MISRA C:2023 Addendum 3

Coverage of MISRA C:2023 against CERT C 2016 Edition

January 2025

This document published January 2025 by The MISRA Consortium Limited
1 St James Court
Whitefriars
Norwich
Norfolk
NR3 1RU
UK

www.misra.org.uk

ISBN 978-1-911700-15-9 PDF

British Library Cataloguing in Publication Data
A catalogue record for this book is available from the British Library.

MISRA C:2023 Addendum 3

Coverage of MISRA C:2023 against CERT C 2016 Edition

January 2025

MISRA Mission Statement

MISRA provides world-leading best practice guidelines for the safe and secure application of both embedded control systems and standalone software.

MISRA is a collaboration between manufacturers, component suppliers, engineering consultancies and academics which seeks to research and promote best practice in developing safety- and security-related electronic systems and other software-intensive applications.

To this end, MISRA conducts research projects and publishes documents that provide accessible information for engineers and management.

MISRA also facilitates the dissemination and exchange of information between practitioners through supporting and holding technical events.

Foreword

The vision of MISRA C is set out in the opening paragraph of the Guidelines:

> "The MISRA C Guidelines define a subset of the C language in which the opportunity to make mistakes is either removed or reduced".

Many standards for the development of safety-related software require, or recommend, the use of a language subset, and this can also be used to develop any application with high integrity or high reliability requirements.

Unfortunately, many people focus on the *safety-related* software reference, and a perception exists that MISRA C is only *safety-related* and not *security-related*.

In 2008, the Software Engineering Institute at Carnegie Mellon University published CERT C, as a "secure coding standard". A second edition was published in 2014, with a further update released in 2016 (PDF only).

This third Addendum to MISRA C:2023 sets out the coverage by MISRA C:2023 of the 2nd Edition of CERT C and justifies the viewpoint that MISRA C is equally as applicable in a *security-related* environment as it is in a *safety-related* one — particularly relating to the development of *freestanding* applications. Ongoing developments of MISRA C will further address issues in the *hosted* domain.

Andrew Banks FBCS CITP
Chairman, MISRA C Working Group

Acknowledgements

The MISRA C Working Group

The MISRA Consortium Limited would like to thank the following members of the MISRA C Working Group for their significant contribution to the writing of this document:

Andrew Banks	LDRA Ltd (also Intuitive Consulting)
Roberto Bagnara	BUGSENG and The University of Parma
Jill Britton	Perforce
Daniel Kästner	AbsInt Angewandte Informatik GmbH

The MISRA Consortium Limited also wishes to acknowledge contributions from the following members of the MISRA C Working Group during the development and review process:

Dave Banham	Blackberry Ltd.
Tibor Milić	Rimac Technology
Chris Miller	GE Aviation Ltd
Hamzath Pitchai Mohammed	Robert Bosch GmbH
Chris Tapp	Keylevel Consultants Ltd

The MISRA Consortium Limited also wishes to acknowledge contributions from the following individuals during the development and review process:

David Ward	HORIBA MIRA Limited

Other acknowledgements

DokuWiki was used extensively during the drafting of this document. Our thanks go to all those involved in its development.

This document was typeset using fonts licensed under the SIL Open Font License, Version 1.1:

- Open Sans — Copyright © 2020, The Open Sans Project Authors.

Contents

1 Introduction

1.1 Background

Throughout the development of MISRA C, the main focus has been to address vulnerabilities in the C language, particularly for use in embedded systems, and primarily targeted at safety-related applications. MISRA C particularly applies to freestanding applications, which use a sub-set of the C Standard Library.

One of the great successes of MISRA C has been its adoption across many industries, and in environments where safety-criticality is less of a concern, but where security is more of an issue.

There have been discussions as to the applicability of MISRA C for secure applications. The MISRA C Working Group have listened to those concerns, and have compiled this Addendum to document the coverage of MISRA C against CERT C.

1.2 Applicability

This document provides a mapping of the guidance provided by the SEI CERT C Coding Standard [2] against MISRA C.

