NA 060 DIN-Normenausschuss Maschinenbau (NAM)
NA 060-33-01 AA Aufzüge (SpA CEN/TC 10 und ISO/TC 178)
E-Mail des Bearbeiters/der Bearbeiterin bei DIN: can.demircan@vdma.org

Datum des Dokumentes	2024-02-13
Aktion	Information

N_556CommentsOnDIS_8100-2_disapproval

Template for comments and secretariat observations

Date: 2024-02-12	Document: ISO/DIS 8100-2:2023	Project: Enquiry

MB/ NC[1]	Line number (e.g. 17)	Clause/ Subclause (e.g. 3.1)	Paragraph/ Figure/ Table/ (e.g. Table 1)	Type of comment[2]	Comments	Proposed change	Observations of the secretariat
DE					Germany disagrees for the following reasons: The document has to be improved and cannot be issued as it is. Many technical improvements have to be done, for details see following various comments		
DE				ge	All SILx without space between SIL and its associated number shall be inserted a space after SIL.	SIL 1 SIL 2 SIL 3	
DE		Page V	European Foreword	ed	This document will supersede EN 81-20:2020. This a spelling mistake.	This document will supersede EN 81-50:2020.	
DE		4.2.1		ge	After adding ISO/DIS 8100-1:2023, 4.3.9.1.1, 2nd paragraph, it is not clear with components or parts are meant with locking device, locking element, locking hock or pin, lock and locking. ISO/DIS 8100-1:2023, 4.3.9.1.1, 2nd paragraph states that each component taking part at the door locking and in the checking forms part of the locking device. E.g. hanger plates, their guides and lower guides take part at the door locking, but some tests cannot be performed with these devices (complete door). Is the locking pin/hock a locking element or does the locking element include the linkage of the locking pin/hock.	Clarify first definitions and then correct wording in ISO 8100-2 and probably -1 accordingly to avoid misunderstandings.	
DE		4.2.1.2.2	Paragraph 2	te	It shall be clearly distinguished between “locking device” and “locking element”. General Explanation: According to ISO 8100-1:2023, 4.3.9.1.1, “Each component taking part in the locking of doors and in the checking of the locking forms part of the **locking device”** and ISO 8100-	Alternative paragraph 2 of ISO 8100-2:2023, 4.2.1.2.2: “The driving of the locking element of the locking device shall be smooth, without shocks, and at a rate of 60 (±10 %) cycles per minute.”	

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 (e.g. 17)	Clause/ Subclause (e.g. 3.1)	Paragraph/ Figure/ Table/ (e.g. Table 1)	Type of comment[2]	Comments	Proposed change	Observations of the secretariat
					1:2023, 4.3.9.1.6 requires the application of 1000 N in opening direction of the door on a height of 1.50 m ± 0,1 m above the sill level, in case of sliding doors. Issue: According to ISO 8100-2:2023, 4.2.1.2.1, paragraph 2 “The driving of the device shall be smooth, without shocks, and at a rate of 60 (±10 %) cycles per minute.” This rate is meant in our point of view and have been taken up to now for the test of the locking element (e.g. hook for a sliding door or bolt type locking element for hinged doors) but not for the locking device.		
DE		4.2.1.2.2	Paragraph 3	te	Issue: According to ISO 8100-2:2023, 4.2.1.2.2, paragraph 3 “During the endurance test, the electrical contact of the lock shall close a resistive circuit under the rated voltage and at a current value double that of the rated current.”	During the endurance test, the electric~~al~~ safety device ~~contact~~ of the locking device ~~of the locking element~~ shall close a resistive circuit under the rated voltage and at a current value double that of the rated current	
DE		4.2.1.2.2	Paragraph 3	te	Here is the requirement “During the endurance test, the electrical contact of the lock shall close a resistive circuit under the rated voltage and at a current value double that of the rated current.” The “rated current” of what? 1. The rated current of the locking device? ➔ Then, if the producer of the locking device writes in its data sheet that max. current of the locking device is e.g. 500 mA, the endurance test is to performed with a switched current of 1 A. 2. The rated current of the electric contact? ➔ Then, if the max. current in the data sheet of the contact is e.g. 2 A, the endurance test	During the endurance test, the electrical safety device contact of the locking element shall close a resistive circuit under the rated voltage and at a current value double that of the rated current of the locking device.	.

