ANSI B11.26–2024

American National Standard for Machines –

Functional Safety:

General Principles for Designing Safety–Related Parts of Control Systems for Machinery

ANSI-Accredited Standards Developer and Secretariat:

B11 Standards, Inc.
Houston, Texas, USA
www.b11standards.org

APPROVED: 6 NOVEMBER 2024
by the American National Standards Institute
Board of Standards Review

COPYRIGHT PROTECTED DOCUMENT
Copyright © 2024 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 people 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 document 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 does B11 Standards, Inc. undertake 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.
Houston TX 77069 USA
www.b11standards.org

Copyright © 2024 by B11 Standards, Inc. **All rights reserved.** Printed in the United States of America

TABLE OF CONTENTS PAGE

Foreword (The Foreword is NOT a normative part of ANSI B11.26-2024) **12**
Introduction & Overview of the ANSI B11 Series of Machinery Safety Standards **15**
1 Scope **18**
2 References **18**
2.1 Normative References **18**
2.2 Informative References **18**
3 Definitions **19**
3.17 emergency stop: The stopping of a machine, manually initiated, for emergency purposes. **20**
3.18 engineering controls: Guards or devices and associated safety-related parts of the control system (SRP/CS) used to reduce risk. See ANSI B11.19. ..... **20**
4 How to Use ANSI B11.26 ..... **26**
4.1 Circuit Examples and Analysis Tables **26**
4.2 Circuit Analysis Tables **27**
5 Preparations for Functional Safety Design **28**
5.1 Conduct a Risk Assessment (per ANSI B11.0) **28**
5.2 Identify Risk Reduction Measures that Involve the SRP/CS **29**
5.3 Define the Safety Function **29**
5.4 Determine the Reliability Design Specification for Each Circuit **30**
5.4.1 Categories **31**
5.4.1.1 Architecture 31
5.4.1.2 Diagnostic Coverage (DC) 32
5.4.1.3 Common Cause Failure (CCF) 32
5.4.1.4 Category design considerations 32
5.4.2 Performance Level (PL) Methodology (ISO 13849-1) **33**
5.4.2.1 General 33
5.4.2.2 Select Components 33
5.4.2.3 Fault considerations 33
5.4.2.4 Diagnostic Coverage (DC) 33
5.4.2.5 Common Cause Failure (CCF) 34
5.4.2.6 Calculating a PL 34
5.4.3 Safety integrity level (SIL) **34**
5.5 Define Basic Input, Logic and Output Elements Required **34**
5.5.1 Inputs **35**
5.5.2 Logic **35**
5.5.3 Outputs **35**
6 General Design Requirements **36**
6.1 Integration of SRP/CS in the Overall Machine Controls **36**
6.1.1 Typical Non-Safety Control Components Augmented by SRP/CS Components to Achieve Safety-Related Functions **36**
6.2 Specific Functions **37**
6.2.1 Protective Stop **37**
6.2.2 Start Function **37**
6.3 Electrical Design Requirements **37**
6.3.1 Opening of Circuits for Time Dependent Functions **37**
6.3.2 Positive/Negative Logic **37**
6.3.3 Interfacing SRP/CS with Non-Safety PES/PLC **38**
6.3.4 Electro-Mechanical Contact Requirements **38**
6.4 Fluid Power (Pneumatics and Hydraulics) Design Requirements **38**
6.4.1 Protective Stops in Fluid Power Systems **39**
6.4.2 Reset Function of Safety Valves **39**
6.4.3 Reapplication of Pressure **39**

6.4.4 Fluid Power Valve Crossover 39
6.5 Mechanical design requirements 39
6.5.1 Design Requirements 40
6.5.2 Design Considerations 40
6.5.2.1 General Information 40
7 Fault Consideration 41
7.1 Common Cause Failure 41
7.2 Fault Exclusion 41
7.3 Electrical Failure Modes 41
7.4 Fluid Power Failure Modes 42
7.4.1 General Failure Modes 42
7.4.2 Pneumatic Failure Modes 43
7.4.3 Hydraulic Failure Modes 44
7.4.4 Avoiding an overly complex design 45
7.5 Mechanical failure modes 45
7.5.1 Tampering / Defeat 45
7.5.2 Failure Modes 45
8 Monitoring / Diagnostic Coverage 46
8.1 Electrical Monitoring / Diagnostic Coverage Methods 46
8.1.1 Input Masking on Series Connected Devices 46
8.2 Fluid Power Monitoring / Diagnostic Coverage Methods 47
8.2.1 Direct monitoring 47
8.2.2 Indirect monitoring 47
8.2.3 Monitoring by the process 47
8.2.4 Monitoring of three position valves 47
8.2.5 Monitoring of response time 47
9 Design Requirements – Input Devices (Engineering Control – Devices) 48
9.1 Emergency Stop Devices 48
9.1.1 Design Requirements 48
9.1.2 Design Considerations 48
9.1.2.1 Tampering / Defeat 48
9.1.2.2 Failure Modes 48
9.1.3 Application Examples 49
9.1.3.1 Single Channel E-stop Using a Control Relay (Category 1) 49
9.1.3.2 Dual Channel E-stop Using Redundant Control Relays (Category 2) 50
9.1.3.3 Dual Channel E-Stop Using Force-Guided Relays (FGR) and Cross Monitoring (Category 3) 51
9.1.3.4 Multiple Dual Channel E-Stop with a Safety Interface Module (SIM)(Category3) 52
9.1.3.5 Single Button Dual Channel E-stop with a SIM (Category 4) 53
9.1.3.6 Single Button Dual Channel E-stop w/ Self-Monitoring and a SIM (Category 4) 54
9.2 Mechanical (Contacting) Interlocking Devices 54
9.2.1 Design Requirements 54
9.2.2 Design Considerations 55
9.2.2.1 General Information 55
9.2.3 Application Examples 58
9.2.3.1 Basic Interlocked Guard Circuit (Category B) 58
9.2.3.2 Interlocked Guard Circuit – Single Channel (Category 1) 59
9.2.3.3 Interlocked Guard Monitoring – Single Channel w/ a SIM and PES (Category 2) 60
9.2.3.4 Single Interlock to a SIM (Category 3) 61
9.2.3.5 Series Connection of Interlocks to a SIM (Category 3) 62
9.2.3.6 Interlocked Guard Monitoring – Dual Channel w/ Relay/Contactor and Reset Button (Category 4) 63

9.2.3.7 Interlocked Guard Monitoring – Dual Channel w/ a SIM (Category 4) 64
9.2.3.8 Control Interlocking using Trapped Key Interlocking Systems 65
9.2.3.9 Prevention of unexpected start-up using a Trapped Key Interlocking System 66
9.2.3.10 Single access control procedure using a Trapped Key Interlocking System 67
9.2.3.11 Access control using a Trapped Key Interlocking System including key exchange 69
9.3 Non-Contact Interlocking Devices 69
9.3.1 Design Requirements 69
9.3.2 Design Considerations 70
9.3.3 Application Examples 70
9.3.3.1 Description of Non-Contact Interlocking Devices 70
9.3.3.2 Inductive Switches 70
9.3.3.3 Optical Switches 70
9.3.3.4 Magnetic Switches 70
9.3.3.5 Transponder Switches 70
9.3.3.6 Interlocking Device “type” Characteristics 71
9.3.3.7 Non-Contact Interlocked Guard Monitoring using Standard Retro-Reflective Photo Sensor (Category B) 72
9.3.3.8 Non-Contact Interlocked Guard Monitoring using Standard Magnetic Sensor (Category B) 73
9.3.3.9 Non-Contact Interlocked Guard Monitoring – Single Channel w/ a SIM and PES (Category 2) 74
9.3.3.10 Non-Contact Interlocked Guard Monitoring Circuit (Category 3) .. 75
9.3.3.11 Interlocked Guard Monitoring – Dual Channel with a SIM (Category 3) 76
9.3.3.12 Interlocked Guard Monitoring – Dual Channel with a SIM (Category 4) 77
9.3.3.13 Interlocked Guard Monitoring – Dual Channel with a SIM (Category 4) 78
9.3.3.14 Interlocked Guard Monitoring – Dual Channel with a SIM (Category 4) 79
9.3.3.15 Interlocked Guard Monitoring – Dual Channel with a SIM (Category 4) 80
9.4 Guard Locking Interlocks 81
9.4.1 Design Requirements 81
9.4.2 Design Considerations 81
9.4.2.1 General Information 81
9.4.2.2 Power to Release, Inline Guard locking Interlock (Category 2) 82
9.4.2.3 Power to Release, Dual Axis Guard Locking Interlock (Category 3) 83
9.4.2.4 Power to Release, Dual Axis Interlock Connected with secondary guard interlock switch to a SIM (Category 4) 84
9.4.2.5 Power to Release, Dual Axis Interlock Connected with Secondary Guard Interlocking Device to a SIM (Category 4) 85
9.5 Optical Presence Sensing Devices 86
9.5.1 Design Requirements 86
9.5.2 Design Considerations 86
9.5.2.1 General Information 86
9.5.2.2 Light Curtains 86
9.5.2.3 Single/Multiple Beam Devices (Point or Grid Devices) 86
9.5.2.4 Scanners 87
9.5.3 Application Examples 87
9.5.3.1 IEC 61496 Type 2 Presence Sensing Device with Control Relay (Category 1) 87
9.5.3.2 IEC 61496 Type 2 Presence Sensing Device with Force-Guided

Relay (Category 2) 88
9.5.3.3 IEC 61496 Type 2 Presence Sensing Device with Force-Guided Relay (Category 2) 89
9.5.3.4 IEC 61496 Type 3 Presence Sensing Device with Safety Interface Module (Category 3) 90
9.5.3.5 IEC 61496 Type 4 Presence Sensing Device with OSSD (Category 4) 91
9.5.3.6 IEC 61496 Type 4 Presence Sensing Device with Safety Interface Module (Category 4) 92
9.6 Safety Mats / Edges 93
9.6.1 Design Requirements 93
9.6.2 Application Examples 93
9.6.2.1 Single Safety Mat using a Safety Interface Module (Category 2) ... 93
9.6.2.2 Multiple Safety Mats using a Safety Interface Module (Category 3) 94
9.7 Two-Hand Control 95
9.7.1 Design Requirements 95
9.7.2 Design Considerations 95
9.7.2.1 General Information 95
9.7.2.2 Tampering / Defeat 95
9.7.2.3 Failure Modes 95
9.7.3 Application Examples 96
9.7.3.1 Two-Hand Control Device (Type IIIa Category 1) 96
9.7.3.2 Two-Hand Control Device (Type IIIa Category 1) 97
9.7.3.3 Two-Hand Control Device (Type IIIb Category 3) 98
9.7.3.4 Two-Hand Control Device (Type IIIb Category 3) 99
9.7.3.5 Two-Hand Control Device (Type IIIc Category 4) 100
9.8 Speed Detection 101
9.8.1 Design Requirements 101
9.8.2 General Information and Design Considerations 101
Common means of determining speed are given in 9.8.2.1 – 9.8.1.3..... 101
9.8.2.1 Back EMF Sensing 101
9.8.2.2 Encoder Sensing 101
9.8.2.3 Proximity Switch Sensing 101
9.8.2.4 Tampering / Defeat 101
9.8.2.5 Failure Modes 101
9.8.3 Application Examples 102
9.8.3.1 Single Proximity Sensing (Category 1) 102
9.8.3.2 Dual Proximity Sensors to Timers and Force-Guided Relay Monitoring (Category 3) 103
9.8.3.3 Dual Proximity Sensors to Timers and Force-Guided Relay Monitored by a SIM (Category 3) 104
9.8.3.4 Dual Proximity Sensors to Dual Frequency Counters Monitored by a SIM (Category 3) 105
9.8.3.5 Dual Proximity Sensors Plus Zero-speed or Stand Still SIM (Category 3 or 4) 106
9.8.3.6 Encoder Speed Monitoring (Category 3) 107
9.8.3.7 Motor Drive Back EMF Detection (Category 3 or 4) 108
9.9 Enabling Devices 109
9.9.1 Design Requirements 109
9.9.2 Design Considerations 109
9.9.2.1 Tampering / Defeat 109
9.9.2.2 Failure Modes 109
9.9.3 Application Examples 110
9.9.3.1 Non-Contact Interlocked Guard Monitoring – Single Channel w/ a SIM and PES (Category 2) 110
9.9.3.2 Enabling device with an interlock for manual operation (Category 3) 111
9.9.3.3 Enabling Device with Manual/Auto Switch (Category 3) 112

