

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 !

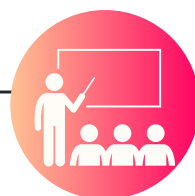


# NOS FORMATIONS

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



Près de  
**50**  
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**.



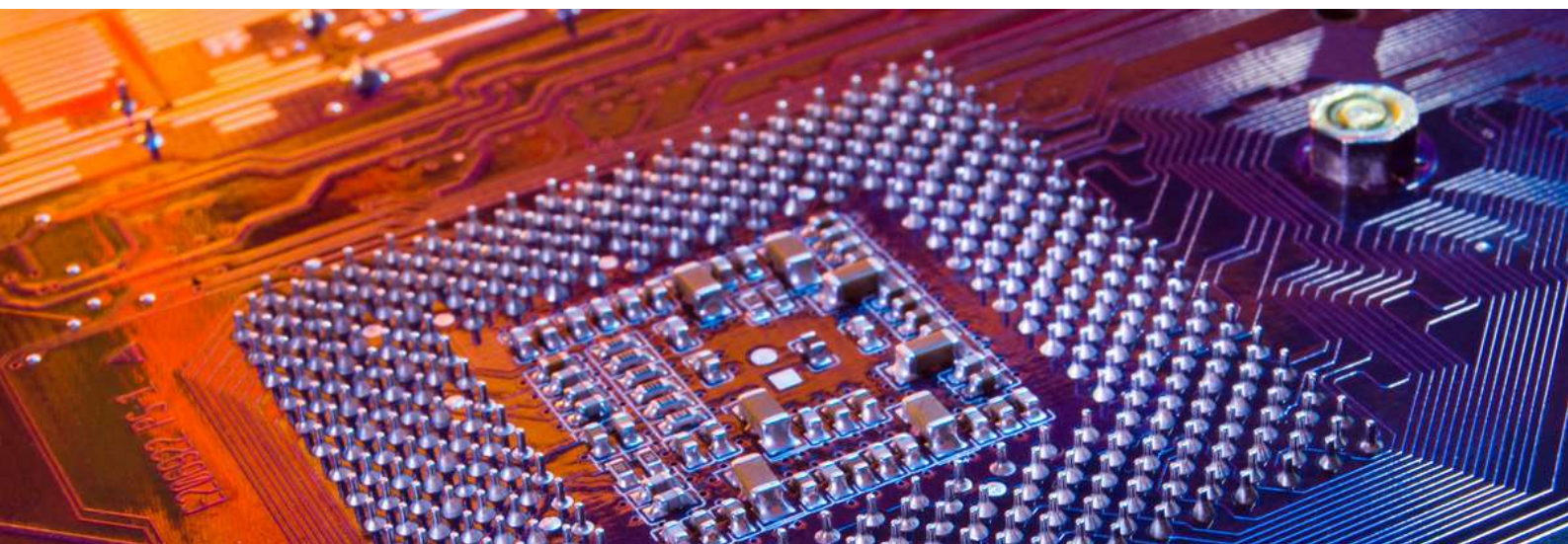
### À DISTANCE

**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](mailto: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

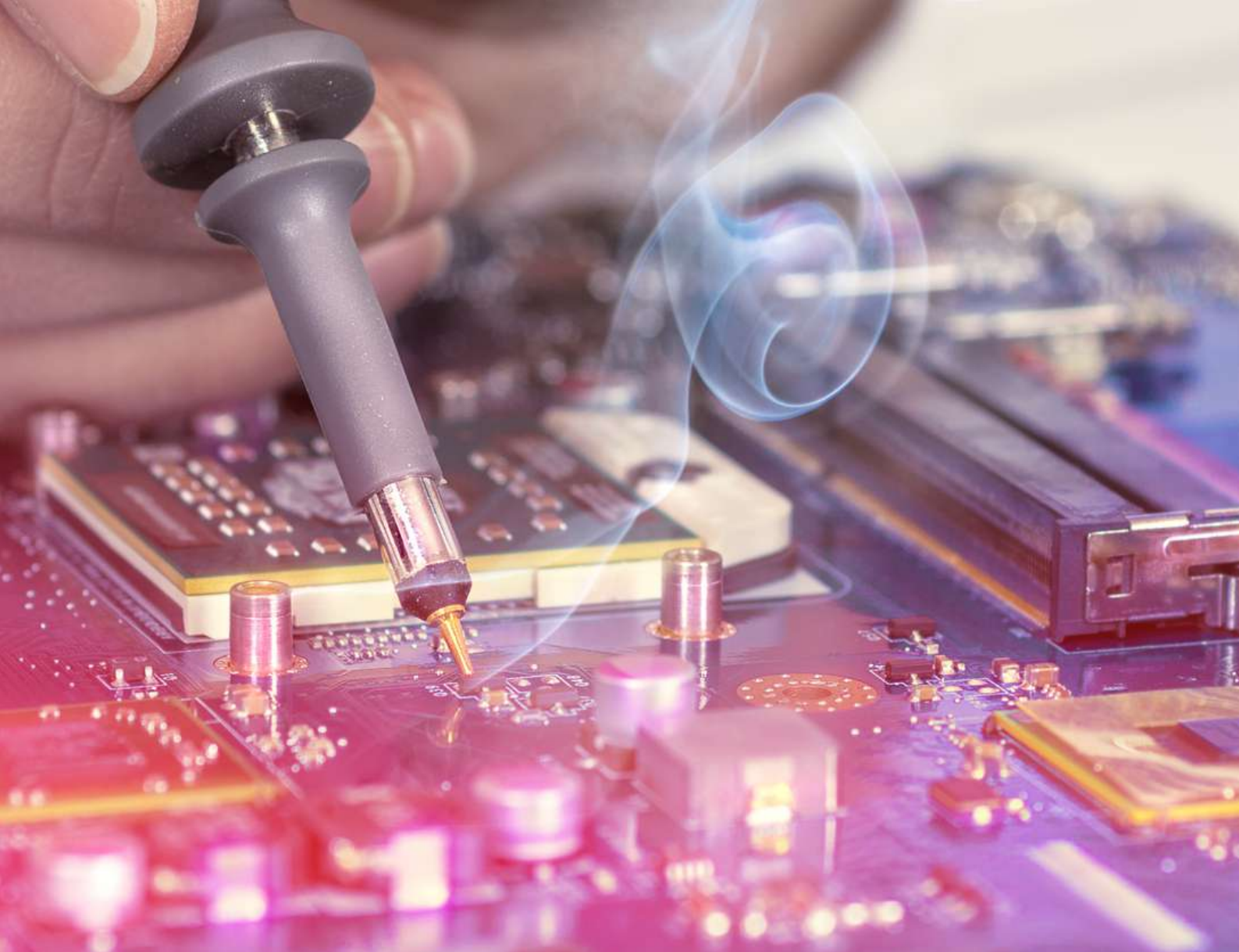
- **Par chèque** : d'un montant total TTC indiqué sur la facture à l'ordre de SERMA Technologies
- **Par virement bancaire** :

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](mailto: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

## TECHNOLOGIES DE L'ÉLECTRONIQUE

Habilitation électrique BR / BE Essais et Mesurages.....	1
Technologies des circuits imprimés.....	3
Technologies des composants passifs* .....	5
Technologies des composants actifs* .....	7
Mécanismes de défaillance* .....	9
Analyses des causes de défaillance (RCA) sur cartes électroniques* .....	11
Analyse physique des composants.....	14
Sécurisation des composants issus de la distribution non-officielle.....	16

## CARTES ET SYSTÈMES ÉLECTRONIQUES

Introduction à l'assemblage de cartes électroniques* .....	18
Assemblage des cartes électroniques* .....	20
ESD Protections antistatiques.....	23
Industrialisation cartes et sous-ensembles électroniques - Conduite de projet.....	25
Audit de ligne d'assemblage des cartes électroniques* .....	28
Management de l'obsolescence des composants électroniques.....	31
Stockage des composants.....	33
Certification inspecteur IPC-A-610 « Acceptabilité des assemblages électroniques ».....	35
Re-certification inspecteur IPC-A-610 « Acceptabilité des assemblages électroniques ».....	38
Fiabilisation d'un ensemble électronique* .....	41
Qualification des composants électroniques* .....	44
Qualification des systèmes électroniques automobiles* .....	46
Fiabilité électronique et vibration.....	49
Fiabilité et électronique de puissance* .....	51

## BATTERIES

Stockage énergie électrique : batteries.....	53
Sécurité des batteries.....	55
Technologies des supercondensateurs.....	57

## HYDROGÈNE

Sensibilisation aux systèmes hydrogènes* .....	59
--	----

## MATÉRIAUX

Techniques d'analyse physico-chimiques des surfaces de matériaux.....	61
---	----

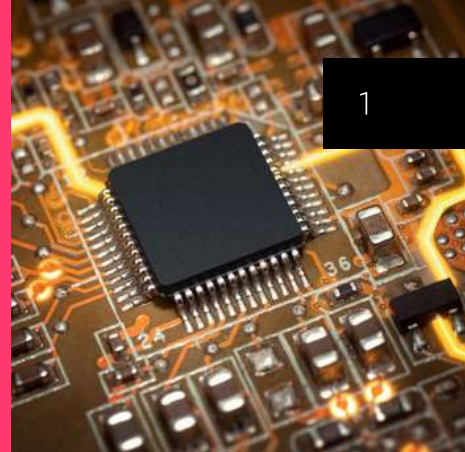
## CYBERSÉCURITÉ

Cybersécurité et conformité IoT – Directive RED* .....	63
Cybersécurité et conformité automobile – UN R155 & ISO 21 434* .....	65
Cybersécurité et conformité ferroviaire TS 50 701* .....	67
Cybersécurité des systèmes embarqués et des objets connectés* .....	70
Cybersécurité des applications WEB OWASP Top 10:2021* .....	73
Cybersécurité des systèmes industriels IEC-62443* .....	76

## SÛRETÉ DE FONCTIONNEMENT

Sûreté de fonctionnement des systèmes et matériels (CEI 61508-1 & 2) .....	80
Sûreté de fonctionnement des logiciels embarqués (CEI 61508-3).....	82
Sensibilisation à la sécurité fonctionnelle des systèmes électroniques (CEI 61508-1 & 2).....	85
Sensibilisation à la sûreté de fonctionnement des logiciels embarqués (CEI 61508-3).....	87
Norme ISO 26262 – Sécurité fonctionnelle – Véhicules routiers.....	89
Formation aux normes EN 50126 & 50129 « Sûreté de fonctionnement ferroviaire ».....	92
Formation aux normes EN 50128/EN 50657 – Logiciels du ferroviaire.....	94
Sensibilisation aux normes EN 50128/EN 50657 – Logiciels du ferroviaire.....	97
Sensibilisation au système de management de la qualité pour les dispositifs médicaux ISO 13485:2016.....	99
Sensibilisation à la norme EN 62304 – Logiciels de dispositifs médicaux.....	101
AMDEC en conception électronique.....	103
Sûreté de fonctionnement des électroniques (Hardware).....	105

# HABILITATION ÉLECTRIQUE BR / BE ESSAIS ET MESURAGES



## DURÉE

- 1.5 ou 2 jours

## TARIF

Sur demande

## LANGUES



## PRÉREQUIS

Posséder des compétences techniques en électricité est obligatoire pour suivre cette formation.

