Barrières de sécurité et tests de révision

Dominique Charpentier, Florent Brissaud

Barrières de Sécurité & Tests de Révision


D. Charpentier/F. Brissaud

Les Systèmes Instrumentés de Sécurité (SIS) constitués de capteurs (mesure de pression, détection de gaz, etc.), d'unités de traitement (automates) et d'actionneurs (vannes) jouent un rôle clef dans la prévention des risques industriels, en tant que barrières de sécurité. L'objectif d'un SIS est de maintenir un état sûr d'un process industriel par rapport à un événement dangereux (rejet de substance, incendie, explosion, etc.). L'enjeu est de connaître la disponibilité du SIS qui est la capacité à accomplir une ou plusieurs fonctions de sécurité à un instant donné (lorsqu'elles sont sollicitées), et dans des conditions données (leurs environnements). Les recherches de l'INERIS sur l'évaluation des SIS ont consisté à quantifier la disponibilité et la probabilité de défaillance à la sollicitation sur les architectures complexes et d'optimiser ainsi les périodicités de tests des SIS.

Ces travaux s'appuient sur les méthodes d'évaluation de la norme CEI 61508 [3] et le développement de modèles mathématiques pour des architectures redondantes complexes. La norme CEI 61508 propose des méthodes basées sur les diagrammes de fiabilité, arbres de défaillance, chaînes de Markov. L'approche de l'INERIS est différente : une approche analytique est proposée afin de disposer d'une expression paramétrique de la probabilité de défaillance dangereuse moyenne et de pouvoir ainsi faire une analyse paramétrique et d'optimiser les tests.

EXPRESSION DES PROBABILITÉS DE DÉFAILLANCE DANGEREUSE NON DÉTECTÉE

La politique de maintenance et de contrôle des systèmes de sécurité s'appuie sur la prévision du comportement de ces systèmes lors d'une sollicitation et sur la quantification de leur disponibilité et de leurs probabilités de défaillance. Ceci afin de s'assurer de l'adéquation entre les risques des installations et les moyens de tests mis en œuvre. En déterminant les probabilités de défaillance à la sollicitation de SIS soumis à des tests de révision partiels et complets*, il est possible de quantifier le niveau de sécurité de ces systèmes et d'en déduire un plan de tests afin de maintenir ce niveau. Le plan de test peut être optimisé en adaptant la durée entre tests (partiels et complets) afin de maintenir constant le niveau de sécurité.

L'étude porte sur les systèmes complexes avec une architecture redondante de type MooN, c'est-à-dire que le bon fonctionnement de M composants parmi N suffit à accomplir la fonction de sécurité. Les expressions analytiques des probabilités de défaillances (formules exactes ou approchées) sont simples à utiliser pour un exploitant d'une installation industrielle.

Il faut toutefois se méfier des évaluations de probabilité de défaillances de ces systèmes instrumentés qui s'appuient sur de nombreuses hypothèses qui sont trop souvent oubliées par les utilisateurs de ces formules comme par exemple :

RÉFÉRENCES

[1] Brissaud F., Baros A., Bérenguer C. Probability of Failure of Safety-Critical Systems Subject to Partial Tests, dans les actes de la conférence RAMS 2010, San Jose, USA, 2010.

[2] Bukowski J. V. A comparison of techniques for computing PFD average, dans les actes de la conférence RAMS 2005, Alexandria VA, USA, 2000.

[3] IEC, IEC 61508 Functional safety of electrical/electronic/programmable electronic safety-related systems, Genève : International Electrotechnical Commission, 2002.

[4] Rausand M., Høyland A., System reliability theory; models, statistical methods, and applications, 2nd edition, New York : Wiley, 2002.

[5] Rouvroye J. L., van den Bliek E. G. Comparing safety analysis techniques, Reliability Engineering & System Safety, vol. 75, p. 289-294, 2002.

[6] Rouvroye J. L., Wiegerinck J. A. Minimizing costs while meeting safety requirements: Modeling deterministic (imperfect) staggered tests using standard Markov models for SIL calculations, ISA transaction, vol. 45, p. 611-621, 2006.

• les N composants du système sont en service et opérationnels au démarrage ;
• les N composants du système sont testés simultanément lors de chaque test ;
• les défaillances détectées au cours d'un test partiel ou complet sont réparées immédiatement et, durant ce temps, des mesures sont prises afin de maintenir l'installation dans un état sûr.

