

ANSI B11.26-2018

American National Standard for Machines— Functional Safety for Equipment: General Principles for the Design of Safety Control Systems Using ISO 13849-1

ANSI-Accredited Standards Developer and Secretariat:



B11 Standards, Inc.
POB 690905
Houston, TX 77269
www.b11standards.org

Approved: **27 NOVEMBER 2018**
by the American National Standards Institute, Inc.



COPYRIGHT PROTECTED DOCUMENT

Copyright © 2018 by B11 Standards, Inc.

All rights reserved. Printed in the United States of America

No part of this publication may be reproduced in any form, in an electronic retrieval system or otherwise, without the prior written permission of B11 Standards, Inc.

AMERICAN NATIONAL STANDARDS

By approving this American National Standard, the ANSI Board of Standards Review confirms that the requirements for due process, consensus, balance and openness have been met by B11 Standards, Inc. (the ANSI-accredited standards developing organization).

American National Standards are developed through a consensus process. Consensus is established when substantial agreement has been reached by directly and materially affected interests. Substantial agreement means much more than a simple majority, but not necessarily unanimity. Consensus requires that all views and objections be considered, and that a concerted effort be made toward resolution. This process brings together volunteers and/or seeks out the views of persons who have an interest in the topic covered by this publication. While B11 Standards, Inc. administers the process and establishes procedures to promote fairness in the development of consensus, it does not write the documents, and it does not independently test, evaluate or verify the accuracy or completeness of any information or the soundness of any judgments contained in its standards or guidelines.

American National Standards are promulgated through ANSI for voluntary use; their existence does not in any respect preclude anyone, whether they have approved the standards or not, from manufacturing, marketing, purchasing, or using products, processes, or procedures not conforming to the standards. However, users, distributors, regulatory bodies, certification agencies and others concerned may apply American National Standards as mandatory requirements in commerce and industry.

The American National Standards Institute does not develop standards and will in no circumstances give an interpretation of an American National Standard. Moreover, no person shall have the right or authority to issue an interpretation of an American National Standard in the name of the American National Standards Institute. Requests for interpretations should be addressed to the Secretariat (B11 Standards, Inc.).

B11 STANDARDS, INC. MAKES NO WARRANTY, EITHER EXPRESSED OR IMPLIED AS TO THE FITNESS OF MERCHANTABILITY OR ACCURACY OF THE INFORMATION CONTAINED WITHIN THIS STANDARD AND DISCLAIMS AND MAKES NO WARRANTY THAT THE INFORMATION IN THIS DOCUMENT WILL FULFILL ANY OF YOUR PARTICULAR PURPOSES OR NEEDS. B11 STANDARDS, INC. DISCLAIMS LIABILITY FOR ANY PERSONAL INJURY, PROPERTY OR OTHER DAMAGES OF ANY NATURE WHATSOEVER, WHETHER SPECIAL, INDIRECT, CONSEQUENTIAL OR COMPENSATORY, DIRECTLY OR INDIRECTLY RESULTING FROM THE PUBLICATION, USE OF, APPLICATION OR RELIANCE ON THIS DOCUMENT. B11 STANDARDS, INC. DOES NOT UNDERTAKE TO GUARANTEE THE PERFORMANCE OF ANY INDIVIDUAL MANUFACTURER OR SELLER'S PRODUCTS OR SERVICES BY VIRTUE OF THIS STANDARD OR GUIDE, NOR DOES IT TAKE ANY POSITION WITH RESPECT TO THE VALIDITY OF ANY PATENT RIGHTS ASSERTED IN CONNECTION WITH THE ITEMS WHICH ARE MENTIONED IN OR ARE THE SUBJECT OF THIS DOCUMENT, AND B11 STANDARDS, INC. DISCLAIMS LIABILITY FOR THE INFRINGEMENT OF ANY PATENT RESULTING FROM THE USE OF OR RELIANCE ON THIS DOCUMENT. USERS OF THIS DOCUMENT ARE EXPRESSLY ADVISED THAT DETERMINATION OF THE VALIDITY OF ANY SUCH PATENT RIGHTS, AND THE RISK OF INFRINGEMENT OF SUCH RIGHTS, IS ENTIRELY THEIR OWN RESPONSIBILITY.

