

DIN EN ISO 13849-1:2008-12 (E)

Safety of machinery - Safety-related parts of control systems - Part 1: General principles for design (ISO 13849-1:2006)

Contents		Page
Foreword		4
Introduction		5
1	Scope	7
2	Normative references	7
3	Terms, definitions, symbols and abbreviated terms	8
3.1	Terms and definitions	8
3.2	Symbols and abbreviated terms	14
4	Design considerations	15
4.1	Safety objectives in design	15
4.2	Strategy for risk reduction	17
4.2.1	General	17
4.2.2	Contribution to the risk reduction by the control system	17
4.3	Determination of required performance level (PLr)	20
4.4	Design of SRP/CS	20
4.5	Evaluation of the achieved performance level PL and relationship with SIL	21
4.5.1	Performance level PL	21
4.5.2	Mean time to dangerous failure of each channel (MTTFd)	23
4.5.3	Diagnostic coverage (DC)	24
4.5.4	Simplified procedure for estimating PL	24
4.6	Software safety requirements	27
4.6.1	General	27
4.6.2	Safety-related embedded software (SRESW)	27
4.6.3	Safety-related application software (SRASW)	28
4.6.4	Software-based parameterization	31
4.7	Verification that achieved PL meets PLr	32
4.8	Ergonomic aspects of design	32
5	Safety functions	32
5.1	Specification of safety functions	32
5.2	Details of safety functions	34
5.2.1	Safety-related stop function	34
5.2.2	Manual reset function	35
5.2.3	Start/restart function	35
5.2.4	Local control function	36
5.2.5	Muting function	36
5.2.6	Response time	36
5.2.7	Safety-related parameters	36
5.2.8	Fluctuations, loss and restoration of power sources	37
6	Categories and their relation to MTTFd of each channel, DCavg and CCF	37
6.1	General	37
6.2	Specifications of categories	38
6.2.1	General	38
6.2.2	Designated architectures	38
6.2.3	Category B	38
6.2.4	Category 1	39

6.2.5	Category 2	40
6.2.6	Category 3	41
6.2.7	Category 4	42
6.3	Combination of SRP/CS to achieve overall PL	45
7	Fault consideration, fault exclusion	46
7.1	General	46
7.2	Fault consideration	46
7.3	Fault exclusion	47
8	Validation	47
9	Maintenance	47
10	Technical documentation	47
11	Information for use	48
Annex A (informative) Determination of required performance level (PLr)		50
Annex B (informative) Block method and safety-related block diagram		53
Annex C (informative) Calculating or evaluating MTTFd values for single components		55
Annex D (informative) Simplified method for estimating MTTFd for each channel		63
Annex E (informative) Estimates for diagnostic coverage (DC) for functions and modules		65
Annex F (informative) Estimates for common cause failure (CCF)		68
Annex G (informative) Systematic failure		70
Annex H (informative) Example of combination of several safety-related parts of the control system		73
Annex I (informative) Examples		76
Annex J (informative) Software		83
Annex K (informative) Numerical representation of Figure 5		86
Annex ZA (informative) Relationship between this European Standard and the Essential Requirements of EU Directive 98/37/EC, amended by Directive 98/79/EC		89
Annex ZB (informative) Relationship between this European Standard and the Essential Requirements of EU Directive 2006/42/EC		90
Bibliography		91