Template for comments and secretariat observations

Date:2023-03-28	Document:	Project:

MB/ NC[1]	Line number	Clause/ Subclause	Paragraph/ Figure/Table	Type of comment[2]	Comments	Proposed change	Observations of the secretariat
**-001				Ge	The document has been reviewed by an ISO editor.	Please use the file named "Word with trackchanges", from ISO CS available on ISO Projects as a basis for any further drafting	
		Introduction		Ed	Fully document changes from 2019 version		Stephen to implement
**-002		2		Ed	ISO/IEC 10967-3:2006	This reference is not cited at all in the document. Please delete	Removed
**-003		2		Ed	ISO/IEC 10967-1:2012, Information technology — Language independent arithmetic — Part 1: Integer and floating point arithmetic ISO/IEC 10967-2:2001,	These references are not cited normatively. Please move to bibliography.	Removed
**-004		2		Ed	ISO/IEC/IEEE 60559	This is cited normatively, please remove reference from the bibliography (ref [30])	ISO/IEC/IEEE 60559 is cited in clause 2, and 6.4.
**-005		2		Ed	IEC 61508-1:2010, Functional safety of electrical/electronic/programmable electronic safety-related systems - Part 1: General requirements IEC 61508-3:2010, Functional safety of electrical/electronic/programmable electronic safety-related systems - Part 3: Software requirements ISO/IEC 27001:2019, Information technology—Security techniques—Information security management systems—Requirements	These references are not cited normatively. Please move to bibliography.	They are cited in clause 4.2.

1 **MB** = Member body / **NC** = National Committee (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

MB/ NC[1]	Line number	Clause/ Subclause	Paragraph/ Figure/Table	Type of comment[2]	Comments	Proposed change	Observations of the secretariat
					ISO/IEC 27002:2019, Information technology—Security techniques—Code of practice for information security controls		
**-006		2		Ed	IEC 61508-1:2010	This reference is cited without a date in the document so it must be without a date in Clause 2/bibliography.	Done.
**-007		3		Ed	, symbols and conventions	A symbols clauses is only allowed when it provides a list of the symbols used. Please delete or list all the symbols used in this document under 3.2.	Removed.
**-008		3.1		Ed	Other terms are defined where they appear in *italic* type.	This is not allowed. Please change to upright. The only thing that is allowed is using italics types for cross references within Clause 3 (this is only allowed within clause 3, and for cross-references to terms defined in clause 3). Please correct. This is an example or what is allowed by the DP2 EXAMPLE 3.1.2 **terminological entry** part of a terminological data collection which contains the *terminological data* (3.1.3) related to one *concept* (3.2.1)	This approach has been used in 24772 since first publication in 2010.
**-009		3.1		Ed	ISO/IEC 2382–1	This reference does not exist. Please correct. Also, a reference in the boilerplate text if	Done

1 **MB** = Member body / **NC** = National Committee (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

MB/ NC[1]	Line number	Clause/ Subclause	Paragraph/ Figure/Table	Type of comment[2]	Comments	Proposed change	Observations of the secretariat
						clause 3 is normative and must thus be listed in clause 2	
**-010		3.1.1		Ed	3.1Communication	Please correct subsequent numbering	Done.
**-011		3.1.2.5		Ed	3.1.2.5 static thread activation	Only terms that are used in the document shall be listed in the Terms and definitions clause. See ISO/IEC Directives, Part 2, 16.5.4. Please delete unused terms or cite in document.	Fixed.
**-012		3.1.2.6		Ed	3.1.2.6 dynamic thread activation	Only terms that are used in the document shall be listed in the Terms and definitions clause. See ISO/IEC Directives, Part 2, 16.5.4. Please delete unused terms or cite in document.	Fixed
**-013		3.1.2.7		Ed	3.1.2.7 thread abort	Only terms that are used in the document shall be listed in the Terms and definitions clause. See ISO/IEC Directives, Part 2, 16.5.4. Please delete unused terms or cite in document.	Fixed
**-014		3.1.2.8		Ed	3.1.2.8 termination-directing thread	Only terms that are used in the document shall be listed in the Terms and definitions clause. See ISO/IEC Directives, Part 2, 16.5.4. Please delete unused terms or cite in document.	Deleted the hyphen to make the term consistent with usage.
**-015		3.1.3.1		Ed	3.1.3.1 software quality	Only terms that are used in the document shall be listed in the Terms and definitions clause. See ISO/IEC Directives, Part 2, 16.5.4.	Delete.