## PUBLIC CONCERNÉ

Personnel électricien ou électromécanicien chargé en BT de réaliser des essais électriques en laboratoire.

## OBJECTIF

Réaliser en toute sécurité les essais électriques qui lui seront demandés dans le domaine Basse Tension selon les exigences de la norme NF C 18-510.

## 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****PLANNING DE LA FORMATION SUR 2 JOURS (INITIAL)**

- Introduction
- Présentation
- Situation initiale
- L'électricité
- Electricité - Les risques
- Electricité - Les Mesures de Sécurité
- Les habilitations
- Les Habilitations BR-BE
- QCM - Habitation BR
- QCM - Habitation BE Mesures
- QCM - Habitation BE Essais
- Les installations Electriques
- Les particularités SERMA

**PARTIE PRATIQUE**

- Installation électrique
- Plateforme de test

**PLANNING DE LA FORMATION SUR 1,5 JOUR (RECYCLAGE)****JOUR 1 - THEORIE**

Matin :

- La réglementation
- L'électricité - Les notions
- Risques électriques
- Les mesures de sécurité
- Isolation/Obstacle
- Éloignement

Après-midi :

- Les habilitations
- Les différents titres
- Les installations électriques
- Les particularités de SERMA

**JOUR 2 - PRATIQUE**

Matin :

- Installation électrique
- Plateforme de test

# TECHNOLOGIES DES CIRCUITS IMPRIMÉS

3

## DATES & LIEUX

- 18-19 juin - Pessac

## DURÉE

- 2 jours

## TARIF

1 460 €

## LANGUES



## PRÉREQUIS

Connaissance des processus d'assemblage des cartes électroniques.

## PUBLIC CONCERNÉ

Ingénieur, chef de projet, technicien... ayant des problématiques de circuits imprimés : technique de fabrication des matériaux, contrôle de production, mécanismes de défaillance.

## OBJECTIF

Connaître les principales étapes de fabrication des PCB afin d'identifier les origines des défauts.

## 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

### GÉNÉRALITÉS TECHNIQUES

- Histoire et évolution
- Les différentes catégories de circuits imprimés.

### ETAPES DE PROCÉDES POUR PCB MULTICOUCHES

- Documents de définition
- CAM to CAD, DFM
- Coupons de test – IPC2221
- Pannélisation
- Classes IPC
- Photo-lithographie
- Gravure
- Empilage et laminage
- Perçage
- Métallisation
- Vernis épargne
- Finitions
- Test et emballage

### MATÉRIAUX DE BASE

- Couche de stratifié élémentaire
- Trous traversants – enterrés - borgnes
- Constante diélectrique et angle de pertes
- Tissus de verre renforcés
- Comportement thermique (Tg, CTE et MOT)
- Différentes résines
- Quelques défauts

### AUTRES TECHNOLOGIES

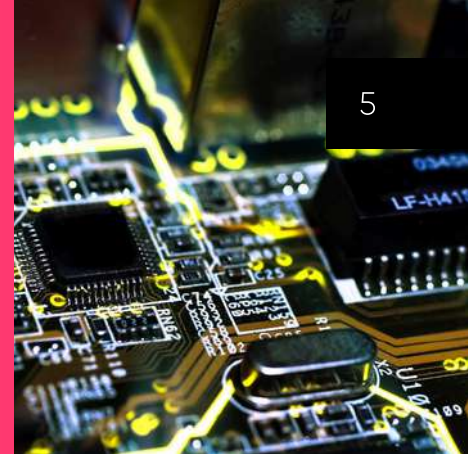
- Haute densité et micro-via
- Circuits Flex
- Circuits Flex Rigide

### MÉCANISMES DE DÉFAILLANCE

- Défauts de Métallisation, de finition, Black Pad, ...



# TECHNOLOGIES DES COMPOSANTS PASSIFS



## DATES & LIEUX

- 12 mars - Pessac
- 15 octobre - Pessac

## DURÉE

- 1 jour

## TARIF

750 €

## LANGUES



## PRÉREQUIS

Connaissances de base en technologie des composants passifs.

## PUBLIC CONCERNÉ

Responsable qualité, personnel de laboratoire, bureau d'études, achats, etc.

## OBJECTIF

Comprendre les technologies abordées.

## FORMATEUR

Responsable Pôle Compétences Laboratoire.

## 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

### CONDENSATEURS (CAPACITORS)

- Généralités : paramètres électriques, les différents types de condensateurs, les applications, les gammes, le choix d'un type.
- Les condensateurs céramiques : procédés de fabrication, modes de défaillance typiques, les risques à l'assemblage (Film).
- Les condensateurs tantale : idem
- Les autres condensateurs : électrolytique aluminium, films, super condensateurs...

### RÉSISTANCES FIXES (RESISTORS)

- Généralités, paramètres électriques, les différents types de résistances, les applications.
- Les résistances à couches épaisses (Thick film) : principes de fabrication, modes de défaillance typiques, les risques à l'assemblage.
- Les résistances à couches fines (Thin film) : principe de fabrication, modes de défaillance typiques, les risques à l'assemblage.
- Les résistances bobinées (Wire wound) : principes de fabrication, modes de défaillance typiques, les risques à l'assemblage.

### QUARTZ / RESONNATEURS (RESONATORS)

- Généralités, paramètres électriques, les applications.
- Technologie, construction
- Process de fabrication
- Principaux défauts et mécanismes

### SELF (INDUCTORS)

- Généralités, paramètres électriques, les applications.
- Technologie, construction
- Process de fabrication
- Principaux défauts et mécanismes

# TECHNOLOGIES DES COMPOSANTS ACTIFS

7

## DATES & LIEUX

- 13 mars - Pessac
- 16 octobre - Pessac

## DURÉE

- 1 jour

## TARIF

750 €

## LANGUES



## PRÉREQUIS

Connaissances de base en technologie des composants actifs.

## PUBLIC CONCERNÉ

Responsables qualité, chefs de projets, personnel de laboratoire et bureau d'études.

## OBJECTIFS

Comprendre les principes de fabrication d'une puce et son encapsulation, et appréhender l'analyse de défaillance à travers des exemples concertés d'étude de cas.

## 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

### 1E PARTIE / PRINCIPES DE FABRICATION DES PUCES

- Introduction
- Matériaux (semi-conducteurs, conducteurs et isolants)
- Procédés de fabrication
- Les technologies
  - Process CMOS
  - Process bipolaire
  - Process BICMOS
- Exemples de défaut de fabrication

### 2E PARTIE / LE PACKAGING

- Généralités sur le packaging
- Technologies d'assemblage
  - Découpe du wafer
  - Fixation de la puce
  - Câblage filaire
- Types de boîtiers

### 3E PARTIE / L'ANALYSE DE DÉFAILLANCE

- But et étapes de l'analyse de défaillance sur circuits actifs
- Techniques et méthodes
- Exemples de défauts de fabrication sur composants actifs (diodes, transistors, CI et composants optoélectroniques ...)

# MÉCANISMES DE DÉFAILLANCE



## DATES & LIEUX

- 15 au 16 mai - Pessac
- 17 au 18 sept. - Distanciel
- 5 au 6 nov. - Pessac
- 3 au 4 dec. - Distanciel

## DURÉE

- 2 jours

## TARIF

1 460 €

## LANGUES



## PRÉREQUIS

Connaissances de base en électronique générale.

## PUBLIC CONCERNÉ

Responsable qualité ou technique, ingénieur d'analyse retour terrain/SAV.

## OBJECTIFS

Appréhender la faiblesse des composants passifs, discrets, actifs à travers leurs principaux mécanismes de défaillance. Des cas concrets de défaut et quelques techniques de révélation sont présentés.

## FORMATEUR

Ingénieur fiabilité des composants/cartes électroniques.

## 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

**Définition et introduction méthodologique**

**Introduction de la technologie (matériaux en présence) pour chaque famille de composant**

**Présentation des faiblesses principales et des moyens de révélation de chaque famille de composant**

**Exercice d'application**

**Quizz/Evaluation des acquis**

### JOUR 1

**Famille de composants concernée :**

- Circuits imprimés (PCB)
- Brasure : Sn/Pb, SAC
- Résistances : couche épaisse, couche mince
- Condensateurs : Céramique, Tantale, Electrolytique, Film
- Quartz : PTH et CMS
- Bobine

### JOUR 2

**Famille de composants concernée :**

- Semi-conducteurs discrets : diode, LED et transistors MOS
- Semi-conducteurs actifs : circuits intégrés Si
- Boîtiers de circuits discrets et intégrés
- Optocoupleur

# ANALYSE DES CAUSES DE DÉFAILLANCE (RCA) SUR CARTES ÉLECTRONIQUES

11



## DATES & LIEUX

- 6 et 7 fév. – Distanciel
- 4 et 5 juin – Pessac

## DURÉE

- 2 jours

## TARIF

1 460 €

## LANGUES



### PRÉREQUIS

Connaissances de base en électronique générale.

### PUBLIC CONCERNÉ

Responsable qualité ou technique, ingénieur d'analyse retour terrain/SAV ou confronté à un besoin d'amélioration de la fiabilité de carte électronique.

### OBJECTIFS

Appréhender une méthode pratique de recherche de cause de défaillance sur carte électronique.

