Optimisation de la politique de tests d'épreuve des systèmes redondants relatifs à la sécurité

F. Brissaud, C Vinuesa, C. Folleau

Optimisation de la politique de tests d'épreuve des systèmes redondants relatifs à la sécurité

Optimising proof test policy of redundant safety-related systems

F. Brissaud
GRTgaz, RICE
florent.brissaud@grtgaz.com

C. Vinuesa, C. Folleau
SATODEV
25 rue Marcel Issartier
33700 Mérignac

Résumé

Cette étude propose une démarche d'optimisation de la politique de tests d'épreuve des systèmes redondants relatifs à la sécurité.

L'intégrité de sécurité (mesurée par la PFDavg) est évaluée par arbre de défaillance, en tenant compte des taux de défaillance, probabilités d'erreur humaine, causes communes de défaillances et d'erreurs humaines, temps de réparation, dates et durées des tests d'épreuve.

Sous certaines conditions raisonnables d'exploitation et de maintenance, il est ainsi possible d'améliorer l'intégrité de sécurité tout en maintenant ou en réduisant les coûts d'exploitation (par la réduction du nombre de tests d'épreuve et/ou une meilleure définition de leurs dates de réalisation).

Summary

This study proposes a framework for optimizing proof test policy of redundant safety-related systems.

The safety integrity (measured by the PFDavg) is assessed by fault tree analysis, taking into account: the failure rates, the probabilities of human errors, the common cause failures, the common cause of human errors, the repair times, the dates and duration of proof tests.

Under reasonable conditions of usage and maintenance, it is possible to increase safety integrity while decreasing operational costs (by reducing the number of proof tests and/or optimizing the dates of proof tests).

1. Introduction

Les systèmes relatifs à la sécurité sont conçus pour mettre en œuvre des fonctions de sécurité, qui permettent d'assurer ou maintenir l'état de sécurité d'équipements/systèmes/installations par rapport à des événements dangereux spécifiques. L'intégrité de sécurité est l'aptitude d'un tel système à mettre en œuvre les fonctions de sécurité requises, quand et tel que requis.

Cette communication porte sur les exigences relatives à l'intégrité de sécurité dite « du matériel » (i.e. relative aux défaillances aléatoires du matériel), telles que définies dans les normes de sécurité fonctionnelle CEI 61508 et CEI 61511 [CEI 61508 & CEI 61511]. De plus, les fonctions de sécurité considérées sont en mode « faible sollicitation », c'est-à-dire réalisées uniquement sur sollicitation et moins d'une fois par an. L'intégrité de sécurité est alors mesurée par la probabilité moyenne de défaillance dangereuse en cas de sollicitation (PFDavg). Celle-ci doit être inférieure à un « objectif chiffré de défaillance » (i.e. intégrité de sécurité cible), préalablement spécifié sur la base d'une analyse des dangers et des risques [F. Brissaud 2016]. En pratique, la PFDavg est calculée par l'indisponibilité moyenne « de sécurité » (i.e. vis-à-vis de la fonction de sécurité) du système relatif à la sécurité.

Les normes CEI 61508 et CEI 61511 définissent plusieurs critères à prendre en compte dans l'évaluation de la PFDavg, dont notamment : l'architecture du système, les taux de défaillance dangereuse, les causes communes de défaillance, les essais de diagnostic et tests d'épreuve, les temps de réparation et les erreurs humaines aléatoires. Les méthodes permettant cette évaluation incluent : les équations simplifiées, les diagrammes de fiabilité, les arbres de défaillance, les chaînes de Markov et les réseaux de Petri.

La politique de tests d'épreuve est une des premières mesures d'ajustement permettant d'obtenir une PFDavg inférieure à l'objectif. En effet, moyennant un certain coût d'exploitation (OPEX), ces tests permettent de révéler des pannes dangereuses non détectées en ligne (puis de les réparer et/ou de mettre en place des mesures compensatoires) et donc de réduire la PFDavg. Une optimisation de la politique de tests d'épreuve vise à améliorer l'intégrité de sécurité (par la réduction de la PFDavg) tout en maintenant ou en réduisant les coûts d'exploitation (par le maintien ou la réduction du nombre de tests d'épreuve). Dans cette communication, nous illustrerons un tel exemple d'optimisation à l'aide du cas d'étude ci-après.

