IRSN
INSTITUT
DE RADIOPROTECTION
ET DE SÛRETÉ NUCLÉAIRE

02 Novembre 2009

Analyse de sûreté des systèmes informatisés : l'approche de l'IRSN

1 ROLE DES SYSTEMES INFORMATISES DANS LES CENTRALES NUCLEAIRES

Les centrales nucléaires sont de plus en plus pilotées et surveillées au moyen de systèmes informatisés. Le plus important d'entre eux du point de vue de la sûreté, le Système de Protection, ne participe pas au pilotage mais observe en permanence des dizaines de paramètres physiques (températures, pressions, flux neutroniques, etc.) qui lui permettent de détecter en temps réel une éventuelle dérive pouvant entrainer un risque d'incident ou d'accident.

En cas de besoin le Système de Protection arrête automatiquement le réacteur en laissant chuter gravitairement des absorbants neutroniques qui étouffent la réaction en chaîne, et peut déclencher d'autres actions de sûreté telles que le démarrage du système d'injection de sécurité d'eau dans le circuit primaire pour assurer le refroidissement du cœur du réacteur lors d'une situation incidentelle ou accidentelle entraînant une fuite de ce circuit.

Le Système de Protection est classé au plus haut niveau de sûreté (il est dit « critique ») ; à ce titre, il est redevable du plus haut niveau d'exigences techniques.

2 PRINCIPES D'OBTENTION D'UN NIVEAU SATISFAISANT DE SURETE

L'obtention d'un niveau satisfaisant de sûreté nécessite de pallier les différents types de défaillances qui pourraient affecter le Système de Protection.

2.1 DEFAILLANCES ALEATOIRES

Les composants électroniques peuvent défaillir de manière aléatoire, par exemple à cause de leur dégradation dans le temps. Une telle défaillance est efficacement combattue au niveau du système par la « redondance » matérielle : chaque Système de Protection informatisé utilisé en France comporte quatre « divisions », ou ensembles identiques de calculateurs, qui élaborent par vote[1] un ordre de commande global pour chacun des dispositifs mécaniques de sûreté tels que les pompes du système d'injection d'eau de sécurité, dispositifs eux-mêmes redondants.

De plus, ces divisions « redondantes » du Système de Protection sont installées dans des zones géographiques séparées pour réduire les risques de défaillance de mode commun par des agressions telles que l'incendie ou l'inondation.

Dans le cadre des expertises qu'il mène à la demande de l'ASN, l'IRSN s'assure par une analyse détaillée de l'architecture et des circuits de vote qu'aucune défaillance unique ne peut bloquer une fonction de

[1] L'action de sûreté est typiquement déclenchée dès que deux des quatre divisions la demandent, ce qui permet de tolérer par exemple une défaillance dans l'une d'elles et un arrêt pour maintenance d'une autre.

sûreté et que la fiabilité matérielle des calculateurs, évaluée par des méthodes statistiques, est suffisante pour éviter l'accumulation de pannes dans les divisions « redondantes » entre deux contrôles périodiques.

2.2 ERREURS DE CONCEPTION

Une erreur dans le logiciel des calculateurs pourrait fausser le traitement de certains cas, affecter toutes les divisions « redondantes » identiques et bloquer ainsi une fonction de sûreté. Les approches probabilistes ne sont pas applicables à ce problème déterministe, qui ne remplit pas les hypothèses indispensables à l'application des théorèmes statistiques. Les méthodes basées sur un tirage aléatoire des tests butent sur l'impossibilité de pondérer tous les cas d'évolution combinée des signaux d'entrée avec la précision et la rigueur nécessaires pour démontrer une très haute fiabilité.

Les défaillances dues à des erreurs de conception doivent donc être combattues par des moyens déterministes. Pour cela trois familles de dispositions sont mises en œuvre ; elles sont présentées ci-après.

3 EVITER D'INTRODUIRE DES ERREURS DANS LE LOGICIEL

Les fonctions du Système de Protection sont simples, donc leur réalisation est peu sujette à erreur : la spécification d'une fonction de protection dépasse rarement une vingtaine d'opérations élémentaires tels que des sommes, des comparaisons à des seuils ou des mémorisations.