In publishing or making this document available, B11 Standards, Inc. is not undertaking to render professional or other services for or on behalf of any person or entity, nor is B11 Standards, Inc. undertaking to perform any duty owed by any person or entity to someone else. Anyone using this document should rely on his or her own independent judgment, or as appropriate, seek the advice of a competent professional in determining the exercise of reasonable care in any given circumstances.

B11 Standards, Inc. has no power, nor does it undertake to police or enforce conformance to the requirements of this document. B11 Standards, Inc. does not certify, test or inspect products, designs, or installations for safety or health purposes. Any certification or other statement of conformance to any health or safety-related information in this document shall not be attributable to B11 Standards, Inc. and is solely the responsibility of the certifier or maker of the statement.

NOTICE: This American National Standard may be revised or withdrawn at any time. The procedures of the American National Standards Institute require that action be taken periodically to reaffirm, revise, or withdraw this standard. You may contact the Secretariat for current status information on this, or other B11 standards.

Published by:

B11 Standards, Inc.

POB 690905, Houston TX 77269 USA

dfelinski@b11standards.org

Copyright © 2018 by B11 Standards, Inc. **All rights reserved.** Printed in the United States of America

TABLE OF CONTENTS

PAGE

Foreword 8

Introduction & Overview of the ANSI B11 Series of Machinery Safety Standards 10

1 Scope 13

2 References 13

2.1 Normative References..... 13

2.2 Informative References 13

3 Definitions 14

4 How to use ANSI B11.26 20

4.1 Circuit Examples and Analysis Tables..... 20

5 Preparations for Functional Safety Design..... 21

5.1 Conduct a Risk Assessment (per ANSI B11.0)..... 21

5.2 Identify Risk Reduction Measures that Involve the SRP/CS 23

5.3 Define the Safety Function 23

5.4 Determine the Reliability Design Specification for Each Circuit..... 24

5.4.1 Performance Level (PL) Methodology (ISO 13849-1)..... 24

 5.4.1.1 Architecture..... 24

 5.4.1.2 Select Components 25

 5.4.1.3 Fault considerations 25

 5.4.1.4 Diagnostic Coverage (DC)..... 25

 5.4.1.5 Common Cause Failure (CCF)..... 25

 5.4.1.6 Calculating a PL 26

5.4.2 Category methodology (ISO 13849-1 and EN 954)..... 26

 5.4.2.1 Architecture..... 26

 5.4.2.2 Summary of ISO 13849-1 Categories 26

5.4.3 Control reliable methodology (ANSI B11)..... 27

5.5 Define Basic Input, Logic and Output Elements Required 27

5.5.1 Inputs..... 27

5.5.2 Logic 27

5.5.3 Outputs..... 27

6 General Design Requirements 28

6.1 Integration of SRP/CS in the Overall Machine Controls 28

6.1.1 Typical Non-Safety Control Components Augmented by SRP/CS Components to Achieve Safety-Related Functions 28

6.2 Specific Functions..... 29

6.2.1 Protective Stop 29

6.2.2 Start Function 29

6.3 Electrical Design Requirements..... 29

6.3.1 Opening of Circuits for Time Dependent Functions 29

6.3.2 Positive/Negative Logic 29

6.3.3 Interfacing SRP/CS with Non-Safety PES/PLC 30

6.3.4 Electro-Mechanical Contact Requirements 30

6.4 Fluid Power (Pneumatics and Hydraulics) Design Requirements 30

6.4.1 Protective Stops in Fluid Power Systems..... 30

6.4.2 Reset Function of Safety Valves 31

6.4.3 Reapplication of Pressure 31

6.4.4 Fluid Power Valve Crossover 31

7	Fault Consideration	32
7.1	Fault Exclusion	32
7.2	Electrical Failure Modes	32
7.2.1	General Failure Modes	32
7.3	Fluid Power Failure Modes	33
7.3.1	General Failure Modes	33
7.3.2	Pneumatic Failure Modes	34
7.3.3	Hydraulic Failure Modes	34
8	Monitoring / Diagnostic Coverage	35
8.1	Electrical Monitoring / Diagnostic Coverage Methods	36
8.1.1	Input Masking on Series Connected Devices	36
8.2	Fluid Power Monitoring / Diagnostic Coverage Methods	36
9	Design Requirements – Input Devices (Engineering Control – Devices)	37
9.1	Emergency Stop Devices	37
9.1.1	Design Requirements	37
9.1.2	Design Considerations	37
