DRAFT INTERNATIONAL STANDARD ISO/DIS 13849-1

ISO/TC 199

Voting begins on: **2020-06-08**

Secretariat: **DIN**

Voting terminates on: 2020-08-31

Safety of machinery — Safety-related parts of control systems —

Part 1: General principles for design

Sécurité des machines — Parties des systèmes de commande relatives à la sécurité — Partie 1: Principes généraux de conception

ICS: 13.110

iTeh STANDARD PREVIEW (standards.iteh.ai)

ISO/DIS 13849-1 https://standards.iteh.ai/catalog/standards/sist/0ec4d0c2-c2ee-4bac-b69f-0a883595198b/iso-dis-13849-1

THIS DOCUMENT IS A DRAFT CIRCULATED FOR COMMENT AND APPROVAL. IT IS THEREFORE SUBJECT TO CHANGE AND MAY NOT BE REFERRED TO AS AN INTERNATIONAL STANDARD UNTIL PUBLISHED AS SUCH.

IN ADDITION TO THEIR EVALUATION AS BEING ACCEPTABLE FOR INDUSTRIAL, TECHNOLOGICAL, COMMERCIAL AND USER PURPOSES, DRAFT INTERNATIONAL STANDARDS MAY ON OCCASION HAVE TO BE CONSIDERED IN THE LIGHT OF THEIR POTENTIAL TO BECOME STANDARDS TO WHICH REFERENCE MAY BE MADE IN NATIONAL REGULATIONS.

RECIPIENTS OF THIS DRAFT ARE INVITED TO SUBMIT, WITH THEIR COMMENTS, NOTIFICATION OF ANY RELEVANT PATENT RIGHTS OF WHICH THEY ARE AWARE AND TO PROVIDE SUPPORTING DOCUMENTATION. This document is circulated as received from the committee secretariat.

ISO/CEN PARALLEL PROCESSING



Reference number ISO/DIS 13849-1:2020(E)

iTeh STANDARD PREVIEW (standards.iteh.ai)

ISO/DIS 13849-1 https://standards.iteh.ai/catalog/standards/sist/0ec4d0c2-c2ee-4bac-b69f-0a883595198b/iso-dis-13849-1



COPYRIGHT PROTECTED DOCUMENT

© ISO 2020

All rights reserved. Unless otherwise specified, or required in the context of its implementation, no part of this publication may be reproduced or utilized otherwise in any form or by any means, electronic or mechanical, including photocopying, or posting on the internet or an intranet, without prior written permission. Permission can be requested from either ISO at the address below or ISO's member body in the country of the requester.

ISO copyright office CP 401 • Ch. de Blandonnet 8 CH-1214 Vernier, Geneva Phone: +41 22 749 01 11 Fax: +41 22 749 09 47 Email: copyright@iso.org Website: www.iso.org

Published in Switzerland

Contents

Fore	word		vi			
Intro	duction	1	vii			
1	Scope	9	1			
2	Norm	ative references				
3	Terms and definitions					
5	3.1	Terms and definitions	2			
	3.2	Symbols and abbreviated terms				
4	Overview					
	4.1	Requirements for risk assessment and risk reductions				
	4.2	Contribution to the risk reduction by the safety function				
	4.3	Risk reduction using an SRP/CS				
	4.4	Methodology				
	4.5	Required Information				
	4.6	Safety function realization by using subsystems	16			
5	Speci	fication of safety functions				
	5.1	General				
	5.2	Safety requirements specification (SRS)				
		5.2.1 General requirements				
		5.2.2 Decomposition of SKP/LS into subsystems				
	53	5.2.5 Required norformance level (PL) for each safety function				
	5.4	Review of the safety requirement specification	25			
~			05			
6	Design considerations					
	0.1	Evaluation on the atmergen perior mance level CD-c2cc-4bac-b69f				
		6.1.2 Correlation between PL and SIL				
		6.1.3 Architecture – Categories and their relation to $MTTF_{\rm p}$ of each channel.				
		DC and CCF				
		6.1.4 Mean time to dangerous failure (MTTF _D)				
		6.1.5 Diagnostic coverage (DC)				
		6.1.6 Common cause failures (CCF)				
		6.1.7 Systematic failures				
		6.1.8 Simplified procedure for estimating the PL				
		6.1.9 Alternative procedure to determine the PL and PFH_D without $MTTF_D$	38			
		6.1.10 Fault consideration and fault exclusion				
	62	Combination of subsystems to achieve an overall PL of the safety function				
	0.2	6.2.1 General	41			
		6.2.2 Known PFH _D values				
		6.2.3 Unknown PFH _D values				
7	Softw	are safety requirements	42			
,	7.1 General					
	7.2	Safety-related embedded software (SRESW)				
	7.3	Safety-related application software (SRASW)				
	7.4	Limited variability language (LVL)				
		7.4.1 General				
		7.4.2 Full variability language (FVL)				
		7.4.3 Decision for LVL or FVL				
	/.5	Software-based parameterization				
		7.5.1 Utilt[7]				
		7.5.2 Influences on salety-related parameteris				
		, isis negationents for software based manual parameterization				

