



ISO/IEC JTC 1/SC 27 **N 8129**

ISO/IEC JTC 1/SC 27/WG 3 **N 38129**

REPLACES: N

ISO/IEC JTC 1/SC 27

Information technology - Security techniques

Secretariat: DIN, Germany

DOC. TYPE: dispositions of comments

TITLE: Dispositions of comments on ISO/IEC 1st WD SC 27 N7902 -- Information technology -- Security techniques – Secure system engineering principles and techniques

SOURCE: 39th SC 27/WG 3 meeting

DATE: 2009-11-04

PROJECT: 1.27.79

STATUS: Output document of the editing session for 1st WD SC 27 N7902 held during the 39th SC 27/WG 3 meeting Redmond, US, 2nd – 6th November 2009. This document was available at the above-mentioned meeting. It is being circulated for information.

ACTION: FYI

DUE DATE:

DISTRIBUTION: P-, O-, and L- Members
W. Fumy, SC 27 Chairman, M. De Soete, SC 27 Vice Chair
E. Humphreys, K. Naemura, M. Bañón, M.C. Kang, K. Rannenber, WG-
Conveners

MEDIUM: Server

NO. OF PAGES: 1 + 28

Attachment 1 to SC 27 N8129

French comments on ISO/IEC 1st WD 29193

Date: 2009-10-28

Document: **SC 27 N7902**

1	2	(3)	4	5	(6)	(7)
NB ¹	Clause No./ Subclause No./ Annex (e.g. 3.1)	Paragraph/ Figure/Table/ Note (e.g. Table 1)	Type of com- ment ²	Comment (justification for change) by the NB	Proposed change by the NB	Resolution on each comment
[FR] 1.			ge	This draft should introduce the concept of security strategy. A security strategy encompasses all dimensions of security and safety in a consistent manner and enables to derive a set of security requirements from the security objectives. Many different strategies are generally possible, for instance, one specific strategy is to try to prevent all the attacks against the system, another is to detect and react to the security events before experiencing important losses. In fact, such a strategy determines the way to derive a set of specific security requirements from the list of security objectives.		Accepted – define the approach to achieve risk coverage - This chapter must not be redundant with risk assessment chapter but support risk management
[FR] 2.			ge	This technical report should include a section dealing with the topic of assurance. It is necessary to demonstrate that a so-called secure system holds its security claims, otherwise such a system cannot be trusted and is therefore useless. The demonstration is usually given by a security case which relies upon a set of evidences generated throughout the development lifecycle of the system		Accepted – see SC7 comments Engineering Process should demonstrate evidence of assurance whatever the configuration of the system or operating conditions (dynamic situations)
[FR] 3.	§4 Defining the security problem	§4.2.2 Safety, privacy, reliability, fault tolerance	te	The integration of safety and security should be emphasized and developed through a discussion about the similarities of and differences between security and safety concepts. That discussion should also address the distinction between safety and liveness properties. That point may seem to be too theoretical but it is necessary to express such kind of (mathematical) property when building a formal model (cf. 7.2).		Accepted in principle Integration of safety and security should be developed in the document See definitions in 15026-1 for safety Liveness is out of scope No extensive formal model should be discussed in this document

1 **MB** = Member body (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by **)

2 **Type of comment:** **ge** = general **te** = technical **ed** = editorial

NOTE Columns 1, 2, 4, 5 are compulsory.

Attachment 1 to SC 27 N8129

French comments on ISO/IEC 1st WD 29193

Date: 2009-10-28

Document: **SC 27 N7902**

1	2	(3)	4	5	(6)	(7)
NB ¹	Clause No./ Subclause No./ Annex (e.g. 3.1)	Paragraph/ Figure/Table/Note (e.g. Table 1)	Type of comment ²	Comment (justification for change) by the NB	Proposed change by the NB	Resolution on each comment
[FR] 4.	§5 Define the system security requirements		te	This section should give a precise definition of what is a security requirement because this concept is not so easy to use. Some authors make a distinction between functional and non-functional requirements (cf. “ a framework for security requirements engineering – Haley and al.”)		Accepted Add reference to “framework for security requirements engineering” Haley and “” Gibbs Explain some distinction between functional and non-functional requirements
[FR] 5.	§7 Design Techniques	§7.2 Formal methods	te	The term “formal method” is used today with many understandings and should be clarified. All formal methods are not equivalent; John Rushby from SRI International established a comparison among the major categories of formal methods according to the level of assurance provided. In consequence, the project team must carefully choose the kind of method to implement. That is why this draft should present and argue a set of criteria to help choosing an adequate method with regard to the system to be developed and to its security concerns.		Accepted

¹ **MB** = Member body (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by **)

² **Type of comment:** **ge** = general **te** = technical **ed** = editorial

NOTE Columns 1, 2, 4, 5 are compulsory.

Attachment 2 to SC 27 N8129

JP comments on ISO/IEC 1st WD 29193

Date: 2009-10-28

Document: **SC 27 N7902**

1	2	(3)	4	5	(6)	(7)
NB ¹	Clause No./ Subclause No./ Annex (e.g. 3.1)	Paragraph/ Figure/Table/ Note (e.g. Table 1)	Type of com- ment ²	Comment (justification for change) by the NB	Proposed change by the NB	Resolution on each comment
JP 1	2	4	te	French text is included as follows: (sûreté = état dans lequel il n'y a pas de risque inacceptable)	Change the text into English. Or, add the English equivalence.	Accepted Safety : state enabling no unacceptable risk
JP 2	2	3, 4, 5	te	The term "secured system" is used on top of "secure system." To make the clarity choose only single notation.	Replace all the "secured system" with "secure system."	Accepted
JP 3	Introduction Etc	2 nd paragraph	ge	"must" is used ten times in this draft. The ISO directives part 2 states in Annex H as follows: Do not use "must" as an alternative for "shall". (This will avoid any confusion between the requirements of a document and external statutory obligations.)	Replace all the "must" with "shall."	Accepted in principle In next version of this TR, only use "should"
JP 4	3.1 to 3.14 All the definitions		ge	Follow the ISO/IEC directives part 2 in defining the terms Example is: 3.1 AVAILABILITY degree to which the services of a system or component are operational and accessible when needed by their intended/authorized users NOTE: In the context of security, availability pertains to authorized services/actions only, and the need for availability generates the requirement that the system or component is able to resist or withstand attempts at unauthorized deletion or denial of service, regardless of whether those attempts are intentional or accidental. [Avizienis et al, IEEE Std 610.12-1990, NIST SP 800-27-Rev.A]		Accepted

¹ **MB** = Member body (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by **)

² **Type of comment:** **ge** = general **te** = technical **ed** = editorial

NOTE Columns 1, 2, 4, 5 are compulsory.