9.1.2.1	Tampering / Defeat	37
9.1.2.2	Failure Modes	37
9.1.3	Application Examples	38
9.1.3.1	Single Channel E-stop Using a Control Relay (Category 1)	38
9.1.3.2	Low / Intermediate Risk Reduction (Category 2)	39
9.1.3.3	Intermediate / High Risk Reduction (Category 3)	40
9.1.3.4	Highest risk reduction (Category 4)	42
9.2	Mechanical (Contacting) Guard Interlocking Devices	43
9.2.1	Design Requirements	43
9.2.2	Design Considerations	43
9.2.2.1	General Information	44
9.2.3	Application Examples	46
9.2.3.1	Basic Circuit (Category B)	46
9.2.3.2	Lowest Risk Reduction (Category 1)	47
9.2.3.3	Low / Intermediate Risk Reduction (Category 2)	48
9.2.3.4	Intermediate / High Risk Reduction (Category 3)	49
9.2.3.5	Highest Risk Reduction (Category 4)	51
9.3	Non-Contact Guard Interlocking Devices	53
9.3.1	Design Requirements	53
9.3.2	Design Considerations	53
9.3.3	Application Examples	53
9.3.3.1	General information	53
9.3.3.2	Basic Risk Reduction (Category B)	55
9.3.3.3	Low / Intermediate Risk Reduction (Category 2)	57
9.3.3.4	Intermediate / High Risk Reduction (Category 3)	58
9.3.3.5	Highest Risk Reduction (Category 4)	60
9.4	Guard Locking Interlocks	64
9.4.1	Design Requirements	64
9.4.2	Design Considerations	64
9.4.3	Application Examples	64
9.4.3.1	General Information	64
9.4.3.2	Low / Intermediate Risk Reduction (Category 2)	65
9.4.3.3	Intermediate / High Risk Reduction (Category 3)	66
9.4.3.4	Highest Risk Reduction (Category 4)	67
9.5	Optical Presence Sensing Devices	70
9.5.1	Design Requirements	70
9.5.2	Design Considerations	70
9.5.2.1	General Information	70
9.5.2.2	Safety Light Curtains	70
9.5.2.3	Single/Multiple Safety Beam Devices (Point or Grid Devices)	71

	9.5.2.4 Scanners.....	71
9.5.3	Application Examples	71
	9.5.3.1 Lowest Risk Reduction (Category 1).....	72
	9.5.3.2 Low / Intermediate Risk Reduction (Category 2).....	73
	9.5.3.3 Intermediate / High Risk Reduction (Category 3).....	75
	9.5.3.4 Highest Risk Reduction (Category 4).....	76
9.6	Safety Mats / Edges	78
	9.6.1 Design Requirements.....	78
	9.6.2 Design Considerations	78
	9.6.3 Application Examples	78
	9.6.3.1 Low / Intermediate Risk Reduction (Category 2).....	78
	9.6.3.2 Intermediate / High Risk Reduction (Category 3).....	79
9.7	Two-Hand Control.....	80
	9.7.1 Design Requirements.....	80
	9.7.2 Design Considerations	80
	9.7.2.1 General Information.....	80
	9.7.2.2 Tampering / Defeat.....	80
	9.7.2.3 Failure Modes.....	80
	9.7.3 Application Examples	81
	9.7.3.1 Lowest Risk Reduction Two Hand Control (Type IIIa Category 1).....	81
	9.7.3.2 Intermediate / High Risk Reduction Two-Hand Control (Type IIIb Category 3).....	83
	9.7.3.3 Intermediate / High Risk Reduction Two-Hand Control (Type IIIb Category 3).....	84
	9.7.3.4 Highest Risk Reduction Two-Hand Control (Type IIIc Category 4).....	85
9.8	Speed Detection.....	86
	9.8.1 Design Requirements.....	86
	9.8.2 General Information and Design Considerations.....	86
	Common means of determining speed are given below.....	86
	9.8.2.1 Back EMF Sensing.....	86
	9.8.2.2 Encoder Sensing.....	86
	9.8.2.3 Proximity Switch Sensing.....	86
	9.8.2.4 Tampering / Defeat.....	86
	9.8.2.5 Failure Modes.....	86
	9.8.3 Application Examples	87
	9.8.3.1 Lowest Risk Reduction (Category 1).....	87
	9.8.3.2 Intermediate / High Risk Reduction (Category 3).....	88
9.9	Enabling Devices	94
	9.9.1 Design Requirements.....	94
	9.9.2 Design Considerations	94
	9.9.2.1 Tampering / Defeat.....	94
	9.9.2.2 Failure Modes.....	94
	9.9.3 Application Examples	95
	9.9.3.1 Low / Intermediate Risk Reduction (Category 2).....	95
	9.9.3.2 Intermediate / High Risk Reduction (Category 3).....	96
	9.9.3.3 Enabling Device with Manual/Auto Switch (Category 3).....	97
	9.9.3.4 Highest Risk Reduction (Category 4).....	99
10	Design Requirements - Logic Devices	100
	10.1 General	100
	10.1.1 Design Requirements.....	100
	10.1.2 Design Considerations	100
	10.1.2.1 Safety Interface Module General Information.....	100
	10.1.2.2 Tampering / Defeat.....	100
	10.1.2.3 Failure Modes.....	101
	10.1.2.4 Reset Function of the Safety Circuit.....	101
	10.1.3 Application Examples	101