 Verification that achieved PL meets PL, S3 Performance of software based manual parameterization Validation taspects of design S3 Validation principles S3 Validation principles S3 10.1 Validation principles S3 10.1 Validation principles S3 10.1 Ceneral S3 10.2 Validation principles S6 10.3 General S6 10.4 Specific fault lists S6 10.4 Specific fault lists S6 10.2 Validation by analysis S7 10.2.2 Analysis techniques S8 10.3 Validation by testing S8 10.3 Validation by testing S9 10.3.4 Mumber of test samples S9 10.3.5 Testing methods S99 10.4 Validation of the safety Requirements Specification (SRS) S0 S0.4 Validation of the safety Requirements Specification (SRS) S0 S0.5 Checking/verification of safety-feature satisfy structures S1.6 Checking/verification of safety-feature software S2.7 Checking/verification of safety-feature software S1.6 Checking/verification of safety-feature software S1.6 Checking/verification of safety-feature software S1.7 General S2.7 Checking/verification of safety-feature software S3.1 General S3.1			7.5.4	Verification of the parameterization tool				
9 Fignonic aspects of design 53 10 Validation 53 10.1 Validation principles 53 10.1.1 Cleneral 53 10.1.2 Validation plan 55 10.1.3 Cleneral 53 10.1.4 Specific fault lists 56 10.1.5 Information for validation 56 10.2 Validation by analysis 57 10.2.2 Analysis techniques 58 10.3.1 General 59 10.3.2 Measurement accuracy 59 10.3.2 Measurement accuracy 59 10.3.2 Measurement accuracy 59 10.3.4 Number of test samples 59 10.4 Validation of the safety Requirements Specification (SRS) 60 10.5 Validation of safety Requirements Specification (SRS) 60 10.6.1 Validation of safety Strengto Strengt	Q	Vorifi	7.3.3 cation th	parachieved PI meets PI				
10 Validation 53 10 Validation principles 53 10.1 General 53 10.1.2 Validation plan 55 10.1.3 General 53 10.1.4 Specific fault lists 56 10.1.3 General 57 10.1.4 Specific fault lists 56 10.1.2 Validation by analysis 57 10.2.2 Analysis techniques 58 10.3 Validation by testing 58 10.3.1 General 59 10.3.2 Masurement accuracy 59 10.3.3 Additional requirements for testing 59 10.3.4 Number of test samples 59 10.4 Validation of the safety function 60 10.6 Validation of the safety function of acaystem (S) 60 10.6.1 Validation of combination of subsystems 63 10.6.2 Validation of acaystem (S) 64 10.6.2 Validation of acaystem (S) 64 10.6.2 Validation of acaystem (S) 64 10.6.	0	Frgon		nacts of design				
10 Valuation principles 53 10.1 Valuation principles 53 10.1.2 Valuation plan 53 10.1.2 Valuation plan 55 10.1.3 Generic fault lists 56 10.1.4 Specific fault lists 56 10.1.5 Information for validation 56 10.2.1 General 57 10.2.2 Analysis techniques 58 10.3 Valuation by testing 58 10.3.4 Mumber of test samples 59 10.3.5 Testing methods 59 10.4 Validation of the safety Requirements Specification (SRS) 60 10.5 Validation of the safety function 60 10.6.1 Validation of the safety function 61 10.6.2 Validation of safety seques against systematic failures 62 10.6.3 Validation of safety seques against systematic failures 63 10.6.4 Validation of safety seques against systematic failures 62 10.6.5 Checking/verification of safety/reliated software 63 10.6.5 Checking/verification of s	10	Ligonomic aspects of uesign						
10.1.1 General 53 10.1.2 Validation plan 53 10.1.3 Generic fault lists 56 10.1.4 Specific fault lists 56 10.1.5 Information for validation 56 10.2 Validation by analysis 57 10.2.1 General 57 10.2.2 Analysis techniques 58 10.3.1 General 59 10.3.3 Malditional requirements for testing 59 10.3.4 Number of test samples 59 10.3.5 Testing methods 59 10.4 Validation of the safety Requirements Specification (SRS) 60 10.5 Validation of the safety function 60 10.6 Validation of acsures against systematif failures 62 10.6.1 Validation of acsures against systematif failures 63 10.6.2 Validation of acsure samples set velocid-2-cece-theo-b67- 64 11 Maintenance 63 10.6.6 Checking /verification of safety integrify of the safety set velocid-2-cece-theo-b67- 13.1 Information for use 65 13.1	10	vanua 10.1	Validati	on principles	33			
10.12 Validation plan 55 10.13 Generic fault lists 56 10.14 Specific fault lists 56 10.15 Information for validation 56 10.21 General 57 10.22 Analysis techniques 58 10.31 General 57 10.32 Analysis techniques 58 10.32 Analysis techniques 59 10.33 Additional requirements for testing 59 10.34 Number of test samples 59 10.35 Testing methods 59 10.4 Validation of the safety integrity of the SRP/CS 61 10.61 Validation of measures against systematic failures 62 10.62 Validation of combination of subsystems 63 10.63 Validation of combination of subsystems 63 10.64 Validation of combination of subsystems 63 10.65 Checking/verification of safety/integrity 64 11 Maintenance 65 61 10.64 Validation of combination of subsystem(S) 63		1011	10.1.1	General				
10.1.3 Generic fault lists 56 10.1.4 Specific fault lists 56 10.1.5 Information for validation 56 10.2 Validation by analysis 57 10.2.1 General 57 10.2.2 Analysis techniques 58 10.3 Validation by testing 58 10.3.1 General 59 10.3.2 Measurement accuracy 59 10.3.3 Additional requirements for testing 59 10.3.4 Number of test samples 59 10.4 Validation of the Safety Requirements Specification (SRS) 60 10.5 Validation of the safety function 60 10.6 Validation of measures acainst systematic failures 62 10.6.1 Validation of subsystems 63 10.6.2 Validation of subsystems 63 10.6.3 Validation of subsystems 63 10.6.4 Validation of subsystems 63 10.6.5 Checking/verification of safety integrity 64 11 Maintenance 65 13.1 Inf			10.1.2	Validation plan				
10.1.4 Specific fault lists 56 10.1.5 Information for validation 56 10.2 Validation by analysis 57 10.2.1 General 57 10.2.2 Analysis techniques 58 10.3.3 General 58 10.3.4 General 58 10.3.4 Musta curacy 59 10.3.5 Testing methods 59 10.3.5 Testing methods 59 10.5 Validation of the safety function 60 10.6 Validation of the safety function 60 10.6.1 Validation of safety enguirements Specification (SRS) 60 10.6.2 Validation of safety enguirements of the SRP/CS 61 10.6.2 Validation of safety enguirements of the safety struction 63 10.6.3 Validation of safety enguirements of the safety struction 63 10.6.4 Validation of safety enguirements of the safety struction 64 10.6.5 Checking/verification of safety struction 64 11 Maintenance (mostify enguirements of the safety enguirements of the safety enguirements of the safety enguirem			10.1.3	Generic fault lists	56			
10.1.5 Information for validation 56 10.2 Validation by analysis 57 10.2.1 General 57 10.2.2 Analysis techniques 58 10.3.4 General 58 10.3.5 General 58 10.3.4 General 59 10.3.4 Mumber of test samples 59 10.3.5 Testing methods 59 10.3.4 Number of test samples 59 10.3.5 Testing methods 59 10.4 Validation of the safety Requirements Specification (SRS) 60 10.5 Validation of measures against systematic failures 62 10.6.1 Validation of measures against systematic failures 63 10.6.2 Validation of combination of subsystems 63 10.6.4 Validation of safety integrity 64 11 Maintenance 60 64 10.6.4 Validation of safety integrity of the Safety integrity 64 11 Maintenance 63 10.6.4 Validation of safety integrity of the safety integrity 11 Maint			10.1.4	Specific fault lists	56			
10.2 Validation by analysis 57 10.2.1 General 57 10.3 Validation by testing 58 10.3 Validation by testing 58 10.3.1 General 58 10.3.2 Measurement accuracy 59 10.3.4 Number of test samples 59 10.3.5 Testing methods 59 10.3.5 Testing methods 59 10.5 Validation of the safety Requirements Specification (SRS) 60 10.6 Validation of the safety function 60 10.6.1 Validation of combination of subsystem(S) 61 10.6.2 Validation of combination of subsystems 63 10.6.3 Validation of combination of subsystems 63 10.6.4 Validation of combination of subsystems 63 10.6.5 Checking/verification of safety integrity 64 11 Maintenance Mess395195195196046542942 64 12 Technical documentation 64 65 13.1 General 65 13.3 Information for SRP/CS integrator 65			10.1.5	Information for validation				
10.2.1 General 57 10.3 Validation by testing 58 10.3.1 General 58 10.3.2 Measurement accuracy 59 10.3.4 Weasurement accuracy 59 10.3.4 Mumber of test samples 59 10.3.4 Number of test samples 59 10.4 Validation of the safety function 60 10.6 Validation of the safety function 61 10.6.1 Validation of measures against systematic failures 62 10.6.2 Validation of measures against systematic failures 63 10.6.4 Validation of safety-flatted software 63 10.6.5 Checking/verification of safety-flatted software 63 10.6.5 Checking/verification of safety-flatted software 64 11 Maintenance (ms395) % host det 1349-1 64 12 Technical documentation 64 64 13 Information for SRP/CS integrator 65 65 13.2 Information for SRP/CS integrator 65 66 13.3 Information for SRP/CS integrator 66<		10.2	Validati	on by analysis				
