ISO/IEC JTC1/SC7
Software Engineering
Secretariat: CANADA (SCC)

ISO/IEC JTC1/SC7 N2324

2000-05-25

Doc. Type	Report
Title	Report of the Study Group on the Future of WG9
Source	Study Group on the Future of Working Group 9 Convener
Project	
Status	Final
References	
Action ID	FYI or ACT
Due Date	
Mailing Date	2000-05-25
Distribution	SC7_AG
Medium	Encoded Acrobat
No. of Pages	7
Note	

Address reply to: ISO/IEC JTC1/SC7 Secretariat
Bell Canada - Quality Engineering & Research
1050 Beaver Hall Hill, 2nd Floor, Montréal (Québec) Canada H2Z 1S4
Tel.: +1 (514) 391-8286 Fax: +1 (514) 870-2246
sc7@qc.bell.ca

Report of the Study Group on the Future of WG9

Resolution 570 mandated the creation of a Study Group on the *Future of Working Group* 9. The matter was discussed at a mini-BPG meeting in Nantes last October and progressed during the winter. The members of this Study Group are:

- Paul Croll (US) as convener
- Jim Welsh (Australia)
- Hans Daniel (Germany)
- Thuy Nguyen (France)
- Dave Kiang (Convener of WG9)

The Study Group was requested to prepare its report with recommendations by 5 May 2000, so that the report could be circulated to Member Bodies for consideration at the upcoming plenary meeting in Madrid.

Summary

A summary of our observations and recommendations follows:

1. The need for integrity standards reflects a business necessity.
2. Integrity is a fundamental element within the SC7 standards framework.
3. SC7 should retain WG9 as the group responsible for integrity-related standards and issues, and should ensure appropriate coordination between WG9 and WG7, and any other SC7 group dealing with relevant issues.
4. An even-handed, liaison-based, relationship to all sector groupings with integrity interests should be maintained.
5. The Joint Working Group relationship with TC56/WG4 should be replaced by a formal liaison.
6. A new Convenor for the reconstituted WG9 should be appointed as soon as possible, to begin developing and executing a new SC7-related program of work.
7. Near term actions:
   - 7.1. A new mandate and terms of reference for the new WG9 should be defined.
   - 7.2. A business plan should be established to guide standards development in aid of project management.
   - 7.3. A product plan should be developed to address the priority and scope of each PNWI to formalize the SC7 projects.
   - 7.4. Market needs for each of the PNWIs should be identified.
   - 7.5. The program of work and resource availability should be established,
   - 7.6. A Requirements Document for justification in launching each new project should be developed and approved, to validate project goals and objectives.
8. The Study Group further recommends that a time limit be set for the actions described in recommendation 7, above. Should no new work items be approved prior to the 2001 Plenary, WG9 should be dissolved at that time.

Finally, the Study Group wishes to thank Dave Kiang for his outstanding leadership, good spirit, and dedication to quality during his tenure as JWG Convenor.

Study Group Report

The Study Group posed a set of questions regarding the future of WG9, and proceeded to build a consensus position through discussion of responses to those questions. The questions considered by the Study Group, and our consensus position for each, are listed below.

Q1. Are integrity-specific standards needed?

The answer, Yes, is obvious to us, but may need elaboration for some members of the SC7 community. Computer-based systems are increasingly pervasive and many play a critical role in our lives. Assuring integrity in the design, implementation and evolution of critical systems becomes a dominant concern. Compliance to Standards is universally recognized as the key to managing the provision of the required assurance. Development and improvement of such standards is therefore of paramount concern.

The business needs for standardization of Software and Systems Integrity within SC7 are reflected in the generic system engineering management model, and closely associated with the system and software life cycle processes for designing/building/acquiring/supporting software products and systems.

This generally involves:

- The need to determine risk exposure and related containment;
- The need to establish integrity requirements and integrity assurance criteria;
- The need to define integrity design and assurance processes/activities;
- The need to validate integrity assessment methods for assurance;
- The need to analyze and interpret integrity data;
- The need to justify resources and expenditures on integrity effort, e.g. for project management.

