Contrecarrer les cybermenaces sur les centrales nucléaires

La centrale nucléaire de Nogent-sur-Seine, laquelle compte deux réacteurs.
Photo © EDF via l'auteur.

Protection de la population

Contrecarrer les cybermenaces sur les centrales nucléaires

Morand Fachot
Rédacteur technique à la Commission électrotechnique internationale (IEC)

Des normes internationales et des bonnes pratiques sont nécessaires pour assurer la cyber-résilience des centrales nucléaires. La Commission électrotechnique internationale (IEC) coopère avec l'Agence internationale de l'énergie atomique et d'autres organismes de normalisation et des organisations nationales et internationales, ainsi qu'avec l'industrie nucléaire de tous les pays pour assurer cette cyber-résilience.

La protection des infrastructures critiques – une priorité pour tous les pays

La portée et le coût des cyber-activités malveillantes (« cyberattaques ») augmentent dans le monde entier. Outre les pertes financières, les attaques contre les infrastructures critiques suscitent de plus en plus d'inquiétude en raison de conséquences catastrophiques possibles.

Le concept d'infrastructure critique couvre des domaines différents selon les pays. Le gouvernement américain répertorie 16 secteurs d'infrastructures critiques. Trois d'entre eux, les barrages, l'énergie et les « réacteurs nucléaires, matériaux et déchets » sont directement liés aux systèmes électriques. Les listes d'autres pays peuvent être similaires ou regrouper les centrales hydroélectriques et nucléaires et l'approvisionnement électrique dans un seul secteur « énergie », ce qui est le cas en Suisse.

La protection des infrastructures critiques contre les cyberattaques devient une priorité pour une majorité de pays. Les installations énergétiques sont au cœur même de l'ensemble de l'infrastructure critique. Ces dernières années, elles sont devenues une cible de choix des cyberattaques, dont certaines visaient, très probablement également, à identifier d'éventuelles vulnérabilités susceptibles d'être exploitées dans l'avenir.

Des réseaux électriques ont été ciblés (Irlande 2017) et même paralysés (Ukraine 2015-2016), ainsi que des installations hydroélectriques (Etats-Unis 2013) et nucléaires (Etats-Unis 2014, Inde septembre 2019, etc.). La compagnie Symantec annonçait, en octobre 2017, une recrudescence des cyberattaques dirigés contre les secteurs de l'énergie en Europe et en Amérique du Nord et affectant, entre autres, des opérateurs de centrales nucléaires aux Etats-Unis.

Les cyberattaques contre des centrales nucléaires, si elles réussissaient, auraient certainement les conséquences les plus dévastatrices en ce qui concerne l'approvisionnement électrique, mais également en raison d'un impact potentiel très grave et à très long terme sur l'environnement et la santé des populations avoisinantes.

Centrales nucléaires construites pour la sécurité, pas les cybermenaces

Selon Bill Gross, chef de projet principal à l'US Nuclear Energy Institute (NEI), les systèmes d'une centrale nucléaire se divisent en deux catégories principales.

Les systèmes primaires qui contrôlent le réacteur lui-même et, si nécessaire, le débranchent et le maintiennent dans les conditions de sureté nécessaires pour le protéger. Les systèmes secondaires qui eux contrôlent les équipements de production d'énergie. Un grand nombre de ces systèmes, construits il y a des années, reposent toujours sur un équipement analogique non connecté au réseau et donc moins vulnérable aux cyberattaques.

« *Les systèmes primaires sont conçus dès le départ pour assurer la fonction de sécurité voulue indépendamment de tout type de phénomène naturel ou d'origine humaine. Il n'y a pas de cyberattaque susceptible d'empêcher nos systèmes de sécurité d'arrêter efficacement le réacteur* », car, selon Bill Gross, les systèmes primaires et secondaires

des centrales nucléaires sont isolés les uns des autres pour une plus grande protection.

Cependant, les deux systèmes des anciennes centrales nucléaires sont progressivement équipés d'équipements numériques, tandis que les nouvelles centrales sont conçues avec des systèmes primaires et secondaires entièrement numériques.

Protection protéiforme contre multiplicité d'acteurs hostiles et de menaces

Les attaques contre les infrastructures critiques sont fréquentes et peuvent être lancées par une multiplicité d'acteurs – états, organisations non-étatiques ou criminelles et également, dans le cas spécifique des installations nucléaires, activistes antinucléaires.

Sans compter les cyberattaques, la protection des infrastructures critiques, nucléaires en particulier, nécessite des mesures physiques comme le contrôle d'accès aux installations et aux matières radioactives sur site et pendant leur transport, et la prévention des menaces internes (employés, fournisseurs de systèmes et services, etc.)