### FORMATEUR

Ingénieur process, 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

### DÉFINITIONS

- Défaut, mode de défaillance, dégradation, mécanisme de défaillance, cause de défaillance, cause racine

### INTRODUCTION AUX ÉTAPES DE LA RECHERCHE DE CAUSE

- L'état des lieux : la description du défaut et son contexte d'apparition
- Confirmation/caractérisation du défaut
- Localisation du défaut niveau carte et composant
- Observation/expertise du défaut
- Recherche et pondération du mécanisme de défaillance
- Recherche et pondération des causes de défaillance

### LA DESCRIPTION DU DÉFAUT ET SON CONTEXTE D'APPARITION

- La description du produit et du défaut
- Le produit : sa conception, son procédé de fabrication, son historique, ...
- Le défaut : les faits (données), les conditions d'apparition, le REX, ...
- Les méthodes : QQOQC, 5W, IS-IS NOT, Graphique, ...
- Exemples

### MÉTHODES DE LOCALISATION/CARACTÉRISATION DU DÉFAUT SUR CARTE

- Les modes de défaillances et leurs cas particuliers (intermittence, instabilité, combustion, ...)
- Les outils de localisation (objectifs, limites et risques d'altération du défaut)
- Introduction aux familles de mécanisme de dégradation
- Les méthodes de caractérisation d'un défaut
- L'analyse de cohérence des résultats

### INTRODUCTION AUX MÉCANISMES DE DÉFAILLANCE

## LA FORMALISATION DES HYPOTHÈSES ET CRITÈRES DE PONDÉRATION (OBJECTIFS, MÉTHODES, MOYENS, LIMITES) :

- Exemple d'application

## CAUSES DE DÉFAILLANCE SUR CARTE ÉLECTRONIQUE ET PONDÉRATION

- Rappel de définition : ce qu'est / n'est pas une cause
- Revue des familles de causes de défaillance sur carte électronique
- Méthodes de revue des hypothèses : Brainstorming, Arbre de défaillance, Diagramme cause-effet, Mind mapping, ...
- Les outils et critères de pondération (objectifs, méthodes, moyens, limites) :
  - Le plan d'expérience
  - L'expertise en laboratoire
  - L'essai de robustesse
  - L'audit de procédé de fabrication
  - Les mesures sur le terrain
  - L'avis d'expert, ...
- Exemple

## CAUSE ET CAUSE RACINE DE DÉFAILLANCE SUR CARTE ÉLECTRONIQUE

## QCM ET CORRECTION

# ANALYSE PHYSIQUE DES COMPOSANTS

14



## DATES & LIEUX

- 18 au 21 mars – Pessac
- 10 au 13 juin – Pessac
- 7 au 10 oct. – Pessac

## DURÉE

- 4 jours

## TARIF

2 600 €

## LANGUES



## PRÉREQUIS

Connaissance de la technologie des composants, fiabilité, assemblage, analyse des composants et des systèmes électroniques.

## PUBLIC CONCERNÉ

Techniciens, ingénieurs/chefs de projet, qui doivent réaliser, suivre, challenger, synthétiser des analyses de composants, cartes, dans leur laboratoire ou laboratoires extérieurs.

## OBJECTIFS

Se familiariser avec les techniques permettant de réaliser des analyses de construction et de défaillance sur tous les types de composants électroniques ainsi que sur l'analyse des brasures et des circuits imprimés. Cette formation s'adresse au personnel de laboratoire et aux correspondants qualité.

## FORMATEUR

Ingénieurs et techniciens de laboratoire.

## 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****TECHNIQUE D'ANALYSE APPLIQUÉ À**

- Analyses de construction
  - Analyse de composants
  - Analyse de packaging
  - Analyse puces
- Analyses de défaillance
  - Composants
  - Cartes

**TEST ÉLECTRIQUE**

- Test paramétrique
- Confirmation du défaut
- Mesure comparative

**ANALYSE NON DESTRUCTIVE**

- Visuel optique
- Radiographie x
- Microscopie acoustique

**OUVERTURE CHIMIQUE**

- Acides et lasers pour ouverture des boîtiers plastiques
- Techniques d'analyse des boîtiers : ouverture chimique spécifique
- inspection au MEB, pull test et shear test
- Ouvertures chimiques pour analyse de défaillance
- Artefacts d'ouverture

**OUVERTURES MÉCANIQUES**

- Ouverture mécaniques des boîtiers à cavité

**LOCALISATION DES DÉFAUTS**

- Visuel optique
- Probing
- Détection de points chauds par la technique des cristaux liquides
- Principe de la microscopie à émission de lumière
- Microscopie infra rouge

**MICRO SECTION**

- Enrobée pour composants PCB et brasures
- Puces
- Révélations chimiques

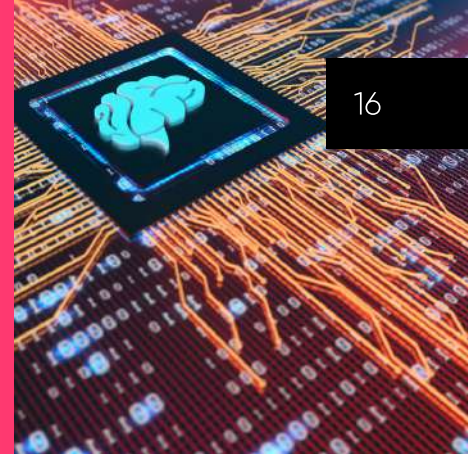
**OBSERVATION AU MEB**

- Préparation des échantillons
- Observation en mode secondaire et rétro diffusé
- Technique d'analyse EDX (Electron Dispersion X-rays analysis)

**QUESTIONS**



# SÉCURISATION DES COMPOSANTS ISSUS DE LA DISTRIBUTION NON-OFFICIELLE



16

## DATES & LIEUX

- 5 au 6 juin - Pessac

## DURÉE

- 2 jours

## TARIF

1 460€

## LANGUES



## PRÉREQUIS

Sensibilisation aux problèmes liés aux approvisionnements «broker».

## PUBLIC CONCERNÉ

Distributeurs, acheteurs/utilisateurs de composants obsolètes, contrôle d'entrée.

## OBJECTIF

Sécuriser les lots issus de la distribution non officielle.

## FORMATEUR

Responsable Pôle de compétences Laboratoire « contrôle de lot ».

## 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

### JOUR 1

#### TECHNOLOGIES DES COMPOSANTS

#### PRÉCAUTIONS ESD, MANIPULATION ET STOCKAGE DES COMPOSANTS :

- Composants sensibles aux ESD
- Composants sensibles à l'humidité (MSL)

#### TEST : TECHNIQUE ET APPLICATION AU CONTRÔLE DE LOTS BROKER

- Notions d'échantillonnage

#### TEST : NON DESTRUCTIFS

- Optique
- Radiographie X
- Microscopie acoustique
- Fluorescence X
- Notions de test électrique

#### TEST : DESTRUCTIFS

- Brasabilité
- Ouvertures chimique/mécanique
- Microsection

#### DEFAUTS RENCONTRES LORS DES CONTROLES DE LOTS BROKER

Défauts : détection, origine, impact sur le composant

- Défauts liés aux conditions de stockage
- Défauts liés aux manipulations
- Défauts liés au démontage
- Défauts liés au reconditionnement
- Falsification
- Contrefaçon

### JOUR 2

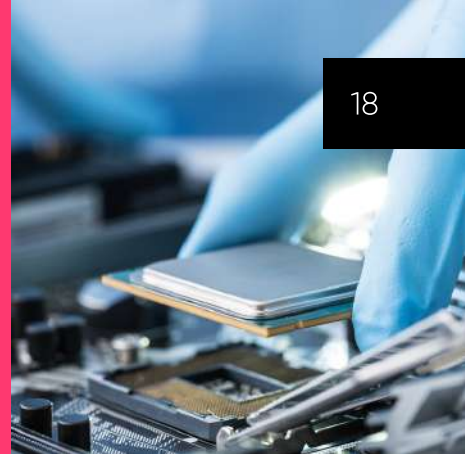
#### PRÉSENTATION DES ÉQUIPEMENTS - VISITE DU LABORATOIRE

#### CAS CONCRÈTS DE CONTRÔLE DE LOTS (PIÈCES SERMA ET AUTRES) ET DE FALSIFICATION

#### TEST (QCM) DE CONTRÔLE D'ACQUISITION DE CONNAISSANCES

# INTRODUCTION À L'ASSEMBLAGE DE CARTES ÉLECTRONIQUES

18



## DURÉE

- 0,5 jour

## TARIF

Sur devis

## LANGUES



## PRÉREQUIS

Connaissance en électronique.

## PUBLIC CONCERNÉ

Chef de projet, acheteur, coordinateur métier, magasinier, technicien de laboratoire...

## OBJECTIFS

- Définir ce qu'est une carte électronique et ce qui la compose, enseigner la base des procédés de fabrication, expliquer les phénomènes physiques (brasage), apporter une vue globale des métiers impliqués afin de connaître le vocabulaire technique courant.

## 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

### PRÉSENTATION GÉNÉRALE DU MILIEU DE L'ÉLECTRONIQUE INDUSTRIELLE

### QU'EST-CE QU'UNE CARTE ÉLECTRONIQUE ?

### CONTRAINTES ENVIRONNEMENTALES EN PRODUCTION

- MSL
- ESD
- Stockage
- Manutention

### LA PRODUCTION D'UNE CARTE ÉLECTRONIQUE

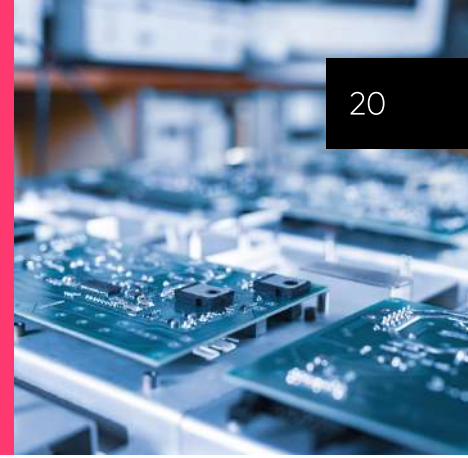
- Les moyens de production et de contrôle.