1 **MB** = Member body / **NC** = National Committee (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

MB/ NC[1]	Line number	Clause/ Subclause	Paragraph/ Figure/Table	Type of comment[2]	Comments	Proposed change	Observations of the secretariat
						Please delete unused terms or cite in document.	
**-016		3.1.4.1		Ed	Note 1 to entry: IEC 61508–4[20]: defines a Hazard as a potential source of harm, where harm is physical injury or damage to the health of people either directly or indirectly as a result of damage to property or to the environment. Some derived standards, such as UK Defence Standard 00-56, broaden the definition of harm to include material and environmental damage (not just harm to people caused by property and environmental damage).	What is the purpose of this note to entry? The purpose of this seems to be to define the term "harm". Definitions are not given in notes to entry. Please delete and create an entry for "harm" with whatever definition that applies.	Agree in principle, change text of the definition to “potential source of harm where harm is material or environmental damage or physical injury or damage to the health of people” All notes in clause 3 removed and either integrated into each definition or placed with relevant text.
**-017		3.1.4.2		Ed	3.1.4.2 safety-critical software	Only terms that are used in the document shall be listed in the Terms and definitions clause. See ISO/IEC Directives, Part 2, 16.5.4. Please delete unused terms or cite in document.	Corrected spelling deviations.
**-018		3.1.5.2		Ed	The term *property* can mean *the presence or the absence of a specific feature, used singly or in combination*.	Definitions are not given in notes to entry. Please delete and create an entry for "property" with whatever definition that applies.	Moved to clause 4.1. Agree and removed all other notes to terms.

1 **MB** = Member body / **NC** = National Committee (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

Template for comments and secretariat observations

Date:2023-03-28	Document:	Project:

MB/ NC[1]	Line number	Clause/ Subclause	Paragraph/ Figure/Table	Type of comment[2]	Comments	Proposed change	Observations of the secretariat
CA-2-019		3.1.5.7		ed	The term “timing_failure” is wrongly underlined	Remove the underline from “timing failure”	Done
**-020		3.2		Ed	Symbols and conventions	Please delete.	Agree
**-021		3.2.1		Ed	the symbols given in ISO 80000–2 apply	Please move text elsewhere. Either cite ISO 80000-2 normatively or define every single used in the document.	Unnecessary. Removed.
**-022		3.2.2		Ed	Programming language tokens and syntactic tokens appear in courier font.	This can be added as a note after the first use courier.	Agree. Added in 5.2 item 17.
**-023		4.1		Ed	Because new vulnerabilities are always being discovered, it is anticipated that this document will be revised and new descriptions added.	Please delete speculative content	Reject. Not speculative but a statement of fact.
**-024		4.1		Ed	Parts	what does "part" refer to? a Clause? a Subclause? parts in the ISO 24772 series? Please clarify.	Agreed. Changed to add improve the explanation
PL-025		4.1 Purpose of this document	Last para	ge	We don't understand the point of randomly generated short names. The paragraph states that there is no particular order and the whole process of identifying security vulnerabilities is a never-ending process and new types of vulnerabilities may be found. This explains why there is no strict order but doesn't explain why names are random instead of shortcuts like NUL for null pointer dereference or BO for buffer overflow.		This was a choice made by the original development team to avoid collisions and arguments over abbreviations. Better explanation provided.

1 **MB** = Member body / **NC** = National Committee (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

Template for comments and secretariat observations

Date:2023-03-28	Document:	Project:

MB/ NC[1]	Line number	Clause/ Subclause	Paragraph/ Figure/Table	Type of comment[2]	Comments	Proposed change	Observations of the secretariat
**-026		4.2		Ed	ISO/IEC 27000 series standards	This is not a series of standards.	ISO/IEC/JTC 1/SC 27 calls them a series of standards. Changed to "family of standards"
**-027		4.2		Ed	27000	Please cite in the bibliography	27000 is cited normally in clause 2.
JP1-028		4.2	item 8	ed	Clause 5.4 does not exist.		Agreed. Changed to 5.2
**-029		4.3		Ed	Parts	Please clarify	Further explanation added. ISO defines Parts. 24772-1 is this Part. 24772-2 is the ADA Part, etc.
**-030		4.3		Ed	*Vulnerability Issues,*	Please do not provide titles in the body text. Please delete throughout document.	Reject. The document is designed to create clarity for the reader. The complete name of the clause, including the 3 letter code is always used in a reference. This is particularly important as clause numbers have historically changed between editions.
**-031		4.3		Ed	Clause 5	ISO documents only use "subclause + X.X" at the beginning of a sentence. Otherwise the word "subclause" is never used when giving a subclause number. Clause is always used when expressing first-level clauses.	Updated.