This document should be read in conjunction with MISRA C:2023 *Guidelines for the use of the C language in critical systems* [1].

2 Coverage

2.1 Coverage classification

The coverage of each CERT C guideline against MISRA C is classified as follows:

Status	Interpretation
Explicit	The CERT C guideline is EXPLICITLY covered by one or more MISRA C Guidelines, which directly addresses the undesired behaviour.
Implicit	The CERT C guideline is IMPLICITLY covered by one or more MISRA C Guidelines, although the behaviour is not explicitly referenced.
Restrictive	The CERT C guideline is covered by one or more MISRA C Guidelines that prohibit a language feature in a RESTRICTIVE manner.
Partial	Some aspects of the CERT C guideline are covered by one or more MISRA C Guidelines. However, some aspects of the CERT C guideline are not covered by any MISRA C Guideline.
None	The CERT C guideline is not covered by any MISRA C Guideline.

2.2 Coverage strength

The strength of the coverage of each CERT C guideline against MISRA C is classified as follows:

Status	Interpretation
Strong	The CERT C guideline is covered by one or more targeted MISRA C Rules (excluding Rule 1.3 on its own).
Weak	The CERT C guideline is only covered by one or more MISRA C Directives, or by Rule 1.3.
None	The CERT C guideline is not covered by any MISRA C Guidelines.

Note: For language vulnerabilities with Partial coverage, a combination of Strength coverages is shown.

3 CERT C cross reference

3.1 Guideline by Guideline

CERT C Rule	MISRA C:2023 Guidelines			Comments
	Guidelines	Coverage		
PRE30-C	Rule 1.3	Implicit	Weak	
PRE31-C	Rule 13.2	Explicit	Strong	
PRE32-C	Rule 1.3, 20.6	Explicit	Strong	
DCL30-C	Rule 1.3, 18.6	Explicit	Strong	
DCL31-C	Rule 8.1, 17.3	Explicit	Strong	
DCL36-C	Rule 8.2, 8.4, 8.8, 17.3	Explicit	Strong	
DCL37-C	Rule 1.3, 21.1, 21.2	Explicit	Strong	
DCL38-C	Rule 1.1, 1.3, 21.3	Restrictive	Strong	Dynamic memory allocation is not permitted by MISRA C
DCL39-C		None	None	
DCL40-C	Rule 1.3, 5.1, 5.2, 8.3, 8.4, 8.5	Explicit	Strong	
DCL41-C	Rule 16.1	Implicit	Strong	
EXP30-C	Rule 1.3, 13.2	Explicit	Strong	
EXP32-C	Rule 1.3, 11.8	Explicit	Strong	
EXP33-C	Dir 4.1 Rule 1.3, 9.1, 21.3	Explicit	Strong	
EXP34-C	Dir 4.1, 4.14 Rule 1.3	Implicit	Weak	
EXP35-C	Rule 18.9	Explicit	Strong	
EXP36-C	Rule 1.3, 11.1, 11.2, 11.3, 11.4, 11.5, 11.6	Explicit	Strong	
EXP37-C	Rule 8.2, 17.3	Explicit	Strong	
EXP39-C	Rule 1.3, 11.1, 11.2, 11.3, 11.7	Explicit	Strong	
EXP40-C	Rule 1.3, 7.4, 11.8	Implicit	Strong	
EXP42-C	Rule 21.16	Explicit	Strong	
EXP43-C	Rule 1.3, 8.14	Restrictive	Strong	
EXP44-C	Rule 13.6, 18.10, 23.2, 23.7	Explicit	Strong	
EXP45-C	Rule 13.4	Explicit	Strong	
EXP46-C	Rule 10.1	Explicit	Strong	
INT30-C	Rule 12.4	Partial	Strong	MISRA C only addresses wrap-around of constant expressions.
INT31-C	Rule 10.1,10.3, 10.4, 10.5, 10.6, 10.7, 10.8 21.6, 21.13, 21.18	Explicit	Strong	
INT32-C	Dir 4.1 Rule 1.3	Implicit	Weak	
INT33-C	Dir 4.1 Rule 1.3	Implicit	Weak	
INT34-C	Rule 10.1, 12.2	Explicit	Strong	
INT35-C	Dir 4.1 Rule 1.3	Implicit	Weak	
INT36-C	Dir 1.1 Rule 11.1, 11.2, 11.4, 11.6, 11.7	Explicit	Strong	
FLP30-C	Rule 14.1	Explicit	Strong	
FLP32-C	Dir 4.11	Explicit	Weak	

