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.

Environnement du cours

- Cours théorique
  - Support de cours au format PDF (en anglais) et une version imprimée lors des sessions en présentiel
  - Cours dispensé via le système de visioconférence Teams (si à distance)
  - 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

Audience visée

- Tout ingénieur ou technicien en systèmes embarqués possédant les prérequis ci-dessus.

Modalités d'évaluation

- Les prérequis indiqués ci-dessus sont évalués avant la formation par l'encadrement technique du stagiaire dans son entreprise, ou par le stagiaire lui-même dans le cas exceptionnel d'un stagiaire individuel.
- Les progrès des stagiaires sont évalués par des quizz proposés en fin des sections pour vérifier que les stagiaires ont assimilé les points présentés
- En fin de formation, une attestation et un certificat attestant que le stagiaire a suivi le cours avec succès.
  - En cas de problème dû à un manque de prérequis de la part du stagiaire, constaté lors de la formation, une formation différente ou complémentaire lui est proposée, en général pour conforter ses prérequis, en accord avec son responsable en entreprise le cas échéant.

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

Renseignements : 2 jours