1 **MB** = Member body / **NC** = National Committee (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

Template for comments and secretariat observations

Date:2023-03-28	Document:	Project:

MB/ NC[1]	Line number	Clause/ Subclause	Paragraph/ Figure/Table	Type of comment[2]	Comments	Proposed change	Observations of the secretariat
CA-3-032		4.3	5	te	Not all parts will be technical reports in the future.	Change reference to “Technical Reports” to “International Standards or technical Reports”	Agreed, but qualify with (Parts) for clarity as Parts is used throughout the document.
JP2-033		4.3	paragraph 2	ed	Clause (Subclause) 5.4 does not exist (two occurrences).		Agreed. Changed to 5.2.
JP3-034		4.3	paragraph 3	ed	Is it appropriate to call other parts of 24772 “Technical Reports”?		Agreed. Change to Standards or Technical Reports and TR removed in references.
**-035		5.1.1		Ed	*Predictable execution* is a property of a program such that all possible executions have results that can be predicted from examination of the source code.	Definitions are given in Clause 3 only.	Agreed. Put in 3.4.1
CA-5-036		5.1.2.1		te	The use of “semantics” in “Sometimes the semantics of new or complex features . . .” is confusing.	Sometimes the full implications and the interactions of new or complex features are not completely known …	Accepted.
CA-4-037		5.1.2.1	1	Ed	Change the dash “-“ in the sentence with a comma.		Accepted.
**-038		5.1.3.2		Ed	needs to	Please avoid using verbal forms that are not defined in the ISO/IEC Directives, Part 2, 2021, Clause 7. In the English language, the words “shall”, “must” and “need to” are often used interchangeably. The subtle differences in	Accepted. Changed to “should” This document provides avoidance mechanisms that programmers should consider using. It does not contain requirements.

1 **MB** = Member body / **NC** = National Committee (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

MB/ NC[1]	Line number	Clause/ Subclause	Paragraph/ Figure/Table	Type of comment[2]	Comments	Proposed change	Observations of the secretariat
						meaning are not easily translated into other languages when ISO documents are used around the world. To ensure that a document is understood and applied correctly, use “shall” to express requirements of the document and “must” to express constraints or obligations defined outside the document, and which are given for the information of the user. Avoid substituting either of these terms with “need(s) to”, even if this seems logical in English. Revise a sentence that uses “need(s) to” to avoid confusion and misapplication of the text. Please correct throughout the document.	
**-039		5.2		Ed	Primary avoidance mechanisms	In the table, second column: These are recommendations, however, verbs are in the imperative. In ISO deliverables, verbs in the imperative express requirements. Please correct by, e.g. adding "should", e.g. "should validate"...	Text was added to 4.2 to clarify that the imperative forms of the avoidance are not requirements imposed by this standard. In addition, the column title made clear that “Software developers can:” followed by choices of actions
CA-6-040		5.2	17	Te	Table item 17 does not clearly differentiate code from the explanation of the code	Beware of short-circuiting behaviour when expressions with side effects are used on the right side of a short-circuited Boolean expression, such that the left-hand expression evaluates to `false`,	Agreed. Text replaced.

1 **MB** = Member body / **NC** = National Committee (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

MB/ NC[1]	Line number	Clause/ Subclause	Paragraph/ Figure/Table	Type of comment[2]	Comments	Proposed change	Observations of the secretariat
						then the right-hand expression, including function calls with side effects, will not be evaluated.	
**-041		6.1		Ed	this Part	Self-reference is done using "this document".	Accept.
**-042		6.1		Ed	standard	International Standard?	Disagree. Used "language standard. Some are not international standards.
**-043		6.2.2		Ed	Cross reference	"Cross-referencing" concerns references within this document. Please rename to "references" instead. Please correct the title to all 6.x.2 subclauses	Changed "cross reference" to "Related coding guidelines"
**-044		6.2.3		Ed	It is desirable	If the purpose is to express a recommendations, please use "should"	Agreed. "Should" used.
**-045		6.2.5		Ed	Avoiding the vulnerability or mitigating its effects	In ISO deliverables, verbs in the imperative express requirements. The purpose of this subclause seems to be to provide users with possibilities. Using requirements here does not seem adapted. Please correct all the verbal forms uses within Clause 6 and ensure that verbal forms are used correctly.	Text was added to 4.2 to clarify that the imperative forms of the avoidance are not requirements imposed by this standard. In addition, the text is clear that "Software developers can:" followed by choices of actions
CA-7-046		6.3.1		Te	The term "endianness" and the phrase (see below) is incomplete. Suggest improved text.	Mistakes can be made as to what bits are to be accessed because of the *endianness* of the processor (whether the highest order bit is called bit 0 or bit n) or because of miscalculations.	Accept.
**-047		6.3.2		Ed	Hogaboom, Richard, *A Generic API Bit Manipulation in C*Reference [17]	References to books shall not be spelled out in the body ISO deliverables (only in the	Replaced with an in-line reference in 6.3.3.

