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

# ISO/IEC JTC1/SC7 /N3185

**2005-02-21**

| | |
|---|---|
| **Document Type** | Study Group Report |
| **Title** | Initial Report Of The Study Group System and Software Assurance Requirements |
| **Source** | Study Group Chair |
| **Project** | |
| **Status** | Final |
| **Reference** | Resolution 794 |
| **Action ID** | FYI or ACT |
| **Due Date** | |
| **Distribution** | AG |
| **No. of Pages** | 11 |
| **Note** | To be discussed at the Helsinki SC7 Plenary |

Address reply to: ISO/IEC JTC1/SC7 Secretariat
École de technologie supérieure – Département de génie électrique
1100 Notre Dame Ouest, Montréal, Québec Canada H3C 1K3
secretariat@jtc1-sc7.org

www.jtc1-sc7.org

To: SC7 Secretariat
From: Jim Moore
Date: 15 February 2005
Subject: SC7 Study Group on System and Software Assurance Requirements – First Report

At its May 2004 plenary meeting, SC7 approved resolution 794:

> JTC1/SC7 instructs its Secretariat to establish a Study Group to determine the derived system and software assurance requirements from ISO/IEC 15288, ISO/IEC 12207, and ISO/IEC 15026, and to recommend requirements for the development, modification, adoption, or reference of supporting standards.
>
> The Study Group shall be chaired by Mr. James Moore (IEEE-CS). Its membership will consist of: Alec Dorling (UK), Trevor King (UK), Paul Croll (USA). Additional members can be added until 2004-09-15. Nominations must be sent to the SC7 secretariat.
>
> The group will submit its report by 2005-02-15.

The group initially waited for NB nominations. At that time it was determined that additional participation would be desirable. A new call was issued. With one exception, national bodies did not provide any confirmation of their representatives in the study group. After waiting in vain for such confirmation, the chairman decided in mid-January to simply proceed with the personnel who had expressed interest:

- Tony Coletta
- Paul Croll
- Alec Dorling
- Cheryl Jones
- Trevor King
- Jim Moore (chair)
- Paul Rogoway
- Larry Wagoner
- David Wheeler

The mechanism for interaction was an archived email distribution list. There were no face-to-face meetings or telecoms.

In order to proceed with our work, the group had to make some assumptions about the environment of its work. The chair's notes from the Brisbane plenary include the following:

- ISO/IEC 12207 and ISO/IEC 15288 (or their eventual harmonized equivalents) will be umbrella documents for the software and system life cycle processes.
- The current project to revise 15026 is intended to accomplish several goals: retain the concept of "integrity level" from the existing standard; introduce the concept

of a rigorous "assurance argument"; explain the relationship to risk management; and embed the process implications of system and software assurance in the life cycle processes provided by the two standards mentioned previously.

From this viewpoint, the process aspects of 15026 become a "delta" on the existing processes of 12207 and 15288. The chair offered a study plan exploiting that relationship:

| | |
|---|---|
| 1. Determine the relationships among the existing documents. | For this purpose, we will consider:<br>ISO/IEC 12207:1995 with its two amendments<br>ISO/IEC 15288:2002<br>WD3 15026<br>We would develop "mappings" from the process needs of 15026 to the processes of 12207 and 15288. |
| 2. Determine if items are missing from 15026, or if items in 15026 should be decomposed or refactored for a better fit. | Of course, a complete study of this question is probably beyond our expertise and beyond the charge of our study group. We would study the results of the mappings to determine if they reveal obvious missing items, such as documents being used that were never prepared. We would use this determination to revise the results of Step 1. We would also submit the results to WG9 for its use in preparing the next draft of 15026. |
| 3. Determine if items are missing from 12207 and 15288. | The objective of this exercise is to see if the process needs of assurance are a good fit to the current processes of 15288 and 12207, or if those process needs commend revision of the processes or additions to the set of processes. |
| 4. Determine "gaps" in the treatment of system and software assurance. | With the completion of the previous steps we will have completed mappings of the process aspects of assurance onto the processes provided by SC7. Furthermore, we will have posited achievable improvements in those mappings. We now need to ask ourselves if the combination of the improved 15026, improved 15288, and improved 12207 provide an adequately detailed treatment of the process aspects of assurance. One way to consider this question is to compare our results with some external reference. By the time we reach this point, I anticipate that the US DoD will have released a study of assurance practices that we can use for comparison. |

| | |
|---|---|
| 5. Find existing standards or other references that can fill the identified gaps. Develop recommendations for "development, modification, adoption, or reference of supporting standards." | |

The plan was not completed during the available time. The result of step 1 is attached as a part of this initial report.