10.2 Analysis techniques 58 10.3.1 General 58 10.3.2 Measurement accuracy 59 10.3.3 Additional requirements for testing 59 10.3.4 Number of test samples 59 10.3.5 Testing methods 59 10.4 Validation of the safety function 60 10.6 Validation of the safety integrity of the SRP/CS PREVIEW 61 10.6.1 Validation of measures arainst systematic failures 62 10.6.2 Validation of asfety feature of softwares 63 10.6.4 Validation of safety feature of softwares 10.6.4 Validation of safety feature of software 63 10.6.5 Checking/verification of safety functify 64 11 Maintenance Outstation of safety feature of software 65 13.1 66 11 Maintenance Outstation of safety feature of software 65 13.2 Information for use 65 13.1 General 65 13.3 Information for user 66 13.2 Information for use 65 13.3 10.6 10.6			10.2.1	General				
10.3 General 58 10.3.1 General 58 10.3.2 Measurement accuracy 59 10.3.3 Additional requirements for testing 59 10.3.4 Number of test samples 59 10.3.5 Testing methods 59 10.4 Number of test samples 59 10.5 Validation of the safety function 60 10.6 Validation of the safety function 60 10.6.1 Validation of subsystem(s) 61 10.6.2 Validation of subsystems 63 10.6.3 Validation of safety-related software 63 10.6.4 Validation of safety-related software 63 10.6.5 Checking/verification of safety-integrity 64 11 Maintenance 1000000000000000000000000000000000000		10.3	10.2.2 Validati	Analysis techniques				
10.3.2 Measurement accuracy 59 10.3.3 Additional requirements for testing 59 10.3.4 Number of test samples 59 10.3.5 Testing methods 59 10.4 Validation of the safety function 60 10.5 Validation of the safety function 60 10.6 Validation of the safety function 60 10.6.1 Validation of subsystem(S) 61 10.6.2 Validation of subsystem(S) 61 10.6.3 Validation of safety related software 63 10.6.4 Validation of safety related software 63 10.6.5 Checking/verification of safety integrity 64 11 Maintenance 65 13.1 General 65 13.1 General 65 13.2 Information for use 65 13.3 Information for sRP/CS integrator 65 13.3 Information of safety-related block diagram 72 Annex A (informative) Determination of required performance level (PL _r) 68 Annex B (informative) Simplified method for estimating MTTFD for each channel <td></td> <td>10.5</td> <td>1031</td> <td>General</td> <td></td>		10.5	1031	General				
10.3.3 Additional requirements for testing 59 10.3.4 Number of test samples 59 10.3.5 Testing methods 59 10.4 Validation of the safety Requirements Specification (SRS) 60 10.5 Validation of the safety integrity of the SRP/CS PREVIEW 61 10.6.1 Validation of measures against systematic failures 62 10.6.2 Validation of safety-related software 63 10.6.4 Validation of safety-related software 63 10.6.4 Validation of safety-related software 63 10.6.5 Checking/verification of safety-fuelds/site/de/de/de/de/de/de/de/de/de/de/de/de/de			10.3.2	Measurement accuracy				
10.3.4 Number of test samples 59 10.3.5 Testing methods 59 10.4 Validation of the safety function 60 10.5 Validation of the safety function 60 10.6 Validation of the safety function 60 10.6.1 Validation of subsystem(S) 61 10.6.2 Validation of subsystem(S) 62 10.6.3 Validation of safety related software 63 10.6.4 Validation of safety integrity 63 10.6.5 Checking/verification of safety integrity 64 11 Maintenance 0683595198/sock=13849-1 64 12 Technical documentation 64 64 13 Information for use 65 65 13.1 General 65 65 13.2 Information for SRP/CS integrator 65 13.3 Information of SRP/CS integrator 65 13.4 General 65 13.5 Information of SRP/CS integrator 65 13.6 Cherelal 72 Annex A (informative) Determination of required performance			10.3.3	Additional requirements for testing				
10.3.5 Testing methods 59 10.4 Validation of the Safety Requirements Specification (SRS) 60 10.5 Validation of the safety integrity of the SRP/CS PREVIEW 61 10.6.1 Validation of measures gazingt systematic failures 62 10.6.2 Validation of combination of subsystems 63 63 10.6.4 Validation of safety-related software 63 63 10.6.5 Checking/verification of safety integrity 64 11 Maintenance 0683395198b/scode-19849-1 64 12 Technical documentation 64 64 13 Information for use 65 65 13.1 General 65 65 13.2 Information for user 66 Annex A (informative) Determination of required performance level (PL _p) 68 Annex B (informative) Simplified method for estimating MTTF _D values for single components 74 Annex C (informative) Simplified method for estimating MTTFD for each channel 81 Annex E (informative) Systematic failure 92 Annex I (informative) Systematic failure 92 Annex K (informative) System			10.3.4	Number of test samples				
10.4 Validation of the Safety Requirements Specification (SRS) 60 10.5 Validation of the safety function 60 10.6 Validation of the safety integrity of the SRP/CS 61 10.6.1 Validation of subsystem(s) 61 10.6.2 Validation of safety-related software 63 10.6.4 Validation of safety-related software 63 10.6.5 Checking/verification of safety-integrity 64 11 Maintenance 0x83395198b/so-dk=13849-1 64 12 Technical documentation 64 64 13 Information for use 65 65 13.1 General 65 65 13.2 Information for user 66 Annex A (informative) Determination of required performance level (PL _r) 68 Annex B (informative) Block method and safety-related block diagram 72 Annex C (informative) Simplified method for estimating MTTFD for each channel 81 Annex E (informative) Simplified method for several subsystems 92 Annex G (informative) Systematic failure 92 Annex I (informative) Systematic failure 92 Annex			10.3.5	Testing methods	59			
10.5 Validation of the safety integrity of the SRP/CS 60 10.6 Validation of subsystem(s) 61 10.6.1 Validation of subsystem(s) 61 10.6.2 Validation of subsystem(s) 61 10.6.3 Validation of safety-related software 63 10.6.4 Validation of combination of subsystems 63 10.6.5 Checking/verification of safety/integrity 64 11 Maintenance 64 12 Technical documentation 64 13 Information for use 65 13.1 General 65 13.2 Information for use 65 13.3 Information of user 66 Annex A (informative) Determination of required performance level (PL _r) 68 Annex B (informative) Block method and safety-related block diagram 72 Annex C (informative) Simplified method for estimating MTTFD for each channel 81 Annex E (informative) Bestimates for diagnostic coverage (DC) for functions and modules 83 Annex G (informative) Systematic failure 92 Annex I (informative) Systematic failure 97 Annex I (informativ		10.4	Validati	on of the Safety Requirements Specification (SRS)	60			
10.6 Validation of the safety integrity of the SRP/CS_PREVIEW 61 10.6.1 Validation of subsystem(s) 61 10.6.2 Validation of measures against systematic failures 62 10.6.3 Validation of safety-related software 63 10.6.4 Validation of safety-related software 63 10.6.5 Checking/verification of safety/integrity 64 11 Maintenance 64 12 Technical documentation 64 13 Information for use 65 13.1 General 65 13.2 Information for user 65 13.3 Information for user 66 Annex A (informative) Determination of required performance level (PLr) 68 Annex D (informative) Simplified method for estimating MTTFD for each channel 81 Annex E (informative) Estimates for diagnostic coverage (DC) for functions and modules 83 Annex G (informative) Estimates for diagnostic coverage (DC) for functions and modules 83 Annex G (informative) Systematic failure 92 Annex G (informative) Example of combination of several subsystems 95 Annex I (informative) Software <t< td=""><td></td><td>10.5</td><td>Validati</td><td>on of the safety function</td><td>60</td></t<>		10.5	Validati	on of the safety function	60			
10.6.1 Validation of subsystem (s) Automatic failures 62 10.6.2 Validation of safety'-felated software 63 10.6.3 Validation of safety'-felated software 63 10.6.4 Validation of software 63 10.6.5 Checking/verification of safety'Integrity 64 Information for combination of subsystems 63 11 Maintenance 0a883595198b/so-ds-13849-1 12 Technical documentation 64 13 Information for use 65 13.1 General 65 13.2 Information for SRP/CS integrator 65 13.3 Information for user 66 Annex A (informative) Determination of required performance level (PL _r) 68 Annex D (informative) Simplified method for estimating MTTF _D values for single components 74 Annex E (informative) Simplified method for estimating MTTFD for each channel 81 Annex F (informative) Measures against common cause failures (CCF) 88 Annex G (informative) Systematic failure 92 Annex I (informative) Software 105 Annex I (informative) Software 105 <		10.6	Validati	on of the safety integrity of the SRP/CS	61			
