



oC1 - 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.

Audience visée

- Le cours est destiné aux développeurs, ingénieurs et architectes ainsi qu'aux ingénieurs V&V et chefs de projet. Le contenu est destiné vers les personnes ayant une compréhension pratique du langage de programmation C; cependant, aucune connaissance préalable de MISRA C n'est requise. Le cours, qui privilégie autant que possible les approches participatives, est basé sur les méthodologies suivantes : cours/conférences, discussions, questions et réponses, démonstrations, sessions pratiques, exercices. Un examen final optionnel est également prévu.

Pré-requis

- Le contenu est destiné aux personnes ayant une compréhension pratique du langage de programmation C ; cependant, aucune connaissance préalable de MISRA C n'est requise.

Environnement du cours

- Cours théorique
 - Support de cours au format PDF (en anglais).
 - Cours dispensé via le système de visioconférence Teams.
 - Le formateur répond aux questions des stagiaires en direct pendant la formation et fournit une assistance technique et pédagogique.
- Au début de chaque demi-journée une période est réservée à une interaction avec les stagiaires pour s'assurer que le cours répond à leurs attentes et l'adapter si nécessaire

Course Outline

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.