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 (e.g. 17)	Clause/ Subclause (e.g. 3.1)	Paragraph/ Figure/ Table/ (e.g. Table 1)	Type of comment[2]	Comments	Proposed change	Observations of the secretariat
					is to be performed with a switched current of 4 A.		
DE		4.2.1.2.2	Paragraph 3	te	Since 4.2.5.3.1 c) and 4.3.9.1.1 of ISO 8100-1 requires an “electric safety device”, not only a contact can be used, also the usage of an electric safety circuit or of a SIL-rated circuit is possible to check the locked position. It is not clear whether the requirement of the usage of double the rated current also apply to electric safety circuits and to SIL-rated circuits, or only to the named “electrical contact”. ➔ The components of electric safety circuits and SIL-rated circuits shall be over-dimensioned by the factor 1,5 according to ISO 8100-1. To double the rated current would be an over-dimensioning by the factor 2!	Precise the requirement.	
DE		4.2.1.2.2	Paragraph 5	te	Issue: According to ISO 8100-2:2023, 4.2.1.2.2, paragraph 5 “The driving of the device shall be smooth, without shocks, and at a rate of 60 (±10 %) cycles per minute.” This rate is meant in our point of view and have been taken up to now for the mechanical checking device for the locking pin or the position of the locking element.	Alternative paragraph 5 of ISO 8100-2:2023, 4.2.1.2.1: “The driving of the mechanical checking device for the locking pin or the position of the locking element of the locking device shall be smooth, without shocks, and at a rate of 60 (±10 %) cycles per minute.”	
DE		4.2.1.4.1	General	ed	Here is used the term “contact”, where any kind of electric safety device is meant.	4.2.1.4.1 Endurance test of ~~contacts~~ electric safety device~~s~~	
DE		4.2.1.4.2.2	Paragraph 1 2nd sentence	ed	Here is used the term “contact”, where any kind of electric safety device is meant.	“The electric safety device shall remain conductive for at least 0,5 s.”	
DE		4.2.1.4.2.2		te	In this two sub-clauses is distinguished between “A.C. locking devices” and	4.2.1.4.2.2 ~~A.C.~~ locking devices for AC current shall open and close an electric circuit under a voltage equal to 110 % of the rated voltage of 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 (e.g. 17)	Clause/ Subclause (e.g. 3.1)	Paragraph/ Figure/ Table/ (e.g. Table 1)	Type of comment[2]	Comments	Proposed change	Observations of the secretariat
		and 4.2.1.4.2.3			"D.C. locking devices" Both types are undefined! Assuming that "A.C." means "AC current" and "D.C." means "DC current", it is not clear which current is meant: 1. The current to operate the locking device in order to unlock the door? 2. The current, which is used to check the locked position by an electric safety device? Possibility 2. seems to make no sense, because the producers of locking devices do not know the type of current, their customers will use later for the electric safety chain. This is unknown when type-testing is done! ➔ Also ISO 8100-1 does not know the terms "A.C. locking device" and "D.C. locking devices". According to 4.3.9.1.11 of ISO 8100-1, on the data plate of the locking device an indication about the type (A.C. type or D.C. type) is not necessary.	electrical safety device of the locking device 50 times, at normal speed and at intervals of 5 s to 10 s. The electrical safety device ~~contact~~ shall remain closed for at least 0,5 s. The testing circuit shall comprise a choke and a resistance in series. Its power factor shall be 0,7 ± 0,05 and the test current shall be 11 times the rated current indicated by the manufacturer of the electrical safety device. 4.2.1.4.2.3 ~~D.C.~~ locking devices for DC current shall open and close an electric circuit under a voltage equal to 110 % of the rated voltage of the electrical safety device of the locking device 20 times, at normal speed and at intervals of 5 s to 10 s. The electrical safety device ~~contact~~ shall remain closed for at least 0,5 s. The testing circuit shall comprise a choke and a resistance in series having values such that the current reaches 95 % of the steady-state value of the test current in 300 ms. The test current shall be 110 % of the rated current indicated by the manufacturer of the electrical safety device.	
DE		4.2.1.4.2.3	Paragraph 1 2nd sentence	ed	Here is used the term "contact", where any kind of electric safety device is meant.	"The electric safety device shall remain conductive for at least 0,5 s."	
DE		4.2.1.4.5	headline	ed	Here is used the term "contact(s)", where any kind of electric safety device is meant.	"**4.2.1.4.5 Verification of the requirements appropriate to electric safety devices and their accessibility**"	
DE		4.2.2.1	Paragraph 1	te	Issue: The second sentence "The number of cycles per minute in endurance tests shall be between 45 – 60" shall be deleted as the number of cycles per minute in such endurance tests shall be suited to the dimensions of the construction.	Devices providing direct mechanical linkage between panels shall be included in the tests mentioned in 4.2.1 except the number of cycles per minute. ~~The number of cycles per minute in endurance tests shall be reduced to a between 45 – 60~~.	