10.6.2 Validation of measures against systematic failures 62 10.6.3 Validation of safety-related software 63 10.6.4 Validation of safety-integrity 64 10.6.5 Checking/verification of safety-integrity 64 11 Maintenance 64 12 Technical documentation 64 13 Information for use 65 13.1 General 65 13.2 Information for SRP/CS integrator 65 13.3 Information for user 66 Annex A (informative) Determination of required performance level (PL _r) 68 Annex B (informative) Block method and safety-related block diagram 72 Annex C (informative) Simplified method for estimating MTTFD for each channel 81 Annex E (informative) Simplified method for estimating MTTFD for each channel 83 Annex F (informative) Systematic failure 92 Annex I (informative) Systematic failure 92 Annex I (informative) Systematic failure 92 Annex K (informative) Software 105 Annex K (informative) Numerical representation of Figure 12 108 Annex K (informative) Numerica			10.6.1	Validation of subsystem(s)				
10.6.5 Validation of safety-related software 63 10.6.5 Validation of combination of subsystems 63 10.6.5 Checking/verification of safety/intégrifty 64 11 Maintenance 64 12 Technical documentation 64 13 Information for use 65 13.1 General 65 13.2 Information for user 65 13.3 Information for user 66 Annex A (informative) Determination of required performance level (PL _r) 68 Annex B (informative) Block method and safety-related block diagram 72 Annex C (informative) Simplified method for estimating MTTFD for each channel 81 Annex F (informative) Simplified method for estimating MTTFD for each channel 83 Annex G (informative) Systematic failure 92 Annex G (informative) Systematic failure 92 Annex I (informative) Software 105 Annex I (informative) Software 105 Annex I (informative) Software 105 Annex K (informative) Numerical representation of Figure 12 108 Annex K (informative) Numerical representation of Figure 12 108			10.6.2	Validation of measures against systematic failures				
10:0-7 validation of combination of safety/integrity 63 10:0-5 Checking/verification of safety/integrity 64 11 Maintenance 0x883595198b/iso-die-13849-1 64 12 Technical documentation 64 13 Information for use 65 13.1 General 65 13.2 Information for user 65 13.3 Information of required performance level (PL _r) 68 Annex A (informative) Determination of required performance level (PL _r) 68 Annex D (informative) Block method and safety-related block diagram 72 Annex D (informative) Simplified method for estimating MTTFD for each channel 81 Annex E (informative) Measures against common cause failures (CCF) 88 Annex G (informative) Systematic failure 92 Annex I (informative) Example of combination of several subsystems 95 Annex K (informative) Numerical representation of Figure 12 108 Annex K (informative) Software 105			10.6.3	Validation of combination of subsystems				
11 Maintenance 01 12 Technical documentation 64 12 Technical documentation 64 13 Information for use 65 13.1 General 65 13.2 Information for SRP/CS integrator 65 13.3 Information for use 65 13.1 General 65 13.2 Information for user 66 Annex A (informative) Determination of required performance level (PLr) 68 Annex B (informative) Block method and safety-related block diagram 72 Annex C (informative) Simplified method for estimating MTTFD tor each channel 81 Annex E (informative) Estimates for diagnostic coverage (DC) for functions and modules 83 Annex F (informative) Measures against common cause failures (CCF) 88 Annex I (informative) Systematic failure 92 Annex I (informative) Software 105 Annex K (informative) Numerical representation of Figure 12 108 Annex L (informative) Additional Information for Safety Requirements Specification 115 Annex N (informative) Additional Information for Safety Requirements Specification 115			10.0.4	Checking/verification of safety integrity				
11 Informatice 0x883395198b/tso-dis-13849-1 0x 12 Technical documentation 64 13 Information for use 65 13.1 General 65 13.2 Information for SRP/CS integrator 65 13.3 Information for user 65 13.3 Information of required performance level (PLr) 68 Annex A (informative) Determination of required performance level (PLr) 68 Annex B (informative) Block method and safety-related block diagram 72 Annex C (informative) Calculating or evaluating MTTF _D values for single components 74 Annex D (informative) Simplified method for estimating MTTFD for each channel 81 Annex F (informative) Estimates for diagnostic coverage (DC) for functions and modules 83 Annex G (informative) Measures against common cause failures (CCF) 88 Annex G (informative) Systematic failure 92 Annex I (informative) Example of combination of several subsystems 95 Annex I (informative) Software 105 Annex K (informative) Numerical representation of Figure 12 108 Annex L (informative) Additional Information for Safety Requirements Specification 115	11	Maint	enance	https://standards.iteh.ai/catalog/standards/sist/0ec4d0c2-c2ee-4bac-b69f-				
12 Information for use 65 13 Information for use 65 13.1 General 65 13.2 Information for SRP/CS integrator 65 13.3 Information for user 66 Annex A (informative) Determination of required performance level (PL _r) 68 Annex B (informative) Block method and safety-related block diagram 72 Annex C (informative) Simplified method for estimating MTTFD for each channel 81 Annex D (informative) Simplified method for estimating MTTFD for each channel 81 Annex F (informative) Bestimates for diagnostic coverage (DC) for functions and modules 83 Annex G (informative) Measures against common cause failures (CCF) 88 Annex G (informative) Systematic failure 92 Annex I (informative) Example of combination of several subsystems 95 Annex I (informative) Software 105 Annex K (informative) Numerical representation of Figure 12 108 Annex L (informative) Additional Information for Safety Requirements Specification 115 Annex N (informative) Avoiding of systematic failure in software-design 117	17	Techn		0x8833595198b/iso-dis-13849-1	64			
13.1 General. 65 13.2 Information for SRP/CS integrator 65 13.3 Information for user 66 Annex A (informative) Determination of required performance level (PL _r) 68 Annex B (informative) Determination of required performance level (PL _r) 68 Annex C (informative) Block method and safety-related block diagram 72 Annex C (informative) Simplified method for estimating MTTFD for each channel 81 Annex E (informative) Simplified method for estimating MTTFD for each channel 81 Annex F (informative) Bestimates for diagnostic coverage (DC) for functions and modules 83 Annex G (informative) Measures against common cause failures (CCF) 88 Annex G (informative) Systematic failure 92 Annex I (informative) Example of combination of several subsystems 95 Annex I (informative) Software 105 Annex K (informative) Numerical representation of Figure 12 108 Annex L (informative) Additional Information for Safety Requirements Specification 115 Annex N (informative) Additional Information for Safety Requirements 117	12	Information for usa						
13.1 Generation 05 13.2 Information for SRP/CS integrator 65 13.3 Information for user 66 Annex A (informative) Determination of required performance level (PL _r) 68 Annex B (informative) Block method and safety-related block diagram 72 Annex C (informative) Calculating or evaluating MTTF _D values for single components 74 Annex D (informative) Simplified method for estimating MTTFD for each channel 81 Annex E (informative) Estimates for diagnostic coverage (DC) for functions and modules 83 Annex F (informative) Measures against common cause failures (CCF) 88 Annex G (informative) Systematic failure 92 Annex I (informative) Example of combination of several subsystems 95 Annex I (informative) Software 105 Annex K (informative) Numerical representation of Figure 12 108 Annex L (informative) EMC immunity requirements 113 Annex M (informative) Additional Information for Safety Requirements Specification 115 Annex N (informative) Additional Information for Safety Requirements Specification 115	13	1110F1 12 1	Conoral	ur use				