The need for integrity reflects a business necessity. The degree of engineering rigor required to achieve an acceptable integrity level depends on its specific application. Standardization of integrity fosters supplier-customer communications and facilitates producer-user dialogue for international trade. We now live in an Information Society, where e-business and dot.com manias are omni-present in our daily lives. The performance of current network services and IT (Information Technology) equipment still leaves much room for improvement in terms of cost and services. Many of these e-based transactions are utilizing software products and systems where integrity would play a pivotal role. We have performance measures in Quality, Dependability, Safety, and Security that tell us the extent of efficiency and user satisfaction. But the improvement cannot be achieved by measurements alone. Integrity has to

be put into the products and systems to make them dependable, safe and secure to enhance our quality of life. The rapid evolution of technology, and its diverse adaptation for use when dealing with software products and systems, present a new dimension of challenge in addressing the integrity issue in general, and the standardization effort in particular. The need for integrity standards to support existing SC7 related standards, such as ISO/IEC 15288 and ISO/IEC 12207 is part of the standards harmonization process within the portfolio of SC7 standards product offerings.

Q2. Are integrity-related standards SC7's concern?

The need for assurance of system and software integrity arises from a variety of `risk dimensions' -- safety, security, dependability of service, etc. This has led to development of integrity-based standards by a variety of sector-specific standards groupings. While some variations exist in the concepts and techniques adopted across sectors, by and large integrity concepts and techniques are generic across these sectors. This is particularly obvious at the software level, but is largely the case at system level, too. Unnecessary variations lead to duplication of effort (and of errors) across sectors, and poses real problems for system suppliers who operate across sectors. Collaboration between SC7 and sector-specific standards groups is an obvious corollary of this conclusion, which is addressed at Q4 below.

The SC7 terms of references call for the standardization of processes, supporting tools and supporting technologies for the engineering of software products and systems. Integrity is the inherent property designed/built into the software products and systems to provide the capability of fault tolerance and failure mitigation for risk containment. In order to achieve this prime integrity objective, it is essential that rules, processes and activities related to integrity be established for guidance in the proper design/build, acquisition or support of the software products and systems. This represents the relevant engineering effort needed where applicable to meet planned project activities. Integrity is a well-sought attribute exemplified in a quality product that adds value to meet customer’s expectation. Hence integrity is a fundamental element within the SC7 standards framework.

Q3. How should SC7 address integrity concerns?

The processes/activities involved in integrity and its assurance are necessarily embedded within the overall system and software processes addressed by 12207 and 15288 -- figure 1 in 15026 makes that clear. To provide a usable framework for the compliance assurance needed on high-integrity applications, however, these assurance-related processes and activities need to be spelled out in much greater detail than 12207 or 15288 are meant to provide. Equally it is unreasonable to expect the spread of expertise needed to develop high-level standards such as 12207 and 15288 to deal competently with critical integrity issues.

The logical solution, therefore, is for SC7 to retain WG9 as the group responsible for integrity-related standards and issues, and to ensure appropriate coordination between WG9 and WG7, and any other

SC7 group dealing with relevant issues.

Q4. How should SC7/WG9 relate to other standards organizations?

The answer given to Q2 makes it clear that the generic approach to integrity and its assurance taken within SC7 must mesh effectively with the sector-specific concerns relating to safety, security, dependability, etc. In effect, standards defined in such sectors must either refer to or `tailor' the generic standards developed by SC7. To ensure that this can be done effectively, some form of liaison or collaboration between SC7 and sector groups is essential, both at the time of development of the generic standards and in any subsequent sector-specific reference to or tailoring of them. The Joint Working Group (JWG) with TC56/WG4 is one way to achieve collaboration with this specific sector.