9.9.3.4 Enabling Device with Manual Suspension Enable (Category 3) ... 113
9.9.3.5 Enabling Device with Manual Suspension and Reduced Speed (Category 4) ... 114
10 Design Requirements - Logic Devices ... 115
10.1 General ... 115
10.1.1 Design Requirements ... 115
10.1.2 Design Considerations ... 115
10.1.2.1 Safety Interface Module General Information ... 115
10.1.2.2 Tampering / Defeat ... 115
10.1.2.3 Failure Modes ... 116
10.1.2.4 Reset Function of the Safety Circuit ... 116
10.2 Software and Programming ... 116
10.2.1 General ... 116
10.2.2 Software Safety Requirements Specifications (SSRS) ... 117
10.2.3 Components ... 117
10.2.3.1 Inputs ... 117
10.2.3.2 Logic ... 117
10.2.3.3 Outputs ... 117
10.2.4 Structure ... 117
10.2.5 Programming ... 118
10.2.6 Software validation ... 118
10.2.7 Cybersecurity ... 118
10.2.8 Remote access ... 118
11 Design Requirements – Output Devices (MPCE) ... 119
11.1 Relays and Contactors ... 119
11.1.1 Design Requirements ... 119
11.1.2 Design Considerations ... 119
11.1.2.1 Tampering / Defeat ... 119
11.1.2.2 Failure Modes ... 119
11.1.3 Application Examples ... 120
11.1.3.1 Contactor (Category 1) ... 120
11.1.3.2 Force-Guided Contactor (Category 2) ... 121
11.1.3.3 Dual Force-Guided Contactor (Category 3) ... 122
11.1.3.4 Dual Force-Guided Contactor (Category 4) ... 123
11.2 Power Drive Systems for Safe Torque Off ... 124
11.2.1 Design Considerations ... 124
11.2.1.1 General Information ... 124
11.2.2 Application Examples ... 126
11.2.2.1 Single Channel Interlock Functional Stop Category 0 (per NFPA 79) of an AC Motor using Standard Rated AC Drive (Category 1) 126
11.2.2.2 Single Channel Interlock Functional Stop Category 1 (per NFPA 79) of an AC Motor using Standard Rated AC Drive (Category 1) 127
11.2.2.3 A Functional Stop Category 0 (per NFPA 79) of an AC Motor using Safety-related AC Drive (Category 3) ... 128
11.2.2.4 Functional Stop Category 1 (per NFPA 79) of an AC Motor using Safety-rated AC Drive (Category 3) ... 129
11.2.2.5 Dual Channel Interlock Functional Stop Category 0 (per NFPA 79) of an AC Motor using Standard Rated AC Drive with Checking (Category 4) ... 130
11.2.2.6 Dual Channel Interlock Functional Stop Category 0 (per NFPA 79) of an AC Motor using Safety-rated AC Drive with Checking and one Force Guided Contactor (Category 4) ... 131
11.3 Pneumatic Systems ... 132
11.3.1 Design Requirements ... 132
11.3.2 Design Considerations ... 132
11.3.3 Supply Circuit ... 132
11.3.4 Energy Isolation/Lockout Valve ... 132

11.3.5 Air Preparation (Contamination Control) 132
11.3.6 Filtration 132
11.3.7 Regulator 132
11.3.8 Lubrication 132
11.3.8.1 Non-Lubricated (preferred) 132
11.3.8.2 Lubricated (not recommended) 132
11.3.9 Air Valve Mufflers 133
11.3.10 Pneumatic Safety Functions 134
11.3.10.1 Exhaust (Blocking/Dump) Safety Function 134
11.3.10.2 Exhaust (blocking/Dump) – 3/2 Normally Closed Valve (Category 1) 134
11.3.10.3 Exhaust (Blocking/Dump) – 5/3 Open Center Valve (Category 1) 135
11.3.10.4 Exhaust (blocking/Dump – 3/2 Normally Closed Valve with Integrated Sensor (Category 2) 135
11.3.10.5 Exhaust (Blocking/Dumping) – 3/2 Normally Closed Valve with Pressure Sensor (Category 2) 136
11.3.10.6 Exhaust (Blocking/Dump) – 3/2 Normally Closed Valve with Integrated Sensor in Series with 5/3 Open Center Valve (Category 3) 136
11.3.10.7 Exhaust (Blocking/Dump) – 3/2 Normally Closed Valve with Pressure Sensor in Series with 5/3 Open Center Valve (Category 3) 137
11.3.10.8 Exhaust (Blocking/Dump) 3/2 Normally Closed Valves with Integrated Sensors in Series (Category 3 or 4) 138
11.3.10.9 3/2 Exhaust (Blocking Dump) – Normally Closed Safety-Rated Dual Valve with Sensors, Automatic Reset (Category 4) 139
11.3.10.10 Exhaust (Blocking/Dump) – 3/2 Normally Closed Safety-Rated Dual Valve with Internal Monitoring and Feedback Sensor, Automatic Reset (Category 4) 140
11.3.10.11 Exhaust (Blocking Dump) 3/2 Normally Closed Safety-Rated Dual Valve with Internal Monitoring, Feedback Sensor, Manual Reset (Category 4) 141
11.3.11 Safe Valve Position/Direction (Safe Return) 141
11.3.11.1 Design Requirements 141
11.3.11.2 Design Considerations 141
11.3.11.3 Safe Valve Position/Direction (Safe Return) – 5/2 Valve (Category 1) 142
11.3.11.4 Safe Valve Position/Direction (Safe Return) – 5/2 Valve with Integrated Sensor (Category 2) 142
11.3.11.5 5/2 Safe Valve Position/Direction (Safe Return) – Safety-Rated Dual Valve with Integrated Sensors, Automatic Reset (Category 3 or 4) 143
11.3.11.6 Safe Valve Position/Direction(Safe Return) – Dual Safety-Rated 5/2 Valve with Internal Monitoring, Feedback Sensor, Automatic Reset (Category 4) 144
11.3.11.7 Safe Valve Position/Direction (Safe Return) – Dual Safety-Rated Valve with Internal Monitoring, Feedback Sensor, Manual Reset (Category 4) 144
11.3.12 Maintain End of Stroke Position (Safe Last Position) 145
11.3.12.1 Design Requirements 145
11.3.12.2 Design Considerations 145
11.3.12.3 Maintain End of Stroke Position (Safe Last Position) - 5/2 Detented Valve (Category 1) 145
11.3.12.4 5/2 Maintain End of Stroke Position (Safe Last Position) - Detented Valve with Integrated Sensor (Category 2) 146
11.3.13 Safe Stopping (Load Holding) 146
11.3.13.1 Control and Stop/Hold 146

11.3.13.2 Control and Stop/Hold 5/2 Closed Center Valve (Category 1) ... 147
11.3.13.3 Control and Stop/Hold – 5/3 Closed Center Safety-Rated Dual Valve with Integrated Sensors, Automatic Reset (Category 3 or 4) 147
11.3.14 Stop (Load Holding) ... 148
11.3.14.1 Stop (Load Holding) Pilot Operated (P.O.) Check ... 148
11.3.14.2 Stop (Load Holding) – Pilot Operated Check Valve (Category 1) 149
11.3.14.3 Stop (Load Holding) Pilot Operated Check Valve with Integrated Sensor (Category 2) ... 149
11.3.14.4 Stop (Load Holding) Pilot Operated Check Valve with Actuator Sensor Feedback (Category 2) ... 150
11.3.14.5 Stop (Load Holding) 5/3 Closed Center Valve with Pilot Operated Check Valve with Integrated Sensor (Category 3) ... 151
11.3.14.6 Stop (Load Holding) – 5/3 Open Center Valve with Redundant Pilot Operated Check Valve with Integrated Sensors and Safety-Rated Exhaust Valve (Category 3) ... 152
11.3.14.7 Stop (Load Holding) – 5/3 Open Center Valve with Redundant Pilot Operated Check Valve with Integrated Sensors and Redundant Control Valves (Category 3) ... 153
11.3.15 Rod locks / brakes ... 154
11.3.15.1 Design Requirements ... 154
11.3.15.2 Design Considerations ... 154
11.3.15.3 Rod Locks / brakes – 3/2 Normally Closed Valve (Category 1) . 154
11.3.15.4 Rod Locks / Brakes – 3/2 Normally Closed Valve with Pressure feedback and Safety-Rated Rod Lock with position feedback (Category 2) ... 155
11.3.15.5 Rod locks / brakes – Redundant 3/2 Normally Closed Valve with Pressure feedback and Redundant Safety-Rated Rod Lock with position feedback (Category 3) ... 156
11.3.15.6 Rod Locks / Brakes – Redundant 3/2 Normally Closed Safety-Rated Dual Valve with Sensors, Automatic Reset and Redundant Safety-Rated Rod Lock with Dual position feedback (Category 4) 157
11.3.16 Flow Control ... 158
11.3.16.1 Design Requirements ... 158
11.3.16.2 Design Considerations ... 158
Meter-IN 158
11.3.16.3 Flow Control – Meter Out Flow Control Example ... 159
11.3.16.4 Flow Control – Meter Out Flow Control Example ... 160
11.3.17 Safe Pressure (force) Selection ... 160
11.3.17.1 Design Requirements ... 160
11.3.17.2 Design Considerations ... 161
11.3.17.3 Safe pressure (force) selection - 5/2 Valve (Category 1) ... 161
11.3.17.4 Safe pressure (force) selection - 5/2 Valve with Integrated Sensor (Category 2) ... 161
11.3.17.5 5/2 Safe Valve Position/Direction (Safe Return) – Safety-Rated Dual Valve with Integrated Sensors (Category 4) ... 162
11.3.18 Velocity Fuse ... 162
11.3.18.1 Design Requirements ... 162
11.3.18.2 Design Considerations ... 162
11.3.18.3 Velocity fuse (Category 1) ... 163
11.4 Hydraulic Systems ... 163
11.4.1 Hydraulic Design Requirements ... 163
11.4.2 Fluid Preparation (Contamination Control) ... 164
11.4.3 Dump and Block Fluid to the Hazardous Motion ... 165
11.4.3.1 Design Requirements ... 165
11.4.3.2 Design Considerations ... 165
11.4.3.3 Dump and Block - 5/3 Open Center (Float Center) Valve (Category

1) 165
11.4.3.4 Dump and Block - 4/2 Valve (Category 1) 166
11.4.3.5 Dump and Block - 4/2 Valve with Integrated Sensor (Category 2) 166
11.4.3.6 Dump and Block - 4/2 Valve with Pressure Sensor (Category 2) 167
11.4.3.7 Dump and Block – 3/2 Normally Closed Valve with Integrated Sensor in Series with 5/3 Open Center (Float Center) Valve (Category 3) 167
11.4.3.8 Dump and Block – Redundant 4/2 Valve with Integrated Sensor in Series 168
(Category 3 or 4) 168
11.4.4 Return 168
11.4.4.1 Design Requirements 168
11.4.4.2 Design Considerations 168
11.4.4.3 4/2 Valve (Category 1) 169
11.4.4.4 4/2 Valve with Integrated Sensor (Category 2) 169
11.4.5 Maintain End of Stroke Position 170
11.4.5.1 Design Considerations 170
11.4.5.2 Design Considerations 170
11.4.5.3 4/2 Detented Valve (Category 1) 170
11.4.6 Control and Stop/Hold 170
11.4.6.1 Design Requirements 170
11.4.6.2 Design Considerations 170
11.4.6.3 Control and Stop/Hold – 4/3 Closed Center or Tandem Center Valve (Category 1) 171
11.4.7 Load Holding - Spring Return Blocking and Pilot Operated Check Valves 171
11.4.7.1 Design Requirements 172
11.4.7.2 Design Requirements 172
11.4.7.3 Load Holding – Pilot Operated Check Valve or 2/2 Normally Closed Valve (Category 1) 172
11.4.7.4 Load Holding – Pilot Operated Check Valve or 2/2 Normally Closed with Integrated Sensor (Category 2) 173
11.4.7.5 Load Holding – Low / Intermediate Risk Reduction Pilot Operated Check Valve or 2/2 Normally Closed with Actuator Sensor Feedback (Category 2) 174
11.4.7.6 Load Holding – Pilot Operated Check Valve or 2/2 Normally Closed with Integrated Sensor (Category 2) 174
11.4.7.7 Load Holding – 5/3 Closed Center Valve with Redundant Pilot Operated Check Valves or 2/2 Normally Closed Valves w/ Integrated Sensors and Redundant Control Valves (Category 3) 175
11.4.8 Load Holding – Counter-balance Valves 175
11.4.9 Rod Locks and Rod Brakes 176
11.4.9.1 Design Requirements 176
11.4.9.2 Design Considerations 176
11.4.9.3 Rod Lock/Brake (Category 1) 176
11.4.10 Speed Control Flow Controls 177
11.4.11 Velocity Fuse 178
12 Validation 179
13 Change Management 180
14 Information for Use 180

Annex A – Symbols **181**
Annex B – Performance Levels and Safety-Related Block Diagrams **187**
Annex C – Categories and How to Make a Selection **193**
Annex D – Section 1: Mean Time to Failure, Dangerous ($MTTF_D$) **200**
Annex D – Section 2: Diagnostic Coverage **206**
Annex D – Section 3: Estimating the Common Cause Failure (CCF) **210**
Annex E – Calculation Aids for Determination of SRP/CS PFH & PL **212**
Annex F – Analysis of Circuit Considerations **221**
Annex G – Failures, Systemic **226**
Annex H – General Overview of Valves **228**
Annex I – Performance of the Safety-Related Function(s) (Overview) **232**
Annex J – External Device Monitoring by the Safety-Related Function **234**
Annex K – Validation Tools for Mechanical Systems **236**
Annex L – Validation Tools for Pneumatic Systems **239**
Annex M – Validation Tools for Hydraulic Systems **247**
Annex N – Validation Tools for Electrical Systems **253**
Annex O – Consideration for Fluid Power DC (Diagnostic Coverage) **261**
Annex P – Change Management System **267**
Annex Q – Example of avoiding an overly complex pneumatic design **268**

Foreword (The Foreword is NOT a normative part of ANSI B11.26-2024)

The content of this American National Standard was first developed and released as ANSI Technical Report B11.TR6 and published in December 2010. In the subsequent years of use, the B11 Standards Development Committee decided that the content of the document was sufficiently important to be elevated to a standard and agreed to a revision of B11.TR6 as American National Standard ANSI B11.26 in order to address the dynamic state of ongoing international and national/regional standard revisions regarding functional safety and in particular, to provide a more practical "application-type" document for the complicated ISO 13849 standard. The primary attributes of the first edition of the ANSI B11.26 standard were the allowance of different methodologies to characterize reliability, detailed example schematic diagrams, and "Circuit Analysis Tables" that provided additional technical detail for each example. Detailed annexes for understanding performance levels and category block diagrams as outlined in ISO 13849-1 were also provided. The detailed, generic (non-supplier specific) schematic diagrams were based on actual applications that have been successfully implemented in industry.

