

MISRA C2 Update

3/5/2003





Introduction

- Gavin McCall C.Eng., M.I.E.E.
- Technical Fellow – Systems Safety
- Visteon Representative to MISRA Steering Team
- Visteon Representative and Leader of MISRA C2 working group
- MISRA C2 is the working name





Background

- Guidelines For The Use Of The C Language in Vehicle Based Systems
- Known as MISRA C
- Published April 1998
- Translated into Japanese
- Extensive Use Beyond Automotive Industry
- Need exists to review and update document



Process

- UK Team are producing a version 2 draft
- Target End March 2003
- Consultation sessions to be held
 - UK
 - USA – Detroit in consultation with SAE J2632
 - Japan – to be established
- Based on consultation MISRA C2 will be published



UK Team

- Automotive OEM (Land Rover)
- Automotive Tier 1 (Tarragon, Visteon)
- Automotive Research (MIRA)
- Tool Vendor (Hitex, LDRA, Programming Research)
- UK Defence (QinetiQ)
- Academic (Univ. Kent at Canterbury)
- Independent Software Consultants
- Plus others
- Beyond automotive





Status

- 112 Rules and normative texts are ready
- 13 Rules remain for further review
- 3 Rules are deprecated
- Some Rules are split, leading to 146 Rules
- 56 Rule texts are unchanged
- Rule numbering to be defined



Principle

- Language used is consistent with Standard language
- Generalised rules for Undefined Behaviour replaced with specific rule targeted at Undefined Behaviour Only
- Complex rules split into atomic rules - compliance
- Examples added and improved
- Tool-less use removed
- Avoid new material



Example – Rule1

- Required: All code shall conform to ISO 9899 standard C, with no extensions permitted
- Required: All code shall conform to ISO 9899:1990 C programming language
- Accurate reference to specific C version
- MISRA C 2 will not address ISO 9899:1999 -> MISRA C 3



Example – Rule4

- Advisory: Provision should be made for appropriate run-time checking.
- Required: Minimisation of run-time failures must be ensured by the use of at least one of (a) static analysis tools/techniques; (b) dynamic analysis tools/techniques; (c) explicit coding of checks to handle run-time faults.
- Specific direction to use a defined technique



Example – Rule5

- Required: Only those characters and escape sequences which are defined in the ISO C standard shall be used
- Required: Only those escape sequences which are defined in the ISO C standard shall be used.
- Undefined behaviour is only related to escape sequences



Example – Rule48 tbe

- Advisory: Mixed precision arithmetic should use explicit casting to generate the desired result.
- Required: The value of an expression shall not be assigned to an object whose type differs from the underlying type of the expression.

```
uint8_t a, b, c;
```

```
a = b + c;
```

- Casting not required



Example – Rule48 tbe

```
uint8_t a, b, c;
```

```
a = (uint8_t) ((signed int) b + (signed int) c);
```

- explicit casting equivalent to “as if” rule for promotion
- Note: fails Rule13?

```
a = (uint8_t) ((sint16_t) b + (sint16_t) c);
```

```
/* 16 bit integer */
```

```
a = (uint8_t) ((sint32_t) b + (sint32_t) c);
```

```
/* 32 bit integer */
```





Example – Rule43 tbe

- Required: Implicit conversions which may result in a loss of information shall not be used.
- Required: No implicit balancing conversions shall be permitted in the evaluation of expressions.
- Required: Casts shall only be of a permitted, narrowing type unless the operand is a literal constant or an lvalue.
- Casts should not be applied to expressions



Example – Rule43 tbe

```
uint16_t a, b, c;  
float32_t f, g, h;  
f = a / b; /* Fail - inconsistent type */  
f = (float32_t) (a / b); /* widening */  
f = (float32_t) a / b; /* implicit balance */  
f = (float32_t) a / (float32_t) b; /* ok */  
c = a / b; /* ok */  
f = c; /* cast not required */  
c = (uint16_t) f; /* ok - overflow? */
```





Publication

- Traditional printed document
- PDF
- PDF is available for company intranet of current and future versions



Contacts

- gmccall@visteon.com
- david.ward@mira.co.uk
- PDF is available for company intranet
- <http://www.misra.org.uk/>
- mailing list available at above site
send body “subscribe misra-c” to robot@misra.org.uk
- consultation will be announced via mailing list
and SAE J2632