Attachment 2 to SC 27 N8129

JP comments on ISO/IEC 1st WD 29193

Date: 2009-10-28	Document: SC 27 N7902
------------------	------------------------------

1	2	(3)	4	5	(6)	(7)
NB ¹	Clause No./ Subclause No./ Annex (e.g. 3.1)	Paragraph/ Figure/Table/Note (e.g. Table 1)	Type of comment ²	Comment (justification for change) by the NB	Proposed change by the NB	Resolution on each comment
JP 5	3		te	If the editor wishes to define security in relation to the safety and quality, please add some of the following terms:	Add some of the definitions of the words mentioned in this comment column.	Accepted in principal Find ISO definition for these terms (JTC1/ SC27/ or SC7/ , ISO/)
				Anomaly(IEEE) anything observed in the documentation or operation of software that deviates from expectations based on previously verified software products or reference documents NOTE: See bug, defect, error, exception, fault		
				Bug(IEEE) fault in a program which causes the program to perform in an unintended or unanticipated manner NOTE: See anomaly, defect, error, exception, fault.		
				Correctness(IEEE) degree to which software is free from faults in its specification, design and coding NOTE: The degree to which software, documentation and other items meet specified requirements. The degree to which software, documentation and other items meet user needs and expectations, whether specified or not.		
				Crash(IEEE) sudden and complete failure of a computer system or component http://www.riceconsulting.com/public_pdf/ISTQBGlossaryVersion1dot3.pdf		

1 MB = Member body (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by **)

2 Type of comment: ge = general te = technical ed = editorial

NOTE Columns 1, 2, 4, 5 are compulsory.

Attachment 2 to SC 27 N8129

JP comments on ISO/IEC 1st WD 29193

Date: 2009-10-28	Document: SC 27 N7902
------------------	------------------------------

1	2	(3)	4	5	(6)	(7)
NB ¹	Clause No./ Subclause No./ Annex (e.g. 3.1)	Paragraph/ Figure/Table/Note (e.g. Table 1)	Type of comment ²	Comment (justification for change) by the NB	Proposed change by the NB	Resolution on each comment
				<p>Defect: flaw, non-conformance to requirements, in a component or system that can cause the component or system to fail to perform its required function, e.g. an incorrect statement or data definition. NOTE: A defect, if encountered during execution, may cause a failure of the component or system.</p>		
				<p>Error(ISO) discrepancy between a computed, observed, or measured value or condition and the true, specified, or theoretically correct value or condition NOTE: See anomaly, bug, defect, exception, fault.</p>		
				<p>Exception(IEEE) event that causes suspension of normal program execution NOTE: Types include addressing exception, data exception, operation exception, overflow exception, protection exception, underflow exception.</p>		
				<p>Failure (IEEE) Inability of a system or component to perform its required functions within specified performance requirements (ISTQB) Deviation of the component or system from its expected delivery, service or result</p>		Termination of the ability of a functional unit to perform a required function [61508-4]

¹ MB = Member body (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by **)

² Type of comment: ge = general te = technical ed = editorial

NOTE Columns 1, 2, 4, 5 are compulsory.

Attachment 2 to SC 27 N8129

JP comments on ISO/IEC 1st WD 29193

Date: 2009-10-28	Document: SC 27 N7902
------------------	------------------------------

1	2	(3)	4	5	(6)	(7)
NB ¹	Clause No./ Subclause No./ Annex (e.g. 3.1)	Paragraph/ Figure/Table/ Note (e.g. Table 1)	Type of com- ment ²	Comment (justification for change) by the NB	Proposed change by the NB	Resolution on each comment
				Fault incorrect step, process, or data definition in a computer program which causes the program to perform in an unintended or unanticipated manner		Abnormal condition that may cause in reduction, or loss, of the capability of the functional unit to perform a required function
JP 6	4.4.3		ed	The term “Unvolunteer” does not seem to be an English word.	Use English term.	Accepted, replace by Unintentional

Safety : freedom from unacceptable risk

¹ **MB** = Member body (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by **)

² **Type of comment:** **ge** = general **te** = technical **ed** = editorial

NOTE Columns 1, 2, 4, 5 are compulsory.

Attachment 3 to SC 27 N8129

ZA comments on ISO/IEC 1st WD 29193

Date: 2009-10-28	Document: SC 27 N7902
------------------	------------------------------

1	2	(3)	4	5	(6)	(7)
NB ¹	Clause No./ Subclause No./ Annex (e.g. 3.1)	Paragraph/ Figure/Table/ Note (e.g. Table 1)	Type of comment ²	Comment (justification for change) by the NB	Proposed change by the NB	Resolution on each comment

ZA 1	All	All	te	<p>ISO/IEC published the following standards in 2008:</p> <ul style="list-style-type: none"> - ISO/IEC 15288, Systems and software engineering – System life cycle processes - ISO/IEC 12207, Systems and software engineering – Software life cycle processes <p>From the introduction of ISO/IEC 15288:</p> <p>“This International Standard provides a common process framework covering the life cycle of man-made systems. This life cycle spans the conception of ideas through to the retirement of a system. It provides the processes for acquiring and supplying systems. In addition, this framework provides for the assessment and improvement of the life cycle processes.”</p> <p>From clause 1.1 Scope of ISO/IEC 15288:</p> <p>“It defines a set of processes and associated terminology. These processes can be applied at any level in the hierarchy of a system’s structure. Selected sets of these processes can be applied throughout the life cycle for managing and performing the stages of a system’s life cycle. This is accomplished through the involvement of all interested parties ...”</p> <p>From clause 1.4 Limitations of ISO/IEC 15288:</p> <p>“This International Standard does not prescribe a specific system life cycle model, development methodology, method, model or technique. This International Standard does not detail the life cycle processes in terms of methods or procedures required to meet the requirements and outcomes of a process.</p> <p>This International Standard does not detail documentation in terms of name, format, explicit content and recording media.</p> <p>This International Standard is not intended to be in conflict with any organization’s policies, procedures, and</p>	<p>The scope of WD 29193 states that the TR will provide guidance related to secure system design. This should be done within the context of ISO/IEC 15288 and using or adding to the processes defined in this International Standard.</p>	<p>Accepted</p> <p>Add a reference to ISO 15288 that provides requirements for processes to follow for system lifecycle (and ISO 12207 for software lifecycle processes)</p> <p>ISO 29193 should use terms and concepts used in ISO 15288</p>
------	-----	-----	----	---	---	---

1 MB = Member body (enter the ISO 3166 two-letter country code, e.g. CN for China) and comments from the ISO/IEC editing unit are identified by **)

