à des composants ayant des défaillances aléatoires et modélisés par conséquent par une distribution exponentielle. Les taux de défaillance sont présumés être à taux constant et indépendant du temps.
- Les pannes sont classées en quatre catégories. On distingue les défaillances sûres des défaillances dangereuses, chacune de ces catégories étant divisée en défaillances détectées et non détectées.
- On définit le terme diagnostic de couverture qui exprime la proportion des défaillances dangereuses détectées :

$$\mathrm{DC} = \frac{\lambda_{\mathrm{dd}}}{\lambda_d}$$

- La probabilité moyenne de défaillance dangereuse (PFD_{avg}) à la sollicitation est due :
  - A l'apparition de défaillances dangereuses détectées (λ_{dd}) lors de tests on line.
  - A la présence de défaillances dangereuses non détectées (λ_{du}) pendant la phase de fonctionnement et nécessitant une intervention. Pendant la phase de réparation, la fonction de sécurité n'est pas assurée.
- Les défaillances dangereuses totales (λ_d) sont égales aux défaillances dangereuses détectées et non détectées.
- Le temps de détection des tests on line est considéré comme nul.

La norme introduit également des défaillances de causes communes pour les architectures redondantes. Des études sur la mise en place et l'évaluation des modes communs ont été réalisées [3 ;4 ;5], l'article ne le traite pas pour des raisons de facilité de compréhension. De plus, la validité d'un mode commun ne prenant pas en considération l'architecture est contestable.

Notons également que le taux de défaillance d'un système redondant de deux équipements à taux constant n'est plus à taux constant. La simple addition des taux de défaillance des composants suggérée par la norme génère des erreurs (conservatives).

2.2 Structure 1oo1

Pour un système monocanal, la probabilité moyenne de défaillances dangereuses détectées est :

$$PFD_{avg1oo1} = \lambda_{dd} \cdot MTTR$$

En effet, la norme considère que ces défaillances sont réparées immédiatement. L'indisponibilité du canal est donc uniquement liée au temps de réparation moyen (MTTR) et à la probabilité d'apparition des défaillances.

La probabilité de défaillance pour des défaillances dangereuses non détectées est, elle :

$$PFD_{avg1oo1} = \lambda_{du} \cdot \left(\frac{T_i}{2} + MTTR \right)$$

On considère qu'une défaillance dangereuse non détectée est découverte lors des tests de révision. L'indisponibilité moyenne du canal est donc directement liée à la moyenne des temps entre test de révision T_i auquel on ajoute le temps de réparation MTTR.

Au final, la probabilité moyenne de défaillance pour une structure mono-canal s'exprime donc sous la forme :

$$PFD_{avg1oo1} = \lambda_{du} \cdot \left(\frac{T_i}{2} + MTTR \right) + \lambda_{dd} \cdot MTTR$$

Cette relation peut également s'écrire de la façon suivante:

$$PFD_{avg1oo1} = \lambda_d \cdot \left(\frac{\lambda_{du} \cdot \left(\frac{T_i}{2} + MTTR \right)}{\lambda_d} \right) + \lambda_d \cdot \left(\frac{\lambda_{dd}}{\lambda_d} \cdot MTTR \right)$$

et en posant :

$$T_{ce} = \left(\frac{\lambda_{du} \cdot \left(\frac{T_i}{2} + MTTR \right)}{\lambda_d} \right) + \left(\frac{\lambda_{dd}}{\lambda_d} \cdot MTTR \right)$$

la probabilité de défaillance devient donc

$$PFD_{avg1oo1} = \lambda_d \cdot T_{ce}$$

qui est l'équation proposée dans la norme EN 61508. Le facteur T_{ce} est désigné dans cette norme comme le temps d'indisponibilité équivalent du canal.

