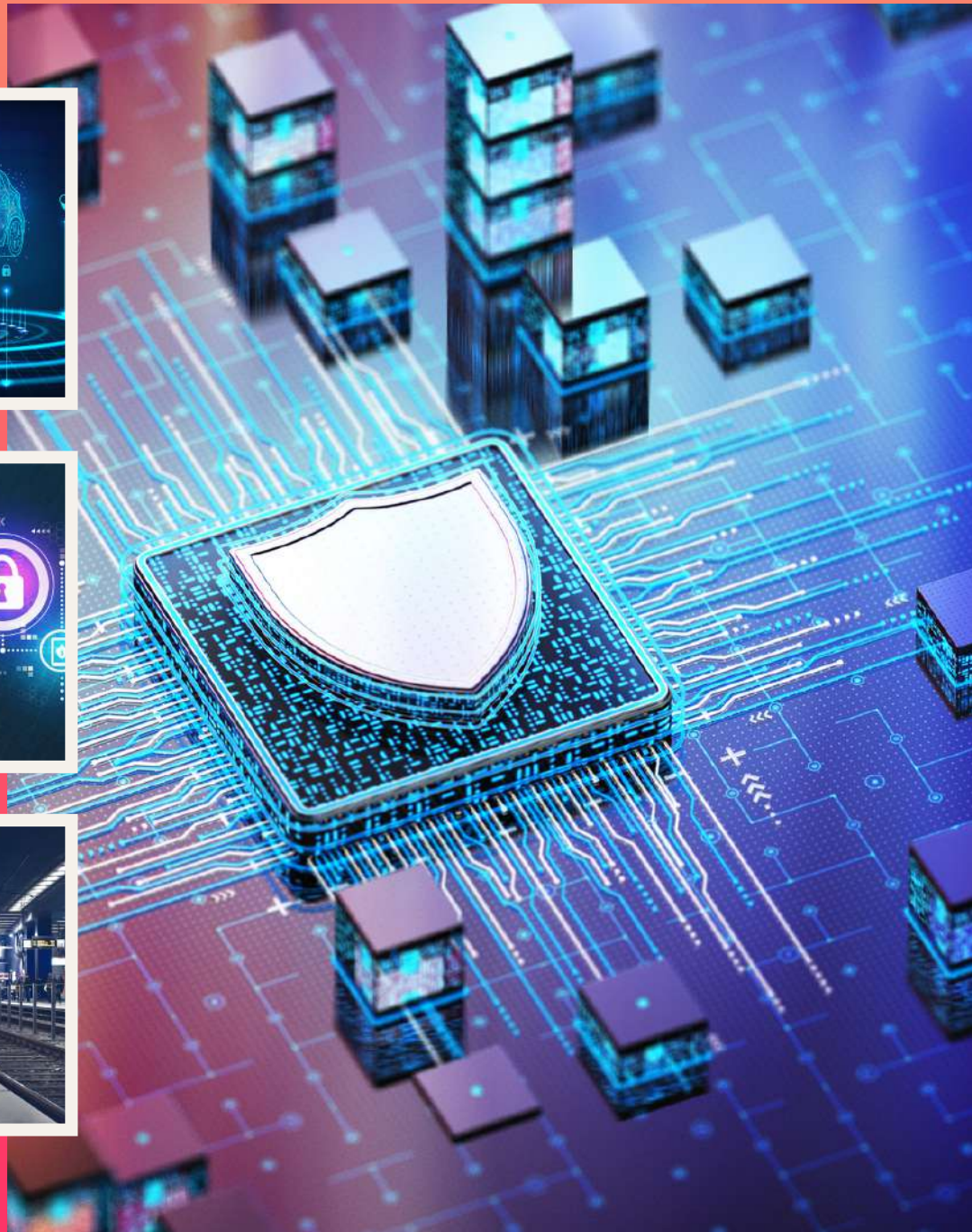


SECURE YOUR FUTURE



SERMA ACADEMY

CATALOGUE DE FORMATIONS 2024

À PROPOS DU GROUPE SERMA

Créé en 1991, le Groupe SERMA est un expert français et indépendant, interlocuteur unique pour les enjeux de fiabilité et de sécurité des produits, systèmes et données. Spécialisé dans les secteurs à forte contrainte d'environnement, SERMA se caractérise par sa culture d'excellence technique et son réseau d'experts.

Expert des technologies de l'Électronique, de l'Énergie, de la Cybersécurité et des Télécoms.

Au travers de ses différentes filiales, le Groupe SERMA intervient tout au long du cycle de vie des produits : depuis les phases de R&D et conception jusqu'au maintien en conditions opérationnelles. Le Groupe dispose de plusieurs laboratoires d'expertise électronique, matériaux et cybersécurité, de bureaux d'études et de différentes plateformes de test (composants, cartes, équipements, électroniques de puissance, moteurs électriques, batteries, sécurité).

Avec 1300 collaborateurs et près de 10 000 expertises par an conduites dans nos laboratoires, SERMA est un expert reconnu auprès de nombreux grands comptes, tous secteurs d'activité confondus.

Le Groupe s'est développé grâce à de nombreux investissements, tant en moyens qu'en croissances externes, dans les domaines de l'audit, du conseil, du design, du test, de l'expertise et plus largement de la compréhension des technologies.



Découvrez SERMA en vidéo !

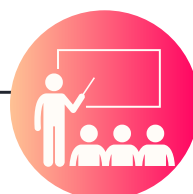


NOS FORMATIONS

SERMA vous accompagne dans le renforcement et le développement de vos savoir-faire et ceux de vos équipes.



500
stagiaires
formés
chaque année



Près de
100
formations
dispensées
chaque année



Plus de
40
formations au
catalogue



25
experts
formateurs

Qualiopi
processus certifié
RÉPUBLIQUE FRANÇAISE

Nos formations sont
certifiées Qualiopi

Nos formations professionnelles sont disponibles en **présentiel** et **à distance** : cours pratiques ou théoriques, prédéfinis, personnalisés, **inter ou intra-entreprises**, en français ou en anglais, nos formations sont assurées par nos équipes dont l'expérience quotidienne du terrain dans tous les secteurs d'activité en font des référents dans leurs domaines respectifs.



INTER-ENTREPRISE

Nous sommes à votre écoute pour mettre en place des **formations adaptées à vos besoins** en termes de date, de lieu, de programme ou de contenu.



INTRA-ENTREPRISE

Les sessions planifiées dans notre catalogue et **dispensées dans toute la France**.



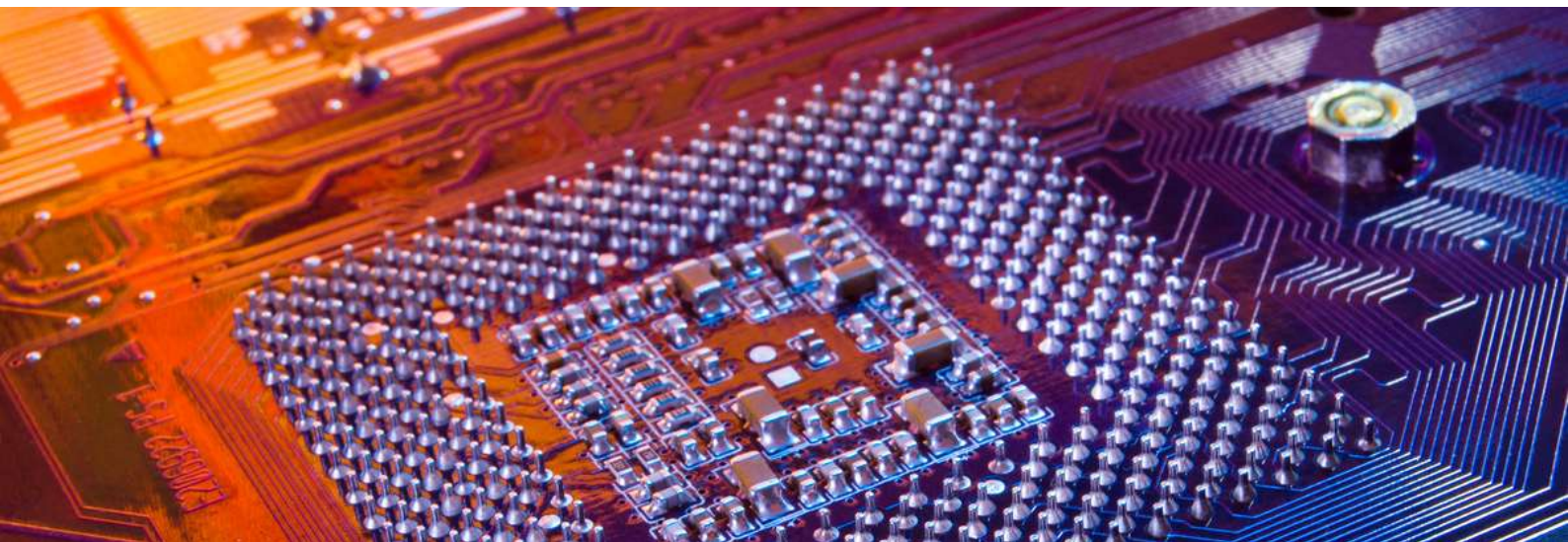
À DISTANCE

En direct ou préenregistrées, les formations en ligne sont disponibles pour les formations se déroulant sur 1 à 2 jours maximum.



SUR MESURE

Nous vous accompagnons dans la transformation de votre entreprise en créant avec vous **des solutions au plus près de vos besoins**.





Nos sites de formation

Nos formations prévues au catalogue en inter-entreprises se déroulent dans nos différents locaux partout en France.

Les formations en intra ou sur mesure peuvent avoir lieu dans vos locaux et partout en France et dans le monde.

Conditions et modalités d'inscription

SERMA Technologies est enregistrée sous le numéro 75 33 11 38 933.
Cet enregistrement ne vaut pas agrément de l'état.