CERT C Rule	MISRA C:2023 Guidelines			Comments
	Guidelines	Coverage		
FLP34-C	Rule 10.3, 10.4, 10.5, 10.8	Explicit	Strong	
FLP36-C	Dir 1.1 Rule 1.3, 10.3, 10.4, 10.5, 10.8	Explicit	Strong	
FLP37-C	Rule 21.16	Explicit	Strong	
ARR30-C	Rule 1.3, 18.1, 21.17, 21.18	Implicit	Strong	
ARR32-C	Rule 18.8	Restrictive	Strong	
ARR36-C	Rule 18.2, 18.3	Explicit	Strong	
ARR37-C	Rule 18.1, 18.4	Explicit	Strong	
ARR38-C	Rule 1.3, 21.6, 21.17, 21.18	Restrictive	Strong	
ARR39-C	Rule 1.3, 18.4	Explicit	Strong	
STR30-C	Rule 7.4	Explicit	Strong	
STR31-C	Dir 4.1 Rule 1.3, 18.1, 21.6, 21.17, 21.18	Implicit	Strong	
STR32-C	Rule 21.16	Explicit	Strong	
STR34-C	Rule 10.1, 10.3, 10.4	Explicit	Strong	
STR37-C	Rule 21.13	Explicit	Strong	
STR38-C	Rule 1.3, 10.3	Explicit	Strong	
MEM30-C	Dir 4.12 Rule 1.3, 21.3, 22.2	Explicit	Strong	
MEM31-C	Rule 22.1	Explicit	Strong	
MEM33-C	Rule 18.7	Restrictive	Strong	
MEM34-C	Rule 22.2	Explicit	Strong	
MEM35-C	Dir 4.1, 4.12 Rule 1.3, 21.3	Restrictive	Strong	
MEM36-C	Rule 21.3	Restrictive	Strong	
FIO30-C	Dir 4.14	Implicit	Weak	
FIO32-C	Rule 21.6	Restrictive	Strong	Rule 21.6 restricts use of all I/O functions in `<stdio.h>`
FIO34-C	Rule 22.7	Explicit	Strong	
FIO37-C	Rule 21.6	Restrictive	Strong	Rule 21.6 restricts use of all I/O functions in `<stdio.h>`
FIO38-C	Rule 22.5	Implicit	Strong	
FIO39-C	Dir 4.13 Rule 21.6	Restrictive	Strong	Rule 21.6 restricts use of all I/O functions in `<stdio.h>`
FIO40-C	Rule 21.6	Restrictive	Strong	Rule 21.6 restricts use of all I/O functions in `<stdio.h>`
FIO41-C	Rule 21.6	Restrictive	Strong	Rule 21.6 restricts use of all I/O functions in `<stdio.h>`
FIO42-C	Rule 22.1	Explicit	Strong	
FIO44-C	Rule 21.6	Restrictive	Strong	Rule 21.6 restricts use of all I/O functions in `<stdio.h>`
FIO45-C	Dir 5.1	Implicit	Weak	
FIO46-C	Rule 22.6	Explicit	Strong	
FIO47-C	Rule 21.6	Restrictive	Strong	Rule 21.6 restricts use of all I/O functions in `<stdio.h>`
ENV30-C	Rule 21.10, 21.19	Explicit	Strong	
ENV31-C	Rule 1.3	Implicit	Weak	
ENV32-C	Rule 21.4, 21.8	Restrictive	Strong	
ENV33-C	Rule 21.21	Restrictive	Strong	
ENV34-C	Rule 21.20	Explicit	Strong	