2. Cas d'étude

2.1 Description du système

Le cas d'étude illustrant la démarche d'optimisation de la politique de tests d'épreuve est un système relatif à la sécurité constitué de deux canaux redondants (i.e. la disponibilité d'un seul canal est suffisant pour mettre en œuvre la fonction de sécurité). Chaque canal est disponible s'il n'est pas en panne dangereuse ni en cours de test d'épreuve. Une panne dangereuse peut être causée par une défaillance dangereuse (modélisée par un taux de défaillance constant) ou par une erreur humaine dangereuse (modélisée par une probabilité constante) provoquée par l'intervention d'un personnel de maintenance (test d'épreuve ou réparation). Une défaillance dangereuse ou une erreur humaine dangereuse peut se produire de façon indépendante, en impactant un seul canal du système, ou par une cause commune (modélisée par un facteur β), en impactant tous les canaux du système simultanément.

Cette étude se concentre uniquement sur les pannes non détectées en ligne. Ainsi, la panne dangereuse d'un canal reste présente jusqu'à la réalisation du prochain test d'épreuve du canal (permettant de révéler la panne) et la fin de la réparation induite (modélisée par un taux de réparation constant, défini par l'inverse du temps moyen de réparation). Les tests d'épreuves sont définis par des dates de réalisation et une durée fixe pendant laquelle le canal en cours de test est indisponible.

Dans la politique de tests d'épreuve de base, les deux canaux du système sont testés périodiquement, à la suite l'un de l'autre (i.e. séquentiellement) pour éviter une mise en indisponibilité totale du système durant les tests et ainsi réduire la PFDavg [Torres-Echeverría 2009, Liu 2013]. De plus, un « délai de sécurité » entre les deux tests permet de s'assurer que le second canal n'est pas testé pendant que le premier est en réparation. Chaque canal sera testé deux fois dans la période de référence utilisée pour le calcul de la PFDavg.

2.2 Paramètres de base

$\lambda=5{,}0\times10^{-6}$ /h Taux de défaillance dangereuse de chacun des canaux du système (les pannes n'étant pas détectées en ligne, ce taux est noté λ_{DU} dans les normes CEI 61508 et CEI 61511)

$\gamma=5{,}0\times10^{-3}$ Probabilité d'erreur humaine dangereuse applicable à chacun des canaux du système lorsqu'il est soumis à un test d'épreuve (la panne dangereuse induite n'est révélée que lors du prochain test d'épreuve)

$\beta_D=0{,}05$ Proportion des défaillances dangereuses impliquant la défaillance simultanée de tous les canaux du système (due à une cause commune)

$\beta_H=0{,}25$ Proportion des erreurs humaines dangereuses impliquant la défaillance simultanée de tous les canaux du système (due à une cause commune)

$MRT_{ind}=8$ h Temps moyen de réparation d'une panne dangereuse d'un canal due à une défaillance ou erreur humaine se produisant de façon indépendante

$MRT_{DCC}=8$ h Temps moyen de réparation des pannes dangereuses de tous les canaux dues à une défaillance ou erreur humaine de cause commune

$t_{1,C1}=1$ an Date de réalisation du 1er test d'épreuve du 1er canal du système

$t_{1,C2}=1$ an + D + 2 × MRT_{ind} Date de réalisation du 1er test d'épreuve du 2e canal du système (« D + 2 × MRT_{ind} » est le « délais de sécurité », cf. Paragraphe 2.1)

$t_{2,C1}=2$ ans Date de réalisation du 2e test d'épreuve du 1er canal du système

$t_{2,C2}=2$ ans + D + 2 × MRT_{ind} Date de réalisation du 2e test d'épreuve du 2e canal du système (« D + 2 × MRT_{ind} » est le « délais de sécurité », cf. Paragraphe 2.1)

D=4 h Durée d'indisponibilité applicable à un canal lorsqu'il est soumis à un test d'épreuve

$T_0=3$ ans Période de référence pour le calcul de la PFDavg du système

2.3 Modélisation de la politique de base

L'évaluation de la PFDavg est réalisée par arbre de défaillance, en utilisant le module Tree du logiciel GRIF. Cette approche est particulièrement adaptée pour les calculs de PFDavg des systèmes relatifs à la sécurité [F. Brissaud 2012].

