LDRA
Software Technology

MISRA C:2012 at a Glance

MISRA C is a software development language subset that was originally created to promote the use of the C programming language in safety-critical embedded applications within the motor industry. The original version was released in 1998 (MISRA C:1998) to target C90, and the 2004 version (MISRA C:2004) included a host of extensions and improvements to the original.

MISRA C:2012 is an evolution of the earlier MISRA C standards, ensuring that its contents will feel familiar for existing MISRA users while providing additional benefits for newcomers too. It benefits not only from the addition of rules to accommodate C99 functionality but also from improved rule precision, better rule categorisation, and more comprehensive explanation to educate as well as instruct.

With the aid of appropriate checking tools, it provides invaluable assistance to any organisation looking to protect themselves from the problems inherent in the inadvertent or deliberate misuse of the C language.

Key Details

- **Extend the coding guidelines to embrace unsafe elements of C99 while retaining support for C90**
- **Support and enhance the improved definition of undefined or unspecified behavior in C99**
- **Correct issues found in the 2004 version**
- **Provide backwards compatibility as much as possible to make it unnecessary to modify code when moving from MISRA-C:2004 to MISRA C:2012**
- **Ensure all guidelines include a detailed rationale and remove rules without strong rationale**
- **Increase the number of decidable rules to allow better tool enforcement and reduce the amount of manual checking, saving time and money**
- **Include guidance on the applicability of guidelines to automatically generated code**

Other Benefits

Instead of MISRA-C:2004's use of the term "rule", MISRA C:2012 subdivides "guidelines" into "rules" and "directives" where a directive is a guideline for which it is not possible to provide the full description necessary to perform a check for compliance.

In MISRA C:2012, rules have been made more precise so that the standard will not prevent reasonable uses or behaviours that have no undesirable consequences. This will be good news for developers who may have been frustrated in the past by rules that were more restrictive than was necessary to avoid dangerous or bad practices.

The new MISRA standard further defines rules as applying to a "system" or "single translation unit" analysis. And all guidelines now include detailed rationale, which should help developers understand the need for each of them, rather than lead them to try to second-guess its intent.

The updated version also tells developers if a rule is "decidable"—those against which an analysis tool can always determine compliance or non-compliance— versus undecidable, in which this is not the case (generally due to pointer or data values affecting control flow). Undecidable rules can result in false-positive or false-negative test results simply because the tool has inadequate information available to it during analysis. This improvement in rules definition can significantly help reduce manual code-review requirements, and lets developers know ahead of time if another method of testing should be used.

www.ldra.com

LDRA

LDRA UK & Worldwide
Portside, Monks Ferry,
Wirral, CH41 5LH
Tel: +44 (0)151 649 9300
e-mail: info@ldra.com

LDRA Technology Inc.
2540 King Arthur Blvd, 3rd Floor, 12th Main Lewisville Texas 75056
Tel: +1 (855) 855 5372
e-mail: info@ldra.com

LDRA Technology Pvt. Ltd
#2989/1B, 3rd Floor, 12th Main, 80 Feet Road,
HAL II Stage, Bangalore- 560008. Near BSNL Building
Tel: +91 80 4080 8707
e-mail: india@ldra.com