Modélisation des systèmes instrumentés de sécurité

Dominique Charpentier, Jean-Michel Dranguet

SYSTÈMES INDUSTRIELS COMPLEXES

Modélisation des systèmes instrumentés de sécurité

Dominique Charpentier, Jean-Michel Dranguet

1

Centrale électrique de General Electric (Kemalpasa, Turquie).

La qualification des fonctions de sécurité nécessite de modéliser les systèmes instrumentés de sécurité pour calculer les probabilités de défaillance dangereuse. L'INERIS mène des recherches sur cette thématique en partenariat avec des industriels et oriente ses travaux vers la fiabilité dynamique des systèmes.
L'étude des dangers d'une installation industrielle conduit à déterminer les fonctions importantes pour la sécurité et à déterminer le niveau de sécurité requis pour ces fonctions. Le Laboratoire d'évaluation des équipements électriques de l'INERIS s'assure ensuite que les solutions techniques retenues satisfont aux exigences requises.
Ces fonctions sont de plus en plus fréquemment réalisées par des systèmes instrumentés de sécurité constitués de capteurs, d'unités logiques de traitement et d'actionneurs agissant sur l'installation. Ces systèmes ont beaucoup évolué au cours des deux dernières décennies, passant de technologies simples et robustes dont l'évaluation était aisée à des technologies plus performantes, paramétrables, assemblées en systèmes complexes tant par l'architecture que par les modes de fonctionnement.

MODÉLISER LES SYSTÈMES UTILISÉS DANS LES INSTALLATIONS À RISQUE

L'INERIS a engagé une recherche visant à modéliser les systèmes utilisés dans les installations à risque, en partenariat avec des industriels, concepteurs d'équipements avec Schneider Electric et concepteurs de centrales électriques avec General Electric. Ces recherches partenariales ont consisté à analyser le comportement et la fiabilité de boucles de sécurité en déterminant les différents états du système associé aux nombreux modes de fonctionnement ainsi qu'aux événements redoutés correspondants. Par exemple, il est nécessaire de déterminer les états amenant le système à un état sûr (l'arrêt pour certains systèmes, la continuité de service pour d'autres). Ces principes fondamentaux de la sûreté de fonctionnement ont été mis en œuvre pour déterminer les probabilités de défaillance dangereuse de ces systèmes en considérant les différents modes de fonctionnement.
Les problèmes relatifs à la nature des probabilités calculées et aux outils mathématiques associés ont été identifiés et des solutions ont été apportées pour les résoudre. Certains systèmes n'interviennent qu'en secours par rapport à d'autres dispositifs. Ils ne sont utilisés que sur sollicitation externe ou lors de tests périodiques. Le mode de fonctionnement est alors à faible sollicitation, contrairement au mode continu où la fonction de sécurité est toujours sollicitée. Un système est donc caractérisé par la probabilité de défaillance dangereuse pour une utilisation à la sollicitation et par la probabilité de défaillance dangereuse par unité de temps pour un fonctionnement continu.
Les outils mathématiques comme les arbres de défaillances, les blocs-diagrammes de fiabilité, adaptés à une analyse statique ou les graphes de « Markov » adaptés à une étude de fiabilité dynamique sont déterminants dans la modélisation et influencent considérablement le résultat.

RÉFÉRENCES

[1] Gruffaz F., Signoret J.P., Charpentier D. (2006). "SIL rated protection relays meet IEC 61508 safety requirements without lowering process availability". *Automation Technology in Practice International*, vol. 4, n° 1.
[2] Lanternier B., Charpentier D., Lyonnet P. (2006). "Failure rate model for spring loaded relief valves". GUEDES SOARES C., ZIO E. (Eds.). Safety and reliability in managing risk: proceedings of the ESREL conference, 18-22 September 2006, Estoril, Portugal. Leiden, The Netherlands: Taylor & Francis, 2006, vol. 2.
[3] Lanternier B., Dranguet J.M., Charpentier D. (2006). « Limites d'utilisation des normes EN 61508 - EN 61511. Retour d'expérience d'un organisme de certification ». Colloque de maîtrise des risques et sûreté de fonctionnement - Risques et performances, 10-12 octobre 2006, Lille, France.

