

# Contents

<b>Preface</b>	<b>7</b>	Other directives	21
		Low-voltage Directive 2006/95/EC	22
		EMC Directive 2004/108/EC	22
		ATEX Product Directive 94/9/EC	22
		Pressure Equipment Directive 97/23/EC	22
		Directive on Simple Pressure Vessels 2009/105/EC	23
<b>Part A: Basics of machine safety – Legal and normative requirements</b>	<b>11</b>		
<b>A-1 European directives and national acts</b>	<b>13</b>	<b>A-2 Basic standards for functional safety</b>	<b>25</b>
Directives	14	Structure of international standards for machine safety	25
National acts and regulations	14	Standardization organizations	26
Standards	14	Presumption of conformity by harmonized standards	27
Requirements of the Machinery Directive and the Use of Work Equipment Directive	14	Consideration of failure probabilities	27
Scope of the Machinery Directive	15	Standards for functional safety	27
With the Machinery Directive to the Declaration of Conformity	15	ISO 12100	28
What does the CE mark stand for?	16	IEC 61508	28
Implementation of the Machinery Directive in machinery	17	IEC 61800-5-2	28
Definition	17	IEC 60204-1	28
Implementation	17	IEC 62061	29
Supplied documentation	17	ISO 13849 (replacement of EN 954-1)	29
CE mark	17	History of the standards for functional safety	29
Implementation of the Machinery Directive in partly completed machinery	19	Functional safety – scope of ISO 13849	29
Definition	19	One control system, several standards	30
Implementation	19	Global markets and local regulations	31
Supplied documentation	19		
CE mark	19	<b>Part B: 10 steps to performance level</b>	<b>33</b>
Implementation of the Machinery Directive in safety components	20	<b>B-1 Risk assessment</b>	<b>35</b>
Definition	20	Basics	35
“Safety components” versus “safety-related parts”	20	Risk assessment as the basis for machine safety	35
Implementation	20	Risk assessment based on standards	37
Supplied documentation	20	Procedure	37
CE mark	20	Example	47
Significant changes in machinery	20	Documents for the validation	49
Definition	20		
Implementation	21		
New documentation	21		
CE mark	21		

<b>B-2 Identification of the safety functions</b>	<b>51</b>	<b>B-6 Faults and diagnosis</b>	<b>89</b>
Basics	51	Basics	89
Safety functions	51	Consideration of failures (fault list)	89
Procedure	52	Fault exclusion	91
Determination of the safety functions	52	Diagnostic Coverage (DC)	91
Determining the safety-relevant properties of the safety functions	52	Procedure	95
Variants of the safety functions	55	Example	95
Partial safety functions of electric drive systems according to IEC 61800-5-2	56	Fault list	95
Example	60	Determining the Diagnostic Coverage (DC) of the components	98
Documents for the validation	61	Calculation of the $DC_{avg}$	98
<b>B-3 Determination of the <math>PL_r</math></b>	<b>63</b>	Documents for the validation	98
Basics	63	<b>B-7 Determination of the PL</b>	<b>99</b>
Selecting the procedure	64	Basics	99
Determination of the $PL_r$ according to ISO 13849	64	Reliability ( $MTTF_d$ , $B_{10d}$ )	101
Determination of the $PL_r$ based on IEC 62061	65	Determination of the performance level ( $PL_{SRP/CSI}$ )	102
Procedure	65	Procedure	104
Example	68	Example	105
Identification of the safety function	68	Subsystem 1: $SRP/CS_{Cat3/4}$	105
Determination of the $PL_r$	68	Subsystem 2: $SRP/CS_{cert}$	108
Comparison with the procedure of ISO 13849	68	Determination of the $PL_{SF}$	108
Documents for the validation	69	Adjustment of the $PL_{SF}$	108
<b>B-4 Category selection</b>	<b>71</b>	Documents for the validation	109
Basics	71	<b>B-8 Evaluation of the control system robustness – Failure avoidance</b>	<b>111</b>
Relationship between performance level and category	71	Basics	111
Free category selection	72	Measures against Common Cause Failures (CCF)	111
Recursive process	73	Basic and well-tried safety principles	113
Properties of the categories	73	Well-tried components	116
Procedure	75	Systematic failures	117
Example	76	Procedure	119
Documents for the validation	77	Example	120
<b>B-5 Modeling the block diagram</b>	<b>79</b>	Example 1: Measures against CCF	120
Basics	79	Example 2: Safety principles	121
Analysis	79	Documents for the validation	123
Modeling principles	80	<b>B-9 Software requirements</b>	<b>125</b>
Division into subsystems	80	Basics	125
Procedure	81	Software-based parameterization	126
Example	84	Safety-related application software (SRASW)	126
Description of the SRP/CS components	84	Safety-related embedded software (SRESW)	127
Characteristics of the safety function	85	Procedure	127
Documents for the validation	87	Project-independent preparations	128
		Project-specific activities for SRASW	128

