

Objectifs

- Présenter la problématique de la cybersécurité des systèmes de contrôle,
- Comprendre la démarche et le contenu des documents normatifs ISA/IEC 62443 (ISA-99) afin de faciliter leur accès aux futurs utilisateurs.
- Donner les lignes directrices pour construire un système de gestion de la cybersécurité
- Traiter deux exemples d'application de l'IEC 62443
- Préconiser des pratiques de défense de nature à accroître le niveau de cybersécurité des installations.
- Aborder la problématique de l'internet des objets et les solutions spécifiques qu'il appelle.

Public

Ce stage est destiné aux responsables et aux ingénieurs et techniciens appelés à intégrer la notion de cybersécurité dans leurs activités, notamment développement, l'installation, l'exploitation ou l'analyse des systèmes de contrôle industriels.

Pré-requis

Connaissances techniques générales

Éléments pédagogiques

Ce cours est supporté par un ensemble documentaire composé de 500 diapositives, illustrations graphiques, informations méthodologiques pour l'utilisation pratique des connaissances acquises.

Une clé USB avec le support de recours est remise aux participants ainsi qu'un lien de téléchargement

Contenu

Première partie : La menace

- La sécurité des systèmes de contrôle : rappels et définitions
- Cybersécurité et sécurité fonctionnelle
- Comprendre les attaques pour savoir y faire face
- La veille cybersécuritaire : où trouver des informations
- Pourquoi les IACS sont-ils vulnérables ?
- Les solutions de l'informatique classique ne sont pas suffisantes – L'utilité d'un référentiel

Deuxième partie : l'ISA-99 et l'IEC 62443

- Le comité de standardisation ISA99
- L'approche générale de l'IEC 62443
- L'IEC 62443 : plan documentaire et introduction aux principaux documents
- IEC 62443 : Synthèse de la démarche
- Evaluation et certification
- IEC 62443-1-5 : Industrial automation and control system protection levels
- IEC TR62443-1-4 : Exemples de détermination et d'analyse des zones et des conduits

Troisième partie : Se protéger

- Les mesures organisationnelles
- Les mesures techniques

Quatrième partie : La problématique de l'Internet des objets

Approfondissement des principaux documents de l'IEC 62443 :

IEC 62443-1-1: Models and Concepts

Terminologie et concepts vue de permettre la compréhension de la cybersécurité dans l'environnement des systèmes de contrôle et d'automatisation industriels.

IEC 62443-2-1: Security program requirements for IACS owners

Exigences de sécurité techniques et organisationnelles à satisfaire par les responsables des systèmes de contrôle.

IEC TR 62443-2-2 (projet): IACS protection levels
– Définition de Security Program Ratings permettant d'évaluer la confiance que l'on peut porter à un système en opération.

IEC 62443-2-4 : Security program requirements for IAC service providers

Exigences à satisfaire par les fournisseurs de services d'intégration et de maintenance

IEC 62433-3-2: Security risk assessment and system design

Analyse de risques, détermination des zones et conduits et des objectifs de cybersécurité

IEC 62443-3-3: System Security Requirements and Security Levels

Notion de vecteurs SLs. Méthodologie et règles techniques permettant de déterminer le niveau de sécurité atteints par un système donné.

IEC 62443-4-2 : Technical security requirements for IACS components

Complément à l'IEC 62443-3-3 pour les composants constitutifs des systèmes

Contact auteur - formateur :

Jean-Pierre Hauet – Voting member de l'ISA99

jean-pierre@hauet.com

Inscriptions :

+33 (0)1 41 29 05 09 contact@isa-france.org