2 Type of comment: ge = general te = technical ed = editorial

NOTE

Attachment 3 to SC 27 N8129

ZA comments on ISO/IEC 1st WD 29193

Date: 2009-10-28

Document: **SC 27 N7902**

1	2	(3)	4	5	(6)	(7)
NB ¹	Clause No./ Subclause No./ Annex (e.g. 3.1)	Paragraph/ Figure/Table/Note (e.g. Table 1)	Type of comment ²	Comment (justification for change) by the NB	Proposed change by the NB	Resolution on each comment
ZA 2 Refer ence	All	All	ge	<p>ISO/IEC is in the process of publishing ISO/IEC TR 24748-1, Systems and software engineering – Guide for life cycle management</p> <p>From the Introduction:</p> <p>“The Technical Report will also aid in identifying and planning use of life cycle processes described in ISO/IEC 15288 and ISO/IEC 12207 that will enable the project to be completed successfully, meeting its objectives/requirements for each stage and for the overall project.</p> <p>Besides the above, there is also increasing recognition of the importance of ensuring that all life cycle stages, and all aspects within each stage, are supported with thorough guidance to enable alignment with any process documents that may subsequently be created that focus on areas besides systems and software ...”</p>	ISO/IEC TR 24748-1 will provide helpful information relating to the ISO systems standards, life cycle stages etc.	Accepted Add a reference to 24748-1 that provides guidance on 15288 lifecycle management
ZA 3	All	All	te	<p>The title and scope of the WD clearly indicates that systems, not only software systems, will be addressed.</p> <p>Much of the current content focuses only on software without indicating a narrowing of scope for those parts.</p>	It is understood that this is just the 1 st WD, but care must be taken not to start focussing only on software systems.	Accepted
ZA 4	All	All	te	Consistency with ISO/IEC 15288 and 12207	Use the term “stage” in stead of “phase” when referring to life cycles.	Accepted

1 **MB** = Member body (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by **)

2 **Type of comment:** **ge** = general **te** = technical **ed** = editorial

NOTE Columns 1, 2, 4, 5 are compulsory.

Attachment 3 to SC 27 N8129

ZA comments on ISO/IEC 1st WD 29193

Date: 2009-10-28	Document: SC 27 N7902
------------------	------------------------------

1	2	(3)	4	5	(6)	(7)
NB ¹	Clause No./ Subclause No./ Annex (e.g. 3.1)	Paragraph/ Figure/Table/Note (e.g. Table 1)	Type of comment ²	Comment (justification for change) by the NB	Proposed change by the NB	Resolution on each comment
ZA 5	All	All	ge	<p>JTC 1 SC 7 (Systems and software engineering) is currently busy with the review of ISO/IEC 15026.</p> <p>The new edition consists of the following 4 parts:</p> <p>ISO/IEC TR 15026-1, <i>Systems and software engineering — Systems and software assurance – Part 1: Concepts and vocabulary</i> (currently in publication)</p> <p>ISO/IEC 15026-2, <i>Systems and software engineering — Systems and software assurance – Part 2: Assurance case</i> (4th CD)</p> <p>ISO/IEC 15026-3, <i>Systems and software engineering — Systems and software assurance – Part 3: System integrity levels</i> (2nd WD)</p> <p>ISO/IEC 15026-4, <i>Systems and software engineering — Systems and software assurance – Part 4: Assurance in the life cycle</i> (1st WD)</p>	<p>These documents and liaison with SC 7 WG 7 regarding 29193 may prove valuable for the general aspects relating to assurance.</p>	<p>Accepted</p> <p>Add a reference on 15026-1</p> <p>Add in design stage that people have assurance requirements to achieve, formalised following assurance case principles (ref. to 15026-2)</p>
ZA 6	All	All	ed	<p>Although not mandatory, using the bullets provided for unnumbered lists in the ISO template contributes to consistency in the document and between documents.</p>	<p>E.g. Replace · with – as provided by the template.</p> <p>Use the indentations as provided by the template for bullet lists.</p>	<p>Accepted</p>
ZA 7	Introduction	Par. 1	ed	<p>Unnecessary words.</p>	<p>Replace</p> <p>“guidance on the topic of secure system design”</p> <p>with</p> <p>“guidance on the secure system design”</p>	<p>Accepted</p>

¹ MB = Member body (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by **)

² Type of comment: ge = general te = technical ed = editorial

NOTE Columns 1, 2, 4, 5 are compulsory.

Attachment 3 to SC 27 N8129

ZA comments on ISO/IEC 1st WD 29193

Date: 2009-10-28	Document: SC 27 N7902
------------------	------------------------------

1	2	(3)	4	5	(6)	(7)
NB ¹	Clause No./ Subclause No./ Annex (e.g. 3.1)	Paragraph/ Figure/Table/Note (e.g. Table 1)	Type of comment ²	Comment (justification for change) by the NB	Proposed change by the NB	Resolution on each comment
ZA 8	Introduction	Par. 1	te	The Concise Oxford English dictionary defines <i>product</i> as an <i>article or substance manufactured or refined for sale</i> . This is also the common understanding of the term. Reading the document gave the impression that systems in general are addressed, not only those acquired as a product. Also, the Scope includes communication systems.	Replace “design of IT products” with “design of ICT systems”	Accepted ICT systems or products (define clearly the difference between system and product)
ZA 9	Introduction	Par. 1	te	The scope and rest of the document give the impression that the security of all ICT systems are addressed, not only those that provide security functionality.	Remove the words “with security functionality”	Accepted
ZA 10	Introduction	Par. 1	te	I consider “design” as part of the engineering of a system. Thus, it does not make sense to refer to the engineering aspects of system design, unless the idea was to contrast it to something such as the project management aspects. However, the project management aspects are also important in secure system design.	Remove the words “and places emphasis on the engineering aspects of this activity”	Accepted
ZA 11	Introduction	Par. 2	te	It is unclear what is meant by “engineering guidance” (as e.g. compared to just guidance).	Remove the word “engineering”, or replace “engineering guidance” with a elaboration of the term.	Accepted Suppress the whole sentence – rewrite introduction

1 **MB** = Member body (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by **)

2 **Type of comment:** **ge** = general **te** = technical **ed** = editorial

NOTE Columns 1, 2, 4, 5 are compulsory.

