Embedded Systems Secure Software Development

Duration: 3 Days

Description

Embedded Systems Secure Software Development aims to provide participants with knowledge and practical skills in secure software development by addressing the software and hardware components, communication infrastructures, and security requirements of embedded systems with a holistic approach.

Within the scope of the training, cyber security threats, vulnerabilities, and risks related to embedded systems are evaluated, and secure software development models, standards, and best practices are examined. Secure coding with C/C++, embedded system architectures, firmware security, communication protocols, cryptography fundamentals, and software security analyses are covered.

The program also addresses communication technologies such as Bluetooth, Wi-Fi, Zigbee, LoRa, and MQTT, secure data communication, sensor and actuator usage, and static and dynamic code analysis. Theoretical knowledge is reinforced through hardware-based laboratory applications using the C language on ESP32 and ESP8266 NodeMCU platforms.

At the end of the training, participants are expected to be able to evaluate security risks that may be encountered in embedded systems, recognize secure software development approaches, and gain knowledge of secure communication infrastructures for embedded systems.

Audience

Software developers and system designers who want to learn embedded systems and secure software development models and processes for embedded systems, software security testers, and industrial control system and IoT security testers can attend.

Outline

1. Threats and risks related to software and embedded systems

- Cyber security facts
- Why software security is critical
- Software attack examples

2. Information security fundamentals

- Information assets that need to be protected
- Vulnerabilities and threats
- Risk analysis

3. Secure software development models and frameworks

- Software development models
- CMMI, SSE-CMM, Microsoft Secure SDLC, OWASP OpenSAMM
- IEC 62443, Common Criteria

4. Vulnerability Databases

- CWE, CVE, CERT, DISA, OWASP Top 10, etc.

5. Industry 4.0 and Digital Transformation

6. Internetworking Infrastructure and TCP/IP Protocol Communication

7. Secure C/C++ coding

8. Collecting, Processing, and Presenting Data from Embedded Systems to Users

9. Communication Protocols of Embedded Systems

- Embedded system protocol characteristics
- Comparison of embedded system protocols and TCP/IP
- Embedded system communication protocols and areas of use (Bluetooth, Wi-Fi, Zigbee, LoRa, MQTT, etc.)
- Embedded system communication applications

10. Embedded System Sensors and Actuators

11. Firmware security

12. Cryptography fundamentals

- Symmetric and asymmetric cryptosystems
- Encryption algorithms
- Hashing algorithms
- Secure communication protocols

13. Software Security Analysis in Embedded Systems

- Static code analysis
- Dynamic code analysis

14. Social Engineering

Prerequisites

Basic knowledge of the C or C++ programming language. Applications will be carried out in the C language and on ESP32 and ESP8266 NodeMCU embedded systems.