13.3Information for user.6513.3Information for user.66Annex A (informative) Determination of required performance level (PL _r)68Annex B (informative) Block method and safety-related block diagram72Annex C (informative) Calculating or evaluating MTTF _D values for single components.74Annex D (informative) Simplified method for estimating MTTFD for each channel81Annex E (informative) Estimates for diagnostic coverage (DC) for functions and modules.83Annex F (informative) Measures against common cause failures (CCF)88Annex G (informative) Systematic failure.92Annex H (informative) Example of combination of several subsystems95Annex I (informative) Software105Annex K (informative) Numerical representation of Figure 12108Annex L (informative) EXAmples113Annex N (informative) Additional Information for Safety Requirements Specification115Annex N (informative) Avoiding of systematic failure in software-design117		13.1	Informa	ation for SRP/CS integrator				
Annex A (informative) Determination of required performance level (PL _r). 68 Annex B (informative) Block method and safety-related block diagram 72 Annex C (informative) Calculating or evaluating MTTF _D values for single components 74 Annex D (informative) Simplified method for estimating MTTFD for each channel 81 Annex E (informative) Estimates for diagnostic coverage (DC) for functions and modules 83 Annex F (informative) Measures against common cause failures (CCF) 88 Annex G (informative) Systematic failure 92 Annex I (informative) Example of combination of several subsystems 95 Annex J (informative) Software 105 Annex K (informative) Numerical representation of Figure 12 108 Annex L (informative) EMC immunity requirements 113 Annex M (informative) Additional Information for Safety Requirements Specification 115 Annex N (informative) Avoiding of systematic failure in software-design 117		13.3	Informa	ation for user				
Annex B (informative) Block method and safety-related block diagram72Annex B (informative) Calculating or evaluating MTTFD values for single components74Annex D (informative) Simplified method for estimating MTTFD for each channel81Annex E (informative) Estimates for diagnostic coverage (DC) for functions and modules83Annex F (informative) Measures against common cause failures (CCF)88Annex G (informative) Systematic failure92Annex H (informative) Example of combination of several subsystems95Annex J (informative) Software105Annex K (informative) Numerical representation of Figure 12108Annex L (informative) EMC immunity requirements113Annex N (informative) Additional Information for Safety Requirements Specification115Annex N (informative) Avoiding of systematic failure in software-design117	Annex	\mathbf{A} (info	ormative) Determination of required performance level (PL)	68			
Annex B (informative) Block method and safety-related block diagram72Annex C (informative) Calculating or evaluating MTTF _D values for single components74Annex D (informative) Simplified method for estimating MTTFD for each channel81Annex E (informative) Estimates for diagnostic coverage (DC) for functions and modules83Annex F (informative) Measures against common cause failures (CCF)88Annex G (informative) Systematic failure92Annex H (informative) Example of combination of several subsystems95Annex J (informative) Software105Annex K (informative) Numerical representation of Figure 12108Annex L (informative) EMC immunity requirements113Annex N (informative) Additional Information for Safety Requirements Specification115Annex N (informative) Avoiding of systematic failure in software-design117	Annov	\mathbf{D} (inf	ormativo) Plack method and cafety related block diagram				
Annex C (informative) Calculating or evaluating MT1Fp values for single components.74Annex D (informative) Simplified method for estimating MTTFD for each channel81Annex E (informative) Estimates for diagnostic coverage (DC) for functions and modules83Annex F (informative) Measures against common cause failures (CCF)88Annex G (informative) Systematic failure92Annex H (informative) Example of combination of several subsystems95Annex I (informative) Examples97Annex J (informative) Software105Annex K (informative) Numerical representation of Figure 12108Annex M (informative) Additional Information for Safety Requirements Specification115Annex N (informative) Avoiding of systematic failure in software-design117	Annex) Geleviating or evoluting MTTE relies for single components				
Annex D (informative) Simplified method for estimating MTTFD for each channel81Annex E (informative) Estimates for diagnostic coverage (DC) for functions and modules83Annex F (informative) Measures against common cause failures (CCF)88Annex G (informative) Systematic failure92Annex H (informative) Example of combination of several subsystems95Annex I (informative) Examples97Annex J (informative) Software105Annex K (informative) Numerical representation of Figure 12108Annex L (informative) EMC immunity requirements113Annex M (informative) Additional Information for Safety Requirements Specification115Annex N (informative) Avoiding of systematic failure in software-design117	Annex		ormative) calculating or evaluating MTTF _D values for single components				
Annex E (informative) Estimates for diagnostic coverage (DC) for functions and modules83Annex F (informative) Measures against common cause failures (CCF)88Annex G (informative) Systematic failure92Annex H (informative) Example of combination of several subsystems95Annex I (informative) Examples97Annex J (informative) Software105Annex K (informative) Numerical representation of Figure 12108Annex L (informative) EMC immunity requirements113Annex M (informative) Additional Information for Safety Requirements Specification115Annex N (informative) Avoiding of systematic failure in software-design117	Annex	D (inf	ormative) Simplified method for estimating MTTFD for each channel				
Annex F (informative) Measures against common cause failures (CCF)88Annex G (informative) Systematic failure92Annex H (informative) Example of combination of several subsystems95Annex I (informative) Examples97Annex J (informative) Software105Annex K (informative) Numerical representation of Figure 12108Annex L (informative) EMC immunity requirements113Annex M (informative) Additional Information for Safety Requirements Specification115Annex N (informative) Avoiding of systematic failure in software-design117	Annex	E (info	ormative]) Estimates for diagnostic coverage (DC) for functions and modules				
Annex G (informative) Systematic failure92Annex H (informative) Example of combination of several subsystems95Annex I (informative) Examples97Annex J (informative) Software105Annex K (informative) Numerical representation of Figure 12108Annex L (informative) EMC immunity requirements113Annex M (informative) Additional Information for Safety Requirements Specification115Annex N (informative) Avoiding of systematic failure in software-design117	Annex	F (info	ormative]) Measures against common cause failures (CCF)				
Annex H (informative) Example of combination of several subsystems95Annex I (informative) Examples97Annex J (informative) Software105Annex K (informative) Numerical representation of Figure 12108Annex L (informative) EMC immunity requirements113Annex M (informative) Additional Information for Safety Requirements Specification115Annex N (informative) Avoiding of systematic failure in software-design117	Annex	G (info	ormative) Systematic failure	92			
Annex I (informative) Examples	Annex	H (inf	ormative) Example of combination of several subsystems				
Annex J (informative) Software105Annex K (informative) Numerical representation of Figure 12108Annex L (informative) EMC immunity requirements113Annex M (informative) Additional Information for Safety Requirements Specification115Annex N (informative) Avoiding of systematic failure in software-design117	Annex	I (info	rmative)	Examples				
Annex K (informative) Numerical representation of Figure 12108Annex L (informative) EMC immunity requirements113Annex M (informative) Additional Information for Safety Requirements Specification115Annex N (informative) Avoiding of systematic failure in software-design117	Annex	J (info	rmative)	Software				
Annex L (informative) EMC immunity requirements113Annex M (informative) Additional Information for Safety Requirements Specification115Annex N (informative) Avoiding of systematic failure in software-design117	Annex	K (inf	ormative) Numerical representation of <u>Figure 12</u>				
Annex M (informative) Additional Information for Safety Requirements Specification 115 Annex N (informative) Avoiding of systematic failure in software-design 117	Annex	L (info	ormative) EMC immunity requirements				
Annex N (informative) Avoiding of systematic failure in software-design 117	Annex	M (inf	ormative	e) Additional Information for Safety Requirements Specification				
	Annex	x N (inf	ormative) Avoiding of systematic failure in software-design				

