Business Plan and Convener's Report
ISO/IEC JTC 1/SC 22/WG 23 (Programming Language Vulnerabilities)

Document:
ISO/IEC JTC 1/SC 22/WG 23/N0470

Date:
2014-08-08

PERIOD COVERED:
July 2013 – July 2014

SUBMTTED BY:

Convener, ISO/IEC JTC 1/SC 22/WG 23: Vulnerabilities
Thomas Plum
Plum Hall, Inc.
PO Box 44610
Kamuela HI 96743
USA

Office: *+1 (808) 882-1255*
E-mail: *tplum@plumhall.com*

1. MANAGEMENT SUMMARY

1.1. JTC 1/SC 22/WG 23

Guidance to Avoiding Vulnerabilities in Programming Languages through Language Selection and Use

1.2. PROJECT REPORT

1.2.1. COMPLETED PROJECTS

ISO/IEC TR 24772:2012, *Guidance to Avoiding Vulnerabilities in Programming Languages through Language Selection*. This is a Technical Report.

1.2.2. PROJECTS UNDERWAY

JTC 1 NP 24772, *Guidance to Avoiding Vulnerabilities in Programming Languages through Language Selection*. This is the 3rd edition.

JTC 1 NP 17960, *Code Signing for Source Code.* This project is to produce an International Standard, and currently is in DIS ballot.

1.2.3. CANCELLED PROJECTS

None over this time period.

1.2.4. COOPERATION and COMPETITION

Where appropriate, WG 23 has established active liaisons with other SC22 working groups and other standards organizations.

There is no apparent direct competition with any other current SC22 working group.

2. PERIOD REVIEW

2.1. MARKET REQUIREMENTS

Knowledge about vulnerabilities and matching advice for their avoidance is essential information for the reliability, safety and security of software applications. By identifying these vulnerabilities in a language-independent fashion and giving language communities the opportunity to add their language-specific advice, significant benefits accrue to writers of coding guidelines, quality management organizations, testers, and the ultimate users of the software produced in accordance with these guidelines. WG 23 feels that it is responding to the needs of the programming language community by inclusion. WG 23 will accept input and liaison by any and all appropriate organizations.

2.2. ACHIEVEMENTS

WG 23 had published the second edition of TR 24772, and worked on the third edition, when the loss of its convenor for more than six months and an SC22 discussion over the merits of WG23 put the group in a forced hiatus.

WG 23 worked on the 17960 project, a second CD ballot and concluded with unanimous approval without comments, see SC 22 N4892.

2.3. RESOURCES

WG 23 is waiting to know the outcome of the decision of SC 22, whether or not to disband WG 23. Six national bodies are currently participating in the most recent teleconference meeting: Canada, Italy, Japan, Spain, UK, and the USA, as well as several liaisons.

Over the last several years WG 23 has made Web conferencing capabilities available for those that are finding it difficult to travel. WG 23 would like to thank ISO for the Web conferencing support.

Liaison with five SC 22 Language groups, and four groups outside of SC 22 has been established.

Current WG 23 liaisons are:

Group	Name/Type	Person assigned
SC 22/WG4	Cobol	Barry Tauber
SC 22/WG5	Fortran	Dan Nagle
SC 22/WG9	Ada	Erhard Ploedereder

SC 22/ WG14	C	Tom Plum
SC 22/ WG 21	C++	Group (Tom Plum)
SC 7/WG 19	Open Distributed Processing and Modeling Languages	Cesar Gonzalez-Perez
ECMA TC39/TG2	C#	Tom Plum
JSR-282/JSR-302	Real-Time/Safety-Critical Java	Ben Brosgol
Linux Foundation	Linux	Nick Stoughton
MDC	MUMPS	Ed de Moel

3. FOCUS NEXT WORK PERIOD

The future of WG 23 will depend upon the decision of SC 22 as per N4928 agenda item 8.

3.1. DELIVERABLES

None.

