ISO 13849-1:2023-04 (E)

Safety of machinery - Safety-related parts of control systems - Part 1: General principles for design

Contents

Page

Foreword vi

Introduction viii

1 Scope 1

2 Normative references 1

3 Terms,definitions,symbolsandabbreviatedterms 2
3.1 Terms and definitions 2
3.2 Symbols and abbreviated terms 10

4 Overview 12
4.1 Risk assessment and risk reduction process at the machine 12
4.2 Contribution to the risk reduction 14
4.3 Design process of an SRP/CS 14
4.4 Methodology 15
4.5 Required information 16
4.6 Safety function realization by using subsystems 17

5 Specificationofsafetyfunctions 17
5.1 Identification and general description of the safety function 17
5.2 Safety requirements specification 18
5.2.1 General requirements 18
5.2.2 Requirements for specific safety functions 21
5.2.3 Minimizing motivation to defeat safety functions 24
5.2.4 Remote access 25
5.3 Determination of required performance level (PLr) for each safety function 25
5.4 Review of the safety requirements specification (SRS) 26
5.5 Decomposition of SRP/CS into subsystems 26

6 Design considerations 27
6.1 Evaluation of the achieved performance level 27
6.1.1 General overview of performance level 27
6.1.2 Correlation between performance level (PL) and safety integrity level (SIL) 29
6.1.3 Architecture -- Categories and their relation to MTTFD of each channel, average diagnostic coverage and common cause failure (CCF) 29
6.1.4 Mean time to dangerous failure (MTTFD) 36
6.1.5 Diagnostic coverage (DC) 37
6.1.6 Common cause failures (CCFs) 38
6.1.7 Systematic failures 38
6.1.8 Simplified procedure for estimating the performance level for subsystems 39
6.1.9 Alternative procedure to determine the performance level and PFH without MTTFD 40
6.1.10 Fault consideration and fault exclusion 42
6.1.11 Well-tried component 43
6.2 Combination of subsystems to achieve an overall performance level of the safety function 43
6.2.1 General 43
6.2.2 Known PFH values 43
6.2.3 Unknown PFH values 44
6.3 Software based manual parameterization 44

6.3.1 General ... 44
6.3.2 Influences on safety-related parameters ... 45
6.3.3 Requirements for software based manual parameterization ... 46
6.3.4 Verification of the parameterization tool ... 47
6.3.5 Documentation of software based manual parameterization ... 47

7 Software safety requirements ... 47
7.1 General ... 47
7.2 Limited variability language (LVL) and full variability language (FVL) ... 49
7.2.1 Limited variability language (LVL) ... 49
7.2.2 Full variability language (FVL) ... 49
7.2.3 Decision for limited variability language (LVL) or full variability language (FVL) ... 49
7.3 Safety-related embedded software (SRESW) ... 51
7.3.1 Design of safety-related embedded software (SRESW) ... 51
7.3.2 Alternative procedures for non-accessible embedded software ... 52
7.4 Safety-related application software (SRASW) ... 52

8 Verificationoftheachievedperformancelevel ... 55

9 Ergonomic aspects of design ... 55

10 Validation ... 55
10.1 Validation principles ... 55
10.1.1 General ... 55
10.1.2 Validation plan ... 57
10.1.3 Generic fault lists ... 58
10.1.4 Specific fault lists ... 58
10.1.5 Information for validation ... 58
10.2 Validation of the safety requirements specification (SRS) ... 59
10.3 Validation by analysis ... 60
10.3.1 General ... 60
10.3.2 Analysis techniques ... 60
10.4 Validation by testing ... 60
10.4.1 General ... 60
10.4.2 Measurement accuracy ... 61
10.4.3 Additional requirements for testing ... 62
10.4.4 Number of test samples ... 62
10.4.5 Testing methods ... 62
10.5 Validation of the safety functions ... 63
10.6 Validation of the safety integrity of the SRP/CS ... 63
10.6.1 Validation of subsystem(s) ... 63
10.6.2 Validation of measures against systematic failures ... 64
10.6.3 Validation of safety-related software ... 65
10.6.4 Validation of combination of subsystems ... 66
10.6.5 Overall validation of safety integrity ... 66
10.7 Validation of environmental requirements ... 66
10.8 Validation record ... 67
10.9 Validation maintenance requirements ... 67

11 MaintainabilityofSRP/CS ... 67

12 Technical documentation ... 68

13 Information for use ... 68
13.1 General ... 68
13.2 Information for SRP/CS integration ... 68
13.3 Information for user ... 69

Annex A (informative) Guidance for the determination of required performance level (PLr) ... 71

Annex B (informative)Blockmethodandsafety-relatedblockdiagram ... 76

Annex C (informative) Calculating or evaluating MTTFD values for single components 78

Annex D (informative) Simplified method for estimating MTTFD for each channel 86

Annex E (informative) Estimates for diagnostic coverage (DC) for functions and subsystems 88

Annex F (informative) Method for quantification of measures against common cause failures (CCF) 92

Annex G (informative) Systematic failure 96

Annex H (informative) Example of a combination of several subsystems 100

Annex I (informative) Examples for the simplified procedure to estimate the PL of subsystems 103

Annex J (informative) Example of SRESW realisation 111

Annex K (informative) Numerical representation of Figure 12 115

Annex L (informative) Electromagnetic interference (EMI) immunity 120

Annex M (informative) Additional information for safety requirements specification (SRS) 124

Annex N (informative) Avoiding systematic failure in software design 126

Annex O (informative) Safety-related values of components or parts of control systems 146

Bibliography 149