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 (e.g. 17)	Clause/ Subclause (e.g. 3.1)	Paragraph/ Figure/ Table/ (e.g. Table 1)	Type of comment[2]	Comments	Proposed change	Observations of the secretariat
DE		4.5.3.2.5	Number of tests	ed	The text of ISO/PRF 8100-2:2023 corresponds to the text of EN 81-50:2020 - 5.5.3.2.5 – 3. paragraph. “In the three tests with maximum mass, the reference value of the buffer force at a stroke given by its instructions, equal to 50 % of the real height of the buffer, shall not vary by more than 5 %. In the tests with minimum mass, this shall be observed in analogy.” Not part of 4.5.3.2.5 number of tests.	Move text to "4.5.3.2.6 Checks".	
DE		4.5.3.2.5		te	If the buffer is not compressed to 50 % of its rated height with minimum load, this requirement cannot be fulfilled. The wording “this shall be observed in analogy” is not clear. The validation at maximum mass is sufficient to cover the risk of to high tolerances.	In the three tests with maximum mass, the reference value of the buffer force at a stroke given by its instructions, equal to 50 % of the real height of the buffer, shall not vary by more than +/- 5 %. ~~In the tests with minimum mass, this shall be observed in analogy.~~	
DE		4.5.3.2.5	Number of tests	ed	The text of ISO/PRF 8100-2:2023 corresponds to the text of EN 81-50:2020 - 5.5.3.2.5 – 4 paragraphs. “Within 30 min before the test, the buffer shall be once loaded, either statically or dynamically, in order to prevent further settlement and deviations during the test.” Not part of 4.5.3.2.5 number of tests.	Move text to "4.5.3.2.1 Test procedure".	
DE		4.5.3.2.6.2	Check of the condition of the buffer after tests	te	The text of ISO/PRF 8100-2:2023 corresponds to the text of EN 81-50:2020 - 5.5.3.6.2. After the tests with the maximum mass, no parts of the buffer shall show any permanent deformation or be damaged, so that is condition shall guarantee normal operation. It is not possible to be sure the buffer can	Possible proposal: After the tests with the maximum load, no parts of the buffer shall show any permanent deformation or be damaged~~, so that is condition shall guarantee normal operation~~.	

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 (e.g. 17)	Clause/ Subclause (e.g. 3.1)	Paragraph/ Figure/ Table/ (e.g. Table 1)	Type of comment[2]	Comments	Proposed change	Observations of the secretariat
					continue to function normally because the buffer looks undamaged after the loads. Damages may have occurred in the foam, e.g. micro cracks. In addition, the statement suggests that a buffer works if it looks good. Consider the notes, e.g. from operators and manufacturers, from practice. "Just" looking is not enough to assess the buffer for normal functioning. Therefore, buffer producers create technical operational instructions and drawings. Can the certification laboratory guarantee that the buffer will function normally after being forced to loads three times? We, as a manufacturer, would not make such a statement. It's already in the direction of warranty service which means at the end the risk of legal disputes. It is not clear who takes the guarantee and a guarantee is defined.		
DE		4.6.3.1.2	Last line	ed	After testing, clearances and creepeages shall at least be as required	After tests, clearances and creepage distances shall not become smaller than the minimum ~~accepted~~ required.	
DE		4.10.4	Combination of bending and compression/ tension or bucling stresses	te	Bending and buckling: $\sigma = \sigma_k + 0{,}9 \times \sigma_y \leq \sigma_{perm}$ Wrong formula for Bending and buckling	$\sigma = \sigma_k + 0{,}9 \cdot \sigma_m \leq \sigma_{perm}$	
DE		4.11.2.3.1.2		ed	the "n" is missing in the formula for "sine"	$f = \mu \cdot \frac{4\left(1-\sin\frac{\beta}{2}\right)}{\pi-\beta-\sin\beta}$	
DE		4.12.3	Figure 10	ed	Dt/Dr starts at 34	Expand to Dt/Dr = 30 as this is given as minimum Dt/Dr in Table 11	
DE		4.13.3		ed	Sub-clauses d) e) f) e) and f) are sub-clauses to d)	d) termination and wedge security test (…-6) • pull-force of 20%... acceptance criteria…	