1 **MB** = Member body / **NC** = National Committee (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

MB/ NC[1]	Line number	Clause/ Subclause	Paragraph/ Figure/Table	Type of comment[2]	Comments	Proposed change	Observations of the secretariat
						bibliography), please use Reference + callout. Please correct throughout the document.	
**-048		6.3.3		Ed	must	If the purpose is to express a requirement of the document, please use "shall" instead. Please correct all the relevant occurrences of "must" in the document.	Agreed. Changed to "is a must".
**-049		6.3.3		Ed	must	"Must" is only used to express external requirements. If the purpose is to express a requirement of the document, please use "shall" instead. Please correct throughout the document.	Agreed. Change Knowledge of the storage and ordering of the bits is a must when doing bit-wise operations across multiple words as bytes may be stored in big-endian or little-endian format.d wording to
CA-8-050		6.3.3	Para 3 Sentence 1	te	The phrase "The kind of storage can cause problems when interfacing with external devices that number the bits in opposite order." does not explain the issue. . . Suggest improved wording.	Replace with "Storage organization can cause problems when interfacing with external devices that number the bits in opposite order."	Agreed. Changed.
CA-9-051		6.3.3	Para 3 sentence 2		The term "external constructs" is confusing. Devices interface with external data sources or data syncs.	Replace "external constructs" with "data sources or sinks"	Agreed in principal. Text clarified.
**-052		6.3.5		Ed	Software developers can avoid the vulnerability or mitigate its ill effects in the following ways:	See comment in 6.2.5. Please use "by"+ verb+ing as in 6.2.5. Please correct all the 6.X.5 subclauses.	General style applied throughout the document, addressing the comment. The recommendations are worded in the imperative so that organizations can use

Commented [GC1]: If the purpose is to express a requirement of the document, please use "shall" instead. Please correct all the relevant occurrences of "must" in the document.

1 **MB** = Member body / **NC** = National Committee (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

MB/ NC[1]	Line number	Clause/ Subclause	Paragraph/ Figure/Table	Type of comment[2]	Comments	Proposed change	Observations of the secretariat
							directly in their own coding guidelines.
**-053		6.4.3		Ed	min and max	Should this be written in courier?	No. References to the functions deleted and wording cleaned up.
**-054		6.4.3		Ed	your	ISO standards do not use second person pronouns. Please correct throughout document	Corrected to "the target" (system) Steve – check for all occurrences of "your"
CA-10-055		6.4.5	Bullet 5		The first sentence of Bullet 5 is a single avoidance mechanism. The second one is another avoidance mechanism.	Make "use library functions with known numerical characteristics" bullet 5. Make the rest of that bullet a new bullet.	Agreed fixed.
**-056		6.4.6		Ed	Providinge	In ISO deliverables, verbs in the imperative are used to express requirements. Please correct if the intent is not to express a requirement of this document.	Resolved by uniform new wording. Changed elsewhere where applicable.
**-057		6.6.5		Ed	you	ISO deliverables do not use second person pronouns. Please correct throughout document.	Replaced with alternate wording throughout document.
**-058		6.8.4		Ed	Footnote 1	In ISO deliverables, numbered footnotes are only used in two cases: - to indicate the publication stage of another ISO publication - to add a disclaimer when citing a trademark or trade name.	Removed.

1 **MB** = Member body / **NC** = National Committee (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

MB/ NC[1]	Line number	Clause/ Subclause	Paragraph/ Figure/Table	Type of comment[2]	Comments	Proposed change	Observations of the secretariat
						Lettered footnotes are only used in the context of figures and tables. Move this content outside the footnote and move to a NOTE. Please correct all the footnotes in the document or the document submission might be rejected at the FDIS stage.	
CA-11-059		6.11.4	Bullet 2	Te	The clause addresses the conversion of function pointers to data pointers, but does not address the other scenario where data pointers can be converted to function pointers.	Change bullet 2 to say - Pointers to functions can be converted to or from pointers to data.	Changed.
**-060		6.14.1		Ed	A dangling reference is a reference to an object whose lifetime has ended due to explicit deallocation or the stack frame in which the object resided has been freed due to exiting the dynamic scope	Definitions to terms are exclusively given in Clause 3. Please delete from here and add to Clause 3.	Tighter correspondence between clause 6.14.1 and the definition in clause 3.
**-061		6.14.5		Ed	Footnote 2	Please move content to NOTE: see comment to footnote 1. Please correct all the footnotes in the document.	Fixed. Material moved to 6.14.1.
JP4-062		6.15.1	footnote 3	ed	The phrase “Edition 1 of this International technical report” looks inappropriate.		Footnote removed
JP5-063		6.16.1	footnote 4	ed	The phrase “Edition 1 of this International technical report” looks inappropriate.		Footnote removed

