



Comprendre les exigences de l'ISO/SAE 21434 et définir les moyens pour y répondre (Niveau 2)

Délais d'accès à la formation : entre 1 et 3 mois (délais de planification).

Modalités d'inscription : renvoyer le bulletin d'inscription complété, nous contacter pour toute demande d'inscription.

Pour les formations INTRA, au moins un entretien téléphonique préliminaire sera réalisé.

CYBERSECURITE - SOFTWARE



OBJECTIFS

A l'issue de cette formation, les stagiaires seront capables de réaliser un diagnostic pour son organisation, de définir et identifier un plan d'action pour répondre aux exigences de la norme.

PUBLIC VISÉ

Constructeurs, Equipementiers, Ingénieristes, Prestataires de services connectés, Fournisseurs de composants électroniques/logiciels, Collectivités, Fournisseurs de services de mobilité, Service Qualité, Homologation, Conception, R&D, BE,

PRÉ REQUIS

Connaitre l'approche processus et les processus du système de management de son organisation ou avoir suivi la formation 308.1 (Niveau 1)



OBJECTIFS PÉDAGOGIQUES

- Préparer les livrables pour les constructeurs automobiles en vue de l'homologation UNR 155
- Définir ou adapter les processus en place dans le système de management de l'entreprise pour intégrer les exigences de l'ISO/SAE 21434 (cybersécurité automobile) et l'analyse des risques

MÉTHODES ET MOYENS PÉDAGOGIQUES

Présentation théoriques, analyse de son organisation, échanges avec le formateur.
Remise d'une documentation pédagogique numérique pendant le stage.

QUALIFICATION INTERVENANT(E)(S)

Expert Système management qualité (IATF 16949) et en cybersécurité

PARCOURS PÉDAGOGIQUE

Rappel du contexte réglementaire en cybersécurité automobile, de l'environnement et des besoins actuels

Rappel des principales exigences "cybersécurité" automobile

Comprendre la cybersécurité et les risques associés

Définition des objectifs de cybersécurité : Concept et activités amonts de cybersécurité

L'analyse de risques

Identifier et gérer les risques organisationnels et produits /Surveiller les risques de cybersécurité durant tout le cycle de vie

Qualifier et traiter les risques et les scénarios/Mettre en place des actions préventives et correctives

Analyse des exigences techniques selon le cycle de vie :Clarification des exigences cybersécurité

Analyse des exigences organisationnelles

Revue et étude des exigences de chaque chapitre (Chap. 5 à 8)

Parrallèle avec les normes ISO 9001 ou IATF 16949 et les processus d'un système de management de la qualité existant au sein d'une entreprise

Analyse avec les stagiaires des solutions/documentation pouvant être mises en place pour répondre aux exigences de la norme / Elaboration



MÉTHODES ET MODALITÉS D'ÉVALUATION

Evaluation individuelle des connaissances en fin de formation.

MODALITÉS D'ACCESSIBILITÉ

Personne en situation de handicap, nous contacter pour échanger sur vos éventuels besoins d'aménagement à prévoir. Référent handicap : christelle.auger@utac.com



Comprendre les exigences de l'ISO/SAE 21434 et définir les moyens pour y répondre (Niveau 2)



14.00 Heures
2 Jours



De 4 à 12 Personnes



Intra (par jour) : Nous consulter
Inter (par stagiaire) : 1 697.00 €



Contactez-nous !

Audrey RISSOT
Chargée de formation

Tél. : 0169801708
Mail : audrey.rissot@utacceram.com

Janvier 2026
Version : 3082-20260217

