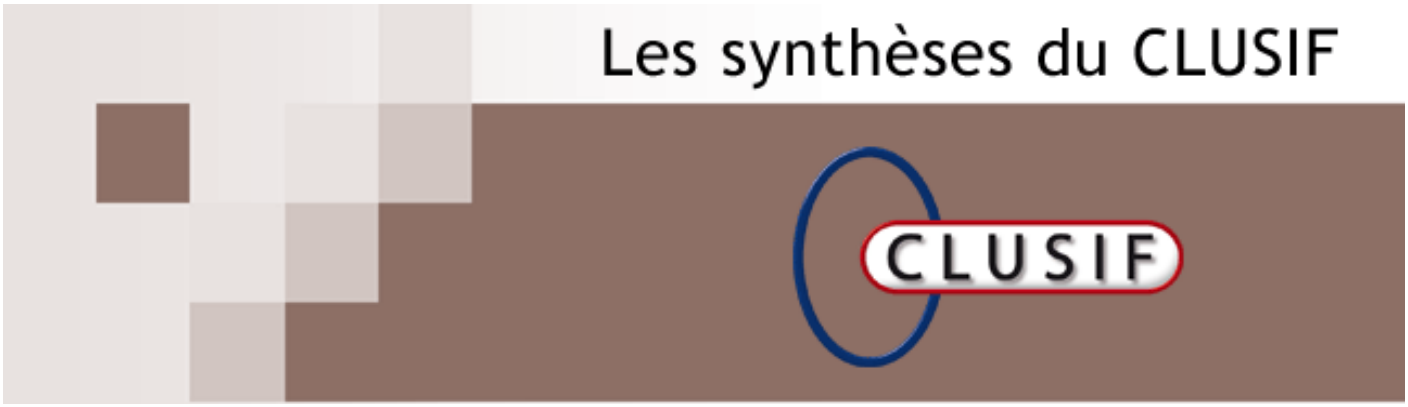

Systèmes Industriels et Sécurité de l'Information : Comment les rapprocher ?

Synthèse de la conférence thématique du CLUSIF du 18 décembre 2014.

Dans les années 2000, la sécurité des systèmes d'information industriels (SI-I) connaissait ses premiers balbutiements chez un petit nombre d'industriels. Les automates intégraient progressivement des solutions logicielles[1]. C'est avec l'actualité du ver StuxNet diffusée par la presse en 2010 que les industriels ont pris conscience des vulnérabilités des SCADA (supervisory control and data acquisition)[2]. Dans ce contexte, le Clusif a monté un Groupe de travail SCADA en 2013, animé par Gérôme Billois (Solucom) et co-animé par Hervé Schauer (Hervé Schauer Consultants), en partenariat avec l'ANSSI[3]. Il regroupe différents acteurs, tant du milieu industriel que de celui de la sécurité des systèmes d'information (SSI). Le Groupe a récemment publié ses travaux : « Cybersécurité des systèmes industriels - Par où commencer ? Panorama des référentiels et synthèse des bonnes pratiques ».

Pour les présenter, le Clusif a organisé, le 18 décembre 2014 au CCI Paris, la conférence «Systèmes industriels et sécurité de l'information, comment les rapprocher ? » en présence de Lazaro Pejsachowicz (Président du Clusif, CNAMTS), Stéphane Meynet (SGDSN-ANSSI), Gérôme Billois (Solucom), Thierry Jeannin (RTE) et Thierry Cornu (Euriware). Elle s'est achevée par une démonstration pratique de prise en main à distance d'un automate présentée par Arnaud Soullié (Solucom).

Des industriels confrontés à une abondance de référentiels[4]

L'un des objectifs du Groupe de travail SCADA était de dresser un panorama des référentiels consacrés à la sécurité des systèmes d'information industriels (SSI-I). Cinquante-trois documents hétéroclites ont été référencés, classés et ordonnés. À l'issue de l'étude, vingt documents ont été retenus. Ces référentiels s'adressent à trois populations distinctes : les professionnels de la conception, de l'intégration et de la maintenance, les experts de la SSI et les industriels. Pour démarrer la sécurité des SI-I, trois documents apparaissent incontournables : le guide de l'ANSSI « Maîtriser la SSI pour les systèmes industriels », le référentiel du NIST[5] (NIST SP800-82) et celui du DHS CSSP[6] (DHS CSSP Recommended practices). Pour autant, aucun document ne s'impose dans le monde de la sécurité des systèmes industriels. Aucun vocabulaire, ni principe commun ne se dégage. Les années à venir devraient permettre une montée en maturité des différents documents.