Anhang ZA (informative) Relationship between this European Standard and the essential	
requirements of EU Directive 2006/42/EC aimed to be covered	124
Bibliography	125

iTeh STANDARD PREVIEW (standards.iteh.ai)

ISO/DIS 13849-1 https://standards.iteh.ai/catalog/standards/sist/0ec4d0c2-c2ee-4bac-b69f-0a883595198b/iso-dis-13849-1

Foreword

ISO (the International Organization for Standardization) is a worldwide federation of national standards bodies (ISO member bodies). The work of preparing International Standards is normally carried out through ISO technical committees. Each member body interested in a subject for which a technical committee has been established has the right to be represented on that committee. International organizations, governmental and non-governmental, in liaison with ISO, also take part in the work. ISO collaborates closely with the International Electrotechnical Commission (IEC) on all matters of electrotechnical standardization.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular, the different approval criteria needed for the different types of ISO documents should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation of the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT), see www.iso.org/iso/foreword.html.

This document was prepared by Technical Committee ISO/TC 199, Safety of machinery.

The first edition of ISO 13849-1/was published in 1999 based/on EN 954-1:1996.69f-

0a883595198b/iso-dis-13849-1

The second edition of ISO 13849-1 was revised in 2006.

The third edition was amended and published in 2015.

This fourth edition cancels and replaces the third edition (ISO 13849-1:2015), which has been technically revised.

A list of all parts in the ISO 13849 series can be found on the ISO website.

Any feedback or questions on this document should be directed to the user's national standards body. A complete listing of these bodies can be found at <u>www.iso.org/members.html</u>.

Introduction

The structure of safety standards in the field of machinery is as follows.

- a) Type-A standards (basis standards) give basic concepts, principles for design and general aspects that can be applied to machinery.
- b) Type-B standards (generic safety standards) deal with one or more safety aspect(s), or one or more type(s) of safeguards that can be used across a wide range of machinery:
 - type-B1 standards on particular safety aspects (e.g. safety distances, surface temperature, noise);
 - type-B2 standards on safeguards (e.g. two-hands controls, interlocking devices, pressure sensitive devices, guards).
- c) Type-C standards (machinery safety standards) deal with detailed safety requirements for a particular machine or group of machines.

This part of ISO 13849 is a type-B-1 standard as stated in ISO 12100.

This document is of relevance, in particular, for the following stakeholder groups representing the market players with regard to machinery safety:

- machine manufacturers (small, medium and large enterprises);
- health and safety bodies (regulators, accident prevention organisations, market surveillance etc.).

Others can be affected by the level of machinery safety achieved with the means of the document by the above-mentioned stakeholder groups:

- machine users/employers (small, mediumand large enterprises);
- https://standards.iteh.ai/catalog/standards/sist/0ec4d0c2-c2ee-4bac-b69f machine users/employees (e.g. trade unions, organizations for people with special needs);
- service providers, e.g. for maintenance (small, medium and large enterprises);
- consumers (in case of machinery intended for use by consumers).

The above-mentioned stakeholder groups have been given the possibility to participate at the drafting process of this document.

In addition, this document is intended for standardization bodies elaborating type-C standards.

The requirements of this document can be supplemented or modified by a type-C standard.

When provisions of a type-C standard are different from those which are stated in type-A or type-B standards, the provisions of the type-C standard take precedence over the provisions of the other standards for machines that have been designed and built according to the provisions of the type-C standard.

NOTE 1 The examples and basis for most content is based on stationary machines in factory applications. However, other machines are not excluded. This document was written with the intent of being used across many machinery industries and as a basis for type-C standards developers.

This part of ISO 13849 is intended to give guidance to those involved in the design and assessment of control systems, and to Technical Committees preparing type-B2 or type-C standards.