CERT C Rule	MISRA C:2023 Guidelines			Comments
	Guidelines	Coverage		
SIG30-C	Rule 21.5	Restrictive	Strong	Rule 21.5 restricts use of all functions in `<signal.h>`
SIG31-C	Rule 21.5	Restrictive	Strong	Rule 21.5 restricts use of all functions in `<signal.h>`
SIG34-C	Rule 21.5	Restrictive	Strong	Rule 21.5 restricts use of all functions in `<signal.h>`
SIG35-C	Rule 21.5	Restrictive	Strong	Rule 21.5 restricts use of all functions in `<signal.h>`
ERR30-C	Rule 22.8, 22.9, 22.10	Explicit	Strong	
ERR32-C	Rule 21.5	Explicit	Strong	Rule 21.5 restricts use of all functions in `<signal.h>`
ERR33-C	Dir 4.7	Explicit	Weak	
CON30-C	Dir 4.12 Rule 22.1, 22.13	Explicit	Strong	
CON31-C	Rule 22.15, 22.16	Explicit	Strong	
CON32-C	Dir 5.1	Implicit	Weak	
CON33-C	Dir 5.1 Rule 9.7, 21.8, 21.19, 21.24	Explicit	Strong	
CON34-C	Dir 4.12, 5.3 Rule 18.6, 18.9, 22.13, 22.15	Explicit	Strong	
CON35-C	Dir 5.2	Explicit	Weak	
CON36-C	Dir 4.13, 5.1	Implicit	Weak	
CON37-C	Rule 21.5	Restrictive	Strong	Rule 21.5 restricts use of all functions in `<signal.h>`
CON38-C		None	None	
CON39-C	Rule 22.11	Explicit	Strong	
CON40-C	Rule 13.2	Explicit	Strong	
CON41-C		None	None	
MSC30-C	Rule 21.24	Explicit	Strong	
MSC32-C	Rule 21.24	Explicit	Strong	
MSC33-C	Rule 21.10	Restrictive	Strong	
MSC37-C	Rule 17.4	Explicit	Strong	
MSC38-C	Rule 1.1, 1.3	Implicit	Weak	
MSC39-C	Rule 17.1	Restrictive	Strong	
MSC40-C	Rule 1.1	Restrictive	Strong	

3.2 Excluded CERT C Guidelines

The following CERT C guidelines are not included in the above assessment — these have either been removed from CERT C, or are additions to the website edition but have not been included in a published edition.

CERT C Rule	MISRA C:2023 Guidelines			Comments
	Guidelines	Coverage		
FIO31-C	Rule 22.3	Explicit	Weak	Removed from CERT C prior to 2016 edition
EXP47-C		None	None	Added subsequent to publication of 2016 edition
ERR34-C	Dir 4.7	Explicit	Weak	
CON42-C		None	None	CERT C Rule still under construction
CON43-C	Dir 5.1	Explicit	Weak	
MSC41-C		None	None	

3.3 Coverage summary

In summary, the coverage of MISRA C:2023 against CERT C is as follows:

Classification	Strength	Number
Explicit	Strong	52
	Weak	3
Implicit	Strong	5
	Weak	11
Restrictive	Strong	24
	Weak	0
Partial	Strong	1
None	None	3
Total		99 (of 99)

4 References

The following documents are referenced from within this amendment:

4.1 MISRA C

[1] MISRA C:2023 *Guidelines for the use of the C language in critical systems*
ISBN 978-1-911700-08-1 (paperback), ISBN 978-1-911700-09-8 (PDF),
The MISRA Consortium Limited, Norwich, April 2023

4.2 Other documents

[2] SEI CERT C Coding Standard
Rules for Developing Safe, Reliable, and Secure Systems 2016 Edition

5 Change log

Date	ISBN	Revisions
January 2018	978-1-906400-19-4 PDF	Original release, for MISRA C:2012
July 2024	978-1-911700-15-9 PDF	Revised for MISRA C:2023
		Incorporate AMD3, AMD4
		Revised other assessments