"The MISRA-C open conformance suite: work in progress"

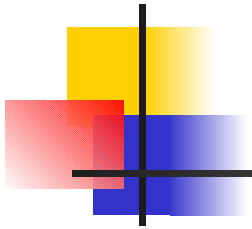
by

Les Hatton

Professor of Forensic Software Engineering,
CIS, University of Kingston, UK
L.Hatton@kingston.ac.uk, lesh@oakcomp.co.uk

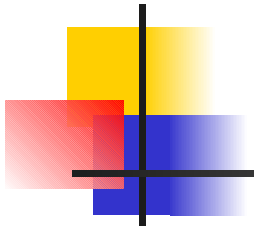
Version 1.3: 15/Oct/2004

Overview



Principles
Technical input
Implementation policy
Architecture
Status
Future direction

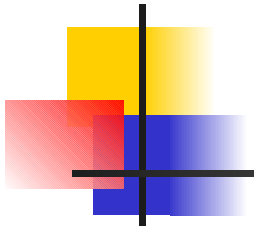
Open policy



Note the following:-

- The suite will be operated under the auspices of the Forensic Software Engineering Institute, University of Kingston, UK
- The suite will be distributed under the GPL, (GNU public licence), giving
  - Legal amnesty for contributors
  - Successful model for cooperative development
  - Positive encouragement for useful feedback from anyone.

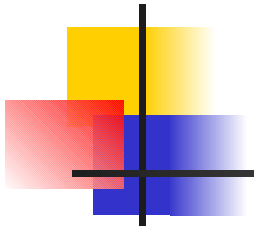
Principles



The following guiding principles are being used:-

- The infrastructure is open as is the suite itself
- The suite is evolutionary and is intended to match the official wording at any one time as well as possible
- It is intended to:-
  - educate users with code examples, (there are many non-English speaking MISRA-C users)
  - provide a basis for conformance as wording improves
- To be *independent* of tool implementation issues, (for example warning format / positions)

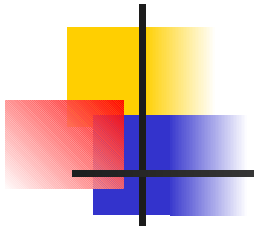
Technical input



The following sources are being used for version 2.1:-

- Version 1.3 of the original exemplary test suite
- The October 2004 MISRA version 2 document
- The original conformance suites provided by Andrew Burnard, Derek Jones and Les Hatton
- Ongoing input from the steering committee and outside commentators, (of which there have been several).

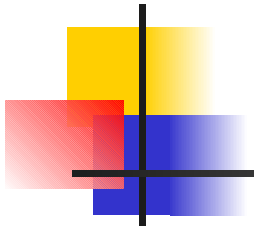
Implementation policy



The following simple policy was used:-

- Hierarchy of wording
  - Bold face part of rule assumed normative overriding any commentary
  - Commentary used if bold face ambiguous
  - False positives favoured if commentary ambiguous; query files produced; rationale modified.
- No dependence on file inclusion
- Required rules done first

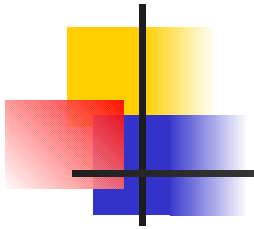
Architecture: Goals



Goals:-

- Orthogonality, (no crosstalk but *not* 1 item 1 file). This is unlikely to be satisfied just as it was a problem in v1.3.
- Portability. (The architecture should run on any platform)
- Verifiability. There must be a way of detecting whether the source of a rule was altered. There must also be no dependence on inclusion, so parts of the C standard headers had to be constructed.

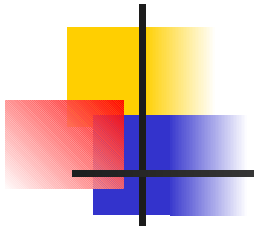
Architecture: Construction



Construction:-

- Perl was used for the engine. This should run without change on Windows, Linux, Unix and so on although there are still two shell scripts in v1.3. These will be converted to Perl in v2.1
- An automatic checksum is inserted into the conformance suite on a file by file basis so that external source change can be detected. The suite is therefore self-verifying.