La modélisation du cas d'étude avec la politique de tests d'épreuve de base, selon les caractéristiques et paramètres définis dans les sections précédentes, est présentée sur la Figure 1. Les résultats en termes d'indisponibilité au temps t du système relatif à la sécurité sont présentés sur la Figure 2. Les PFDavg obtenue (i.e. indisponibilité moyenne) est alors de $2{,}61\times10^{-3}$.

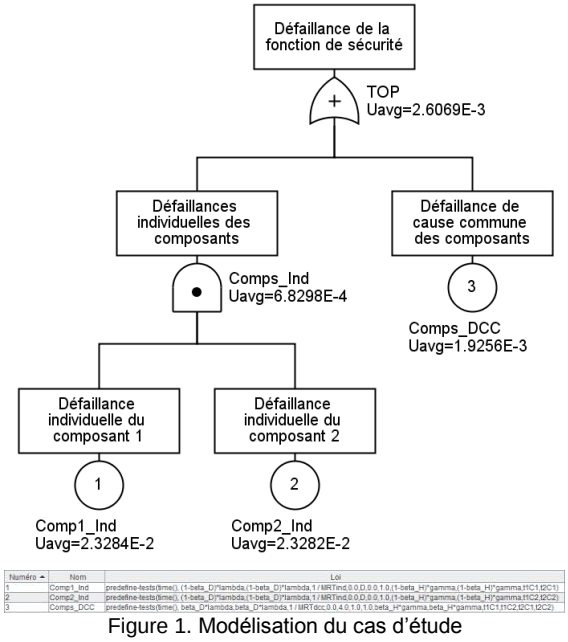

Figure 1. Modélisation du cas d'étude

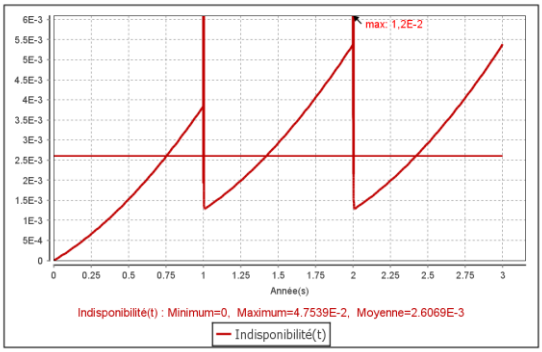

Figure 2. Résultats pour la politique de tests de base

3. Optimisation de la politique de tests

3.1 Un seul canal est testé à chaque intervention

Dans cette politique de tests d'épreuve alternative, un seul canal est testé à chaque intervention. C'est-à-dire qu'à la première occasion de test d'épreuve (à t=1 an), seul le premier canal est testé ; puis à la deuxième occasion de test d'épreuve (à t=2 ans), seul le deuxième canal est testé. Cette politique se traduit alors par les paramètres suivants (en comparaison aux paramètres de base) :

$t_{1,C1}$=1 an La date de réalisation du 1er test d'épreuve du 1er canal du système est inchangée

$t_{1,C2}$=2 ans La date de réalisation du 1er test d'épreuve du 2e canal du système est modifié

$t_{2,C1}$=Ø La date de réalisation du 2e test d'épreuve du 1er canal du système est supprimée

$t_{2,C2}$= Ø La date de réalisation du 2e test d'épreuve du 2e canal du système est supprimée

Cette politique de tests d'épreuve alternative vise à réduire les coûts d'exploitation (en réduisant le nombre total de tests d'épreuve), mais peut se faire au détriment de l'intégrité de sécurité. En effet, les pannes dangereuses sont alors moins souvent révélées que dans le cas de base. Les résultats en termes d'indisponibilité au temps t, avec cette politique de tests d'épreuve alternative, sont présentés sur la Figure 3. Les PFDavg obtenue (i.e. indisponibilité moyenne) est alors de $3{,}22\times10^{-3}$, soit une perte d'intégrité de sécurité d'environ 23%.