1 **MB** = Member body / **NC** = National Committee (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

Template for comments and secretariat observations

Date:2023-03-28	Document:	Project:

MB/ NC[1]	Line number	Clause/ Subclause	Paragraph/ Figure/Table	Type of comment[2]	Comments	Proposed change	Observations of the secretariat
CA-12-064		6.17.1.	Para 2	Te	The advice provided in this bullet is not substantiated in 6.17.1.	Add to the end of 6.17.1 para 2 "Typing errors can lead to unintended bindings. The lack of a language requirement for explicit declarations of names amplifies the problem."	Accepted with minor changes.
CA-13-065		6.22.3	Para 2 and 3	Te	Para 2 and 3 should be one continuous paragraph. Para 3 expands the topic introduced in para 2.	Combine 6.22.3 paragraphs 2 and 3.	Corrected
CA-14-066		6.22.5	Bullet 7	Te	The bullet says to "Consider initializing each object at declaration …"		No change.
**-067		6.23.1		Ed	*Developer beliefs about binary operator precedence*	Please clarify, is this a reference or a subclause?	Bibliography entry added
**-068		6.23.5		Ed	24 Side effects and order of evaluation of operands [SAM]	When referencing a clause or subclause in the text, please only provide (sub)clause number, do not provide clause or subclause title. Please delete throughout document.	Reject. The title and three letter coding are crucial to understanding the document.
CA-15-069		6.25.1	Para 1, 4th sentence	Te	The sentence currently mentions the C programming language in the example of the flaw of mistyping equality (==) by assignment (=). This should be generalized to the issue, and not the programming language.	Replace the 4th sentence with "A common example arises in languages that use "==" for equality and "=" for assignment and allow assignments as expressions: the use of = in a Boolean expression where the programmer intended to perform an equality test using ==". Then remove all references to "C" in 6.25.1 and 6.25.3.	Accept. Also removed pejorative language about programmers.

1 **MB** = Member body / **NC** = National Committee (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

MB/ NC[1]	Line number	Clause/ Subclause	Paragraph/ Figure/Table	Type of comment[2]	Comments	Proposed change	Observations of the secretariat
**-070		6.26.3		Ed	it is essential that	This reads as a requirement of the document. Please clarify intention. if the intention is to express a requirement of the document please use "shall" instead. Otherwise please use "should" to express a recommendation or "must" to express an external requirement.	Reformulated as Therefore, it is important to understand and document why dead code is present
**-071		6.26.3		Ed	Dead code is code that exists in an application, but which can never be executed, either because there is no call path to the code (for example, a function that is never called) or because the execution path to the code is semantically infeasible	Definitions from the documents are given in Clause 3. Please correct	Reformulated to remove the difficulty.
**-072		6.26.3		Ed	— Deactivated code – Executable object code (or data) which by design is either (a) not intended to be executed (code) or used (data), for example, a part of a previously developed software component, or (b) is only executed (code) or used (data) in certain configurations of the target computer environment, for example, code that is enabled by a hardware pin selection or software programmed options.	Definitions from the documents are given in Clause 3. Please correct	Removed.
**-073		6.26.3		Ed	RTCA DO-178B[37] defines Dead and Deactivated code as: — Dead code – Executable object code (or data) which cannot be executed (code) or used (data) in an operational configuration of the target computer environment and is	Adding additional definitions to those provided by this document is confusing to users as they will not know which definition to apply. Please delete.	Removed.

1 **MB** = Member body / **NC** = National Committee (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

MB/ NC[1]	Line number	Clause/ Subclause	Paragraph/ Figure/Table	Type of comment[2]	Comments	Proposed change	Observations of the secretariat
					not traceable to a system or software requirement.		
**-074		6.27.5		Ed	Note 2: Using multiple labels on individual alternatives is not a violation of this recommendation.	The list item preceding this does not express a recommendation. The text introducing the list uses "can", which expresses a possibility. If the intent is to express a recommendation, please change "can" to "should": Besides, "Avoid" is a verb in the imperative, which expresses a requirement in ISO documents Please change to "by avoiding". Please correct the rest of document accordingly.	Note 1 and 2 removed.
**-075		6.33.6		Ed	in subclause 5 of this vulnerability	Please provide the exact (sub)clause number.	Agreed. Done
**-076		6.36.3		Ed	The risk and the failure mechanism is that	Please check for grammar	Agreed. Done.
**-077		6.38.1		Ed	the objects designated by the references are to be copied	"are to be" = "shall" in ISO documents	Reject. These are not requirements, but elements of a decision. Reworded to avoid apparent requirements.
**-078		6.40.1		Ed	in this subclause	Please provide subclause number instead because "this subclause" refers to 6.40.1	Deleted “in this subclause”