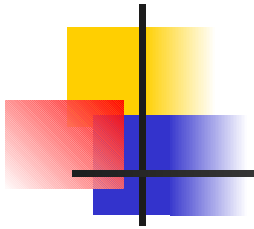
Architecture: Deliverables



All deliverables are open source, released under the GPL:-

- Readme + Rationale (html) + GPL licence
- MISRA-C conformance suite, (completely self-contained)
  - Every rule has a positive file (must detect) and a negative file (must not detect)
  - Some rules have query files (e.g. not part of conformance but may be in future or interpretation issues)
- Conformance suite architecture

Status



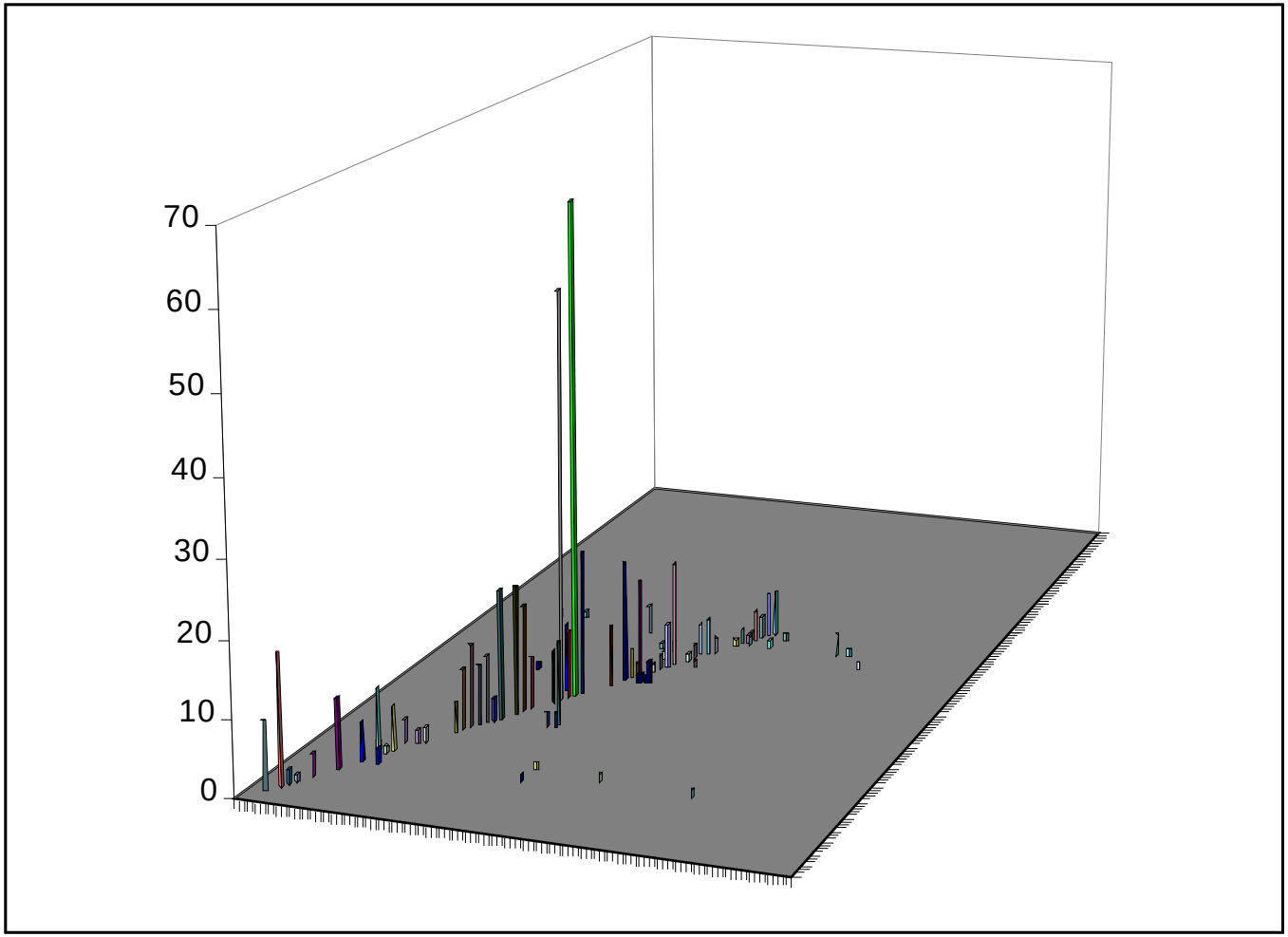
Version 1.1c available now:-

- 497 test cases for 45 rules in 90 files. (40 days work so far in 46 CRs). (Milestone 15-10-2001, 23:59:00)