Attachment 3 to SC 27 N8129

ZA comments on ISO/IEC 1st WD 29193

Date: 2009-10-28	Document: SC 27 N7902
------------------	------------------------------

1	2	(3)	4	5	(6)	(7)
NB ¹	Clause No./ Subclause No./ Annex (e.g. 3.1)	Paragraph/ Figure/Table/Note (e.g. Table 1)	Type of comment ²	Comment (justification for change) by the NB	Proposed change by the NB	Resolution on each comment
ZA 12	Introduction	Par. 2	te	A system by definition is a “combination of interacting elements organized to achieve one or more stated purposes”. Some of these elements can be other systems or products. It is unclear why it is necessary to put emphasis on “secure composition”, since “secure system design” in itself also addresses it.		Accepted (same as comment ZA11)
ZA 13	Introduction	Par. 3	te	The word “catalogue” gives the impression of a comprehensive list of principles. This TR cannot give all principles, only a subset of the most well known.	Replace “A catalogue of” with “A list of possible” or “Examples of”	Accepted
ZA 14	1	Par. 1	ed	Unnecessary word.	Replace “security-specific engineering aspects” with “security-specific aspects”	Accepted
ZA 15	2	Par. 2 Bullet 1	te	Reliability is a field on its own, not within the scope of SC 27, nor this document. Although security contributes to reliability, and the other way around, this document cannot include design for reliability.	Remove “reliability”.	Accepted in principle (See below)

1 **MB** = Member body (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by **)

2 **Type of comment:** **ge** = general **te** = technical **ed** = editorial

NOTE Columns 1, 2, 4, 5 are compulsory.

Attachment 3 to SC 27 N8129

ZA comments on ISO/IEC 1st WD 29193

Date: 2009-10-28

Document: **SC 27 N7902**

1	2	(3)	4	5	(6)	(7)
NB ¹	Clause No./ Subclause No./ Annex (e.g. 3.1)	Paragraph/ Figure/Table/Note (e.g. Table 1)	Type of comment ²	Comment (justification for change) by the NB	Proposed change by the NB	Resolution on each comment
ZA 16	2	Par. 2 Bullet 1	te	In general, safety refers to the safety of humans. Safety is distinct from security. One definition of safety is “the expectation that a system does not, under defined conditions, lead to a state in which human life, health, property, or the environment is endangered” (ISO/IEC 15026:1998) Safety is not in the scope of SC 27, nor this document.	Remove “safety”.	Accepted in principle This document should include how safety principles can support security of system & vice-versa
ZA 17	2	Par. 2 bullet 1	te	Proposal for what a secure system is.	A secure system is a system of which the specified security requirements are assured within a specific context or environment.	Accepted And add a ref. to 25000
ZA 18	2	Par. 2 bullet 2	te	“Safe” means no harm or injury, not exposed to danger etc. A system that is secure is not necessarily safe, and the other way around. One can say that a secure system is a system which does not have or contribute unacceptable security risks. However, “unacceptable risks” will have to be explained.	Remove the bullet.	Accepted in principle Rewrite (Secure not necessarily safe, but contributes to safety and reliability)
ZA 19	All	All	te	As explained in a previous comment, safety is not in the scope of SC 27, nor this document.	Remove all references to “safe” and “safety” throughout the document, where it is used as if it is part of security or a synonym for security, or in a description of a secure system etc.	Accepted in principle Same ZA 18

¹ MB = Member body (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by **)

² Type of comment: ge = general te = technical ed = editorial

NOTE Columns 1, 2, 4, 5 are compulsory.

Attachment 3 to SC 27 N8129

ZA comments on ISO/IEC 1st WD 29193

Date: 2009-10-28	Document: SC 27 N7902
------------------	------------------------------

1	2	(3)	4	5	(6)	(7)
NB ¹	Clause No./ Subclause No./ Annex (e.g. 3.1)	Paragraph/ Figure/Table/Note (e.g. Table 1)	Type of comment ²	Comment (justification for change) by the NB	Proposed change by the NB	Resolution on each comment
ZA 20	2	Par. 3 bullet 1	te	<p>This bullet does not make sense.</p> <p>The system does not assure the functions. Other mechanisms and processes provide the necessary evidence so that one can be assured of the security claims made about the system.</p> <p>Also, assurance has to be provided regarding the security requirements of the system, not the functions.</p>	Remove the bullet or rephrase.	<p>Accepted</p> <p>Replace <i>assure</i> by <i>provide</i></p>
ZA 21	2	Par. 3 bullet 3	te	<p>The phrase “Use a development / operation process enabling to allocate security requirements” is unclear. Is the intent to convey the need that the requirements processes must make provision for allocating security requirements to both the system and the environment? But this also does not make sense, since the environment contributes to requirements and restrictions on the system. The system can not change the environment.</p>	Please clarify.	<p>Accepted.</p> <p>Rewrite - Replace “between the system and its environment” to “”</p>

¹ MB = Member body (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by **)

² Type of comment: ge = general te = technical ed = editorial

NOTE Columns 1, 2, 4, 5 are compulsory.

Attachment 3 to SC 27 N8129

ZA comments on ISO/IEC 1st WD 29193

Date: 2009-10-28	Document: SC 27 N7902
------------------	------------------------------

1	2	(3)	4	5	(6)	(7)
NB ¹	Clause No./ Subclause No./ Annex (e.g. 3.1)	Paragraph/ Figure/Table/Note (e.g. Table 1)	Type of comment ²	Comment (justification for change) by the NB	Proposed change by the NB	Resolution on each comment
ZA 22	2	Par. 3 bullet 3 sub bullet 1	te	<p>The question does not make sense. Requirements are stated for the system. A system is developed to work in a specific environment. The system does not place restrictions on the environment. If the environment already makes provision for security capabilities, this will be reflected in the requirements of the system.</p> <p>Where the environment can be considered a higher layer system, then obviously if the system-of-interest cannot fulfil the requirements placed on it, or provide assurance of the fulfilment of the requirements, this must be communicated back to the project team responsible for the higher layer. This requirement must then be allocated to other sub-systems.</p>	Please clarify.	Accepted in principle (see above)
ZA 23	2	Par. 3 bullet 3 sub bullet 2	te	<p>The phrase “strength of engineering principles and measures” does not make sense. Does it refer to the fact that different levels of assurance may place different requirements and restrictions on the development processes?</p> <p>Note: 15026-3 also refers to “integrity levels”.</p>	Please clarify.	Accepted Add a reference to the concept of assurance level / integrity level
ZA 24	2	p. 2 Par.1	ed	Spelling.	Replace “lifecycle” with “life cycle” throughout the document.	Accepted
ZA 25	2	p. 2 Par.1	ed	Unnecessary word. Stating the term “life cycle” on its own implies the complete life cycle.	Remove the word “whole” from the phrase “whole life cycle”.	Accepted Lifecycle from inception to retirement

1 **MB** = Member body (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by **)

2 **Type of comment:** **ge** = general **te** = technical **ed** = editorial

NOTE Columns 1, 2, 4, 5 are compulsory.