Risk reduction according to ISO 12100:2010, Clause 6, is accomplished by applying, in the following sequence, inherently safe design measures, safeguarding and/or complementary risk reduction measures and information for use. A designer may reduce risks by risk reduction measures that can have safety functions. Parts of machinery control systems that are assigned to provide safety functions are called safety-related parts of control systems (SRP/CS). These can consist of hardware and/

ISO/DIS 13849-1:2020(E)

or software, and can either be separate from the machine control system or an integral part of it. In addition to implementing safety functions, SRP/CS can also implement operational functions.

ISO 12100 is used for risk assessment of the machine. ISO 13849-1, Annex A, can be used for the determination of the required performance level of a safety function performed by the SRP/CS, where PL_r is not specified in the applicable type-C standard.

ISO 13849-1 is relevant for the SRP/CS safety functions that are used to address risks for cases where a risk assessment conducted according to ISO 12100 has initiated a risk reduction measure (e.g. interlocking guard) that relies on a safety-related control system. In those cases, the safety-related control system has to perform a safety function. ISO 13849-1 should be used to design and evaluate the safety-related parts of the control system. Only the part of the control system that is safety-related falls under the scope of ISO 13849-1.

Figure 1 illustrates the relationship between ISO 12100 and ISO 13849-1.



NOTE 2 See also ISO/TR 22100-2:2013 for further information.

Figure 1 — Integration of ISO 13849-1 within the risk reduction process of ISO 12100

NOTE 3 Figure 1 shows where the SRP/CS contributes to the risk reduction process of ISO 12100: Step 2. The SRP/CS supports the combined risk reduction measures by the implementation of safety functions.

The ability of safety-related parts of control systems to perform a safety function under foreseeable conditions is allocated one of five levels, called performance levels (PL). The required performance level (PLr) for a particular safety function will be determined by risk estimation.

The probability of dangerous failure of the safety function depends on several factors, including hardware and software structure, the extent of fault detection mechanisms [diagnostic coverage (DC)], reliability of components [mean time to dangerous failure ($MTTF_D$), common cause failure (CCF)], design process, operating stress, environmental conditions and operation procedures.

Functional safety includes a categorization of architecture according to specific design and specified behaviours under fault conditions. This architecture is allocated one of five categories B, 1, 2, 3 and 4.

Functional safety considers the failure characteristics of elements/components performing a safety function. For each safety function, this failure characteristic is expressed as the probability of dangerous failure per hour (PFH_D).

Risk estimation will show a variance because of the subjective nature of the evaluation criteria. Type-C standards can have more specific risk estimation methods for specific machine applications, which can be less subjective in nature. Therefore, using the methodology in this document should be considered as valuable guidance for the design of the safety-related parts of the control system rather than a strict requirement. The performance levels and categories can be applied to safety-related parts of control systems, such as

- control units (e.g. a logic unit for control functions, data processing, monitoring, etc.) and
- electro-sensitive protective devices (e.g. photoelectric barriers), pressure sensitive devices.

The performance levels can be calculated, and categories determined for

- SRP/CS performing safety functions for machinery,
- subsystems of SRP/CS using safety parts (components) such as
- protective devices (e.g. two-hand control devices, interlocking devices);
- power control elements (e.g. relays, valves);
- Sensors and HMI elements (position sensors, enable switches).

Machinery considered by this standard can range from simple (e.g., small kitchen machines, or automatic doors and gates) to complex (e.g., packaging machines, printing machines, presses).

IEC 62061 and this part of ISO 13849 both specify a methodology and provide related guidance for the design and implementation of safety-related control systems of machinery.

NOTE ISO/TR 23849 gives guidance on the relation between both standards, how they complement each other.

The requirements of Clause 10 of ISO 13849-15 supersede the requirements of ISO 13849-2:2012 with the exception of the informative lannexes An SRP/CS that meets the requirements of Clause 10 is considered to meet the requirements of ISO 13849-2:2012.

iTeh STANDARD PREVIEW (standards.iteh.ai)

ISO/DIS 13849-1 https://standards.iteh.ai/catalog/standards/sist/0ec4d0c2-c2ee-4bac-b69f-0a883595198b/iso-dis-13849-1

Safety of machinery — Safety-related parts of control systems —

Part 1: General principles for design

1 Scope

This part of ISO 13849 specifies a methodology and provides related guidance for the design and integration of safety-related parts of control systems (SRP/CS), including the design of software. This document specifies the characteristics needed to determine the performance level required of safety functions. This document applies to SRP/CS for high demand and continuous mode including their subsystems, regardless of the type of technology and energy (e.g. electrical, hydraulic, pneumatic, mechanical), for many kinds of machinery. The standard does not apply to low demand mode.

This document does not specify the safety functions or required performance levels that are to be used in particular applications.

This document does not give specific requirements for the design of products that are parts of SRP/CS.

This document does not provide specific measures for security (e.g. physical, IT-security, cyber security) aspects.

NOTE 1 This document specifies a methodology for SBP/CS design without considering if certain machinery (e.g. mobile machinery) requires specific requirements. These specific requirements can be considered in a Type-C standard. 0a883595198b/iso-dis-13849-1

NOTE 2 See IEC 61508 for low demand mode.

NOTE 3 See also ISO/TR 22100-4 for IT-security aspects and IEC/TR 63074 for security aspects.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO 12100:2010, Safety of machinery — General principles for design — Risk assessment and risk reduction

ISO 13849-2:2013, Safety of machinery — Safety-related parts of control systems — Part 2: Validation

IEC 60204-1:2016, Safety of machinery — Electrical equipment of machines — Part 1: General requirements

IEC 61508-3:2010, Functional safety of electrical/electronic/programmable electronic safety-related systems — Part 3: Software requirements

IEC 62046:2018, Safety of machinery — Application of protective equipment to detect the presence of persons

ISO 62061:2015, Safety of machinery — Functional safety of safety-related electrical, electronic and programmable electronic control systems

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO 12100 and the following apply.

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

- IEC Electropedia: available at http://www.electropedia.org/
- ISO Online browsing platform: available at <u>https://www.iso.org/obp</u>

3.1 Terms and definitions

3.1.1

safety-related part of a control system SRP/CS

part of a control system that performs a safety function, starting from safety-related input(s) to generating safety-related output(s)

Note 1 to entry: The safety-related parts of a control system starts at the point where the safety-related inputs are initiated (including, for example, the actuating cam and the roller of the position switch) and end at the output of the power control elements (including, for example, the main contacts of a contactor).

3.1.2

safety requirement specification SRS

specification containing the requirements for the safety functions that have to be performed by the safety related control system in terms of characteristics of the safety functions (functional requirements) and required performance levels

[SOURCE: IEC 61508-4:2010, 3:5.11 and 3:5.12, modified, NOTE added]

3.1.3 category

(standards.iteh.ai)

classification of the subsystem in respect of the resistance to faults and the subsequent behaviour in the fault condition which is achieved by the structural arrangement of the parts, fault detection and/or by their reliability

0a883595198b/iso-dis-13849-1

3.1.4

fault

state of a device characterized by the inability to perform a required function, excluding the inability during preventive maintenance or other planned actions, or due to lack of external resources

Note 1 to entry: A fault is often the result of a failure of the item itself, but can exist without prior failure.

