To: Participants in SC22 Study Group on Support of High Integrity Applications
From: Jim Moore, Convener, JTC1/SC22/WG9
Subject: Proposed New Work on Support for High Integrity Applications
Date: 27 October 2004

The purpose of this note is to kick off a study group to create a proposal for new work by SC22 in the area of "Support for High Integrity Applications". Those of you who aren't familiar with the organization of international standardization may want to take a quick look at the appendix of this document.

Additional participants are welcomed to our study group. Please feel free to circulate new of our work. People who are interested in joining should send me an email: mailto:James.W.Moore@ieee.org.

At its recent plenary meeting, SC22 approved the following resolution:

Resolution 04-13: Ad Hoc on the Future Directions for SC 22
JTC 1/SC 22 resolves that the Ad Hoc on the Future Directions for SC 22 be continued for a period of one year with Jonathan Hodgson as convener. The Ad Hoc is charged to explore the following four areas agreed upon at the Ad Hoc Meeting on the Future of SC 22 held on 6 September 2004:

- Support for High Integrity Applications
- Libraries
- Industrial Consortia
- Standards Education

SC 22 instructs the convener to organize a meeting of the Ad Hoc in March 2005 to report on and prepare recommendations for the 18th SC 22 plenary, on future work directions for SC 22. SC 22 instructs that agenda time at the March meeting is to be given only to those items for which a written contribution is submitted by 15 January 2005. Should no written contributions be submitted for this meeting, the meeting shall be canceled.

I was selected as the coordinator for "Support for High Integrity Applications". In order to prepare for the March 2005 meeting, I need to develop responses to, at least, the following questions:

1. What kind of deliverable would this area produce: Standard, Technical Report, workshop, or other?

2. What kind of structure should SC22 set up to manage any new project, a Working Group or something else.

3. Who should be approached to involve themselves in any Working Group or other structure that SC22 might set create.

The remainder of this note summarizes my own ideas for performing work on this subject. I would like to hear your ideas.

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 disciplined 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 commensurate 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 (Standard or Technical Report) to selecting a programming language suitable to a high-integrity application
- A comparison (Technical Report) 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 (probably Technical Reports) 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 participation by other organizations engaged in programming language definition or practices for the use of programming languages in high integrity applications.

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)

[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/)

Appendix: International Standardization of programming languages

First, let me give a quick overview of organization:

- The International Electrotechnical Commission (IEC) is responsible for standardization of electrical and electronic devices;
- The International Organization for Standardization (ISO) is responsible for standardizing nearly everything else;
- ISO/IEC Joint Technical Committee 1 (JTC1) is responsible for standardization of Information Technology;
- ISO/IEC JTC1 Subcommittee 22 (SC22) is responsible for standardization of programming languages and operating system interfaces;

SC22 created a study group to look at possible new projects for SC22. My suggestion for supporting high integrity applications was submitted to this study group and I was told to proceed with a sub-study group to flesh out the idea.

Our results will be submitted to the Future Directions Study Group for their consideration at a meeting in March. They will report to SC22. If our idea is favorably received, we will be asked to write a New Work Item Proposal (NP) for approval by SC22 and JTC1.

Upon submission of the NP, life becomes more formal. Now we are simply a group of interested people. After submission of the NP, all decisions are made by votes of national standards bodies. For our NP to be approved, at least five nations would have to agree to participate.

Assuming our NP is approved, SC22 would probably create a Working Group to perform the work.