C Safety / Security Study Group
Inaugural Meeting - Agenda

Date: Wednesday 08 February 2017
Time: 17:00 GMT, 12:00 EST, 09:00 PST
Conference Line: WebEx - link here

Invitees

Robert Seacord	~~Kayvan Memarian~~	~~David Keaton~~
Laurence Urhegyi	Roberto Bagnara	~~Elisa Heymann~~
~~Andrew Banks~~	~~Barnaby Stewart~~	~~Gerard Holzmann~~
~~Paul Sherwood~~	~~Jim MacArthur~~	~~Joe Jarzombek~~
~~David Wheeler~~	~~Murali Somanchy~~	Konstantin Serebryany
~~Aaron Ballman~~	~~Daniel Godas-Lopez~~	~~Gavin McCall~~
Clive Pygott	~~Barton Miller~~	~~Steve Christie~~
~~Peter Sewell~~	~~Chris Polin~~	~~Bob Martin~~
~~Yozo Toda~~	~~Masaki Kubo~~	**Adele Carter**
~~Robin Randhawa~~	~~Ian Hawkes~~	~~William Forbes~~
~~Michael Feiri~~	Martin Sebor	Jill Britton
~~Ralf Huuck~~	David Tarditi	

Note: names that are struck through indicates absence from the meeting.

Agenda

Time	Topic and Key Points Discussed	Owner
10 mins	Topic ● Review of actions from previous meeting. Key Points ● More analyser vendors still need to be contacted, action is ongoing: if anyone knows of any then please invite them to join. ● Venn diagram on TS document and MISRA / CERT not yet started.	Laurence Urhegyi

	● Other actions to be carried forward.	
10 mins	Topic ● Update on the recent MIRA meeting. Key Points ● Andrew Banks not present today: Laurence to email the list and see if Andrew could update the group there.	Andrew Banks
10 mins	Topic ● Annotations Key Points ● Gavin could not attend today's meeting, but has informed the mailing list that we should re-visit this subject after the meeting in Markham takes place, as a proposal is planned to be discussed there.	Gavin McCall
10 mins	Topic ● Terminology - Security Flaw / Weakness / Vulnerability / Exploit Key Points ● Joe was absent from today's meeting. This topic may in fact not need to be covered.	Joe Jarzombek
10 mins	Topic ● Conformance Key Points ● There was a discussion around the fact that the TS 17961 provides machine checkable rules for analysers, whereas MISRA-C provides guidelines for developers. It was discussed that all Rules in MISRA-C are machine readable, and the Directives are rules focused on developer behaviour. Only some of these are machine checkable, such as 'D4.12 Dynamic memory allocation shall not be used'. ● The update from the MIRA meeting is highly important here, in that it will sway the group in one direction or the other: essentially, the output of the group will either combine the TS 17961 and MISRA-C, or will become a quasi competitor. Either way, the group needs to adapt MISRA-C rules and develop our own description of them, which should happen naturally from an analysis of them. ● The schedule for Markham needs to be based on the scope of the work for the group, so it was decided to choose some MISRA-C rules to assign to people in order to be analysed for the next meeting. Each person to be become an 'advocate' for their rule, read through it and analyse it, propose whether or not the TS document covers this, in full or in part. Then think about whether the rule is a safety rule or a security rule. This should inform a group discussion on whether or not we want to modify	All

	and include the rule. This is the approach for now: it could change depending on the update from the MIRA meeting. ● Assignment details: 2 rules per person. ○ Robert Seacord - 2.4, 5.1 ○ Roberto Bagnara - 2.5, 5.2 ○ Adele Carter - 1.1, 2.6 ○ Clive - 1.2, 2.7 ○ Kostya - 2.2, 4.1 ○ Jill Britton - 2.1, 3.2 ○ Martin Sebor - 2.3, 4.2 ○ David Tarditi - 1.3, 3.1 ● Roberto raised the point that MISRA rules are written in a different spirit than the TS rules, and the focus of the group should be something in between the two, rather than starting off with the MISRA rules and potentially creating rules in a similar fashion (ie, very strict guidelines for developers). ● Robert said that this is the perennial issue with what the study group is trying to do. One approach could be to establish the 3 different profiles: Safety, Security and Safety / Security. Rules could fall into different categories. ● Ultimately, we will not be writing guidance for programmers: only rules for analysers to diagnose code constructs.What is included and what is left out is a large and open discussion. ● Clive: The way that MISRA expects conformance to be done is quite relevant to the group. A project could come back on a certain guideline and give a legitimate reason why it should not be followed in a specific case. So the MISRA view is that the guidelines are applicable in 95% of cases, but it is sensible to allow for this justification via a feedback mechanism, where a project can present its argument. This argument can then become part of the documentation and is available to look back on. MISRA took this route, rather than thinking about the edge cases and the exceptions for them. So MISRA does not expect 100% conformance, but a project needs a solid reason for not conforming and must justify this. This is thinking in terms of project conformance rather than the tool conformance. ● Robert: in terms of deviations and what's allowed: the group is not producing a set of requirements for conforming software, but is producing rules for what analysers do or do not have to diagnose. There is a distinction between this technical specification for analysers (what they should be checking for) and the behaviour expected of a programmer to follow. One way to handle this, could be to have tools capable of conforming to one or more profiles, as touched on earlier.	

	● Another point to make is that if someone says that a piece of software has to conform to TS 17961, that is a misuse of the standard. What should be said is that the software has to be free of diagnostics when analysed by a tool conforming to the the analyser specifications in TS 17961.Therefore we need to make it completely clear what the scope and purpose of the document is. ● Martin: the important question is: what's the minimum requirement? In practice, minimum conformance requirements are fairly weak: essentially tools need to diagnose a violation of such and such a rule. This is often fine when good quality tools are used, but what about when an updated tool is run and get warnings, but your product has already shipped? This conversation is one which is worth continuing. The struggle here is that things can become very hard to check for conformance - we need to establish the absolute minimum required.It is a different mindset: ● Perhaps there could be a different conformance requirement for different profiles in the TS.	
05 mins	Any Other Business ● Nothing that was not covered in the above comments. Key Points ● N/A.	All
05 mins	Topic ● Summary of all actions from today's meeting. Key Points ● See Action Log	Laurence Urhegyi

Action Log

See here

Gitlab Wiki

See here