Safety and security

Embedded security

Embedded security is the practice of protecting embedded systems from cyber threats. These systems are found in a wide range of devices, including smartphones, automobiles, and medical equipment, and they are often used in critical applications. 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. Our courses are designed to provide professionals with the knowledge and skills they need to design and implement secure embedded systems. C1 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. 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. 2 days **Inquiry** C2 MISRA Compliance for Project Managers 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. 1 day **Inquiry** SEC1 Developing C/C++ Secure Embedded Systems This course provides an introduction to embedded security and covers industry standards such as ISO/SAE 21434, IEC 62443, NIST SP 800-53, Common Criteria, and OWASP. It covers secure coding practices for C/C++ and introduces the RUST programming language with its built-in security features. Students will learn about secure software development methodologies, security testing, and cryptography in embedded systems. The course covers the design and implementation of secure embedded system hardware architecture and communication protocols. Additionally, it provides an overview of security best practices for IoT devices and systems. 18 h **Inquiry** SEC10 Cyber Resilience Act and Embedded Systems This course provides embedded system developers and cybersecurity professionals with an in-depth 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 ensure adherence to the regulation while enhancing product resilience. 1 day **Inquiry** SEC2 Advanced Embedded Systems Security Discover how to protect your programs from malicious user input, Secure System Software and Consideration, Apprehend the context and the use of Hypervisors and System virtualization and Discover Security checks and Tools. 12 h **Inquiry** SEC12 Comprehensive Secure Systems Programming The oSEC12 course is designed for software engineers that need to design and program secure systems. This course is a combination of oSEC1 - Secure C/C++ Development for Embedded Systems course and oSEC2 - Advanced Embedded Systems Security course with a special price when both consecutive sessions are booked at once. 30 h **Inquiry** SEC6 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. 2 days **Inquiry** SEC7 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. 1 day **Inquiry** SEC8 Secured Embedded Linux Platform Build 2 days **Inquiry** SEC9 Advanced Embedded Linux Security 3 days **Inquiry** C8 Critical Systems Safety Embedded systems are more and more critical and subject to safety constraints. This training introduces the main concepts and standards applicable to safety-critical systems. 3 days **Inquiry**