There have been problems in the JWG arrangement, however. The need to constrain the JWG to meet at the plenary sessions of each parent organization has caused some concern. If the parties in the JWG are to maintain adequate integration with their parents organizations, and with relevant sibling working groups of either parent, this is an unavoidable constraint. The trend towards co-location of the alternate meetings of related WGs within SC7 was a complication in this context. Clearly it is more difficult, if not impossible, for WG9 to negotiate co-location with both the TC56 plenary and, say, SC7/WG7's alternate meeting, when the latter is appropriate. The fact that JWG projects were each “owned” by one and only one parent led to an obvious problem, where the dissolution of SC7/WG9 was suggested "because it had no program of work.” The JWG perceived the “WG9” program of work to be the completion of several projects owned by TC56, while the integrity issue had not been discussed with other sectors.

The argument is equally strong for collaborative relationships between SC7 and any other relevant sector-specific group. The arguments for continuing the JWG with TC56, in particular, are largely based on its history of collaboration. TC56 at its Kyoto meeting confirmed that the door to continued collaboration remains open; the review of the terms of reference of TC56's new WG4 confirmed that TC56/WG4 is the logical target for such collaboration.

However, to extend the JWG with TC56/WG4 to an N-way collaboration with other sector groupings is impractical. Finding the appropriate structural fit, agreeing a common form of working and meeting the procedural requirements of the multiple parent bodies are all obstacles that seem to guarantee failure.

The choice for SC7 therefore seems to be either to continue its existing collaboration with TC56, and seek looser liaison arrangements with other sector groupings, or to adopt an even-handed, liaison-based, relationship to all sector groupings with integrity interests.

This Study Group recommends the latter course of action -- adopt an even-handed, relationship to all

sector groupings with integrity interests on the basis of formal liaisons.

Q5. What form of Working Group is most effective?

An additional problem is identifiable with respect to convenorship of the JWG. While Dave Kiang has done an excellent job in meeting the expectations of both SC7 and TC56, having a single convenor for a JWG (who is "owned" by or owes allegiance to both) has also led to problems -- serving two masters is never easy!

The Study Group recommends that WG9 be continued as an SC7 Working Group; that the Joint Working Group relationship with TC56/WG4 be replaced by a formal liaison; and that a new Convenor for the reconstituted WG9 be appointed as soon as possible to begin developing and executing a new SC7-related program of work.

Q6. What new SC7 work items might be proposed in the area of systems integrity?

Depending on how integrity is defined and used as a prime requirement in standards application, Systems Integrity could cover the potential areas of business needs as identified in Q1, above. The scope and application of software products and systems should also be clarified. Unlike reliability and dependability, which are time-dependent quality characteristics, integrity is inherent and stable property of an entity. This is like controlling the amount of gold content in minting a coin to maintain its precise monetary value. The integrity of a business system demands accuracy and completeness of information for validation (audit) of business values and expectations. The integrity of a nuclear power plant maintains a level of energy output delivery without compromising regulated safety criteria. These are but few of the examples to show the diversity of systems integrity applications.

The term "system," defined in ISO/IEC 15288: System Life Cycle Processes, is very broad. It is taken directly from ISO 9000:2000: Quality Management Systems-Fundamentals and Vocabulary. Our focus here is on man-made systems, consisting of a combination of hardware, software, and human interactions in a set of application environments. The application environments should relate to IT domain within the scope of SC7. The new SC7 thrust is on Systems Integrity, which encompasses the current WG9 mandate on Software Integrity. In this context, there are several potential new work items (PNWI) that might be proposed:

1. Integrity Concepts and Applications
   - Describe integrity concepts for systems life cycle applications.

2. Integrity Requirements
   - Define integrity requirements and assurance criteria for engineering and support of software products and systems.

3. Integrity Design and Assurance Process/Activity Description
   - Describe integrity design and assurance processes/activities supporting the systems and software engineering life cycles.

4. Guidelines for Integrity Design and Assurance Process/Activity Applications
   - Provide guidance for implementation of integrity design and assurance processes/activities.

