

# ISO 13849-1:2015-12 (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>
<b>3.1</b>	<b>Terms and definitions .....</b>	<b>2</b>
<b>3.2</b>	<b>Symbols and abbreviated terms .....</b>	<b>7</b>
<b>4</b>	<b>Design considerations .....</b>	<b>9</b>
<b>4.1</b>	<b>Safety objectives in design .....</b>	<b>9</b>
<b>4.2</b>	<b>Strategy for risk reduction .....</b>	<b>11</b>
<b>4.2.1</b>	<b>General .....</b>	<b>11</b>
<b>4.2.2</b>	<b>Contribution to the risk reduction by the control system .....</b>	<b>11</b>
<b>4.3</b>	<b>Determination of required performance level (PLr) .....</b>	<b>13</b>
<b>4.4</b>	<b>Design of SRP/CS .....</b>	<b>14</b>
<b>4.5</b>	<b>Evaluation of the achieved performance level PL and relationship with SIL .....</b>	<b>15</b>
<b>4.5.1</b>	<b>Performance level PL .....</b>	<b>15</b>
<b>4.5.2</b>	<b>Mean time to dangerous failure of each channel (MTTFD) .....</b>	<b>16</b>
<b>4.5.3</b>	<b>Diagnostic coverage (DC) .....</b>	<b>17</b>
<b>4.5.4</b>	<b>Simplified procedure for estimating the quantifiable aspects of PL .....</b>	<b>17</b>
<b>4.5.5</b>	<b>Description of the output part of the SRP/CS by category .....</b>	<b>19</b>
<b>4.6</b>	<b>Software safety requirements .....</b>	<b>20</b>
<b>4.6.1</b>	<b>General .....</b>	<b>20</b>
<b>4.6.2</b>	<b>Safety-related embedded software (SRESW) .....</b>	<b>21</b>
<b>4.6.3</b>	<b>Safety-related application software (SRASW) .....</b>	<b>22</b>
<b>4.6.4</b>	<b>Software-based parameterization .....</b>	<b>24</b>
<b>4.7</b>	<b>Verification that achieved PL meets PLr .....</b>	<b>25</b>
<b>4.8</b>	<b>Ergonomic aspects of design .....</b>	<b>26</b>
<b>5</b>	<b>Safety functions .....</b>	<b>26</b>
<b>5.1</b>	<b>Specification of safety functions .....</b>	<b>26</b>
<b>5.2</b>	<b>Details of safety functions .....</b>	<b>28</b>
<b>5.2.1</b>	<b>Safety-related stop function .....</b>	<b>28</b>
<b>5.2.2</b>	<b>Manual reset function .....</b>	<b>29</b>
<b>5.2.3</b>	<b>Start/restart function .....</b>	<b>29</b>
<b>5.2.4</b>	<b>Local control function .....</b>	<b>30</b>
<b>5.2.5</b>	<b>Muting function .....</b>	<b>30</b>
<b>5.2.6</b>	<b>Response time .....</b>	<b>30</b>
<b>5.2.7</b>	<b>Safety-related parameters .....</b>	<b>30</b>
<b>5.2.8</b>	<b>Fluctuations, loss and restoration of power sources .....</b>	<b>30</b>
<b>6</b>	<b>Categories and their relation to MTTFD of each channel, DCavg and CCF .....</b>	<b>31</b>
<b>6.1</b>	<b>General .....</b>	<b>31</b>
<b>6.2</b>	<b>Specifications of categories .....</b>	<b>31</b>
<b>6.2.1</b>	<b>General .....</b>	<b>31</b>
<b>6.2.2</b>	<b>Designated architectures .....</b>	<b>32</b>
<b>6.2.3</b>	<b>Category B .....</b>	<b>32</b>

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 (PLr) .....	43
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 .....	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