The current revision further expands on the 2016 edition and includes the following significant changes:

- **Changed title to clarify that the standard is intended to address requirements for functional safety – using a variety of accepted methodologies;**
- **Definitions updated and harmonized with other ANSI B11 standards where practical;**
- **Added and clarified requirements in clause 4, when using categories to specify reliability;**
- **Provided historical information on "control reliability;"**
- **Included Safety integrity level (IEC 62061) methodology as an approved methodology to specify reliability;**
- **Modified Risk Graph for Categories to clarify selection;**
- **Provided information/requirements for trapped key applications;**
- **Provided basic requirements for software used in functional safety applications;**
- **Provided basic requirements for management of change;**
- **Fluid power output applications reorganized by safety function; for example, "directional valves" were separated into exhaust, return, or stopping functions;**
- **Additional fluid power example functions added for safe pressure, closed center stopping, and rod lock applications;**
- **Fluid power monitoring was expanded to explain different methods of monitoring;**
- **Fluid power application chart data simplified;**
- **addition of Annex Q (Example of using ISO 13849 to avoid overly complex designs).**

The B11.26 Subcommittee provided many examples for common solutions of current industrial circuit applications. It is important to understand that there are many ways to fulfil a given engineering requirement, and the examples provided in this standard only present one of those many options. These examples are not normative, nor intended to limit innovation or the advancement of technology.

ANSI B11.26 illustrates safety control circuit design concepts used to realize safety functions. These functions reduce risks identified by a risk assessment. The example circuits, explanations, and minimum fault exclusions are for educational purposes and do not contain complete information on electrical, fluid power, and mechanical design requirements. Substitutions, additions, or changes to the circuits, components, safety modules, or engineering control – devices should be thoroughly researched and examined as to the extent of the impact on the integrity, reliability, and the level of performance of the safety functions. The designer should refer to relevant standards, regulations, and codes to address the installation and safety requirements.

Industry users expressed the desire that example circuits be depicted in a NEMA format. To provide clarity and enhance understanding, the writing subcommittee created symbols for safety components that previously did not exist. These new symbols distinguish safety-rated devices from their non safety-rated counterparts such as emergency stops and forced guided relays. This document also identifies the relationship between risk assessment (ANSI B11.0) and control circuit reliability, including the use of ISO 13849-1.

Internal (intra-document) references are hotlinked to their source; to activate, position the cursor over the hotlink and use control and left-click.

Inquiries with respect to the application or the substantive requirements of this standard, and suggestions for its improvement, are welcomed and should be sent to B11 Standards, Inc.: cfelinski@B11standards.org Attention: B11 Secretariat / B11.26.

This standard was prepared by the B11.26 Subcommittee, processed and submitted for ANSI approval by the B11 Standards Development Committee on Safety Standards for Machines. At the time this standard was approved as an American National Standard, the ANSI B11 Standards Development Committee was composed of the following member organizations:

Alan Metelsky, FS Eng, Chair / Anne Mathias, PE, Vice-Chair / David Felinski, Secretary

Organizations Represented	**Name of Representative**	
	Delegate	**Alternate**
Aluminum Extruders Council	Mel Mitchell, CSP	Brad Wyatt, CSP
Amazon Robotics	Jeread Sines, B11 LMSS, FS Eng	Josh Owens, B11 LMSS, FS Eng
American Society of Safety Professionals	Ted Sberna, Sr.	Anne Mathias, PE
Association for Advancing Automation	Maren Roush	Jeff Fryman
Association For Manufacturing Technology	Doug Otte	Alan Metelsky, FS Eng
Assn. for Packaging & Processing Technologies	Bruce Main, PE, CSP	Tom Egan
The Boeing Company	Rhiannon McPherson	Mark Ellingson
Bridgestone	Kenji Furukawa, FS Eng	Joey Hinson, FS Eng
Canadian Standards Association	Ana Andronescu, P.Eng.	Walter Veugen
Deere & Co.	Scott Winter	Liz Frimel
Eli Lilly	Bryan Harrell, FS Eng	Danny Deighton
Euchner	Andrew Smith	Jilani Bouchane
Exponent	Steve Andrew, PE, CSM	Alex Zelhofer, PhD, PE
FDR Safety	Mike Taubitz	Luke Contos, Joe Wolfsberger
Fortress Safety	Jenny Tuertscher, B11 LMSS, FS Eng	
Honda Development & Mfg. of America	Todd Dickey	Doug Titus, Tyler Willis
General Motors Corporation	Tony Ross	Phyllis Childs
IDEM Safety	Mark Witherspoon	Amir Mohtasham
International Union, UAW	Jim Holton	Matt Uptmor
Komatsu America Industries	George Schreck	James Landowski
Liberty Mutual	Ashlee Blum, CSP, CSE	Julie Thompson, CSP
MAG Automotive	Erik Carrier	Doug Watts
Metal Powder Industries Federation	Bill Edwards	James Adams
National Inst. for Occupational Safety & Health	Rick Current, PE	
Occupational Safety & Health Administration	Ken Stevanus	Mary Bauer, CIH, CSP, B11 LMSS
Omron Scientific Technologies Incorporated	Rex Kiehl	Tina Hull, FS Exp
Pilz Automation Safety, LP	Mike Beerman, CMSE	Dino Mariuz
Plastics Industry Association	Jeff Linder	Dale Bartholomew
Precision Metalforming Association	Jim Barrett, Jr. PhD	David Klotz
Rockwell Automation	Darin Magnuson, FS Eng	Jonathan Barrett, FS Eng
Rockford Systems	Brian Boes, B11 LMSS	Matt Brenner
Ross Controls	Chris Brogli	Eric Cummings, B11 LMSS, FS Eng
Safe–T–Sense	Mike Poynter, FS Eng	Federico Badillo
SICK PCA	Chris Soranno, FS Exp	Christian Bidner
Sheet Metal & Air Cond. Contractors Nat'l. Assn.	Justin Crandol, CSP	Rick Di Ioli
Toyota Motor Manufacturing North America	Chip Boertlein	Mike Collier, B11 LMSS

At the time this standard was approved, the **B11.26 Functional Safety Subcommittee** had the following members who participated in and contributed to the development of this American National Standard:

Alan Metelsky, Chairman	Gleason Works	Eric Cummings, Vice-Chair	Ross Controls
Jim Barrett	Link Systems	Marc Lewandowski	Proctor & Gamble
Craig Brockway	Machine Safety Specialists	Bruce Main	design safety engineering
Chris Brogli	Ross Controls	Rhiannon McPherson	Boeing
David Brown	DuPont	Nathan O'Connor	Nexen Group
Patric Brown	Grantek	Alex Parry	Safe-T-Sense
Eric Carrier	MAG Automotive	Mike Poynter	Safe-T-Sense
Eddie Crawford	Rockwell	Jacob Prange	Nexen Group
Chase Davis	EOSYS Group	Ted Sberna, Sr.	White Horse Safety
Todd Dickey	Honda	Jeread Sines	Amazon
Bryant Eismeier	Flexware Innovation	Marco Tacchini	GT Engineering, Italy
Kenji Furukawa	Bridgestone	Marty Timm	Centigrade Services
Bryan Harrell	Eli Lilly	Jenny Tuertscher	Fortress Safety
Ryan Hayworth	Airline Hydraulics	Mark Witherspoon	IDEM Safety
Jim Holton	International UAW	Chris Felinski, Secretary	B11 Standards, Inc.

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

Introduction

The purpose of the ANSI B11 series of machinery safety standards and technical reports is to devise and propose ways to eliminate or minimize risks of the potential hazards associated with the required tasks. This can be accomplished either by an appropriate machine design or by restricting personnel or other individuals' access to hazard zones, and by devising work procedures to minimize personnel exposure to hazardous situations. This is the essence of the ANSI B11 series of safety standards. This standard recognizes that zero risk does not exist and cannot be attained. However, a good faith approach to risk assessment and risk reduction should achieve an acceptable risk level.

Organization and Application of B11 Documents

The ANSI B11 series of standards and technical reports can be associated with the ISO "type A-B-C" structure as described immediately below, and as shown in Figure 1.

- **Type-A standards** (basis standards) give basic concepts, principles for design, and general aspects that can be applied to machinery;
- **Type-B standards** (generic safety standards) deal with one or more safety aspects or one or more types of engineering controls that can be used across a wide range of machinery:
- **Type-C standards** (machinery safety standards) deal with detailed safety requirements for a particular machine or group of machines**.**

The B11 Standards Development Committee recognizes that an additional type of standard has emerged, which we categorize as a so-called "**Hybrid standard."** These hybrid standards represent an evolutionary development in machinery safety standardization that combines some unspecified percentage of the typical content and requirements found in any two (or even all three) of the standard types described above. Usually, there are some combinations of requirements generally found in type-A and type-C standards. With the possible exception of ANSI B11.0, none of the other documents in the B11 portfolio fit into this new type, numerous examples of these hybrid machinery safety standards exist outside of ANSI B11.

The B11.0 standard on general safety requirements common to ANSI B11 machines is primarily a "type -A" standard in that it applies to a broad array of machines and contains very general requirements. However, in many areas it also contains very specific requirements. B11.19, B11.20, B11.21, B11.25, B11.26, as well as the entire B11 series of Technical Reports are all typical "type-B" documents addressing general safety elements that can be used across a wide range of machinery (such as B11.19 and B11.26) or as a standard when combining machines (B11.20). The B11 series of Technical Reports are informative documents that may be generally applied to many different machines, and as such would fall into the "type-B" category. The machine-specific ("type-C") B11 standards contain detailed safety requirements for a particular machine or group of machines (such as this standard). The type-A B11.0 and the type-C (machine-specific) B11 standards are intended to be used concurrently by the supplier and user of machines. When a type-C standard deviates from one or more provisions dealt with by this standard or by a type-A standard, the type-C standard requirement generally takes precedence. Any deviation in conforming to a requirement of any standard should be carefully evaluated and based on a documented risk assessment.

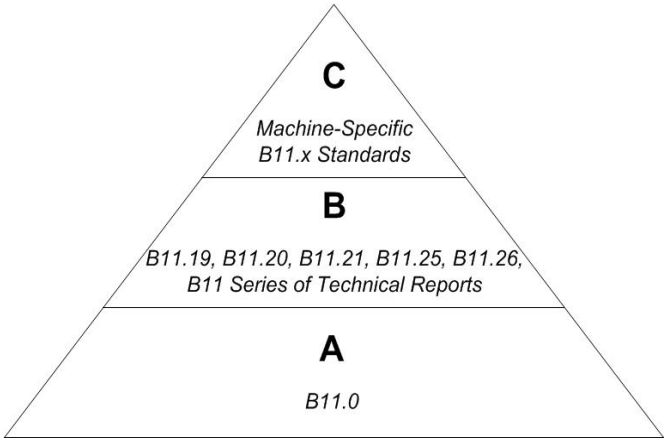


Figure 1: Organization of the B11 Series of Documents

ANSI B11.26 applies when a control system is used as a risk reduction measure. The responsibility for reducing these risks to an acceptable level is divided between the equipment supplier, the equipment modifier, the equipment user and its operating personnel. Figure 2 (below) provides the structure of a typical type-C standard and in particular, the responsibilities of and requirements for the supplier, modifier, user, and the user personnel. Figure 2 is provided so the reader can better understand the responsibilities for reducing risk, since this type-B standard applies when a control system is used as a risk reduction measure. Parenthetical numbers denote the particular clause/subclause of the type-C standard.