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 (e.g. 17)	Clause/ Subclause (e.g. 3.1)	Paragraph/ Figure/ Table/ (e.g. Table 1)	Type of comment[2]	Comments	Proposed change	Observations of the secretariat
DE		4.13.3		ed	Sub-clauses g) h) i) h) and i) are sub-clauses to g)	Replace g) with e) e) fatigue behaviour of socket …(…-6) • minimum rope force 15%.... acceptance criterion: …	
DE		4.13.4		ed	Sub-clauses a) – h) should be rearranged	a) the minimum free… • 600 mm for elastomeric coated ropes • 500 mm for elastomeric coated belts… b) after 80 % of the minimum…. • the test bay be terminated … • the test may be discounted… o 6 x nominal diameter for steel wire ropes o 6 x nominal diameter of load bearing …. and when the minimum breaking load has not been reached.	
DE		4.13.6.2	5th paragraph	ed	"It shall be performed."	Remove "."	
DE		4.13.6.2		ed	a) and b) described above;	Add " " : a) and b) described above;	
DE		4.14.3.2		ed	The following visual discarding criteria shall be considered.	Replace "." with ":" at the end of the sentence The following visual discarding criteria shall be considered:	
DE		4.17	1st §	ed	List of limits to be considered is non-exhaustive, therefore formulation like in 2nd § shall be used.	Fault exclusion shall only be considered provided that components are applied within their relevant worst-case operating parameter limits ~~of characteristics~~, e. g. value, temperature, humidity,	

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 (e.g. 17)	Clause/ Subclause (e.g. 3.1)	Paragraph/ Figure/ Table/ (e.g. Table 1)	Type of comment[2]	Comments	Proposed change	Observations of the secretariat
						voltage and vibrations.	
DE		4.17	Table 3, 1.1 (b)	te	(b) is located in column for change to lower value, therefore "< infinite" does not make sense here. Comma missing after "resistor".	Random change of value from R_N down to $0{,}5R_N$ ≤ ~~R < infinite~~, where R_N is the nominal value of the resistor, shall be considered.	
DE		4.17	Electrical and electronic components – Fault exclusion Table 3, Row 1.1	te	Resistor fixed: Conditions for exclusion of the fault "Change to lower" value unclear. If condition (a) applies, is then the change of the resistor limited to (b)?	Needs to be specified more precisely in column 5, line 3: (a) (1 (b) (1 (c) (1 Note 1: If (a) is not applicable (b), If (a) and (b) are not applicable (c) if applicable.	
DE		4.17	Electrical and electronic components – Fault exclusion Table3, Row 1.5	te	Inductive components: No fault exclusions for the faults "Change to higher value" / "Change to lower value", not according state of the art. See ISO 13849-2:2012, Table D.13: Random change of value limited to 0,5*Ln<L<Ln+tolerance, where Ln is the nominal value	Limitation of the change of value to 0,5*Ln<L<Ln+tolerance, where Ln is the nominal value.	
DE		4.17	Table 3, 2.4 (a)	te	Internal overload caused by external fault shall be considered.	Measures are taken to ensure that an external fault on primary or secondary signal side or an internal fault of the signal isolation component cannot result in excessive temperature of its insulating material.	
DE		4.17	Table 3, 2.4, Conditions	ed	Stated standards are not dated.	see also ISO 13849-2:2012 and IEC 61800-5-2:2016.	
DE		4.17	Table 3, 3.1 (a)	ed	Example for clearances and creepage distances is valid up to 2000 m altitude. Dot at end of sentence after V_{rms} is missing	That means that the creepage distances are 4 mm and the clearances 3 mm ~~at~~ up to 2000 m altitude for 250 V_{rms}.	
DE		4.17	Table 3, 3.1 (a)	te	When protection degree of connector is IP54 use for pollution degree 2 of column "printed wiring	If the protection of the connector is IP54 or better, pollution degree 2 of column "printed wiring	

