C Safety / Security Study Group
Meeting Agenda and Minutes

Date: Wednesday 22 March 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 ● Robert has met recently with representatives from MISRA and had further positive discussions, but not yet any substantial commitments regarding their stance on collaboration and combining the work of MISRA and the TS 17961.	Laurence Urhegyi

	● We'll continue to progress as we are, for now. ● This meeting has changed to 1pm in the US now, but due to UK time changes soon, will be back to a 12pm start time. This can be reviewed periodically. ● Should we hold a meeting during the WG14 / C Standards meeting in Markham, w/c Monday 03 April. ● It probably won't be feasible to hold a meeting there, so let's cancel the next meeting in 4 weeks. ● **Action:** Laurence to send out a mail informing everyone that the next study group meeting is cancelled. ● **Action:** Robert to send out a mail asking if members are still interested in the study group, to try and encourage participation in the group.	
10 mins	Topic ● Rule 1.1 ● **Vote**: should the 'constraint violations' rule be included in the standard? ● No consensus last time. Key Points ● Rules without a consensus should be added to 'the end of the queue' rather than being discussed immediately again during the next meeting. For this reason we'll re-visit this rule at a later date.	Robert Seacord
10 mins	Topic ● Rule 1.2 ● Discussion of this rule may be dependent on the proposal of how language extensions should be handled, from Gavin. Key Points ● Not discussed today: awaiting discussion on the mailing list after Gavin's post.	Clive Pygott Gavin McCall
10 mins	Topic ● Rule 1.3 Key Points ● Not discussed today: no submission to the wiki yet.	David Tarditi
10 mins	Topic ● Rule 2.1 Key Points ● Not discussed today: Jill was not present.	Jill Britton
10 mins	Topic ● Rule 2.4 (no consensus last time). Key Points ● Placed at the back of the queue.	Robert Seacord
10 mins	Topic ● Rule 2.6	Adele Carter

	Key Points ● Not discussed today: Adele was not present.	
10 mins	Topic ● Rule 2.7 Key Points ● Aaron provided an update the mailing list on ‘unused code’ in general. For a security profile, it does not seem to make much sense to add in rules around the use of unused code. They don’t have any impact on the security of the program. For a safety profile, ‘unused code’ can be used against you in court if a safety critical system contains dead or unused code. This is also a question of style ● Clive: unused code is not just a style issue: it’s in the mindset of writing the code, so the question is ‘what is a system doing with code if it is not using it?’ - everything should be traced back to the requirements of the system. ● Aaron: this is not true because of the use of libraries in use. Code that runs on top of a real time Operating System, which includes a lot of code there which will not be used. ● Clive: when creating a safety critical system, you should not be writing general purpose libraries - you are creating a system to meet very specific requirements. This is where a deviation comes into play. ● Aaron: the distinction seems to be between general code written by the developers of a safety critical system, and general code which is ‘inherited’ by the team developing the system. Should these be treated differently in terms of deviation? ● Clive: Yes. It’s related to code that comes from within a controlled environment or code from outside of a controlled environment. You need to justify why you’d be using code from outside of your own controlled environment and not creating it yourself. ● Aaron: that makes sense. It is useful to include these rules in the safety critical profile in that case. ● Robert: I am wondering if we need an exception here for comments. ● Aaron: A good example of something which makes things clearer and is very helpful but has no impact whatsoever on the code. ● Robert: analyser tools to be used in the safety critical market will need to be able to diagnose unused code. We should capture the points of the above discussion as a ‘rationale’ against each rule. ● **Vote:** No specific vote taken on this rule, as we reached a conclusion on the general point made above, ie: to include rules that focus on dead code.	Clive Pygott

10 mins	Topic ● Rule 4.1 Key Points ● Kostya did a write up which he included on the wiki, but is not participating in the group any more so it was decided that we should discuss this rule now. ● Clive: I can see the logic in this rule, it seems to be more of a style rule: it seems to have an issue in that it does not capture something which is a genuine mistake. If two characters are used: is the second digit intended or is it part of the hex, as it will be compiled as part of the hex? ● Robert: this is what Kostya suggests in his write up as well. From a security perspective, this should not be considered, since it takes correct code and makes it non-conforming. ● Clive: I do not see that as significant as the rules around 'unused code'. From a security perspective this is not a vulnerability. ● Robert: Should this be safety only or is it not needed at all? Kostya's suggestion on the wiki seems sensible, where it says it should only be 2 characters if it's a hex, which seems to be a reasonable extension of this. ● See here for that write-up: https://gitlab.com/trustable/C_Safety_and_Security_Rules_Study_Group/wikis/misrarules4 ● Robert: it's a stylistic choice because it is recommending the use of a constrained style to indicate intent beyond the semantics of the language. ● Clive: agreed that this is a style rule, it seems strong to say this should be required. ● Robert: with only 3 people on the call it's probably not fair to hold a vote, so we should re-visit this as we don't have a quorum. But it seems as though this rule could be one which does not make the cut.	Robert
10 mins	Topic ● Rule 5.6 Key Points ● Aaron: this rule prohibits re-using the name of a typedef across all translation units (including other typedefs). Can't see any place for this rule in a security profile, but certainly seems appropriate for a safety profile. However, the rule should be re-written, because it is actually very restrictive: it does not take account of scope at all. For example, if you have a translation unit which has a typedef that is local to a function and then in a different translation unit you have a static function with the same name that is a violation of this rule, yet it has no chance at all of having any impact on this code, and is also highly unlikely to even cause confusion to a user.	Aaron Ballman

	● Clive: this seems to be a category of a 'meta-rule', as it comes up a number of times. Ie. not re-using names. I'd say the rule as it is written should be fine: I don't think we need to include anything about specific scope here. ● Aaron: that means that the amount of data to be tracked is huge. Which is fine, it is certainly not impossible to do, but for projects with a large code base it will be very expensive. Every identifier will have to be tracked, across the entire program. ● Clive: there are other rules which will specify that a tracking mechanism such as the above should be kept for the project. ● Roberto: although I can't hear the conversation so well I believe this rule should in the safety profile. ● Robert: there is a consensus that this rule belongs in the safety profile.	
05 mins	Any Other Business ● SafSec Action Research Day 31st October at the BCS entitled: ○ 7 years on SafeSec Software is a common expression - do the Cloud and IoT make a difference? Key Points ● Not discussed today: Adele was not present.	Adele Carter
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