2.3 Structure 1oo2

la loi d'indisponibilité des défaillances dangereuses d'une structure ayant deux canaux identiques peut s'exprimer par la relation :

$$PFD_{avg1oo2} = \frac{1}{T_i} \int_0^{T_i} PFD_1(t) \cdot PFD_2(t) dt$$

La norme EN 61508 établie pour une structure 1oo2, la formule approchée suivante :

$$PFD_{avg1oo2} = 2 \cdot \lambda_d^2 \cdot T_{ce} \cdot T_{ge}$$

Avec

$$T_{ge} = \left(\frac{\lambda_{du} \cdot \left(\frac{T_i}{3} + MTTR \right)}{\lambda_d} \right) + \left(\frac{\lambda_{dd}}{\lambda_d} \cdot MTTR \right)$$

En considérant la loi d'indisponibilité des défaillances dangereuses uniquement non détectées et après simplification (ex : MTTR négligé), les relations suivantes sont obtenues :

$$\mathrm{PFD}_{\mathrm{avg1oo2\_}\lambda_{\mathrm{du}}} = \frac{1}{T_i}\int_0^{T_i} \lambda_{du} \cdot \lambda_{du} \cdot t^2 dt$$

$$\mathrm{PFD}_{\mathrm{avg1oo2\_}\lambda_{\mathrm{du}}} = \lambda_{du}^2 \cdot \frac{T_i^2}{3}$$

soit encore :

$$\mathrm{PFD}_{\mathrm{avg1oo2\_}\lambda_{\mathrm{du}}} = 2 \cdot \lambda_{du}^2 \cdot \left(\frac{T_i}{2} \cdot \frac{T_i}{3}\right)$$

Au sens de la norme EN 61508, le terme T/2 correspond au temps d'indisponibilité d'un canal (T_{ce}) et T/3 à celui liée à la redondance, ceci pour des défaillances dangereuses non détectées et avec les temps de réparation (MTTR) négligés.

Ces formules sont parfois difficiles à appliquer car elles ne correspondent pas à la configuration du système à étudier. En outre, certaines grandeurs peuvent conduire à des confusions notamment avec les notions de :

- probabilité de défaillance à la demande (PFD)
- probabilité de défaillance moyenne (PFD_{avg})
- probabilité de défaillance en continu (PFH)
- et taux de défaillance (λ)

Ces grandeurs utilisées pour caractériser la perte de sécurité dans la norme sont en effet peu précises.

3 MODELISATION A L'AIDE DE GRAPHES DE MARKOV

3.1 Introduction

La modélisation par graphes de Markov est une des approches évoquées dans la norme. Cette technique est souvent utilisée en sûreté de fonctionnement lorsque l'on souhaite modéliser un système avec des composants à taux de défaillance constant et réparable (pour la prise en compte des taux de réparation). Il permet ainsi de faire une analyse dynamique du système. On ne se trouve plus dans une modélisation à deux états (fonctionnement-panne). Cependant ce modèle est délicat à utiliser.

L'approche markovienne peut être appliquée aux systèmes dont le comportement varie de manière discrète ou aléatoire dans le temps ou l'espace. Ces variations aléatoires discrètes ou continues sont connues sous le nom de processus stochastique. Un exemple de processus stochastique est le processus de poisson. Ce processus décrit les défaillances aléatoires d'un composant, du point de vue des phénomènes physiques qui créent ces causes. Un processus de Markov est une forme spéciale de processus stochastique.

Un processus stochastique est appelé processus de Markov si la distribution de probabilité est exclusivement déterminée par la valeur présente, et non par l'enchaînement des valeurs passées. Cette propriété Markovienne signifie que le processus n'a pas de mémoire, ce qui implique que même si on connaît ce qui s'est passé jusqu'au temps t, la suite du processus dépend uniquement de l'état du processus au temps t.

En conséquence de cette propriété, un composant réparé est considéré comme neuf (AGAN) et le taux de défaillance de chaque matériel est considéré indépendant des séquences de défaillances de ces composants.

Les modèles de Markov avec des transitions constantes entre les différents états sont dit homogènes. Ceci signifie que les défaillances et les réparations ont des distributions exponentielles. Lorsque les transitions dépendent du temps, on parle de modèles de Markov non homogènes.

3.2 Difficultés rencontrées

Le premier inconvénient admis par tous est l'augmentation très rapide du nombre d'état en fonction du nombre de composants. Des solutions existent pour atténuer ce problème (par exemple l'approche par cut-set).

Un autre désavantage de l'approche markovienne se situe au niveau de l'interprétation des résultats nettement plus complexes que pour un arbre de défaillance par exemple.