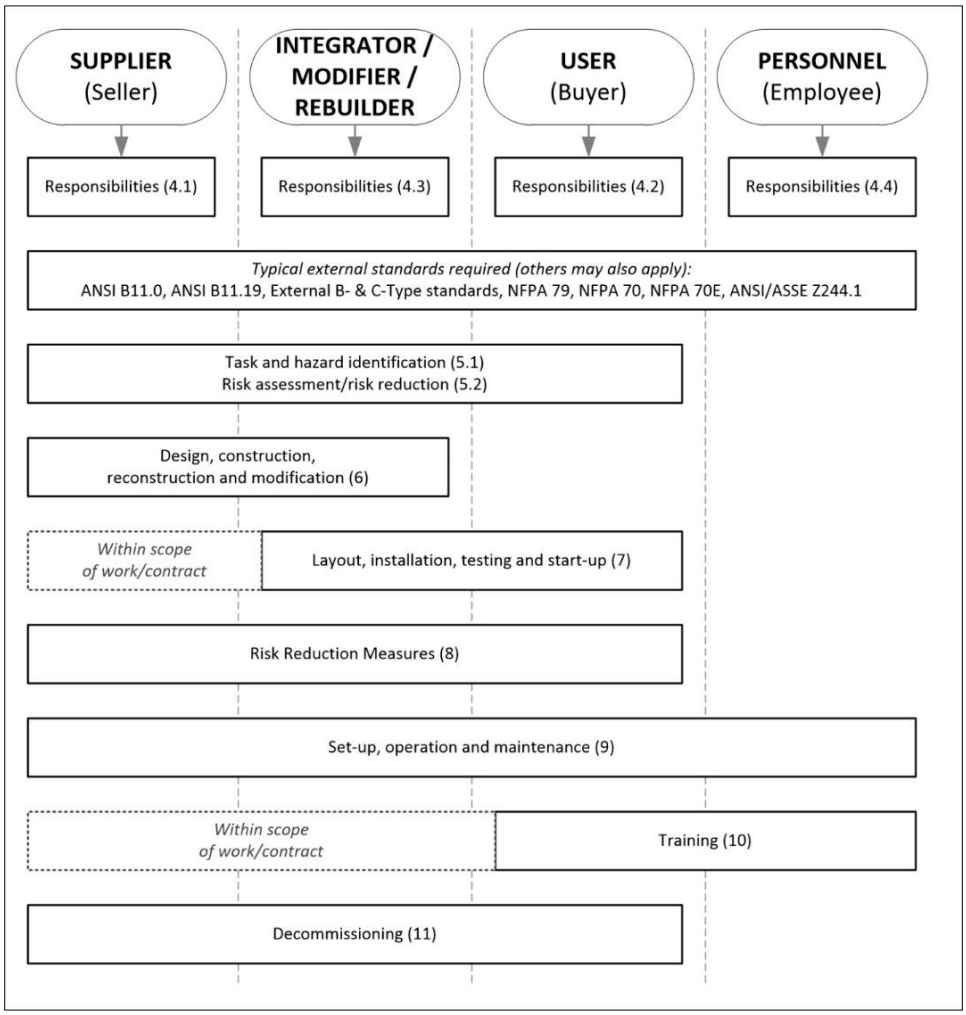


Figure 2: Typical clause layout of B11 base (type-C) standards showing the various responsibilities

- **SUPPLIER:** The early stages of a project present the greatest opportunity to determine project requirements and to anticipate and eliminate hazards and hazardous situations.
- **MODIFIER:** The entity (OEM, Supplier, or the expert) in that discipline responsible for creating or modifying the system, machinery or equipment, shall have all relevant design standards documentation. The entity shall begin by working with the end user to list all tasks to achieve an appropriate comprehensive task list based on the “context of use” for the system, machine or equipment.
- **USER:** The company representatives (can be from many disciplines) where the system, machinery or equipment will reside during its productive life. They should engage in participating in or reviewing the risk assessment and what will be necessary for a final safety buy-off at the final location.
- **PERSONNEL:** The group “at risk” from any hazards or hazardous situation presented by the system, machinery, or equipment while performing their tasks to achieve the company’s desired productive life. This would include, at a minimum, operators, maintenance personnel for both planned and unplanned maintenance, housekeeping and safety representatives. This group would evaluate the engineering controls and administrative controls (see ANSI B11.19).

As of the date of approval of this standard, the ANSI B11 series of American National Standards and Technical Reports on machinery safety consisted of the following documents shown in the list below. The user should check a licensed reseller such as ANSI (www.ansi.org) for the current versions of any of these documents. All archival / historical versions of the documents are available at www.b11standards.org.

List of the ANSI B11 Series of Safety Standards and Technical Reports

#	SHORT TITLE / TOPIC	YEAR	TYPE
B11.0	Safety of Machinery	2023	A
B11.1	Mechanical Power Presses	2009 (R2020)	C
B11.2	Hydraulic & Pneumatic Power Presses	2013 (R2020)	C
B11.3	Power Press Brakes	2022	C
B11.4	Shears	2003 (R2020)	C
B11.5	Ironworkers	1988 (R2020)	C
B11.6	Manual Turning Machines w/ or without Auto Control	2022	C
B11.7	Cold Headers and Cold Formers	2020	C
B11.8	Manual Milling, Drilling, & Boring Machines	2022	C
B11.9	Grinding Machines	2010 (R2020)	C
B11.10	Sawing Machines	2003 (R2020)	C
B11.11	*Withdrawn* (Gear and Spline Cutting Machines; covered by B11.0)	2001 (R2012)	C
B11.12	Roll Forming and Roll Bending Machines	2005 (R2020)	C
B11.13	Single & Multiple-Spindle Automatic Bar and Chucking Machines	2020	C
B11.14	*Withdrawn* (Coil Slitting Machines; combined into B11.18)	(1996)	C
B11.15	Pipe, Tube and Shape Bending Machines	2022	C
B11.16	Powder / Metal Compacting Presses	2014 (R2020)	C
B11.17	Horizontal Extrusion Presses	2023	C
B11.18	Machines Processing or Slitting Coiled or Non-Coiled Metal	2006 (R2020)	C
B11.19	Performance Requirements for Risk Reduction Measures (Safeguarding)	2019	B
B11.20	Integration of Machinery into a System	2017 (R2022)	B
B11.21	Machine Tools Using Lasers for Processing Materials	2006 (R2020)	B
B11.22	Turning Centers and Automatic Numerically Controlled Turning Machines	2002 (R2020)	C
B11.23	Machining Centers & CNC Milling, Drilling & Boring Machines	2002 (R2020)	C
B11.24	Transfer Machines	2002 (R2020)	C
B11.25	Large Machines	2022	B
B11.26	Functional Safety: Designing SRP/CS for Machinery	2024	B
B11.27	Electro-Discharge Machines	2024	C
B11.TR0	Guide to Establishing a Machine Safety Process Using ANSI B11 Stds	2024	B
B11.TR1	Ergonomics	2016	B
B11.TR2	*Withdrawn (*Metal Working Fluids)	1997 (R2016)	B
B11.TR3	*Withdrawn* (Risk Assessment / Risk Reduction Guide)	(2000 R2015)	B
B11.TR4	Selection of Programmable Electronic Systems (PES/PLC)	2004 (R2015)	B
B11.TR5	Noise Measurement	2006 (R2017)	B
B11.TR6	*Withdrawn* (Safety Control Systems for Machines)	(2010)	B
B11.TR7	Integration of Lean and Safety	2007 (R2017)	B
B11.TR8	Sustainable Safety Systems Thru Inspection of Risk Reduction Measures	2022	B
B11.TR9	Cybersecurity	2019	B
B11.TR10	Guidance on Artificial Intelligence into Machinery Safety Applications	2020	B
B11.TR11	Using ANSI Standards for CE-marking of Machinery	2024	B
ANSI/ISO 12100	Safety of machinery (identical adoption of ISO 12100-2010)	2012	A

Functional Safety:
General Principles for Designing Safety-Related Parts of Control Systems for Machinery

1 Scope

This American National Standard provides requirements and guidance for the implementation of safety-related control functions (also known as "functional safety") as they relate to electrical, electronic, pneumatic, hydraulic, and mechanical components of control systems.

Informative Note 1: *This document includes a large number of detailed schematic circuit diagrams that are provided as EXAMPLE circuits only, representing common solutions in use at the time of creating this document. It is important to understand that there are many ways to fulfil a given engineering requirement and the examples only present one option. These examples are not normative, nor intended to limit innovation or the advancement of technology.*

Informative Note 2: *This document references ISO 13849-2 – Validation as part of an annex.*

Informative Note 3: *See also, clause 4 on "How to use this standard."*

2 References

The following normative documents contain provisions that, through reference in this text, constitute provisions of this American National Standard. At the time of publication, the editions indicated were valid. All normative documents are subject to revision, and parties to agreements subject to this American National Standard should consider applying the most recent editions of the normative documents listed below. This standard is intended to be used in conjunction with the following American National Standards:

2.1 Normative References

ANSI B11.0 – 2023, Safety of Machinery

ANSI B11.19 – 2019, Performance Requirements for Risk Reduction Measures: Safeguarding and Other Means for Reducing Risk

NFPA 79 – 2024, Electrical Standard for Industrial Machinery

ANSI / ASSP Z244.1-2016, Control of Hazardous Energy – Lockout, Tagout and Alternative Methods

Informative Note 1: *At the time of approval of ANSI B11.26, this reference standard has been revised and approved and is expected to be published relatively soon – check the ANSI Standards Store.*

2.2 Informative References

ANSI B11.TR4 – 2004 (R16), Selection of Programmable Electronic Systems (PES/PLC) for Machine Tools

ANSI / ISO 12100:2012 (ISO 12100:2010 IDT), Safety of machinery – General principles for design – Risk assessment and risk reduction

ASME Boiler and Pressure Vessel Code Section VIII Division 1.

ISO 1219-1:2012, Fluid power systems and components – Graphical symbols and circuit diagrams Part 1: Graphical symbols for conventional use and data-processing applications

ISO 4406:2021 Hydraulic fluid power. Fluids. Method for coding the level of contamination by solid particles

ISO 4413:2010, Hydraulic fluid power – General rules and safety requirements for systems and their components

ISO 4414:2010, Pneumatic fluid power – General rules and safety requirements for systems and their components

ISO 13849-1:2023, Safety of machinery – Safety-related part of control systems – Part 1: General Principles for Design

ISO 13849-2:2012, Safety of machinery – Safety-related part of control systems – Part 2: Validation

Informative Note: *At the time of approval of ANSI B11.26, this informative reference standard was in revision and is expected to be approved sometime in 2026.*

ISO 14119:2024 Interlocking devices associated with guards – Principals for design and selection

ISO 19973-2:2015 Pneumatic fluid power - Assessment of component reliability by testing - Part 2: Directional control valves
ISO 8573:2001 - Compressed air -- Part 1: Contaminants and purity classes
IEC 60204-1:2018 – Safety of electrical equipment of machinery used for general electrical safety aspects
IEC 61508 Parts 1-7 – Functional safety of electrical / electronic / programmable electronic safety-related systems used for the design of complex subsystems
IEC 62061:2021 - Safety of machinery – Functional safety of safety-related electrical, electronic and programmable electronic control systems
IEC 60947-5-8:2020 – Low voltage switchgear and control gear – Part 5-8: Control circuit devices and switching elements – Three-position enabling switches
UL/IEC 60947-5-1:2024 - Low voltage switchgear and control gear – Part 5-1: Control circuit devices and switching elements- Electromechanical Control Circuit Devices
EN 61810-1:2015 Electromechanical elementary relays, General requirements

3 Definitions

For the purposes of this document, the terms and definitions provided in this clause apply, in *addition* to those terms and definitions found in clause 3 of ANSI B11.0.

3.0 Acronyms: The following Table contains acronyms used in this standard, with their meaning given in the second column:

CH	Channel
CR	Control Relay
FGC	Force-Guided Contactor
FGR	Force-Guided Relay
LS	Limit Switch
MPCE	Machine Primary Control Element
OSSD	Output Signal Switching Device
PED	Programmable Electronic Device
PES	Programmable Electronic System
PFH	Probability of Dangerous Failure per Hour
PL	Performance Level
SIL	Safety Integrity Level
SIM	Safety Interface Module
SOL	Solenoid
SPES	Safety Programmable Electronic System
SRP/CS	Safety-Related Part(s) of the Control System
TR	Timer Relay

3.1 access control: A sub function of a trapped key interlocking system that controls access to safeguarded spaces or access to machine operating modes and functions.

3.2 access lock: A device intended to lock a guard in the closed position for trapped key interlocking systems and linked to the control system via the key transfer.

Informative Note: *Access locks can also be used for locking in position objects other than guards, e.g., isolators, valves or barriers.*

3.3 actuator: A mechanical device used for moving or controlling motion or energy.

3.4 actuating control(s): An operator control used to initiate or maintain machine motion(s) or other machine function(s).

Informative Note: *Also referred to as:* ***foot control***, ***hand control***, ***pedal***, ***presence sensing device initiation***, ***treadle bar***, ***two-hand control***, *or* ***two-hand trip***.

3.5 architecture (system): The configuration or structure of the control system.

3.6 brake: A mechanism for stopping, slowing or preventing machine motion (see also, *fluid power rod brake*).

3.7 bypass: See ***manual suspension***.

3.8 captive contact: See ***Force-Guided***.

3.9 Category (safety performance): The classification of the subsystem with respect to its resistance to faults and the subsequent behavior in the fault condition which is achieved by the structural arrangement of the parts, fault detection and/or by their reliability. Categories state the required behavior of a safety-related part of a control system with respect to its resistance to faults (B, 1, 2, 3, 4, as detailed in Clause 7). See also, ISO 13849-1.

3.10 Category (stop): The stop categories state the required behavior of the control system with respect to a stop command (0, 1, 2). See also, NFPA 79.

3.11 common cause failure: A failure that is the result of one or more events, causing concurrent failures of two or more items, leading to failure of a safety function.
Informative Note: *Common cause failures should not be confused with common mode failures.*

3.12 common mode failure: Failures of items characterized by the same fault mode.
Informative Note: *Common mode failures should not be confused with common cause failures, as common mode failures can result from different causes.*

3.13 commissioning: Validation of the safety function after the initial installation/modification of the machine and/or related equipment.

3.14 control relay: A mechanical relay used for non-safety-related functions. See *safety relay*.

3.15 control reliability: The capability of the machine control system, the engineering control – devices, other control components and related interfacing to achieve a safe state in the event of a failure within the safety-related parts of the control system.

3.16 direct (positive) opening: Achievement of contact separation as the direct result of a specified movement of the switch actuator through non-resilient members (e.g., not dependent on springs).

3.17 emergency stop: The stopping of a machine, manually initiated, for emergency purposes.