1 **MB** = Member body / **NC** = National Committee (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

Template for comments and secretariat observations

Date:2023-03-28	Document:	Project:

MB/ NC[1]	Line number	Clause/ Subclause	Paragraph/ Figure/Table	Type of comment[2]	Comments	Proposed change	Observations of the secretariat
**-079		6.41.5		Ed	Note: You mustUsers shall delegate in particular when the parent has data components not visible to methods of the subclass.	NOTEs cannot express requirements	Note moved to continuation text.
CA-16-080		6.52.1	Para 1, first sentence	Te	The first sentence is confusing.	Replace the first sentence with “Some languages provide runtime checking to detect errors that can lead to vulnerabilities, and thus prevent them.	Accept. Also removed permissive “may” in paragraph 2 and replaced with “often provide a mechanism”
CA-17-081		6.54.1	Para 1, third sentence	Te	The third sentence forms a new thought and should be a new paragraph.	Proposed rewrite for 6.54.1. Every programming language has features that are obscure, difficult to understand or difficult to use correctly. The problem is compounded if a software design must be reviewed by people who may not be language experts, such as hardware engineers, human-factors engineers, or safety officers. Even if the design and code are initially correct, maintainers of software may not fully understand the intent. The consequences of the above problems are more severe if the software is to be used in trusted applications, such as safety or mission-critical ones. Misunderstood language features or misunderstood code sequences can lead to application vulnerabilities in development or in maintenance.	Agreed. Editorial changes implemented.
CA-18-082		6.58.5		Te	The list of recommendations ignores static analysis.	Create a new bullet to be placed as the second bullet: Use multiple compilers and other static analysis tools to help identify and eliminate deprecated features.	Accepted.

1 **MB** = Member body / **NC** = National Committee (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

Template for comments and secretariat observations

Date:2023-03-28	Document:	Project:

MB/ NC[1]	Line number	Clause/ Subclause	Paragraph/ Figure/Table	Type of comment[2]	Comments	Proposed change	Observations of the secretariat
**-083		6.58.5		Ed	Note Discussions and meeting notes will give an indication of problem prone features that are recommended not be used or only be used with caution.	Please clarify what discussions and what meeting notes this refers to. If this refers to SC 22 meetings, please delete. SC internal content is not allowed in ISO deliverables.	Note deleted.
CA-19-084		6.58.5	First note	Te	The note recommends reviewing language design meeting minutes, which are typically not public. Therefore the note is incorrect.	Remove the note.	Agreed.
CA-20-085		6.59.5	Bullet 3	Te	Bullet 3 has no specific connection to concurrency and should be removed or reworded.	Remove bullet 3 and add the following to bullet 1 "… before processing any other parameters or attempting to access any activated threads."	Moved to be a continuation of the first bullet.
		6.60	Para 2	Te	Eliminate footnotes		Footnote on directed termination from 6.60.1 was moved into the subclause as paragraph 2.
**-086		6.62.2		Ed	ISO/IEC 8652:2012	This document is being revised, please update the date of this reference.	Date removed.
		6.62.3			Eliminate footnotes		Footnote from 6.62.3 reworked and placed in normative text as the first paragraph andto the end or paragraph 3.
CA-22-087		6.62.3	Para 4	Te	The first sentence contains the phrase "… for return to master tasks". This document uses the term "threads" exclusively.	Change the text to "… for return to the master thread …"	Agree. Changed.
CA-21-088		6.62.3, 6.62.5		Te	This clause contains a recommendation to use static analysis techniques such as model checkers to show thread termination is safely handled.	Add a final paragraph to 6.52.3: "Static analysis techniques, specifically model checking, can be used to statically verify a number	Implemented to provide rationale for the

1 **MB** = Member body / **NC** = National Committee (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

