CODE
5506

GÉNIE INDUSTRIEL / AUTOMATISME - ARCHITECTURE DE COMMANDES

POSSIBLE EN INTRA

CYBERSÉCURITÉ INDUSTRIELLE POUR PUBLIC D'AUTOMATICIENS : VULNÉRABILITÉS & SÉCURISATION DES SYSTÈMES

Les systèmes industriels sont de plus en plus exposés aux cyberattaques. Cette formation aide automaticiens et informaticiens à identifier les vulnérabilités, acquérir un langage commun et renforcer la sécurité des installations critiques.

2415 € HT | **3 JOURS** (21 H.) | **VILLEURBANNE**
DU 06/07/2027 AU 08/07/2027

COMPÉTENCE PRINCIPALE VISÉE

Appréhender les vulnérabilités des systèmes existants et mettre en œuvre une méthodologie de renforcement du niveau de cybersécurité d'un système de contrôle-commande industriel



LES + DE LA FORMATION

Approche collaborative entre automaticiens et informaticiens. Alternance théorie/TP et études de cas. Mise en pratique des normes, bonnes pratiques et recommandations ANSSI pour anticiper, détecter et contrer efficacement les cyberattaques industrielles.

PUBLIC

- Automaticiens
- Techniciens et ingénieurs chargés d'installer, programmer, régler ou dépanner des équipements automatisés, machines-outils et robots industriels

PRÉREQUIS

- Connaissances techniques dans le domaine du contrôle-commande industriel

OBJECTIFS PÉDAGOGIQUES

- Appréhender les enjeux de la cybersécurité dans la production industrielle (manufacturing, production et distribution d'énergie, traitement d'eau, etc.)
- Identifier les menaces sur les systèmes de contrôle-commande industriels
- Évaluer, vérifier et valider le niveau de sécurité
- Mettre en œuvre des solutions afin d'éviter les intrusions extérieures, déjouer les cyberattaques
- Fournir un socle de connaissances aux automaticiens afin de leur permettre de travailler en collaboration avec les informaticiens

OBJECTIFS PÉDAGOGIQUES

- Appréhender les enjeux de la cybersécurité dans la production industrielle (manufacturing, production et distribution d'énergie, traitement d'eau, etc.)
- Identifier les menaces sur les systèmes de contrôle-commande industriels
- Évaluer, vérifier et valider le niveau de sécurité
- Mettre en œuvre des solutions afin d'éviter les intrusions extérieures, déjouer les cyberattaques
- Fournir un socle de connaissances aux automaticiens afin de leur permettre de travailler en collaboration avec les informaticiens

97,2%
de clients satisfaits*
* enquête réalisée auprès de nos clients en septembre 2025

CONTENU

Cette formation est à destination de 2 publics, le profil « automaticien » et le profil « informaticien ».

La formation permet à un public d'automaticiens et d'informaticiens :

- d'appréhender les apports et enjeux de chaque métiers sur des projets relatifs à la cybersécurité d'installations industrielles,
- d'acquérir les bases de la cybersécurité des systèmes industriels,
- ainsi qu'un vocabulaire commun leur permettant de travailler ensemble

La première journée est spécifique à chaque profil.

Les stagiaires sont ensuite réunis en un seul groupe afin d'initier des échanges et des collaborations.

MODULE OT (1 jour)

L'objectif essentiel de ce module est de donner les connaissances nécessaires pour appréhender la sécurité de la sécurité des systèmes d'information (SSI) à un public d'automaticiens.

Des TP sont réalisés tout au long de la journée

- Définitions de la cybersécurité/SSI et principaux concepts
- Enjeux de la cybersécurité/SSI
- Catégories d'attaques (DDOS, Advanced Persistent Threat (APT), Vers, MITM, spoofing, ingénierie sociale, détournement de sessions, etc.) et modes opératoires
- Exemples d'attaques
- Grands principes de déploiement d'un projet cybersécurité
- Connaître les bonnes pratiques
- Panorama des normes et standards
- Introduction à la Cryptographie

MODULE PRINCIPAL (2 jours)

1 ½ journée cours théorique – ½ journée de TP

- Enjeux de la cybersécurité industrielle
- État des lieux et historique
- Dualité Sûreté De Fonctionnement (SDF) et cybersécurité industrielle
- Exemples d'incidents sur les systèmes industriels
- Les vulnérabilités et vecteurs d'attaques classiques
- Panorama des normes et standards
- En France, la Loi de Programmation Militaire (LPM)
- Le projet de cybersécurité du système industriel
- Les recommandations de l'Agence Nationale de la Sécurité des Systèmes d'Informations (ANSSI)
- Etat des lieux des équipements et produits de cybersécurité : apports et limites
- Exercices et travaux pratiques

ÉQUIPE PÉDAGOGIQUE

Enseignants/chercheurs du laboratoire AMPERE de l'INSA Lyon spécialistes du milieu industriel et experts publics et privés en cybersécurité OT et IT.

MOYENS ET MÉTHODES PÉDAGOGIQUES

Cours - Travaux Pratiques - Exercices - Etude de cas et Echanges avec des experts publics et privés du domaine Un support de cours sera remis à chacun des participants.

PROCHAINE SESSION

VILLEURBANNE : DU 06/07/2027 AU 08/07/2027

Frais pédagogiques individuels : 2 415 € H.T. (* Repas inclus)

L'ouverture de la session est conditionnée par un nombre minimum de participants. Nous consulter pour d'autres dates.

ÉVALUATION ET RÉSULTATS

Évaluation des acquis de la formation

Evaluation des acquis des apprenants par auto-examen. 95.4% des apprenants ont acquis la compétence principale visée. (sur 215 apprenants évalués sur cette thématique depuis 2020)

Évaluation de la satisfaction des participants en fin de formation (Niveau 1 KIRKPATRICK)

4.4 par les participants. (sur 244 participants ayant suivi une formation dans la thématique depuis 2020)

RENSEIGNEMENTS ET INSCRIPTION
Tel : +33 (0)4 72 43 83 93
Fax : +33 (0)4 72 44 34 24
mail : formation@insavalor.fr
Préinscription sur formation.insavalor.fr

Accueil des personnes en situation de handicap nécessitant un besoin spécifique d'accompagnement : nous contacter à l'inscription. Nos locaux sont accessibles aux personnes à mobilité réduite.

Actualisée le 19/06/2026