Les demandes d'inscriptions et de renseignements peuvent être effectuées auprès de Gwenola BOIREAU :

- **Par téléphone** : +33 (0)5 57 26 29 92
- **Par email** : formation@serma.com
- **Sur notre site Internet** <https://www.serma.com/formation-serma/formations-et-sensibilisations/>

L'inscription devient définitive dès réception de la convention, après le délai légal de rétractation de 10 jours et au moins 15 jours avant la date de formation prévue.

Les frais d'inscriptions incluent l'accès d'une personne au stage, les supports documentaires et les déjeuners et pauses café.

Les frais d'inscriptions excluent les frais de déplacement et les frais liés à l'hébergement des stagiaires.

L'inscription à l'une de nos formations implique l'acceptation de l'ensemble des conditions et du règlement. Aucun accord verbal non confirmé par courrier ne pourra être pris en considération.

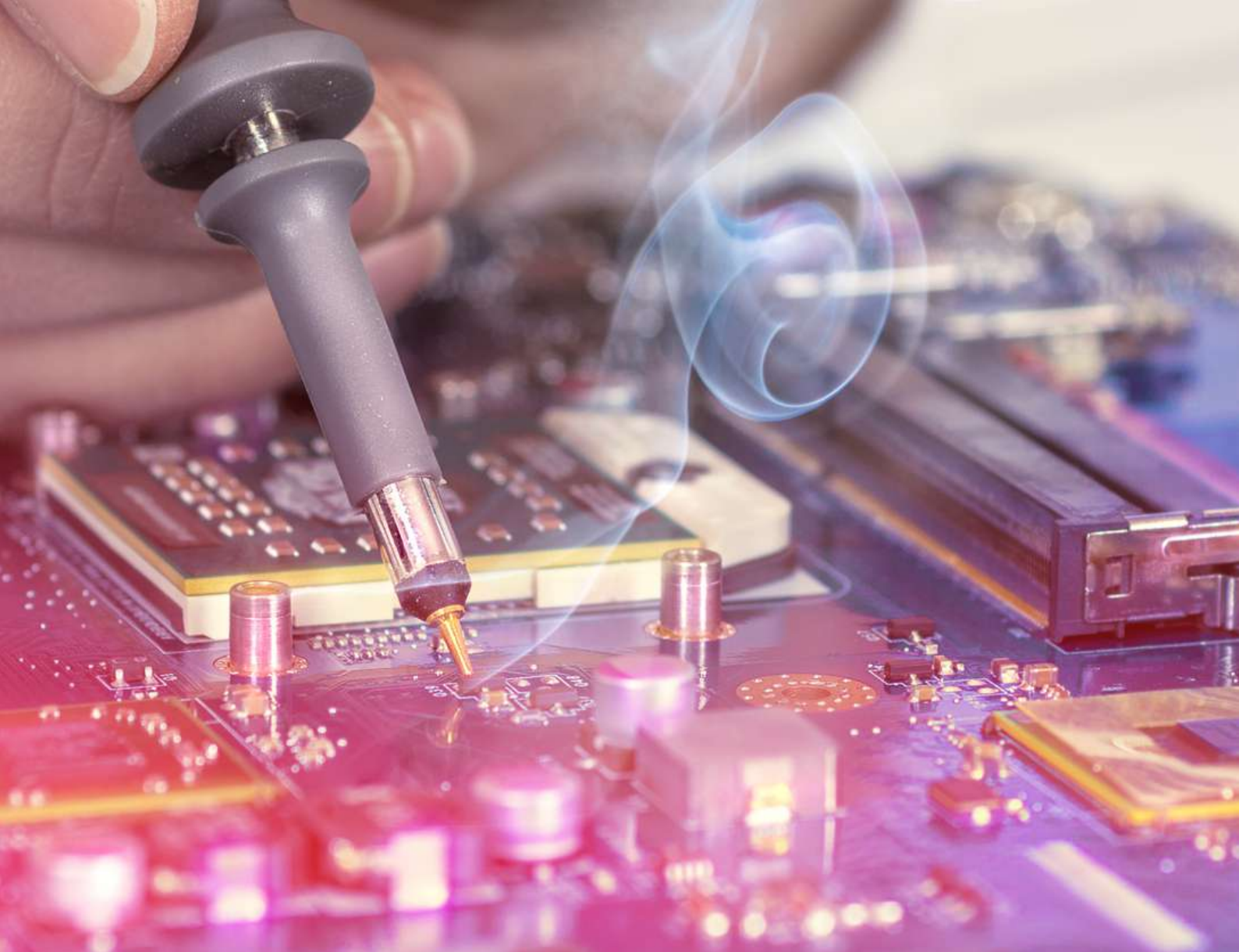
Conditions de règlement

- **Par chèque** : d'un montant total TTC indiqué sur la facture à l'ordre de SERMA Technologies
- **Par virement bancaire** :

Banque	Guichet	N° de compte	Clé	Devise
10 057	19012	003886501	80	EUR

Accessibilité

Pour toute demande ou information handicap, merci de vous adresser à Gwenola BOIREAU : formation@serma.com, +33 (0)5 57 26 29 92.



Report de formation

Dans le cas où le quorum ne serait pas atteint et afin de préserver un meilleur équilibre dans l'organisation des groupes, SERMA se réserve le droit de reporter une session au plus tard 2 semaines avant la date de démarrage de celle-ci.

Annulation d'une session :

- Du fait de SERMA Technologies : En dehors d'un cas de report de formation, SERMA Technologies s'engage à rembourser les sommes déjà perçues.
- Du fait du stagiaire : Toute annulation d'inscription non parvenue à SERMA Technologies par écrit au plus tard 10 jours avant le début de la session entraîne le paiement d'un dédommagement de 30% du montant du stage (TVA au taux en vigueur).


Un participant peut se faire remplacer sur la même session par une autre personne du même établissement à tout moment, sans frais supplémentaires, à condition de prévenir de ce remplacement avant le début du stage.



Restez informés

Retrouvez l'ensemble de nos formations sur notre **site Internet** :

<http://www.serma.com/formations>

Pour vous tenir informée de nos actualités et ne rater aucune formation, **suivez-nous sur** .

SOMMAIRE

CYBERSÉCURITÉ

Cybersécurité et conformité IoT – Directive RED*	1
Cybersécurité et conformité automobile – UN R155 & ISO 21 434*	3
Cybersécurité et conformité ferroviaire TS 50 701*	5
Cybersécurité des systèmes embarqués et des objets connectés*	8
Cybersécurité des applications WEB OWASP Top 10:2021*	11
Cybersécurité des systèmes industriels IEC 62 443*	14

SÛRETÉ DE FONCTIONNEMENT

Sûreté de fonctionnement des systèmes et matériels (CEI 61508-1 & 2)	18
Sûreté de fonctionnement des logiciels embarqués (CEI 61508-3)	20
Sensibilisation à la sécurité fonctionnelle des systèmes électroniques (CEI 61508-1 & 2)	23
Sensibilisation à la sûreté de fonctionnement des logiciels embarqués (CEI 61508-3)	25
Norme ISO 26262 – Sécurité fonctionnelle – Véhicules routiers	27
Formation aux normes EN 50126 & 50129 « Sûreté de fonctionnement ferroviaire »	30
Formation aux normes EN 50128/ EN 50657 – Logiciels du ferroviaire	32
Sensibilisation aux normes EN 50128/ EN 50657 – Logiciels du ferroviaire	35
Sensibilisation au système de management de la qualité pour les dispositifs médicaux ISO 13485:2016	37
Sensibilisation à la norme CEI 62304 – Logiciels de dispositifs médicaux	39
AMDEC en conception électronique	41
Sûreté de fonctionnement des électroniques (Hardware)	43

CYBERSÉCURITÉ ET CONFORMITÉ IOT DIRECTIVE RED

Introduction à la cybersécurité et application de l'ETSI EN 303 645.



1

DATES & LIEUX

- 23 et 24 janv. – Distanciel
- 9 et 10 avril. – Distanciel
- 4 et 5 juin. – Distanciel
- 24 et 25 sept.- Paris
- 12 et 13 nov. – Distanciel
- 11 et 12 dec. – Distanciel

DURÉE

- 2 jours

TARIF

1 800€

LANGUES



PRÉREQUIS

Aucune expérience en cybersécurité nécessaire. Néanmoins des connaissances sur les réseaux et les architectures d'objets connectés sont souhaitables.

Si en distanciel :

- Un accès internet stable via Ethernet ou Wi-Fi avec un débit correct (1.2 Mb/s en débit descendant minimum est recommandé)
- Un PC / MAC avec l'outil Teams d'installé ainsi qu'un accès non restreint à internet.

PUBLIC CONCERNÉ

Cette formation vise les personnes travaillant dans le milieu des objets connectés et notamment celles qui participent à des projets devant être en conformité avec la nouvelle directive RED. Elle peut être dispensée à un public sans première connaissance de la cybersécurité.

OBJECTIF

L'objectif de cette formation est dans un premier temps d'inculquer les bases et principes fondamentaux de la cybersécurité pour ensuite présenter la norme ETSI EN 303 645, son guide d'implémentation ETSI TR 103 621 et la méthodologie d'évaluation ETSI TS 103 701 afin de vous préparer au mieux à la certification de votre produit.

FORMATEUR

Expert en cybersécurité IoT et embarqué.

MODALITÉS PÉDAGOGIQUES

- Présentation PowerPoint projetée (support en français)
- Plateforme web interactive (Klaxoon)

MODALITÉS D'ÉVALUATION

Evaluation en début et fin de formation, quizz...

DÉLAI D'INSCRIPTION

5 jours ouvrés avant le début de la formation (si financement OPCO).

SANCTION

Une attestation de formation conforme aux dispositions de l'Article L. 6353-1 alinéa 2 remise au stagiaire.