Attachment 3 to SC 27 N8129

ZA comments on ISO/IEC 1st WD 29193

Date: 2009-10-28

Document: **SC 27 N7902**

1	2	(3)	4	5	(6)	(7)
NB ¹	Clause No./ Subclause No./ Annex (e.g. 3.1)	Paragraph/ Figure/Table/Note (e.g. Table 1)	Type of comment ²	Comment (justification for change) by the NB	Proposed change by the NB	Resolution on each comment
ZA 26	2	p. 2 bullet 1	te	It is not only the system life cycle (assuming that the life cycle stages are implied) that must be considered. The life cycle processes must also be considered.	Replace “system life cycle” with “system life cycle stages and processes”	Accepted
ZA 27	2	p.2 bullet 1 sub bullet	te	It is assumed that “risk” refers to “security risk”. However, in a project, project risk is also addressed in the risk management process (ISO/IEC 16085).	Provide a clear explanation of which risk is being referred to.	Accepted
ZA 28	3	All	te	Most of the terms and definitions do not adhere to the ISO/IEC directives, part 2.	Adhere to the ISO/IEC Directives, part 2, annex D.	Accepted
ZA 29	3	All	te	The following standard supersedes IEEE 610.12-1990. ISO/IEC 24765:2009 Systems and software engineering vocabulary	References can be made to ISO/IEC 24765 instead of IEEE 610.12	Accepted
ZA 30	3	All	te	Many of the definitions refer only to software, whereas the term is applicable to systems in general, e.g. reliability (3.10)	Where applicable, terms must be defined for systems, not software only.	Accepted
ZA 31	3.3		te	COTS is not a term, but an abbreviation.	Create the necessary clause for abbreviations and move COTS there.	Accepted
ZA 32	3.14		ed	Clause 3.14 is a repetition of 3.13	Remove clause 3.14.	Accepted
ZA 33	4.1	Par. 1	te	Safety is not in the scope of this document.	Remove the word “safety”.	Accepted in principle Place below in the document relation between security and safety

¹ MB = Member body (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by **)

² Type of comment: ge = general te = technical ed = editorial

NOTE Columns 1, 2, 4, 5 are compulsory.

Attachment 3 to SC 27 N8129

ZA comments on ISO/IEC 1st WD 29193

Date: 2009-10-28

Document: **SC 27 N7902**

1	2	(3)	4	5	(6)	(7)
NB ¹	Clause No./ Subclause No./ Annex (e.g. 3.1)	Paragraph/ Figure/Table/ Note (e.g. Table 1)	Type of com- ment ²	Comment (justification for change) by the NB	Proposed change by the NB	Resolution on each comment
ZA 34	4.1	Par. 3	te	Not sure what is meant by "system attempt to user health"	Please clarify.	Accepted Replace " <i>attempt</i> " by " <i>cause damages</i> "
ZA 35	4.1	Par. 4	te	Paragraph does not make sense.	Please clarify.	Accepted - To reword
ZA 36	4.2.1	Par. 1	te	Incorrect reference to International Standard.	Replace "ISO 9126" with "ISO/IEC 9126".	Accepted
ZA 37	4.2.1	Par. 1	te	Which part of ISO/IEC 9126 are being referred to? Many of the parts have also been replaced by documents in the ISO/IEC 25000-series (SQuaRE).	Replace "ISO/IEC 9126" with the correct part or a reference to the applicable document in the ISO/IEC 25000 series.	Accepted
ZA 38	4.3	All	te	The stages, descriptions and concepts should adhere to ISO/IEC 15288, with guidance for ISO/IEC TR 24748-1. Using the example life cycle stages in these documents will also contribute to consistency.	Refer to ISO/IEC 15288 and ISO/IEC TR 24748-1.	Accepted
ZA 39	Bibliography		te	ISO/IEC 15288, 12207, 15026 are not referenced.	Add ISO/IEC 15288, 12207, TR 15026-1 to the Bibliography. Add references to ISO/IEC 15026-2, 15026-3, 15026-4 as "to be published."	Accepted
ZA 40	7.3.2	Example	ed	Incorrect syntax for an example.	Use EXAMPLE as provided for in the template.	Accepted
ZA 41	7.6	All	te	What is meant by "secure-system life cycle"? Is there a difference between the "secure-system" and the "system"?	Please clarify or replace "secure-system" with "system".	Accepted Reword

¹ **MB** = Member body (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by **)

² **Type of comment:** **ge** = general **te** = technical **ed** = editorial

NOTE Columns 1, 2, 4, 5 are compulsory.

Attachment 3 to SC 27 N8129

ZA comments on ISO/IEC 1st WD 29193

Date: 2009-10-28	Document: SC 27 N7902
------------------	------------------------------

1	2	(3)	4	5	(6)	(7)
NB ¹	Clause No./ Subclause No./ Annex (e.g. 3.1)	Paragraph/ Figure/Table/ Note (e.g. Table 1)	Type of com- ment ²	Comment (justification for change) by the NB	Proposed change by the NB	Resolution on each comment
ZA 42	7.6.1	p. 16, bullet 1	te	<p>“Using structured and compiled language” is definitely not a principle to secure the development process.</p> <p>Apart from this fact, other overriding factors will often dictate which language to use, e.g. business requirements, environment restrictions, organisational policies and practices.</p>	Remove this bullet.	<p>Accepted</p> <p>Replace by “whatever the language used, use secure good practices for this language (e.g. CERT Secure C, …)”</p>

¹ **MB** = Member body (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by **)

² **Type of comment:** **ge** = general **te** = technical **ed** = editorial

NOTE Columns 1, 2, 4, 5 are compulsory.

Attachment 4 to SC 27 N8129

UK comments on ISO/IEC 1st WD 29193

Date: 2009-10-28	Document: SC 27 N7902
------------------	------------------------------

1	2	(3)	4	5	(6)	(7)
NB ¹	Clause No./ Subclause No./ Annex (e.g. 3.1)	Paragraph/ Figure/Table/Note (e.g. Table 1)	Type of comment ²	Comment (justification for change) by the NB	Proposed change by the NB	Resolution on each comment
UK 1	1	3	Ed	The audience should include software engineers. Software engineers implement (at a low level) advice, guidance and instructions from architects and designers.	Replace second sentence by "The audience will include system architects, software engineers and designers."	Accepted Add software engineers in the audience
UK 2	2	Section 1 Bullet 2	Te	There are many ways to treat risk, such as a) accept b) transfer c) insure against d) mitigate. It would be good to explicitly state this rather than just stating 'unacceptable'. A frame work for discussing and treating these risks is needed (Maybe refer to ISO 27001?)	Replace by "A secured system is safe, that means, in its state, there is no unacceptable risk. NOTE - Risks can be: a) Accepted by a Senior responsible owner, b) Transferred to another entity c) Accepted and insured against; d) Mitigated by deployment of controls and countermeasures."	Accepted – rewrite risk management sub clauses and refer to ISO 13335 and 27005 about risk management Add a sentence about the fact that risk is a central notion in secure engineering and refer to ISO 21827
UK 3	2	Section 2 Bullet 1	Ed	The meaning of 'know the functions' is not clear.	Replace by "Understand the components, functions and architectures the responsible owner is required to assure".	Accepted (same than ZA 20 comment)
UK 4	2	Section 2 Bullet 2	Te	Does the system 'know' the environment, or are we referring to its controllers, administrators etc. Also, authorised users can be attackers.	Replace by "Understand the environment in which the system and its wider owners must assure specified functions. This must include Threats, Vulnerabilities and possible exploitation routes".	Accepted in principle Make clear that this paragraph must be preceded by a sentence : The project manager / developer must know : ... Suppress (including users & attackers)
UK 5	3	-	Te	Need to add definition of 'confidentiality'.	Add suitable definition from one of the existing sources used.	Accepted See ISO 27000 : property that information is not made available or disclosed to unauthorized individuals, entities, or processes (2.31)

¹ MB = Member body (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by **)

² Type of comment: ge = general te = technical ed = editorial

NOTE Columns 1, 2, 4, 5 are compulsory.

