



Update on MISRA activities

Dr David Ward
MISRA Project Manager
General Manager, Functional Safety / HORIBA MIRA

October 2015



Agenda



- Overview of MISRA
- MISRA C activities
- MISRA C++ activities
- Other activities

The MISRA project



- Started in 1990
- Mission: We provide world-leading best practice guidelines for the safer and more secure application of both embedded control systems and standalone software
- The original project was part of the UK Government's "SafeIT" programme
- Now self-supported
- HORIBA MIRA provides the project management support

MISRA's interests

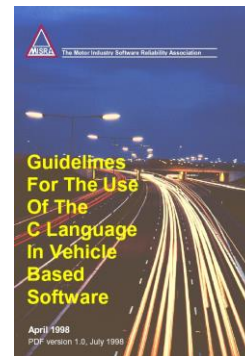


- MISRA aims to
 - ✓ Promote best practice in safety-related systems engineering
 - ✓ Develop guidance in specific technical areas e.g.
 - C language
 - Software readiness for production
 - Safety analysis
 - Safety cases
- MISRA does not
 - ✗ Run certification schemes
 - ✗ Promote or endorse specific products

Original MISRA publications



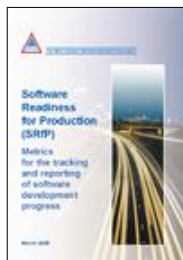
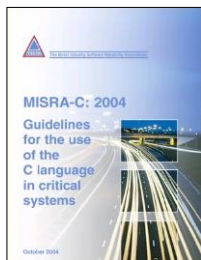
- November 1994: *Development guidelines for vehicle based software* (The MISRA Guidelines)
 - The first automotive publication concerning functional safety, more than 10 years before work started on ISO 26262 ...
- April 1998: *Guidelines for the use of the C language in vehicle based software* (MISRA C)
 - Addressing a specific requirement for a language subset in the MISRA Guidelines



Further MISRA publications



- October 2004: *MISRA-C:2004 – Guidelines for the use of the C language in critical systems* (MISRA C2)
- March 2006: *Software Readiness for Production* (SRfP)
- November 2007: *Guidelines for safety analysis of vehicle based programmable systems* (MISRA SA)
- November 2007: MISRA Autocode TL and AGC
- June 2008: *Guidelines for the use of the C++ language in critical systems* (MISRA C++)
- June 2009: MISRA Autocode GMG and SLSF
- March 2013: *MISRA C:2012 – Guidelines for the use of the C language in critical systems* (MISRA C3)



Ongoing MISRA activities



- MISRA C and MISRA C++ to be discussed separately...
- MISRA Autocode
 - Updates of MISRA AC GMG and MISRA AC SLSF in preparation
 - MISRA AC TL will no longer be supported by MISRA
 - MISRA AC AGC is now part of MISRA C:2012
- MISRA Safety Cases
 - Guidance on structuring and providing evidence for an ISO 26262 safety case
 - Draft for comment expected Q1/2016
 - For a current summary see www-users.cs.york.ac.uk/~ihabli/Papers/2013Habli_Safecomp.pdf