Réseau
Sortir du nucléaire

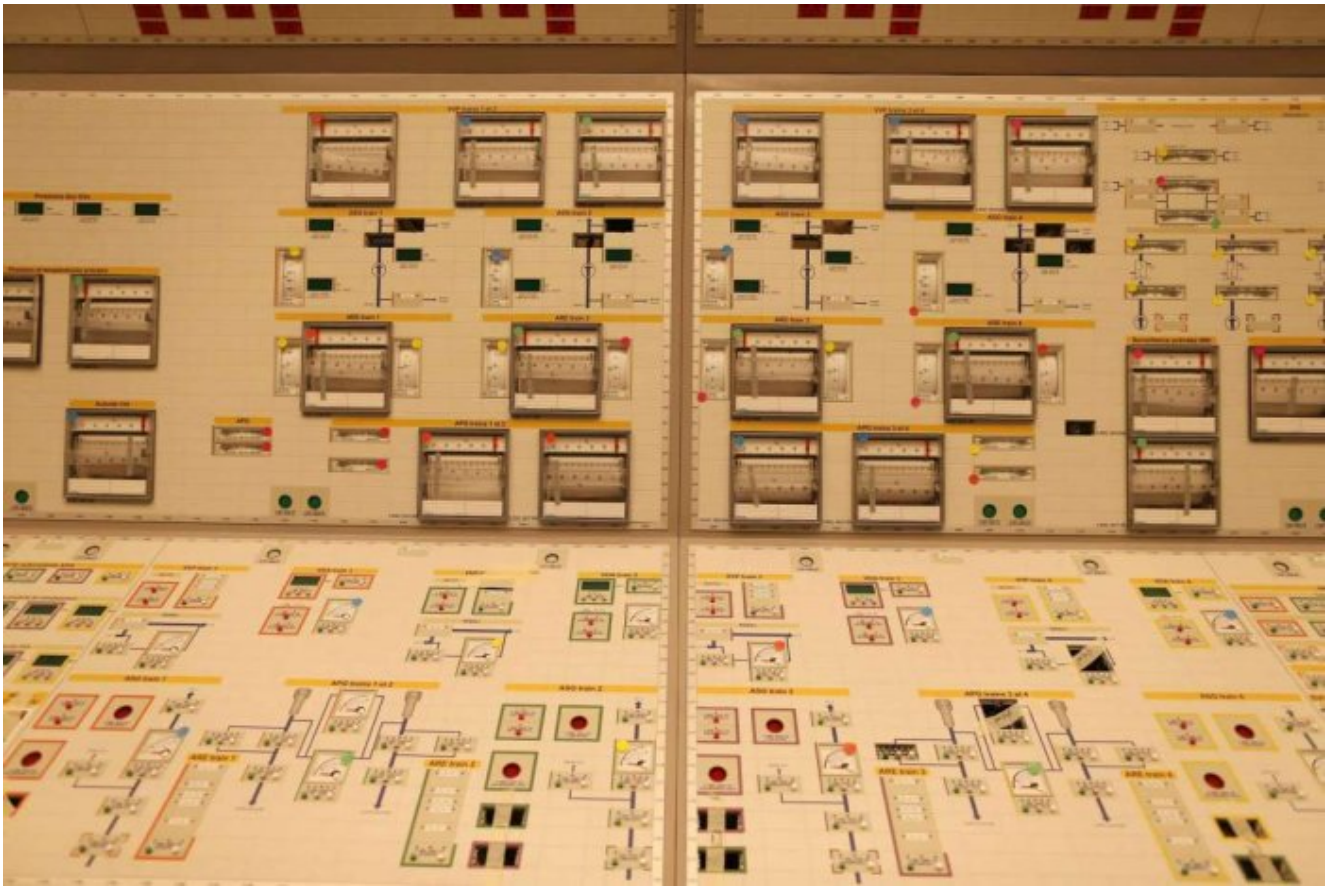
Réseau "Sortir du nucléaire"
9 rue Dumenge - 69317 Lyon
Tél : 04 78 28 29 22 Fax : 04 72 07 70 04
www.sortirdunucleaire.org

Source : https://www.sortirdunucleaire.org/Un-reacteur-entierement-informatise-complexe-et

9 août 2016

Un réacteur entièrement informatisé : complexe et vulnérable

En 2009, les autorités de sûreté nucléaire de Finlande, de France et du Royaume-Uni ont publié une position commune exprimant leurs extrêmes réserves sur le système numérique de contrôle-commande (SNCC) du réacteur EPR [1], "qui incarne ainsi l'abandon systématique du pilotage analogique câblé" [2].



Un pupitre de la salle de commande du réacteur EPR

Du point de vue des autorités de sûreté, ces gros problèmes de conception ont depuis été résolus, mais cela aura tout de même pris pas moins de cinq ans, et une solution différente dans chacun des trois pays pour répondre aux exigences respectives des autorités de sûreté [3]. Il n'en reste pas moins que "*le choix de conduire la tranche de manière privilégiée dans toutes les situations avec une IHM* [interface homme-machine] *informatisée dont la sophistication permet d'assister fortement l'opérateur*" n'a pas été fondamentalement remis en question malgré la révision substantielle du SNCC [4] , et que ce choix s'attirait en juin 2009 ce commentaire de l'Institut de Radioprotection et de Sûreté Nucléaire : "*L'IRSN relève que cette évolution vers davantage de complexité soulève des problèmes de fond et que de futures conceptions ne devraient pas continuer à évoluer dans ce sens.*" [5]

