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

ISO/IEC JTC1/SC7 N4174

2008-12-05

Document Type	**NWIP**
Title	NWIP, Software and Systems Engineering – Process Assessment-Part 10 Safety Extensions
Source	WG10
Project	**NWIP**
Status	Final
References	
Action ID	ACT
Due Date	2009-05-18
Start Date	2008-12-08
Distribution	SC7 AG
Medium	PDF
No. of Pages	7
Note	2009-02-16: Balloting time has been extended to 2009-05-18 to enable electronic balloting.

Please vote using the ISO Electronic Balloting Facilities (Resolution 937)

Address reply to: ISO/IEC JTC1/SC7 Secretariat
École de technologie supérieure – Departement of Software and IT Engineering
1100 Notre Dame Ouest, Montréal, Québec Canada H3C 1K3
secretariat@jtc1-sc7.org

www.jtc1-sc7.org

New Work Item Proposal

November 2008

PROPOSAL FOR A NEW WORK ITEM

Date of presentation of proposal: 2008-12-05	WG10
Secretariat: Standards Council of Canada (SCC)	**ISO/IEC JTC 1 N** ISO/IEC JTC 1/SC 7 N 4174

A proposal for a new work item shall be submitted to the secretariat of the ISO/IEC joint technical committee concerned with a copy to the ISO Central Secretariat.

Presentation of the proposal

Title Software and Systems Engineering – Process Assessment- Part 10 Safety Extensions
Scope: The scope of this work is to develop a Safety Extension that defines additional processes and guidance to support the use of the exemplar process assessment models for systems and software (ISO/IEC 15504 Parts 5 and 6) when applied to the assessment of safety related systems developments in order to make consistent judgement regarding process capability and/or improvement priorities.

Purpose and justification:

The published ISO/IEC 15504 process assessment models for systems and software do not currently provide a sufficient basis for performing a process capability assessment of processes with respect to the development of complex safety critical systems.

The ISO/IEC 15504 standard does provide a general framework in which assessments can take place, however additional guidance and processes are needed to support the use of the existing process assessment models for systems and software when applied to safety related systems development in order to make consistent judgement regarding process capability or improvement priorities.

Developing safety-critical systems requires specialised processes, techniques, skills and experience. Process amplifications are needed in the area of safety management, safety engineering and the selection and qualification of software tools and libraries together with additional informative components concerning additional lifecycle verification activities related to the methods and techniques selected relevant to safety integrity levels adopted and tailoring guidance for users intending to use the Safety Extension as part of a process assessment.

The Safety Extension will be developed as a standalone document that can be used in conjunction with the Part 5 and/or Part 6 process assessment models by experienced assessors with minimal support from safety domain experts.

The Safety Extension will be developed independent of any specific safety standards that define safety principles, methods, techniques and work products, however elements of relevant safety standards will be able to be mapped to the Safety Extensions and the Safety Extensions will be extendable to be able to include specific safety standards requirements.

The Safety Extension will need to include a glossary of new terms such as hazard, FMEA, safety argument, safety incident etc. Such terms will be defined with reference to existing source materials with commonly accepted terms and usage.

The following provides an initial list of expected processes needed to be defined in the Safety Extension:

Safety Management – in order to ensure that safety activities are planned and performed.

Determining regulatory, legal and other requirements; establishing safety criteria (e.g. safety targets, hazards, risks) that reflect the level of acceptable safety: establishing safety organization and structure (e.g. roles, responsibilities, authorities, reporting lines); developing safety plan (including coverage of safety engineering and support activities for safety verification, validation and independent safety audits and evaluation and the appropriate selection of methods and techniques to be used); monitor safety incidents (using hazard analysis and risk assessment); manage and monitor agreements and requirements with suppliers.

Safety Engineering – in order to ensure safety is adequately addressed throughout all stages of the engineering lifecycle.

Identify potential hazards, perform hazard analysis and risk assessment (e.g using FMEA, FTA); define and maintain safety requirements, determine safety target for each safety requirements and allocate safety requirements to components; apply safety principles to ensure safety requirements are satisfied; ensure safety assurance activities are performed to validate safety case (using appropriate techniques); develop a safety case argument with supporting evidence; perform independent evaluations of product, safety processes and safety cases; safety measurement and analysis.

Selection and qualification of software tools and libraries – to ensure confidence in the software tools and libraries to be used to support safety critical systems development.
Initiation. Selection, qualification (development process, tool validation, operational suitability), certification, usage and guaranteeing of functional safety.

Market requirements demand the need for the Safety Extensions to support process assessments and to promote consistency with domain specific safety standards currently under development.

Programme of work

If the proposed new work item is approved, which of the following document(s) is (are) expected to be developed?

_X___ a single International Standard (Technical Report Type 2) **as Part 10 of ISO/IEC 15504**

____ more than one International Standard (expected number: .....)

____ a multi-part International Standard consisting of ..... parts

____ an amendment or amendments to the following International Standard(s) .....

____ a technical report , type .....

And which standard development track is recommended for the approved new work item?

_X___a. Default Timeframe

____b. Accelerated Timeframe

____c. Extended Timeframe

If the proposed new work item is approved, it shall be allocated to SC7/WG10.

