[redacted]

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.

- **oC1** Effective MISRA C: 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's processes. 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. 20 h **Renseignements**
- **oSEC2** Cybersecurity Professionals with an Embedded Systems Focus: This course provides embedded system developers and cybersecurity professionals with a comprehensive understanding of the cyber resilience Act and its impact on digital products. Participants will learn essential cybersecurity requirements, explore compliance pathways, and discover practical strategies for securing embedded systems throughout their lifecycle. The course also highlights market-ready tools and solutions to streamline adherence to the regulation while enhancing product resilience. 1 jour **Renseignements**
- **oSEC3** Développer en Sécurité des Systèmes Embarqués: Ce cours propose une introduction à la sécurité informatique 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 embarqués. Le cours couvre la conception et la mise en œuvre d'une architecture matérielle sécurisée et de protocoles de communication pour les systèmes IoT. Enfin, il propose un aperçu des méthodes pratiques pour sécuriser les dispositifs et les systèmes IoT. 18 h **Renseignements**
- **oSEC4** Sûreté et Sécurité des Systèmes Critiques: Les systèmes critiques doivent répondre à des contraintes de sûreté de fonctionnement de plus en plus drastiques. Cette formation vous présente les différents concepts et les standards qui s'appliquent aux systèmes critiques. 3 jours **Renseignements**
- **oC2** MISRA Compliance for Project Managers: MISRA for Project Managers provides essential insights for managers overseeing projects that require MISRA compliance. It emphasizes 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, ensuring 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 balance organizational efficiency. 8 h **Renseignements**
- **oSEC5** Sécurisation des applications embarquées: Ce cours est conçu pour les développeurs logiciel qui ont besoin de concevoir, programmer et mettre en œuvre des systèmes embarqués communicants sécurisés. Ce cours est avancé et les systèmes embarqués, abordés lors des deux sessions pratiques, sont restreints. 20 h **Renseignements**
- **oSEC6** 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. 12 h **Renseignements**
- **oSEC7** 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. 12 h **Renseignements**
- **oSEC8** ARM TrustZone for Cortex-M based devices: This course aims to provide an in-depth understanding of the ARM Cortex-M architecture and its security features. It covers topics such as the memory protection mechanism, security attribution unit configuration, and management of secure faults and interrupts. The course also delves into the development of secure and non-secure software. The objective is to equip attendees with the necessary knowledge and skills to develop secure applications for ARM Cortex-M based systems. 6 h **Renseignements**
- **oSEC9** Advanced Embedded Linux Security: 3 jours **Renseignements**
- **oSEC10** Secure Embedded Linux Platform Build: 12 h **Renseignements**
- **oSEC11** Development Secure Bootloaders: This course provides a comprehensive overview of the security challenges in embedded systems, focusing on the development of secure bootloaders. It covers topics such as cryptographic algorithms, secure boot processes, and hardware security features. The course also delves into the implementation of secure boot mechanisms, key management, and firmware updates. The objective is to equip attendees with the knowledge and skills to develop secure bootloaders for embedded systems. 12 h **Renseignements**
- **oSEC12** Développer des systèmes embarqués communicants sécurisés: Le cours oSEC12 est conçu pour les développeurs logiciel qui ont besoin de concevoir, programmer et mettre en œuvre des systèmes embarqués communicants sécurisés. Ce cours est avancé et les systèmes embarqués, abordés lors des deux sessions pratiques, sont restreints. 20 h **Renseignements**
- **oSEC13** Développer des applications sécurisées sous Linux: Ce cours est conçu pour les développeurs logiciel qui ont besoin de concevoir, programmer et mettre en œuvre des systèmes embarqués communicants sécurisés. Ce cours est avancé et les systèmes embarqués, abordés lors des deux sessions pratiques, sont restreints. 20 h **Renseignements**
- **oSEC14** Sécurisation des applications embarquées: Ce cours est conçu pour les développeurs logiciel qui ont besoin de concevoir, programmer et mettre en œuvre des systèmes embarqués communicants sécurisés. Ce cours est avancé et les systèmes embarqués, abordés lors des deux sessions pratiques, sont restreints. 20 h **Renseignements**
- **oSEC15** Sécurisation des systèmes Linux: Ce cours est conçu pour les développeurs logiciel qui ont besoin de concevoir, programmer et mettre en œuvre des systèmes embarqués communicants sécurisés. Ce cours est avancé et les systèmes embarqués, abordés lors des deux sessions pratiques, sont restreints. 20 h **Renseignements**
- **oSEC16** Sécurisation des systèmes Linux: Ce cours est conçu pour les développeurs logiciel qui ont besoin de concevoir, programmer et mettre en œuvre des systèmes embarqués communicants sécurisés. Ce cours est avancé et les systèmes embarqués, abordés lors des deux sessions pratiques, sont restreints. 20 h **Renseignements**
- **oSEC17** Sécurisation des systèmes Linux: Ce cours est conçu pour les développeurs logiciel qui ont besoin de concevoir, programmer et mettre en œuvre des systèmes embarqués communicants sécurisés. Ce cours est avancé et les systèmes embarqués, abordés lors des deux sessions pratiques, sont restreints. 20 h **Renseignements**
- **oSEC18** Sécurisation des systèmes Linux: Ce cours est conçu pour les développeurs logiciel qui ont besoin de concevoir, programmer et mettre en œuvre des systèmes embarqués communicants sécurisés. Ce cours est avancé et les systèmes embarqués, abordés lors des deux sessions pratiques, sont restreints. 20 h **Renseignements**
- **oSEC19** Sécurisation des systèmes Linux: Ce cours est conçu pour les développeurs logiciel qui ont besoin de concevoir, programmer et mettre en œuvre des systèmes embarqués communicants sécurisés. Ce cours est avancé et les systèmes embarqués, abordés lors des deux sessions pratiques, sont restreints. 20 h **Renseignements**
- **oSEC20** Sécurisation des systèmes Linux: Ce cours est conçu pour les développeurs logiciel qui ont besoin de concevoir, programmer et mettre en œuvre des systèmes embarqués communicants sécurisés. Ce cours est avancé et les systèmes embarqués, abordés lors des deux sessions pratiques, sont restreints. 20 h **Renseignements**