Attachment 4 to SC 27 N8129

UK comments on ISO/IEC 1st WD 29193

Date: 2009-10-28

Document: **SC 27 N7902**

1	2	(3)	4	5	(6)	(7)
NB ¹	Clause No./ Subclause No./ Annex (e.g. 3.1)	Paragraph/ Figure/Table/ Note (e.g. Table 1)	Type of com- ment ²	Comment (justification for change) by the NB	Proposed change by the NB	Resolution on each comment
UK 6	4.1	1	Ed	Unclear sentence structure and meaning.	Replace by "The properties of safety and security should be considered through the whole life of the systems development life cycle This should be treated in the same way as quality is treated in ISO9000 standards"	Accepted Replace " <i>defined</i> " by " <i>considered</i> "
UK 7	4.1	2	Te	The statement around '100 times' is unjustified. This is a relative statement which has immense variability.	Replace by "It is widely known that the correction of software defects costs significantly more the further along the development process you are. The ability to change design principles and mitigate against technical risks identified also diminishes the further along you are".	Accepted
UK 8	4.1.	3	Ed	This paragraph makes no sense.	Delete or reword.	Accepted See ZA 34 comment

¹ **MB** = Member body (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by **)

² **Type of comment:** **ge** = general **te** = technical **ed** = editorial

NOTE Columns 1, 2, 4, 5 are compulsory.

Attachment 4 to SC 27 N8129
UK comments on ISO/IEC 1st WD 29193

Date: 2009-10-28	Document: SC 27 N7902
------------------	------------------------------

1	2	(3)	4	5	(6)	(7)
NB ¹	Clause No./ Subclause No./ Annex (e.g. 3.1)	Paragraph/ Figure/Table/Note (e.g. Table 1)	Type of comment ²	Comment (justification for change) by the NB	Proposed change by the NB	Resolution on each comment
UK 9	4.1.	4	Ed	The sentence is very long and grammatically incorrect.	Replace by “Within the systems design lifecycle it is necessary to establish appropriate security policies, technical standards and standard operating procedures. Security systems design requirements should be incorporated in both functional and non-functional requirements as appropriate. These principles should be incorporated with the five system development phases 1) Initiation 2) Development/Acquisition 3) Implementation 4) Maintenance/Operation 5) Disposal. Each phase must include relevant security principles”.	Accepted in principle See ZA 35 Reword
UK 10	4.4.3	1	Ed	The scope of the TR is more than just software. It also deals with environmental, design and process issues.	Replace first sentence by “Sources of threats to software and system development fall into four main categories:”	Accepted Replace <i>software</i> by <i>system</i>
UK 11	4.4.3	Table	Te	This table is confusing. Is it listing threat sources or attackers? A threat is a ‘potential’ of an event, a ‘threat actor’ entity that may potentially launch an attack.	Perhaps the horizontal table title should read ‘Malicious’ / ‘Benign’ and vertically ‘Internal’ / ‘External’, but this is not clear.	Accepted in principle Reconsider the table / Add a title “main System threat categories”

¹ **MB** = Member body (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by **)

² **Type of comment:** **ge** = general **te** = technical **ed** = editorial

NOTE Columns 1, 2, 4, 5 are compulsory.

Attachment 4 to SC 27 N8129
UK comments on ISO/IEC 1st WD 29193

Date: 2009-10-28	Document: SC 27 N7902
------------------	------------------------------

1	2	(3)	4	5	(6)	(7)
NB ¹	Clause No./ Subclause No./ Annex (e.g. 3.1)	Paragraph/ Figure/Table/Note (e.g. Table 1)	Type of comment ²	Comment (justification for change) by the NB	Proposed change by the NB	Resolution on each comment
WG7 1			ge	<p>The draft is explicitly incomplete. It needs to take advantage of prior work in compiling principles, guidelines and techniques. In particular, it should use:</p> <p>ISO/IEC 15026-1 Systems and software engineering — Systems and software assurance — Part 1: Concepts and vocabulary (in publication)</p> <p>Redwine, Samuel T., Jr.</p> <ul style="list-style-type: none"> Towards an Organization for Software System Security Principles and Guidelines Version 1.0. IIIA Technical Paper 08-01. Institute for Infrastructure and Information Assurance, James Madison University, February 2008. Available at http://www.jmu.edu/iiia/webdocs/Reports/SwA_Principles_Organization-sm.pdf Software Assurance: A Curriculum Guide to the Common Body of Knowledge to Produce, Acquire, and Sustain Secure Software, version 1.2. US DHS, October 2007 https://buildsecurityin.us-cert.gov/daisy/bsi/940-BSI/version/default/part/AttachmentData/data/CurriculumGuideToTheCBK.pdf <p>Berg, Clifford J, High-Assurance Design: Architecting Secure and Reliable Enterprise Applications, Addison Wesley, 2006.</p>	<p>Other sources include:</p> <p>Karen Mercedes Goertzel (editor). on Software Security Assurance State-of-the-Art Report, Information Assurance Technology Analysis Center (IATAC), July 31, 2007 at http://iac.dtic.mil/iatac/download/security.pdf,</p> <p>Levin, T. E., Irvine, C. E., Benzel, T. V., Bhaskara, G., Clark, P. C., and Nguyen, T. D., Design Principles and Guidelines for Security, NPS-CS-08-001, Naval Postgraduate School, November 2007. http://cistr.nps.edu/downloads/nps_cs_05_010.pdf</p>	<p>Accepted</p> <p>Add a reference to ISO 15026-1</p>

¹ **MB** = Member body (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by **)

² **Type of comment:** **ge** = general **te** = technical **ed** = editorial

NOTE Columns 1, 2, 4, 5 are compulsory.