MB/ NC[1]	Line number	Clause/ Subclause	Paragraph/ Figure/Table	Type of comment[2]	Comments	Proposed change	Observations of the secretariat
					Clause 6.62.3 does not discuss model checking to support the recommendation.	of concurrency properties, including correct data access and termination protocols."	recommendation in subclause 5
**-089		6.63.2		Ed	ISO/IEC 8652:2012	This document is being revised, please update the date of this referenced.	Fixed.
CA-23-090		7.2.1	Sentence 1		Sentence 1 is confusing. It is not clear if we are trying to do something with an existing executable on the system, or if we are trying to load an executable code.	Reword as: "A first step often used in an attack is to get an executable developed by the attacker loaded on the system under attack."	Accepted.
**-091		7.2.4		Ed	Note 2 All of the above have some shortcomings, for example, a GIF (.gif) file may	In ISO deliverables, NOTES cannot express permission ("may", see DP 2, Table 8). Please change NOTE to body text or replace "may" with "can".	Replaced "may" with "might"
**-092		7.2.4		Ed	*black-list*	Insensitive, archaic and non-inclusive terms shall be avoided. For the purposes of this principle, "inclusive terminology" means terminology perceived or likely to be perceived as welcoming by everyone, regardless of their sex, gender, race, colour, religion, etc. Please correct. See DP2, 8.6	Terms deleted.
**-093		7.2.4		Ed	*white-list*	Insensitive, archaic and non-inclusive terms shall be avoided. For the purposes of this principle, "inclusive terminology" means terminology perceived or likely to be perceived as welcoming by everyone,	Term deleted.

1 **MB** = Member body / **NC** = National Committee (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

MB/ NC[1]	Line number	Clause/ Subclause	Paragraph/ Figure/Table	Type of comment[2]	Comments	Proposed change	Observations of the secretariat
						regardless of their sex, gender, race, colour, religion, etc. Please correct. See DP2, 8.6	
CA-24-094		7.4.4	Final bullet	Te	Bullet 5 need editorial rewording.	Connect the two sentences with “and”, and change “Built” to”build”.	Accepted
CA-25-095		7.6.3		Ed	“section 6“ is incorrect	Replace with “clause 6”	Accepted
**-096		7.6.3		Ed	section 6	Do you mean Clause 6?	Accepted
**-097		7.6.4		Ed	that it wo not	Please correct	Accepted
CA-26-098		7.8.4		Ed	There are two bullets, of which bullet 1 has 4 sub-bullets, but the final sub-bullet ends with “and”, connecting it to the final bullet.	Replace “and” in the fourth sub-bullet with a period, add “and” to the third sub-bullet.	Fixed.
**-099		7.8.4		Ed	rejected	Insensitive, archaic and non-inclusive terms shall be avoided. For the purposes of this principle, “inclusive terminology” means terminology perceived or likely to be perceived as welcoming by everyone, regardless of their sex, gender, race, colour, religion, etc.	Fixed, replaced white list with inclusion list and black list with exclusion list.

1 **MB** = Member body / **NC** = National Committee (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

MB/ NC[1]	Line number	Clause/ Subclause	Paragraph/ Figure/Table	Type of comment[2]	Comments	Proposed change	Observations of the secretariat
						Please correct	
**-100		7.12.4		Ed	Footnote 16	Please use callout instead and move link to bibliography.	Accepted.
**-101		7.34.1		Ed	Windows and Linux	Whenever citing a registered trademark, the following rule applies: If, exceptionally, trade names or trademarks cannot be avoided, their nature shall be indicated, for example by the symbol ® for a registered trademark (see Example 1) and by the symbol ™ for a trademark. If it is considered essential to give an example (or examples) of commercially available products suitable for successful application of the document because the product characteristics are difficult to describe in detail, trade names or trademarks may be given in a footnote as shown in Example 3. EXAMPLE 3 ... [trade name(s) or trademark(s) of product(s)] .. This information is given for the convenience of u or IEC] ... of this (these) product(s). The trademark text must be added as a numbered footnote.	

1 **MB** = Member body / **NC** = National Committee (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

MB/ NC[1]	Line number	Clause/ Subclause	Paragraph/ Figure/Table	Type of comment[2]	Comments	Proposed change	Observations of the secretariat
						If other tradenames or trademarks are cited in the document, please add relevant symbol and disclaimer EXAMPLE 3 ... [trade name(s) or trademark(s) of product(s)] .. This information is given for the convenience of u or IEC] ... of this (these) product(s).	
**-102		A.2		Ed	of Programming Language Vulnerabilities	Please avoid overuse of capitalization. Please correct all the titles in this annex.	Fixed
CA-27-103		A.2.5.3		Ed	Some subitems are indented incorrectly, in particular in A.2.5.3	Fix indentation in A.2.5.3	Fixed
**-104		A.4		Ed	Vulnerability List	Please remove page number from the table as the page numbering in the Word file is often different from the page numbering in the PDF files. ISO sells PDF documents.	Fixed
**-105		Annex B		Ed	Avoid use of unchecked casts or marking them to be immediately recognizable as unsafe.	This does not express a principle, this expresses a requirement. Verbs in the imperative express requirement. Please rephrase or change "principle" to a better suited word. This comment applies to the whole of B.2	Rephrased to express principles and to be clear they are not requirements.
**-106		Annex B		Ed	B.21	Please remember subsequent clauses	Assume this means "renumber" Implemented

1 **MB** = Member body / **NC** = National Committee (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