La cyberprotection des centrales nucléaires exige un ensemble de mesures techniques, l'adoption de normes internationales et de bonnes pratiques de la part des entreprises productrices d'énergie, et de l'ensemble de leurs chaînes logistiques, y compris les prestataires de services, fournisseurs et leur personnel.

Outre l'Agence internationale de l'énergie atomique (AIEA), dont le rôle est d'assurer un usage sûr et pacifique des technologies et des sciences liées au nucléaire, d'autres organisations nationales et internationales s'occupent d'assurer la protection des installations nucléaires, en particulier dans le domaine de la cyberprotection.

Le nucléaire en Suisse – présent et futur

Selon les dernières indications de l'Office fédéral de l'énergie, la part de l'énergie nucléaire dans la production d'électricité en Suisse s'élève à 36 % en moyenne annuelle sur 10 ans, avec des pointes pouvant atteindre 47 % en hiver. Les cinq centrales nucléaires suisses ont une puissance globale de 3,3 GW. Leur taux d'utilisation annuel avoisine les 83 %.

L'accident nucléaire de Fukushima (Japon) de mars 2011, suite à un tsunami, a conduit certains pays à reconsidérer le rôle de l'énergie nucléaire dans leur production d'électricité. C'est le cas de l'Allemagne qui a annoncé en avril 2011 sa décision de se retirer du nucléaire à l'horizon 2020. En Suisse, suite à la votation de mars 2017, le Conseil fédéral et le Parlement décident de sortir progressivement le pays de l'énergie nucléaire, avec la mise à l'arrêt des cinq centrales du pays à la fin de leur durée d'exploitation entre 2019 – en commençant par la centrale de Mühleberg qui arrête sa production le 20 décembre – et 2034. Les autres centrales restant en service « aussi longtemps que la sécurité est garantie » et elles ne seront pas remplacées par de nouvelles centrales nucléaires.

Selon le classement du Nuclear Threat Initiative (NTI), organisme indépendant estimant les risques d'attaques catastrophiques au moyen d'armes de destruction massive (nucléaires, biologiques, radiologiques, chimiques et cyber) la Suisse, avec un score de 80/100, se range dans les pays disposant d'un haut niveau de cybersécurité. Ce classement repose sur les cinq cyber critères suivants : cybersécurité obligatoire, protection des systèmes numériques critiques, cybersécurité pour les menaces de référence [DBT – design basis threats], évaluations de la cybersécurité, dispositif de réponse à des cyber incidents. Cependant ce bon classement ne doit pas donner lieu à une certaine suffisance en raison de la multiplicité des vulnérabilités et de la détermination de certains acteurs hostiles.

Engagement de longue date de l'IEC dans la cybersécurité
L'IEC est étroitement associée au développement de normes liées à la cybersécurité depuis des années grâce à ses travaux au sein de l'ISO/IEC JTC 1/SC 27, un sous-comité développant les normes internationales pour les Techniques de sécurité informatique, cybersécurité et protection de la vie privée, mis en place par ISO/IEC JTC 1, le Comité d'étude commun pour les Technologies de l'information, créé par l'IEC et l'Organisation internationale de normalisation (ISO), dont le siège, comme celui de l'IEC, se trouve à Genève. A noter que le siège de la troisième organisation globale de normalisation, l'Union internationale des télécommunications (UIT/ITU) se trouve également à Genève. Ces trois organisations forment le World Standards Cooperation (WSC).

ISO/IEC JTC 1/SC 27 a préparé des dizaines de documents couvrant divers aspects des techniques de sécurité informatique, y compris la famille de normes ISO/IEC 270** sur les systèmes de gestion de la sécurité de l'information.

Les centrales nucléaires ont des besoins distincts

Pour combler les besoins spécifiques [manquants] de l'industrie nucléaire, le sous-comité SC 45A de l'IEC: Instrumentation, systèmes de contrôle et systèmes électriques des installations nucléaires, un sous-comité du TC 45: Instrumentation nucléaire, a été chargé de développer des normes spécifiques pour la cyberprotection de ces installations.

Jusqu'à récemment, le SC 45A n'avait pas abordé le problème générique de la cybersécurité des centrales nucléaires. Son objectif a donc été de développer des normes pour prévenir, détecter et réagir aux cyberattaques sur les centrales nucléaires.

Cela a conduit à la publication en août 2014 de la norme IEC 62645, première norme internationale IEC visant à définir « des mesures programmatiques adéquates pour la prévention, la détection et la réaction aux actes

de malveillance commis par les cyberattaques » sur les systèmes informatiques des centrales nucléaires.