PROGRAMME ↓

PROGRAMME

INTRODUCTION À LA CYBERSÉCURITÉ

- Pourquoi la cybersécurité ?
- « Internet of Things »
- TP : Définir l'architecture d'une serrure biométrique connectée

FONDAMENTAUX DE LA CYBERSÉCURITÉ

- La triforme des critères de protection
- Nouvelles technologies, nouvelles menaces.

LE RISQUE EN CYBERSÉCURITÉ

- Marché de la cybersécurité
- Les mécanismes de sécurité
- TP : Définir la surface d'attaque d'une serrure biométrique connectée

CYBERSÉCURITÉ DÈS LA CONCEPTION

- Etude de cas
- 12 principes de cybersécurité

LA DIRECTIVE RED

- Aspects légaux, réglementaires et normatifs
- La protection des réseaux 3(3)(d)
- La protection des données personnelles et de la vie privée 3(3)(e)
- La protection contre la fraude 3(3)(f)
- TP : Identifier les vulnérabilités potentielles d'une serrure biométrique connectée

LA NORME ETSI EN 303 645

- Périmètre d'application
- Les 13+1 exigences de la norme
- TP : Définir les dispositions s'appliquant à une serrure biométrique connectée

LE GUIDE D'IMPLEMENTATION ETSI TR 103 621

- Analyse de risque et évaluation de la sécurité
- Cycle de développement de la sécurité des produits (SDLC)
- Les implémentations proposées

LES SPÉCIFICATIONS D'ÉVALUATION ETSI TS 103 701

- Fonctionnement de l'évaluation
- Implémentation Conformance Statement (ICS)
- Implémentation eXtra Information for Testing (IXIT)
- TP : Préparer le dossier d'évaluation d'une serrure biométrique connectée

POUR ALLER PLUS LOIN

- NIST 8425
- Certification ioXt
- Evaluation GSMA
- Schéma PSA Certified
- Schéma SESIP

CYBERSÉCURITÉ ET CONFORMITÉ AUTOMOBILE - UN R155 & ISO 21 434

Comprendre les enjeux pour mieux l'implémenter.

3



DATES & LIEUX

- 11 et 12 juin. – Distanciel
- 17 et 18 sept. – Distanciel
- 26 et 27 nov. – Distanciel
- 17 et 18 dec. – Distanciel

DURÉE

- 2 jours

TARIF

1800€

LANGUES



PRÉREQUIS

Aucune expérience en sécurité embarquée nécessaire. Néanmoins des notions sur les infrastructures automobiles sont souhaitables.

Si en distanciel :

- Un accès internet stable via Ethernet ou Wi-Fi avec un débit correct (1.2 Mb/s en débit descendant minimum est recommandé).
- Un PC / MAC avec l'outil Teams d'installé ainsi qu'un accès non restreint à internet.

PUBLIC CONCERNÉ

Cette formation cible les personnes intéressées par les problématiques de cybersécurité liées au domaine automobile. Elle s'adresse aux professionnels intervenants sur une ou plusieurs étapes du cycle de vie des systèmes automobiles mais aussi aux développeurs, architectes, intégrateurs, concepteurs, chefs de projet ou la direction du domaine.

OBJECTIFS

Cette formation vise à comprendre comment mener à bien une politique de sécurité cohérente et efficace dans le domaine automobile. L'objectif est de comprendre et se sensibiliser au travers de la réglementation n° 155 de l'ONU et de la norme ISO/SAE 21434 ce qu'est :

- Une politique de cyber sécurité, les règles et processus spécifiques
- L'instauration et le maintien d'une culture cyber sécurité (amélioration continue)
- La gestion et l'évaluation du risque
- L'intégration de la cyber sécurité au sein des phases du cycle de vie

FORMATEUR

Expert en cybersécurité automobile.

MODALITÉS PÉDAGOGIQUES

- Présentation PowerPoint projetée (support en français)
- Plateforme Web interactive (Klaxoon)

MODALITÉS D'ÉVALUATION

Evaluation en début et fin de formation, quizz...

DÉLAI D'INSCRIPTION

5 jours ouvrés avant le début de la formation (si financement OPCO).

SANCTION

Une attestation de formation conforme aux dispositions de l'Article L. 6353-1 alinéa 2 remise au stagiaire.

PROGRAMME ↓

PROGRAMME

CONTEXTE DE LA CYBERSÉCURITÉ

- Définitions
- Revue du contexte
- Réseaux des véhicules
- La surface d'attaque
- Aspects légaux/réglementaires
- Protéger les données
- Critères de protections
- Sûreté & Cybersécurité
- Nouvelles technologies

FONDAMENTAUX DE LA CYBERSÉCURITÉ

- Le risque en cybersécurité
- Marché de la cybersécurité
- Cybersécurité dès la conception

LA RÉGLEMENTATION N° 155 DE L'ONU

- Périmètre
- Demande d'homologation
- Mise en place d'un CSMS
- Supply chain

LA NORME ISO/SAR 21 434

- Introduction / Définitions
- Gestion CS organisationnelle
- Gestion CS sur projet
- Activités distribuées de la CS
- Activités de CS continues
- Phase de concept
- Analyse de risque
- Développement du produit
- Validation de la CS
- Production
- Opération et maintenance
- Décommissionnement

CYBERSÉCURITÉ ET CONFORMITÉ FERROVIAIRE - TS 50701

Comprendre les enjeux pour mieux l'implémenter.



DATES & LIEUX

- 4 et 5 juin. - Distanciel
- 8 et 9 oct. - Distanciel
- 6 et 7 nov. - Distanciel

DURÉE

- 2 jours

TARIF

1800€

LANGUES



PRÉREQUIS

Aucune expérience en sécurité embarquée nécessaire. Néanmoins des notions sur les infrastructures automobiles sont souhaitables.

Si en distanciel :

- Un accès internet stable via Ethernet ou Wi-Fi avec un débit correct (1.2 Mb/s en débit descendant minimum est recommandé).
- Un PC / MAC avec l'outil Teams d'installé ainsi qu'un accès non restreint à internet.

PUBLIC CONCERNÉ

Cette formation vise les personnes travaillant dans le milieu ferroviaire et notamment celles qui participent à des projets incluant des aspects numériques et des systèmes de traitement automatisé de la donnée. Elle peut être dispensée à un public sans première connaissance de la cybersécurité ou venant du monde de la sécurité ferroviaire.

OBJECTIF

L'objectif de cette formation est dans un premier temps d'inculquer les bases et principes fondamentaux de la cybersécurité pour ensuite dérouler la Spécification Technique 50701 propre à la cybersécurité dans les projets ferroviaires.

FORMATEUR

Expert en cybersécurité ferroviaire.

MODALITÉS PÉDAGOGIQUES

- Présentation PowerPoint projetée (support en anglais)
- Plateforme web interactive (Klaxoon)

MODALITÉS D'ÉVALUATION

Evaluation en début et fin de formation, quizz...

DÉLAI D'INSCRIPTION

5 jours ouvrés avant le début de la formation (si financement OPCO).

SANCTION

Une attestation de formation conforme aux dispositions de l'Article L. 6353-1 alinéa 2 remise au stagiaire.

PROGRAMME 

PROGRAMME

INTRODUCTION À LA CYBERSÉCURITÉ

- Vocabulaire et définition
- Comprendre le besoin et son évolution au fil du temps
- La notion de « surface d'attaque »

ASPECTS LÉGAUX, RÉGLEMENTAIRES ET NORMATIFS

- Les différents organismes
- Directive NIS 2
- Initiatives au niveau européen et international

FONDAMENTAUX DE LA CYBERSÉCURITÉ

- Sécurité, sûreté et cybersécurité
- Comment protéger la donnée
- Valeur de nos données

LE RISQUE EN CYBERSÉCURITÉ

- Définitions et concepts
- Nouvelles technologies, nouvelles menaces
- L'analyse de risque

LE MARCHÉ DE LA CYBERSÉCURITÉ

- Le prix des données
- Bug bounty

CYBERSÉCURITÉ DÈS LA CONCEPTION

- Etude de cas
- 12 principes de cybersécurité

LA NORME TS 50701

- La TS 50701, quoi, qui, comment ?
- Modélisation et cartographie
- Cycle de vie d'un système
- Activités de cybersécurité durant un cycle de vie cybersécurité
 - Concept
 - Définition d'un système
 - Analyse de risque simple et détaillée
 - Spécifications
 - Architecture de cybersécurité
 - Intégration
 - Validation & Acceptation
 - Opération, maintenance et surveillance
 - Décommissionnement

CYBERSECURITÉ DES SYSTÈMES EMBARQUÉS ET DES OBJETS CONNECTÉS

Comprendre les attaques hardware/software et comment s'en prémunir



DATES & LIEUX

- 14 au 16 mai – Paris
- 10 au 12 sept. – Courbevoie
- 8 au 10 oct. – Pessac
- 22 au 24 oct. – Lyon
- 3 au 5 dec. – Nancy

DURÉE

- 3 jours

TARIF

2 700€

LANGUES



PRÉREQUIS

Aucune expérience en sécurité informatique nécessaire. Néanmoins quelques notions en électronique ou logiciel embarqué sont souhaitables. Matériel Fourni : Le matériel électronique et informatique nécessaires pour les exercices seront fournis aux participants sur place :

- Ecran Full HD avec port HDMI
- Clavier, souris
- Raspberry Pi pré-préparé
- Hardsplit avec sa carte d'entraînement
- Outils d'analyse radio...

PUBLIC CONCERNÉ

Cette formation cible les personnes intéressées par les aspects de sécurité liés au hardware ou à l'embarqué. Les amateurs ou professionnels en électronique ainsi que les professionnels de la sécurité IT (développeur, architecte, intégrateur, concepteur hardware, chef de projet).

OBJECTIF

Cette formation vise à comprendre les faiblesses de sécurité des systèmes embarqués, maîtriser les techniques d'attaque utilisées par les pirates pour savoir comment limiter les impacts, apprendre à sécuriser les systèmes embarqués dès les phases de conception et comprendre les vulnérabilités pour pouvoir ensuite limiter les risques.