Template for comments and secretariat observations

Date:2023-03-28	Document:	Project:

MB/ NC[1]	Line number	Clause/ Subclause	Paragraph/ Figure/Table	Type of comment[2]	Comments	Proposed change	Observations of the secretariat
**-107		Annex C		Ed	Each language-specific Part has the following heading information and initial sections:	The technical content of a given ISO document starts on the page where there is the scope. It seems more appropriate to only include technical content in the template. Even better, the content should focus of clause 6 as this document states "Annex C, provides a template for the writing of programming language specific Parts that explain how the vulnerabilities from Clause 6 are realized in that programming language (or show how they are absent), and how they might be mitigated in language-specific terms"	Changed. Since language-specific parts rely upon this document, wording in parts 1 through 4 are are neded. Simplified the template to only provide any wording in addition to the standard ISO template.
**-108		Bibliography		Ed	[30] ISO/IEC/IEEE 60559:2011, Information technology - Microprocessor Systems - Floating-Point arithmetic language	THis reference is already referenced in Clause 2. Delete reference from here.	Implemented.
**-109		Bibliography		Ed	[20] IEC 61508, Parts 1-7, Functional safety: safety-related systems. 2010 (Part 3 920160 is concerned with software). International Electrotechnical Commission. Geneva Switzerland, 2010, 2016	The format of this citation is incorrect. Please reference each standard in an entry (except the ones referenced in Clause 2)	Moved to clause 3 and separated documents.
GB-110		*Bibliography*		*ed*	*Items [21] to [25] and [30] refer to withdrawn or superseded standards. Item [28] lacks a reference date.*	*Replace the referenced items with the following:* *[21] ISO/IEC 1539-1:2018, Information technology — Programming languages — Fortran — Part 1: Base Language* *[22] ISO/IEC 8652:2012, Information technology — Programming languages — Ada, with Cor.1:2016, Technical Corrigendum 1*	Removed year of publication. Document text does not reference specific subclauses.

1 **MB** = Member body / **NC** = National Committee (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

MB/ NC[1]	Line number	Clause/ Subclause	Paragraph/ Figure/Table	Type of comment[2]	Comments	Proposed change	Observations of the secretariat
						[23] ISO/IEC 9899:2018, Information technology — Programming languages — C *[24] ISO/IEC 14882:2020, Information technology — Programming languages — C++* *[25] ISO/IEC 15408:2022, Information technology -- Security techniques -- Evaluation criteria for IT security* *[28] ISO/IEC/TR 24731-1:2007, Information technology — Programming languages, their environments and system software interfaces — Extensions to the C library — Part 1: Bounds-checking interfaces* *[30] ISO/IEC 60559:2020, Information technology - Microprocessor Systems - Floating-Pointarithmetic*	
**-111		Cover Page		Ed	Programming languages — Avoiding vulnerabilities in programming languages – Part 1: Language-independent catalogue of vulnerabilities	Many aspects of this document are not in accordance with the ISO/IEC Directives. Please ensure to correct the document otherwise the document submission might be rejected at the FDIS stage.	
**-112		Foreword		Ed	— xxx xxxxxxx xxx xxxx	Please provide main changes as a list instead.	
**-113		FOREWORD		Ed	FOREWORD	Please use lower cases instead of small caps. Please correct throughout the table of content.	
CA-1-114		Index			All subclauses of clause 6.x are identically named and must not appear in the index. Similarly for subclauses in 7.x	Provide only clause numbering x and x.y in the index.	
**-115		Introduction		Ed	may	In ISO deliverables, “may” is used to express permission (of the document). See ISO/IEC Directives, Part 2, Tables 5 and 6. Check the occurrences of “may” throughout the document and	

1 **MB** = Member body / **NC** = National Committee (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

Template for comments and secretariat observations

Date:2023-03-28	Document:	Project:

MB/ NC[1]	Line number	Clause/ Subclause	Paragraph/ Figure/Table	Type of comment[2]	Comments	Proposed change	Observations of the secretariat
						correct to "can" (used to express possibility) accordingly.	

1 **MB** = Member body / **NC** = National Committee (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

ISO_IEC DIS 24772-1_BSI.doc: Collation successful

ISO_IEC DIS 24772-1_ISO.docx: Collation successful

ISO_IEC DIS 24772-1_JISC.docx: Collation successful

ISO_IEC DIS 24772-1_PKN.doc: Collation successful

ISO_IEC DIS 24772-1_SCC.doc: Collation successful

Collation of files was successful. Number of collated files: 5

SELECTED (number of files): 5

PASSED TEST (number of files conformed to CCT table model): 5

FAILED TEST (number of files conformed to CCT table model): 0

CCT - Version 2020.1