

LE STANDARD ISO 21434:2021 ET L'HOMOLOGATION

Réalisable en présentiel ou à distance (FOAD)

Type	Référence	Durée	Tarif HT
INTER	1.01.04.0006	3 jours (21 h)	2 450 €
INTRA	2.01.04.0006	3 jours (21 h)	5 400 € *

* forfait pour 6 pers max

DESCRIPTIF DE LA FORMATION

L'objectif de cette formation est de donner aux participants une vue détaillée du standard ISO 21434:2021. Cette formation présente de manière détaillée les principes fondamentaux de la démarche d'ingénierie de la cybersécurité applicable aux véhicules routiers devant satisfaire les prescriptions uniformes spécifiées par le règlement ONU No. 155.

OBJECTIFS PÉDAGOGIQUES

A l'issue de la formation, l'apprenant sera capable de :

- ▶ Connaître les dispositions organisationnelles relatives au système de gestion de la cybersécurité (CSMS),
- ▶ Adapter les activités d'ingénierie de la cybersécurité relatives aux projets incluant les activités distribuées (e.g., fournisseurs),
- ▶ Organiser et appliquer la démarche d'analyse des risques relatifs à la cybersécurité (TARA) sur les systèmes embarqués du secteur automobile de sorte à en spécifier des objectifs de cybersécurité,
- ▶ Implémenter ces objectifs lors des activités de développement.

PROGRAMME

- ▶ **Introduction aux enjeux de la cybersécurité**
- ▶ **Contexte normatif**
Positionnement du standard ISO 21434:2021 dans le contexte des prescriptions du règlement ONU R. 155
- ▶ **Présentation détaillée du standard ISO 21434:2021 et du R.155**
Principes généraux / Notions & Définitions / Organisation
- ▶ **Gestion organisationnelle du cycle de vie de la cybersécurité**
Gouvernance & Culture / Gestion de l'information / Système de gestion (CSMS) / Gestion des outils
- ▶ **Gestion de la cybersécurité relative aux projets**
Planification & Adaptation des activités / Réutilisation, composants non contextuels, COTS / Dossier de cybersécurité / Evaluations des risques & Transition vers la production
- ▶ **Activités de cybersécurité distribuées**
- ▶ **Activités de cybersécurité continues**
Surveillance, Gestion des événements & Prescriptions réglementaires (R.155) / Analyse et Gestion des vulnérabilités
- ▶ **Phase de projet (Concept)**
Définition de l'article (*Item*) / Concept de cybersécurité
- ▶ **Phase de développement du produit**
Spécifications de cybersécurité / Intégration & Vérification
- ▶ **Validation de la cybersécurité & Production, Utilisation, Maintenance & Démantèlement**
- ▶ **Analyse des menaces et évaluation des risques (TARA)**
Apprentissage des étapes du processus par un exemple.

INFORMATIONS UTILES

Public concerné

Cette formation s'adresse aux Responsables de services d'ingénierie (R&D), Responsables qualité, Chefs de projet, Ingénieurs de développement, Ingénieurs de tests, Ingénieurs sûreté de fonctionnement (incl. Sécurité fonctionnelle) du secteur automobile.

Prérequis

Connaissance des démarches d'ingénierie des systèmes embarqués et/ou développement logiciels.

Moyens pédagogiques, techniques et d'encadrement

Un support de cours est remis à chaque apprenant. Le déroulé pédagogique de la session liste les méthodes retenues.

Modalités de suivi du stagiaire

Questionnaire d'entrée, quiz de milieu de formation, questionnaire de sortie et un questionnaire de satisfaction.

Délai d'accès

Groupe constitué en fonction de la demande, maximum 4 semaines avant le début de la session.

Accueil situation de handicap

Notre offre de formation est accessible à tous. En cas de situation de handicap nécessitant un aménagement particulier, vous pouvez joindre notre **Correspondant Handicap** au :
Tél : 05 61 30 69 00 Email : formation@isit.fr

Plusieurs formats de formations possibles, veuillez nous contacter.