FORMATEUR

Expert en cybersécurité embarqué.

MODALITÉS PÉDAGOGIQUES

- Présentation PowerPoint projetée (support en anglais)
- Utilisation de l'outil de tests IoT Hardsplit pour la réalisation d'un exercice de tests d'intrusion matériel
- Plateforme Web interactive (Klaxoon)
- Scénario pratique d'attaque / défense d'un mini - drone

MODALITÉS D'ÉVALUATION

Evaluation en début et fin de formation, quizz...

DÉLAI D'INSCRIPTION

5 jours ouvrés avant le début de la formation (si financement OPCO).

SANCTION

Une attestation de formation conforme aux dispositions de l'Article L. 6353-1 alinéa 2 remise au stagiaire.

PROGRAMME ↓

PROGRAMME

COMPRENDRE LES BASES DU HARDWARE HACKING

- Comprendre le contexte historique des attaques sur les objets connectés
- Revoir les vulnérabilités et les aspects offensifs et défensifs
- Connaître les fondamentaux de l'électronique
- Réaliser la prise d'information sur une cible (fingerprint des composants)

COMMENT LES PIRATES ACCÈDENT AU HARDWARE ?

- Présenter des outils et méthodes disponibles pour auditer un produit
- Extraire des données sensibles avec les outils d'audit (HardSploit)
- Acquérir les signaux électroniques, outils et démonstration

COMMENT ACCÉDER AU LOGICIEL ?

- Présenter les différents types d'architecture (Microcontrôleur, FPGA), et les différents accès directs au logiciel via les interfaces d'entrée et sortie (JTAG / SWD, I2C, SPI, UART, RF bande ISM, etc.)
- Accéder au Firmware via différentes interfaces

ATTAQUES SUR UN SYSTÈME EMBARQUÉ PARTICULIER, L'OBJET CONNECTÉ (IOT)

- Réaliser un audit complet appliqué à notre système embarqué vulnérable :
 - Identifier les composants électroniques
 - Acquérir des signaux électroniques
 - Intercepter et analyser des signaux électroniques avec HardSploit
 - Modifier et extraire un firmware via les fonctions de debug JTAG avec HardSploit
 - Réaliser un fuzzing des interfaces externes pour détecter des vulnérabilités basiques sur l'embarqué
 - Exploiter des vulnérabilités (dépassement de mémoire tampon) durant un audit de sécurité hardware

COMMENT SÉCURISER VOTRE MATÉRIEL ?

- Découvrir la cryptographie et les différents moyens de sécuriser son système et ses communications
- Appréhender la conception sécurisée et la notion de cycles de développement (SDLC)
- Comprendre les meilleures pratiques de sécurité matérielle pour limiter les risques
- Limiter les accès JTAG et les vulnérabilités logicielles au niveau de l'embarqué

PIRATAGE AVEC LA TECHNOLOGIE SDR

- Apprendre la méthodologie d'audit SDR (capture, analyse, exploitation avec des logiciels radio)
- Utiliser des outils (GQRX, GNU Radio, etc.)
- Faire de la rétro-ingénierie d'un protocole sans fil à partir des émissions radio capturées dans les airs (communication sans fil d'un panneau à LED)

EXERCICE « CAPTURE THE DRONE »

- Présenter un scénario pratique d'attaque/défense d'un mini drone
- Défendre son drone et attaquer les autres en utilisant les outils et méthodes apprises au cours de la formation

CYBERSÉCURITÉ DES APPLICATIONS WEB OWASP TOP 10:2021

Découvrir les attaques populaires pour mieux s'en prémunir



DATES & LIEUX

- 18 et 19 juin. Distanciel
- 19 et 20 nov. - Rennes

DURÉE

- 2 jours

TARIF

1800€

LANGUES



PRÉREQUIS

Des connaissances en développement d'application web ainsi que des notions en informatique et réseau sont souhaitables.

Si en distanciel :

- Un accès internet stable via Ethernet ou Wi-Fi avec un débit correct (1.2 Mb/s en débit descendant minimum est recommandé)
- Un PC / MAC avec l'outil Teams d'installé ainsi qu'un accès non restreint à internet.

PUBLIC CONCERNÉ

Cette formation cible les personnes intéressées par les aspects de sécurité liés aux applications web. Les amateurs ou professionnels en développement ainsi que les professionnels de la sécurité IT (développeur, intégrateur, concepteur, chef de projet).

OBJECTIF

Cette formation vise à sensibiliser les équipes aux problématiques de développement sécurisé, transmettre aux collaborateurs les bonnes pratiques de développement sécurisé tout en présentant les risques liés aux mauvaises pratiques et apprendre à sécuriser votre code.

FORMATEUR

Expert en cybersécurité des applications web.

MODALITÉS PÉDAGOGIQUES

- Présentation PowerPoint projetée (support en français)
- Plateforme web interactive (Klaxoon)
- Scénarios pratiques d'attaque sur une application web vulnérable

MODALITÉS D'ÉVALUATION

Evaluation en début et fin de formation, quizz...

DÉLAI D'INSCRIPTION

5 jours ouvrés avant le début de la formation (si financement OPCO).

SANCTION

Une attestation de formation conforme aux dispositions de l'Article L. 6353-1 alinéa 2 remise au stagiaire.

PROGRAMME ↓

PROGRAMME

INTRODUCTION À LA CYBERSÉCURITÉ

- Vocabulaire et définition
- Comprendre le besoin et son évolution au fil du temps
- La notion de « surface d'attaque »

LES RÉFÉRENTIELS

- Présentation de l'OWASP Top 10
- Présentation de CWE Top 25

ECOSYSTÈME DES VULNÉRABILITÉS

- CVE : Common Vulnerability Enumeration
- CVSS : Common Vulnerability SCoring System
- Trouver et rapporter une vulnérabilité

A01:2021-CONTRÔLE D'ACCÈS DÉFAILLANT

- Présentation de la catégorie de vulnérabilité
- Exercice/Démo
- Remédiation/Outillage

A02:2021-DÉFAILLANCES CRYPTOGRAPHIQUES

- Présentation de la catégorie de vulnérabilité
- Exercice/Démo
- Remédiation/Outillage

A03:2021-INJECTION

- Présentation de la catégorie de vulnérabilité
- Exercice/Démo
- Remédiation/Outillage

A04:2021-CONCEPTION NON SÉCURISÉE

- Présentation de la catégorie de vulnérabilité
- Exercice/Démo
- Remédiation/Outillage

A05:2021-MAUVAISE CONFIGURATION DE SÉCURITÉ

- Présentation de la catégorie de vulnérabilité
- Exercice/Démo
- Remédiation/Outillage

A06:2021-COMPOSANTS VULNÉRABLES ET OBSOLÈTES

- Présentation de la catégorie de vulnérabilité
- Exercice/Démo
- Remédiation/Outillage

A07:2021-IDENTIFICATION ET AUTHENTIFICATION DÉFAILLANTE

- Présentation de la catégorie de vulnérabilité
- Exercice/Démo
- Remédiation/Outillage

A08:2021-MANQUE D'INTÉGRITÉ DES DONNÉES ET DU LOGICIEL

- Présentation de la catégorie de vulnérabilité
- Exercice/Démo
- Remédiation/Outillage

A09:2021-MANQUE DE SURVEILLANCE ET DE JOURNALISATION

- Présentation de la catégorie de vulnérabilité
- Exercice/Démo
- Remédiation/Outillage

A10:2021-FALSIFICATION DE REQUÊTE CÔTÉ SERVEUR

- Présentation de la catégorie de vulnérabilité
- Exercice/Démo
- Remédiation/Outillage

CYBERSÉCURITÉ DES SYSTÈMES INDUSTRIELS IEC-62443

Comprendre la norme afin de sécuriser son architecture

14



DATES & LIEUX

- 28 au 30 mai. – Paris
- 28 au 30 mai. – Nancy
- 25 au 27 juin. – Lyon
- 17 au 19 sept. – Courbevoie
- 22 au 24 oct. – Lyon
- 5 au 7 nov. – Toulouse
- 10 au 12 dec. – Nancy

DURÉE

- 3 jours

TARIF

2 700€

LANGUES



PRÉREQUIS

Aucune expérience en sécurité industrielle nécessaire. Néanmoins des connaissances en systèmes industriels ainsi que quelques notions en informatique, électronique, logiciel embarqué sont souhaitables.

- Un PC / MAC avec l'outil Teams d'installé ainsi qu'un accès non restreint à internet

Si en distanciel :

- Un accès internet stable via Ethernet ou Wi-Fi avec un débit correct (1.2 Mb/s en débit descendant minimum est recommandé)

PUBLIC CONCERNÉ

Cette formation cible les personnes intéressées par les aspects par les aspects de design d'architecture dans le milieu industriel. Les amateurs ou professionnels en électronique ainsi que les professionnels de la sécurité IT (développeur, architecte, intégrateur, concepteur hardware, chef de projet).

OBJECTIF

Cette formation vise à sensibiliser les architectes de systèmes et de produits aux préoccupations, problèmes, contraintes et défis en matière de cybersécurité qui peuvent avoir un impact sur leurs responsabilités actuelles, leurs livrables et leur travail quotidien.

FORMATEUR

Expert en cybersécurité industrielle.

MODALITÉS PÉDAGOGIQUES

- Présentation PowerPoint projetée (support en anglais)
- Plateforme web interactive (Klaxoon)
- Scénario pratique d'attaque / défense sur une mini usine connectée

MODALITÉS D'ÉVALUATION

Evaluation en début et fin de formation, quizz...

DÉLAI D'INSCRIPTION

5 jours ouvrés avant le début de la formation (si financement OPCO).

SANCTION

Une attestation de formation conforme aux dispositions de l'Article L. 6353-1 alinéa 2 remise au stagiaire.