The chair anticipates that study will consider during the time leading up to the May 2005 plenary meeting of JTC 1/SC 7. Additional study results will be submitted as they become available.

# Mapping of ISO/IEC 15026 Activities onto ISO/IEC 12207 Processes

The following table maps the activities of ISO/IEC 15026, clause 6 into the processes of ISO/IEC 12207, Amendment 1, Annex F. Each single activity of 15026 is mapped to the lowest level process of 12207 in which it should be fully included. For some processes, a number in parentheses indicates the specific outcome to which the activity is mapped.

In 12207, there are separate primary life cycle processes for system and for software. In 15026, no such distinction is made for its activities. So, some 15026 activities map to both a system and a software process in 12207, depending on whether that activity is being applied software.

| **ISO/IEC 15026.3 Activity** Clause 6 | **ISO/IEC 12207 Process** Amd.1, Annex F | **Explanation / Justification** |
|---|---|---|
| 6.2.1.1 | F.1.1.1 (3)<br>F.3.1.5 (3, 4) | Initial customer requirements, critical or not (15026.3), are defined by the customer prior to selecting a supplier. *Note 1.* |
| 6.2.1.2 | F.1.2.2 (1) | This (15026.3) is a technical part of contract negotiation (12207 Amd.1). |
| 6.2.1.3 | F.1.3.2 (3) | To fully understand and analyze requirements, the domain properties (15026.3) must be understood. Without the Domain Engineering of F.3.7 (*Note 2)*, the only other mapping is to System Requirements Analysis (12207 Amd.1). |
| 6.2.1.4 | F.1.3.2 (5.3.2.2 Evaluate…) | Evaluation of domain properties (15026.3) would need to be repeated at planned times/phases. Evaluation activities are defined in 12207.0, but not in Amd.1. *Note 3.* |
| 6.2.1.5 | — | This (15026.3) is a compound activity and is dissected into four distinct activities following this entry to properly map them into 12207 Amd.1. *Note 4.* |
| 6.2.1.5 – A set of integrity levels shall be established by reference to integrity levels defined in the relevant specific standard(s) for the application domain or risk dimension(s) associated with the system. | • F.3.2 (1-5)<br>• 5.3.1.3 | • Although not mentioned in F.3.2 of Amd.1, 7.2 of 12207.0 includes standards as part of the infrastructure. This seems to include the selection and adoption of any applicable standards.<br>• Also in 12207.0, section 5.3.1.3 (which has no corresponding section in Amd.1) calls on the supplier to "select, tailor, and use those standards…that are appropriate…" |
| 6.2.1.5 – If no such standards exist, then a suitable set of integrity levels (conformant with the criteria set out in Clause 8), must either be created by the acquirer, or created by the supplier and approved by the acquirer. | F.3.1.5 (2) | Outcome (2) (12207 Amd.1) on strategies is appropriate, because this probably refers to mitigation strategies. The selection of processes associated with an integrity level is a form of mitigation strategy. |

