

CYBERSÉCURITÉ DES DISPOSITIFS MÉDICAUX

IEC 81001-5-1

Réalisable en présentiel ou à distance

English version on the next page ›

Plusieurs formats de formation sont disponibles, contactez-nous pour plus d'informations.

DESCRIPTIF DE LA FORMATION

Cette formation est une introduction à la démarche de cybersécurité appliquée aux dispositifs médicaux, décrivant les processus du cycle de vie du dispositif médical et de son logiciel et les méthodologies utilisables pour répondre aux exigences réglementaires et normatives relatives à la gestion des risques de cybersécurité.

OBJECTIFS PÉDAGOGIQUES

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

- Situer la cybersécurité dans l'écosystème médical et appréhender les exigences réglementaires en la matière
- Conduire l'appréciation des risques de cybersécurité
- Mettre en œuvre les exigences de la norme IEC 81001-5-1
- Planifier le détail des actions à mener et des vérifications à effectuer pour chaque partie du cycle de vie du DM
- Sélectionner les outils requis pour mener des audits de code
- Planifier la réponse à un incident de cybersécurité

PROGRAMME

- **Introduction – rappel des concepts de base**
- **Contexte réglementaire et normatif de la cybersécurité des DM**
 - Règlements UE et US, principes et démarche
 - Panorama des normes applicables
- **Exigences de l'IEC 62304 et de l'IEC 60601-1**
- **Présentation de la norme IEC 81001-5-1**
 - Processus et activités requis
- **Présentation des normes IEC 62443 & 60601-4-5**
 - Définition des niveaux de sûreté et des exigences fondamentales
 - Détermination des capacités de sûreté : IEC 62443-4-2
 - Application aux SEMP : IEC 60601-4-5
- **Normes collatérales applicables aux DM connectés**
 - IEC 80001-1 et rapports techniques associés
- **Gestion des risques de sûreté**
 - Appréciation des risques / ISO 14971
 - Modélisation des menaces (Threat Modeling)
 - Evaluation des vulnérabilités / standard CVSS
- **Processus de développement sécurisé**
 - Standard de conception sécurisée (Secure by design)
 - Utilisation de logiciels tierce-partie (SOUP, OTS)
- **Outils d'audit de cybersécurité des logiciels**
- **Réponse aux événements de cybersécurité**
- **Questions et conclusion**

TARIFS ET RÉFÉRENCES

Type	Référence	Durée	Tarif HT
INTER	1.01.04.0018	1 jour (7 h)	960 €
INTRA	2.01.04.0019	1 jour (7 h)	1 980 €*

* Forfait pour 6 personnes maximum

INFORMATIONS UTILES

Public concerné

Ce stage s'adresse aux chef de projet ou de produits, développeurs logiciels, architectes système, responsables cybersécurité, auditeurs internes, responsables des règlements et affaires médicales.

Prérequis

Principes généraux d'ingénierie système et logiciel ; la connaissance du système de gestion de l'assurance qualité (ISO 13845) et des principes de base de la gestion des risques est souhaitable.

Moyens pédagogiques, techniques et d'encadrement

Chaque participant reçoit un support de cours numérique. Le programme pédagogique de la session précise les méthodes utilisées. Nos formations sont 100 % synchrones, avec un formateur expert.

Modalités de suivi des stagiaires

Questionnaire d'entrée, quiz à mi-parcours, questionnaire de sortie et questionnaire de satisfaction.

Sanction de la formation

Le suivi de ce parcours donne lieu à la délivrance d'une Attestation de fin de formation nominative détaillant les compétences acquises, ainsi qu'un Certificat de réalisation destiné à votre OPCO.

Financements

Cette formation peut être prise en charge par votre OPCO, selon les conditions applicables à votre branche professionnelle. Une demande de subrogation de paiement peut également être étudiée.

Délai d'accès

Les groupes sont constitués en fonction de la demande, au plus tard quatre semaines avant le début de la session.

Accessibilité aux personnes en situation de handicap

Nos formations sont ouvertes à tous. Si vous êtes en situation de handicap et avez besoin d'aménagements spécifiques, contactez notre correspondant handicap :

Tél. : +33 5 61 30 69 00 • formation@isit.fr

Formation non certifiante au titre du RNCP et du Répertoire spécifique (RS).

Mise à jour : 01/10/2026

MEDICAL DEVICE CYBERSECURITY IEC 81001-5-1

Available in person or remotely

Several training formats are available, please contact us for more information.

COURSE DESCRIPTION

This course is an introduction to the cybersecurity approach applied to medical devices. It describes the life-cycle processes of the medical device and its software, together with the methodologies available to meet the regulatory and normative requirements for cybersecurity risk management.

LEARNING OBJECTIVES

By the end of the course, the learner will be able to:

- ▶ Position cybersecurity within the medical ecosystem and understand the applicable regulatory requirements
- ▶ Carry out cybersecurity risk assessment
- ▶ Implement the requirements of IEC 81001-5-1
- ▶ Plan in detail the actions and verifications required for each part of the medical device life cycle
- ▶ Select the tools needed to perform code audits
- ▶ Plan the response to a cybersecurity incident

PROGRAM

- **Introduction – review of the basic concepts**
- **Regulatory and normative context of medical device cybersecurity**
 - EU and US regulations: principles and approach
 - Overview of the applicable standards
- **Requirements of IEC 62304 and IEC 60601-1**
- **Introduction to IEC 81001-5-1**
 - Required processes and activities
- **Introduction to IEC 62443 & IEC 60601-4-5**
 - Definition of security levels and foundational requirements
 - Determining security capabilities: IEC 62443-4-2
 - Application to MEES: IEC 60601-4-5
- **Collateral standards applicable to connected medical devices**
 - IEC 80001-1 and related technical reports
- **Security risk management**
 - Risk assessment / ISO 14971
 - Threat modeling
 - Vulnerability assessment / CVSS standard
- **Secure development process**
 - Secure-by-design standards
 - Use of third-party software (SOUP, OTS)
- **Software cybersecurity audit tools**
- **Response to cybersecurity events**
- **Questions and conclusion**

PRICES AND REFERENCES

Type	Reference	Duration	Price excl. VAT
INTER	1.01.04.0018	1 day (7 h)	€960
INTRA	2.01.04.0019	1 day (7 h)	€1,980*

* Flat rate for up to 6 participants

USEFUL INFORMATION

Target audience

This course is intended for project or product managers, software developers, system architects, cybersecurity managers, internal auditors and regulatory / medical affairs managers.

Prerequisites

General principles of system and software engineering; knowledge of the quality assurance management system (ISO 13485) and of the basics of risk management is recommended.

Teaching methods, technical resources and supervision

Each participant receives a digital course manual. The training program for the session specifies the methods used. Our training courses are 100% instructor-led and live, delivered by an expert trainer.

Trainee monitoring

Entry questionnaire, mid-course quiz, exit questionnaire and satisfaction survey.

Training completion certification

Completion of this training program leads to the issuance of a personalized Certificate of Training Completion detailing the skills acquired, as well as a Certificate of Attendance/Completion intended for your OPCO.

Funding

This training course may be funded by your OPCO, subject to the conditions applicable to your professional sector. A payment subrogation request may also be considered.

Lead time for enrollment

Training groups are formed according to demand, no later than four weeks before the start of the session.

Accessibility for people with disabilities

Our training courses are open to everyone. If you have a disability and require specific accommodations, please contact our Disability Coordinator:

Tel.: +33 5 61 30 69 00 • formation@isit.fr

Non-certified training program under the RNCP and the Specific Directory (RS).

Last updated: 01/10/2026