

# ISO 13849-1:2006-11 (E)

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

---

<b>Contents</b>		<b>Page</b>
Foreword .....		v
Introduction .....		vi
<b>1</b>	<b>Scope .....</b>	<b>1</b>
<b>2</b>	<b>Normative references .....</b>	<b>1</b>
<b>3</b>	<b>Terms, definitions, symbols and abbreviated terms .....</b>	<b>2</b>
3.1	Terms and definitions .....	2
3.2	Symbols and abbreviated terms .....	8
<b>4</b>	<b>Design considerations .....</b>	<b>9</b>
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 (PLr) .....	14
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 (MTTFd) .....	17
4.5.3	Diagnostic coverage (DC) .....	18
4.5.4	Simplified procedure for estimating PL .....	18
4.6	Software safety requirements .....	21
4.6.1	General .....	21
4.6.2	Safety-related embedded software (SRESW) .....	21
4.6.3	Safety-related application software (SRASW) .....	22
4.6.4	Software-based parameterization .....	25
4.7	Verification that achieved PL meets PLr .....	26
4.8	Ergonomic aspects of design .....	26
<b>5</b>	<b>Safety functions .....</b>	<b>26</b>
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 .....	31
<b>6</b>	<b>Categories and their relation to MTTFd of each channel, DCavg and CCF .....</b>	<b>31</b>
6.1	General .....	31
6.2	Specifications of categories .....	32
6.2.1	General .....	32
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 .....	39
7	Fault consideration, fault exclusion .....	40
7.1	General .....	40
7.2	Fault consideration .....	40
7.3	Fault exclusion .....	41
8	Validation .....	41
9	Maintenance .....	41
10	Technical documentation .....	41
11	Information for use .....	42
Annex A (informative) Determination of required performance level (PLr) .....		44
Annex B (informative) Block method and safety-related block diagram .....		47
Annex C (informative) Calculating or evaluating MTTFd values for single components .....		49
Annex D (informative) Simplified method for estimating MTTFd for each channel .....		57
Annex E (informative) Estimates for diagnostic coverage (DC) for functions and modules .....		59
Annex F (informative) Estimates for common cause failure (CCF) .....		62
Annex G (informative) Systematic failure .....		64
Annex H (informative) Example of combination of several safety-related parts of the control system .....		67
Annex I (informative) Examples .....		70
Annex J (informative) Software .....		77
Annex K (informative) Numerical representation of Figure 5 .....		80
Bibliography .....		83