3.18 engineering controls: Guards or devices and associated safety-related parts of the control system (SRP/CS) used to reduce risk. See ANSI B11.19.

3.18.1 engineering controls – guard: A barrier that provides protection from a hazard.
Informative Note: *A guard is intended to restrict access to a hazard by minimizing the possibility of unintentionally reaching the hazard.*

3.18.2 engineering controls – control function: Safety functions associated with engineering controls (guards or devices) intended to reduce risk.

3.18.3 engineering controls – device (safeguarding device): A device that provides protection from a hazard(s) by preventing or detecting exposure to the hazard zone.

3.19 external device monitoring (EDM): A means by which a safety-related device monitors the state of external devices.

3.20 failure: Termination of the ability of an item to perform a required function.
Informative Note: *After one or more failures, the item has a fault. "Failure" is an event, as distinguished from "fault," which is a state. The concept as defined does not apply to items consisting of software only.*

3.21 fault: A state of an item characterized by the inability to perform a required function after a failure.

Informative Note 1: *A fault does not include the inability to perform during preventive maintenance or other planned actions, or due to lack of material, product, utilities or other external resources.*
Informative Note 2: *A fault is often the result of a failure of the item itself but may exist without prior failure. In this standard, "fault" means a random fault.*

3.22 fault consideration: The identification of various failure modes that could negatively impact the ability of the safety system to resist faults.

3.23 fault exclusion: The elimination from consideration of a specific identified failure within the SRP/CS because its probability is low relative to the system's required performance, through design, selection of components or implementation of additional measures.

3.24 fault tolerance: The number of faults under which the safety-related control system will continue to perform its required safety function.
Informative Note: *For a zero fault tolerant system, the safety-related control system loses its ability to perform its required safety function due to one fault. For a single fault tolerant system, the safety-related control system will perform its required safety function in the presence of one fault but may fail to perform its required safety function in the presence of multiple faults.*

3.25 feedback: A means by which a device is monitored.

3.26 fluid power (cylinder piston) rod brake: A device attached to a cylinder that mechanically grips the piston rod while it is in motion and causes the cylinder to stop. Its ability to stop motion has a capacity rating.

3.27 fluid power (cylinder piston) rod lock: A device attached to a cylinder that mechanically grips the piston rod when it is motionless. Its ability to hold a position motionless has a rating and is not typically capable of braking.
Informative Note: *The rod lock is not intended to stall a moving cylinder and has a limitation on the amount of force resistance.*

3.28 force-guided: Constructed in such a way that normally closed contact element(s) and normally open contact element(s) cannot simultaneously be in the closed position.
Informative Note: *Also called **mechanically linked**. The following symbol is used to designate force guided contacts.*

3.29 functional safety: That portion of the safety of the machine and the machine control system which depends on the correct functioning of the SRP/CS, other technology safety-related systems and external risk reduction facilities (IEC 61508).

3.30 hand control: A hand-operated mechanism or device used as a control device.
Informative Note: *Also referred to as: **actuating control**, **two-hand control device**, **two-hand trip device**, **single control device**, or **single trip device**.*

3.31 immediate stop command: A command that initiates an action(s) to stop a hazardous motion (or situation) at any point in the machine cycle.

3.32 listed for such use: Equipment, materials, or services included in a list published by a Nationally Recognized Testing Laboratory (NRTL) and concerned with evaluation of products or services, that maintains periodic inspection of the production of listed equipment or materials or periodic evaluation of services, and whose listing states that either the equipment, material, or service meets identified standards or has been tested and found suitable for a specified purpose.

3.33 interlocking device (interlock): A mechanical, electrical or other type of device, the purpose of which is to prevent the operation of hazardous machine functions under specified conditions (generally as long as a guard is not closed).

3.33.1 type 1 interlocking device: a mechanically actuated device operated with an uncoded actuator

(e.g., cam-operated or hinge-operated interlock);

3.33.2 type 2 interlocking device: a mechanically actuated device operated with a coded actuator (e.g., tongue-operated switch actuator);

3.33.3 type 3 interlocking device: non-contact actuated device with uncoded actuator (e.g., proximity switch);

3.33.4 type 4 interlocking device: non-contact actuated device with coded actuator (e.g., low, medium or high-level coding);

3.33.5 type 5 interlocking device (Trapped key interlocking device): A device which fulfils a function by trapping or releasing one or more keys in a given trapped key interlocking system (e.g., door locks, key-operated switches, key exchange devices).

3.34 key-operated switch (key-operated switch as part of trapped key systems): A trapped key interlocking device comprising a switch which can only be operated by means of a key.

3.35 key-operated solenoid-controlled switch (key operated solenoid-controlled switch as part of trapped key systems): A trapped key interlocking device comprising a key operated switch which can be mechanically locked by the operation of a solenoid.

3.36 key exchange device: A trapped key interlocking device in which the insertion of one or more keys releases one or more keys with a different coding, trapping the inserted key(s).

3.37 key releasable: A key which is not locked and so can be (turned and) removed at any time causing a change of state of the device.

Informative Note: *Change of state of the device releases or traps another key or changes contact state.*

3.38 key trapped: A situation in which a key is locked until energization of a solenoid, or insertion of an actuator, allows the release of it.

Informative Note: *A solenoid or the insertion of an actuator releases the trapped key.*

3.39 lock: See ***fluid power rod lock***.

3.40 machine control [control system]: Part of a machine that includes but is not necessarily limited to control devices, display functions, data processing or storage, sensors, safety-related functions, and power control elements (e.g., contactors, valves, speed control, etc.).

Informative Note: *The machine control system can use any technology or any combination of different technologies (e.g., electrical/electronic, hydraulic, pneumatic and mechanical).*

3.41 machine start-up: Initial cycle after the machine has been through extended idle time or after the machine has been powered down.

3.42 manual suspension: A suspension that is actuated or selected by an individual that disables or renders ineffective, one or more safety function(s).

Informative Note: *Also known as* ***overriding*** *or* ***bypassing****.*

3.43 mechanically linked: See ***Force-Guided***.

3.44 monitoring: The checking of system components to detect a failure or fault of a component, subassembly or module that affects the performance of the safety function(s).

3.45 muting: The automatic temporary suspension of any safety-related function(s) of the control system or engineering control – device.

3.46 OSSD (Output Signal Switching Device): A component of electro-sensitive protective equipment connected to the machine control system which, when the sensing device is actuated during normal operation, responds by going to the OFF state.

3.47 Performance Level: The ability of safety-related parts of control systems to perform a safety function

under foreseeable conditions and this ability is allocated as one of five levels. These levels are defined in terms of probability of dangerous failure per hour.

3.48 positively driven: Use of a mechanical non-resilient linkage that is designed to separate the contacts upon actuation of the device (commonly referred to as *direct positive opening*, see 3.16). The following symbol is used to designate positive driven contacts:

3.49 positively guided: See ***Force-Guided***.

3.50 positive mode mounting: Mounting of the switch such that the opening of the guard actuates the safety switch via direct contact or rigid elements. This typically applies to type 1 switches. See also, 9.2.2.1.1.

3.51 presence-sensing device: A device that creates a sensing field, area or plane to detect the presence of an individual or object and provides an output signal.

3.52 PED (Programmable Electronic Device): A device with input and output ports, central processing unit(s), communication ports, sequenced or controlled by a program. For example: PLC, PC, CNC, Embedded Microprocessors, etc.

3.53 PES (Programmable Electronic System): An electronic system that performs logical, decision-making, or arithmetic functions by executing instructions in a specified manner. The system usually includes input and output elements (ports) and is usually reprogrammable.

3.54 protective stop: The stopping of a machine initiated by an engineering control – device for risk reduction purposes.

3.55 redundancy: The use of multiple means to perform the same function.
Informative Note: *Redundancy is typically used to improve the reliability of the system.*

3.56 relay: An electromagnetic device for remote or automatic control that is actuated by variation in conditions of an electric circuit and that operates other devices (as switches) in the same (or different) circuit.

3.57 reset: A function that initializes or returns a device, circuit, or other measure to its operating or enabling state.
Informative Note: *The function can be either safety-related or unrelated to safety.*

3.58 risk reduction: That part of the risk assessment process involving the elimination of hazards or the selection of other appropriate and feasible risk reduction measures (protective measures) to reduce the probability of harm or its severity.

3.59 safety control system: A part or subpart(s) of a control system (e.g., operator inputs, sensors, logic, and actuators) that perform safety-related functions. The combined SRP/CS begins at the point where the safety-related input signals are initiated and ends at the output of the energy control elements. This also includes safety-related monitoring systems.

3.60 safety event: When a safety-rated device performs its intended function.

3.61 safety integrity level (SIL): Discrete level (one out of a possible four) for specifying the safety integrity requirements of the safety function(s) to be allocated to the electrical / electronic / programmable electronic safety-related systems, where safety integrity level 4 has the highest level of safety integrity and safety integrity level 1 has the lowest.

3.62 safety interface module (SIM): A device incorporating monitored redundancy in a single body using safety principles to control electrical circuits. A safety interface module usually consists of monitored, multiple, force-guided, captive contact relays, or other devices. A single discrete force-guided, captive contact relay is not a safety interface module.

3.63 safety-rated device: A device designed to an applicable safety standard and intended for use as a safety-related device.

3.64 safety-related manual control device: A control device, when properly applied, that reduces the level of risk. These include but are not limited to valves and engineering controls (guards and devices) which require deliberate human action that may cause or result in potential harm to individuals.

Informative Note: *Examples include actuating devices such as pushbuttons, selector switches, or foot pedals designed for functions like reset, start/restart, guard unlocking or hold-to-run control (e.g., jog, inching).*

3.65 safety-related function (safety function): That portion of the control system or engineering control – device that either eliminates or reduces exposure to a hazardous situation.

3.66 safety-related part of a control system (SRP/CS): That portion of the control system that responds to safety-related input signals and generates safety-related output signals.

Informative Note 1: *SRP/CS are those part(s) of the machinery control system that provide safety functions which can consist of separate components of the hardware and software and can either be separate from the machine control or be an integral part of it.*

Informative Note 2: *The combined safety-related parts of a control system start at the point where the safety-related input signals are initiated (including for example, the actuating cam and the roller of the position switch) and end at the output of the power control elements (including for example, the main contacts of a contactor).*

Informative Note 3: *If monitoring systems are used for diagnostics, they are also considered as SPR/CS.*

3.67 safety relay: See Force-Guided and Safety Interface Module (SIM).

Informative Note: *The term safety relay has two common usages: to mean an individual Force-Guided Relay or to mean a SIM containing one or more Force-Guided Relays.*

3.68 safety-related reset: A function within the SRP/CS used to restore one or more safety functions before restarting a machine.

Informative Note: *This can be automatic or manual.*

3.69 safety valve: A device incorporating monitored redundant function elements in a single body using safety principles to control fluids. Monitoring may be internal or external.

3.70 SPES (Safety Programmable Electronic System): A Programmable Electronic System for control of safety-related functions. This is also referred to as SRECS (Safety-Related Electrical Control System).

3.71 stop command: An action(s) to cause a safe condition (including cessation of machine motion) either automatically or through human intervention. The stop command may be immediate or normal.

3.72 structure: See ***architecture***.

3.73 synchronous (actuation): Concurrent actuation where the time lag between the start of one input signal and the start of the other is less than or equal to a predetermined time.

Informative Note: *For two-hand control and/or two-hand trip devices, the time lag is less than or equal to 500 milliseconds.*

3.74 transponder: A device which processes electromagnetic fields from a transmitter to the receiver. A transponder system receives and processes electromagnetic fields between a master and slave element.

3.75 trapped key (type 5) interlocking system: A system fulfilling safety function(s) or part of safety function(s) and is comprised of at least two different type 5 interlocking devices which work together through the transfer of a key.

3.76 two-hand control device: An actuating control that requires the synchronous use of both the operator's hands to initiate a machine cycle and concurrent use during the hazardous portion of the machine cycle.

Informative Note 1: *Two-hand control devices only provide risk reduction for the person operating the actuating control.*

Informative Note 2: *Two-hand control devices are sometimes referred to as* ***hostage controls****.*

3.77 two-hand trip device: An actuating control that requires the synchronous use of both of the operator's hands to initiate a machine cycle.

Informative Note 1: *Two-hand trip devices only provide risk reduction for the person operating the actuating control.*

Informative Note 2: *Two-hand trip devices typically cause a full machine cycle and do not initiate an immediate stop command if either or both the operator controls are released.*

3.78 valve: A component that controls the direction, pressure, or flow rate of fluid.

3.79 valve element: Internal part of a valve that, by its movement, provides the basic function of directional control, pressure control, or flow rate control. This may be a spool, a poppet or other design.

3.80 validation: Confirmation, through the provision of testing on the as-built machine, that the risk assessment requirements have been fulfilled.

Informative Note 1: *Validation can involve answering two questions:*

1. *Are we doing the right things? (Is the risk reduction measure appropriate?);*
2. *Are we doing things right? (Is the risk reduction measure used properly?).*

Informative Note 2: *"Validate" as used in this standard means to check and test, to confirm and document, but does not imply formal validation as that term is used, for example, in the pharmaceutical industry.*

Informative Note 3: *For additional information about the process of validation, see IEC 61508, IEC 62061, and ISO13849-1.*

3.81 verification: The process of checking that the design and development outputs have met the requirements of the risk assessment during the design phase.