11 Design Requirements – Output Devices (MPCE) 101

11.1 Relays and Contactors 101

11.1.1 Design Requirements 101

11.1.2 Design Considerations 101

11.1.2.1 Tampering / Defeat 102

11.1.2.2 Failure Modes 102

11.1.3 Application Examples 102

11.1.3.1 Lowest Risk Reduction (Category 1) 102

11.1.3.2 Low / Intermediate Risk Reduction (Category 2) 103

11.1.3.3 Intermediate / High Risk Reduction (Category 3) 104

11.1.3.4 Highest Risk Reduction (Category 4) 105

11.2 Power Drive Systems for Safe Torque Off 105

11.2.1 Design Requirements 105

11.2.2 Design Considerations 105

11.2.2.1 General Information 105

11.2.3 Application Examples 107

11.2.3.1 Lowest Risk Reduction (Category 1) 107

11.2.3.2 Intermediate / High Risk Reduction (Category 3) 109

11.2.3.3 Highest Risk Reduction (Category 4) 111

11.3 Pneumatic Systems 113

11.3.1 Design Requirements 113

11.3.2 Design Considerations 113

11.3.3 Application Examples 113

11.3.3.1 Supply Circuit 113

11.3.3.2 Exhaust (Blocking, Dump) Valve 114

11.3.3.3 Directional Valve Selection 122

11.3.3.4 Spring Return Blocking and Pilot Operated Check Valves 130

11.3.3.5 Flow Controls 139

11.3.3.6 Rod Locks and Brakes 142

11.3.3.7 143

11.3.3.8 Velocity Fuse 143

11.4 Hydraulic Systems 144

11.4.1 Design Requirements 144

11.4.2 Design Considerations 144

11.4.3 Application Examples 144

11.4.3.1 Dump and Blocking fluid to the hazardous motion 144

11.4.3.2 Directional Valve Selection 149

11.4.3.3 Spring Return Blocking and Pilot Operated Check Valves 154

11.4.3.4 Counter Balance Valves 163

11.4.3.5 Flow Controls 164

11.4.3.6 Rod Locks and Rod Brakes 165

11.5 Velocity Fuse 166

12 Validation 167

INFORMATIVE ANNEXES

Annex A – Symbols 168

Annex B – Performance Levels and Safety-Related Block Diagrams 173

Annex C – Categories and How to Make a Selection 179

Annex D – Section 1: Mean Time to Failure, Dangerous (MTTF_D) 185

Annex D – Section 2: Diagnostic Coverage 190

Annex D – Section 3: Estimating the Common Cause Failure (CCF) 194

Annex E – Calculation Aids for Determination of SRP/CS PFH_D & PL 195

Annex F – Analysis of Circuit Considerations 204

Annex G – Failures, Systemic 209

Annex H – General Overview of Valves 211

Annex I – Performance of the Safety-Related Function(s) (Overview) 215

Annex J – Safety-Related Performance 217

Annex K – External Device Monitoring by the Safety-Related Function 219

Annex L – Validation Tools for Mechanical Systems 221

Annex M – Validation Tools for Pneumatic Systems 224

Annex N – Validation Tools for Hydraulic Systems 231

Annex O – Validation Tools for Electrical Systems 237