3.2.1 Modélisation de l'architecture

Selon l'interprétation que l'on a du système, plusieurs graphes de Markov peuvent être mis en place. De plus, la distinction entre défaillance dangereuse détectée et défaillance dangereuse non détectée complique encore la représentation. Par exemple, un système redondant avec une architecture 1oo2 composée d'éléments identiques, peut être modélisé de manières différentes en terme de sécurité avec les différents concepts de défaillances introduits par la norme CEI 61508. Selon les défaillances considérées, on obtient donc :

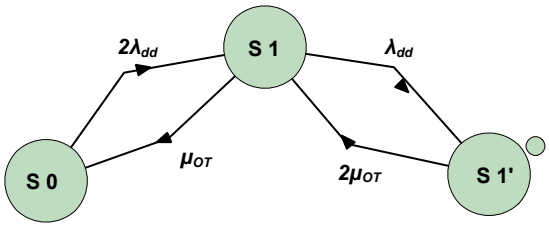

Fig 1. Architecture 1oo2 avec défaillance détectée.

Dans le cas de défaillances dangereuses non détectées, le graphe devient :

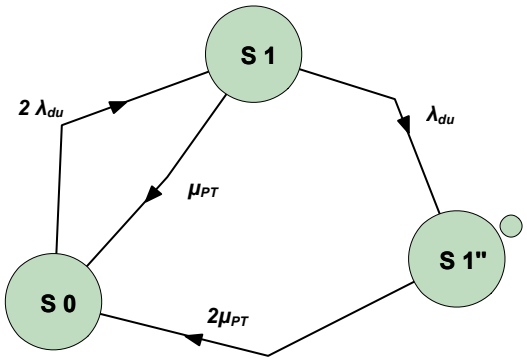

Fig 2. Architecture 1oo2 avec défaillance non détectée

Le taux de réparation μ_{PT}, taux de réparation des tests périodiques, symbolise le fait qu'il est possible de détecter les pannes dangereuses non détectées uniquement lors des tests de révisions. Il est alors égal à l'inverse du temps de mission (Ti).

Le taux de réparation μ_{OT}, taux de réparation des tests on-line, symbolise le fait que des tests périodiques permettent de détecter un pourcentage de pannes dangereuses. Il est alors égal à l'inverse du temps moyen d'indisponibilité (MDT) que l'on considère équivalent au temps moyen de réparation (MTTR).

4 APPLICATION

En considérant la combinaison de défaillances dangereuses détectées et non détectées, un système 1oo2 peut être modélisé comme suit :

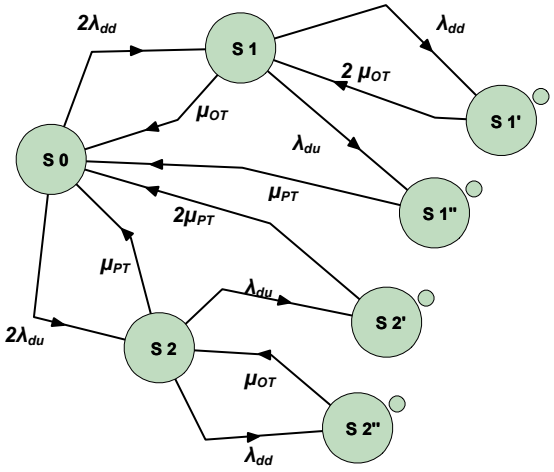

Fig 3. Architecture 1oo2 avec défaillance détectée et non détectée

Le calcul du $PFD_{markov1oo2}$ en état stationnaire est égal à :

$$PFD_{markov1oo2} = \sum_{i=1}^{n} PFD_i$$

où PFD_i correspond aux indisponibilités des états S1', S1'', S2', S2''.