Informative Note 1: *For example: evaluation of components to confirm they meet the requirements of the safety function; analysis of the safety circuits to confirm that the performance achieves the requirements of the risk assessment.*

Informative Note 2: *For additional information about the process of verification, see IEC 61508, IEC 62061, and ISO 13849-1.*

3.82 well-tried component: A component which has been either:

- widely used in the past with successful results in a similar application(s);
  or
- made and verified using principles which demonstrate their suitability and reliability for safety-related applications.

3.83 well-tried safety principles: A principle of safety which has been validated for:

- how the expected modes of failure have been avoided;
- how faults have been avoided or their probability has been reduced.

4 How to Use ANSI B11.26

This standard shall be applied as follows:

1) Conduct a risk assessment and determine the risk reduction measures required to achieve acceptable risk (clause 5.1);
2) Identify those risk reduction measures that involve the SRP/CS (subclause 5.2);
3) Define safety function(s) - what needs to happen (if not done as part of the risk assessment - clause 5.3);
4) Determine the required reliability design specification for each safety function (e.g., performance level, category, safety integrity level) (clause 5.4);
5) Define the basic input, logic and output elements required to realize the safety function (clause 5.5);
6) Apply the general design requirements for all elements of the system (clause 6);
7) Determine Failure Modes/Fault Considerations to achieve reliability commensurate with the risk (clause 7);
8) Determine monitoring and diagnostic coverage to be applied, where required to achieve reliability that is commensurate with the risk (clause 8);
9) Apply specific design requirements for each circuit element (clauses 9, 10 and 11);
10) Evaluate the effectiveness of that system for the desired results (clause 12).

Informative Note: *Steps 5 through 10 represent an iterative design process. As the design progresses, the user may need to loop back to previous steps.*

ANSI B11.0 applies primarily to steps 1-4. ANSI B11.26 applies primarily to steps 5-10. Steps 3 and 4 can occur within the parameters of either standard.

Alternative methods used in lieu of lockout/tagout frequently include the use of safety-related parts of control systems and functional safety aspects. The requirements for an Alternative Method as defined in ANSI / ASSP Z244.1 include specifying and evaluating the reliability of SRP/CS related to the Alternative Method; ANSI B11.26 can be used to meet these requirements. See also ANSI / ASSP Z244.1.

4.1 Circuit Examples and Analysis Tables

Clauses 9, 10 and 11 of this standard contain specific design requirements for each element of the SRP/CS as well as application examples and analysis tables for category architectures (these examples do not imply any Performance Level or SIL). Example schematics, such as Figure 3 below, depict *examples* of how to integrate given devices for a required reliability design specification. Symbols used in these schematics are shown in Annex A.

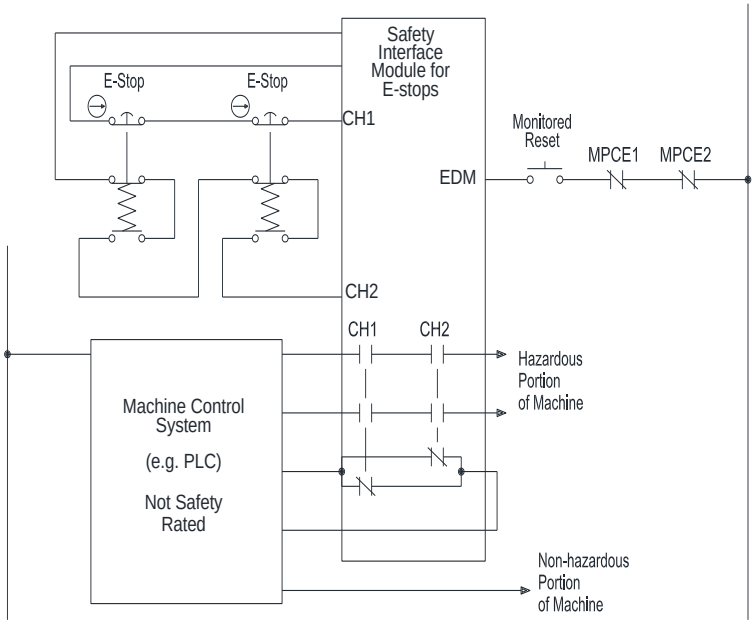


Figure 3: Sample schematic diagram depicting
"Multiple Dual Channel E-Stop with a Safety Interface Module (SIM)(Category3)"

Informative Note 1: *There are many ways to fulfil a given engineering requirement and the examples only present one option. These examples are not normative, nor intended to limit innovation or the advancement of technology*.
Informative Note 2: *The use of SIMs within the diagrams of this document does not preclude the use of a SPES (Safety Programmable Electronic System) to perform the functionality of the SIM, with properly designed software/logic.*

4.2 Circuit Analysis Tables

The "**Circuit Analysis Tables**" that follow each schematic example diagram contain four elements that describe the safety details for each safety circuit:

- Safety Function;
- Fault Considerations;
- Fault Exclusions; and
- Safety Principles.

Informative Note: *See Table 1.*

Table 1 — Content/Overview of a Circuit Analysis Table

Safety Function:	Purpose or goal of the safety circuit. That portion of the control system or engineering control – device that either eliminates or reduces exposure to a hazardous situation (from this document). Function initiated by an input signal processed by the SRP/CS to enable the machine (as a system) to achieve a safe state. This is also known as "Functional Safety." The function of the safety circuit, whose failure can result in an immediate increase in risk(s) (see also, ANSI B11.0 / ISO 12100).
Fault Considerations:	Consideration of faults and other related issues with the circuit that can lead to loss of the safety function as defined in this example circuit. What faults can occur that cannot be detected (see Annex F). For additional examples of fault consideration refer to Annex M, N, and O (see also, Annex B, C & D of ISO 13849-2).
Fault Exclusions:	Consideration of faults and other related issues with the circuit that may be excluded, and that can lead to the loss of the safety function as defined in this example circuit. What faults may be excluded and that cannot be detected. For examples of fault exclusion, refer to Annexes M, N, and O (see also, Annex B, C & D of ISO 13849-2).
Safety Principles:	Engineering recommendations, best practices and requirements as described in standards-related documents such as ANSI B11.19, NFPA 79, ISO 13849-2 etc., to achieve a desired risk level based on, or as part of, the requirements from an overall risk assessment such as ANSI B11.0.

This information provides a high confidence level that the safety functions described in the Table perform properly or will fail to a safe state or condition.

Informative Note 1: *As used throughout this document, the Circuit Analysis Table is for informational use and general guidance for design considerations, to provide comparisons for the various circuit options.*
Informative Note 2: *These "Circuit Analysis Tables" can also be used to provide a baseline comparison for other safety-related functions and the supporting safety circuits not covered in this document.*

5 Preparations for Functional Safety Design

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

ANSI B11.26 illustrates design concepts for safety-related parts of the control system to help mitigate the risks identified by a risk assessment. The general approach used in this standard follows the risk assessment process of ANSI B11.0 (and also, the same process as that used in ISO 12100) to identify hazards, assess the risks, and determine the need for risk reduction measures to achieve acceptable risk (see Figure 4 for an overview of the risk assessment process).

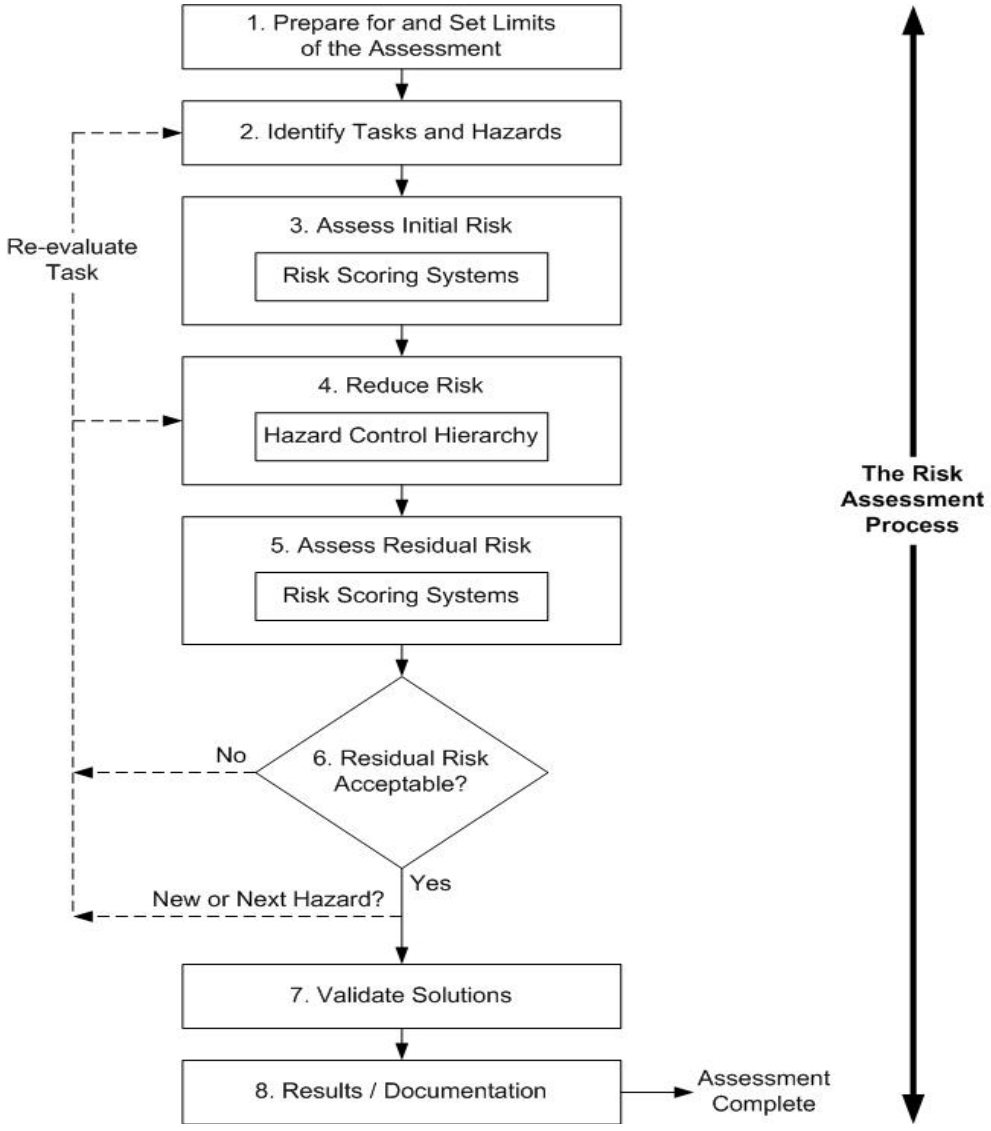


Figure 4: Overview of the risk assessment process

This standard requires that a risk assessment be completed for the machine or equipment. The risk assessment will determine the level of risk presented by the task/hazard pair. After risk evaluation, a decision is made whether risk reduction measures are required and what form they shall take. See ANSI B11.0 for further information on risk assessment and ANSI B11.19 for further information on risk reduction.

As part of the risk assessment, risks shall be assessed using a risk scoring system.

Informative Note 1: *A risk scoring system, whether qualitative or quantitative, is a tool used to characterize how these risk factors combine to determine a risk level. The risk factors typically evaluated are the severity of harm and the probability of occurrence of that harm. It is also important to consider the risk control methods of the systems to reduce risk in an acceptable manner. In selecting a risk scoring system, one or more of the following criteria should be considered.*

A risk scoring system that:

- *is specified by the user;*
- *is developed for the industry application;*
- *is published by an industry trade organization in some relevant technical literature;*
- *best suits the safety / health objectives of the organization;*
- *in addition to assessing risk, best prioritizes actionable risk reduction measures.*

Informative Note 2: *The selected system should appropriately address high severity of harm even when the probability of that harm is thought to be low. Severe injuries may occur during infrequent tasks, such as maintenance, machine jams, troubleshooting, etc.*

Informative Note 3: *An example of a two-factor risk scoring system using severity and probability is shown in Table 2. Other risk scoring systems may be used. See ANSI B11.0 for more information.*

Informative Note 4: *Examples used in ANSI B11.26 refer to risk levels as used in Table 2.*

Table 2 — Example Risk Scoring System

Probability of Occurrence of Harm	Severity of Harm			
	Catastrophic	Serious	Moderate	Minor
Very Likely	High	High	High	Medium
Likely	High	High	Medium	Low
Unlikely	Medium	Medium	Low	Negligible
Remote	Low	Low	Negligible	Negligible

A formal risk assessment is conducted to determine the risk level of each task-hazard pair using the risk assessment tool of choice. For each task-hazard pair whose level of risk is not acceptable, risk reduction measures shall be identified using the Hazard Control Hierarchy. These measures may be machine design or process changes, engineering controls (guards, control functions or devices), operational controls, personnel training, and personal protective equipment (PPE), singularly or in combination. Engineering control – devices are integrated into the SRP/CS through the implementation of Functional Safety.

5.2 Identify Risk Reduction Measures that Involve the SRP/CS

Some risk reduction measures involve safety functions which are performed/executed by a system of controls. The components in the system of controls that perform/execute the safety function(s) are the Safety-Related Part(s) of the Control System (SRP/CS). The SRP/CS may consist of a combination of an input device (e.g., interlocks, safety light curtains), a logic device (e.g., SIMs, safety controllers) and an output device (e.g., contactors, valves).

