

To: Jonathan Hodgson
cc: John Hill (Chairman, ISO/IEC JTC1/SC22), Sally Seitz (Secretariat, SC22)
Date: 31 August 2004
Subject: Future Standards Development in SC22
Re: N3792, "Announcement of Ad Hoc on Future Standards Development in SC 22"

I suggest consideration of work dealing with "High Integrity Language Usage".

There is a growing body of evidence that when developing software for a system that must exhibit a critical property—such as safety or security—it is appropriate to use programming languages in a more disciplined manner. We have seen examples of several approaches:

- Special languages, e.g. SPARK [Barnes]
- Language subsets, e.g. MISRA C [Hatton, MISRA]
- Language profiles or dialects, e.g. [Kwon]
- Usage guidelines, e.g. [Erkinnen]

We have also seen examples of standardization activity on this subject, e.g. ISO/IEC TR 15942, "Guide for the use of the Ada programming language in high integrity systems" [ISO15942] and MISRA C [Hatton, MISRA].

To date, though, nearly every sustained effort has considered individual languages in isolation. There has been no effort to describe the existing languages in a commensurable manner supporting comparison. There has been no effort to provide consensually-validated guidance in how to go about selecting a language suitable to a problem with given integrity requirements.

The proposal is to establish a working group with the charter to:

Develop language-independent and cross-language guidance for the selection and use of programming languages in high integrity systems.

The working group could consider the following projects among others:

- A guide to selecting a programming language suitable to a high-integrity application
- A comparison of programming language characteristics suitable to high-integrity usage
- Standards for meta-language constructions—e.g. assertions and other mechanisms for demonstrating correctness—in a manner that is uniform or comparable across programming languages
- Standards for subsets, profiles, or dialects of programming languages suitable for high integrity application
- Guides for usage of programming languages in a manner suitable for high integrity application

I believe that this work should be focused in a single working group in order to achieve commensurate treatment across the body of programming languages. Furthermore, separating the work from the programming language working groups will permit the

consideration of non-ISO languages where appropriate, e.g. usage guidelines for Java. Nevertheless, it is clear that it would be a serious mistake to neglect the resource provided by the working groups of SC22.

Therefore, I would suggest that this working group would be staffed by experts provided by the other programming language working groups as well as by national body experts. Furthermore, the working group would seek liaisons with other standard-making organizations engaged in programming language definition. It would probably be appropriate for the working group to schedule one of its meetings each year to be collocated with plenary meeting of SC22.

References:

[Barnes] John Barnes, "High Integrity Software: The SPARK Approach to Safety and Security", Addison-Wesley, 2003.

(Ordering info: http://www.amazon.com/exec/obidos/tg/detail/-/0321136160/qid=1093294642/sr=1-3/ref=sr_1_3/103-2049930-1905419?v=glance&s=books)

[Bhansali] P. V. Bhansali, "A Systematic Approach to Identifying a Safe Subset for Safety-Critical Software," P. V. Bhansali, "A Systematic Approach to Identifying a Safe Subset for Safety-Critical Software," ACM SIGSOFT Software Engineering Notes, Volume 28, Issue 4 (July 2003).

(Text at: <http://doi.acm.org/10.1145/882240.882252>)

[Erkinnen] Tom Erkkinen, "Developing High-Integrity Software in C and Ada" SAE Technical Paper Series 1999-01-0265

(Ordering information:

http://www.sae.org/servlets/productDetail?PROD_TYP=PAPER&PROD_CD=1999-01-0265)

[Hatton] Les Hatton, "Safer Language Subsets: an overview and a case history, MISRA C," Information and Science Technology, 46 (2004), p. 465-472.

(Text at: <http://www.leshatton.org/Documents/MISRAC.pdf>)

[ISO15942] ISO/IEC TR 15942:2000, "Information technology -- Programming languages -- Guide for the use of the Ada programming language in high integrity systems"

(Text at:

[http://www.iso.org/iso/en/ittf/PubliclyAvailableStandards/c029575_ISO_IEC_TR_15942_2000\(E\).zip](http://www.iso.org/iso/en/ittf/PubliclyAvailableStandards/c029575_ISO_IEC_TR_15942_2000(E).zip))

[Kwon] Jagun Kwon, Andy Wellings, Steve King, "Ravenscar-Java: A High Integrity Profile for Real-Time Java," Joint ACM Java Grande / ISCOPE 2002 Conference, November 2002, Seattle

(Text at: <http://doi.acm.org/10.1145/583810.583825>)

Also their presentation:

(Text at: <http://www.opengroup.org/rtforum/info/jul2002/slides/wellings.pdf>)

[Mazzanti] Franco Mazzanti, "Coding Regulations for Safety Critical Software Development," Second IEEE International Software Standards Symposium, August 1995

(Text at:

<http://ieeexplore.ieee.org/iel3/3966/11453/00525958.pdf?tp=&arnumber=525958&isnumber=11453&arSt=134&ared=138&arAuthor=Mazzanti%2C+F.%3B>)

[MISRA] Motor Industry Software Reliability Association (MISRA), "Guidelines for the Use of the C Language in Vehicle Based Software", ISBN 0 9524156 9 0, April 1998.

(Ordering information: <http://www.misra.org.uk/>)