# Mapping of ISO/IEC 15026 Activities onto ISO/IEC 12207 Processes

| **ISO/IEC 15026.3 Activity** Clause 6 | **ISO/IEC 12207 Process** Amd.1, Annex F | **Explanation / Justification** |
|---|---|---|
| 6.2.1.5 – A mapping from integrity requirements to integrity levels must either be created by the acquirer, or created by the supplier and approved by the acquirer. | ~~F.3.1.5 (4)~~<br>F.3.1.5 (2) | Assigning an integrity level to a risk (15026.3) is equivalent to assigning priority for resources (12207 Amd.1). |
| 6.2.1.5 – A mapping from integrity levels to appropriate life cycle processes must either be created by the acquirer, or created by the supplier and approved by the acquirer. | F.3.2 (1) | Section 7.2.1.1 of 12207.0 includes the words: ".. to meet the requirements of the process employing this process…" This closely corresponds to the requirement to map integrity levels to development processes (15025.3). |
| 6.2.2.1 | F.1.3.2 (1)<br>F.1.3.4 (1) | This activity (15026.3) maps well to the purpose and/or one outcome of system and/or software requirements analysis (12207 Amd.1). |
| 6.2.2.2 | F.1.3.2 (2)<br>F.1.3.4 (2) | This activity (15026.3) maps well to the purpose and/or one outcome of system and/or software requirements analysis (12207 Amd.1). |
| 6.2.2.3 | F.1.3.2 (6)<br>F.1.3.4 (4) | This activity (15026.3) maps well to the purpose and/or one outcome of system and/or software requirements analysis (12207 Amd.1). |
| 6.2.2.4 | F.1.3.2<br>F.1.3.4 | This activity (15026.3) maps well to the purpose and/or one outcome of system and/or software requirements analysis (12207 Amd.1). |
| 6.2.2.5 | F.1.3.2<br>F.1.3.4 | This activity (15026.3) maps well to the purpose and/or one outcome of system and/or software requirements analysis (12207 Amd.1). |
| 6.2.3.1 | F.3.1.5 (3, 4) | This activity (15026.3) does not map to any task or outcome of F.1.3.3 (5.3.3) in 12207 Amd.1, it happens after a design process. It is a risk analysis, intended for deriving more requirements. This might be another turn, iteration or recursion of a life cycle. *Note 5.* |
| 6.2.3.2 | F.1.3.2 (1) | The need to mitigate an internal threat (15026.3) is equivalent to a derived requirement (12207 Amd.1). |
| 6.2.3.3 | F.1.3.2<br>F.1.3.4 | Determining the integrity requirement of a mitigation function (15026.3) clearly belongs to a requirement-related process. The analytical aspect puts it in requirements analysis (12207 Amd.1). |
| 6.2.3.4 | F.1.3.3 (1)<br>F.1.3.5 (1) | This design activity (15026.3) addresses the requirements derived from the previous risk analysis. |
| 6.2.3.5 | F.1.3.3<br>F.1.3.5 | This (15026.3) is a design activity, but it has no analog among the existing design outcomes of F.1.3.3 or F.1.3.5 in 12207 Amd.1. |

Mapping of ISO/IEC 15026 Activities onto ISO/IEC 12207 Processes

| **ISO/IEC 15026.3 Activity** Clause 6 | **ISO/IEC 12207 Process** Amd.1, Annex F | **Explanation / Justification** |
|---|---|---|
| 6.2.3.6 | F.3.1.5 (3, 4) | The risk management process is applied in the midst of system architectural design and/or software design. |
| 6.2.3.7 | F.2.9 (3)<br>F.1.3.3 (3) | In 12207 Amd.1, F.2.9 (3) describes the need to train operators; and for F.1.3.3 (3), some system elements may be human. |
| 6.2.3.8 | F.1.1.1 (4) | The supplier (15026.3) may recurs into an acquisition process for some system components. The "acquisition strategy" of 12207 Amd.1 may be to use COTS. See 12207.0, section 5.1.1.6 (a). |
| 6.2.4.1 | F.1.3.6 (1) | The language attributes specified (15026.3) are a subset of a software unit's verification criteria (12207 Amd.1). |
| 6.2.5.1 | F.2.4 (3)<br>{F.2.3 (4)<br>F.2.6 (2)<br>F.2.7 (2)} | The specifications of mitigating functions (15026.3) are correctly treated as technical requirements. {Products and/or processes are also subject to QA reviews, Joint Reviews, and Audits in 12207 Amd.1.} |
| 6.2.5.2 | F.2.4 (3)<br>{F.2.3 (4)<br>F.2.6 (2)<br>F.2.7 (2)} | Integrity level (15026.3) is a new concept which must be verified (12207 Amd.1). {Products and/or processes are also subject to QA, Joint Reviews, and Audits in 12207 Amd.1.} |
| 6.2.5.3 | F.2.4 (3)<br>{F.2.3 (4)<br>F.2.6 (2)<br>F.2.7 (2)} | The specifications of mitigating functions (15026.3) are correctly treated as technical requirements (12207 Amd.1). Integrity level (15026.3) is a new concept against which several interim products must be verified (12207 Amd.1). {Products and/or processes are also subject to QA, Joint Reviews, and Audits, in 12207 Amd.1.} |
| 6.2.5.4 | F.2.4 (3)<br>{F.2.3 (4)<br>F.2.6 (2)<br>F.2.7 (2)} | The specifications of mitigating functions (15026.3) are correctly treated as technical requirements (12207 Amd.1). {Products and/or processes are also subject to QA, Joint Reviews, and Audits in 12207 Amd.1.} |
| 6.2.5.5 | F.2.4 (3)<br>{F.2.3 (4)<br>F.2.6 (2)<br>F.2.7 (2)} | Integrity level (15026.3) is a new concept against which several interim products must be verified (12207 Amd.1). {Products and/or processes are also subject to QA, Joint Reviews, and Audits in 12207 Amd.1.} |
| 6.2.6.1 | F.1.5 (4) | Testing in 12207 Amd.1 is augmented by adding the verification activities of 15026. The entire maintenance process is affected, but the other outcomes do not need explicit augmentation. |