Note 2 to entry: In this part of ISO 13849-1, "fault" means random fault or fault caused by a systematic failure.

[SOURCE: IEC 60050-192:2015; modified: NOTE 2 to entry amended]

3.1.5

fault exclusion

exclusion of certain faults within an SRP/CS, if this can be justified due to their improbability and their negligible contribution to the reliability of the SRP/CS

3.1.6 failure

termination of the ability of a device to perform a required function

Note 1 to entry: After a failure, the device has a fault.

Note 2 to entry: "Failure" is an event, as distinguished from "fault", which is a state.

Note 3 to entry: Failures which only affect the availability of the process under control are outside of the scope of this part of ISO 13849.

[SOURCE: IEC 60050-192:2015; modified: NOTE 4 to entry amended]

3.1.7

dangerous failure

failure which has the potential to put the SRP/CS in a hazardous or fail-to-function state

Note 1 to entry: Whether or not the potential is realized can depend on the channel architecture of the system; in redundant systems a dangerous hardware failure is less likely to lead to the overall dangerous or fail-to-function state.

[SOURCE: IEC 61508-4:2010, 3.6.7]

3.1.8 common cause failure CCF

failure, that is the result of one or more events, causing concurrent failures of two or more separate channels in a multiple channel subystem, leading to failure of a safety function

Note 1 to entry: Common cause failures should not be confused with common mode failures (see ISO 12100:2010, 3.36).

[SOURCE: IEC 61508-4:2010]

3.1.9

systematic failure

failure related in a deterministic way to a certain cause, which can only be eliminated by a modification of the design or of the manufacturing process, operational procedures, documentation or other relevant factors

iTeh STANDARD PREVIEW

Note 1 to entry: Corrective maintenance without modification will usually not eliminate the failure cause.

(standards.iteh.ai)

Note 2 to entry: A systematic failure can be induced by simulating the failure cause.

Note 3 to entry: Examples of causes of systematic failures include human error in

https://standards.iteh.ai/catalog/standards/sist/0ec4d0c2-c2ee-4bac-b69f-

- the safety requirements specification 3595198b/iso-dis-13849-1
- the design, manufacture, installation, operation of the hardware, and
- the design, implementation, etc., of the software.

[SOURCE: IEC 60050-192:2015]

3.1.10 muting

temporary automatic suspension of a safety function(s) by the SRP/CS

3.1.11

manual reset

safety function within the SRP/CS used to restore manually one or more safety functions before restarting a machine

3.1.12 harm

physical injury or damage to health

[SOURCE: ISO 12100:2010, 3.5]

3.1.13 hazard potential source of harm

Note 1 to entry: A hazard can be qualified in order to define its origin (e.g. mechanical hazard, electrical hazard) or the nature of the potential harm (e.g. electric shock hazard, cutting hazard, toxic hazard and fire hazard).

Note 2 to entry: The hazard envisaged in this definition:

- either is permanently present during the intended use of the machine (e.g. motion of hazardous moving elements, electric arc during a welding phase, unhealthy posture, noise emission, high temperature);
- or can appear unexpectedly (e.g. explosion, crushing hazard as a consequence of an unintended/unexpected start-up, ejection as a consequence of a breakage, fall as a consequence of acceleration/deceleration).

[SOURCE: ISO 12100:2010, 3.6, modified, Note 3 deleted]

3.1.14

hazardous situation

circumstance in which a person is exposed to at least one hazard

Note 1 to entry: The exposure can result in harm immediately or over a period of time.

[SOURCE: ISO 12100:2010, 3.10]

3.1.15

risk

combination of the probability of occurrence of harm and the severity of that harm

[SOURCE: ISO 12100:2010, 3.12]

3.1.16

residual risk

risk remaining after risk reduction measures (protective measures) have been taken

Note 1 to entry: See Figure 2.

iTeh STANDARD PREVIEW [SOURCE: ISO 12100:2010, 3.13, Note 1 modified] (standards.iteh.ai)

3.1.17

risk assessment ISO/DIS 13849-1

overall process comprising risk/analysis and risk evaluationst/0ec4d0c2-c2ee-4bac-b69f-

[SOURCE: ISO 12100:2010, 3.17]

0a883595198b/iso-dis-13849-1

3.1.18

risk analysis combination of the specification of the limits of the machine, hazard identification and risk estimation

[SOURCE: ISO 12100:2010, 3.15]

3.1.19

risk evaluation

judgement, on the basis of risk analysis, of whether risk reduction objectives have been achieved

[SOURCE: ISO 12100:2010, 3.16]

3.1.20

intended use of a machine use of the machine in accordance with the information provided in the instructions for use

[SOURCE: ISO 12100:2010, 3.23]

3.1.21

reasonably foreseeable misuse

use of a machine in a way not intended by the designer, but which can result from readily predictable human behaviour

[SOURCE: ISO 12100:2010, 3.24]

3.1.22 safety function

function of the machine whose failure can result in an immediate increase of the risk(s)

Note 1 to entry: A safety function is a function to be implemented by a safety-related part of a control system, which is needed to achieve or maintain a safe state for the machine, in respect of a specific hazardous event.

[SOURCE: ISO 12100:2010, 3.30]

3.1.23 monitoring

diamastia maasuna which datasta a a

diagnostic measure which detects a state and compares it to the expected value

Note 1 to entry: Monitoring is realised by following methods: plausibility check (direct or indirect monitoring), cyclic test stimulus or cross monitoring

3.1.24

cross monitoring

diagnostic measure which checks plausibility of redundant signals in both channels of a redundant logic unit

3.1.25

programmable electronic system PE system

system for control, protection or monitoring based on one or more programmable electronic devices, including all elements of the system such as power supplies, sensors and other input devices, data highways and other communication paths, and actuators and other output devices

[SOURCE: IEC 61508-4:2010, 3.3(standards.iteh.ai)

3.1.26

<u>ISO/DIS 13849-1</u>

performance level_{https://standards.iteh.ai/catalog/standards/sist/0ec4d0c2-c2ee-4bac-b69f-PL}

PL 0a883595198b/iso-dis-13849-1 discrete level used to specify the ability of safety-related parts of control systems to perform a safety function under foreseeable conditions

Note 1 to entry: See <u>6.1</u>.

3.1.27 required performance level PL.

performance level (PL) applied in order to achieve the required risk reduction for each safety function

Note 1 to entry: See Figure 2 and Figure A.1.

3.1.28 mean time to dangerous failure

MTTF_D expected value of time to dangerous failure

Note 1 to entry: In the case of items with an exponential distribution of operating times to dangerous failure (i.e. a constant failure rate) the MTTF D is numerically equal to the reciprocal of the dangerous failure rate".

[SOURCE: IEC 62061:2005, 3.2.34, NOTE 1 to entry modified]

3.1.29 mean time between failure MTBF

expected value of the operating time between consecutive failures