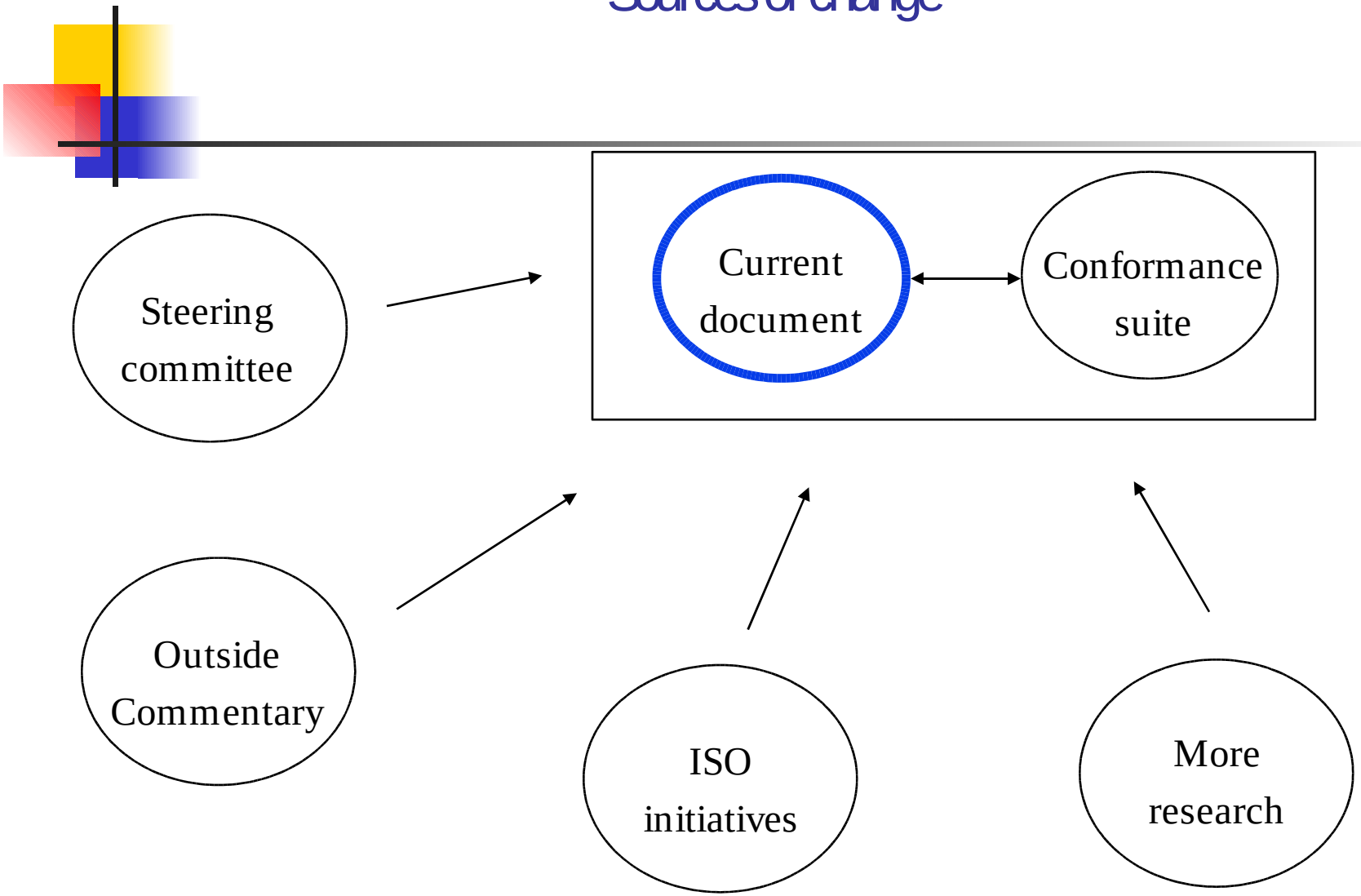
Version 2.1

- Work in progress. All rules common to both versions of the conformance suite now converted.

