Sécuriser les technologies numériques de la prochaine génération de réacteurs nucléaires

Par Joanne Liou

Toutes les innovations sont porteuses d'avantages susceptibles de transformer les industries mais comportent aussi des risques. Dans le domaine nucléaire, les réacteurs nucléaires avancés, notamment les petits réacteurs modulaires (PRM), intègrent des technologies innovantes, en particulier des technologies numériques qui apportent des solutions inédites.

Les PRM suscitent un intérêt croissant. Ces réacteurs réacteurs nucléaires avancés ont une capacité électronucléaire limitée – habituellement jusqu'à 300 MWe par tranche, soit environ un tiers de la capacité de production des réacteurs nucléaires de puissance traditionnels. Pour autant, l'utilisation d'une technologie numérique de pointe dans ces nouveaux réacteurs pose de nouveaux défis en termes de sûreté et de sécurité nucléaires. À travers le monde, on compte plus de 80 modèles et concepts de PRM à différents stades de développement.

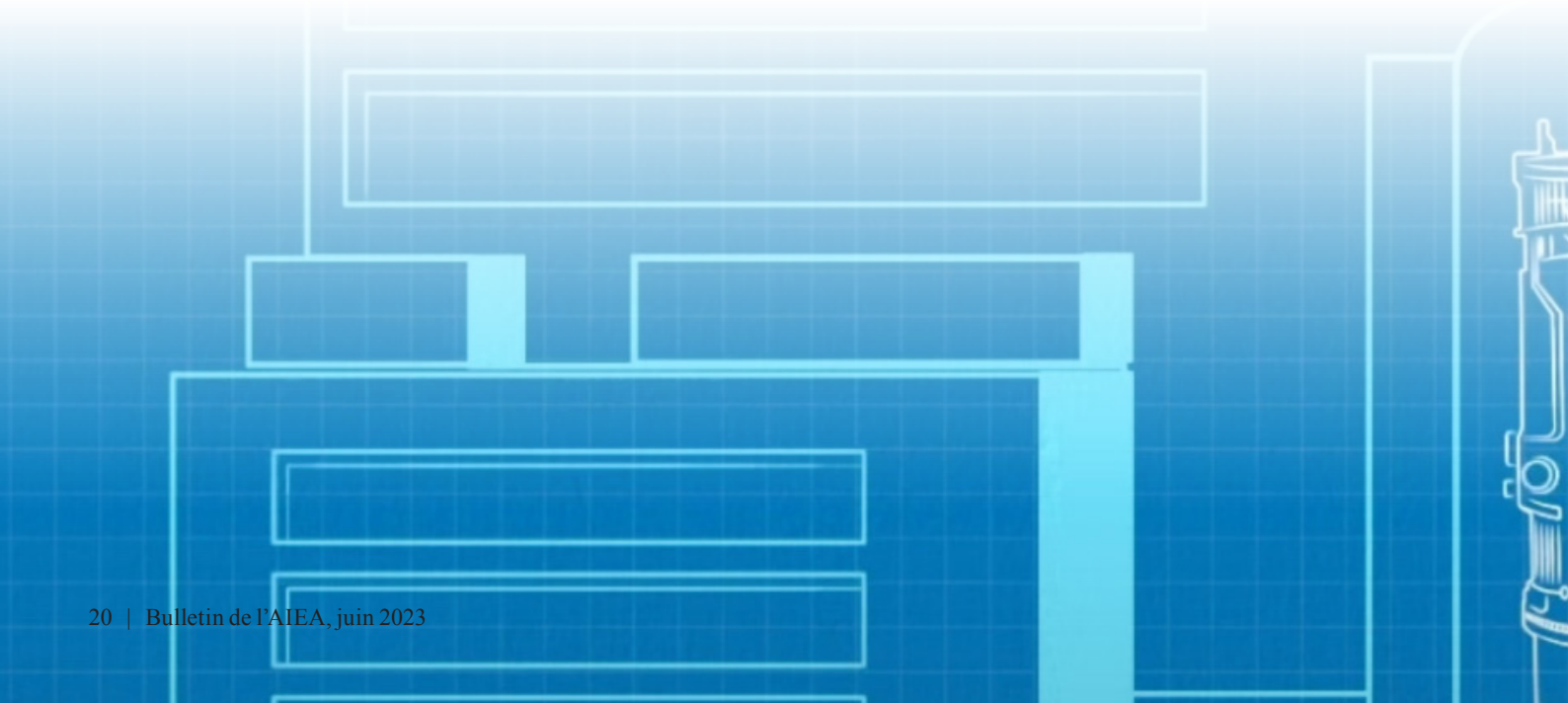
« L'un des défis du déploiement des PRM est d'accélérer la mise au point de leur technologie et de démontrer leur niveau de préparation tout en respectant les normes de sûreté et de sécurité nucléaires », fait observer Rodney Busquim e Silva, responsable de la sécurité de la technologie de l'information à l'AIEA. « Il faut donc mieux concevoir les solutions de commande-contrôle numériques et de sécurité informatique et les maintenir tout au long du cycle de vie du PRM ».

