N2035

MISRA C – WG14 Liaison Report
WG14 Meeting, London
11th-14th April 2016

Andrew Banks
BSc IEng MIET FBCS CITP
Frazer-Nash Research Limited, and
Chairman, MISRA C Working Group
1. MISRA Project Management

2. Where are we now?
   a. MISRA Compliance
   b. Amendment 1 for C-Secure
   c. Technical Corrigendum 1
   d. Next Steps

3. The Standard Library
   a. Freestanding v Hosted
   b. Annex K
The minutes of the Kona meeting [N1978] report, at 2.6:

- “The company that supports MISRA has been taken over by a for-profit organisation. Situation not clear.”

For reassurance, and for the avoidance of doubt:

- The MISRA Consortium
  o MISRA is coordinated by a Steering Committee of the member companies.
  o This is unchanged.
- Project Management
  o The project management of MISRA has been provided by MIRA Limited, from the initial establishment of the Consortium.
  o MIRA Limited was a for-profit organisation...
  o The transfer of MIRA Limited into HORIBA-MIRA Limited has no effect on the ongoing operation of MISRA.
MISRA C
Where are we now?
MISRA C SitRep (1)

MISRA Compliance

- Provides enhanced guidance on the *process* of complying with the MISRA language guidelines, especially in the documentation of *deviations*.
- To be issued as a standalone PDF
- Issue date: end of April 2016
C Secure

- MISRA C:2012 v ISO/IEC 17691 Matrix
  - Ready to be issued (imminently) as a standalone PDF report
  - MISRA will share with WG14
  - Feedback and comments welcome

- MISRA C:2012 Amendment 1
  - Adds a small number of new Rules to cover gaps in coverage... mostly these are in areas of the *hosted* Standard Library that MISRA C has traditionally not considered.
  - To be issued as a standalone PDF
  - Issue date: end of April 2016
MISRA C SitRep (3)

- Bulletin Board Questions (and other feedback)
  - MISRA C:2012 Technical Corrigendum 1
    - Work In Progress
    - To be issued as a standalone PDF, Q2/Q3 2016
MISRA C – Next Steps

- MISRA C:2012 is published
- Technical Corrigendum 1
  - To incorporate into the Core Document
- Amendment 1 (Security)
  - To incorporate into the Core Document
  - Some consequential amendments (eg to scope of Rule 21.8)
- MISRA Compliance
  - Core Document to be revised to reference, and remove duplication
- **Proposal: To publish consolidated Core Document as MISRA C:201x**
MISRA C – What Next?

- CERT C Coverage
  - Compiling coverage matrix
  - No plans to directly address CERT C rules

- Review of C99
  - Review of the C99 rules, in particular where a more targeted approach is possible, and appropriate.

- C11 new features
  - Review of new features for undesirable behaviours
    - Undefined
    - Unspecified
    - Implementation Defined
    - etc
The Standard Library
Freestanding v Hosted
Conformance: Freestanding v Hosted

Chapter 4 of the ISO Standard defines the following:

- A conforming freestanding implementation shall accept any strictly conforming program in which the use of the features specified in the library clause is confined to the contents of the standard headers:
  
  - `<float.h>`
  - `<iso646.h>`
  - `<limits.h>`
  - `<stdarg.h>`
  - `<stdbool.h>`
  - `<stddef.h>`
  - `<stdint.h>`

MISRA C:2012 has no explicit library-specific restrictions on these headers.
Conformance: Freestanding v Hosted

- MISRA C:2012 places major restrictions (including out-right prohibition) on many of the remaining standard headers:

  - `<assert.h>`  Implicit restriction
  - `<complex.h>`  Implicit restriction
  - `<ctype.h>`
  - `<errno.h>`
  - `<fenv.h>`  Major restrictions
  - `<inttypes.h>`
  - `<locale.h>`  Major restrictions
  - `<math.h>`
  - `<setjmp.h>`  Shall not be used
  - `<signal.h>`  Shall not be used
  - `<stdio.h>`  Shall not be used
  - `<stdlib.h>`  Major restrictions
  - `<string.h>`
  - `<tgmath.h>`  Shall not be used
  - `<time.h>`  Shall not be used
  - `<wchar.h>`  Shall not be used
  - `<wctype.h>`

- The restricts are due to the extent of the undefined, unspecified and/or implementation defined behaviour, and the functionality is mostly associated with accessing the external environment.
Review of Exclusions

- Review the blanket bans of standard library functionality that is essential to the operation of Hosted code
  - eg use of getenv(), signal()
- Consider relaxing the restrictions on use of Dynamic Memory Allocation
  - eg to permit dynamic memory use during initialisation phase

Freestanding v Hosted

- Where necessary, maintain separate Rules pertaining to Standard Library header files permitted in Freestanding applications from those pertaining to header files only used in Hosted applications (none yet?).
Annex K

- MISRA C notes:
  - the proposal to deprecate Annex K (introduced in C99)
  - the rationale, and the limited take-up of Annex K implementations
  - the “don’t break existing code” mantra of WG14

- MISRA C had proposed (in early C11 work drafts) to encourage adoption of Annex K functions and deprecate the unbounded functions

- MISRA C is of the view that:
  - bounds checking is a necessary facility in safety and security related code
  - it would have been desirable for EXISTING functions to have been modified with optional additional parameter(s), rather than a new _s set added

- MISRA C would like to support (and take part in) future discussions in this area