### LE TEST D'UNE CARTE ÉLECTRONIQUE

- Les moyens test et de contrôle électrique.



# ASSEMBLAGE DES CARTES ELECTRONIQUES



## DATES & LIEUX

- 12 au 14 mars - Toulouse
- 17 au 19 sept. - Pessac

## DURÉE

- 3 jours

## TARIF

2 160 €

## LANGUES



### PRÉREQUIS

Connaissance de base en assemblage des cartes.

### PUBLIC CONCERNÉ

Ingénieur qualité AQF, responsables produits, auditeur, chef de projet, ingénieur, technicien Process « Assembly »... Cette formation est spécifique aux assembleurs, elle approfondit les thèmes : matériaux, maîtrise process.

### OBJECTIFS

- Acquérir les informations nécessaires à la mise en œuvre maîtrisée des procédés d'assemblage des composants électroniques.
- Savoir juger de la qualité des assemblages à partir de l'étude des différents éléments entrant dans la fabrication du produit final : circuits imprimés, circuits hybrides, composants, matériaux de brasage avec et sans plomb matériaux de collage et autres.
- Savoir mettre en œuvre : assemblage (PTH, SMT), fluxage, brasures, profils, conditionnement stockage, nettoyage...
- Aborder les aspects de contrôles et d'analyses de défaillance ainsi que les règles essentielles permettant d'assurer la maîtrise des processus.

### FORMATEUR

Ingénieur Process 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

### INTRODUCTION

- Environnement industriel
- Risques fiabilité

### CHAPITRE 1 : BRASURE

- Terminologie et définitions : brasure, soudure, joint brasé...
- Diagramme de phase (plomb étain)
- Les alliages plomb /étain utilisés
- Les brasures sans plomb
- Fusion et refusion
- Phases : morphologies et évolution
- Intermétalliques
- La mouillabilité
- Les crèmes à braser
- Impact du sans plomb sur les composants et les alliages
- Backward process

### CHAPITRE 2 : CIRCUITS IMPRIMÉS ET PRINCIPAUX COMPOSANTS ELECTRONIQUES

#### Circuits imprimés :

- Technologies : double face, multicouche
- Caractéristiques physiques : coefficient d'expansion thermique, flambage, Tg
- Finitions métallurgiques des surfaces de brasure
- Sensibilité à l'humidité

#### Composants électroniques :

- Condensateurs
- Relais
- Quartz

#### Les composants à boîtier plastique :

- Les matériaux des terminaisons des broches, billes (LED, BGA,  $\mu$ BGA et flip chip)
- Sensibilité à l'humidité
- Contrôles non destructifs : visuel optique, acoustique et rayons X

### CHAPITRE 3 : MANAGEMENT DU RISQUE LIÉ AUX DÉCHARGES ÉLECTROSTATIQUES

- Définition
- Composants sensibles
- Zone EPA

## CHAPITRE 4 : LIGNE D'ASSEMBLAGE DES CARTES ELECTRONIQUES

- Process Flow
- Influence du design carte sur le choix de process
- Stockage des composants électroniques et circuits imprimés
- Les modes de dépôt : sérigraphie, seringue
- Les machines de placement (report)
- Profil de température et contrôle (refusion)
- Contrôles de fabrication
- Composants traversants
- Press Fit
- Brasage à la vague
- Autres moyens de brasure
- Dépannelisation
- Nettoyage
- Test
- Vernis
- Intégration du système
- Packaging

## CHAPITRE 5 : MAÎTRISE DU PROCESS

- Qualification des machines et des process
- Contrôle des paramètres influents
- Main d'œuvre et instructions de travail
- Capabilité
- Gage R&R
- Les mécanismes de défaillance

## CHAPITRE 6 : NORMES PRINCIPALES ET PRINCIPAUX ACRONYMES

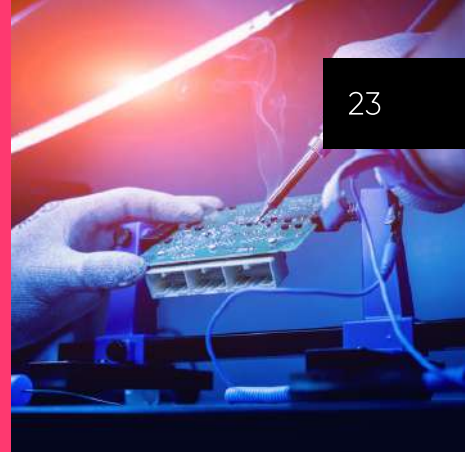
## CHAPITRE 7 : AUDIT DIGEST

**Inclus dans le 3ème jour dans le cas où cette formation est dispensée à Pessac :**

Visite d'un atelier d'assemblage de cartes (moyens CMS, traversant (PTH), brasage manuel).

# ESD PROTECTIONS ANTISTATIQUES

23



## DURÉE

- 1 jour

## TARIF

Sur devis

## LANGUES



## PRÉREQUIS

Aucun.

## PUBLIC CONCERNÉ

Tout public manipulant des composants ou cartes électroniques.

## OBJECTIF

Prévenir et comprendre les décharges électrostatiques dans un site industriel par la mise en œuvre, le contrôle et la maintenance des protections nécessaires.

## 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****FORMATION THÉORIQUE  
(UNE DEMI-JOURNÉE) :**

- Module 1 : Définition d'une décharge électrostatique
- Module 2 : Gestion du risque ESD en atelier d'assemblage et de test :  
Phénomènes et conséquences sur les circuits intégrés
- Module 3 : Gestion du risque ESD en atelier d'assemblage et de test :  
Règles de prévention

**FORMATION PRATIQUE  
(UNE DEMI-JOURNÉE) :**

- Sur postes de travail, auto audit en travail de groupes, avec équipements de mesure : tera-ohmmètre, mesureur de champs (option : test du marcheur)
- Débriefing par groupe sur les anomalies constatées et propositions d'amélioration

Cette formation intra-entreprise pourra être adaptée en fonction de vos besoins.

# INDUSTRIALISATION CARTES ET SOUS-ENSEMBLES ÉLECTRONIQUES - CONDUITE DE PROJET

25

## DATES & LIEUX

- 6 au 8 fev. - Distanciel
- 15 au 17 oct. - Distanciel

## DURÉE

- 2.5 jours

## TARIF

1 820 €

## LANGUES



### PRÉREQUIS

Connaissance en conception ou fabrication des cartes et sous-ensembles électroniques.

### PUBLIC CONCERNÉ

Responsable méthodes, R&D, ingénieur conception, routage PCB, responsable Qualité, chef de projet industriel.

### OBJECTIFS

- Aborder un projet industriel dans sa phase de pré-étude et de faisabilité
- Maîtriser les risques lors des phases de conception (conception préliminaire et conception de détail)
- Appréhender les typologies de procédés de fabrication adaptées au projet
- Piloter les phases prototypes, la validation des produits (certification), la qualification produit/process
- Elaborer le planning du projet et le suivre en mode opérationnel
- Calculer le budget du projet (investissement et coût projet) et le suivre en mode opérationnel

### FORMATEUR

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

### MODULE 1 : AVANT-PROJET/STRATÉGIE INDUSTRIELLE/FAISABILITÉ

- Périmètre & rôle de l'industrialisation
- Faisabilité économique
- Notion de prix/coûts
- Sélection d'un EMS (Electronic manufacturing services)

### MODULE 2 : DÉVELOPPEMENT D'UN PRODUIT PHASE PRÉLIMINAIRE

- Faisabilité technique/plan de développement
- Spécification du besoin et exigences
- Conception préliminaire
- Analyse des risques (AMDEC produit) – Choix des composants – Validation du concept

### MODULE 3 : DÉVELOPPEMENT DÉTAILLÉ D'UN PRODUIT

- Conception design
- DFM (Design for Manufacturing)/DFT (Design for testability)
- Règles de conception et de fabrication
- Circuit imprimé – techno – finitions – spécifications – panélisation
- ESD (Electrostatic Sensitive Device)
- Développement mécanique
- Typologie du process d'assemblage/contraintes de fabrication
- Moyens de contrôle et de test – stratégie de test
- Dossier de définition produit

### MODULE 4 : PROTOTYPE - VALIDATION DESIGN

- Fabrication des prototypes
- Plan de validation – process – robustesse – fiabilité
- Certification – normes – label CE

## **MODULE 5 : PILOT RUN – INDUSTRIALISATION LIGNE**

- Gestion système (EMS)
- Industrialisation des moyens
- Industrialisation des lignes de fabrication
- Introduction au Lean manufacturing
- Lancement moyens de test/spécifications/qualifications des moyens

## **MODULE 6 : PILOT RUN – QUALIFICATION**

- Fabrication du Pilot run – Rapport Qualité - exploitation
- Plan de qualification - Livrables

## **MODULE 7 : PROCESS PARALLÈLES**

- Standard IPC
- Gestion des changements / évolutions techniques
- Retours clients – process de réparation
- Qualification / formation du personnel chargé de la production

# AUDIT DE LIGNE D'ASSEMBLAGE DES CARTES ELECTRONIQUES

28



## DATES & LIEUX

- 22 au 23 mai - Pessac
- 19 au 20 nov. - Distanciel

## DURÉE

- 2 jours

## TARIF

1 460 €

## LANGUES



## PRÉREQUIS

Notions de base en électronique.

## PUBLIC CONCERNÉ

Ingénieurs qualité AQF, responsables produits, techniciens process « Assembly », auditeurs.

## OBJECTIFS

Évaluer ses capacités techniques et organisationnelles pour ceux ayant des activités comprenant des visites ou audits de fournisseurs de cartes assemblées. Cette formation s'appuie sur notre longue expérience dans le domaine de l'audit, de notre connaissance des techniques d'assemblage et de leurs mécanismes de défaillance.