DÉTERMINER LES LIMITES D'UTILISATION DE CES MÉTHODES

Contrairement à la pratique courante consistant à fournir un résultat en termes de probabilité sans spécifier les outils de modélisation et les hypothèses associées, l'INERIS poursuit des recherches afin de déterminer les limites d'utilisation de ces méthodes.
Parmi les paramètres déterminants dans la qualité d'un résultat, il est nécessaire d'analyser la couverture des tests lors des inspections périodiques et la prise en compte de la réparabilité partielle de ces matériels.
Pour un système redondant, le tableau ci-dessous montre l'influence du taux de couverture des tests (DC), du temps de réparation (MTTR) et de la période entre tests (TI) sur le calcul des probabilités. Plus on parvient à détecter les défaillances dangereuses (DC élevé), plus il est important de tenir compte de l'aptitude à effectuer les réparations ; la probabilité calculée de défaillance du système dépend ainsi de l'organisation industrielle (stockage, rapidité d'intervention...) et il est nécessaire de vérifier cette hypothèse avant de réaliser une évaluation probabiliste.
L'écart entre P1 et P2 s'explique par la nature des réparations qui ne suivent pas une distribution stochastique (ne se produisent pas au hasard dans le temps) car la réparation n'a lieu qu'après test périodique et identification de la défaillance du système.
Dans ce cas, une analyse par graphe de « Markov » n'est valable qu'à condition d'éviter les confusions entre le temps de réparation et le temps entre les tests périodiques.

LA MODÉLISATION DES SYSTÈMES COMPLEXES

Les travaux de recherche de l'INERIS s'orientent donc vers la modélisation de systèmes complexes afin de prendre en compte les facteurs d'influence des modes de fonctionnement, du type de maintenance, dans le but de déterminer les limites d'utilisation des outils de la sûreté de fonctionnement et de retenir les méthodes les mieux adaptées. Ces travaux sont valorisés sur des applications industrielles dans le cadre de recherches partenariales.
Ainsi, l'INERIS a étudié les systèmes instrumentés de la centrale électrique de General Electric à Kemalpasa, en Turquie. La conformité à la norme CEI/EN 61511, qui spécifie les exigences techniques de conception, de construction et de validation du niveau de sécurité de ces systèmes instrumentés, a été évaluée. Les exigences de ce référentiel portent principalement sur la gestion de la sécurité fonctionnelle au travers des deux thèmes suivants :
- le cycle de vie de sécurité, de la conception jusqu'à la fin de vie de l'installation ;
- l'évaluation qualitative et quantitative d'un système en déterminant les probabilités de défaillance dangereuse lors d'un dysfonctionnement.

MODÉLISATION D'UN SYSTÈME REDONDANT EN 1002

DC	MTTR (h)	Ti (h)	P1*	P2*	P1/P2
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
0,99	**8**	**8760**	**7,7 e^{-9}**	**1,1 e^{-8}**	**0,73**

* P1 probabilité de défaillance dangereuse sans tenir compte des réparations du système
* P2 probabilité de défaillance dangereuse en tenant compte des réparations du système

SUMMARY

MODELLING OF SAFETY INSTRUMENTED SYSTEMS

Safety Instrumented Systems (SIS) have to be assessed in order to determine the probability of dangerous failure. These SIS are important safety devices in high-risk level process industries and need to be highly reliable. Preventive maintenance and periodic tests are tools for maintaining such SIS at a low probability of failure.
The assessment of SIS incorporates modelling and calculation. The research identifies modelling topics and the limits of the mathematical methods used. We have analysed the influence of test coverage and repair capability to calculate the probability of dangerous failure.
We have shown that models based on Markov graphs can only be used if confusion is avoided between the repair time and the interval between periodic tests. We have also demonstrated that the reliability and safety of a redundant system constituted of two detectors, two programmable logic controllers (PLC) and two actuators depend on the desynchronisation of periodic tests for each channel. The optimisation of safety levels is a function of the interval between tests and the desynchronisation between periodic tests.
INERIS carries out research in partnership with industry (manufacturers and users) and develops assessment of dynamic reliability. The aim is to define methods for analysing complex systems composed of sensor networks, communication field bus and PLC.