Relevant documents to be considered

- ISO/IEC 15504-5:2003 Part 5: An exemplar (software life cycle) Process Assessment Model
- ISO/IEC 15504-7:2008 Part 6: An exemplar system life cycle Process Assessment Model
- ISO 61058 Functional safety of electrical/electronic/programmable electronic safety-related systems Parts 1 to 7
- ISO/IEC 15026 Systems and Software Assurance
- +SAFE V1.2 A Safety Extension to CMMI-DEV.V1.2 March 2007
- Relevant domain specific safety standards e.g. ISO 26262, IEC 62061, IEC 60880, DO 178B, Def-Stan 00-56, MIL-STD-882C, IEEE 1012

Co-operation and liaison:

- ISO TC22 SC3 (automotive functional safety)
- IEC TC 56 (functional safety)
- IEC TC 62 (Medical devices – software life cycle processes)

Preparatory work offered with target date(s)

Members from the UK, Finland and Italy intend to work jointly together to develop and submit an initial working draft following approval of the NWI prior to a first meeting

Support for this New Work Item Proposal has been offered by UK, Australia, Finland, Italy, Korea, Luxembourg, Germany, France, Japan, SPICE User Group

Project editors have been offered by Finland, Germany and Italy

Signature: A. Dorling, WG10 Convener

Will the service of a maintenance agency or registration authority be required? ..... No .....
- If yes, have you identified a potential candidate? .....
- If yes, indicate name .....

Are there any known requirements for coding? ..... No .....
-If yes, please specify on a separate page

Does the proposed standard concern known patented items? .. No .....
- If yes, please provide full information in an annex

Are there any known accessibility requirements and/or dependencies (see: http://www.jtc1access.org)? No
-If yes, please specify on a separate page
Are there any known requirements for cultural and linguistic adaptability?. No
-If yes, please specify on a separate page

Comments and recommendations of the JTC 1 or SC 7 Secretariat - attach a separate page as an annex, if necessary

This new work item is to be assigned to JTC 1/SC 7/WG10 and developed as ISO/IEC 15504 Part 10.

Voting on the proposal - Each P-member of the ISO/IEC joint technical committee has an obligation to vote within the time limits laid down (normally three months after the date of circulation).

Date of circulation:	**Closing date for voting:**	**Signature of Secretary:**
2008-12-08	2009-03-08	W. Suryn

NEW WORK ITEM PROPOSAL - PROJECT ACCEPTANCE CRITERIA		
Criterion	**Validity**	**Explanation**
A. Business Requirement		

A.1 Market Requirement	Essential __X_ Desirable ___ Supportive ___	The published exemplar process assessment models for systems and software do not currently provide a sufficient basis for performing a process capability assessment of processes with respect to the development of complex safety critical systems. The models do provide a general framework in which safety activities can take place, however additional guidance and processes are needed to make consistent judgement regarding process capability or improvement priorities. Developing safety-critical systems requires specialised processes, techniques, skills and experience. Process amplifications are needed in the area of safety management, safety engineering and the selection and qualification of software tools and libraries together with additional informative components concerning additional lifecycle verification activities related to the methods and techniques selected relevant to safety integrity levels adopted. The Safety Extension need to be developed as a standalone document that can be used in conjunction with Part 5 and/or Part 6 by experienced assessors with minimal support from safety domain experts. The Safety Extension needs to be developed independent of any specific safety standard and standards that defined safety principles, methods, techniques and work products, however elements of relevant safety standards need be able to be mapped to the Safety Extensions and the Safety Extensions need to be extendable for specific standards requirements.
A.2 Regulatory Context	Essential ___ Desirable ___ Supportive_X_ Not Relevant ----	Safety is a regulatory concern specifically in the domain of medical, nuclear, aerospace, defence, railways and automotive applications. Process assessment (especially when conducted according to conformity assessment regulations) will support customer requirements for conformance to safety standards.
B. Related Work		

B.1 Completion/Maintenance of current standards	Yes _ X __ No___	The Safety Extension will be developed as a new part of the existing published ISO/IEC 15504 standard. Market requirements demand that the Safety Extension is published before the publication of ISO/IEC 15504 in its revision cycle during 2010-2012, however the requirements for the revision of ISO/IEC 15504 will be planned to accommodate publication of the Safety Extensions in any new architecture.
B.2 Commitment to other organisation	Yes ___ No_ X __	
B.3 Other Source of standards	Yes __X_ No___	See '**Relevant documents to be considered'**
C. Technical Status		
C.1 Mature Technology	Yes _ X __ No___	A fast development cycle is envisaged as source materials are technology are mature. The publication will facilitate and promote consistency with domain safety standards such as ISO 26262 that are under parallel development work. It will also promote harmonisation between life cycle process standards within JTC1/SC7 and other sector and domain specific standardisation committees.
C.2 Prospective Technology	Yes ___ No_ X __	
C.3 Models/Tools	Yes _ X __ No -----	The Safety Extension will be developed as a standalone document that can be used in conjunction with ISO/IEC 15504 Part 5 and/or Part 6 by experienced assessors with minimal support from safety domain experts. ISO/IEC 15504-5,and 6 define exemplar Process Assessment Models for software and system life cycle processes respectively.
D. Conformity Assessment and Interoperability		
D.1 Conformity Assessment	Yes__ X _ No___	Safety is a regulatory concern specifically in the domain of medical, nuclear, aerospace, defence, railways and automotive applications. Process assessment (especially when conducted according to conformity assessment regulations) will partial conformance to safety standards.
D.2 Interoperability	Yes _ __ No__X_	

E. Adaptability to Culture, Language, Human Functioning and Context of Use		
E.1 Cultural and Linguistic	Yes_____ No___X____	
E.2 Adaptability to Human Functioning and Context of Use	Yes_____ No___X____	
F. Other Justification		