## FORMATEUR

Ingénieur Process 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

- Environnement industriel
- Problèmes fiabilité

### BRASURE

- Brasure
- Brasure avec plomb
- Mouillabilité
- Intermétalliques
- Evolution des phases
- RoHS et REACH
- Contrôle
- Brasure sans plomb
- Brasure avec et sans plomb
- Whiskers

### LES CIRCUITS IMPRIMÉS ET LES PRINCIPAUX COMPOSANTS ÉLECTRONIQUES

- Circuits imprimés
- Condensateurs
- Quartz
- Composants en boîtier plastique

### DÉCHARGES ÉLECTROSTATIQUES

- EOS et ESD
- Sensibilité des composants
- Environnement des ateliers
- Transport des pièces sensibles
- Moyens de contrôle

### LIGNE D'ASSEMBLAGE DES CARTES ÉLECTRONIQUES

- Process Flow
- Ligne CMS
- Composants traversants (PTH) seulement
- Composants CMS sur 1 face
- Composants CMS sur 1 face + quelques PTH
- Pin In Paste
- Composants CMS sur les 2 faces
- CMS et traversants : technologie mixte



## INTRODUCTION À LA MAITRISE DES PROCESSUS

- Qualification
- Contrôles des paramètres
- SPC, CP, CPK, control chart

## TECHNIQUE DE L'AUDIT

- Généralités
- Préparation
- Organisation
- Agenda
- Attitude
- Déroulement sur ligne

## FINALISATION DE L'AUDIT

- Grille d'Audit
- Wrap up

## DESCRIPTION ET AUDIT DÉTAILLÉ DES ÉTAPES DU PROCÉDÉ D'ASSEMBLAGE

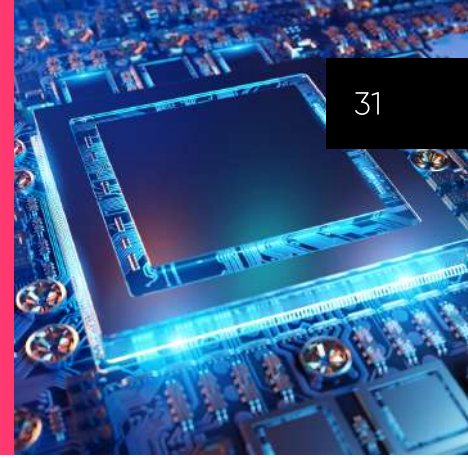
- Propreté et management visuel
- Réception et Stockage
- Sérigraphie
- Report
- Refusion
- Contrôle
- Traversant
- Brasage à la vague
- Autres moyens de brasure
- Vernis
- Test
- Intégration du système
- Packaging

## ANNEXES

- Normes principales et principaux acronymes
- Audit digest

# MANAGEMENT DE L'OBSOLESCENCE DES COMPOSANTS ÉLECTRONIQUES

31



## DATES & LIEUX

- 26 mars – Pessac
- 24 sept. – Distanciel

## DURÉE

- 1 jour

## TARIF

750€

## LANGUES



## PRÉREQUIS

Aucun.

## PUBLIC CONCERNÉ

Chef de projet, ingénieur, technicien, responsable et correspondant qualité.

## OBJECTIF

Connaissance des causes et gestion des conséquences de l'obsolescence.

## FORMATEUR

Responsable Pôle de Compétence AQC.

## 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

- Objectifs
- Les causes de l'obsolescence
- Notion de cycle de vie
- Impact financier

### ANALYSE PRÉVISIONNELLE D'OBSOLESCENCE AU NIVEAU COMPOSANT

- Mise en place d'indicateurs (technologies, fabricants)

### EVENTAIL DES SOLUTIONS DE TRAITEMENT

- Grille d'analyse
- Impact
- Contrefaçon

### EVALUATION ET MANAGEMENT DES RISQUES AU NIVEAU CARTES/SYSTÈMES FINIS

- Estimation de coefficient de criticité et de probabilité

### CONCLUSION

### QUESTIONS

# STOCKAGE DES COMPOSANTS

33



## DATES & LIEUX

- 27 mars – Distanciel
- 25 sept. – Distanciel

## DURÉE

- 1 jour

## TARIF

750€

## LANGUES



## PRÉREQUIS

Notions de base en physique des composants.

## PUBLIC CONCERNÉ

Personnes amenées à stocker des composants ou des cartes électroniques.

## OBJECTIF

Être à même d'identifier les exigences acceptables pour les différents stockages. Connaître et prendre des décisions lors de la mise en place d'un tel programme.

## FORMATEUR

Responsable Pôle de Compétence AQC.

## 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

### CONTEXTE

### INTRODUCTION

- Vues des composants et des cartes assemblées

### MÉCANISMES DE DÉFAILLANCE

- Contraintes mécaniques
- Contraintes chimiques/Action de l'humidité
- Champs électrostatiques
- Contraintes thermomécaniques
- Autres (empoussièrement)

### MÉTHODOLOGIE DE STOCKAGE

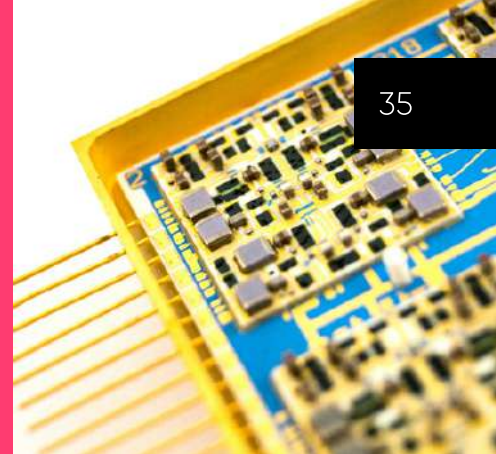
- Achat
  - Dimensionnement
  - Conditionnement
- Contrôle réception
  - Traçabilité
  - Conformité
- Validation technique initiale
  - Physique
  - Electrique
  - Fiabilité
- Stockage
  - Atmosphère
  - Solution
  - Local
- Validation technique périodique
- Déstockage
  - Logistique
  - Gestion

### CONCLUSION

### QUESTIONS

# FORMATION ET CERTIFICATION INSPECTEUR IPC-A-610 « ACCEPTABILITÉ DES ASSEMBLAGES ÉLECTRONIQUES »

35



## DATES & LIEUX

- 27 au 30 mai - Pessac

## DURÉE

- 3.5 jours

## TARIF

1 850€

## LANGUES



## PRÉREQUIS

Notions de base assemblage PCB et technologies composants.

## PUBLIC CONCERNÉ

Responsables qualité, ingénieurs Process, techniciens et opérateurs, contrôleurs visuels et réparateurs des produits électroniques.

## OBJECTIF

Utilisation et compréhension des critères de la norme IPC-A-610. Support de formation IPC-A-610 selon indice H. Maîtrise de cet outil de communication entre clients et fournisseurs. Validation de la formation par un certificat officiel de l'IPC.

## FORMATEUR

Formateur certifié IPC.

## 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/RÈGLES ET PROCÉDURES PROFESSIONNELLES IPC

- Introduction
- Programme et durée de la certification
- Formateurs et spécialiste IPC
- Recertification et épreuve par challenge.

### AVANT-PROPOS, DOCUMENTS APPLICABLES ET MANIPULATION

- Champ d'application
- Conceptions spécialisées
- Termes et définitions
- Méthodologie d'inspection
- Vérification des dimensions
- Instruments grossissants et éclairage
- Documents applicables
- Manipulation des cartes électroniques.

### INSTALLATION DES ACCESSOIRES

- Installation des accessoires, isolement, éléments de fixation
- Connecteurs, poignées, extracteurs, loquets
- Broches de connecteurs
- Harnais, faisceau de câblage, laçage
- Cheminement, croisements, rayon de courbure.

### CONNEXIONS À BORNE (INSTALLATION ET BRASAGE)

- Clip latéral
- Accessoires sertis
- Préparation fil, étamage
- Préformage, réducteur de tension
- Installation
- Isolants, conducteurs
- Bornes, brasures
- Dommages

## CRITÈRES BRASURES (HAUTE TENSION INCLUSE)

- Exigences d'acceptabilité du brasage
- Anomalies de brasage
- Haute tension

## CRITÈRES POUR LA TECHNOLOGIE AVEC TROUS MÉTALLISÉS TRAVERSANTS

- Installation de composants
- Radiateur
- Arrimage de composants
- Trous non métallisés
- Trous métallisés
- Fils de liaison

## ASSEMBLAGES AVEC COMPOSANTS MONTÉS EN SURFACE

- CHIP, MELF, LCCC, SOIC QFP, SOJ PLCC, connexions droites et plates, composants de grande taille, DPAK, PQFN, BGA
- Fils de liaisons

## CONNEXIONS ENROULÉES SANS BRASURE

- Nombres de spires, espacement
- Enroulement de l'extrémité de l'isolant
- Chevauchement des spires
- Disposition et mou du fil
- Isolants, conducteurs et bornes endommagés

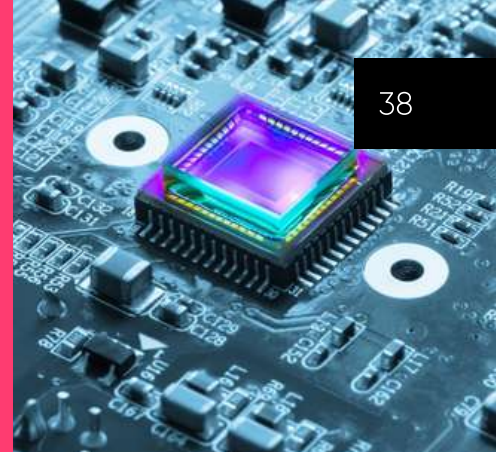
## COMPOSANTS ENDOMMAGÉS, CARTES DE CIRCUIT IMPRIMÉ ET ASSEMBLAGES

- Circuit imprimé : contacts dorés, conditions des laminés, marquage, propretés, revêtements
- Composant endommagé

## TESTS

- 1 test par module (9) sous forme de QCM

# RE-CERTIFICATION INSPECTEUR IPC-A-610 « ACCEPTABILITÉ DES ASSEMBLAGES ÉLECTRONIQUES »



38

## DURÉE

- 2 jours

## TARIF

Sur devis

## LANGUES



## PRÉREQUIS

Notions de base assemblage PCB et technologies composants.

## PUBLIC CONCERNÉ

Responsables qualité, ingénieurs Process, techniciens et opérateurs, contrôleurs visuels et réparateurs des produits électroniques.

## OBJECTIF

Utilisation et compréhension des critères de la norme IPC-A-610. Support de formation IPC-A-610 selon indice H. Maîtrise de cet outil de communication entre clients et fournisseurs. Validation de la formation par un certificat officiel IPC.