Solutions et défis informatiques

Les modèles innovants de PRM reposent sur des systèmes de contrôle-commande numériques qui leur confèrent des caractéristiques novatrices. Le nombre croissant de technologies numériques nécessaires à l'automatisation, au contrôle et à la maintenance à distance, et à d'autres caractéristiques nouvelles, montre qu'il faut disposer de solutions informatiques.

Certains PRM sont conçus pour être déployés dans des zones isolées et avec peu de personnel sur place, ce qui peut nécessiter une surveillance à distance constante et fiable. Compte tenu de la conception des systèmes de contrôle-commande numériques, l'application de mesures de sécurité informatique devrait être une condition préalable à une communication sécurisée entre le site du PRM et un centre de soutien. « La nécessité d'échanger des informations peut ouvrir des brèches susceptibles d'être exploitées par les cybercriminels et impose donc de prendre des mesures de cybersécurité solides pour protéger l'infrastructure de communication », indique Mike St. John-Green, expert en cybersécurité informatique basé au Royaume-Uni. « La confidentialité, la disponibilité et l'intégrité des informations doivent être protégées pour les opérations à distance afin de garantir un fonctionnement sûr et fiable des PRM et des infrastructures connexes ».

L'intelligence artificielle (IA) et l'apprentissage automatique (AA) appuient également l'exploitation des PRM. L'IA fait référence aux technologies qui produisent des systèmes capables de suivre des problèmes complexes, tandis que les technologies d'AA apprennent à accomplir une tâche particulière à partir de données. En combinant des simulations numériques d'installations nucléaires et des systèmes de surveillance et de contrôle avec des systèmes d'IA, l'industrie nucléaire cherche à optimiser des fonctions complexes, ce qui pourrait accroître l'efficacité opérationnelle. Ces avantages comportent toutefois un risque de cyberattaques. Par exemple, les algorithmes logiciels de l'IA et de l'AA reposent sur des bases de données qui pourraient être manipulées et ainsi entraîner une prise de décision erronée de l'IA.



« Ces systèmes peuvent par exemple, par injection de code, être alimentés intentionnellement avec des données corrompues, au cours du processus de développement, de la livraison ou de l'installation du logiciel. Le défi global est de savoir comment assurer une transparence suffisante des algorithmes d'IA/AA. L'utilisation acceptable de l'IA/AA doit être clairement définie et liée à des niveaux de risque acceptables », fait observer Si Wen, doctorant à l'Université de Tsinghua (Chine).

La sécurité dès la conception

Les experts s'accordent à dire que la sécurité informatique des installations nucléaires doit être prise en compte dès le commencement. Cette approche proactive, dite planification de la sécurité dès la conception, s'appuie sur les meilleures pratiques et les enseignements tirés. Elle répond au principe d'« intégration dans la conception » qui s'applique également à la sûreté, aux garanties et au déclassement nucléaires.

La sécurité informatique dès la conception vise à réduire les risques de sécurité à la source par une approche qui envisage systématiquement et de manière cohérente la sécurité à toutes les étapes de la durée de vie de l'installation ou du processus.

« Les mesures de sécurité informatique doivent être prises en compte et appliquées tout au long du cycle de vie des PRM, dès leur conception, pendant leur exploitation et jusqu'à leur déclassement », souligne M. Busquim e Silva. « Lorsque la sécurité, y compris la cybersécurité, est intégrée à la conception dès le départ, les concepteurs des installations peuvent faire des choix qui les rendront plus sûres, plus efficaces et moins coûteuses. »

Rôle de l'AIEA

L'AIEA met en relation des experts d'organisations nucléaires et autres, qui examinent les questions de sécurité informatique liées aux caractéristiques technologiques et opérationnelles des PRM et décèlent les difficultés en la matière. Par exemple, en février 2022, l'AIEA a organisé une réunion technique sur les systèmes de contrôle-commande et la sécurité informatique pour les PRM afin d'encourager la coopération et de faciliter l'échange d'informations entre experts internationaux. Les participants ont convenu de la nécessité d'harmoniser les approches et les réglementations nationales afin de rendre le marché international des PRM viable. « Les solutions de contrôle-commande concernant les PRM standardisés ouvrent un tout nouveau champ technique. L'automatisation toujours plus poussée nécessaire aux nouveaux modes d'exploitation et l'utilisation généralisée des systèmes numériques exigent des mesures de sécurité informatique et des solutions d'ingénierie dès la conception afin de garantir une exploitation sûre et sécurisée des centrales », déclare Jorge Casanova, qui a participé à la réunion en tant que représentant de l'Autorité argentine de réglementation nucléaire.

En mars 2023, l'AIEA a également organisé un atelier pour approfondir la réflexion sur le développement des capacités techniques liées à la sécurité informatique et aux systèmes de contrôle-commande pour les PRM. En outre, l'AIEA envisage de lancer un projet de recherche coordonnée sur le sujet en 2024.

À travers le monde, on compte plus de 80 modèles et concepts de PRM à différents stades de développement.