MISRA clarifies safe and secure uses of the C language

New documents to be launched at the Device Developer Conference

Nuneaton, April 22nd 2016

MISRA is releasing new documents to clarify use of the MISRA C Guidelines in developing any application with high integrity or high reliability requirements – both safety related and security-related. The release will take place at a MISRA workshop at the Device Developer Conference in Cambridge on April 27th.

The MISRA C Guidelines (The latest version is MISRA C:2012 Guidelines for the Use of the C Language in Critical Systems.) are internationally accepted as setting out a subset of C for use in critical systems. Generally this is understood to mean for use in safe systems. However the guidelines are equally appropriate for secure systems, a topic of increasing concern with the growth of the Internet of Things. ISO/IEC JTC1/SC22/WG14 (the committee responsible for maintaining the C Standard) has published its C Language Security Guidelines (ISO/IEC 17961:2013). MISRA has carried out a coverage comparison between this and MISRA C:2012 and is publishing the resulting coverage matrix as MISRA C:2012 Addendum 2. Alongside MISRA C:2012 Amendment 1 "Additional security guidelines for MISRA C:2012", which includes a small number of additional guidelines, to improve the coverage of the security concerns highlighted by the ISO C Secure Guidelines, particularly in the use of "untrustworthy data", MISRA C is demonstrably suitable for both safe and secure applications.

"Anyone using the C language for system development, particularly for systems that have to safe and/or secure should be using the MISRA C Guidelines," said Andrew Banks Chairman of the MISRA C Committee. "The coverage matrix, plus the new rules, provides reassurance that code will be of high quality."

The other two documents address the issues of deviation and conformance.

Since the earliest days of MISRA C it has been recognised that it might, on occasion, be impracticable or unreasonable to follow the requirements of a specific guideline, so there has always been the option to declare and document a deviation, that is, an approved violation. However there is often confusion as to how a deviation can impact on declaring something as "MISRA Compliant" and even on what MISRA Compliance actually means.

MISRA Compliance 2016: Achieving compliance with MISRA Coding Guidelines, is designed to

- Provide clearer guidance on the use of deviations
- Provide a mechanism for establishing pre-approved permits for deviation

- Provide a mechanism for tailoring the classification of guidelines
- Define what is meant by MISRA Compliance

This guidance will become the standard approach for all future editions of both the MISRA C and MISRA C++ Guidelines. It is an optional enhancement to, and fully compatible with, all existing editions of the MISRA language guidelines.

One of the aims of the Compliance document is to "Provide a mechanism for establishing pre-approved permits for deviation." And the final document is MISRA C:2004 Permits, Deviation permits for MISRA Compliance. This gives example permits for use in developing a deviation document.

Copies of these documents will soon be available on the MISRA web site (MISRA.org.uk)

Notes for Editors

MISRA and MISRA C

MISRA, originally created as the Motor Industry Software Reliability Association, is a consortium concerned with promoting best practice in developing safety- and security-related embedded systems. MISRA publishes documents that provide accessible information for engineers and management, and holds events to permit the exchange of experience between practitioners. All contributors to MISRA donate their time as a personal commitment to the development of safer systems.

Current activities are MISRA C, MISRA C++, MISRA Autocode and MISRA Safety Analysis.

More information is available at misra.org.uk

Contact

David Ward, MISRA Project Manager E Mail david.ward@horiba-mira.com Tel 024 7635 5430	Andrew Banks, Chairman MISRA C Committee. E Mail andrew@andrewbanks.com