Example	132	2 <sup>nd</sup> step: Identification of the safety functions	209
Preparation and verification of the software specification	132	3 <sup>rd</sup> step: Determination of the $PL_r$	211
Selection of the engineering tools	133	4 <sup>th</sup> step: Category selection	211
Software design	135	5 <sup>th</sup> step: Modeling the block diagram	211
Combination of safety-related and standard programs	135	6 <sup>th</sup> step: Faults and diagnosis	215
Software coding	136	7 <sup>th</sup> step: Determination of the $PL_{SF}$	217
Test	136	8 <sup>th</sup> step: Evaluation of the robustness	219
Documents for the validation	138	9 <sup>th</sup> step: Software requirements	225
		10 <sup>th</sup> step: Verification and validation	225
<b>B-10 Verification and validation</b>	<b>139</b>	<b>Part D: Appendix</b>	<b>227</b>
Basics	139	<b>D-1 ISO 13849: Machine Safety depends on Reliability</b>	<b>229</b>
Validation plan	141	Overview	229
Documentation of the validation process	141	Reliability basics	229
Validation by analysis	142	Bathtub curve	229
Validation by testing	142	Reliability characteristics	230
Procedure	143	Basis of the statistically based safety technology	231
Documents for the validation	145	State diagram	231
“Validation” checklist	145	Characteristics of the statistically based safety technology	232
Explanation	145	Risk assessment, safety function, performance level (PL)	233
<b>Part C: Application examples</b>	<b>151</b>	Usability of a component for the functional safety	233
<b>C-1 Example: Machine tool</b>	<b>153</b>	Methods for determining the reliability characteristics	234
Machine description	154	Calculations of the life cycle of electronic components	235
1 <sup>st</sup> step: Risk assessment	155	Testing of the life cycle	235
2 <sup>nd</sup> step: Identification of the safety functions	155	Life cycle analyses of field data	236
3 <sup>rd</sup> step: Determination of the $PL_r$	162	Failure probability of a safety function	237
4 <sup>th</sup> step: Category selection	163	Reliability model: Block diagram	237
5 <sup>th</sup> step: Modeling the block diagram	164	Meaning of the $MTTF_d$ value for the safety function	238
6 <sup>th</sup> step: Faults and diagnosis	167	Calculation of the dangerous failure probability ( $PFH_D$ )	239
7 <sup>th</sup> step: Determination of the $PL_{SF}$	170	Example of safety characteristics	239
8 <sup>th</sup> step: Evaluation of the robustness	173	Conclusion	240
9 <sup>th</sup> step: Software requirements	179		
10 <sup>th</sup> step: Verification and validation	188		
<b>C-2 Example: Machine tool, pneumatic subsystem</b>	<b>191</b>	<b>D-2 Terms, symbols and abbreviations</b>	<b>241</b>
1 <sup>st</sup> to 3 <sup>rd</sup> step to PL	191	<b>D-3 Bibliography</b>	<b>255</b>
4 <sup>th</sup> step: Category selection	191	Sources used in the book	255
5 <sup>th</sup> step: Modeling the block diagram	191	Related literature	257
6 <sup>th</sup> step: Faults and diagnosis	193		
7 <sup>th</sup> step: Determination of the $PL_{SF}$	196	<b>D-4 Alphabetical index</b>	<b>259</b>
8 <sup>th</sup> step: Evaluation of the robustness	199		
9 <sup>th</sup> step: Software requirements	206		
10 <sup>th</sup> step: Verification and validation	206		
<b>C-3 Example: Injection molding machine</b>	<b>207</b>		
Machine description	207		
1 <sup>st</sup> step: Risk assessment	208		