Mapping of ISO/IEC 15026 Activities onto ISO/IEC 12207 Processes

| **ISO/IEC 15026.3 Activity** Clause 6 | **ISO/IEC 12207 Process** Amd.1, Annex F | **Explanation / Justification** |
|---|---|---|
| 6.2.6.2 | • F.1.5 (2)<br>• F.3.1.5 (4) | • An impact analysis identifies (12207 Amd.1) high integrity system elements (15026.3).<br>• A risk analysis (12207 Amd.1) identifies additional affected elements. If the integrity level of some element changes (15026.3), lower integrity elements that may affect it are re-examined, and higher level elements that may be affected by it are re-examined. |

**Note 1:** In activity 6.2.1.1 of 15026.3, the supplier should not be designated as the source of critical requirements. Critical requirements come either from the acquirer, or from negotiation and/or conversation between the acquirer and the supplier. Either change who specifies critical requirements or leave it open.

**Note 2:** Although 12207 contains a Domain Engineering Process, F.3.7, it is intended to be paired with the reuse process. The idea is to model the domain for more efficient reuse. If F.3.7 specified a more generic use for the domain engineering, the results could also be applied to the domain engineering required for 6.2.1.3.

**Note 3:** In activity 6.2.1.4 of 15026.3, it is not necessary to say this process gets repeated, because it is understood that all processes are continuous to the extend dictated by the selected life cycle model.

**Note 4:** Activity 6.2.1.5 of 15026.3 is a compound activity. It should be subdivided into its constituent activities, because the four distinct activities map to two different processes of IEEE 12207 Amd.1. The first and fourth activities map to F.3.2, while the second and third activities map to F.3.1.5.

**Note 5:** Process F.3.1.5 of 12207 Amd.1 seems to be directed to project risks and not product risks. Outcome 5, especially, includes checking risk status and the progress of treatment activities. This process should be written so it applies equally well to project and product risks. Process 6.2.3 of 15026.3 is inherently iterative in nature. The activity descriptions should be written so they can fit into any life cycle. At the same time, they should map to process F.3.1.5 Risk Management of 12207 Amd.1.