3.2. STRATEGIES

See "Attachment: Factual Matters which are Unanimously Agreed by WG 23 Members"

3.3. RISKS

See "Attachment: Factual Matters which are Unanimously Agreed by WG 23 Members"

3.4. OPPORTUNITIES

See "Attachment: Factual Matters which are Unanimously Agreed by WG 23 Members"

3.5. WORK PROGRAM PRIORITIES

See 4.1.

4. OTHER ITEMS

4.1. POSSIBLE ACTION REQUESTS AT FORTHCOMING PLENARY

WG 23/N0469 (agenda for July-August 2014 telecons) contained the following item:

> 4. Document Drafting for SC 22 Plenary (Madrid, September 2014)
> WG 23 will prepare several documents for the SC 22 Madrid plenary:
> (a) Factual matters which are unanimously agreed by WG 23 members;
> (b) The arguments for disbanding WG 23;
> (c) The arguments against disbanding WG 23.

Items 4(a) and 4(c) are attached to this Convener's Report, and have been approved by WG 23.

However, item 4(b) ("The arguments for disbanding WG 23") was objected to on the telecon. The convener then said that item 4(b) will be covered in the Convener's Report (this document), since this Convener is committed to full consideration of all arguments (for and against disbanding WG 23).

Item 4(b) appears in "Attachment: The Case for Disbanding WG 23".

If SC 22 does not disband WG 23, then WG 23 will work on the third revision of TR 24772.

4.2. PROJECT EDITOR

The following individuals have been appointed project editors and backup project editors:

- JTC 1 NP 24772, Guidance to Avoiding Vulnerabilities in Programming Languages through Language Selection.
  (Project Editor vacant, backup Project Editor vacant; however, 4 candidates have expressed their willingness to become a Project Editor team)
- JTC 1 NP 17960, Code Signing for Source Code.
  Larry Wagoner (Project Editor), backup Project Editor vacant

4.3. ELECTRONIC DOCUMENT DISTRIBUTION

WG 23 has conducted some of its detailed technical discussion using email reflector maintained by MITRE Corp. WG 23 also has an ftp and Web site at http://grouper.ieee.org/groups/plv/.

WG 23 is providing all the appropriate committee documents on the Committee Web site, eliminating the need for paper mailings. WG 23 has been given permission to maintain this document distribution until SC 22 decides upon the future of WG 23.

4.4. RECENT MEETINGS

#1	26-27 Jun 2006	District of Columbia, US	ANSI/INCITS and Blue Pilot
#2	14-15 Sep 2006	London, UK	BSI
#3	11-13 Dec 2006	District of Columbia, US	ANSI/INCITS and Blue Pilot
#4	30-2 Apr/May 2007	Padova, IT	NNI
#5	18-20 July 2007	Ottawa, Ontario, CA	SCC

#6	14-15 Oct 2007	Kona, HI, US	ANSI/INCITS & Plum Hall
#7	10-10 Dec 2007	Pittsburg, PA, US	ANSI/INCITS & CERT
#8	09-11 Apr 2008	Amsterdam, NL	NEN, ACE
#9	29-01 Sep/Oct 2008	Stuttgart, DE	Universität Stuttgart
#10	13-15 Apr 2009	San Diego, CA, US	ANSI/INCITS & MITRE
#11	13-15 July 2009	Ottawa, Ontario, CA	SCC
#12	01-03 Nov 2009	Santa Cruz, CA, US	ANSI/INCITS & Blue Pilot
#13	26-28 Apr 2010	Padova, IT	UNI
#14	28-30 Jul 2010	Kona, HI, US	ANSI/INCITS & Plum Hall
#15	15-17 Sep 2010	Ottawa, Ontario, CA	SCC
#16	14-16 Dec 2010	San Diego, CA, US	ANSI/INCITS & MITRE
#17	23-25 Mar 2011	Madrid, ES	AENOR & Telefónica I+D
#18	18-20 Jun 2011	Edinburgh, UK	The Ada Connection
#19	05-07 Oct 2011	Teleconference	ISO
#20	14-16 Dec 2011	Washington, DC, US	INCITS & Jim Moore
#21	28-30 Mar 2012	Ottawa, Ontario, CA	SCC
#22	20-22 Jun 2012	Stuttgart, DE	Universität Stuttgart
#23	12-14 Sep 2012	Geneva, CH	IEC
#24	12-14 Dec 2012	Teleconference	ISO
#25	13-15 Mar 2013	New York, NY, USA	ANSI/INCITS & Blue Pilot
#26	08-10 Jun 2013	Berlin, DE	The Ada Connection
#27	18-21 Sep 2013	Tokyo, Japan	ITSCJ
#28	08 Jul 2014 etc.	Teleconference	ISO