5.3 Define the Safety Function

The safety functions define how risks are reduced by risk reduction measures. A safety function shall be defined for each hazard risk reduction measure that is to be integrated into the SRP/CS. The description must show how the risks are reduced by the safety function. It is essential to provide a simple description of the safety function (what does it have to do?) to achieve the required safety with reasonable effort.

Informative Note: *Safety requirements specification (SRS) is one method/example of documenting safety functions.*

Care shall be taken when defining the safety function because it applies to both the inputs and outputs.

The complete safety function includes the entire functionality to reduce the risk to an acceptable level.

Informative Note: *See Table 3. For additional information see ISO 13849-1.*

Table 3 — Example of Relation between Hazard, Safety Related Control Function and Risk Reduction

Hazard / Task	Description of the Safety Function (what does it have to do?)	Initiation	Risk Reduction Measure (ANSI B11.19 / ISO 12100) Safety Requirement Specification (ISO 13849-1)
Entanglement hazard	No safety function	Not applicable	Fixed guard - Prevent contact with the hazard
Access to clear jam	No safety function	Not applicable	Movable guard - Prevent contact with the hazard
Open guard to clear jam	Stop hazardous motion when guard is opened	Opening guard changes the status of the interlock device	Protective stop function
Unexpected start up – entanglement hazard	Prevent unexpected start up when guard is open	Opening guard changes the status of the interlock device	Restart interlock function

5.4 Determine the Reliability Design Specification for Each Circuit

A reliability design specification shall be selected for a circuit using one or more of the following three methodologies:

- **Performance level** (PL) as contained in ISO 13849-1 and described in 5.4.1 and Annex B;
- **Categories** as described in 5.4.2;
- **Safety integrity level** (SIL) described in 5.4.3 and also described in IEC 62061.

Informative Note: *The selection of the methodology will depend on the design, construction, fault exclusions, installation, and maintenance of the safety-related function and a documented risk assessment.*

For each of the three methods, the specification refers to the design of the overall circuit. Capability ratings of individual components (i.e., a Category 3 rated interlock, PLe rated SIM) shall not be used to determine the reliability achieved by a given circuit.

For each SRP/CS, the required reliability design specification shall be determined and documented. The design specification is typically determined using three factors:

a) the severity of harm;
b) the frequency of exposure;
and
c) the possibility of avoidance.

Each factor usually has only two levels (slight/serious; frequent/infrequent; possible/not possible to avoid)

Informative Note: *These two factor systems have been found to be conservative in the specifications - erring on the side of increased safety.*

Using these factors as they apply to a given risk and its reduction, the level of severity, frequency of exposure, and possibility of avoidance is used to determine the design specification (required performance level [PL_r], category or SIL) for the safety function using the risk graph in Annex B, Annex C or IEC 62061.

A design specification used within the B11 series of American National Standards on machinery safety (and by OSHA) is "*Control Reliability.*" See ANSI B11.19 and Annex I for further information on this strategy. While the requirements of control reliability are not directly comparable to the requirements of ISO 13849-1 (1999) or ISO 13849-1 (2023), for the purposes of this standard, complying with Category 3 or 4 and/or Performance Level "d" or "e", at a minimum, will satisfy the requirements of control reliability.

The specification of the functional safety requirement(s) shall be commensurate with the risk. The greater the intended risk reduction to be provided by the SRP/CS, the higher the required reliability performance must be.

A machine often includes several safety functions and not every safety function will have the same reliability design specification.

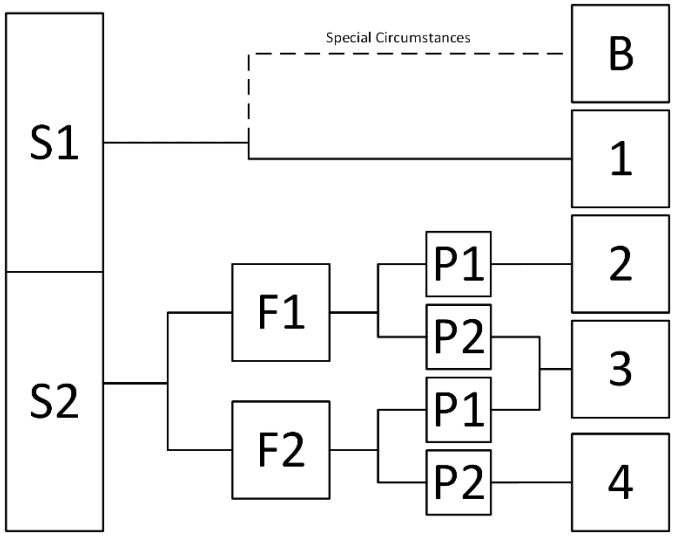
Designs for Category 3/4 and PLd/e functions are very complex. Care should be taken to accurately specify (especially, avoid the tendency to *over specify*) the safety requirement(s). The consequences of an overly complex design include, but are not limited to:

- increased total ownership costs;
- difficulties in troubleshooting;
- long repair time (poor MTTR, mean time to repair);
- the safety function may be bypassed or defeated;
- the design may be modified to a simpler design that is more readily understood (but negatively impacting the safety function);
- advanced training/competence required for maintenance personnel (availability of skilled personnel can impact CCF [common cause failure]).

Informative Note: *Using Performance Levels, higher levels of reliability can be achieved with a lower complexity of architecture (i.e., PLd achieved with Category 2 architecture). See Annex Q for more information.*

5.4.1 Categories

Categories can be used as an effective methodology to specify and evaluate SRP/CS reliability. Figure 5 can be used to determine the category for each safety function. While categories traditionally only address components and architecture, applying categories with design measures that address diagnostic coverage and, where applicable, common cause failure, yields a robust methodology.



Key

S	Severity of injury
S1	Slight injury (normally reversible)
S2	Serious injury or death
F	Frequency and/or exposure to hazard
F1	Low frequency or short duration of exposure
F2	High frequency or continuous exposure
P	Possibility of avoiding hazard or limiting harm
P1	High possibility of avoidance or limit of harm under specific conditions
P2	Scarcely possible of avoidance or limit of harm

Figure 5: Risk Graph for Categories

5.4.1.1 Architecture

The structure of the SRP/CS is a key characteristic having great influence on the reliability of a control circuit. The maximum achievable reliability is limited by the architecture. The design of the SRP/CS shall use a category of architecture or structure that is appropriate for the application. Architecture requirements apply to the Inputs, Logic, and Outputs of a control system.

Informative Note: *Categories were first introduced as a complete functional safety methodology in EN 954-1 (1996), and Categories remain a key part of the more advanced PL functional safety methodology in ISO 13849-1.*

5.4.1.2 Diagnostic Coverage (DC)

Diagnostic Coverage (DC) is a measure of a system's ability to detect failures.

Informative Note: *DC is typically implemented by monitoring the SRP/CS for faults or failures. When a fault or failure occurs, the monitoring provides an indication of the fault or failure (e.g., perform the safety function with redundant component(s) and prevent re-initiation of the hazard, a message, light, alarm, etc.).*

Designers shall provide a DC level for each SRP/CS that is commensurate with the risk. The greater the intended risk reduction to be provided by the SRP/CS, the higher the DC must be.

5.4.1.3 Common Cause Failure (CCF)

Common cause failures are failures of multiple devices due to the same cause, and not necessarily consequences of each other.

For any structure which employs monitoring, a common cause failure could render the monitoring function inoperative.

Informative Note: *For example: Two switches on a rotary cam switch used to monitor the position of a Punch Press crank. A failure of the cam switch drive system, such as a dropping of the coupling chain, will make both switches inoperative, but still in agreement so that the fault will not be detected solely by monitoring the switches, thus losing the ability to determine crank position.*

Designers shall address CCF for each SRP/CS (Cat 2, 3, and 4) and provide design measures that are commensurate with the risk.

5.4.1.4 Category design considerations

Designers shall confirm that the SRP/CS meets the applicable requirements and is sufficient for the required design specification, as described below.

Category B:

- is designed in accordance with relevant standards;
- can withstand the expected influences;
- the occurrence of a fault can lead to loss of the safety function.
  Informative Note: *Typically, Category B circuits may not have diagnostic coverage.*

Category 1 (includes Category B):

- well-tried components and well-tried safety principles are used;
  Informative Note: *Typically, Category 1 circuits may not have diagnostic coverage.*

Category 2 (includes Category B and well-tried safety principles):

- has diagnostic coverage appropriate to level of risk. See clause 8; and at a minimum, the safety function shall be checked at suitable intervals by the machine control system;
- the occurrence of a (single) fault can lead to loss of the safety function between the checks;
- the loss of safety function is detected by the check (automatic or manual);
- is protected from common cause failure as appropriate to the level of risk. See subclause 7.1.
  Informative Note: *A suitable frequency of checking (periodic test interval) will be dependent on the reliability of components and the probability of failure. A tolerable probability of failure will be determined when the design specification is verified to meet the intent of the risk assessment.*

Category 3 (includes Category B and well-tried safety principles):

- a single fault does not lead to loss of the safety function;
- accumulation of undetected faults can lead to loss of the safety function;
- has diagnostic coverage appropriate to the level of risk. See clause 8; at a minimum, whenever reasonably practicable, a single fault is detected (i.e., some but not all faults will be detected);
- is protected from common cause failure as appropriate to level of risk. See subclause 7.1.

Category 4 (includes Category B and well-tried safety principles):

- a single fault does not lead to loss of the safety function;
- has diagnostic coverage appropriate to the level of risk. See clause 8; at a minimum, the single fault is detected at or before the next demand upon the safety function. If this is not possible, then an accumulation of faults shall not lead to loss of the safety function;
- the faults will be detected in time to prevent loss of the safety function;
- is protected from common cause failure as appropriate to level of risk. See subclause 7.1.

5.4.2 Performance Level (PL) Methodology (ISO 13849-1)

5.4.2.1 General

The PLs range from ***a*** to ***e***, where PLa has the highest failure rate to danger, while PLe has the lowest failure rate to danger. In order for the SRP/CS to be capable of meeting the design specification, it shall have a PFH of less than the maximum allowed by the PL_r.

Informative Note: *A DC_{avg} ≥ 60% for the channels in structure Categories 2, 3 and 4 are considered acceptable for monitoring the failures of a safety channel.*

The performance level for a particular SRP/CS depends mainly upon:

- the reduction in risk to be achieved by the safety function to which the subsystem contributes;
- the required performance level (PLr);
- the technology(ies) used;
- the risk arising in the case of a fault(s) in that part;
- the possibilities of avoiding a fault(s) in that part (systematic faults);
- the mean time to dangerous failure ($MTTF_D$);
- the diagnostic coverage (DC);
  and
- the common cause failure (CCF) in the case of categories 2, 3 and 4.
  Informative Note: *A higher level of reliability may be achieved using a combination of better components, diagnostic coverage, and measures to prevent common cause failures.*

The SRP/CS shall be in accordance with the requirements of one or more of the five categories specified in Annex C, summarized in 5.4.1.1 and described in clause 6 of ISO 13849-1.

5.4.2.2 Select Components

Designers shall confirm that the components selected for the control system meet the applicable requirements and are sufficient for the required application.

Informative Note: *One method of evaluating components is the $MTTF_D$. See Annex D, Section 1.*

The supplier instructions and specifications of components and devices shall be followed. The supplier of the device or component shall be consulted whenever conditions or questions arise that are not covered by the supplier's instructions.

5.4.2.3 Fault considerations

Designers shall identify potential faults that could lead to the loss of the safety function. System or component failures shall be considered and managed.

Informative Note: *See Annexes F and G for further information.*

5.4.2.4 Diagnostic Coverage (DC)

Diagnostic Coverage (DC) is a measure of a system's ability to detect failures.

Informative Note: *DC is typically implemented by monitoring the SRP/CS for faults or failures. When a fault or failure occurs, the monitoring provides an indication of the fault or failure (e.g., perform the safety function with redundant component(s) and prevent re-initiation of the hazard, a message, light, alarm, etc.).*

Designers shall provide a DC level for each SRP/CS that is commensurate with the risk. The greater the intended risk reduction to be provided by the SRP/CS, the higher the DC shall be.

Informative Note 1: *See Annex D, Section 2.1 on DC and D2.2 on DC_{avg} for further information.*

Informative Note 2: *DC, for a component or subsystem is expressed as a ratio of the probability of the number of detected dangerous failures divided by probability of the total number of dangerous failures, both detected and undetected, and stated as a percentage. The range of % DC is divided into four levels: **None**, **Low**, **Medium**, and **High** (see also, Table 4).*

Table 4 — Diagnostic Coverage (from ISO 13849-1 Table 7)

Diagnostic Coverage	
Denotation	Range
None	DC < 60 %
Low	60 % ≤ DC < 90 %
Medium	90 % ≤ DC < 99 %
High	99 % ≤ DC

Note 1 - For subsystems consisting of several parts, use an average value DC_{avg} for DC.
Note 2 - The choice of the DC ranges is based on the key values 60%, 90% and 99%, also established in other standards dealing with DC of tests. Investigations show that (1 – DC) rather than DC itself is a characteristic measure for the effectiveness of the test. (1 – DC) for the key values 60%, 90% and 99% forms a kind of logarithmic scale fitting to the logarithmic PL scale. A DC value less than 60% has only a slight effect on the reliability of the tested system and is therefore called "none." A DC value greater than 99% for complex systems is very hard to achieve.
To be practicable, the number of ranges was restricted to four. The indicated limited values of this table are assumed within an accuracy of 5 %.

