



**Understanding MISRA[®]-C testing
tools compliance whitepaper**

COPYRIGHT NOTICE

© Copyright 2011 Atollic AB. All rights reserved. No part of this document may be reproduced or distributed without the prior written consent of Atollic AB.

TRADEMARK

Atollic and **Atollic TrueINSPECTOR** and the Atollic logotype are trademarks or registered trademarks owned by Atollic. "MISRA C" is a registered trademark of MIRA Ltd, held on behalf of the MISRA Consortium. All other product names are trademarks or registered trademarks of their respective owners.

DISCLAIMER

The information in this document is subject to change without notice and does not represent a commitment of Atollic AB. The information contained in this document is assumed to be accurate, but Atollic assumes no responsibility for any errors or omissions. In no event shall Atollic AB, its employees, its contractors, or the authors of this document be liable for any type of damage, losses, costs, charges, claims, demands, claim for lost profits, fees, or expenses of any nature or kind.

DOCUMENT IDENTIFICATION

ASW-MTCWP July 2011

REVISION

First version

Atollic AB

Science Park
Gjuterigatan 7
SE- 553 18 Jönköping
Sweden

+46 (0) 36 19 60 50

E-mail: sales@atollic.com

Web: www.atollic.com

Atollic Inc

115 Route 46
Building F, Suite 1000
Mountain Lakes, NJ 07046-1668
USA

+1 (973) 784 0047 (Voice)

+1 (877) 218 9117 (Toll Free)

+1 (973) 794 0075 (Fax)

E-mail: sales.usa@atollic.com

Web: www.atollic.com

Contents

Abstract	2
Introduction.....	3
What is MISRA®-C?.....	3
The MISRA®-C exemplar test suite.....	4
Test results	6
Overview	6
Detailed list of detected violations	6
Detailed list of false-positives	6
Summary.....	7

Tables

No table of figures entries found.

ABSTRACT

Adhering to the MISRA®-C coding standard is a good way of improving quality of embedded systems software. Many tools exist for MISRA®-C compliance control, but they all support the MISRA®-C coding standard to different levels. This white paper outlines methods and tools for understanding the level of MISRA®-C compliance in source code analysis tools.

INTRODUCTION

Many embedded companies use static source code analysis to improve software quality. Static source code analysis often includes compliance checking versus a formal coding standard. One of the most popular coding standards within the embedded systems industry is the MISRA®-C coding standard.

Some tools for static source code analysis thus check the application source code for MISRA®-C compliance. But claiming MISRA®-C support is not binary, all MISRA®-C compliance checkers fulfill the MISRA®-C coding standard to a various level.

MISRA®-C:2004 contains 141 rules in 21 categories, out of which 121 rules are mandatory. Therefore, a tool that for example checks only 106 rules is inferior to a tool that checks 124 rules (all the 141 rules in the MISRA®-C standard cannot be checked by a software tool and so no tool checks for all 141 rules).

Some MISRA® rules can be tested on a per-file basis, while other rules require a system wide analysis. Tools that only work on a per-file basis (such as a C/C++ compiler) are thus typically unable to check the system wide rules.

Some tools only test a smaller subset of MISRA®-C rules, and it is of course a lot easier and less costly to develop a tool that only checks for a smaller part of the MISRA®-C coding standard, as opposed to a tool that also checks the difficult-to-test rules.

Before selecting a tool for MISRA®-C checking, it is of paramount importance to understand to what level the tool checks MISRA®-C compliance. Prior to selecting a tool, customers should query the supplier on the number of rules being tested. A compliance report from the MISRA®-C exemplar test suite should be provided as well.

This document outlines how the level of MISRA®-C support can be assessed in various tools, and is exemplified with the **Atollic TrueINSPECTOR®** tool.

WHAT IS MISRA®-C?

MISRA® (The Motor Industry Software Reliability Association) was established as a collaboration between various vendors in the automotive industry. The purpose is to promote best practice in developing safety-critical systems in road vehicles and other embedded systems.

MISRA®-C is a coding standard for the C programming language, developed by MISRA®. The purpose is to identify a subset of the C language that improves safety, portability and reliability.

In 1998, the first edition of the MISRA® standard (MISRA®-C:1998, titled "Guidelines for the use of the C language in vehicle based software") was released. MISRA®-C:1998 have 127 rules, of which 93 are required and 34 are advisory.

The MISRA®-C:1998 standard was quite targeted towards automotive systems, and in 2004, a second edition (MISRA®-C:2004, titled "Guidelines for the use of the C language in critical systems") was released.