Des exigences très strictes[2] encadrent le développement des logiciels « critiques » : chaque étape est réalisée selon un plan défini à l'avance précisant les objectifs, les entrées et les sorties, de telle sorte que chaque décision de conception soit justifiée et documentée, et puisse ainsi être analysée par l'IRSN dans le cadre évoqué ci-dessus.

Un logiciel « critique » doit être déterministe par conception, ce qui réduit considérablement la latitude laissée aux développeurs qui doivent prouver que dans n'importe quel cas le programme se déroulera selon le schéma et dans les limites de temps prévus.

Une telle exigence exclut l'utilisation de composants logiciels « courants », sans même parler des systèmes d'exploitation usuels. Elle a pour but, outre de forcer la maîtrise de la programmation par le concepteur, de garantir la reproductibilité des tests ce qui est indispensable pour la vérification.

D'autres exigences concernant les structures de données et de contrôle des programmes ont pour objectif de favoriser leur simplicité et de faciliter leur compréhension, de favoriser la capacité de réalisation des tests, d'éviter les problèmes de synchronisation, etc.

Lors de ses travaux d'analyse critique, l'IRSN examine les choix de conception et de programmation, ainsi que les justifications destinées à démontrer que les programmes s'exécuteront conformément à leurs exigences de sûreté dans tous les cas. Cela peut amener le concepteur à éviter les choix qui demanderaient un effort de démonstration trop important.

---

[2] Exprimées par exemple dans les Règles Fondamentales de Sûreté (RFS II.4.1.a) ou dans les normes de la Commission Electrotechnique Internationale (CEI 60880).

4 ELIMINER LES ERREURS

Des dispositions strictes sont prises pour éliminer les éventuelles erreurs du logiciel, même si tout a été fait pour les éviter.

Un plan établi en préalable au développement fixe les objectifs et les moyens de la vérification pour chaque étape de la conception, ainsi que les critères d'acceptation permettant de passer à l'étape suivante. Par exemple, les valeurs d'entrée des tests et les valeurs attendues en sortie doivent être prédéfinies et la « couverture », c'est-à-dire l'étendue des cas sollicités, doit être suffisante.

Les tests doivent couvrir toutes les fonctions du système de protection dans tous ses modes d'opération, solliciter tous les signaux qui peuvent être élaborés par le procédé physique dans toute leur gamme ainsi que les commandes provenant des opérateurs dans toutes les combinaisons significatives, solliciter toutes les combinaisons de votes, etc. De plus, la couverture des éléments structurels du logiciel - tels que les instructions ou les branchements - lors des tests doit également être vérifiée.

Le plan mentionné ci-dessus doit être établi par des personnes indépendantes de l'équipe de développement du logiciel, de façon à éviter un même oubli ou une même erreur dans celui-ci et dans sa vérification. Cette indépendance constitue un moyen essentiel d'élimination des erreurs.

Sur la base de la documentation de conception, l'IRSN examine les vérifications effectuées, ce qui constitue un troisième regard sur le logiciel. L'IRSN analyse de façon contradictoire l'étendue des vérifications, en particulier des tests qui sont un moyen de vérification essentiel.

Comme il est impossible de tester tous les cas d'exécution du logiciel à cause de leur grand nombre, ils doivent être regroupés en cas équivalents du point de vue du comportement du programme et chaque groupe doit être testé. Mais il n'existe pas de critère universel défini pour un tel regroupement, qui doit être effectué en tenant compte de l'architecture du logiciel et des détails de la programmation. C'est pourquoi l'IRSN analyse le logiciel pour donner un avis pertinent sur l'étendue des tests effectués.

Pour des raisons mathématiques, la plupart des propriétés importantes d'un logiciel ne peuvent pas être vérifiées automatiquement et un outil d'analyse universel « presse-bouton » ne peut pas exister. L'IRSN utilise donc des outils manuels ou semi-automatiques commerciaux, lorsqu'ils existent, ou développés en collaboration avec des organismes de recherche pour pousser l'examen plus loin : analyse de la couverture des tests, réduction de programme conservant tous les éléments intervenant dans le calcul d'une sortie donnée, analyse de la précision numérique ou encore exécution des codes binaires dans un environnement simulé.

