enisa
European Network and Information Security Agency


# Protecting Industrial Control Systems

## Recommendations for Europe and Member States

## Executive Summary in French

This is the executive summary in French of the ENISA report "Protecting Industrial Control Systems. Recommendations for Europe and Member States" published on the 14th of December, 2011. Full report available at: https://www.enisa.europa.eu/act/res/other-areas/ics-scada/protecting-ics-report.

## Résumé

Les *Systèmes de contrôle industriels (SCI)* sont des réseaux et systèmes de contrôle et de commande conçus pour soutenir les processus industriels. Ces systèmes sont utilisés pour surveiller et contrôler un large éventail de processus et d'opérations, tels que la distribution de gaz et d'électricité, le traitement de l'eau, le raffinage de pétrole ou le transport ferroviaire. Les systèmes d'acquisition et de contrôle des données, SCADA (*Supervisory Control and Data Acquisition*) constituent le principal sous-groupe des SCI. Ces dernières années, les SCI ont subi une transformation considérable passant de systèmes propriétaires, isolés, à des architectures ouvertes et des technologies standard fortement interconnectées avec d'autres réseaux d'entreprises et l'Internet. Aujourd'hui, les produits SCI sont principalement basés sur des systèmes informatiques standards, intégrés dans différents dispositifs tels que des routeurs ou des modems-câbles, et ils utilisent souvent des logiciels d'emploi courant disponibles dans le commerce. Tout cela a conduit à des réductions de coûts et à une certaine facilité d'emploi, et a permis le contrôle et la surveillance à distance. Toutefois, l'inconvénient important découlant de la connexion aux intranets et aux réseaux de communication ouverts, est la vulnérabilité accrue aux attaques via les réseaux informatiques.

Les systèmes de contrôle industriels constituent un atout stratégique contre le risque grandissant de graves attaques terroristes affectant des infrastructures critiques[1]. Au cours de la dernière décennie, ces systèmes ont été confrontés à un nombre notable d'incidents, dont l'attaque Stuxnet, qui ont suscité de vives inquiétudes et discussions parmi les acteurs impliqués dans le domaine.

En avril 2007, le Conseil a adopté les conclusions d'un programme européen de protection des infrastructures critiques (EPCIP)[2]. Cette initiative est le résultat de toute une série d'actions menées par la Commission européenne, le Conseil et le Conseil «Justice et affaires intérieures», entreprises en juin 2004. L'élément central de l'EPCIP est la directive[3] concernant le recensement et la désignation des infrastructures critiques européennes. Parallèlement, les questions de sécurité de l'information pour les infrastructures vitales en

[1] ***Commission des communautés européennes.*** *Communication de la Commission au Conseil et au Parlement européen. Protection des infrastructures critiques dans le cadre de la lutte contre le terrorisme COM(2004) 702 final. 2004.*

[2] ***Commission des communautés européennes.*** *Communication de la Commission sur un programme européen de protection des infrastructures critiques COM(2006) 786. 2006.*

[3] ***Commission des communautés européennes.*** *Directive 2008/114/CE du Conseil du 8 décembre 2008 concernant le recensement et la désignation des infrastructures critiques européennes ainsi que l'évaluation de la nécessité d'améliorer leur protection .2008.*

Europe sont traitées par la stratégie numérique pour l'Europe (DAE)[4] et le plan d'action PIIC (protection des infrastructures d'information critiques)[5].

Bien consciente de l'importance du problème, l'ENISA a lancé une série d'activités qui visent à réunir les parties prenantes concernées et à les impliquer dans une discussion ouverte sur la protection des SCI. Ce dialogue ouvert vise essentiellement à identifier les principaux problèmes concernant la sécurité des SCI[6] et à reconnaitre et soutenir les initiatives nationales, paneuropéennes et internationales sur la sécurité des SCI. Parmi les parties prenantes concernées figurent des fournisseurs de services et d'outils de sécurité pour les SCI, des fabricants et intégrateurs de logiciels/matériels pour SCI, des opérateurs d'infrastructures, des organismes publics, des instances de normalisation, le milieu universitaire et des services R&D.

De surcroît, afin d'aider les parties prenantes à mieux comprendre la problématique, l'ENISA a décidé de continuer d'explorer la protection des SCI en y consacrant des recherches et une étude fondée sur une enquête. L'étude vise à élaborer une perspective actuelle sur la protection des SCI essentiellement en Europe, mais aussi dans le contexte international. Elle englobe les menaces, les risques et les enjeux dans le domaine de la protection des SCI ainsi que les initiatives nationales, paneuropéennes et internationales sur la sécurité des SCI.

Le rapport final propose sept recommandations aux acteurs publics et privés du secteur des SCI. Ces recommandations sont destinées à donner des conseils pratiques et utiles en vue d'améliorer les initiatives actuelles, de renforcer la coopération, de développer de nouvelles mesures et les bonnes pratiques et de réduire les obstacles au partage d'informations. Ces recommandations sont basées sur les résultats d'une analyse complète des avis des experts qui ont participé à l'étude. En outre, des données importantes émanant d'une recherche documentaire approfondie sont également prises en considération. Toutes ces données ont été analysées et ont débouché sur une centaine de conclusions clés.

Ce qui suit constitue une brève synthèse de toutes les recommandations.