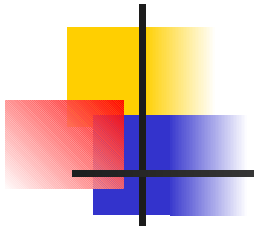
Rule crosstalk in version 1



Future direction: Sources of change



Associated research projects



Signal to noise ratio of safer subsets

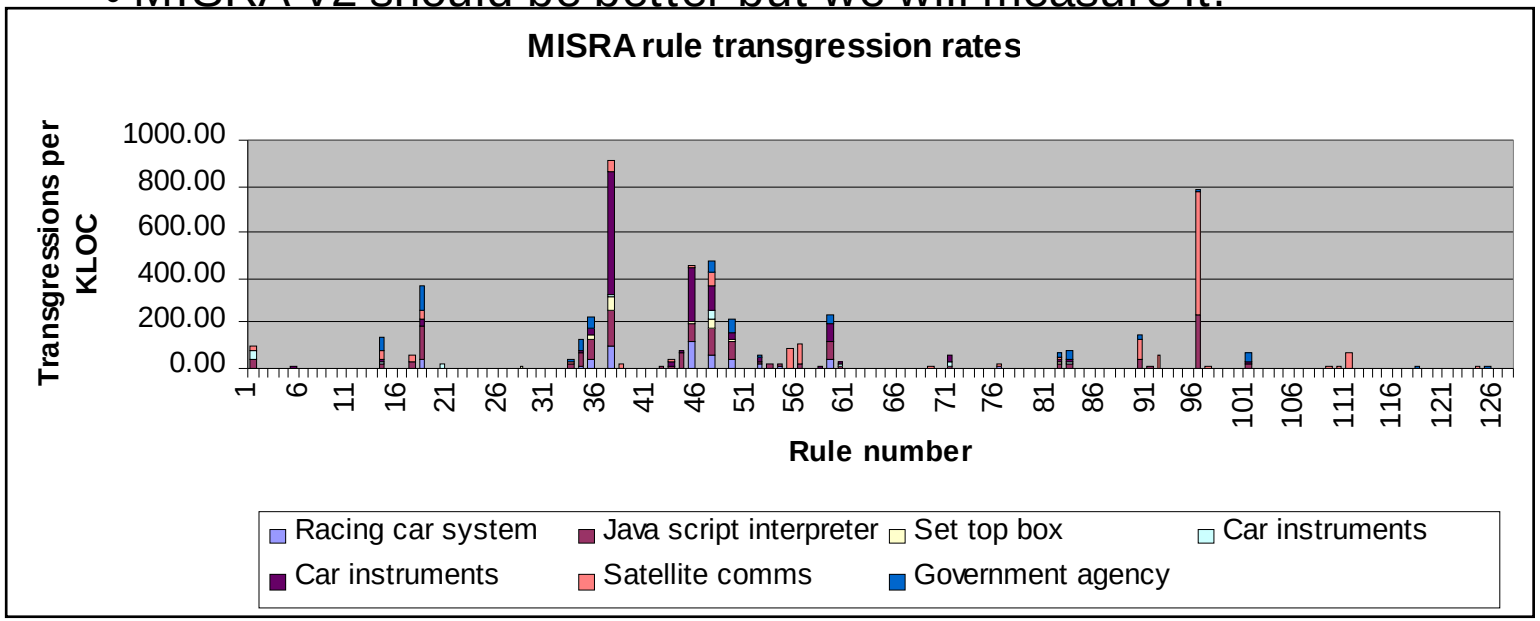
An attempt to quantify the real rate at which safer subset warnings of various kinds produce system failures

- We know from previous experiments that the underlying rate at which statically detectable faults fail is around 3 per 1000 lines of source code randomly occurring from a C population of around 8 per 1000 lines of source code, (references later).

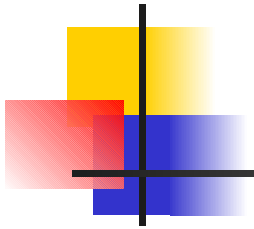
Associated research projects

Signal to noise ratio of safer subsets

- MISRA v1 has an underlying hit rate of around 600 per 1000 lines of source code so the detection rate is around 75 times too high.
- MISRA v2 should be better but we will measure it.



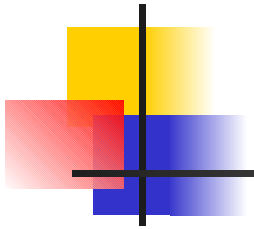
Associated research projects



The dangers of low signal to noise safer subsets

- We know (Adams(1984) and other sources) that changes to software re-inject defects with ratios between about 1/50 and 1/7.
- If a subset forces us to make say 100 changes per 1000 lines of code to comply, the chances of injecting at least 1 defect is very high. To be effective, the subset must remove more than it causes.

Remaining problems



ISO C conformance

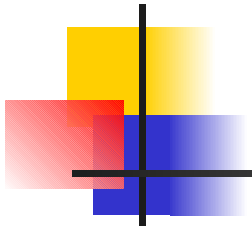
- What to do about C99 -> ?
- ISO conformance testing has effectively ceased so the most fundamental rule of all is difficult to enforce.
- The growing gap between embedded systems compiler implementations and the work of the ISO committee.

Interpretation problems

- Rule 3.2 (req) All implementation defined behaviour shall be documented

  What does this mean ? Documented where ? From a compliance point of view, what message would a tool give ? This will require close collaboration between all interested

Availability



Download sites:-

- Principle site:-

  University of Kingston, (site TBA)

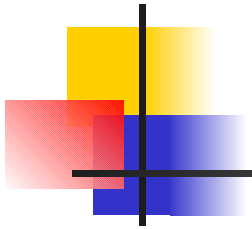
- Secondary sites

  http://www.misra.org.uk/

  http://www.leshatton.org/

  (anybody who wants to mirror it.)

References



This presentation freely available from:-

http://www.leshatton.org/

(Follow links to Presentations)

References to be found under:-

http://www.leshatton.org/

(Follow links to Safer Subsets, Computing and Software.)