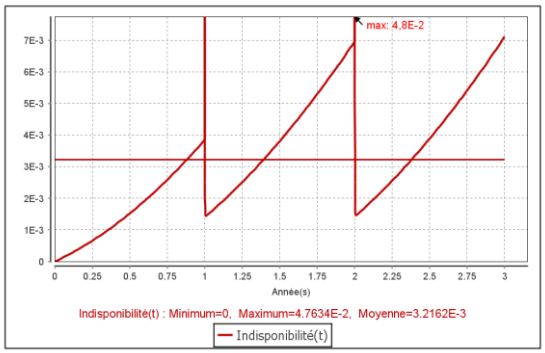

Figure 3. Résultats pour la politique de tests alternative

Cependant, en utilisant cette politique de tests d'épreuve alternative, un seul canal est concerné par l'intervention d'un personnel de maintenance à chacune de ses mobilisations. Ainsi, si la probabilité d'erreur humaine dangereuse (γ) applicable à chaque canal lorsqu'il est soumis à un test d'épreuve reste probablement identique, il est escompté que la proportion d'erreurs humaines dangereuses due à une cause commune (β_H) soit significativement réduite. La Figure 4 présente les résultats en termes de PFDavg, en fonction de la valeur de β_H. Il est ainsi montré que cette politique alternative n'implique pas de perte d'intégrité de sécurité dès lors qu'elle permet de faire baisser β_H sous les 5%. Pour β_H=1%, un gain d'intégrité de sécurité de plus de 5% est même envisageable. Ainsi, une politique de tests d'épreuve alternative où un seul canal est testé à chaque intervention peut, sous certaines conditions raisonnables d'exploitation et de maintenance, tout à la fois apporter un gain économique et un gain de sécurité.

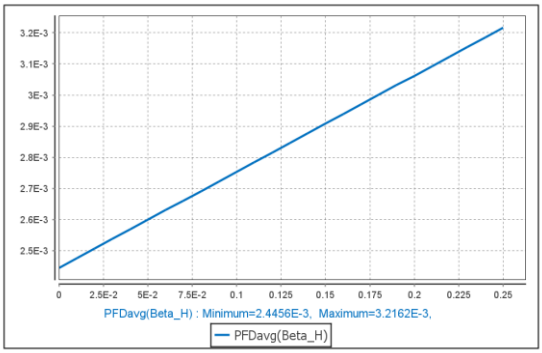

Figure 4. Résultats pour la politique de tests alternative, en fonction de β_H

3.2 Optimisation des dates de tests d'épreuve

Il a déjà été démontré qu'une optimisation des dates de tests d'épreuve permettait de réduire la PFDavg, dans le cas de systèmes redondants, lorsque tous les canaux sont testés simultanément et que les tests sont « partiels » (i.e. ne couvrent qu'une certaine proportion des pannes) [F. Brissaud 2012]. Dans le cas d'étude traité ici, les canaux de ne sont pas testés simultanément et les tests d'épreuve sont « complets ».

Partant de la politique de tests d'épreuve alternative (i.e. un seul canal est testé à chaque intervention), l'optimisation va donc consister à définir les dates de réalisation du test d'épreuve du premier canal ($t_{1,C1}$) et du deuxième canal ($t_{1,C2}$) qui minimisent la PFDavg. Le paramètre β_H sera fixé à 5% et les paramètres $t_{1,C1}$ et $t_{1,C2}$ seront définis symétriquement par rapport au milieu de la période de référence (T_0=3 ans) :

$t_{1,C1}$=1,5 an - α Date de réalisation du test d'épreuve du 1er canal du système

$t_{1,C2}$=1,5 an + α Date de réalisation du test d'épreuve du 2e canal du système

À noter que la configuration initiale de la politique de tests d'épreuve alternative était définie avec α=0,5 an (soit $t_{1,C1}$=1 an et $t_{1,C1}$=2 ans). Avec β_H=5%, la PFDavg était alors de $2{,}60\times10^{-3}$.

La Figure 5 présente les résultats en termes de PFDavg, en fonction de la valeur de α. Il est ainsi montré qu'un PFDavg minimal est atteint pour α=3360 h, soit $t_{1,C1}$=13,4 mois et $t_{1,C2}$=22,6 mois. Les résultats en termes d'indisponibilité au temps t, avec cette politique de tests d'épreuve alternative optimisée, sont présentés sur la Figure 6. La PFDavg obtenue (i.e. indisponibilité moyenne) est alors de $2{,}54\times10^{-3}$, soit un gain d'intégrité de sécurité d'environ 2% par rapport à la politique de tests d'épreuve alternative initiale. Bien que ce gain d'intégrité de sécurité soit faible, celui-ci se fait à coût économique constant puisqu'il implique uniquement de mieux définir les dates de réalisation des tests d'épreuve, sans en changer le nombre.