# Mapping of ISO/IEC 15026 Activities onto ISO/IEC 15288 Process Architecture

The following table maps the activities of ISO/IEC 15026, clause 6 into the system life cycle activities of ISO/IEC 15288. The number indicates the process (5.x.x), the outcomes paragraph of the process (usually 5.x.x.2), or the activities paragraph of the process (usually 5.x.x.3). The letter in parentheses, if there is one, is the specific outcome or activity.

| **ISO/IEC 15026 Activity**<br>Clause 6 | **ISO/IEC 15288 Process**<br>Clause 5 | **Explanation / Justification** |
|---|---|---|
| 6.2.1.1 | 5.2.2.3 (b)<br>5.4.6.2 (a, c)<br>5.4.6.3 (a-j) | Initial requirements, particularly critical requirements, should be part of the request for supply. The critical requirements are derived as part of a risk analysis by the acquirer. *Note 1.* |
| 6.2.1.2 | 5.2.2.2 (e)<br>5.2.2.3 (e)<br>5.2.3.2 (c)<br>5.2.3.3 (d) | This agreement activity of 15026.3 maps closely to the agreement activities of 15288.. |
| 6.2.1.3 | 5.5.2.2 (b, e) | The Stakeholder Requirements Definition Process does not explicitly call for defining domain properties, but it can be inferred and there is no other place for it. These domain properties (15026.3) become system constraints (15288) and will be used for justification or validation (15288). |
| 6.2.1.4 | 5.5.2.3 (l) | Evaluation of domain properties (15026.3) would need to be repeated at "key decision times in the life cycle." (15288) |
| 6.2.1.5 | — | This (15026.3) is a compound activity and is dissected into four distinct activities following this entry to properly map them into 15288. *Note 2.* |
| 6.2.1.5 – A set of integrity levels shall be established by reference to integrity levels defined in the relevant specific standard(s) for the application domain or risk dimension(s) associated with the system. | None | There is no section in 15288 that defines a process for finding and selecting a standard. *Note 3.* |

# Mapping of ISO/IEC 15026 Activities onto ISO/IEC 15288 Process Architecture

| **ISO/IEC 15026 Activity**<br>Clause 6 | **ISO/IEC 15288 Process**<br>Clause 5 | **Explanation / Justification** |
|---|---|---|
| 6.2.1.5 – If no such standards exist, then a suitable set of integrity levels (conformant with the criteria set out in Clause 8), must either be created by the acquirer, or created by the supplier and approved by the acquirer. | 5.4.6.3 (a) | Defining integrity levels is a part of risk management, but is not identified in the risk management process of 15288. |
| 6.2.1.5 – A mapping from integrity requirements to integrity levels must either be created by the acquirer, or created by the supplier and approved by the acquirer. | 5.4.6.3 (a) | Defining integrity levels against integrity requirements is a part of risk management, but is not identified in the risk management process of 15288. |
| 6.2.1.5 – A mapping from integrity levels to appropriate life cycle processes must either be created by the acquirer, or created by the supplier and approved by the acquirer. | 5.3.4.2 (b) | Mapping integrity levels to life cycle processes (15026.3) is a part of defining the policy for applying life cycle processes (15288). |
| 6.2.2.1 | 5.5.2.3 (f) | Direct and obvious mapping. |
| 6.2.2.2 | 5.5.2.3 (i, j) | Adequacy of mitigating functions (15026.3) is justified to stakeholders (15288). |
| 6.2.2.3 | 5.5.3.2 (c) | Mitigating functions are compared to the critical requirements (15026.3), just as an requirements are compared against stakeholder requirements (15288). |
| 6.2.2.4 | 5.5.3.3 (e) | Generalizing “safety integrity” from the note in 15288, these map directly. |
| 6.2.2.5 | 5.5.3.3 (e) | This and the previous activity of 15026.3 are nearly inseparable. |
| 6.2.3.1 | 5.4.6.2 (a, b)<br>5.4.6.3 (b, c, d) | Direct and obvious mapping. |
| 6.2.3.2 | 5.5.3.3 (e) | The 15026.3 activity describes deriving requirements; generalizing “safety integrity” from the note in 15288, these map directly. |