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 (e.g. 17)	Clause/ Subclause (e.g. 3.1)	Paragraph/ Figure/ Table/ (e.g. Table 1)	Type of comment[2]	Comments	Proposed change	Observations of the secretariat
					material" shall be allowed, same as allowed by standards harmonized under MD.	material" of IEC 60664-1:2020, Table F.5 can be used.	
DE		4.17	Table 3, 3.6 (a)	ed	Reference to table 4 shall read F.5 (same as in Table 3, 3,1 (a)).	The column "printed wiring material" of IEC 60664-1:2020, Table 4 F.5 is not used.	
DE		4.17	Table 3, 3.6 (a)	ed	Example for clearances and creepage distances is valid up to 2000 m altitude (same as in Table 3, 3,1 (a)).	That means that the creepage distances are 4 mm and the clearances 3 mm ~~at~~ up to 2000 m altitude for 250 V_{rms}.	
DE		4.17	Table 3, 3.6 (a)	te	When protection degree of PCB is IP54 use for pollution degree 2 of column "printed wiring material" shall be allowed, same as allowed by standards harmonized under MD (same as in Table 3, 3,1 (a)).	If the protection of the PCB is IP54 or better, and the printed side(s) is (are) coated with an ageing-resistant varnish or protective layer covering all conductor paths and for the inner layers of multilayer PCB, pollution degree 2 of column "printed wiring material" of IEC 60664-1:2020, Table F.5 can be used.	
DE		4.17	Table 3, 3.7 (a)	ed	Creepage distances and clearances shall at least be as required.	Short circuit can be excluded under circumstances where the short circuit of the component itself can be excluded and the component is mounted in a way that the creepage distances and clearances are not reduced below the minimum ~~acceptable~~ required values as listed in 3.1 and 3.6 of this table, neither by the mounting technique nor by the PCB itself.	
DE		4.18	Paragraph 1	ed	Wrong reference, 4.11.2.1.7 shall read 4.11.2.4.	SIL-rated circuits shall comply with the requirements in the standard calling for the use of this standard (e.g. ISO 8100-1:2023, ~~4.11.2.1.7~~ 4.11.2.4) and with one of the following:	
DE		4.18	b)	te	Remove restriction on using IEC 61508-2:2010 Table 2 and first line of Table 3. ISO 8100-2 should not force designer of safety-	b) the relevant requirements of IEC 61508 series of standards, with the following restriction~~s~~: ~~— IEC 61508-2:2010,~~	

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 (e.g. 17)	Clause/ Subclause (e.g. 3.1)	Paragraph/ Figure/ Table/ (e.g. Table 1)	Type of comment[2]	Comments	Proposed change	Observations of the secretariat
					related system to a more complex solution (Type B) than is required. Type A solutions are capable of SIL 3. Obviously, IEC 61508 supports use of Type A elements as shown in Table 2	~~Table 2 and first line of Table 3 shall not be used;~~ – IEC 61508-3:2010, Annex G, G.2 Limited variability configuration, limited application configurability is only permitted to be used. Demand interval shall be considered not to exceed 100s	
DE		4.18	b), 2nd bullet point	te	Should “not to exceed” read “to exceed”? I. e. demand interval shall be considered not to be smaller than 100s? Dot at end of sentence missing.	Demand interval shall be considered ~~not~~ to exceed 100 s.	
DE		Annex A	Table A.2	Ge/ed	These tables seem to explicitly refer only to the C/C++ languages. If the rules are prescribed so explicitly here, this sometimes imposes unnecessary restrictions, especially on other languages (e.g. Rust with its memory safety). The points referred to here in IEC61508 reflect this more generically and appropriately in comparison. Therefore, the points that are not in IEC61508 should be deleted and the wording from IEC61508 should be used. Some of these rules are simplified without additional explanation and restrictions and therefore do not make sense when applied without further explanation. Accordingly, therefore the IEC61508 standard does not usually use "shall", but "should". E.g. In the case of error handling, multiple returns can make the code clearer. Exceptions are also good	Clarify topic! E.g., use the formulation directly from the IEC61508 (without simplified and correspondingly shortened sentences in the standard), or change at least “shall” to “should”: - Every subsystem, at all levels of the design, shall be clearly defined and is of restricted size (only a few functions). The interfaces between subsystems shall be kept as simple as possible and the cross-section (i.e. shared data, exchange of information) is minimised. The complexity of individual subsystems shall also be restricted. – a software module (or equivalently, subprogram) should have a single well-defined task or function to fulfil; – connections between software modules should be limited and strictly defined, coherence in one software module shall be strong; – collections of subprograms should be built	

