

Contents

	Page
Foreword	v
Introduction	vi
1 Scope	1
2 Normative references	1
3 Terms, definitions, symbols and abbreviated terms	2
3.1 Terms and definitions.....	2
3.2 Symbols and abbreviated terms.....	7
4 Design considerations	9
4.1 Safety objectives in design.....	9
4.2 Strategy for risk reduction.....	11
4.2.1 General.....	11
4.2.2 Contribution to the risk reduction by the control system.....	11
4.3 Determination of required performance level (PL _r).....	13
4.4 Design of SRP/CS.....	14
4.5 Evaluation of the achieved performance level PL and relationship with SIL.....	15
4.5.1 Performance level PL.....	15
4.5.2 Mean time to dangerous failure of each channel (MTTF _D).....	16
4.5.3 Diagnostic coverage (DC).....	17
4.5.4 Simplified procedure for estimating the quantifiable aspects of PL.....	17
4.5.5 Description of the output part of the SRP/CS by category.....	19
4.6 Software safety requirements.....	20
4.6.1 General.....	20
4.6.2 Safety-related embedded software (SRESW).....	21
4.6.3 Safety-related application software (SRASW).....	22
4.6.4 Software-based parameterization.....	24
4.7 Verification that achieved PL meets PL _r	25
4.8 Ergonomic aspects of design.....	26
5 Safety functions	26
5.1 Specification of safety functions.....	26
5.2 Details of safety functions.....	28
5.2.1 Safety-related stop function.....	28
5.2.2 Manual reset function.....	29
5.2.3 Start/restart function.....	29
5.2.4 Local control function.....	30
5.2.5 Muting function.....	30
5.2.6 Response time.....	30
5.2.7 Safety-related parameters.....	30
5.2.8 Fluctuations, loss and restoration of power sources.....	30
6 Categories and their relation to MTTF_D of each channel, DC_{avg} and CCF	31
6.1 General.....	31
6.2 Specifications of categories.....	31
6.2.1 General.....	31
6.2.2 Designated architectures.....	32
6.2.3 Category B.....	32
6.2.4 Category 1.....	33
6.2.5 Category 2.....	34
6.2.6 Category 3.....	35
6.2.7 Category 4.....	36
6.3 Combination of SRP/CS to achieve overall PL.....	38
7 Fault consideration, fault exclusion	40
7.1 General.....	40
7.2 Fault consideration.....	40

7.3	Fault exclusion.....	40
8	Validation.....	40
9	Maintenance.....	40
10	Technical documentation.....	41
11	Information for use.....	41
Annex A	(informative) Determination of required performance level (PL_r).....	43
Annex B	(informative) Block method and safety-related block diagram.....	47
Annex C	(informative) Calculating or evaluating MTTF_D values for single components.....	49
Annex D	(informative) Simplified method for estimating MTTF_D for each channel.....	56
Annex E	(informative) Estimates for diagnostic coverage (DC) for functions and modules.....	58
Annex F	(informative) Estimates for common cause failure (CCF).....	61
Annex G	(informative) Systematic failure.....	63
Annex H	(informative) Example of combination of several safety-related parts of the control system.....	66
Annex I	(informative) Examples.....	69
Annex J	(informative) Software.....	76
Annex K	(informative) Numerical representation of Figure 5.....	79
Bibliography	84