Attachment 4 to SC 27 N8129
UK comments on ISO/IEC 1st WD 29193

Date: 2009-10-28	Document: SC 27 N7902
------------------	------------------------------

1	2	(3)	4	5	(6)	(7)
NB ¹	Clause No./ Subclause No./ Annex (e.g. 3.1)	Paragraph/ Figure/Table/Note (e.g. Table 1)	Type of comment ²	Comment (justification for change) by the NB	Proposed change by the NB	Resolution on each comment
WG7 2			ge	The scope of the document and the quality characteristics and kinds of risks covered varies and the intended scope becomes unclear. The scope of computing and communications covered is unclear. Are embedded systems included? (They should be, but scope of SC27 should be considered.)		Accepted Complete the § scope
WG7 3	Title	Title	Te	The title used is inconsistent: is it “Secure system engineering principles and techniques” or “Secure system design principles and techniques”?	Change title to “Secure system design principles and techniques throughout as this seems more consistent with content. Secure system engineerg...” sounds too close to “Secure systems engineering” Or could use “System security engineering...” like the SSE-CMM	Accepted Title is “Secure System Engineering Principles and Techniques”

¹ **MB** = Member body (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by **)

² **Type of comment:** **ge** = general **te** = technical **ed** = editorial

NOTE Columns 1, 2, 4, 5 are compulsory.

Attachment 4 to SC 27 N8129
 UK comments on ISO/IEC 1st WD 29193

Date: 2009-10-28	Document: SC 27 N7902
------------------	------------------------------

1	2	(3)	4	5	(6)	(7)
NB ¹	Clause No./ Subclause No./ Annex (e.g. 3.1)	Paragraph/ Figure/Table/Note (e.g. Table 1)	Type of comment ²	Comment (justification for change) by the NB	Proposed change by the NB	Resolution on each comment
WG 7 4	3		te	Definitions of quality characteristics should be those in the ISO/IEC 25000 series. Add references to bibliography.	a) ISO/IEC 25000: 2005 Software engineering - Software product Quality Requirements and Evaluation (SQuaRE) – Guide to SQuaRE b) ISO/IEC CD 25010 Software engineering -- Software product Quality Requirements and Evaluation (SQuaRE) – Quality model c) ISO/IEC 25012: 2008 Software Engineering – Software product Quality Requirements and Evaluation (SQuaRE) - Data Quality Model d) ISO/IEC 25020:2007 Software engineering -- Software product Quality Requirements and Evaluation (SQuaRE) -- Measurement reference model and guide e) ISO/IEC 25030:2007 Software engineering -- Software product Quality Requirements and Evaluation (SQuaRE) -- Quality requirements f) ISO/IEC FCD 25040 Software engineering - Software product Quality model and guide – Requirements and Evaluation (SQuaRE) – Evaluation reference g) ISO/IEC 25051:2006 Software engineering -- Software product Quality Requirements and Evaluation (SQuaRE) -- Requirements for quality of Commercial Off-The-Shelf (COTS) software product and instructions for testing	Accepted in principle Add necessary definitions for Quality, Reliability , ... For examples : Failure termination of the ability of a product to perform a required function or its inability to perform within previously specified limits 4.21 fault incorrect step, process or data definition in a computer program requirements expression of a perceived need that something be accomplished or realized ...

¹ MB = Member body (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by MB)

² Type of comment: ge = general te = technical ed = editorial

NOTE Columns 1, 2, 4, 5 are compulsory.

Attachment 4 to SC 27 N8129
UK comments on ISO/IEC 1st WD 29193

Date: 2009-10-28	Document: SC 27 N7902
------------------	------------------------------

1	2	(3)	4	5	(6)	(7)
NB ¹	Clause No./ Subclause No./ Annex (e.g. 3.1)	Paragraph/ Figure/Table/Note (e.g. Table 1)	Type of comment ²	Comment (justification for change) by the NB	Proposed change by the NB	Resolution on each comment
WG7 5	3.12		ge	Need to maintain consistency with 25000 and other standards	Replace “property” with “characteristic”	Accepted Security properties / quality characteristic
WG7 6	3		ge	Refer to www.computer.org/sevocab for definitions (although latest 25000 might not be included)		Accepted in principle Refer to ISO/IEC 27000 for vocabulary
WG7 7	4.3 and elsewhere		te	The terminology and usage needs to be consistent with ISO/IEC 15288:2008 Systems engineering -- System life cycle processes and where appropriate ISO/IEC 12207 Information technology -- Software life cycle processes SC7 standards and technical reports use “stages” for the life cycle, not “phases”	Replace “phase” with “stage” throughout Also see ISO/IEC 24748-1, Guide for Life Cycle Management, in publication	Accepted See ZA – 4 Align with 15288 concepts
WG7 8	4.3		te	The terminology and usage needs to be consistent with ISO/IEC 15288:2008 Systems engineering -- System life cycle processes and where appropriate ISO/IEC 12207 Information technology -- Software life cycle processes Do not use 15288 process names for the stages of the life cycle (your “phases”)	Replace “Implementation” with “Production/Deployment” or something along those lines. Replace “Operation/Maintenance” with “Deployment/Support” or something similar Replace “Disposal” with “Retirement” or something similar	Accepted – Review the lifecycle in order it will be aligned on 15288 processes

¹ **MB** = Member body (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by **)

² **Type of comment:** **ge** = general **te** = technical **ed** = editorial

NOTE Columns 1, 2, 4, 5 are compulsory.

Attachment 4 to SC 27 N8129

UK comments on ISO/IEC 1st WD 29193

Date: 2009-10-28	Document: SC 27 N7902
------------------	------------------------------

1	2	(3)	4	5	(6)	(7)
NB ¹	Clause No./ Subclause No./ Annex (e.g. 3.1)	Paragraph/ Figure/Table/Note (e.g. Table 1)	Type of comment ²	Comment (justification for change) by the NB	Proposed change by the NB	Resolution on each comment
WG7 9	4.4		te	Risk analysis must address potential consequences – identifying them and conditions/paths to their occurrence as well as their value. Some introductory text is suggested; A reference forward to clause 5 is needed. Also consider ISO/IEC 16085:2006, Risk Management, as a reference	Ultimately, the concern is for adverse consequences or effects. Analysis shows a consequence will occur with associated timings and uncertainty; this will with an associated uncertainty correspond to or follow a dangerous condition or undesirable event possibly varying with their duration or timing. In turn, such a dangerous condition will with some associated uncertainty follow its initiating event that will occur with some timing and associated uncertainty and possibly end with or following a terminating (e.g. termination causing) event. Conditions can be preconditions for other conditions in sequences leading to a condition having a potential for or an actual adverse consequence. Fundamentally, risk analysis is performed to answer three questions: a) What can go wrong? b) When (or under what conditions) will this happen? c) What are the consequences?	Accepted in principle §4.4 will refer to a risk analysis standard (e.g. ISO 27005,) and not develop risk analysis, which is limited to the overall scope of this TR, but develop a method to identify how security objectives output from risk analysis are covered by the system and by assumptions on the environment This method will distinguish system development from product development
WG7 10	4.4		ge	In addition, while it is far from perfect, an Open Group Technical Standard could be worth looking at: Risk Taxonomy, ISBN: 1-931624-77-1, Document Number: C081, Published by The Open Group, January 2009.		Accepted Add a reference in bibliographic list

¹ **MB** = Member body (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by **)

² **Type of comment:** **ge** = general **te** = technical **ed** = editorial

NOTE Columns 1, 2, 4, 5 are compulsory.