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 (e.g. 17)	Clause/ Subclause (e.g. 3.1)	Paragraph/ Figure/ Table/ (e.g. Table 1)	Type of comment[2]	Comments	Proposed change	Observations of the secretariat
					programming practice and there can be several of them in a function without it becoming confusing. There is no obvious reason to restrict the conditions, as a correspondingly high test coverage can ensure that multiple conditions are also possible without risk. If a device fulfills e.g. 6 safety functions, these should also be able to be mapped to an actuator in one step. Also this rule is not in the IEC61508.	providing several levels of software modules; – subprogram sizes should be restricted to some specified value, typically two to four screen sizes; – subprograms should have a single entry and a single exit only; – software modules should communicate with other software modules via their interfaces - where global or common variables are used they should be well structured, access should be controlled and their use should be justified in each instance; – all software module interfaces should be fully documented; – any software module's interface should contain only those parameters necessary for its function. However, this recommendation is complicated by the possibility that a programming language may permit default parameters, or that an object-oriented approach is used. The following principles should be applied to minimise structural complexity: – divide the program into appropriately small software modules, ensuring they are decoupled as far as possible and all interactions are explicit; – compose the software module control flow using structured constructs, that is sequences, iterations and selection; – keep the number of possible paths through a software module small, and the relation between the input and output parameters as simple as possible; – avoid complicated branching and, in particular,	

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 (e.g. 17)	Clause/ Subclause (e.g. 3.1)	Paragraph/ Figure/ Table/ (e.g. Table 1)	Type of comment[2]	Comments	Proposed change	Observations of the secretariat
						avoid unconditional jumps (goto) in higher level languages; – where possible, relate loop constraints and branching to input parameters; – avoid using complex calculations as the basis of branching and loop decisions. Features of the programming language which encourage the above approach should be used in preference to other features which are (allegedly) more efficient, except where efficiency takes absolute priority (for example some safety critical systems).	
DE		Annex A	Table A.3, last line of table before NOTES	ed	Wrong reference: 4.11.2.1.6 should read 4.11.2.1.7	For the response time of a safety function see other standards calling for the use of this standard (e.g. ISO 8100-1:2023, ~~4.11.2.1.6~~ 4.11.2.1.7)	
DE		Annex A	Table A.3, last line of table	te	Response time. ISO 8100-1:2023, 4.11.2.1.6, states: “An electric safety device when operated shall initiate **immediately** stopping of the lift machine and prevent its setting in motion.” This is valid for safety contacts operating directly on the safety chain when being operated. SIL-rated circuits, especially when software based, have an internal processing time and cannot initiate immediately stopping. In order to ensure a safe lift, for SIL-rated circuits, especially software based ones, a maximum response time must be defined.	-> To be reviewed	
DE		Annex A	Table A.6, SIL 3	te	IEC 61508-2:2010, Table A.5 – Invariable memory ranges states in its “Notes” column for measures using signatures: “The effectiveness of the signature depends on the width of the signature in relation to the block length of the	-> To be reviewed Note: Comment is also valid for table A.7, SIL 2 + 3, Block safety with CRC.	

