

C1 - Effective MISRA C

MISRA C:2023, including guidelines for safety and security supporting all published versions of the C standard

Objectives

- Understand the C language pitfalls, the compilation process, static analysis techniques and tools
- Understand the origin and nature of MISRA C and its role in the development of safe and secure software
- Learn all important MISRA C guidelines and the unwanted phenomena they are designed to prevent
- Understand the notion of compliance to MISRA C and the permitted deviation procedures
- Discover and understand the advantages of the adoption of MISRA C and other best practices.

Course Environment

- Theoretical course
 - PDF course material (in English) supplemented by a printed version for face-to-face courses.
 - Online courses are dispensed using the Teams video-conferencing system.
 - The trainer answers trainees' questions during the training and provide technical and pedagogical assistance.
- At the start of each session the trainer will interact with the trainees to ensure the course fits their expectations and correct if needed

Target Audience

- Any embedded systems engineer or technician with the above prerequisites.

Evaluation modalities

- The prerequisites indicated above are assessed before the training by the technical supervision of the trainee in his company, or by the trainee himself in the exceptional case of an individual trainee.
- Trainee progress is assessed by quizzes offered at the end of various sections to verify that the trainees have assimilated the points presented
- At the end of the training, each trainee receives a certificate attesting that they have successfully completed the course.
 - In the event of a problem, discovered during the course, due to a lack of prerequisites by the trainee a different or additional training is offered to them, generally to reinforce their prerequisites, in agreement with their company manager if applicable.

Plan

Introduction

- Review of undefined, unspecified and implementation-defined behavior in C
- How the compilers may take advantage of undefined behavior
- Review of explicit and implicit casts
 - Balancing
 - Promotion
 - Arithmetic conversions
- Review of enumerated, integer and floating-point types: representation and operations.

- Review of common integer pitfalls
 - Overflow
 - Sign error
 - Extension
 - Truncation
- Review of common floating-point pitfalls
 - Error propagation
 - Comparison
 - Excess precision
- Review of arrays, strings, pointer types and associated programming errors
 - access outside bounds
 - Null-termination
 - Truncation
 - Off-by-one errors

Comprehensive Overview of MISRA C

- Introduction to MISRA
- The purpose of MISRA C and its role in improving code quality
- The MISRA C essential type system and other preliminary notions
- MISRA C:2012 guidelines related to not fully defined behavior of C
- Test on not fully defined behavior of C and related MISRA C guidelines

Advanced MISRA Guidelines

- Other important MISRA C:2012 guidelines.
- MISRA C:2012 guidelines for security
- Test on MISRA C violations and the best ways to deal with them.
- Properly formulating defensible claims of MISRA compliance.

Automated MISRA C Compliance

- Automatic verification of compliance to the MISRA C rules
 - Available tools
 - Tools proper configuration and use.
- Demonstrative analysis of the MISRA C violations in real software projects
 - Along with the correct remediation measures.

Renseignements pratiques

Inquiry : 2 days