Accompagnement de l'ANSSI à la sécurisation des systèmes industriels[7]

L'ANSSI a débuté son projet de sécurisation des SI-I en 2010. La première volonté de l'Agence est d'offrir des bases solides à la sécurité des systèmes industriels. Confrontée à la multitude de référentiels, l'ANSSI a souhaité produire, en concertation avec les ministères et les industriels, des outils consacrés à la « Cybersécurité des systèmes industriels » adressés à l'ensemble des acteurs du domaine. En 2012, un premier guide est paru : « Maitriser la SSI pour les systèmes industriels », posant les principes et bonnes pratiques en la matière. Il fut complété par une méthode d'évaluation de la criticité des SI-I[8] et une présentation détaillée des

[1] Lazaro Pejsachowicz (CNAMTS) et Hervé Schauer (HSC), Table ronde
[2] Stéphane Meynet (SGDSN-ANSSI), « Enjeux de la sécurité des Systèmes Industriels »
[3] Agence nationale de la sécurité des systèmes d'information
[4] Gérôme Billois (Solucom), « Sécurité des Systèmes Industriels, par où commencer ? »
[5] National institute of standards and technology
[6] Department of homeland security control systems security program
[7] Stéphane Meynet (SGDSN-ANSSI), « Enjeux de la sécurité des Systèmes Industriels »
[8] « Méthode de classification et mesures principales »

mesures de sécurité[9]. L'ANSSI s'attache également à référencer les produits et prestataires de confiance par un mécanisme de qualification et de certification. En 2015, elle souhaite adopter une « approche globale du risque » par l'intégration de la SSI-I au sein des processus existants en matière de sécurité et de sûreté. L'Agence défend également son approche par-delà les frontières nationales, menant des actions pour la reconnaissance de ses qualifications au niveau européen.

Émergence d'un processus de sécurisation des systèmes industriels[10]

Près de cinq années après StuxNet, les industriels organisent leur gestion de la SSI-I. Un cycle de gestion sur trois à cinq ans apparaît[11]. Il se décompose en cinq étapes : la mise en place de la gouvernance, l'élaboration d'un cadre par la révision des référentiels et procédures de gestion du système industriel existants pour y intégrer le volet sécurité, la réalisation d'un état des lieux de la sécurité, un déploiement des mesures correctives et enfin le maintien du niveau de sécurité dans le temps. En France, l'industrie du nucléaire est la plus avancée dans ce processus suivie de celle de l'énergie électrique. Les transports ferroviaires et aériens se sont lancés en 2014 et la chimie débute le cycle. Pour autant, le déploiement de la SSI-I est freiné par plusieurs obstacles. Outre le coût et les contraintes opérationnelles, les professionnels rencontrent des difficultés dans l'appréciation du risque et la mise en place de la gouvernance. Le principal défi est de surmonter la différence de culture des acteurs. Ainsi, une discipline à part entière émerge qui impose l'alliance des compétences en SSI et en production industrielle.

Sécurisation du système industriel, retour d'expérience de RTE[12]

En juillet 2010, RTE, gestionnaire du réseau de transport d'électricité en France, est contacté par l'un de ses fournisseurs : certains de ses SCADA sont infectés par le ver StuxNet. Le mois suivant, l'organisme mène une campagne d'anti-virus sur les postes contrôle-commande de son système industriel. Le ver n'est pas détecté mais l'opération révèle l'infection de 20% des postes. Il ne s'agit que de programmes malveillants généralistes inadaptés au SI-I. Leur présence démontre que, malgré le cloisonnement du système industriel et l'absence de toute connexion directe à Internet, le système n'est pas à l'abri de toute menace extérieure. Aussi, RTE s'est attelé à la sécurisation de son système industriel par : la production d'un référentiel de sécurité dédié aux postes électriques, des contrôles internes réguliers de la bonne application du référentiel et l'amélioration continue du niveau de sécurité du SI-I. Aujourd'hui, le système industriel de RTE gagne en maturité. La sécurité est intégrée dès la phase de conception des SCADA. Les cahiers des charges adressés aux équipementiers présentent des exigences de sécurité. L'organisme s'est muni d'un service dédié à la sécurité de son système industriel.

Liste des sponsors : ESET, Ilex, NBS, Orange, Telecity Group, Trend Micro

Prochaine conférence Clusif : Panorama de la cybercriminalité – Année 2014, le 14 janvier 2015

[9] « Cybersécurité des systèmes industriels - Mesures détaillées »
[10] Thierry Cornu (Euriware), « 5 ans après StuxNet : état des lieux des pratiques et de la maturité des organisations »
[11] Le caractère cyclique du processus de gestion de la SSI-I a été dégagé par Gérôme Billois (Solucom) dans sa présentation « Sécurité des Systèmes Industriels, par où commencer ? »)
[12] Philippe Jeannin (RTE), « Retour d'expérience de l'alerte StuxNet à RTE »