Mapping of ISO/IEC 15026 Activities onto ISO/IEC 15288 Process Architecture

| **ISO/IEC 15026 Activity** Clause 6 | **ISO/IEC 15288 Process** Clause 5 | **Explanation / Justification** |
|---|---|---|
| 6.2.3.3 | 5.5.3.2 (e) | Determining the integrity requirement of a mitigation function (15026.3) clearly belongs to a requirement-related process. The analytical aspect puts it in requirements analysis (15288). |
| 6.2.3.4 | 5.5.4.2 (a, b) | This design activity (15026.3) addresses the requirements derived from the previous risk analysis. |
| 6.2.3.5 | 5.5.4.3 (f) | Direct and obvious mapping |
| 6.2.3.6 | 5.4.6.2 (a, b, c)<br>5.4.6.3 (b-h) | The risk management process is applied in the midst of architectural design. |
| 6.2.3.7 | 5.5.4.3 (d)<br>5.5.5.3 (c(3)) | Direct and obvious mapping: if human operators are needed, develop training materials. |
| 6.2.3.8 | 5.2.2.2 (a-g) | The supplier (15026.3) may recurs into an acquisition process for some system components. The "strategy for the acquisition" of 15288 may be to use COTS. |
| 6.2.4.1 | 5.5.5.3 (c(2)) | Refers to 12207 Amd.1 for software processes. Does not specifically mention programming language or integrity level. |
| 6.2.5.1 | 5.5.7.2 (a-d) | The outcomes of the process in 15288 are written generically, but the activities target specific system descriptive products. The activities of 15026.3 are added to those of 15288. |
| 6.2.5.2 | 5.5.7.2 (a-d) | The outcomes of the process in 15288 are written generically, but the activities target specific system descriptive products. The activities of 15026.3 are added to those of 15288. |
| 6.2.5.3 | 5.5.7.2 (a-d) | The outcomes of the process in 15288 are written generically, but the activities target specific system descriptive products. The activities of 15026.3 are added to those of 15288. |
| 6.2.5.4 | 5.5.7.2 (a-d) | The outcomes of the process in 15288 are written generically, but the activities target specific system descriptive products. The activities of 15026.3 are added to those of 15288. |
| 6.2.5.5 | 5.5.7.2 (a-d) | The outcomes of the process in 15288 are written generically, but the activities target specific system descriptive products. The activities of 15026.3 are added to those of 15288. |
| 6.2.6.1 | 5.5.1.1 | Although this is the closest mapping, the purpose statement of 15288 is a poor fit for the 15026.3 process. *Note 4.* |

Mapping of ISO/IEC 15026 Activities onto ISO/IEC 15288 Process Architecture

| **ISO/IEC 15026 Activity** Clause 6 | **ISO/IEC 15288 Process** Clause 5 | **Explanation / Justification** |
|---|---|---|
| 6.2.6.2 | • 5.5.11<br>• 5.4.6 | • The 15026.3 activity is a form of impact analysis, but there is no impact analysis described in 15288. *Note 5.*<br>• A risk analysis (15288) identifies additional affected elements. If the integrity level of some element changes (15026.3), lower integrity elements that may affect it are re-examined, and higher level elements that may be affected by it are re-examined. |

**Note 1:** In activity 6.2.1.1 of 15026.3, the supplier should not be designated as the source of critical requirements. Critical requirements come either from the acquirer, or from negotiation and/or conversation between the acquirer and the supplier. Either change who specifies critical requirements or leave it open.

**Note 2:** Activity 6.2.1.5 of 15026.3 is a compound activity. It should be subdivided into its constituent activities, because the four distinct activities map to two different processes of 15288, and one of has no counterpart.

**Note 3:** Some activity of 5.3.4 System Life Cycle Processes in 15288 should address the selection of appropriate standards.

**Note 4:** In 15288, process 5.5.1.1, the words "to sustain the capability" in the first sentence betray the intent to limit maintenance to corrective and preventive maintenance. Although the second sentence lists adaptive and perfective maintenance, activities 1 and 2 only list corrective and preventive.

**Note 5:** In 15288, 5.5.11 Maintenance Process does not include any impact analysis – determining the effect of a change on the rest of the system. This may be because the process does not address changes to the design. Outcome (e) and the note in activity (f) imply that the need for design changes is external to this process. Then, preventive and corrective maintenance would proceed from this process to 5.5.4 Architectural Design Process. Adaptive and perfective maintenance would initiate as a new project with 5.2.2 Acquisition process or 5.5.2 Stakeholder Requirements Definition Process.