On obtient :

$$PFD_{1'} = \frac{2 \cdot \lambda_{dd}^2 \cdot MTTR^2}{4 \cdot \lambda_{dd} \cdot MTTR \ + 2 \cdot \lambda_{dd}^2 \cdot MTTR^2 + 2}$$

$$PFD_{2'} = \frac{2 \cdot \lambda_{du}^2 \cdot T_i^2}{6 \cdot \lambda_{du} \cdot T_i + 2 \cdot \lambda_{du}^2 \cdot T_i^2 + 2}$$

$$PFD_{1''} = \frac{2 \cdot \lambda_{dd} \cdot \lambda_{du} \cdot MTTR \cdot T_i}{2 \cdot \lambda_{dd} \cdot MTTR\left[\lambda_{du} \cdot T_i + 1\right] + 1}$$

$$PFD_{2''} = \frac{2 \cdot \lambda_{dd} \cdot \lambda_{du} \cdot MTTR \cdot T_i}{2 \cdot \lambda_{du} \cdot T_i\left[\lambda_{du} \cdot MTTR + 1\right] + 1}$$

Le tableau 1 montre par plusieurs applications numériques comment se comporte la $PFD_{Markov1oo2}$ en prenant un taux de défaillance dangereuse $\lambda_d = 1^E\text{-}06$.

On s'aperçoit que $PFD_{Markov1oo2} = PFD_{2'}$ si les hypothèses suivantes sont respectées :

- MDT=MTTR
- MTTR<<Ti
- DC < 95%

DC	MTTR (h)	Ti (h)	PFD2'	$PFD_{Markov1oo2}$	$\frac{PFD_{2'}}{PFD_{Markov1oo2}}$
0.6	8	8760	1.2^E-5	1.2^E-5	0.995
0.8	8	8760	3.1^E-6	3.1^E-6	0.986
0.95	8	8760	1.9^E-7	2.1^E-7	0.935
0.97	8	8760	6.9^E-8	7.7^E-8	0.894
0.99	8	8760	7.7^E-9	1.1^E-8	0.73
0.6	8	***4380***	3.1^E-6	3.1^E-6	0.989
0.6	8	***730***	8.5^E-8	9.1^E-8	0.938
0.6	8	***24***	9.2^E-11	3^E-10	0.308

Tableau 1. Comparaison des PFD en fonction du diagnostique de couverture (DC) et des temps de mission

On peut alors faire l'approximation :

$$PFD_{Markov1oo2} = \lambda_{du}^2 \cdot T_i^2$$

Notons alors que cette relation peut-être déterminée plus simplement et rapidement avec un calcul de défiabilité à partir de Blocs Diagrammes Fiabilité (RBD).

En effet, le calcul du PFD par RBD est égale à :

$$PFD_{RBD1oo2} = 1 - R(t)$$

et $R(t) = 1 - \left[\left(1 - e^{-\lambda_{du} \cdot T_i}\right) \cdot \left(1 - e^{-\lambda_{du} \cdot T_i}\right)\right]$

$$R(t) = 1 - \left[\lambda_{du} \cdot T_i \cdot \lambda_{du} \cdot T_i\right]$$

en faisant l'approximation par développement limité que $x = 1 - e^{-x}$ avec $x \langle\langle 0.01$

Au final, on obtient :

$$PFD_{RBD1oo2} \approx \lambda_{du}^2 \cdot T_i^2$$

La notion retenue dans la norme pour évaluer le niveau d'intégrité de la sécurité est la PFD_{avg}.

Pour un calcul d'indisponibilité classique, on a :

$$PFD_{avg1oo2} = \frac{1}{T_i} \int_0^{T_i} \lambda_{du}^2 \cdot t^2 \, dt$$

$$PFD_{avg1oo2} = \frac{\lambda_{du}^2 \cdot T_i^2}{3}$$

5 ANALYSE DES RESULTATS

La probabilité $PFD_{avg1oo2}$ obtenue par graphes de Markov est fonction du nombre de transitions et d'états. Le graphe tend alors à se compliquer et la visualisation de celui-ci n'est plus vraiment explicite.

De plus, pour déterminer la $PFD_{avg1oo2}$ par graphe de Markov, il est nécessaire d'adapter les taux de transition. Il est alors possible de tenir compte des taux de réparations différents des composants (identiques) présents dans l'architecture. Par exemple, pour l'architecture 1oo2, il faut introduire deux valeurs de μ_{pt} différentes, $\mu_{pt1} = \frac{2}{T_i}$ et $\mu_{pt2} = \frac{3}{T_i}$, pour obtenir la probabilité moyenne de défaillance.

Des études concernant ces différents aspects ont été menées [6-8].