MISRA®-C:2004 is more generic and better adapted for any type of embedded system, and have 141 rules of which 121 are required and 20 are advisory. The rules are divided into 21 groups:

Rule group	Description
Group 1	Environment
Group 2	Language extensions
Group 3	Documentation
Group 4	Character sets
Group 5	Identifiers
Group 6	Types
Group 7	Constants
Group 8	Declarations and definitions
Group 9	Initialization
Group 10	Arithmetic type conversions
Group 11	Pointer type conversions
Group 12	Expressions
Group 13	Control statement expressions
Group 14	Control flow
Group 15	Switch statements
Group 16	Functions
Group 17	Pointers and arrays
Group 18	Structures and unions
Group 19	Preprocessing directives
Group 20	Standard libraries
Group 21	Runtime failures

Table 1 - Rule groups

By following the MISRA®-C coding standard, you ensure that unsafe or unreliable coding constructs are not used in your software product, thus improving software quality. It is practically impossible to ensure MISRA®-C compliance without tool support.

Atollic TrueINSPECTOR® for example, performs MISRA®-C:2004 checking by automatically verifying source code compliance, and points out any code lines that breaks any of the coding standard rules.

THE MISRA®-C EXEMPLAR TEST SUITE

There exists no formal certification program for MISRA®-C testing tools. However, the MISRA® consortium has released an exemplar test suite that is the next best thing.

The MISRA[®]-C exemplar test suite is a set of source code files with a predefined set of testing results. Conformance testing tool suppliers typically test their tools towards the MISRA[®]-C exemplar test suite.

Some of the MISRA[®]-C rules are represented by several test cases in the exemplar test suite, i.e. the exemplar test suit contains more tests than there are rules. It is thus important for tools not only to test a rule, but actually pass as many as possible of its test cases for each rule too. Ideally all test cases shall pass for each rule being supported.

Furthermore, a tool shall not only find the violations, it shall also not generate false-positive warnings that confuse developers and reduce their development efficiency.

TEST RESULTS

The sections below outlines the **Atollic TrueINSPECTOR®** test results when checking the source code in the MISRA®-C:2004 exemplar test suite.

OVERVIEW

Atollic TrueINSPECTOR® is one of the most rigorous MISRA®-C:2004 checkers on the market. Using this tool on the MISRA®-C exemplar test suite gives the following test results:

- **Atollic TrueINSPECTOR®** checks 124 out of the 141 rules and 618 of the 661 test cases for violation detection. This translates into 93.5% violation-detection ratio of test cases (keep in mind that all rules cannot be tested with a software tool and hence no tool can achieve 100%).
- **Atollic TrueINSPECTOR®** produces only 0.5% false positives (1 of 185 test cases for false-positives detection).
- **Atollic TrueINSPECTOR®** performs system-wide analysis and checks global rules, not only per-file rules.

The test results outlined above is among the best on the market.

DETAILED LIST OF DETECTED VIOLATIONS

The detailed list of detected violations is removed from the public version of this document. Detailed MISRA®-C:2004 compliance reports for Atollic TrueINSPECTOR® are available upon request from your nearest Atollic representative.

DETAILED LIST OF FALSE-POSITIVES

The detailed list of false-positives is removed from the public version of this document. Detailed MISRA®-C:2004 compliance reports for Atollic TrueINSPECTOR® are available upon request from your nearest Atollic representative.

SUMMARY

Using a tool that checks for MISRA®-C compliance is a good way to improve your software quality in terms of safety, reliability and maintenance.

MISRA®-C compliance checking is not practical to perform without sufficient tool support, and different MISRA®-C compliance checking tools test the compliance on different levels. Selecting a tool with a high-level of compliance is thus paramount for development teams.

No formal certification program exist for MISRA®-C tool certification, but the MISRA® exemplar test suite is a test suite that can be used to understand the compliance level of MISRA®-C checking tools.

Atollic TrueINSPECTOR® is one of the most rigorous MISRA®-C:2004 compliance checkers on the market, detecting 93.5% of the test cases in the MISRA®-C exemplar test suite, while at the same time only generating 0.5% false-positive warnings in the test suite. Worth noting here is that all rules cannot be tested by a software tool.

Atollic provides a family of well integrated tools for professional embedded systems development and debugging, static source code analysis, test automation and test quality measurement.

More information about Atollic, **Atollic TrueSTUDIO®**, **Atollic TrueINSPECTOR®**, **Atollic TrueANALYZER®** and **Atollic TrueVERIFIER™** products is available here:

www.atollic.com

www.atollic.com/truestudio

www.atollic.com/trueinspector

www.atollic.com/trueanalyzer

www.atollic.com/trueverifier