Formation : ISO/IEC 62443, comprendre la cybersécurité des systèmes industriels

Formation pratique - 2j - 14h00 - Réf. SYI

NEW

Une formation immersive pour comprendre les fondamentaux de la norme ISO/IEC 62443, maîtriser son vocabulaire, ses concepts clés (zones et conduits, Security Levels, Foundational Requirements) et savoir appliquer la norme concrètement à un système industriel à travers des études de cas guidées

Objectifs pédagogiques

À l'issue de la formation, le participant sera en mesure de :

- Comprendre les enjeux de la cybersécurité des systèmes industriels (OT/ICS) et leurs spécificités versus IT
- Maîtriser la structure de la famille de normes ISO/IEC 62443 et le rôle de chacun de ses documents
- Réaliser une analyse de risque simplifiée et un découpage zones/conduits sur un cas concret
- Identifier les responsabilités des différents acteurs (asset owner, intégrateur, fournisseur de produit)
- Situer la norme 62443 dans le paysage réglementaire (NIS2, guides ANSSI)

Public concerné

Public mixte IT et OT : analystes SOC, RSSI, ingénieurs systèmes industriels, automaticiens, chefs de projet OT, intégrateurs, auditeurs, consultants cybersécurité.

Prérequis

Connaissance de base en
systèmes industrie
ls (automate, SCADA, capteur) ou
sur les réseaux/systèmes IT
et en
cybersécurité
(CIA, défense en profondeur)
.

PARTICIPANTS

Public mixte IT et OT : analystes SOC, RSSI, ingénieurs systèmes industriels, automaticiens, chefs de projet OT, intégrateurs, auditeurs, consultants cybersécurité.

PRÉREQUIS

Connaissance de base en
systèmes industrie
ls (automate, SCADA, capteur) ou
sur les réseaux/systèmes IT
et en
cybersécurité
(CIA, défense en profondeur)
.

COMPÉTENCES DU FORMATEUR

Les experts qui animent la formation sont des spécialistes des matières abordées. Ils ont été validés par nos équipes pédagogiques tant sur le plan des connaissances métiers que sur celui de la pédagogie, et ce pour chaque cours qu'ils enseignent. Ils ont au minimum cinq à dix années d'expérience dans leur domaine et occupent ou ont occupé des postes à responsabilité en entreprise.

MODALITÉS D'ÉVALUATION

Le formateur évalue la progression pédagogique du participant tout au long de la formation au moyen de QCM, mises en situation, travaux pratiques...
Le participant complète également un test de positionnement en amont et en aval pour valider les compétences acquises.

Modalités d'évaluation

Le formateur évalue la progression pédagogique du participant tout au long de la formation au moyen de QCM, mises en situation, travaux pratiques…

Le participant complète également un test de positionnement en amont et en aval pour valider les compétences acquises.

Programme de la formation

1 cybersécurité industrielle

- Différences fondamentales IT versus OT : priorités (CIA versus AIC), contraintes temps réel, cycles de vie longs, sûreté de fonctionnement.
- Panorama des incidents marquants : Stuxnet, Triton/Trisis, Industroyer, Colonial Pipeline.
- Architecture de référence : le modèle Purdue (niveaux 0 à 5).

2 Présentation de la famille ISO/IEC 62443

- Origine de la norme : ISA-99 ? IEC 62443.
- Structure en 4 catégories : general, policies et procedures, dystem, component.
- Cartographie des documents clés : 62443-1-1, 2-1, 2-4, 3-2, 3-3, 4-1, 4-2.
- Les 3 rôles centraux : asset owner, system integrator, product supplier.

Etude de cas

Cartographie des rôles — à partir d'un schéma d'usine fictive, identifier qui fait quoi et quel document 62443 s'applique à chaque acteur.

3 Le vocabulaire incontournable de la 62443

- IACS, SUC (System Under Consideration), essential function.
- Zones et conduits : définitions, principes de regroupement.
- Security Levels : SL-T (Target), SL-A (Achieved), SL-C (Capability), SL 1 à 4.
- Threat actors selon la 62443 : du script kiddie à l'État-nation.