PROGRAMME ↓

PROGRAMME

INTRODUCTION ET NORMES DE SÉCURITÉ

- Introduction avec des concepts clés et des différences entre les environnements IT et OT
- Panorama des menaces et analyse des risques liés à la cybersécurité industrielle
- Introduction à la norme IEC 62443 méthodologie et évaluation des risques
- Ateliers pratiques sur la définition d'un SuC (Système under consideration) et l'évaluation de risque selon la norme IEC 62443
- Concepts clés de la norme IEC 62443 (zones, conduits et méthodologies d'analyse de risque)
- Défense en profondeur et les différentes couches de sécurité (organisationnelle, physique, périmétrique)
- Démonstration : sécurité des systèmes d'accès, exemple avec la technologie Mifare

SÉCURITÉ RÉSEAU ET CRYPTOLOGIE

- Sécurité des systèmes et les principes de base de sécurité réseau
- Démonstration d'une attaque par force brute sur un réseau WPA2
- Introduction à la cryptologie : présentation des concepts clés (chiffrement symétrique et asymétrique, hash, sel et poivre)
- Démonstration exploitation d'une faille sur des fichiers Python précompilés contenant des secrets

SÉCURITÉ DES PRODUITS ET ARCHITECTURE SÉCURISÉE

- Cycle de vie sécurisé des logiciels (SDLC) et les bonnes pratiques pour le développement de logiciels sécurisés
- Sécurité des hôtes et des applications
- Démonstration des vulnérabilités affectant des ports USB mal protégés avec personnel non sensibilisé aux attaques provenant des dispositifs apparemment inoffensifs.
- Démonstration d'une attaque par rejeu mettant en œuvre des exploits sur un tableau d'affichage
- Sécurité des données
- Ateliers pratiques sur l'évaluation détaillée des risques, estimation des risques et définition des niveaux de sécurité selon la norme IEC 62443
- Méthodes pour identifier et traiter les vulnérabilités
- Présentation des bonnes pratiques pour concevoir une architecture robuste et sécurisée

PROGRAMME DÉTAILLÉ

JOUR 1

INTRODUCTION

- Présentation de SERMA

CYBERSÉCURITÉ DANS LE MONDE INDUSTRIEL

- Comprendre la cybersécurité dans le contexte industriel
- Menaces et méthodologies d'attaques
- Divergence et convergence IT / OT

NORME ISA/IEC 62443

- Comprendre les concepts de la norme
- Processus d'évaluation des risques
- Évaluation initiale des risques détaillés
- Acceptation et comparaison des risques

ATELIERS

- WS1 – Définir le système considéré
- WS2 – Effectuer l'évaluation initiale des risques
- WS3 – Partitionnement des Zones et conduits

JOUR 2

NORME ISA/IEC 62443

- Processus d'évaluation détaillée des risques

DÉFENSE EN PROFONDEUR

- Systèmes – Sécurité physique
- Systèmes – Sécurité périmétrique
- Systèmes – Sécurité interne des réseaux

DÉMONSTRATION

- Cas classique de Mifare
- Attaque par Brute force WPA2 et usurpation ARP
- Crypto : Mauvaise implémentation du chiffrement

CRYPTOGRAPHIE

- Symétrique et asymétrique
- Certificat et PKI (Infrastructure à clés publiques)
- Fonction de hachage avec "sel" et "poivre"

ATELIERS

- WS4 – Évaluation des risques détaillée (1/2) – Scénarios de menaces

JOUR 3

NORME ISA/IEC 62443

- Cycle de vie du développement d'un produit sécurisé
- Exigences fondamentales

DÉFENSE EN PROFONDEUR

- Produit – Sécurité de l'hôte
- Produit – Sécurité des applications
- Produit – Sécurité des données

DÉMONSTRATION

- Rubber Ducky – Attaque USB
- Radiofréquence – Attaque par rejeu

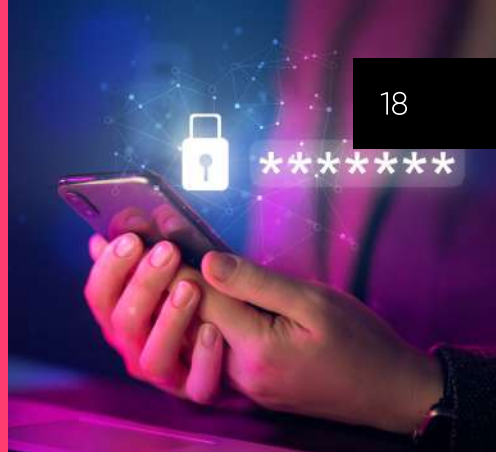
ATELIERS

- WS5 – Évaluation des risques détaillée (2/2) – Estimation des risques
- WS6 – Définition des niveaux de sécurité
- WS7 – Spécification des exigences de cybersécurité

DÉTAILS SUR LES VULNÉRABILITÉS

- MCS, CVE & CVSS

SÛRETÉ DE FONCTIONNEMENT DES SYSTÈMES ET MATÉRIELS (CEI 61508-1 & 2)



18

DATES & LIEUX

- 7 au 8 fev. - Pessac
- 14 au 15 mai - Toulouse
- 5 au 6 nov. - Aix-en-Provence

DURÉE

- 2 jours

TARIF

1460€

LANGUES



PRÉREQUIS

Aucun.

PUBLIC CONCERNÉ

Chef de projet, responsable qualité, concepteur système et matériel.

OBJECTIF

- Cerner les exigences normatives pour spécifier, définir l'architecture HW/SW et contrôler les systèmes et logiciels sûrs de fonctionnement
- Présenter les bonnes pratiques pour la spécification, architecture et conception des Systèmes et Matériels
- Maîtriser les techniques de tests et de validation des systèmes et matériels

FORMATEUR

Experts en Sûreté de Fonctionnement.

MODALITÉS PÉDAGOGIQUES

Présentation PowerPoint projetée et diffusée, étude de cas pratique, exercices, mise en situation, exemple théorique, supports vidéo...

MODALITÉS D'ÉVALUATION

Evaluation en début et fin de formation, quizz...

DÉLAI D'INSCRIPTION

5 jours ouvrés avant le début de la formation (si financement OPCO).

SANCTION

Une attestation de formation conforme aux dispositions de l'Article L. 6353-1 alinéa 2 remise au stagiaire.

PROGRAMME 

PROGRAMME

Cette formation est fondée sur un fort retour d'expérience de mise en œuvre des exigences de la Sûreté de Fonctionnement des systèmes et électroniques embarqués développés pour des applications critiques.

L'apport principal de cette formation réside dans notre capacité à fournir un niveau d'information détaillé sur la compréhension des spécificités de cette norme. Cette formation est ponctuée d'exercices pratiques pour illustrer les sujets abordés.

INTRODUCTION À LA SÉCURITÉ FONCTIONNELLE

PRÉSENTATION GÉNÉRALE DE LA NORME CEI 61508

EXIGENCES TECHNIQUES CEI 61508-1

- Les phases d'analyse
 - Concept et définition globale du domaine d'application
 - Analyse des dangers et des risques
 - Exigences globales de sécurité
 - Allocation des exigences globales de sécurité (architecture HW/SW)
- Les phases d'opération
- Les phases de réalisation

AUTRES EXIGENCES CEI 61508-1

EXIGENCES TECHNIQUES CEI 61508-2

- Intégrité de sécurité du matériel
 - Contraintes architecturales relatives à l'intégrité de sécurité
 - Quantification des défaillances aléatoires du matériel
- Défaillances systématiques
 - Évitement et maîtrise des défaillances systématiques
 - Capabilité systématique
 - Preuve que le matériel est validé en utilisation (« Proven in Use »)
- Comportement du système lors de la détection d'un défaut

Cette formation sera réalisée par l'un de nos spécialistes ayant mis en œuvre la norme CEI 61508-1 & 2 sur de nombreux projets.

SÛRETÉ DE FONCTIONNEMENT DES LOGICIELS EMBARQUÉS (CEI 61508-3)

20



DATES & LIEUX

- 20 au 21 mars - Pessac
- 11 au 12 juin - Paris
- 20 au 21 nov. - Toulouse
- 3 au 4 dec. - Aix-en-Provence

DURÉE

- 2 jours

TARIF

1460€

LANGUES



PRÉREQUIS

Connaissance du processus de développement.

PUBLIC CONCERNÉ

Chef de projet logiciel, responsable qualité logiciel, développeur, vérificateur, testeur.

OBJECTIF

- Cerner les exigences normatives pour spécifier, définir l'architecture, contrôler les logiciels sûrs de fonctionnement
- Présenter les bonnes pratiques pour la spécification, architecture et conception des Logiciels,
- Maîtriser les techniques de tests et de validation des logiciels

FORMATEUR

Experts en Sûreté de Fonctionnement des logiciels.

MODALITÉS PÉDAGOGIQUES

Présentation PowerPoint projetée et diffusée, étude de cas pratique, exercices, mise en situation, exemple théorique, supports vidéo...

MODALITÉS D'ÉVALUATION

Evaluation en début et fin de formation, quizz...

DÉLAI D'INSCRIPTION

5 jours ouvrés avant le début de la formation (si financement OPCO).

SANCTION

Une attestation de formation conforme aux dispositions de l'Article L. 6353-1 alinéa 2 remise au stagiaire.

PROGRAMME 

PROGRAMME

Cette formation est fondée sur un fort retour d'expérience de mise en œuvre des exigences de la Sûreté de Fonctionnement des logiciels embarqués développés pour des applications critiques.

L'apport principal de cette formation réside dans notre capacité à fournir un niveau d'information détaillé sur la compréhension des spécificités de cette norme. Cette formation est ponctuée d'exercices pratiques pour illustrer les sujets abordés.