4.5. FUTURE MEETINGS

#29	18 Sep 2014	Teleconference	ISO

Attachment: Factual Matters which are Unanimously Agreed by WG 23 Members

Some History

The original project proposal for this group came (June 2005) from James W. Moore (MITRE Corporation, US). (Jim was the former convener of SC 22's WG 9 (Ada), a long-time SC7 member, and an experienced standards participant and manager.) He was the founding convener, then the secretariat. From the beginning, he has maintained the group's website, at http://grouper.ieee.org/groups/plv/.
Jim got John Benito involved as convener (appointed September 2006). (John has been WG14 [C language] convener for 18 years, and a member before that; he was a long-term member of WG21 [C++]; and an experienced standard's participant and manager.) He also served as project editor of the TR.

The leadership and TR editor set a high bar in project management and product quality, thanks to the efforts of Jim Moore (who has subsequently left the group) and John Benito (who had taken over the secretary responsibilities).

WG 23's initial work was a TR on "Guidance to Avoiding Vulnerabilities in Programming Languages through Language Selection and Use". By the end of 2013, the committee has produced two editions. After the production of the second edition of TR 24772, the group met and decided unanimously to work towards the development of a third edition. The initial items to be considered are contained in the 2013 WG 23 convenor's report to SC 22.

A couple of years ago, a smaller, unrelated project, a standard for Code Signing for Source Code, was started. The US provided the project editor. That document is currently in DIS ballot.

In the summer of 2013, John Benito announced he had lost funding for his work, so would not be able to attend the September Plenary of SC 22 or the following 3-day WG 23 meeting, in Japan. However, he said, he'd look around for alternate funding sources.

Around November 2013, John Benito resigned as convener, and as has been SC 22's mode of operation, his sponsoring NB, the US, got first shot at coming up with a replacement. It issued a 30-day call for convener nominations. The first call went unanswered. However, Dr. Thomas Plum, INCITS/PL22 chair (and longtime WG 14, WG 21, and WG 23 participant, and former WG 21 convener) responded to the second call. PL22 and INCITS endorsed Dr. Plum, and the SC 22 Secretary appointed him as acting convener, in January 2014.

Overview regarding Resources and Commitments

There are many different ways in which resources are provided for doing the work needed to perform the tasks within WG 23 and they depend on the work to be done: Formulating the technical content and editorial presentation of the Core document of the TR has always been the task of WG23 members. The tasks involving the generation and review of technical content are allocated to members at meetings. The editorial insertion of the content into the document is the responsibility of the Project Editor(s).

Formulating the technical content of the Annexes has been delegated to other working groups, mostly within the ISO context, or to experts that were best qualified to represent the language-specific knowledge, while the editorial polishing of the Annexes was kept within WG23.

The respective Resources need to be available. Where external entities are involved, WG23 trusts the commitments made by these other entities. When a WG23 member commits to do assigned work, WG23 trust the commitment by the member. In all cases, Wg23 presumes that any commitment made is backed up by the necessary resources under control of, or procured by, the committing person.

Beyond the technical and editorial efforts, as in all ISO contexts, members are responsible for the funding needed for their own travel expenses. Presence at physical meetings is not mandatory. To minimize travel costs, meetings are scheduled in conjunction with other events, e.g. conferences, attended by (different) subsets of members. Whenever feasible, physical meeting allow for remote participation via WebEx as well. Four multi-day annual meeting have been the normal schedule of WG23.