Cette analyse contradictoire de la vérification du logiciel peut amener les concepteurs à compléter leurs plans de vérification, voire à simplifier leurs logiciels pour faciliter la réalisation d'un tel complément.

5 TOLERER LES CONSEQUENCES DES ERREURS RESIDUELLES

Le concept de « défense en profondeur » conduit à mettre en place des dispositions permettant de tolérer les conséquences des erreurs qui auraient été introduites en dépit de toutes les précautions prises et non éliminées malgré les vérifications réalisées de façon indépendante.

Pour ce faire, le logiciel inclut des fonctions d'auto-surveillance : son bon comportement est contrôlé pendant son exécution, par exemple en vérifiant le passage par des chemins donnés ou en s'assurant du caractère plausible des entrées, des sorties et des résultats intermédiaires. Par ailleurs, les fonctions du matériel sont testées en permanence (contenu de la mémoire abritant le programme, bon fonctionnement de la mémoire de données et des instructions du microprocesseur, etc.).

En cas de détection d'une anomalie, le Système de Protection émet un message facilitant le diagnostic et ses sorties prennent des valeurs « de repli » spécifiées correspondant à une position sûre de la centrale (par exemple arrêt automatique du réacteur).

L'IRSN analyse l'étendue de cette auto-surveillance, tout en s'assurant qu'elle n'introduit pas de complexité dégradant sensiblement les fonctions principales et que les positions de repli sont correctes dans tous les cas.

6 AU-DELA DU LOGICIEL

L'ensemble des dispositions rapidement présentées ci-dessus - qui relèvent de l'exploitant nucléaire et de ses constructeurs -, complétées par l'analyse technique indépendante menée par l'IRSN, permettent d'avoir une bonne assurance de la capacité du logiciel concerné à répondre aux exigences de sûreté qui lui sont applicables. Malgré ceci, deux dispositions supplémentaires sont mises en œuvre pour améliorer encore la défense en profondeur :

1) la diversification fonctionnelle : chaque incident ou accident est détecté par le Système de Protection sur la base d'un « signal », c'est-à-dire la valeur indiquée par un capteur ou le résultat d'un calcul combinant les données de plusieurs capteurs ; le Système de Protection utilise de plus un deuxième « signal » détectant le même incident sur la base d'autres paramètres physiques de façon à déclencher les actions de sûreté nécessaires en cas de défaillance de la fonction associée au premier « signal » ; cette deuxième fonction est implantée dans d'autres calculateur, du Système de Protection, physiquement différents et indépendants de ceux assurant la première.

L'IRSN analyse la pertinence de cette diversification, qui nécessite la garantie que les événements externes au Système de Protection – par exemple les évolutions du procédé physique, ou des dates calendaires données - ne peuvent pas perturber le fonctionnement des calculateurs, et donc ne peuvent pas faire défaillir simultanément les calculateurs abritant les fonctions diversifiées. L'IRSN analyse donc les interactions des calculateurs avec leur environnement et le déroulement de l'exécution des programmes qu'ils abritent, pour vérifier l'absence de perturbation par les événements externes.

2) un système dénommé ATWS, différent de par ses calculateurs, ses logiciels, ses méthodes de développement, ses spécifications fonctionnelles et ses développeurs, abrite des fonctions de protection diversifiées par rapport à celles du Système de Protection.

Cette disposition est analysée par l'IRSN au titre de l'examen de l'architecture globale du contrôle-commande, en veillant en particulier à vérifier l'indépendance des deux systèmes en matière de communications pour qu'une hypothétique défaillance de l'un ne puisse pas se propager à l'autre.

7 CONCLUSION

Entourés des précautions décrites ci-dessus, et analysés lors de leur conception par l'IRSN, les Systèmes de Protection informatisés sont utilisés avec succès en France depuis plus de 25 ans pour contribuer à la sûreté des réacteurs nucléaires, sans avoir jamais failli à leur mission de protection. L'IRSN a progressivement développé une capacité d'expertise de haut niveau dans ce domaine, faisant appel à des ingénieurs spécialisés qui participent activement aux travaux normatifs mondiaux sur ces sujets, et partagent leur expérience avec les spécialistes d'autres secteurs, aéronautique, spatial ou ferroviaire notamment.