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 (e.g. 17)	Clause/ Subclause (e.g. 3.1)	Paragraph/ Figure/ Table/ (e.g. Table 1)	Type of comment[2]	Comments	Proposed change	Observations of the secretariat
					information to be protected” Therefore, measures with CRC-32 signature require a definition of the maximum block length permitted.		
DE		Annex A	Table A.7, SIL 3	te	IEC 61508-2:2010, Table A.5 – Invariable memory ranges states in its “Notes” column for measures using signatures: “The effectiveness of the signature depends on the width of the signature in relation to the block length of the information to be protected” Therefore, measures with CRC-32 signature require a definition about the maximum block length permitted.		
DE		Annex A	Table A.8 Measure Test pattern	ge	If the electronic circuit being tested here has a discrete design (with the appropriate clearances), an error exclusion can be made with regard to crosstalk. The remaining Stuck-At fault can be tested / detected via a simple common pulse.	For a single digital I/O-signal simple pulses are sufficient. For more than one digital I/O-signal the pulses shall be separated in time in order to be able to detect cross-talk. If the I/Os are built as individual discrete circuits, single pulses are also sufficient if the insulation is sufficient	
DE		Annex A	Table A.13 Measure Sequence Number	ge	It is not understandable why the sequence number must be 16-bit. All the failures here can also be recognized with an 8-bit sequence number. This is also possible not only with a counter, but also by marking the message (what it contains) with a defined sequence (e.g. first message A, then B, then C, then A again). The min. size of the sequence number shall be given in a formula to give flexibility.	A ~~16-bit~~ sequence number is integrated into each message being transmitted. The sequence number is incremented for every message and checked by the receiver against continuity. Formula: ~~After the full range of the 16-bit is reached, the sequence number re-starts.~~	

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 (e.g. 17)	Clause/ Subclause (e.g. 3.1)	Paragraph/ Figure/ Table/ (e.g. Table 1)	Type of comment[2]	Comments	Proposed change	Observations of the secretariat
DE		Tools	Table A.14	ge	The period of 2 years seems to have been chosen arbitrarily. The time alone is not a factor, but it depends primarily on the use (e.g. in the case of the Translater, the number of projects, see C.4.4, IEC61508). Safety can also be ensured by tools certified for this purpose / or checked by specific tests. This generates more safety than time alone. Category T3 and T2 is summarized in the draft of the ISO8100 standard (see IEC61508-4:2010, 3.2.11). It would make sense to separate these so that T2 tools are not subject to correspondingly high requirements.	Listing of all tools and its versions generating any output which goes directly into the or which are being used to test or verify the design or executable code of the product For these tools (unless certified for this purpose) □ a bug list shall be available, □ an evidence of about 2 years of increased confidence from use and/or the corresponding amount of use (depending on the category, see IEC61508-4:2010, 3.2.11) shall exist. □ the version of a tool shall not be changed unless justified	
DE		Annex A	Table A.17	te	Use of 2^{-r} is no longer possible to be used according to IEC 61784-3:2021. Furthermore, properness of CRC must be proven by calculation. Therefore, another formula resp. approach is required.	-> To be reviewed	
DE		Annex A	Measure -> Tools	ed	B.3.5 and C.4.4 is not in the IEC61508-1:2010 (as stated in the table). It is in the IEC61508-7:2010.		
DE		Annex A	Tabelle A.18	ge	This table quoted the IPA/SEC ESCR standard. - This is not widely used in Europe. - It only refers to the C/C++ language. - There are no tools known to us that automatically test the application of these rules (like MISRA has these).	Add a note to Table A.18 and/or at the end of table A.2: Instead of IPA/SEC ESCR3.0, a recognized language standard for the programming language can also be used (e.g. MISRA-C / MISRA-C++), provided that the requirements from IEC61508 are met.	

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: 2024-02-12	Document: ISO/DIS 8100-2:2023	Project: Enquiry

MB/ NC[1]	Line number (e.g. 17)	Clause/ Subclause (e.g. 3.1)	Paragraph/ Figure/ Table/ (e.g. Table 1)	Type of comment[2]	Comments	Proposed change	Observations of the secretariat
DE		Annex C		ed	Formulae (C.2)	Add "." => (C.2)	
DE		Bibliography		ed	IEC 61800-5-2 not listed, used in chapter 4.17, Table3, 2.4, Conditions.	IEC 61800-5-2:2016, Adjustable speed electrical power drive systems — Part 5-2: Safety requirements. Functional	

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