Attachment 4 to SC 27 N8129
UK comments on ISO/IEC 1st WD 29193

Date: 2009-10-28	Document: SC 27 N7902
------------------	------------------------------

1	2	(3)	4	5	(6)	(7)
NB ¹	Clause No./ Subclause No./ Annex (e.g. 3.1)	Paragraph/ Figure/Table/ Note (e.g. Table 1)	Type of comment ²	Comment (justification for change) by the NB	Proposed change by the NB	Resolution on each comment
WG7 11	4.4.3		ge	A possible additional source for ideas is: Methods for the Identification of Emerging and Future Risks, European Network and Information Security Agency (ENISA), November 2007; www.enisa.europa.eu/doc/pdf/deliverables/EFR_Methods_Identification_200804.pdf .		Accepted Add a reference in bibliographic list
WG7 12	4.4.3		te	As safety is a concern, where threats includes what are termed "hazards" in the security community. A large body of knowledge and practice exists regarding their identification and engineering related to them. This large of non-malicious dangers must be covered in some manner even if only at a high level plus references.		Accepted Add references to safety standards : ISO 61508, ISO 15026-1,
WG7 13	4.4.3	table	te	Replace "unvolunteer" (sic) with "unintentional" as this is the complement to "intentional". However, do the authors really mean malicious and non-malicious? Note that many examples exist of intentional, non-malicious actions resulting in security violations.	Replace "Unvolunteer " with "Unintentional"	Accepted – see JP6
WG7 14	4.4.3	table	ed	Benign means kindly, not life-threatening, harmless, or favourable. None of these are appropriate meanings. Use "non-malicious"	Replace "benign" with "non-malicious"	Accepted -
WG7 15	4.4.3	table	te	A reference to Avizienis, Algirdas, Jean-Claude Laprie, Brian Randell, and Carl Landwehr, "Basic Concepts and Taxonomy of Dependable and Secure Computing," IEEE Transactions on Dependable and Secure Computing, vol. 1, no. 1, pp. 11-33, Jan.-Mar. 2004. Available at http://csdl.computer.org/dl/trans/tq/2004/01/q0011.pdf appears to occur elsewhere in the document. However, their work on dimensions relevant tables such as this one does not appear to be reflected here.		Accepted Add a reference in bibliographic references

¹ **MB** = Member body (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by **)

² **Type of comment:** **ge** = general **te** = technical **ed** = editorial

NOTE Columns 1, 2, 4, 5 are compulsory.

Attachment 4 to SC 27 N8129
UK comments on ISO/IEC 1st WD 29193

Date: 2009-10-28	Document: SC 27 N7902
------------------	------------------------------

1	2	(3)	4	5	(6)	(7)
NB ¹	Clause No./ Subclause No./ Annex (e.g. 3.1)	Paragraph/ Figure/Table/Note (e.g. Table 1)	Type of comment ²	Comment (justification for change) by the NB	Proposed change by the NB	Resolution on each comment
WG7 16	4.4.3	Paragraphs 2-8	te	Non-malicious threats/hazards are ignored. These dominate even software vulnerability introduction with more reflecting incompetence or being "mistakes" than deliberately malicious.	Add material on non-malicious dangers	Accepted Add non malicious threats (e.g; correctness issues leading to security concerns in a specific context)
WG7 17	4.4.3	Paragraph 1 and elsewhere.	te	The meaning of "threats to software" is unclear in that the relevant consequences are unclear. Restricting them to the integrity of the software is too small a scope. Despite its broadness including everything is the only realistic alternative.	Explain what "to software" means.	Accepted - Replace software by system in the whole paragraph
WG7 18	4.4.3	Paragraph 4	te	Bullets need to include not just test results but all evidence relevant in assuring the achievement of the claims or requirements regarding properties of interest occurs		Accepted Change test in verification Add building environment in the list
WG7 19	5		te	The division between clauses 4 and 5 is unclear, e.g. risk analysis and requirements is not made clear. Possibly risk analysis should be under or referenced in requirements. However, risk management is relevant throughout the lifecycle.	If the authors intend a problem vs. solution division, then divide/relocate the material to reflect this.	Accepted Add a § in §2 about the division between §4 and §5 Add a § about risk management Security objectives can become requirement issues Add a paragraph about the way to cover security objectives by security requirements allocation to the system
WG7 20	6		ge	See comment 1 particularly the first to sources mentioned.		Accepted - § to be completed
WG7 21	6		te	The sub-clauses do not appear to appropriately divide the subject. Whatever division is made, its logic needs to be explained.		Accepted - § to be completed

¹ **MB** = Member body (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by **)

² **Type of comment:** ge = general te = technical ed = editorial

NOTE Columns 1, 2, 4, 5 are compulsory.

Attachment 4 to SC 27 N8129
UK comments on ISO/IEC 1st WD 29193

Date: 2009-10-28	Document: SC 27 N7902
------------------	------------------------------

1	2	(3)	4	5	(6)	(7)
NB ¹	Clause No./ Subclause No./ Annex (e.g. 3.1)	Paragraph/ Figure/Table/ Note (e.g. Table 1)	Type of com- ment ²	Comment (justification for change) by the NB	Proposed change by the NB	Resolution on each comment
WG7 22	6.1		ed	"Urbanisation" is a non-obvious hard to ensure know what in analogy is relevant	Replace "Urbanisation" with clear term	Accepted - Replace "Urbanisation" by "Architecture"
WG7 23	7		ge	See comment 1 particularly the first to sources mentioned.		Accepted (See SC7 – 20)
WG7 24	10.2		ge	Template appears possibly too ambitious for both the inclusion in document of adequate coverage and meeting a reasonable deadline for producing of document.	One possible compromise would be to also have a short version and use it for many of the entries considered less fundamental or of lesser centrality or narrower usefulness.	Accepted – remove the 10.1 § Template Keep the list of principles as a checklist Describe each principle in two §

¹ **MB** = Member body (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by **)

² **Type of comment:** **ge** = general **te** = technical **ed** = editorial

NOTE Columns 1, 2, 4, 5 are compulsory.