Safety and security

Secure Embedded Systems

Ensuring the security of embedded systems is important to prevent unauthorized access or manipulation of the system and to protect the confidentiality, integrity, and availability of the system and its data.

There are various approaches to securing embedded systems, including the use of secure processors and specialized security hardware, the implementation of security protocols, and the use of secure coding practices. It is also important to have a system in place for distributing updates and patches to address newly discovered vulnerabilities.

At AC6 Training, we offer a range of courses on embedded security, including courses on secure coding practices, hardware security, and the use of secure processors.

Cours principaux

oC1 - Effective MISRA C MISRA C:2023, including guidelines for safety and security supporting all published versions of the C standard MISRA C:2023, the latest version of the MISRA C standard, which includes guidelines for safety and security supporting all published versions of the C standard. The course has been designed for the smooth and successful adoption of MISRA C into an organization. Lectures, exercises, tests, hands-on sessions and, optionally, a final exam, will significantly strengthen the skills and competences of teams involved in the design, development and verification of critical embedded software systems.

oC2 - MISRA Compliance for Project Managers Manage MISRA compliance, ensuring improved project outcomes and code quality in safety-critical systems MISRA for Project Managers, provides essential insights for managers overseeing projects that require MISRA compliance. It highlights the importance of MISRA standards in safety-critical systems across various industries. The training emphasizes key aspects such as negotiation, planning, execution, and assessment of MISRA compliance, and equips managers with the knowledge to make informed decisions. By enhancing managerial awareness and skills, it ensures better project outcomes, reduced costs, and improved code quality. This training is invaluable for project leaders seeking to streamline MISRA integration and enhance organizational efficiency.

oSEC1 - Développement sécurisé pour les systèmes embarqués Il s'agit d'une formation en ligne en direct Ce cours propose une introduction à la sécurité intégrée et traite des normes industrielles telles que ISO/SAE 21434, IEC 62443, NIST SP 800-53, Common Criteria et OWASP. Il aborde les bonnes pratiques de codage sécurisé pour C/C++ et introduit le langage de programmation RUST avec ses fonctionnalités de sécurité intégrées. Les stagiaires apprendront les méthodologies de développement de logiciels sécurisés, les tests de sécurité et la cryptographie dans les systèmes intégrés. Le cours couvre la conception et la mise en Œuvre d'une architecture matérielle sécurisée et de protocoles de communication pour les systèmes intégrés. En outre, il donne un aperçu des meilleures pratiques de sécurité pour les dispositifs et les systèmes IoT.

oSEC2 - Sécurité avancée des systèmes embarqués Créer des systèemes embarqués connectés sécurisés Découvrir comment protéger vos programmes contre les entrées malveillantes des utilisateurs, sécuriser les logiciels et les considérations du système, appréhender le contexte et l'utilisation des hyperviseurs et de la virtualisation du système et découvrir les contrôles et les outils de sécurité

oSEC12 - Programmation de systèmes embarqués sécurisés Le cours oSEC12 est conçu pour les ingénieurs logiciel qui ont besoin de concevoir, programmer et mettre en Œuvre des systèmes embarqués communicants sécurisés.. Ce cours est une combinaison du cours oSEC1 - Développement sécurisé pour les systèmes embarqués et du cours oSEC2 - Sécurité avancée des systèmes embarqués, avec un prix spécial lorsque les deux sessions consécutives sont réservées en une fois.

oSEC3 - wolfSSL pour la sécurité embarquée Le cours oSEC3 est conçu pour les ingénieurs logiciels et matériels afin de comprendre le fonctionnement de SSL/TLS, d'acquérir des connaissances fondamentales sur les algorithmes et les

protocoles cryptographiques et d'apprendre à mettre en Œuvre une authentification sécurisée avec wolfSSL

oSEC4 - wolfSSL avancé pour la sécurité embarquée Le cours oSEC4 est destiné aux ingénieurs logiciels et matériels. L'objectif de ce cours est de découvrir le fonctionnement du chiffrement et la gestion des clés secrètes, d'apprendre à mettre en Œuvre l'authentification sécurisée avec wolfSSL, de construire wolfSSH sur des plates-formes standard, de démarrer de manière sécurisée avec wolfBoot (avec wolfCrypt et WolfSSL) et de comprendre comment construire wolfMQTT sur des plates-formes standard et l'utiliser dans une application IoT

oSEC34 - Sécurité complète avec WolfSSL Le cours oSEC34 est conçu pour les ingénieurs logiciels/matériels qui ont besoin de comprendre pleinement le fonctionnement de SSL/TLS, d'établir une connaissance détaillée des algorithmes et protocoles cryptographiques et de mettre en Œuvre un environnement sécurisé complet, intégré dans une infrastructure à clé publique, avec wolfSSL. Ce cours est une combinaison du cours oSEC3 - wolfSSL pour la sécurité embarquée et du cours oSEC4 - wolfSSL avancé pour la sécurité embarquée, avec un prix spécial lorsque les deux sessions consécutives sont réservées en une fois.

oSEC5 - Embedded Security for STM32-based devices This course is designed to teach you about the security challenges faced by embedded systems and STM32-based devices. You will learn how to identify potential attack vectors and threats and understand the latest security standards and best practices for embedded systems. You will also learn about secure boot and firmware protection mechanisms and how to implement them.

oSEC6 - Embedded Security for NXP i.MX-based processors This course teaches the security challenges of embedded systems and NXP-based devices, covers latest security standards and best practices, and explains how to implement secure boot, network protocols, IoT security, and firmware updates.

oSEC7 - ARM TrustZone for Cortex-M based devices This course aims to provide an in-depth understanding of the ARM v8-M architecture and its security features. It covers topics such as the Memory Protection mechanism, Security Attribution unit configuration, management of Security access faults, and building and debugging secure and non-secure software. The objective is to equip attendees with the necessary knowledge and skills to develop secure applications for ARM v8-M based systems.

oSEC8 - Secured Embedded Linux Platform Build

Autres cours

C8 - Sureté et Fiabilité des Systèmes Critiques Les systèmes embarqués sont de plus en plus critiques et doivent répondre à des contraintes de sureté de fonctionnement de plus en plus drastiques. Cette formation vous présente les différents concepts et les standards qui s'appliquent aux systèmes critiques.