INTRODUCTION À LA SDF DES SYSTÈMES E/E/EP

- Présentation des notions de SDF
- Lien Système/Matériel/Logiciel

PRÉSENTATION DE LA NORME CEI 61508-3

LA PLANIFICATION DES LOGICIELS CRITIQUES

- Organisation des équipes
- Le cycle de développement
- Les phases du développement
- Documentation à produire

LA SPÉCIFICATION DU LOGICIEL

- Présentation de l'attendu normatif
- Bonnes pratiques

L'ARCHITECTURE DU LOGICIEL

- Présentation de l'attendu normatif
- Bonnes pratiques
- Problématiques techniques
 - Les architectures redondées
 - Le multi-SIL
 - Protocoles de communication sécuritaires
 - Intégration des COTS
 - Réutilisation des composants précédemment développés

LA CONCEPTION DU LOGICIEL

- Présentation de l'attendu normatif
- Bonnes pratiques

RÈGLES DE CONCEPTION À PRIVILÉGIER AU NIVEAU ARCHITECTURE, CONCEPTION DÉTAILLÉE ET CODAGE

- Modularité
- Programmation défensive
- COTS...

RÈGLES DE PROGRAMMATION DU LANGAGE C

- Fonctions, Instructions, Données

PRÉSENTATION DES ACTIVITÉS DE TESTS

- Organisation
- Couverture structurelle et fonctionnelle des tests

TESTS BAS-NIVEAU

- Tests unitaires
- Tests d'intégration logiciel/logiciel

TESTS HAUT-NIVEAU

- Tests d'intégration logiciel/matériel
- Tests de validation

VÉRIFICATION DU LOGICIEL

- Analyse documentaire
- Traçabilité
- Lecture croisée
- Analyse statique

MÉTHODES SAFETY DES LOGICIELS

- LCC
- AEEL (AMDEC du logiciel)
- Revue de tests...

OUTILS UTILISÉS

- Analyse statique de code
- Tests unitaires et d'intégration
- Modélisation
- Gestion de configuration
- Compilateurs
- Traçabilité...

CLASSIFICATION DES OUTILS

Cette formation sera réalisée par l'un de nos spécialistes ayant mis en œuvre la norme CEI 61508-3 sur de nombreux projets.

SENSIBILISATION À LA SÉCURITE FONCTIONNELLE DES SYSTÈMES ÉLECTRONIQUES (CEI 61508-1&2)

23



DURÉE

- 1 jour

TARIF

Sur devis

LANGUES



PRÉREQUIS

Aucun.

PUBLIC CONCERNÉ

Chef de projet, développeur, qualiticien.

OBJECTIF

Appréhender la norme CEI61508 (2010) au niveau système et hardware, ainsi que les méthodes et outils utilisés dans le domaine de la sûreté de fonctionnement des systèmes électroniques afin de permettre aux participants de mieux identifier et comprendre leurs finalités.

FORMATEUR

Ingénieur Chef de projet.

MODALITÉS PÉDAGOGIQUES

Présentation PowerPoint projetée et imprimée, étude de cas pratique, exercices, mise en situation, exemple théorique, supports video...

MODALITÉS D'ÉVALUATION

Evaluation en début et fin de formation, quizz...

DÉLAI D'INSCRIPTION

5 jours ouvrés avant le début de la formation (si financement OPCO).

SANCTION

Une attestation de formation conforme aux dispositions de l'Article L. 6353-1 alinéa 2 remise au stagiaire.

PROGRAMME 

PROGRAMME

INTRODUCTION À LA SÉCURITÉ FONCTIONNELLE

PRÉSENTATION GÉNÉRALE DE LA NORME CEI 61508

EXIGENCES TECHNIQUES CEI 61508-1

- Les phases d'analyse
 - Concept et définition globale du domaine d'application
 - Analyse des dangers et des risques
 - Exigences globales de sécurité
 - Allocation des exigences globales de sécurité
- Les phases d'opération
- Les phases de réalisation

EXIGENCES ADDITIONNELLES CEI 61508-1

EXIGENCES TECHNIQUES CEI 61508-2

- Intégrité de sécurité du matériel
- Contraintes architecturales relatives à l'intégrité de sécurité
- Quantification des défaillances aléatoires du matériel

DÉFAILLANCES SYSTÉMATIQUES

- Évitement et maîtrise des défaillances systématiques
- Capabilité systématique
- Preuve que le matériel est validé en utilisation (« Proven in Use »)

COMPORTEMENT DU SYSTÈME LORS DE LA DÉTECTION D'UN DÉFAUT

SENSIBILISATION À LA SÛRETÉ DE FONCTIONNEMENT DES LOGICIELS EMBARQUÉS (CEI 61508-3)

25



DURÉE

- 1 jour

TARIF

Sur devis

LANGUES



PRÉREQUIS

Aucun.

PUBLIC CONCERNÉ

Responsables développement logiciel, responsables qualité, chefs de projets.

OBJECTIF

Appréhender les normes (automobile, nucléaire, ferroviaire, aéronautique...), méthodes et outils utilisés dans le domaine de la sûreté de fonctionnement du logiciel afin de permettre aux participants de mieux identifier et comprendre leurs finalités.

FORMATEUR

Expert en sûreté de fonctionnement.

MODALITÉS PÉDAGOGIQUES

Présentation PowerPoint projetée et diffusée, étude de cas pratique, exercices, mise en situation, exemple théorique, supports vidéo...

MODALITÉS D'ÉVALUATION

Evaluation en début et fin de formation, quizz...

DÉLAI D'INSCRIPTION

5 jours ouvrés avant le début de la formation (si financement OPCO).

SANCTION

Une attestation de formation conforme aux dispositions de l'Article L. 6353-1 alinéa 2 remise au stagiaire.

PROGRAMME 

PROGRAMME

- Introduction à la Sécurité fonctionnelle**
- Présentation de la norme CEI61508-3**
- Cycle de développement logiciel**
- La planification du logiciel**
- La spécification du logiciel**
- L'architecture du logiciel**
- La conception du logiciel (Modularité, programmation défensive, COTS...)**
- Le codage du logiciel (Règles de codage)**
- Les tests du logiciel (Unitaires, intégration, validation)**
- La vérification du logiciel**
- Les outils du logiciel (Analyse statique de code, tests, modélisation, gestion de configuration...)**

Cette formation sera réalisée par l'un de nos spécialistes du domaine ayant mis en œuvre la norme CEI 61508-3 sur de nombreux projets.

ISO 26262 - SÉCURITÉ FONCTIONNELLE - VÉHICULES ROUTIERS

27



DATES & LIEUX

- 12 au 14 mars - Paris
- 25 au 27 juin - Lyon
- 08 au 10 oct. - Toulouse

DURÉE

- 3 jours

TARIF

2 160€

LANGUES



PRÉREQUIS

Connaissance du développement et de la programmation.

PUBLIC CONCERNÉ

Chef de projet, responsable qualité, concepteur, développeur, vérificateur, valideur.

OBJECTIFS

- Comprendre la gestion de la sécurité fonctionnelle et ses objectifs dans le domaine automobile
- Fournir les bases pour comprendre la norme ISO26262 et son vocabulaire
- Apporter les éléments utiles pour le développement d'équipements automobiles afin de challenger vos clients ou fournisseurs
- Etre en mesure d'identifier l'impact des exigences de l'ISO26262 sur les processus et le développement (au niveau système, matériel, logiciel et fabrication)

FORMATEUR

Experts en Sûreté de Fonctionnement.

MODALITÉS PÉDAGOGIQUES

Présentation PowerPoint projetée et imprimée, étude de cas pratique, exercices, mise en situation, exemple théorique, supports vidéo...

MODALITÉS D'ÉVALUATION

Evaluation en début et fin de formation, quizz...

DÉLAI D'INSCRIPTION

5 jours ouvrés avant le début de la formation (si financement OPCO).

SANCTION

Une attestation de formation conforme aux dispositions de l'Article L. 6353-1 alinéa 2 remise au stagiaire.

PROGRAMME 

PROGRAMME

Cette formation est fondée sur un fort retour d'expérience de mise en œuvre des exigences de la Sûreté de Fonctionnement des systèmes et logiciels embarqués développés pour des applications critiques dans le domaine automobile.

L'apport principal de cette formation réside dans notre capacité à fournir un niveau d'information détaillé sur la compréhension des spécificités de cette norme.

PARTIE 1

- Introduction à la Sécurité fonctionnelle
- Présentation générale de la norme ISO 26262
- Gestion de la sécurité fonctionnelle (ISO 26262-2)
 - Gestion globale de la sécurité fonctionnelle
 - Gestion de la sécurité fonctionnelle au sein d'un projet
 - Gestion de la sécurité de la phase de concept à la production (rôle, planning, safety concept, ...)
- Phase de concept (ISO 26262-3)
 - Définition de l'item
 - Analyse de danger et de risque
 - Functional safety concept (FSC) / Décomposition ASIL

PARTIE 2

- Développement du produit au niveau système (ISO 26262-4)
 - Technical safety concept
 - Conception du système
 - Intégration et tests
 - Validation de la sécurité
- Développement du produit au niveau matériel (ISO 26262-5)
 - Spécification des exigences de sécurité du matériel
 - Architecture et conception du matériel
 - Qualification des composants matériels
 - Evaluation des métriques d'architecture matérielle (SPFM, LFM)
 - Evaluation des violations du safety goal dues aux défaillances aléatoires du matériel (PMHF, cut-set)
 - Tests et intégration du matériel
- Phases ultérieures au développement (Production, maintenance, utilisation et démantèlement) (ISO 26262-7)
- Particularités pour les véhicules 2 roues motorisés

 **PARTIE 3**

- Développement du produit au niveau logiciel (ISO 26262-6)
 - Introduction à la sécurité fonctionnelle
 - Management de la sécurité
 - Du Functional safety concept aux exigences du logiciel
 - Spécification des exigences du Logiciel
 - Conception architecturale du logiciel
 - Mécanismes et analyses de sécurité
 - Conception et implémentation des unités logicielles
 - Tests unitaires
 - Intégration du logiciel et tests
 - Vérification des exigences de sécurité du logiciel
 - Safety case
 - Configuration du logiciel
 - Confiance dans l'utilisation des outils du logiciel
 - Qualification des composants logiciel

Cette formation sera réalisée par un de nos spécialistes ayant mis en œuvre la norme ISO 26262 sur de nombreux projets.