Atelier

Exercice de mise en correspondance des termes/définitions, en binôme IT/OT pour favoriser les échanges.

4 Les 7 Foundational Requirements (FR)

- FR1 : Identification & Authentication Control (IAC).
- FR2 : Use Control (UC).
- FR3 : System Integrity (SI).
- FR4 : Data Confidentiality (DC).
- FR5 : Restricted Data Flow (RDF).
- FR6 : Timely Response to Events (TRE).
- FR7 : Resource Availability (RA).
- Lien entre FR, System Requirements (SR) et Component Requirements (CR).

Réflexion collective

Analyse en groupe d'un FR avec ses SR et Requirement Enhancements (RE) associés selon le SL visé.

MOYENS PÉDAGOGIQUES ET TECHNIQUES

• Les moyens pédagogiques et les méthodes d'enseignement utilisés sont principalement : aides audiovisuelles, documentation et support de cours, exercices pratiques d'application et corrigés des exercices pour les formations pratiques, études de cas ou présentation de cas réels pour les séminaires de formation.
• À l'issue de chaque formation ou séminaire, ORSYS fournit aux participants un questionnaire d'évaluation du cours qui est ensuite analysé par nos équipes pédagogiques.
• Une feuille d'émargement par demi-journée de présence est fournie en fin de formation ainsi qu'une attestation de fin de formation si le participant a bien assisté à la totalité de la session.

MODALITÉS ET DÉLAIS D'ACCÈS

L'inscription doit être finalisée 24 heures avant le début de la formation.

ACCESSIBILITÉ AUX PERSONNES HANDICAPÉES

Pour toute question ou besoin relatif à l'accessibilité, vous pouvez joindre notre équipe PSH par e-mail à l'adresse psh-accueil@orsys.fr.

5 Analyse de risque selon 62443-3-2

- Le processus ZCR (Zone and Conduit Requirements) en 7 étapes.
- Identification du SUC et découpage initial en zones/conduits.
- Évaluation du risque initial et détermination du SL-T.
- Notion de risque tolérable et itération.

Etude de cas
(Sur une petite usine de production avec MES, SCADA, automates, capteurs, accès distant fournisseur), les participants découpent le système en zones et conduits sur un plan papier, justifient leurs choix et attribuent un SL-T à chaque zone.

6 Du SL-T aux mesures concrètes

- Comment passer du Security Level cible aux exigences techniques et organisationnelles.
- Lecture pratique de la 62443-3-3 (System Requirements).
- Lecture pratique de la 62443-4-2 (Component Requirements) pour les produits.
- Cohérence SL-T/SL-C/SL-A : que faire quand un composant n'atteint pas le SL visé ? (mesures compensatoires)

Etude de cas
Pour une zone identifiée, lister les SR applicables selon le SL-T choisi et identifier les écarts probables avec un existant industriel typique.

7 Volet organisationnel : 62443-2-1 et 2-4

- 62443-2-1 : le CSMS (Cyber Security Management System) côté asset owner.
- 62443-2-4 : exigences applicables aux prestataires d'intégration et de maintenance.
- Lien avec un SMSI ISO 27001 existant : complémentarité, pas de redondance.
- Cycle de vie sécurité : conception, intégration, exploitation, décommissionnement.

8 Volet produit : 62443-4-1 et certification

- 62443-4-1 : Secure Development Lifecycle (SDL) côté fournisseur.
- 62443-4-2 : exigences techniques par type de composant (logiciel, embarqué, réseau, hôte).
- Panorama des certifications : ISASecure, IECEE, et leur valeur dans un appel d'offres.
- Positionnement réglementaire et écosystème : place de la 62443 dans NIS2 et la directive REC.
- Guides ANSSI sur la cybersécurité des systèmes industriels et leur articulation avec 62443.
- Référentiels complémentaires : NIST SP 800-82, IEC 62351.
- Ressources communautaires, retours d'expérience, organismes (ISA, CLUSIF, CESIN).

Etude de cas
Analyser une fiche technique d'un équipement industriel et identifier les éléments qui démontrent (ou non) la conformité 62443-4-2.