## FORMATEUR

Formateur certifié IPC.

## 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

### RAPPELS SUR LES MODULES FAISANT L'OBJET DE QUESTIONS À LIVRE FERMÉ

#### INTRODUCTION/RÈGLES ET PROCÉDURES PROFESSIONNELLES IPC

- Introduction
- Programme et durée de la certification
- Formateurs et spécialiste IPC
- Re certification et épreuve par challenge

#### AVANT-PROPOS, DOCUMENTS APPLICABLES ET MANIPULATION

- Champ d'application
- Conceptions spécialisées
- Termes et définitions
- Méthodologie d'inspection
- Vérification des dimensions
- Instruments grossissants et éclairage
- Documents applicables
- Manipulation des cartes électroniques

### RAPPELS RAPIDES SUR LES PRINCIPAUX CRITÈRES DES 7 MODULES RESTANTS

#### INSTALLATION DES ACCESSOIRES

- Installation des accessoires, isolement, éléments de fixation
- Connecteurs, poignées, extracteurs, loquets
- Broches de connecteurs
- Harnais, faisceau de câblage, laçage
- Cheminement, croisements, rayon de courbure

#### CRITÈRES BRASURÉS (HAUTE TENSION INCLUSE)

- Exigences d'acceptabilité du brasage
- Anomalies de brasage
- Haute tension

#### CONNEXIONS À BORNE

- Clip latéral
- Accessoires sertis
- Préparation fil, étamage
- Préformage, réducteur de tension
- Installation
- Isolants, conducteurs
- Bornes, brasures
- Dommages

### **CRITÈRES POUR LA TECHNOLOGIE AVEC TROUS MÉTALLISÉS TRAVERSANTS**

- Installation de composants
- Radiateur
- Arrimage de composants
- Trous non métallisés
- Trous métallisés
- Fils de liaison

### **CRITÈRES POUR LA TECHNOLOGIE DES COMPOSANTS MONTÉS EN SURFACE**

- CHIP, MELF, LCCC, SOIC QFP, SOJ PLCC, connexions droites et plates, composants de grande taille, DPAK, PQFN, BGA
- Fils de liaisons

### **COMPOSANTS ENDOMMAGÉS, CARTES DE CIRCUIT IMPRIMÉ ET ASSEMBLAGES**

- Circuit imprimé : contacts dorés, conditions des laminés, marquage, propretés, revêtements
- Composant endommagé

### **CONNEXIONS ENROULÉES SANS BRASURE**

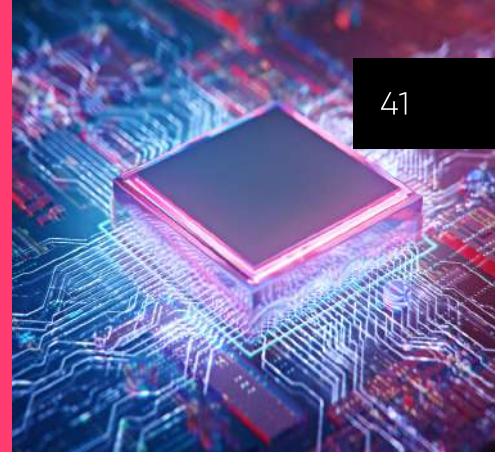
- Nombres de spires, espacement
- Enroulement de l'extrémité de l'isolant
- Chevauchement des spires
- Disposition et mou du fil
- Isolants, conducteurs et bornes endommagés

### **TESTS**

- 1 test par module (9) sous forme de QCM

# FIABILISATION D'UN ENSEMBLE ÉLECTRONIQUE

41



## DATES & LIEUX

- 10 au 12 sept. – Pessac
- 19 au 21 nov. – Pessac

## DURÉE

- 3 jours

## TARIF

2 160€

## LANGUES



### PRÉREQUIS

Niveau de technicien supérieur expérimenté ou d'ingénieur travaillant sur la qualité ou fiabilité d'un produit soit au niveau de sa fabrication ou de sa sélection.

### PUBLIC CONCERNÉ

Responsable technique ou de bureaux d'études, Ingénieur ou Chef de projet, responsable fiabilité.

### OBJECTIF

Apprendre une méthode permettant de fiabiliser un système électronique. La démarche permet de comprendre comment cerner le profil de vie du produit, de réaliser des analyses de risques technologiques afin de construire un plan de levée des risques ciblé (essais environnementaux accélérés par l'utilisation de modèles mathématiques, essais de robustesse, qualification des composants ...).

### 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

- Définitions de la fiabilité
- Défaillance, mode de défaillance et mécanisme de défaillance
- Défaillance abrupte (catalectique) et défaut d'usure
- Exemple de mécanismes de défaillance
- Théorie résistance/contrainte

### QUELQUES NOTIONS MATHÉMATIQUES

- Fonction taux de défaillance  $l(t)$
- Evolution du taux de défaillance dans le temps (courbe en baignoire)
- MTBF, MTTF
- Utilisation des lois statistiques et leur limitation :
  - Exponentielle
  - Weibull
- Echantillonnage :
  - $Ki^2$
  - Binomiale

### NOTRE APPROCHE : « LA FIABILISATION PAR LA TECHNOLOGIE »

- Définition du profil de vie du produit
- Analyse de risques (technologies versus profil de vie)
  - Composants et technologies : AEC-Q-XXX, PPAP, aéronautique, spatial...
  - Design
  - Industrialisation
- Essais de robustesse
  - HALT
  - Elaboration et réalisation d'un plan d'essais
- Essais de durabilité
  - Lois d'accélération (Arrhenius, Coffin Manson et Norris Landzberg, Hallberg Peck ...)
  - Construction d'un plan d'essais et séquençement des essais
- Qualification du procédé de fabrication
  - La maîtrise des procédés
  - L'audit fournisseur

## DÉVERMINAGE

- Définition du déverminage
- Le HASS, HASA, ESS
- POS et SOS
- Efficacité du déverminage

## LES MÉTHODE CLASSIQUES D'ÉVALUATION DE LA FIABILITÉ

- Les calculs théoriques (MIL-HDBK-217, IEC 62380, FIDES)
- Les filières d'essais (DO 160, EN 50155, ESA...)
- Le retour terrain (REX)

## EXERCICES PRATIQUES SUR UN CAS CONCRET

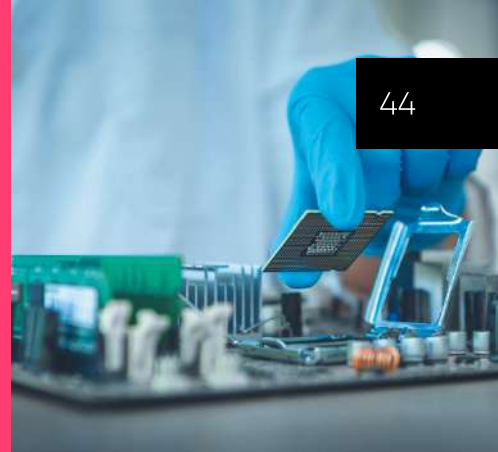
Tout au long de la formation des exercices sont proposés aux stagiaires :

- Exercices mathématiques (exponentielle, Weibull...)
- Définition du profil de vie
- Analyse de risques technologiques et industrialisation
- Définition d'un plan de robustesse
- Définition d'un plan d'essais durabilité (calcul des essais accélérés)

## QUESTIONS/RÉPONSES

# QUALIFICATION DES COMPOSANTS ÉLECTRONIQUES

44



## DATES & LIEUX

- 5 juin – Distanciel

## DURÉE

- 1 jour

## TARIF

750€

## LANGUES



### PRÉREQUIS

Niveau de technicien supérieur expérimenté ou d'ingénieur travaillant sur la qualité ou fiabilité d'un produit soit au niveau de sa fabrication ou de sa sélection.

### PUBLIC CONCERNÉ

Responsable technique ou de bureau d'études, Ingénieur ou Chef de projet, responsable fiabilité, responsable laboratoire d'essais.

### OBJECTIFS

- Comprendre les objectifs des essais de qualification des cartes et systèmes électroniques (milieu automobile) depuis les aspects théoriques de la définition des essais jusqu'aux aspects pratiques de leur réalisation (bonnes règles, réaction en cas de problèmes, rédaction des rapports d'essais...)
- Les principales normes en vigueur seront revues (ISO 16750, normes des fabricants automobiles...). Les aspects mathématiques seront abordés, d'une part pour le calcul des facteurs d'accélération et d'autre part, pour le calcul des échantillons nécessaires en fonction d'objectifs fiabilité.

### 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 GÉNÉRALE

### SENSIBILISATION AUX MÉCANISMES DE DÉFAILLANCES DES COMPOSANTS ÉLECTRONIQUES (CIBLÉ AUX ATTENTES)

- Liens avec les essais de qualification

### CONCEPTS DE BASE UTILES À LA QUALIFICATION

- Paramètres et lois de fiabilité
- Essais types ( HTOL, TC, THB...)
- Facteurs d'accélération (Arrhenius, Black, Coffin, Peck...)

### MÉTHODES ET NORMES DE QUALIFICATION (PLUS OU MOINS APPROFONDIES EN FONCTION DES ATTENTES)

- Knowledge based vs Stress based
- JESD47 (industrielle)
- MIL-STD
- ECSS (Spatial)
- AEC-Q (Automotive)
- JESD94 / JEP148 (exemple électromigration)

# QUALIFICATION DES SYSTÈMES ÉLECTRONIQUES (APPLICATION AUTOMOBILE)



46

## DURÉE

- 2 jours

## TARIF

Sur devis

## LANGUES



## PRÉREQUIS

Niveau de technicien supérieur expérimenté ou d'ingénieur travaillant sur la qualité ou fiabilité des composants soit au niveau de sa fabrication ou de sa sélection.

## PUBLIC CONCERNÉ

Responsable technique ou de bureaux d'études, Ingénieur ou Chef de projet, Responsable fiabilité, technicien d'essais, responsable laboratoire d'essais.

## OBJECTIF

- Comprendre les objectifs des essais de qualification des composants depuis les aspects théoriques de la définition des essais (mécanismes de défaillances, paramètres et lois de fiabilité) jusqu'aux aspects pratiques de leur réalisation (facteurs d'accélération, échantillonnage...).
- Appréhender les principales normes en vigueur (MIL, JEDEC, AEC, ESCC, JESD...)