***Recommandation 1: Élaboration de stratégies nationales et paneuropéennes sur la sécurité des SCI.*** *L'Union européenne devrait définir une stratégie paneuropéenne pour les activités de sécurité des SCI européens et chaque État membre devrait développer une stratégie nationale sur la sécurité des SCI. Les stratégies doivent être conformes à la directive 2008/114/CE du Conseil de l'Union européenne relative aux infrastructures critiques, et tirer avantage des initiatives qui existent pour traiter le problème de la sécurité des SCI (par exemple, EuroSCSiE)*

---

[4] ***Commission des communautés européennes.*** *Communication de la Commission: Une stratégie numérique pour l'Europe, COM(2010) 245. 2010.*

[5] **Commission des communautés européennes.** Communication de la Commission: Protéger l'Europe des cyberattaques et des perturbations de grande envergure: améliorer l'état de préparation, la sécurité et la résilience, COM(2009) 149. 2009.

[6] *À différents niveaux: juridique et réglementaire, organisationnel, économique/financier et technique mais aussi en termes de diffusion et de sensibilisation.*

*ainsi que des partenariats public/privé nationaux et paneuropéens (par exemple EP3R). Les stratégies doivent servir de références pour toutes les parties prenantes des États membres, favoriser les initiatives de partage et encourager la recherche et l'éducation.*

***Recommandation 2: Création d'un guide de bonnes pratiques pour la sécurité des SCI.*** *L'Union européenne devrait prendre l'initiative dans ce domaine et développer un document ou un ensemble de documents, faisant l'objet d'un consensus, concernant les bonnes pratiques en matière de sécurité, intégrant à la fois les aspects physiques et logiques de sécurité, qui servirait de référence pour chaque type de partie prenante. Ce document devrait aider les parties prenantes à assurer que les meilleures pratiques en matière de sécurité soient appliquées dans l'industrie.*

***Recommandation 3: Création de modèles de plan de sécurité pour les SCI.*** *Les différentes stratégies nationales sur la sécurité des SCI devraient inclure dans leurs tâches la création de modèles de plan de sécurité pour les SCI, tant pour l'opérateur que pour les infrastructures, que les experts en sécurité pourraient adapter à leur situation particulière. Ces plans devraient inclure la sécurité physique et opérationnelle, les problèmes techniques, la formation et la sensibilisation, la gouvernance de la sécurité avec des rôles et des responsabilités définis, les mesures pour diminuer l'impact sur les affaires, et la gestion de crises. Ces modèles devraient permettre de réduire considérablement le coût de développement des plans de sécurité et d'accélérer l'adoption de mesures globales de sécurité dans l'industrie.*

***Recommandation 4: Favoriser la sensibilisation et la formation.*** *Dans le cadre des stratégies nationales sur la sécurité des SCI, les États membres devraient encourager les activités de diffusion et de sensibilisation au travers d'évènements de qualité impliquant tous les types de parties prenantes et avec une attention particulière portée à l'engagement des hauts dirigeants. Des programmes et évènements de formation et de sensibilisation devraient être créés pour tous les types d'utilisateurs finaux.*

***Recommandation 5: Création d'un banc d'essai commun, ou, d'un cadre de certification de la sécurité des SCI.*** *La stratégie commune en matière de SCI devrait conduire à la création d'un ou de plusieurs bancs d'essai communs au niveau européen, prenant la forme d'un partenariat public-privé dans lequel des essais pourraient être conduits afin de garantir que l'interaction entre différents systèmes ne risque pas d'occasionner des défaillances en matière de sécurité. Un banc d'essai commun aidera toutes les parties prenantes à identifier d'éventuels problèmes dans un environnement contrôlé, ce qui permettra d'assurer l'intégrité et de renforcer la confiance dans les solutions certifiées.*

*De manière alternative, un cadre de certification de la sécurité, adapté pour les SCI, pourrait être défini en s'appuyant sur les efforts existants tels que les Critères communs ou la norme FIPS. Les organismes de certification existant dans les États membres seraient responsables du processus de certification fondé sur ce cadre.*

***Recommandation 6: Création de capacités nationales de réponse aux urgences informatiques concernant les SCI****. Selon les stratégies nationales en matière de sécurité des SCI, des capacités nationales de réponse aux urgences informatiques concernant les SCI*

*devraient être instaurées, en coopération avec un nombre approprié de CERT (équipes d'intervention en cas d'urgence informatique) publiques et privées. Ces capacités de réponse aux urgences informatiques devraient fournir aux parties prenantes une approche de référence pour partager les informations sur la vulnérabilité, les divulguer, coordonner les actions et aider à traiter efficacement la gestion des risques dans les infrastructures des SCI. Pour faire face à ces problèmes qui franchissent bien évidemment les frontières, les États membres devraient coopérer au niveau paneuropéen [par exemple avec l'aide d'une plate-forme de partage d'informations sur la sécurité des SCI telle qu'EuroSCSiE (European SCADA and Control Systems Information Exchange)].*

***Recommandation 7: Encourager la recherche en matière de sécurité des SCI en exploitant les programmes de recherche existants.*** *Les stratégies nationales et communes sur la sécurité des SCI devraient encourager la recherche à s'intéresser aux menaces actuelles et futures pour les SCI et à s'attaquer aux défis posés par la sécurité, tels que l'intégration SCI-TIC, le matériel existant/non sécurisé, les attaques ciblées ou les questions liées aux projets de réseaux intelligents. Cela devrait s'effectuer en tirant parti des programmes de recherche nationaux ou européens existants, tels que le Programme cadre européen de recherche.*


P.O. Box 1309, 71001 Heraklion, Greece
www.enisa.europa.eu