Des travaux complémentaires permettraient aisément de fournir des outils de maîtrise des risques qui conviendraient à un plus large champ d'applications, comme par exemple :
• des systèmes constitués d'éléments hétérogènes (éléments dont les taux de défaillance ne sont pas tous identiques),
• des systèmes sujets à des causes communes de défaillance,
• des systèmes vieillissants (dont certains taux de défaillance ne sont pas constants).

Ces évolutions peuvent facilement être résolues par des raisonnements similaires à ceux étudiés mais rendent souvent les expressions mathématiques plus difficiles à manipuler. Il conviendrait aussi d'exprimer formellement les intervalles de confiance de ces estimations.

APPLICATION À UN SYSTÈME DE PRÉVENTION D'INCENDIE SUR UNE INSTALLATION INDUSTRIELLE

Le modèle est appliqué à un système de prévention d'incendie par inertage à l'azote de l'atmosphère. Afin d'empêcher les départs et la propagation d'incendie, tout en maintenant l'atmosphère respirable, la teneur en oxygène doit être maintenue autour de 15 %. L'entrepôt considéré comprend 6 capteurs d'oxygène. Comme l'azote introduit se répartit rapidement et de façon homogène, les capteurs sont supposés redondants. L'architecture du système est de type 2oo6 (le bon fonctionnement de 2 capteurs sur 6 suffit à accomplir la fonction de sécurité).

Le constructeur prescrit un test annuel des capteurs, ces tests sont donc supposés complets. Des inspections visuelles sont conseillées, ce sont des tests partiels qui ne permettent pas de détecter certaines défaillances visibles de l'extérieur. L'ensemble des 6 capteurs est testé à chaque test selon une politique qui consiste à effectuer les tests partiels périodiquement tous les 3 mois et un test complet annuellement.

L'évaluation a consisté à :
• utiliser les observations faites par un utilisateur sur une période donnée afin d'estimer le taux de défaillance des capteurs ;
• évaluer l'efficacité des tests partiels ;
• puis en déduire les probabilités de défaillance à la sollicitation du système.

Dans un second temps, une optimisation de la répartition des tests partiels est proposée afin de réduire la probabilité de défaillance dangereuse.

DÉFINITIONS

*** Les tests de révision *complets***
font référence aux essais périodiques permettant de détecter toutes les défaillances d'un SIS : si une défaillance s'est produite depuis la dernière révision, celle-ci peut être réparée et le SIS peut retrouver un état comparable à l'état initial.

Les tests de révision *partiels*
ne permettent, quant à eux, que de détecter certaines défaillances, laissant les autres non détectées jusqu'au prochain test complet. Des inspections visuelles, des contrôles incomplets et des essais imparfaits sont des exemples de tests partiels.

FIGURE 1
PROBABILITÉ MOYENNE DE DÉFAILLANCE DANGEREUSE (PFDavg) ET INDISPONIBILITÉ (U(t)) POUR UNE POLITIQUE DE TESTS PÉRIODIQUES

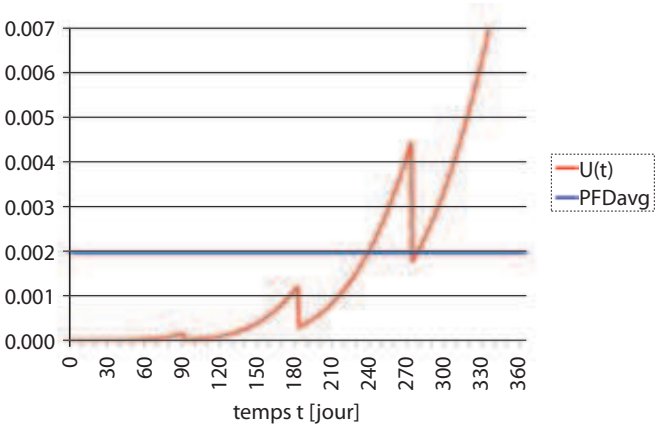
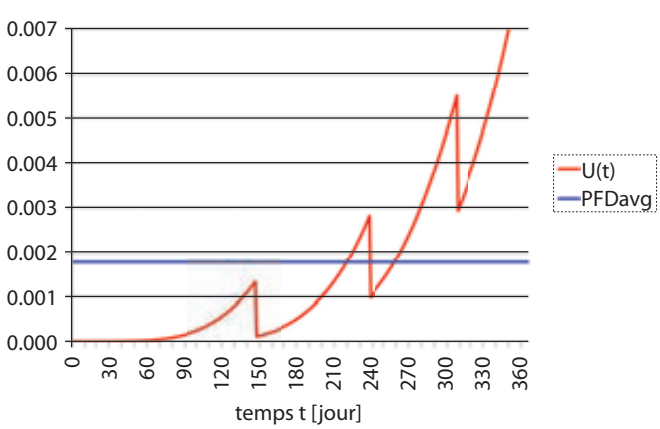


