Assistance à l'homologation

Cybersécurité des systèmes industriels

« L'opérateur d'importance vitale procède à l'homologation de sécurité de chaque système d'information d'importance vitale (SIIV), en mettant en œuvre la procédure d'homologation prévue par sa politique de sécurité des systèmes d'information (PSSI).»

Source: Arrêté sectoriel du 17 juin 2016 relatif à la loi de programmation militaire 2014-2019 – Règle 2 relative à l'homologation de sécurité

La solution Schneider Electric

Pour vous accompagner dans votre démarche d'homologation, Schneider Electric vous propose un ensemble complet de solutions et de services dédiés à la cybersécurité industrielle, depuis l'analyse des risques jusqu'au maintien en condition de sécurité, en passant par l'étude et la mise en œuvre de mesures de sécurité.
Les experts Schneider Electric maîtrisent la triple compétence (SCADA, réseaux, sécurité) nécessaire pour réussir le pari de la cybersécurité industrielle.

Bénéfices client

Préparation à l'audit de la sécurité des systèmes d'information d'importance vitale - SIIV

Gain de temps, économie de ressources grâce à l'accompagnement par nos équipes qui maitrisent parfaitement les exigences des arrêtés sectoriels, ainsi que les normes et les référentiels de cybersécurité industrielle.

Schneider Electric entame sa qualification de Prestataire d'Audit de Sécurité des Systèmes d'Information (PASSI) selon le référentiel de l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI).

Les équipes de services de Schneider Electric sont en première ligne pour renforcer la cybersécurité des systèmes industriels des opérateurs de services essentiels (OSE) et d'importance vitale (OIV).

se.com/fr

Life Is On Schneider Electric

Description de l'offre

Objectif

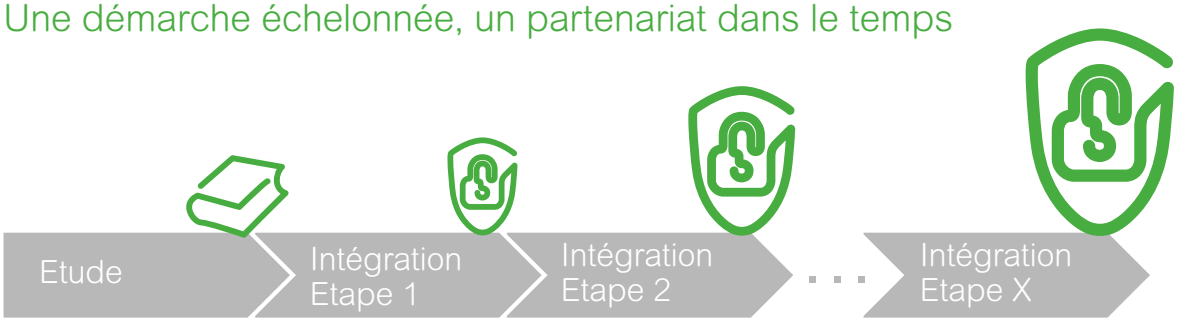
L'objectif de cette prestation est d'accompagner l'opérateur d'importance vitale – OIV pour l'homologation de ses systèmes critiques.

Méthodologie

La démarche consiste à analyser le système et proposer un plan d'action visant à réduire les risques.
Elle est découpée en plusieurs étapes échelonnées dans le temps :

- l'analyse des risques,
- la réduction des risques à l'aide de mesures de sécurité organisationnelles et techniques,
- la justification de l'acceptation des risques résiduels.

Une démarche échelonnée, un partenariat dans le temps



Le dossier de sécurité est rédigé en parallèle de la démarche. Il permettra de simplifier la phase de validation qui sera effectuée par l'opérateur lui-même ou par un prestataire qualifié PASSI :

- Audit de la sécurité du SIIV

Périmètre technologique

L'ensemble des équipements d'automatisme de marque Schneider Electric ou de marque tierce est couvert par ce service.
Ces équipements incluent principalement :

- les Systèmes Numériques de Contrôle-Commande (SNCC ou DCS),
- les systèmes de supervision ou Supervisory Control And Data Acquisition (SCADA),
- les Automates Programmables Industriels (API),
- les Interfaces Homme Machine (IHM),
- les réseaux Ethernet ou propriétaires et les équipements réseaux (commutateurs, routeurs, pare-feux).

Maintien en condition de sécurité - MCS

Tout au long du cycle de vie de votre système industriel, de nouvelles vulnérabilités sont découvertes sur nos matériels et logiciels mis en œuvre dans vos process.
Grâce à notre contrat de service MCS vous êtes alerté lors de la survenance d'un nouveau risque détecté et nous vous proposons dans un délai de 72 heures une méthode de mitigation du risque adaptée.

Schneider Electric à votre service

Schneider Electric NEC - Network Engineering & Cybersecurity – est à votre disposition pour vous accompagner lors de la mise en œuvre du dossier d'homologation de vos infrastructures industrielles.
Contact : FR-NEC@se.com

Schneider Electric France
Direction Marketing Communication France
35, rue Joseph Monier
92500 Rueil-Malmaison
Conseils : 0 825 012 999*
Services : 0810 102 424**

Life Is On Schneider Electric

* Services 0,15 €/appel + prix de l'appel
** Service gratuit + prix de l'appel

09/2021 - ZZ5752-A