

DIN EN ISO 13849-1:2023-12 (E)

Safety of machinery - Safety-related parts of control systems - Part 1: General principles for design (ISO 13849-1:2023)

Contents		Page
European foreword.....		5
Annex ZA (informative) Relationship between this European Standard and the essential requirements of EU Directive 2006/42/EC aimed to be covered.....		6
Foreword.....		8
Introduction.....		10
1	Scope.....	13
2	Normative references.....	13
3	Terms, definitions, symbols and abbreviated terms.....	14
	3.1 Terms and definitions.....	14
	3.2 Symbols and abbreviated terms.....	22
4	Overview.....	24
	4.1 Risk assessment and risk reduction process at the machine.....	24
	4.2 Contribution to the risk reduction.....	26
	4.3 Design process of an SRP/CS.....	26
	4.4 Methodology.....	27
	4.5 Required information.....	28
	4.6 Safety function realization by using subsystems.....	29
5	Specification of safety functions.....	29
	5.1 Identification and general description of the safety function.....	29
	5.2 Safety requirements specification.....	30
	5.2.1 General requirements.....	30
	5.2.2 Requirements for specific safety functions.....	33
	5.2.3 Minimizing motivation to defeat safety functions.....	36
	5.2.4 Remote access.....	37
	5.3 Determination of required performance level (PL _r) for each safety function.....	37
	5.4 Review of the safety requirements specification (SRS).....	38
	5.5 Decomposition of SRP/CS into subsystems.....	38
6	Design considerations.....	39
	6.1 Evaluation of the achieved performance level.....	39
	6.1.1 General overview of performance level.....	39
	6.1.2 Correlation between performance level (PL) and safety integrity level (SIL).....	41
	6.1.3 Architecture — Categories and their relation to MTTF _D of each channel, average diagnostic coverage and common cause failure (CCF).....	41
	6.1.4 Mean time to dangerous failure (MTTF _D).....	48
	6.1.5 Diagnostic coverage (DC).....	49
	6.1.6 Common cause failures (CCFs).....	50
	6.1.7 Systematic failures.....	50
	6.1.8 Simplified procedure for estimating the performance level for subsystems.....	51
	6.1.9 Alternative procedure to determine the performance level and PFH without MTTF _D	52
	6.1.10 Fault consideration and fault exclusion.....	54
	6.1.11 Well-tried component.....	55
	6.2 Combination of subsystems to achieve an overall performance level of the safety function.....	55

6.2.1	General	55
6.2.2	Known PFH values	55
6.2.3	Unknown PFH values	56
6.3	Software based manual parameterization	56
6.3.1	General	56
6.3.2	Influences on safety-related parameters	57
6.3.3	Requirements for software based manual parameterization	58
6.3.4	Verification of the parameterization tool	59
6.3.5	Documentation of software based manual parameterization	59
7	Software safety requirements	59
7.1	General	59
7.2	Limited variability language (LVL) and full variability language (FVL)	61
7.2.1	Limited variability language (LVL)	61
7.2.2	Full variability language (FVL)	61
7.2.3	Decision for limited variability language (LVL) or full variability language (FVL)	61
7.3	Safety-related embedded software (SRESW)	63
7.3.1	Design of safety-related embedded software (SRESW)	63
7.3.2	Alternative procedures for non-accessible embedded software	64
7.4	Safety-related application software (SRASW)	64
8	Verification of the achieved performance level	67
9	Ergonomic aspects of design	67
10	Validation	67
10.1	Validation principles	67
10.1.1	General	67
10.1.2	Validation plan	69
10.1.3	Generic fault lists	70
10.1.4	Specific fault lists	70
10.1.5	Information for validation	70
10.2	Validation of the safety requirements specification (SRS)	71
10.3	Validation by analysis	72
10.3.1	General	72
10.3.2	Analysis techniques	72
10.4	Validation by testing	72
10.4.1	General	72
10.4.2	Measurement accuracy	73
10.4.3	Additional requirements for testing	74
10.4.4	Number of test samples	74
10.4.5	Testing methods	74
10.5	Validation of the safety functions	75
10.6	Validation of the safety integrity of the SRP/CS	75
10.6.1	Validation of subsystem(s)	75
10.6.2	Validation of measures against systematic failures	76
10.6.3	Validation of safety-related software	77
10.6.4	Validation of combination of subsystems	78
10.6.5	Overall validation of safety integrity	78
10.7	Validation of environmental requirements	78
10.8	Validation record	79
10.9	Validation maintenance requirements	79
11	Maintainability of SRP/CS	79
12	Technical documentation	80
13	Information for use	80
13.1	General	80
13.2	Information for SRP/CS integration	80
13.3	Information for user	81

Annex A (informative) Guidance for the determination of required performance level (PL_r)	83
Annex B (informative) Block method and safety-related block diagram	88
Annex C (informative) Calculating or evaluating MTTF_D values for single components	90
Annex D (informative) Simplified method for estimating MTTF_D for each channel	98
Annex E (informative) Estimates for diagnostic coverage (DC) for functions and subsystems ..	100
Annex F (informative) Method for quantification of measures against common cause failures (CCF)	104
Annex G (informative) Systematic failure	108
Annex H (informative) Example of a combination of several subsystems	112
Annex I (informative) Examples for the simplified procedure to estimate the PL of subsystems	115
Annex J (informative) Example of SRESW realisation	123
Annex K (informative) Numerical representation of Figure 12	127
Annex L (informative) Electromagnetic interference (EMI) immunity	132
Annex M (informative) Additional information for safety requirements specification (SRS)	136
Annex N (informative) Avoiding systematic failure in software design	138
Annex O (informative) Safety-related values of components or parts of control systems	158
Bibliography	161