## 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

- Définitions de la fiabilité
- Défaillance, mode de défaillance et mécanisme de défaillance
- Défaillance abrupte (catalectique) et défaut d'usure
- Exemple de mécanismes de défaillance
- Théorie résistance/contrainte

### QUELQUES NOTIONS MATHÉMATIQUES

- Fonction taux de défaillance  $l(t)$
- Evolution du taux de défaillance dans le temps (courbe en baignoire)
- MTBF, MTTF
- Utilisation des lois statistiques et leur limitation :
- Exponentielle
- Weibull

### LOIS D'ACCÉLÉRATION / CONSTRUCTION D'UN PLAN D'ESSAIS

- Lois d'accélération (Arrhenius, Coffin Manson et Norris Landzberg, Hallberg Peck ...)
- Construction d'un plan d'essais et séquençement des essais
- Qualification des procédés de fabrication

### MÉTHODE DE DÉFINITION D'UN PLAN D'ESSAI

- Définition du profil de vie du produit
- Analyse de risques (technologies versus profil de vie)
  - Composants et technologies : PPAP...
  - Design
  - Industrialisation
- Stress Based Testing (AEC Qxxx)
- Essais de robustesse
  - HALT
  - Elaboration et réalisation d'un plan d'essais
- Essais de durabilité
- Revue des différents essais proposés dans les normes (définition et objectif de chaque type d'essai)
  - HTOL/THB/STORAGE/PC/TC/ESD/THB/T&H cyclé/Essais mécaniques, brouillard salin...



## **ECHANTILLONNAGE**

- Lois d'accélération (Arrhenius, Coffin Manson et Norris Landzberg, Hallberg Peck ...)
- Construction d'un plan d'essais et séquençement des essais
- Qualification des procédés de fabrication

## **NIVEAU MSL ET ESD**

- MSL
- ESD

## **DÉVERMINAGE**

- Définition
- Mise en place (SOS, POS, surveillance, monitoring...)

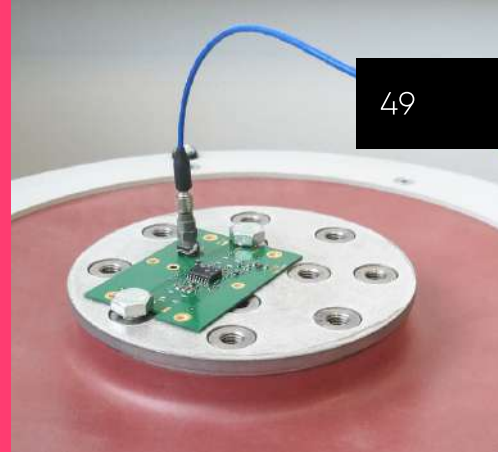
## **SYNTHÈSE**

## **FOCUS AUTOMOBILE, REVUE DES NORMES EXISTANTES (EXEMPLES)**

- ISO 16750
- Spécifications d'essais des principaux fabricants de véhicules automobiles

# FIABILITÉ ÉLECTRONIQUE ET VIBRATION

49



## DATES & LIEUX

- 19 et 20 juin - Ecully
- 3 et 4 déc. - Ecully

## DURÉE

- 2 jours

## TARIF

1 800€

## LANGUES



Cette formation est dispensée dans les locaux de Vibratec, partenaire de SERMA Technologies.

La première journée de formation est dispensée par un formateur de SERMA, et la deuxième journée est dispensée par un formateur de Vibratec



## PRÉREQUIS

Des bases en mécanique et électronique.

## PUBLIC CONCERNÉ

Responsables projets, Techniciens et ingénieurs d'essai, laboratoire et bureaux d'études...

## OBJECTIFS

- Comprendre l'intérêt des mesures vibratoires et différencier les techniques de mesures vibratoires,
- Comprendre l'intérêt du dimensionnement vibratoire,
- Comprendre les tests normatifs.

## FORMATEUR

Ingénieur Chef de Projet / en partenariat avec Vibratec.

## 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****JOUR 1 : ENJEUX ET LIMITES DE LA FIABILITÉ ÉLECTRONIQUE VIS-À-VIS DE LA CONTRAINTE DE VIBRATION**

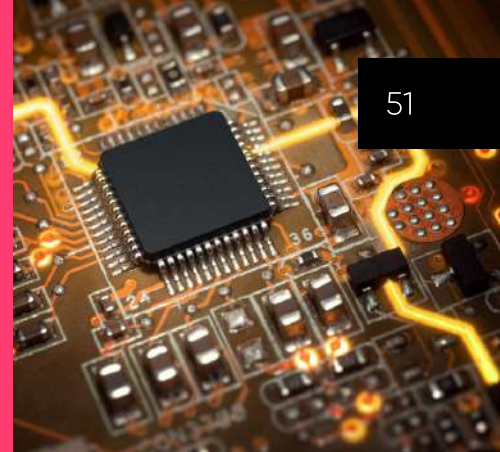
- Introduction à la fiabilité électronique et mécatronique
- Les défaillances des électroniques en vibration
  - Principaux modes et mécanismes de défaillance
  - Cas des brasures
- Les recueils de fiabilité (MIL-HDBK217, IEC62380, FIDES) vs vibration
- Les essais types sur composants et cartes
- Les essais de robustesse et de vieillissement accéléré vs vibration

**JOUR 2 : ANALYSES EXPERIMENTALES ET ESSAIS APPLICABLES À L'ÉLECTRONIQUE**

- Introduction et base théorique :
- L'analyse vibratoire expérimentale :
  - La chaîne de mesure
  - Position des points de mesure
  - Traitement du signal : analyse temporelle, spectre, DSP
  - Déformée en fonctionnement
  - Mesure de déformation
- L'analyse modale expérimentale
  - Fonction de réponse en fréquence
  - Mise en œuvre de l'AME : les différentes étapes
  - Précautions spécifiques sur cartes électroniques
- L'approche fiabiliste appliquée
  - Analyse en fatigue : Courbe de Wöhler et calcul de dommage
  - Les chargements : personnalisation d'essai / normes de transport
  - Les normes transports (selon les participants)
  - Stade de la conception : Modélisation numérique et analyse des résultats
  - Stade de la validation : Essais sur table vibrante

# FIABILITÉ ET ÉLECTRONIQUE DE PUISSANCE

51



## DATES & LIEUX

- 2 au 3 octobre - Pessac

## DURÉE

- 2 jours

## TARIF

1460€

## LANGUES



## PRÉREQUIS

Niveau de technicien supérieur expérimenté ou d'ingénieur avec des connaissances de base en électronique.

## PUBLIC CONCERNÉ

Technicien supérieur expérimenté, ingénieur ou chef de projet, responsable technique ou de bureau d'étude, responsable qualité ou fiabilité.

## OBJECTIF

Connaître les technologies mises en jeu (diode, MOSFET, IGBT en Si, SiC et GaN) et apprendre une méthode permettant de « fiabilisation par la technologie » d'un module de puissance, du profil de vie au plan de levée des risques (performance, robustesse, durée de vie, variabilité process), en passant par l'analyse des risques (mécanismes de défaillances).

## 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

- Généralités sur l'électronique de puissance (historique, définitions)
- Périmètre des modules de puissance traités dans le cours (6500V - 500A)

### PRESENTATION DES TECHNOLOGIES D'UN MODULE DE PUISSANCE

- Puces
  - Diodes
  - MOSFET
  - IGBT
  - Nouvelles technologies SiC et GaN
- Connectiques
  - Connectiques des dessus des puces (câblages filaires, rubans, etc.)
  - Connectiques des dessous des puces et substrats (brasures, frittages, etc.)
  - Connectiques de puissance (broches brasées, vissées, etc.)
- Substrats/Embases
  - Nature et caractéristiques des substrats (SMI, AL<sub>2</sub>O<sub>3</sub>, AlN, Si<sub>3</sub>N<sub>4</sub>, DBC, AMB, etc.)
  - Nature et caractéristiques des embases (Cu, AlSiC, etc.)

### NOTRE APPROCHE DE « FIABILISATION PAR LA TECHNOLOGIE »

- Profil de vie du produit
- Analyse de risques
  - Mécanismes de défaillance (levées de câblages filaires, délaminations dans les brasures, etc.)
- Plan de levée des risques
  - Performance (norme / spécification)
    - automobile (AECQ, AQG-324...), aéronautique (DO), spatial (ESCC...), ferroviaire (IEC...), ...
- Robustesse
  - Définition de la robustesse
  - Construction d'un plan d'essais, séquençement des essais
  - Exemple du HALT
- Durée de vie
  - Revue des essais et leurs lois d'accélération (Arrhenius, Coffin Manson, etc.)
  - Construction d'un plan d'essais, séquençement des essais
- Variabilité des procédés
  - La maîtrise des procédés
  - L'audit fournisseur

# STOCKAGE ÉNERGIE ÉLECTRIQUE : BATTERIES



## DATES & LIEUX

- 19 au 20 mars - Pessac
- 19 au 20 nov. - Chambéry

## DURÉE

- 1,5 jour

## TARIF

1 100 €

## LANGUES



## PRÉREQUIS

Aucun.

## PUBLIC CONCERNÉ

Ingénieur qualité AQF, responsable produits, auditeur, chef de projet, ingénieur, technicien Process, technicien de laboratoire d'expertise...

## OBJECTIFS

- Appréhender les différentes familles de batteries existantes et leurs caractéristiques pour une aide au choix technologique.
- Développement des bonnes pratiques lors de l'utilisation et la manipulation des batteries.

## FORMATEUR

Formateur SERMA Ingénieur Expert Batteries avec plusieurs années d'expérience en R&D matériaux pour le stockage électrochimique.

## 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

Les technologies suivantes seront présentées : Plomb-acide/Ni-MH/Ni-Cd/Lithium Ion. Quelques éléments d'informations complémentaires seront apportés sur les autres technologies de stockage électrochimiques (à savoir les super condensateurs et les piles à combustible).