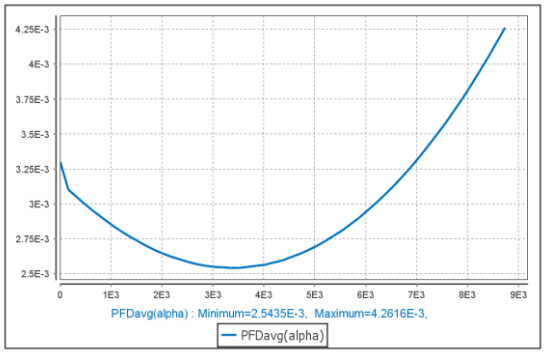

Figure 5. Résultats pour l'optimisation des dates de tests, en fonction de α

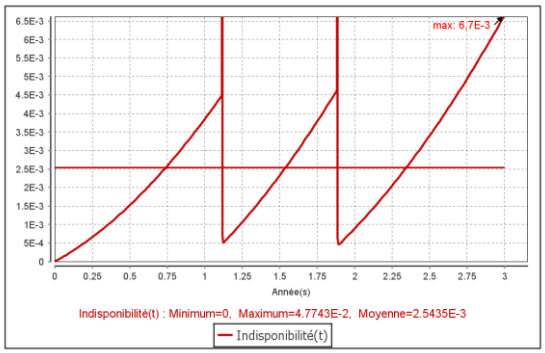

Figure 6. Résultats pour la politique de tests alternative optimisée

4. Conclusion

L'étude présentée dans cette communication propose une démarche d'optimisation de la politique de tests d'épreuve permettant, sous certaines conditions raisonnables d'exploitation et de maintenance, d'améliorer l'intégrité de sécurité (par la réduction de la PFDavg) tout en maintenant ou en réduisant les coûts d'exploitation (par la réduction du nombre de tests d'épreuve et/ou une meilleure définition de leurs dates de réalisation).

Les gains économiques et les gains de sécurité présentés dans le cas d'étude de cette communication sont bien sûr conditionnés par les caractéristiques du système et les paramètres utilisés. Cette étude ne permet donc pas de démontrer que des gains sont toujours permis mais, a minima, qu'ils sont possibles moyennant une analyse adaptée. Des bénéfices directs pour de nombreux exploitants industriels sont ainsi à espérer d'une évaluation et d'une optimisation appropriées de l'intégrité de sécurité de leurs systèmes relatifs à la sécurité.

Références

F. Brissaud, A. Barros, C. Bérenguer, "*Probability of failure on demand of safety systems: impact of partial test distribution*," *Proceedings of the Institution of Mechanical Engineers, Part O: Journal of Risk and Reliability*, vol. 226(4), p. 426-436, 2012.

F. Brissaud, L. F. Oliveira, "*Sécurité fonctionnelle : accorder la complexité des méthodes avec la complexité des systèmes*," *Actes du 18ème Congrès de Maîtrise des Risques et de Sûreté de Fonctionnement*, Tours, France,16-18 octobre 2012.

F. Brissaud, D. Turcinovic, "*Sécurité fonctionnelle des systèmes relatifs à la sécurité : 10 erreurs à éviter*," *Actes du 20ème Congrès de Maîtrise des Risques et de Sûreté de Fonctionnement*, Saint-Malo, France,10-13 octobre 2016.

CEI 61508, *Sécurité fonctionnelle des systèmes électriques/électroniques/électroniques programmables relatifs à la sécurité*, 2e édition. Genève : Commission Électrotechnique Internationale, 2010.

CEI 61511, *Sécurité fonctionnelle – Systèmes instrumentés de sécurité pour le secteur des industries de transformation*, 2e édition. Genève : Commission Électrotechnique Internationale, 2016.

Y. Liu, M. Rausand, "*Reliability effects of test strategies on safety-instrumented systems in different demand modes*," *Reliability Engineering & System Safety*, vol. 119, p. 235-243, 2013.

A. C. Torres-Echeverría, S. Martorell, H. A. Thompson, "*Modelling and optimization of proof testing policies for safety instrumented systems*," *Reliability Engineering and System Safety*, vol. 94(4), p. 838-854, 2009.