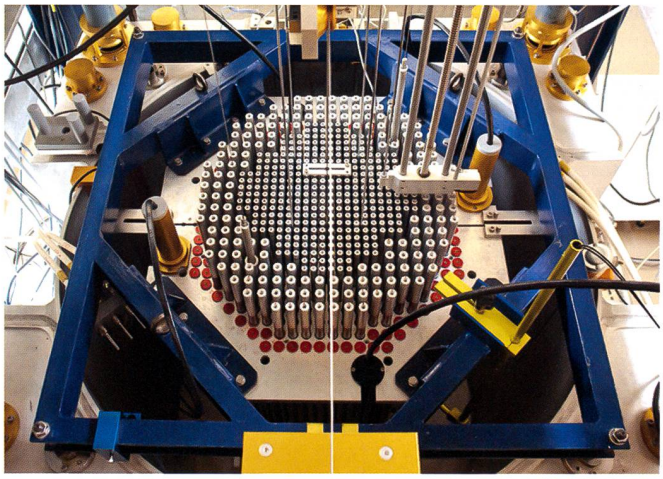
La deuxième édition de cette norme : « Centrales nucléaires de puissance – Systèmes d'instrumentation, de contrôle-commande [I&C] et d'alimentation électrique – Exigences relatives à la cybersécurité », a été publiée en novembre 2019.

Ce document précise que « les normes telles que l'ISO/IEC 27001 et l'ISO/IEC 27002 ne sont pas directement applicables à la cyberprotection des systèmes numériques programmables d'I&C du nucléaire. Ceci est principalement dû aux spécificités propres à ces systèmes, qui comprennent les exigences de sureté et réglementaires inhérentes aux installations nucléaires ». Cependant, il est également précisé que « ce document est construit sur les principes pertinents de haut niveau et les principaux concepts de l'ISO/IEC 27002, les adapte et les complète pour qu'ils s'accordent au contexte nucléaire. »
IEC 62645 compare également le cadre de sécurité global à celui développé par le NIST (Institut national de la normalisation et de la technologie, des Etats-Unis).

IEC 62645 couvre les domaines suivants :
- Mise en place et gestion d'un programme de sécurité des systèmes nucléaires. Cela inclut des concepts généraux pour la préparation du programme, des politiques et procédures, des rôles et des responsabilités, la mise en œuvre et le fonctionnement du programme.
- Mise en œuvre du cycle de vie pour la sécurité du système, comprenant les activités liées aux exigences, à la planification, conception, installation, exploitation, maintenance, etc.
- Tous les aspects des contrôles de sécurité, tels que la stratégie, l'organisation de la sécurité, la gestion des actifs, le contrôle d'accès, etc.

IEC 62645, développée pour prévenir et / ou minimiser l'impact des attaques contre les systèmes informatiques,

Intérieur d'un réacteur nucléaire, EPFL.



est destinée aux concepteurs et aux exploitants de centrales nucléaires, aux titulaires de licence, évaluateurs de systèmes, sous-traitants et autres.

Il s'agit de la première norme spécifiquement conçue pour la cybersécurité dans les centrales nucléaires. En tant que tel, elle devrait s'avérer essentielle pour le secteur nucléaire.

Deuxième norme traite de la coordination entre sécurité et cybersécurité

Une deuxième norme du SC 45A, IEC 62859, Centrales nucléaires – Systèmes d'instrumentation et de contrôle – Exigences pour la coordination de la sécurité et de la cybersécurité, « fournit un cadre pour la gestion des interactions entre la sécurité et la cybersécurité pour les systèmes de centrales nucléaires traitant ces questions et des spécificités des systèmes numériques programmables d'instrumentation et de contrôle-commande nucléaire ».

Elle établit des exigences et des directives pour :
- Intégrer les dispositions relatives à la cybersécurité dans les architectures et les systèmes d'instrumentation et de contrôle-commande nucléaire, qui sont fondamentalement conçus pour la sécurité.
- Éviter les conflits potentiels entre les dispositions relatives à la sécurité et à la cybersécurité.
- Permettre d'identifier et d'exploiter les synergies potentielles entre sécurité et cybersécurité.

Cette norme indique qu'elle adapte et complète les normes ISO/IEC 27001 et ISO/IEC 27002 au contexte nucléaire et est coordonnée avec la série IEC 62443 : Réseaux de communication industriels – Sécurité des réseaux et des systèmes, préparé par le TC 65 : Mesure, commande et automatisation dans les processus industriels.

Comme les autres normes IEC pour les centrales nucléaires IEC 62645 et IEC 62859 ont été élaborées en tenant compte des « principes et aspects fondamentaux de sécurité énoncés dans le code de l'AIEA sur la sécurité des centrales nucléaires ». La terminologie et les définitions utilisées par les normes du SC 45A sont cohérentes avec celles utilisées par l'AIEA.

La présente norme et les travaux en cours de l'IEC SC 45A devraient apporter une contribution significative à une meilleure protection des centrales nucléaires civiles contre les cybermenaces.

M. F.