FIGURE 2
PROBABILITÉ MOYENNE DE DÉFAILLANCE DANGEREUSE (PFDavg) ET INDISPONIBILITÉ (U(t)) POUR UNE POLITIQUE DE TESTS OPTIMISÉE



ESTIMATIONS DE LA DISPONIBILITÉ ET DE LA PROBABILITÉ DE DÉFAILLANCE DANGEREUSE NON DÉTECTÉE

Quatre entrepôts, comprenant 6 capteurs chacun ont été observés sur une durée de 4 ans. Ces données et la modélisation du système permettent d'en déduire le taux de défaillance des capteurs de $6{,}1 \cdot 10^{-5}$/heure, et une estimation de l'efficacité des tests partiels de 0,42.
L'estimation de la probabilité de défaillance dangereuse non détectée du système avec une politique de tests périodiques telle que le préconise le constructeur est évaluée à $2{,}06 \cdot 10^{-3}$ (figure 1).

OPTIMISATION DE LA RÉPARTITION DES TESTS PARTIELS

Une optimisation de la politique de tests consiste à répartir les instants d'occurrence des tests partiels de façon à réduire la probabilité de défaillance dangereuse non détectée. La résolution du problème d'optimisation conduit alors aux occurrences suivantes : le premier test à 4,8 mois puis 3 mois, 2,3 mois et 1,9 mois. La probabilité de défaillance dangereuse non détectée est de $1{,}87 \cdot 10^{-3}$, soit une réduction d'environ 10 % par rapport à la politique de tests classique. De plus, l'indisponibilité maximale du système sur l'intervalle de test complet est réduite de plus de 25 % (figure 2).

CONCLUSION

La modélisation d'un système instrumenté afin d'évaluer la disponibilité et les probabilités de défaillance du système en tenant compte des tests (partiels et complets) permet de disposer d'un outil relativement simple pour l'optimisation du niveau de sécurité et son maintien dans le temps. Ces travaux ont porté sur les systèmes redondants et homogènes constitué de N voies identiques.
L'optimisation de la répartition et de l'occurrence des tests permet d'améliorer notablement les critères de sécurité. Sur le cas d'application présenté, une réduction de 10 % de la probabilité de défaillance dangereuse non détectée et de 25 % de l'indisponibilité maximale est atteinte par rapport à une politique de tests périodiques. Il est ainsi possible d'optimiser les performances du système, sans surcoût associé uniquement en analysant le système et en définissant les durées adéquates entre chaque test.
Pour poursuivre sur l'évaluation des SIS, les recherches s'orientent vers la prise en compte du vieillissement des systèmes instrumentés dans l'optimisation des durées entre chaque test.

ABSTRACT

Safety barriers take an important part of industrial risk management. Even if these systems are not triggered frequently, when an initiating event occurs (overpressure, overflow, etc.), they aim at preventing undesired events on people, environment, and goods. Proof tests have therefore to be performed in order to check the functional state of the safety barriers and, if required, to perform the appropriate maintenance actions. Dependability criteria have then to be assessed by a practical model.
A set of general formulas is proposed for the probability of failure on demand (PFD) assessment of systems subject to partial and full tests. Partial tests (e.g. visual inspections, imperfect testing) may detect only some failures, whereas owing to a full test, the system is restored to an as good as new condition. Following the proposed approach, and according to an example, performance estimations of the system and test policies are presented, by using the feedback from previous tests. An optimization of the partial test distribution is also proposed, which allows reducing the average probability of system failure on demand.