NORME EN50126 & 50129 - SÛRETÉ DE FONCTIONNEMENT FERROVIAIRE

30



DATES & LIEUX

- 3 au 4 avril - Pessac
- 8 au 9 oct. - Toulouse

DURÉE

- 2 jours

TARIF

1460€

LANGUES



PRÉREQUIS

Etre sensibilisé à la sûreté de fonctionnement (FMDS).

PUBLIC CONCERNÉ

Tout acteur du ferroviaire (exploitant, industriel, évaluateur) impliqué dans le développement d'un système ferroviaire.

OBJECTIFS

- Comprendre les étapes du cycle de développement de la sécurité d'un système ou sous-système ferroviaire
- Comprendre la définition, l'allocation et la démonstration des niveaux d'intégrité de la sécurité (SIL)
- Appréhender les méthodes, outils et techniques de sûreté de fonctionnement utilisés
- Comprendre comment constituer un dossier de sécurité

FORMATEUR

Ingénieur.

MODALITÉS PÉDAGOGIQUES

Présentation PowerPoint projetée et diffusée, étude de cas pratique, exercices, mise en situation, exemple théorique, supports vidéo...

MODALITÉS D'ÉVALUATION

Evaluation en début et fin de formation, quizz...

DÉLAI D'INSCRIPTION

5 jours ouvrés avant le début de la formation (si financement OPCO).

SANCTION

Une attestation de formation conforme aux dispositions de l'Article L. 6353-1 alinéa 2 remise au stagiaire.

PROGRAMME 

PROGRAMME

Cette formation est fondée sur un fort retour d'expérience de mise en œuvre des exigences de la Sûreté de Fonctionnement des systèmes embarqués développés pour des applications critiques ferroviaires.

L'apport principal de cette formation réside dans notre capacité à fournir un niveau d'information détaillé sur la compréhension des spécificités de ces normes. Cette formation est ponctuée d'exercices pratiques pour illustrer les sujets abordés.

PARTIE 1 : INTRODUCTION

- Les domaines d'application des normes et leurs limites
- Les grands principes des normes

PARTIE 2 : LA REGLEMENTATION | SECURITE FERROVIAIRE

- Les organismes notifiés par l'état français et l'Europe
- La pyramide réglementaire

PARTIE 3 : LE PROCESSUS DE MANAGEMENT DE LA FMDS

- Cycle en V FMDS
- Appréciation du risque
- Réalisation et démonstration de la conformité aux exigences FMDS
- Exploitation, maintenance et retrait

PARTIE 4 : LES ROLES & RESPONSABILITES

- Définition
- Indépendance des acteurs en fonction des niveaux de SIL

PARTIE 5 : DEFINITION & DEMONSTRATION DU SIL

- Définition du SIL
- Définition de la sécurité technique & contextuelle
- Les principes d'allocation des THR, TFFR et SIL
- Démonstration du SIL
 - Les architectures de sécurité
 - Indépendance entre fonctions
 - Détection des pannes
 - Mise à l'état sûr (passivation)
 - Gestion des outils et éléments préexistants

PARTIE 6 : LE DOSSIER DE SECURITE

- Rapport de gestion de la qualité
- Rapport de gestion de la sécurité
- Rapport de sécurité technique

Cette formation sera réalisée par un de nos spécialistes ayant mis en œuvre les normes EN 50126 et EN 50129 sur de nombreux projets.

FORMATION AUX NORMES EN 50128/ EN 50657 – LOGICIELS DU FERROVIAIRE



32

DATES ET LIEUX

- 6 au 7 fev. - Paris
- 17 au 18 sept. - Lyon

DURÉE

- 2 jours

TARIF

1460€

LANGUES



PRÉREQUIS

Connaissance du processus de développement.

PUBLIC CONCERNÉ

Chef de projet logiciel, responsable qualité logiciel, développeur, vérificateur, testeur.

OBJECTIFS

- Présenter la norme EN 50128 / EN 50657
- Cerner les exigences normatives pour spécifier, définir l'architecture, contrôler les logiciels sûrs de fonctionnement
- Présenter les bonnes pratiques pour la spécification, architecture et conception des Logiciels,
- Maîtriser les techniques de tests et de validation des logiciels

FORMATEUR

Experts en Sécurité de Fonctionnement.

MODALITÉS PÉDAGOGIQUES

Présentation PowerPoint projetée et diffusée, étude de cas pratique, exercices, mise en situation, exemple théorique, supports vidéo...

MODALITÉS D'ÉVALUATION

Evaluation en début et fin de formation, quizz...

DÉLAI D'INSCRIPTION

5 jours ouvrés avant le début de la formation (si financement OPCO).

SANCTION

Une attestation de formation conforme aux dispositions de l'Article L. 6353-1 alinéa 2 remise au stagiaire.

PROGRAMME ↓

PROGRAMME

Cette formation est fondée sur un fort retour d'expérience de mise en œuvre des exigences de la Sûreté de Fonctionnement des logiciels embarqués développés pour des applications critiques ferroviaires.

L'apport principal de cette formation réside dans notre capacité à fournir un niveau d'information détaillé sur la compréhension des spécificités de cette norme. Cette formation est ponctuée d'exercices pratiques pour illustrer les sujets abordés.

INTRODUCTION À LA SDF DES SYSTÈMES FERROVIAIRES

- Présentation des notions de SDF
- Lien Système/Matériel/Logiciel

PRÉSENTATION DES NORMES EN 50128 ET EN 50657

LA PLANIFICATION DES LOGICIELS CRITIQUES

- Organisation des équipes
- Le cycle de développement
- Les phases du développement
- Documentation à produire

LA SPÉCIFICATION DU LOGICIEL

- Présentation de l'attendu normatif
- Bonnes pratiques

L'ARCHITECTURE DU LOGICIEL

- Présentation de l'attendu normatif
- Bonnes pratiques
- Problématiques techniques
 - Les architectures redondées
 - Le multi-SIL
 - Intégration des COTS
 - Réutilisation des composants précédemment développés

LA CONCEPTION DU LOGICIEL

- Présentation de l'attendu normatif
- Bonnes pratiques

RÈGLES DE CONCEPTION À PRIVILÉGIER AU NIVEAU ARCHITECTURE, CONCEPTION DÉTAILLÉE ET CODAGE

Modularité, programmation défensive, COTS...

RÈGLES DE PROGRAMMATION DU LANGAGE C

Fonctions, instructions, données

PRÉSENTATION DES ACTIVITÉS DE TESTS

Organisation, couverture structurelle et fonctionnelle des tests

TESTS BAS-NIVEAU

Tests des composants, tests d'intégration logiciel/logiciel

TESTS HAUT-NIVEAU

Tests d'intégration logiciel/matériel, tests d'ensemble du logiciel

VÉRIFICATION ET VALIDATION DU LOGICIEL

Analyse documentaire, traçabilité, lecture croisée, analyse statique...

MÉTHODES DE VALIDATION/EVALUATION DU LOGICIEL

LCC, AEEL (AMDEC du logiciel), revue de tests...

OUTILS UTILISÉS

Analyse statique de code, tests unitaires et d'intégration, modélisation, gestion de configuration, compilateurs, traçabilité...

EXIGENCES SUR LES LOGICIELS CONFIGURÉS PAR DONNÉES D'APPLICATION

CLASSIFICATION DES OUTILS

Cette formation sera réalisée par l'un de nos spécialistes du domaine ferroviaire ayant mis en œuvre les normes EN 50128 et EN 50657 sur de nombreux projets.

SENSIBILISATION AUX NORMES EN 50128 / EN 50657 - LOGICIELS DU FERROVIAIRE

35



DURÉE

- 1 jour

TARIF

Sur devis

LANGUES



PRÉREQUIS

Aucun.

PUBLIC CONCERNÉ

Responsables développement logiciel, responsables qualité, chefs de projets.

OBJECTIFS

- Présenter les normes EN 50128 / EN50657
- Analyser et cerner l'impact des normes sur le développement des logiciels

FORMATEUR

Experts en Sécurité de Fonctionnement.

MODALITÉS PÉDAGOGIQUES

Présentation PowerPoint projetée et diffusée, étude de cas pratique, exercices, mise en situation, exemple théorique, supports vidéo...

MODALITÉS D'ÉVALUATION

Evaluation en début et fin de formation, quizz...

DÉLAI D'INSCRIPTION

5 jours ouvrés avant le début de la formation (si financement OPCO).

SANCTION

Une attestation de formation conforme aux dispositions de l'Article L. 6353-1 alinéa 2 remise au stagiaire.

PROGRAMME 

PROGRAMME

INTRODUCTION À LA SÛRETÉ DE FONCTIONNEMENT (SDF) DES LOGICIELS

PRÉSENTATION GÉNÉRALE DE LA NORME EN 50128/EN 50657

PROCESSUS DE DÉVELOPPEMENT DU LOGICIEL

- L'Assurance Qualité Logiciel
- La Spécification Logiciel
- L'Architecture et la Conception Logiciel
- La Conception des Composants Logiciels
- Les Règles de Conception et Règles de Programmation
- Les Tests (Composants, Intégration, d'Ensemble)
- La Vérification / La Validation
- Les Méthodes d'Évaluation et les Outils
- Les Données d'Application

Cette formation sera réalisée par l'un de nos spécialistes du domaine ferroviaire ayant mis en œuvre les normes EN 50128/EN 50657 sur de nombreux projets

SENSIBILISATION AU SYSTÈME DE MANAGEMENT DE LA QUALITE POUR LES DISPOSITIFS MÉDICAUX ISO13485 : 2016



37

DATES ET LIEUX

- 3 avril - Paris
- 24 sept - Pessac

DURÉE

- 1 jour

TARIF

750 €

LANGUES



PRÉREQUIS

Notion d'un système de management de la qualité.