At present, the following resources are committed, where most commitments and work initiations are contingent on the premise that WG23 has a clearly defined future:

- Larry Wagoner committed to be Project Editor of the Code Signing Standard.
- WG9 via its Rapporteur Group HRG will update the Ada Annex to match Version 3 of the TR, which is to be constructed by WG23. WG9 asks for a prior commitment of WG23 to continue the WG23 work. HRG has also committed to coordinate with the editors of the Spark Annex about the Ada-specific elements of the two Annexes. Erhard Ploedereder has committed to WG9 the coordination with the Core portion of the TR and to editorial work on the Annex.
- WG 5 has committed to update the Fortran Annex to match Version 3 of the TR. Dan Nagle provides the connection.
- The Japan Ruby committee committed in September 2013 to maintain the Ruby annex. The original author Jim Johnson might be involved as well. Larry Wagoner provides the connection to the latter.
- Talks are well underway to engage two persons of the company that designed the Spark language to update the Spark Annex to match Version 3 of the TR. See also the commitments by WG9.
- Kevin Coyne, the author of the PhP and Python annexes, is willing to updating them to match Version 3 of the TR; he is in the process of procuring the resources
- The C Annex was produced by John Benito in association with WG14. WG14 has not been contacted yet by WG23 to query its willingness to update the C Annex. Here, the MISRA C group might be a suitable replacement if WG14 declares that it has lost interest or has insufficient resources.
- At this point in time, Clive Pygott, Erhard Ploedereder, Stephen Michell and Larry Wagoner have expressed their willingless to serve WG23 in the roles of Convenor, Project Editors and/or Secretary to ensure that the work progresses. The specific assignments of persons to roles still needs to be discussed and decided by WG23 and SC22.
- It is expected that all members of WG23 will, as in the past, commit the necessary time to amend their assigned vulnerability topics and to review their assigned portions of the TR when called upon to do so prior to the republishing of the TR.

Future Work Items:

- Regrettably WG21 is not interested in producing a C++ Annex. The MISRA-C++ group might be a suitable candidate for producing a C++ Annex. The C Annex, amended with the various mitigating mechanisms available in C++ might be a good starting point, given that all vulnerabilities of C are present in C++ by virtue of the subset property.
- At present, there is no Java Annex, nor is there an ISO WG dealing with Java. Finding an expert group for the writing of a Java annex is left as a future work item, since one will have go outside ISO for such work.

Annexes

Annexes to the TR were produced to contain the language-specific elaboration of the vulnerabilities identified by the TR. WGs within ISO responsible for individual languages or top language experts known in the respective language community were invited to contribute such Annexes. When Annexes were produced, they were reviewed by WG 23 for accurate interpretation of the core TR, and, if approved, included by the Project Editor as Annexes of the TR. In this fashion, Annexes for Ada, C, Fortran and Spark were produced in close coopoeration with other WGs within SC 22.

The Ruby annex was originally written by Jim Johnson by the agency of Larry Wagoner, and reviewed by the Japan Ruby committee.

Kevin Coyne produced the Python and PHP annexes and is contacting his sponsor to see if they are interested in continuing that sponsorship.

Opinion within WG 23

There is no doubt that several members of WG 23 are committed to the continuation of WG 23 to at least produce a third edition of TR2 4772. It is reasonable to assume that of the members who attend the WG 23 meetings and telecons, a majority of those members are strongly in favour in continuing work in TR 24772 through WG 23 within SC 22.

An overwhelming majority of the WG 23 members on the telecon August 7 favored the arguments in "Attachment: The Case for WG 23", and a small minority favored the arguments in "Attachment: The Case for Disbanding WG 23".

Attachment: The Case for WG 23

As identified in 2006, vulnerabilities in code make the use of many programs insecure or unsafe. Many of the vulnerabilities are identifiable and preventable, and can be avoided by the application of straightforward sets of rules, many of which are language dependent.

SC 22/WG 23 has been working to identify vulnerabilities and to formulate guidance for coders, and language designers to help eliminate vulnerabilities in real programs.

To date WG 23 has produced 2 editions of TR 24772. The first edition contained only the language-independent portion of the guidance with 51 language-related vulnerabilities and 17 design-related vulnerabilities. The second edition added 12 new language vulnerabilities, 4 new design-related vulnerabilities, and six language-specific annexes. The language-specific annexes were developed out of sync with the main document, meaning that six of the new vulnerabilities had to be placed in a separate clause because there was no language-specific annex material ready.