Une complexité qui n'est justement pas sans avoir déjà causé des problèmes inquiétants. En 1998, des composants majeurs du système de conduite du réacteur allemand Neckarwestheim-1 furent remplacés, passant d'un système câblé au SNCC "TELEPERM XS" développé par Siemens spécifiquement pour l'industrie nucléaire. Le 10 mai 2000, pendant un court laps de temps, la descente des grappes de contrôle (et d'arrêt d'urgence) du réacteur s'est retrouvée bloquée, et cette défaillance a été attribuée à la « complexité du système » de contrôle-commande ; de plus, les fonctions à l'origine de cette défaillance provenaient toutes du SNCC "TELEPERM XS" de Siemens [6]. Or le SNCC de l'EPR de Flamanville utilise précisément la plateforme "TELEPERM XS", dont la conception est jugée "satisfaisante" par l'ASN [7]...

L'association Global Chance relève d'ailleurs qu' "*Un premier essai* [de système de contrôle commande totalement informatisé] *avait été fait sur les réacteurs du palier N4 français et finalement abandonné au profit d'un système plus classique, avec pour conséquence un retard de quatre ans dans la mise en route du premier réacteur de ce palier.*" [8] Jean Gassino, expert du contrôle-commande à l'IRSN, expliquait à Science&Vie en 2010 : "*Au cours de développement de* [la] *plate-forme logicielle* [du SNCC du réacteur de Chooz-B1, connecté au réseau en 1996]*, on s'était aperçus que celle-ci était devenue si complexe qu'il n'était plus possible d'en démontrer la sûreté ; EDF avait été contraint de l'abandonner en route.*" [9]

On peut aussi s'interroger sur les effets indirects de l'introduction d'un système de contrôle-commande entièrement informatisé. En systématisant l'utilisation d'une IHM (interface homme-machine) numérique, il se pourrait qu'EDF cherche aussi au passage à pallier l'expérience et les compétences moindres des nouvelles générations d'agents de conduite (qui pilotent les réacteurs en salle de commande), par rapport aux agents aguerris par de longues années en salle de commande sur les réacteurs existants. Mais le changement de système de conduite ne risque-t-il pas également de perturber la transmission des compétences entre les agents expérimentés, familiers d'autres systèmes, et les agents plus récemment recrutés ?

Vulnérabilité aux cyber-attaques

Par ailleurs, l'informatisation complète du système de commande d'un réacteur nucléaire soulève aussi la question de sa vulnérabilité aux cyber-attaques.

En 1992, un technicien de la centrale nucléaire d'Ignalina (Lituanie), introduit un virus dans le système de contrôle industriel, affirmant par la suite avoir agi pour démontrer sa vulnérabilité aux cyber-attaques. En 2003, la centrale Davis-Besse (USA) est infectée par un "ver" informatique ; sa réplication automatique continuelle submerge le système qui contrôle les paramètres de fonctionnement du réacteur, un système qui se retrouve indisponible pendant près de cinq heures. Par chance, le réacteur était à l'arrêt à ce moment-là... En 2008, une simple mise à jour effectuée par un consultant sur un ordinateur du système de gestion de l'opérateur de la centrale Hatch (USA) induit en erreur le système de contrôle du réacteur, entraînant un arrêt involontaire de celui-ci pendant 48 heures.

En 2010, le virus Stuxnet, attribué aux services secrets américains et israéliens, a infecté l'usine d'enrichissement d'uranium de Natanz (Iran), provoquant la destruction physique de 1000 centrifugeuses. En septembre 2011, Areva découvre que des intrusions dans son système informatique ont lieu depuis deux ans ; la nature et l'étendue des informations compromises n'a jamais été rendue publique. En 2014, des hackers ont infiltré le réseau de KHNP, l'opérateur nucléaire sud-coréen, et volé les plans et manuels de deux réacteurs. Toujours en 2014, Symantec révélait qu'un réseau de hackers manifestement bien financé et probablement implanté en Europe de l'Est, dénommé Dragonfly, était parvenu, depuis 2011 voire avant, à corrompre les systèmes de contrôle de gestionnaires de réseau électrique, d'exploitants de centrales électriques, et autres entreprises en rapport avec la fourniture d'énergie. "*S'ils avaient fait usage des possibilités de sabotage qui étaient à leur portée, ils auraient pu causer des dommages ou une interruption de la fourniture d'énergie dans les pays affectés*". [10] [11] [12]

L'Agence européenne chargée de la sécurité des réseaux et de l'information (ENISA) relève que les systèmes de contrôle industriels SCADA ont subi ces dernières années une transformation substantielle, passant de systèmes propriétaires et relativement isolés à des architectures ouvertes et des technologies standard hautement interconnectées avec d'autres réseaux d'entreprise et avec internet. Et pour l'ENISA, les intranets et les réseaux de communication ouverts présentent une "*vulnérabilité accrue*" aux cyber-attaques [13].

En mars 2016, Gilles de Kerchove, coordinateur de l'Union européenne pour la lutte contre le terrorisme, déclarait : "*je ne serais pas étonné que le secteur nucléaire devienne, dans le futur, la cible de cyberattaques. […] je ne serais pas étonné qu'avant 5 ans, il y ait des tentatives d'utiliser Internet pour commettre des attentats. C'est-à-dire entrer dans le SCADA (Supervisory Control And Data Acquisition), le centre de gestion d'une centrale nucléaire, d'un barrage, d'un centre de contrôle aérien ou l'aiguillage des chemins de fer.*" [