PUBLIC CONCERNÉ

Toute personne impliquée la mise en œuvre et/ou le maintien d'un système de management de la qualité pour les dispositifs médicaux (Novices / Débutants).

OBJECTIFS

- Identifier le rôle de la norme ISO 13485 dans le contexte réglementaire des dispositifs médicaux
- Comprendre les attendus de la norme ISO 13485
- Traduire les exigences de la norme ISO 13485 dans votre système de management de la qualité

FORMATEUR

Ingénieur.

MODALITÉS PÉDAGOGIQUES

Présentation PowerPoint projetée et diffusée, étude de cas pratique, exercices, mise en situation, exemple théorique, supports vidéo...

MODALITÉS D'ÉVALUATION

Evaluation en début et fin de formation, quizz...

DÉLAI D'INSCRIPTION

5 jours ouvrés avant le début de la formation (si financement OPCO).

SANCTION

Une attestation de formation conforme aux dispositions de l'Article L. 6353-1 alinéa 2 remise au stagiaire.

PROGRAMME 

PROGRAMME

PARTIE 1 : INTRODUCTION

- Historique
- Définition d'un dispositif médical
- Le rôle de la norme dans l'obtention du marquage CE

PARTIE 2 : PRÉSENTATION GÉNÉRALE DE LA NORME

- Sommaire de la norme
- Couverture et non couverture de la norme
- Les fondements & particularités

PARTIE 3 : LES EXIGENCES NORMATIVES EN LIEN AVEC :

- Le SMQ
- La responsabilité de la direction
- Le management des ressources
- La réalisation du projet
 - Planification
 - Processus relatif au client
 - Conception et Développement
 - Achats
 - Production et Services
 - Équipement de surveillance et de mesure
- Mesurage, analyse et amélioration
 - Retours d'informations & Réclamations
 - Communication aux autorités réglementaires
 - Audit interne
 - Surveillance de processus
 - Surveillance du produit
 - Produit non conforme avant/après livraison
 - Actions correctives – Actions préventives

Cette formation sera réalisée par un de nos spécialistes du domaine médical ayant mis en œuvre le référentiel ISO 13485 sur de nombreux projets.

SENSIBILISATION À LA NORME EN 62304 LOGICIELS DE DISPOSITIFS MÉDICAUX



39

DATES ET LIEUX

- 4 avril - Paris
- 25 sept - Pessac

DURÉE

- 1 jour

TARIF

750€

LANGUES



PRÉREQUIS

Aucun.

PUBLIC CONCERNÉ

Chef de projet logiciel, responsable qualité logiciel, développeur, vérificateur, testeur.

OBJECTIFS

- Introduire la norme CEI 62304
- Cerner les exigences normatives pour définir les exigences et la conception architecturale du Logiciel
- Cerner les exigences normatives pour réaliser la conception détaillée
- Comprendre les règles préconisées par la norme CEI 62304 pour la vérification et les essais des logiciels de dispositifs médicaux
- Cerner les exigences générales de la norme liées aux différents processus (maintenance, gestion des risques, gestion de configuration du logiciel, résolution de problèmes)

FORMATEUR

Expert en développement Logiciel dans le Médical.

MODALITÉS PÉDAGOGIQUES

Présentation PowerPoint projetée et diffusée, étude de cas pratique, exercices, mise en situation, exemple théorique, supports vidéo...

MODALITÉS D'ÉVALUATION

Evaluation en début et fin de formation, quizz...

DÉLAI D'INSCRIPTION

5 jours ouvrés avant le début de la formation (si financement OPCO).

SANCTION

Une attestation de formation conforme aux dispositions de l'Article L. 6353-1 alinéa 2 remise au stagiaire.

PROGRAMME ↓

PROGRAMME

Cette formation est fondée sur un fort retour d'expérience de mise en œuvre des exigences normatives dans le cadre du développement des logiciels embarqués pour des applications critiques du domaine médical.

INTRODUCTION À LA NORME CEI 62304 (PÉRIMÈTRE, CONCEPTS, ...)

PROCESSUS DE DÉVELOPPEMENT

- Plan de développement du logiciel
- Exigences du logiciel
- Conception architecturale du logiciel
- Conception détaillée du logiciel et vérification
- Intégration, essais et diffusion du logiciel

EXIGENCES DES PROCESSUS DE MAINTENANCE

- Gestion de configuration du logiciel
- Résolution de problèmes...

EXIGENCES DES PROCESSUS DE GESTION DES RISQUES (LIEN AVEC L'ISO 14971)

Cette formation sera réalisée par un de nos spécialistes du domaine médical ayant mis en œuvre le référentiel ISO 13485 sur de nombreux projets.

AMDEC EN CONCEPTION ÉLECTRONIQUE



41

DURÉE

- 2 jours

TARIF

Sur devis

LANGUES



PRÉREQUIS

Connaissance en conception et développement de systèmes électriques.

PUBLIC CONCERNÉ

Techniciens et ingénieurs impliqués dans la conception de systèmes électroniques.

OBJECTIFS

Maîtriser les différentes AMDEC (AMDEC produit, AMDEC fonctionnelle, AMDEC composant ...) couramment utilisées en conception et en sûreté de fonctionnement avec des exemples de réalisation. Cette formation s'appuie sur des analyses concrètes (cartes électroniques du client) effectuées en groupe de travail lors de la formation (50% du temps de formation).

FORMATEUR

Ingénieur Chef de projet.

MODALITÉS PÉDAGOGIQUES

Présentation PowerPoint projetée et imprimée, étude de cas pratique, exercices, mise en situation, exemple théorique, supports vidéo...

MODALITÉS D'ÉVALUATION

Evaluation en début et fin de formation, quizz...

DÉLAI D'INSCRIPTION

5 jours ouvrés avant le début de la formation (si financement OPCO).

SANCTION

Une attestation de formation conforme aux dispositions de l'Article L. 6353-1 alinéa 2 remise au stagiaire.

PROGRAMME ↓

PROGRAMME

INTRODUCTION

- Notions de base
- Mise en œuvre de l'AMDEC

DESIGN FMEA

- Intérêts et principes
- Analyse fonctionnelle
- Grille d'analyse
- Etudes de cas sur exemple client

AMDE(C) DES BLOCS FONCTIONNELS

- Intérêts et principes
- Décomposition organico-fonctionnelle
- Grille d'analyse
- Etudes de cas sur exemple client

AMDEC COMPOSANT

- Intérêts et principes
- Grille d'analyse
- Modes et taux de défaillances
- Etudes de cas sur exemple client

SÛRETÉ DE FONCTIONNEMENT DES ÉLECTRONIQUES (HARDWARE)

43



DATES & LIEUX

- 26 au 28 mars - Pessac
- 8 au 10 oct. - Grenoble

DURÉE

- 3 jours

TARIF

2 160€

LANGUES



PRÉREQUIS

Connaissances en électronique.

PUBLIC CONCERNÉ

Chef de projet, développeur, qualité.

OBJECTIF

Présenter les différentes normes, méthodes, outils et techniques d'analyse utilisés dans le domaine de la sûreté de fonctionnement des systèmes électroniques (niveau hardware) afin de permettre aux participants de comprendre leurs finalités et d'appréhender leur mise en œuvre, dans l'optique d'être appliquées.

FORMATEUR

Ingénieur Chef de projet.

MODALITÉS PÉDAGOGIQUES

Présentation PowerPoint projetée et imprimée, étude de cas pratique, exercices, mise en situation, exemple théorique, supports vidéo...

MODALITÉS D'ÉVALUATION

Évaluation en début et fin de formation, quizz...

DÉLAI D'INSCRIPTION

5 jours ouvrés avant le début de la formation (si financement OPCO).

SANCTION

Une attestation de formation conforme aux dispositions de l'Article L. 6353-1 alinéa 2 remise au stagiaire.

PROGRAMME 

PROGRAMME

INTRODUCTION

- Définitions et concepts de base de la SdF
- Tour d'horizon des activités et outils de la SdF
- Présentation succincte de normes, guides et recueils de SdF

PRESENTATION DE LA SECURITE FONCTIONNELLE

- Norme de base : IEC61508 (focus sur les parties 1 et 2)

OUTILS ET TECHNIQUES D'ANALYSES APPLIQUÉES AUX ÉLECTRONIQUES

- Intérêt, méthode, grille d'analyse, exercice et/ou présentation d'études de cas...
- Analyse préliminaire de risques
- Bases de données de fiabilité
- Analyse par blocs fonctionnels
- AMDEC (introduction)
- AMDEC des blocs fonctionnels
- AMDEC composants
- Analyse de la couverture de diagnostic
- Diagramme de fiabilité des architectures types
- Analyse de défaillances de cause commune
- Arbres de défaillances
- Graphes de Markov

INTRODUCTION À LA CROISSANCE DE FIABILITÉ EN CONCEPTION



A PROPOS DE SAFETY AND SECURITY

SERMA Safety and Security accompagne ses clients pour la sécurité et la sûreté de fonctionnement des produits et systèmes dans les domaines de l'IoT, de l'embarqué, de l'industrie ou des systèmes d'information. L'entreprise bénéficie d'une expertise unique lui permettant d'intervenir sur toute la chaîne de valeur des systèmes : depuis les produits IoT en passant par l'infrastructure réseau et système jusqu'aux applications internes et externes.

SERMA Safety and Security est reconnue pour son excellence technique qui lui vaut d'avoir reçu de nombreuses qualifications et certifications dont CESTI, PASSI RGS, SESIP, FIPS, SBMP, ...

Parallèlement à ces activités, la société propose des formations sur l'ensemble de son périmètre de compétence en sûreté de fonctionnement et cybersécurité. Présente sur 8 sites en France, la société compte plus de 230 collaborateurs et réalise un chiffre d'affaires de plus de 35 millions d'euros. Elle est une filiale du Groupe SERMA.