5. Guidelines for Designing Integrity into Products/Systems
   - Provide guidance for designing/building integrity into software products and systems.

6. Integrity Assessment Methods
   - Provide guidance on application of integrity assessment methods for assurance of software products and systems.

7. Guidelines for Selection and Use of Technologies to Achieve Integrity Objectives
   - Provide guidance for the selection and use of technologies, best practices and techniques to achieve systems integrity objectives.

8. Guidelines for Integrity Cost and Resource Requirements Estimation
   - Provide guidance for estimating cost and resource requirements related to integrity effort for project management.

9. Guidelines for Analysis and Interpretation of Integrity Assurance Data
   - Provide guidance for analysis and interpretation of integrity data.

It should be cautioned here that presenting such a set of comprehensive new work items might be viewed as overly enthusiastic. However, it is easier to start with a bigger picture than tackling the issue on a piece meal basis. A reconstituted WG9 should make a serious effort to plan, select, and prioritize an appropriate work program from these suggested PNWIs. WG9 must ensure that specific market needs of the proposed standards can be justified, and that the resources required to complete them in a timely fashion can be made available.

Many of the PNWIs identified here share similar concepts and application methods with other assurance science disciplines such as in Quality Assurance, as well as in Dependability, Safety and Reliability Engineering. The issue at hand is to differentiate Integrity from other assurance science requirements in the context of the SC7 standards framework. WG9 should maintain vigilance and be persistent to pursue the question regarding the benefit that Integrity standards could provide that existing published standards on Quality, Dependability, and Safety could not provide in similar application environments. It is essential to cross-reference similar work by other standards groups to avoid

duplication of effort. The intensity and extent of liaison and work collaboration with other Committees would come as the needs arise.

Q7. How do existing work items and proposed work items fit into the SC7 product Framework and related Business and Strategic Plans?

The SC7 Business and Strategic Plans are currently focussing on development of generic systems and software engineering standards encompassing systems life cycle processes and software life cycle processes. Systems Integrity fits well into the current SC7 standards framework.

The SC7 Functional Framework can be effectively used to categorize the set of potential integrity standards for possible development within SC7. This is presented in the following diagram. Relevant SC7 standards developed by WG9 and other WGs are also shown in the diagram for references.

General	TR 12182

	Process	**Product**	**Tools**	**Technologies**	**Resources**	**Data**
Principle Standards	15288, 12207	9126-01, PNWI-Integrity Concepts and Applications				
Element Standards	15288, 12207, PNWI-Integrity Design and Assurance Process/Activity Description	15026, PNWI-Integrity Requirements				
Guides & Supplements	PNWI-Guidelines for Integrity Design and Assurance Process/Activity Applications	PNWI-Guidelines for Designing Integrity into Products/ Systems	PNWI-Integrity Assessment Methods	PNWI-Guidelines for Selection and Use of Technologies to Achieve Integrity Objectives	PNWI-Guidelines for Integrity Cost and Resource Requirements Estimation	PNWI-Guidelines for Analysis and Interpretation of Integrity Data

PNWI-Proposed New Work Item
TR 12182, 15026: SC7/WG9 developed standards
15288, 12207, 9126-1: Other SC7/WGs developed standards

Q8. Is there a sufficiently well-defined SC7 program of work to support the continuation of WG9?

The observations described in Q1, Q2 and Q3 support the continuation of WG9 activities. A new mandate and terms of reference for the new WG9 should be defined. A business plan should be established to guide standards development in aid of project management. A product plan should be

developed to address the priority and scope of each PNWI to formalize the SC7 projects. Market needs for each of the PNWIs should be identified. The program of work and resource availability should be established. A Requirements Document for justification in launching each new project should be developed and approved, to validate project goals and objectives.

The Study Group further recommends that a time limit be set for the actions described above. Should no new work items be approved prior to the 2001 Plenary, WG9 should be dissolved at that time.