Les points principaux du programme sont les suivants :

### **PARTIE 1 : INTRODUCTION SUR LE FONCTIONNEMENT GÉNÉRAL D'UN ACCUMULATEUR**

- Appréhender les principes électrochimiques de base
- Comprendre la structure et le fonctionnement d'un accumulateur
- Piles, batteries et autres types d'accumulateurs

### **PARTIE 2 : DÉFINITION DES GRANDEURS ÉLECTRIQUES**

- Tension, énergie, puissance
- Déterminer ses propriétés

### **PARTIE 3 : TECHNOLOGIES DISPONIBLES ET MARCHÉ**

- Plomb-Acide
- Nickel (Ni-Cd et NiMH)
- Le Li-ion et li métal

### **PARTIE 4 : SÉCURITÉ ET FIABILITÉ DES BATTERIES**

- Sécurité des batteries
- BMS
- Bonnes pratiques (Recommandations des conditions de livraison et de réception et points critiques)



# SÉCURITÉ DES BATTERIES

55



## DATES & LIEUX

- 5 juin- Distanciel

## DURÉE

- 1 jour

## TARIF

750 €

## LANGUES



## PRÉREQUIS

Aucun.

## PUBLIC CONCERNÉ

Ingénieur qualité AQF, responsables produits, auditeur, chef de projet, ingénieur, technicien Process, technicien de laboratoire d'expertise...

## OBJECTIF

Développer les bonnes pratiques lors de l'utilisation et la manipulation des batteries.

## FORMATEUR

Ingénieur Process, 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****PARTIE 1 : INTRODUCTION SUR LE FONCTIONNEMENT GÉNÉRAL D'UN ACCUMULATEUR**

- Bases de l'électrochimie et lien avec les batteries
- Comprendre la structure et le fonctionnement d'un accumulateur
- Grandeurs électriques

**PARTIE 2 : TECHNOLOGIES DISPONIBLES ET MARCHÉ**

- Cas des technologies lithium (li-ion).
  - Chimies existantes et matériaux, forces et faiblesses
  - Design cellules, modules et packs

**PARTIE 3 : SÉCURITÉ ET FIABILITÉ DES BATTERIES, FOCUS SUR LES BATTERIES LI-ION**

- Sécurité associées à l'utilisation des batteries
  - Protections intrinsèques
  - Chimies vs. Fiabilité,
  - Normes et certifications (utilisation, transport et safety)
  - Définition d'un Plan de qualification typique
  - Battery Management System
- Bonnes pratiques
  - Recommandations des conditions de livraison, de réception et d'expédition
  - Points critiques à considérer lors de l'utilisation et l'intégration des batteries
  - Recyclage

# TECHNOLOGIES DES SUPERCONDENSATEURS



## DURÉE

- 1 jour

## TARIF

Sur devis

## LANGUES



## PRÉREQUIS

Aucun.

## PUBLIC CONCERNÉ

Ingénieur qualité AQF, responsables produits, auditeur, chef de projet, ingénieur, technicien process, technicien de laboratoire d'expertise...

## OBJECTIFS

- Appréhender et comprendre le fonctionnement d'un supercondensateur afin d'être une aide dans le choix technologique.
- Développer les bonnes pratiques lors de l'utilisation et la manipulation des supercondensateurs.

## FORMATEUR

Formateur SERMA, Ingénieur Expert Batteries avec plusieurs années d'expérience en R&D matériaux pour le stockage électrochimique.

## 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****PARTIE 1 : INTRODUCTION SUR LE FONCTIONNEMENT GÉNÉRAL D'UN SUPERCONDENSATEUR**

- Accumulateurs et lien avec les supercondensateurs
- Comprendre la structure et le fonctionnement d'un supercondensateur
- Positionnement par rapport aux technologies classiques de condensateurs
- Positionnement par rapport aux autres technologies d'accumulateurs
- Grandeurs électriques caractéristiques

**PARTIE 2 : TECHNOLOGIES DISPONIBLES**

- Technologies commerciales de supercondensateurs
  - Chimies existantes et matériaux clés, forces et faiblesses
  - Design cellules, modules et packs
- Performances électriques et vieillissement
  - Fonctionnement nominal
  - Introduction à la problématique du floating et de l'équilibrage
  - Mécanismes de vieillissements

**PARTIE 3 : SÉCURITÉ ASSOCIÉE À L'UTILISATION DES SUPERCONDENSATEURS**

- Risques en fonctionnement normal et hors limites
- Risques en cas d'ouvertures des cellules
- Protections intrinsèques et Battery Management System
- Standards environnementaux (utilisation, transport et safety)

**PARTIE 4 : BONNES PRATIQUES (RAPPORTÉES AU CYCLE DE VIE DES SUPERCONDENSATEURS AU SEIN DE L'ENTREPRISE)**

- Réception et stockage initial
- Sécurisation des manipulations (assemblage, tests électriques, réparations)
- Stockage final (supercondensateurs cyclés, en fin de vie, défaillants)
- Recyclage et/ou réexpédition

# SENSIBILISATION AUX SYSTEMES HYDROGENES



## DURÉE

- 1 jour

## TARIF

Sur devis

## LANGUES



## PRÉREQUIS

Aucun.

## PUBLIC CONCERNÉ

Tout public.

## OBJECTIF

- Avoir une vue globale de la chaîne hydrogène et les systèmes basés sur l'hydrogène.

## FORMATEUR

Ingénieur chargé d'affaires

## 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

### INTRODUCTION

### LES PROPRIÉTÉS GÉNÉRALES DE L'H<sub>2</sub>

- Les propriétés physiques de l'Hydrogène
- Les implications générales (Safety, systèmes etc)

### LA CHAÎNE HYDROGÈNE

- Production de l'hydrogène
- Hydrogène industriel vs Hydrogène Energie
- Stockage de l'hydrogène
- Transport de l'hydrogène

### SYSTÈMES ÉLECTROCHIMIQUES

- Introduction au composant : La pile à combustible
- Présentations des auxiliaires de la pile à combustible
- Les électrolyseurs – une introduction aux technologies usuelles

### LA COMBUSTION H<sub>2</sub> – UNE INTRODUCTION

- La combustion
- Exemples de combustion H<sub>2</sub>
- Phénomènes liés à la combustion

### INITIATIVES, PROJETS, DÉMONSTRATEURS

- Hydrogène gazeux
- Hydrogène liquide
- Combustion
- Initiatives de l'EU, des pays, des entreprises

# TECHNIQUES D'ANALYSES PHYSICO-CHIMIQUES DES SURFACES DE MATÉRIAUX



## DATES & LIEUX

- 8 et 9 oct. - Écully
- + 7 oct (option de 0.5 jour)

## DURÉE

- 2 ou 2.5 jours

## TARIF

1 990€  
Option 1/2 journée : 510€

## LANGUES



### PRÉREQUIS

Formation initiale scientifique Bac+2.

### PUBLIC CONCERNÉ

Ingénieurs et techniciens du milieu industriel qui sont confrontés à des phénomènes liés aux surfaces.

### OBJECTIFS

- Sensibiliser les industriels aux différents aspects de l'analyse de surface, aux informations qu'il est possible d'obtenir afin qu'ils puissent appréhender plus facilement les potentialités de ces techniques.
- Présenter de façon claire et concrète les applications des principales techniques d'analyse de surface.
- Montrer directement, au cours de travaux pratiques sur nos instruments, le déroulement d'une analyse de surface, de la préparation des échantillons à l'interprétation des données analytiques.

### FORMATEUR

Docteurs-ingénieurs et ingénieurs matériaux, spécialistes de l'analyse de surface.

### 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 THÉORIQUE

- Notion de surface
- Interaction rayonnement-matière
- Spectroscopies d'électrons : XPS et AES
- Spectrométries d'ions : SIMS dynamique et SIMS statique
- Spectrométrie GD-OES
- Synthèse et stratégie en analyse de surface

## FORMATION PRATIQUE SUR LES APPAREILS

- TP XPS : analyse chimique et quantitative d'un polymère, estimation de l'épaisseur d'une couche d'oxyde, étude d'une contamination de surface, abrasion ionique
- TP SIMS : SIMS dynamique et statique - recherche et identification d'éléments traces en surface, réalisation d'un profil en profondeur, dépouillement d'un spectre de masse, imagerie d'extrême surface
- TP GD-OES : analyse qualitative d'un matériau multicouches, analyse quantitative d'un revêtement

## TRAVAUX DIRIGÉS

- Applications industrielles basées sur des études de cas adaptés aux domaines des participants.

### PROGRAMME OPTIONNEL (½ JOURNÉE)

## FORMATION THÉORIQUE

- Microscopie Electronique à Balayage (MEB) en analyse de surface
- Infra-Rouge à Transformée de Fourier (IRTF) en analyse de surface

## FORMATION PRATIQUE SUR LES APPAREILS

- TP MEB : observations de multicouches et revêtements, défauts de bonding et pollutions de contacts
- TP IRTF : microscopie sur des pollutions de contacts, identification de composés organiques

# CYBERSÉCURITÉ ET CONFORMITÉ IOT DIRECTIVE RED

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

63



## DATES & LIEUX

- 23 et 24 janv. – Distanciel
- 9 et 10 avril – Distanciel
- 24 et 25 sept.- Paris

## DURÉE

- 2 jours

## TARIF

1800€

## 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

### FONDEMENTAUX 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.

65



## DATES & LIEUX

- 17 et 18 sept. – Distanciel

## DURÉE

- 2 jours

## TARIF

2 600€

## 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

- 8 et 9 oct. – 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
- 8 au 10 oct. – Pessac

## 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

- 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

76



## DATES & LIEUX

- 28 au 30 mai – Paris
- 5 au 7 nov. – Toulouse

## 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 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)

80



## 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.

## OBJECTIFS

- 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)

82



## 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

1 460€

## 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)

85



## 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)

87



## 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

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 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

89



## DATES & LIEUX

- 12 au 14 mars - Paris
- 25 au 27 juin - Lyon
- 15 au 17 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

92



## 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



94

## 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



## 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



99

## 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



101

## 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

103



## 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)

105



## DATES & LIEUX

- 26 au 28 mars - Pessac
- 10 au 12 oct. - Grenoble

## DURÉE

- 3 jours

## TARIF

2 160€

## LANGUES



### PRÉREQUIS

Connaissances en électronique.

### PUBLIC CONCERNÉ

Chef de projet, développeur, qualiticien.

### OBJECTIF

Présenter les différentes normes, méthodes, outils et techniques d'analyse utilisées 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

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

- 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