Nobody in WG 23 believes that the work is finished, i.e. that all relevant vulnerabilities have been identified, or that the set of language-specific annexes is complete or up-to-date. Specifically,

1 Other language developments, such as the addition of contract-based specifications (preconditions, postconditions and invariance);

2 We still lack vulnerabilities associated with multicore or vector-based parallelism; with floating-point and fixed-point arithmetic; with real-time and event-driven processing or concurrency.

3 The rise of strong static analysis tools provide the opportunity to rework some of the guidance to include such factors;

4 Common programming language annexes are missing, such as Fortran, C#, Java, C++, and Objective-C.

Members of the US NB has claimed that we lack resources to complete the work. In September 2013, there were 8 active members working on the core document. With the loss of the convenor and editor, a plan was put into place to populate those positions. Since that time, WG 23 has added commitments from a member from Spain, two members from the UK with expertise in formal methods and numerics, the re-engagement of the member that wrote our PHP and Python annexes, and a request for liaison with SC 27/WG 3 and WG 4. If anything, the group appears to be more robust and more diverse than previously.

In summary, the significant majority of active members of WG 23, and the entities that they represent (national bodies and liaisons) are convinced that the work of WG 23 is relevant and necessary and that WG 23 must continue to function.

Attachment: The Case for Disbanding WG 23

The WG 23 "Endless Loop"

Back when no one anticipated that the committee's most active members would not be able to continue, it seems in retrospect that WG 23 created a recipe for an endless loop, as follows:

1) During the same time as new Language specific Annexes were being created by one or more programming-language groups, WG 23 was working on revising the Vulnerabilities TR (24772).

For example, WG 23/N0461 shows the August 2013 initial draft of TR 24772 3rd edition which has 8 new vulnerabilities in clause 6 and 6 new vulnerabilities in Clause 7, leaving Clause 8 empty.

2) WG5 worked diligently on an Annex, which was supposed to eventually be merged into the 3rd edition of TR 24772, but this Annex referred to the topics of (the published) TR 24772 2nd edition.

3) WG 23 has preferred to defer to the individual programming-language groups to determine the applicability of the topics in clause 6 to their specific programming language.

One might suggest that WG 23 could break this infinite loop by deciding, when new topics are added to clause 6, whether those topics do or don't apply to individual programming languages.

However, in our opinion, that would be a mistake, because those decisions are more likely to be incorrect for those languages that don't happen to have much representation on WG 23. It remains a reasonable decision to defer to the programming-language experts.

Estimates of Resources Required for a Third Edition of TR 24772

Right now, the published TRs (24772:2009 and 24772:2013) represent many hours (approximately 2000 hours) of editorial work, and many more hours (approximately 500 hours) would be required to produce a 3rd edition including an annex for WG5. (To the best of our knowledge, the work of producing the PHP Annex, the Python Annex, and parts of the C Annex to the published TRs was performed on a Contractor basis, paid hourly.) Furthermore, all the other programming language annexes would be required to be updated to meet the requirements of the 8 extra vulnerabilities (plus any new vulnerabilities) required by a 3rd edition (not to mention the extra work of reordering Clauses 6 and 7 of TR 24772; just adding the new vulnerabilities at the end of a Clause brings an inconsistency to the clause). Based on past experience, a rough estimate of that extra work imposed upon the other programming-language groups would be 500 hours of work.

The many hours of work in preparing the WG 5 annex for TR 24772 2nd edition can be salvaged by publishing that annex as a stand-alone document. The same could be done for any other language committee that desires to create a similar annex. Or, as an alternative, this Convener has offered to produce a revised edition of TR 24772 2nd edition which includes the WG 5 annex.

Summary

For all the reasons above, we recognize that there may never be a perfect time to close down the work of WG 23, but the present moment, having completed a successful ballot round on TR 24772 2nd edition, and publication of the 2nd edition, is all-things-considered the moment to disband with the least disruption.
Ultimately, each national body within SC 22 will need to determine whether WG 23 does indeed have the resources to continue its work.