Une des explications de cette remarque provient du fait que le processus n'est pas Markovien car, dans notre cas, les réparations ne sont pas effectuées en fonctionnement. La loi de réparation ne suit donc pas une loi constante.

Un autre problème de l'utilisation des graphes de Markov, pour les systèmes étudiés, repose sur le fait que les hypothèses de départ ne sont pas vérifiées. En effet, les défaillances sont bien aléatoires et suivent un processus de Markov, mais les réparations ne sont pas des processus de Markov puisqu'elles ne se produisent pas au hasard dans le temps.
Elles se produisent de manière déterministe juste après la défaillance, ou à intervalles fixes, dépendant de la politique d'entretien. Dans les deux cas, le taux de réparation est fonction inverse d'une durée et non pas d'une probabilité d'apparition. Les réparations ne sont pas des événements qui se produisent à un instant t mais des processus qui se produisent sur des périodes.

La conséquence de ces hypothèses de départ non vérifiées font que l'analyse par graphe de Markov n'est pas vraiment adaptée au processus de défaillances et de réparations tel que décrit en sécurité fonctionnelle, et les résultats obtenus en l'appliquant de cette manière sont approximatifs et pourtant très largement utilisés.
Une raison plausible de cette erreur de modélisation par graphe de Markov est que le taux de défaillance et le taux de réparation sont trompeusement des grandeurs semblables :

- Elles sont représentées par les lettres grecques (λ pour le taux de défaillance, μ pour le taux de réparation),
- Toutes les deux sont désignées par le terme "taux",
- Elles sont l'inverse d'un temps moyen.

6 CONCLUSION

L'utilisation de graphes de Markov est difficile car pour obtenir de bons résultats, il faut définir des graphes qui ne reflètent pas de manière simple la réalité physique. De plus, les calculs associés peuvent rapidement s'avérer lourds à utiliser. Ces graphes sont souvent mal utilisés pour le domaine de la sécurité fonctionnelle amenant à des résultats plus ou moins approximatifs.

Plusieurs techniques ont été évoquées pour quantifier des probabilités de défaillances dangereuses :

- L'utilisation des formules approchées traitée dans la 61508.
- L'utilisation des blocs diagrammes fiabilité.
- L'utilisation de graphes de Markov
- …..

Les limites d'utilisation des formules approchées de la norme 61508 résident dans le fait que seulement les configurations simples sont traitées avec des hypothèses bien précises à ne pas négliger.

Les blocs diagrammes fiabilité sont une technique simple et efficace, mais ne permettent pas de réaliser des études de fiabilité dynamique et de prendre en compte les différentes défaillances.

Les graphes de Markov sont des outils complexes, nécessitant de nombreuses approximations dans la modélisation.

Rappelons également que les données d'entrées sont bien souvent difficiles à obtenir et sont souvent des approximations (taux de défaillance, DC, SFF, mode commun…).

7 REFERENCES

[1] NF EN 61508, Sécurité fonctionnelle des systèmes électriques / électroniques / électroniques programmables relatifs à la sécurité, 2002.

[2] NF EN 61511, Sécurité fonctionnelle - Systèmes instrumentés de sécurité pour le secteur des industries de transformation, 2005.
[3] Reliability Prediction Method for Safety Instrumented Systems - PDS Method Handbook, 2003.
[4] ICDE project documentation OECD/NEA, 1995-1998
[5] Marshall, F. M., D. M. Rasmuson, and A. Mosleh, "Common Cause Failure Data Collection and Analysis System", Volume 1 - Overview, Nuclear Regulatory Commission, 1998.
[6] Hokstad P. and Corneliussen K., "Loss of safety assessment and the IEC 61508 standard," Reliability Engineering & System Safety, vol. 83, pp. 111-120, 2004.
[7] Gulland W G, "Methods of Determining Safety Integrity Level (SIL) Requirements - Pros and Cons", Proceedings of the Safety-Critical Systems Symposium, Birmingham (England), February 2004.
[8] Zhang T., Long W., Sato Y., "Availability of systems with self-diagnostic components—applying Markov model to IEC 61508-6", Reliability Engineering & System Safety, vol. 80, pp. 133-141, 2004.