5.4.2.5 Common Cause Failure (CCF)

Common Cause Failures are failures of multiple devices due to the same cause, not consequences of each other. For any structure which employs monitoring, a common cause failure could render the monitoring function inoperative.

> ***Informative Note:*** *For example: Two switches on a rotary cam switch used to monitor the position of a Punch Press crank. A failure of the cam switch drive system, such as a dropping of the coupling chain, will make both switches inoperative, but still in agreement so that the fault will not be detected solely by monitoring the switches, thus losing the ability to determine crank position.*

Designers shall provide a CCF level for each SRP/CS that includes monitoring of the channels (Categories 2, 3, and 4). Using Table 12, the design and construction shall achieve a minimum accumulative evaluation score of 65 points. Only full achievement of any one category for all parts of the SRP/CS may be awarded the right column points. If 65 points are not achieved, further measures to reduce CCF are needed to satisfy the monitoring capability for the safety function, or the SRP/CS is considered to be un-monitored and a structure of only B or 1 may be awarded depending on the $MTTF_D$ of the channels.

> ***Informative Note:*** *A means to estimate the CCF can be found in Annex D Section 3. A score is given for each of several measures which may be utilized to reduce CCF. Summing up the relative value of these measures results in a score between 0 and 100 points. For a high level of risk reduction, it is desirable to achieve a higher level of design to reduce CCF.*

5.4.2.6 Calculating a PL

Once the elements of 5.4.2.1 through 5.4.2.5 have been developed and specific components have been selected from a particular supplier(s), the PL achieved can be calculated for a specific example(s) in ANSI B11.26. Component suppliers provide reliability data for their components in online libraries that can be used in performing the calculations.

5.4.3 Safety integrity level (SIL)

Safety Integrity Levels (SILs) per IEC 62061 may also be used to achieve functional safety. The SIL methodology tends to be used more frequently in processing applications rather than for machinery.

5.5 Define Basic Input, Logic and Output Elements Required

The safety function is carried out by elements of the safety related part(s) of the control system. The elements are characterized as inputs, logic, and/or outputs. Appropriate input, logic, and output elements shall be selected and interconnected to achieve the SRP/CS that provides the desired safety function and a level of reliability commensurate with risk. Typically, the input and logic portions of the SRP/CS are primarily electronic/electric, but fluid power logic control circuits exist and, in some cases, can mimic the electric control circuit.

5.5.1 Inputs

The function of input devices is to provide an operator input or detect a state of the machine or safety function (e.g., Guard Closed). Input devices may be manual operator controls (pilot devices), sensors or encapsulated subsystems comprised of input / logic /output elements.

5.5.2 Logic

Logic monitoring circuits of the SRP/CS provide the relationship between the inputs and outputs, and also monitor for:

- faults in input circuit elements;
- faults internal to the logic elements;
- faults in the response of output elements (power control device(s)).

The logic circuits may use designs incorporating discrete component logic or may incorporate Safety Interface Modules (SIMs). The function of logic circuits is to provide an output for the power control device(s) that is used to stop a hazardous motion or condition, or to initiate a safe start function.

Informative Note: *Where the examples shown in this standard make use of SIMS to provide logic and monitoring functions, properly applied and rated PES can also be utilized. See 10.2, ISO 13849-1 and (ANSI) Technical Report B11.TR4 for additional information on the software requirements for such systems.*

Some input devices may also perform the function of the logic monitoring circuit (i.e., safety presence sensing devices). In some machines with low evaluated risk hazards, the input devices may be directly input to a machine control system (see 6.1.1).

5.5.3 Outputs

Outputs are generally the portions of the control system that ultimately and directly enable or control the power to the machine actuators (motors, clutch/brake, fluid operated cylinders, etc.) that produce hazardous motion or situations. Commonly, the final elements in output circuits are a power control device such as contactors, drives, or fluid power valves. This document refers to these power control devices as Machine Primary Control Elements (MPCE).

Informative Note: *This document uses the terminology MPCEx (where x = 1, 2, etc.) in the diagrams to identify that multiple MPCE devices may be in use.*

6 General Design Requirements

This clause provides overall general design requirements for the SRP/CS regardless of the required reliability. The design requirements are based on good engineering practice and are considered to be well–tried.

Informative Note: *See ANSI B11.19 for further information.*

To achieve the rated performance of safety devices, all supplier's installation requirements shall be followed.

Informative Note: *It is possible to achieve acceptable performance in novel or "off label" applications, however such situations require full analysis and engineering supervision.*

The design of the SRP/CS shall take into account the intended use and reasonably foreseeable misuse of the machine, including the tasks and hazards that are necessary for the operation and maintenance of the machine.

The control system design shall allow all necessary tasks to be performed with acceptable risk.

Informative Note: *There is no need to apply the strategy of B11.26 for risk reduction on non-safety-related parts of control systems or purely functional elements of a machine (see ISO/TR 22100-2:2013).*

6.1 Integration of SRP/CS in the Overall Machine Controls

Integration of the SRP/CS with the machine control system shall be such that:

- the machine control is responsible for properly controlling the process;
- the SRP/CS is responsible for reducing the risk associated with a hazard, and where appropriate, providing status information to the machine control.

The machine control shall not override the safety function of the SRP/CS. Any suspension of a safety function shall be performed by the SRP/CS.

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

Figure 6 shows an overview of the interaction between non safety-related machine control components and the SRP/CS components.

Informative Note 1: *For risk assessments that permit Category B or Category 1 applications, the safety-related input may be used as an input to the machine control and the machine control actuators may be used to control low risk hazards without separate SRP/CS augmentation.*

Informative Note 2: *Some machine control systems integrate the SRP/CS into the machine control as a single entity with the appropriate safety performance.*

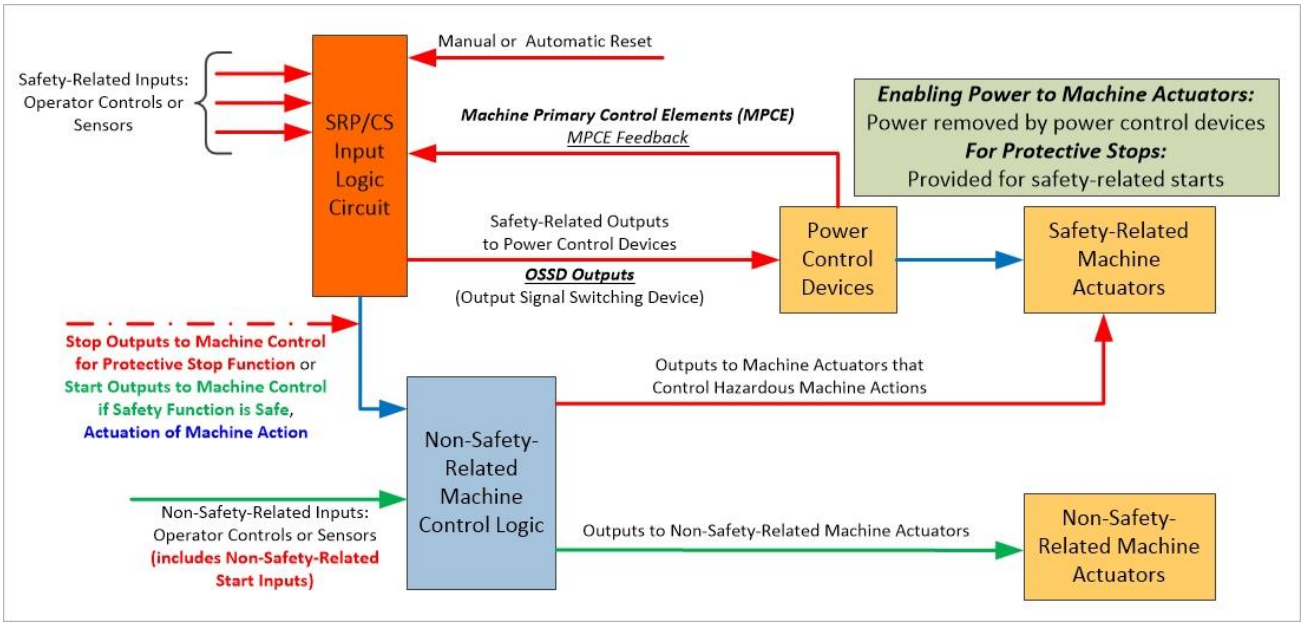


Figure 6: Machine Control integrated with the Safety-Related Part of a Control System (SRP/CS)

6.2 Specific Functions

6.2.1 Protective Stop

A protective stop allows for an orderly cessation of motion for risk reduction purposes, which typically results in a stop of motion and subsequent direct removal of power from the machine actuators (assuming this does not create additional hazards). In certain applications, the protective stop allows for the machine actuators to remain with power available.

In the event of a protective stop being issued by the SRP/CS, the machine control should properly respond by (including, but not be limited to):

- turning OFF appropriate outputs;
- taking appropriate action associated with the stop command;
- updating any machine status that may be required;
- display status information.

Interface with the machine is accomplished by providing a stop command (signal) to the machine control from the SRP/CS which is maintained for the entire time the SRP/CS is actuated, preventing the re-initiation of a hazard. The stop signal to the machine control shall be removed by restoring (resetting) the SRP/CS to its permissive state (power to machine actuators) before the machine control can restart machine action.

6.2.2 Start Function

The machine start function is not generally shown in the diagrams within this standard. NFPA 79 and IEC 60204-1 require that the reclosing or resetting of an engineering control – device that provides a protective stop shall not initiate hazardous machine motion or operation. The Start Function is typically provided by the machine control only when the SRP/CS safety function(s) has been reset.

Where the safety function of the SRP/CS is the safe start of machine action (such as two-hand control devices), the SRP/CS provides a signal to the power control device to enable (provide power to) the output actuator that controls machine action, and a start signal to the machine control to activate the output actuator.

The safety circuits covered by this standard provide energy to the hazardous portion of the machine and do not start the hazardous machine motion or operation. These safety circuits shall perform a permissive function to the machine control prior to the start of the hazardous operation.

Special conditions apply for presence sensing device initiation (PSDI). See ANSI B11.0 and ANSI B11.19. ISO 12100 refers to PSDI as *sensitive protective equipment* when used for cycle initiation. Special conditions also apply for interlocking guards with a start function (control guards).

6.3 Electrical Design Requirements

6.3.1 Opening of Circuits for Time Dependent Functions

Where the speed of opening a circuit impacts the proper safety function (i.e., a light curtain application with a calculated safety distance), the circuit shall be designed to minimize the effects of stored energy. Examples of such designs include, but are not limited to:

- interrupting the DC voltage output side rather than the AC voltage input side of the power supply (for DC control circuits supplied by an AC driven power supply);
- reducing the number of components between the final output contacts and the device being controlled;
- interrupting the output side of a drive versus interrupting the input power to the drive.

6.3.2 Positive/Negative Logic

Positive logic typically uses current sinking inputs (i.e., a signal device applies power) and current sourcing outputs (i.e., the output device supplies power) such that any short circuit to the reference potential or a wire-breakage are interpreted by the inputs and loads as an “off state.” This minimizes the possibility of a fault resulting in an unintended action by the machine.

The methodology of positive logic is typically applicable to PES/PLC logic but can also be incorporated into relay or other forms of machine control logic.

Current sourcing inputs and current sinking outputs (negative logic), have a very low degree of fault tolerance and are not recommended as primary logic.

Informative Note 1: *Negative logic is not recommended by IEC 1131-2 as the primary means of logic.*
Informative Note 2: *Hard wired SRP/CS portions of the control system will typically provide single fault tolerance and software-based SRP/CS may handle one or more faults depending on their sophistication.*

The use of negative logic as the second channel of a diverse redundant Dual Channel system (e.g., NO/NC switching or complementary switching) to minimize the possibility of common mode failures is acceptable.

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

It is important not to remove power from the non-safety PES/PLC power supply or the logic module as a normal part of the safety function, to allow the use of diagnostics to minimize troubleshooting time.

Generally, a protective stop circuit is either placed in the supply line to the output card or is placed in one or more of the output circuits controlling hazardous motion. A status signal from the engineering control – device should be connected to the PLC input for feedback purposes.

If the method of interfacing the protective stop circuit results in removing supply power from a PES/PLC output/card:

- The PES/PLC outputs shall directly control the last electrically powered device or actuator (e.g., valves and solenoids). They should not control interposing relays or contactors, unless they meet the same or greater level of safety performance requirements (e.g., a single failure does not result in an unsafe condition);
- The only source of energy supplied to the outputs, and the devices connected to those outputs, is controlled by the protective stop circuit. Relay output cards should only be used if the source of energy that is switched by the relay output card can be interrupted by the safety device or system;
- Dropping power to the supply for the PES/PLC output card shall remove all sources of energy that can cause hazardous motion (i.e., no secondary sources of power). The resulting uncontrolled, Functional Stop Category 0 (per NFPA 79) shall not cause additional hazards.
  Informative Note: *A failure mode to be considered on outputs with a multiple feed is a fault where an externally supplied voltage to a single output could provide a source for other outputs.*

6.3.4 Electro-Mechanical Contact Requirements

Circuit design shall ensure that the current interrupted by each set of contacts is above the supplier's minimum current or power value, and below the maximum. Overcurrent protection shall be provided such that maximum current values are not exceeded in the event of a fault.

Refer to the supplier specifications to determine minimum current or power requirements in the intended application.

Informative Note 1: *Minimum current for proper operation of contacts may be 30 mA to 50 mA at 21-24V DC. Some contact designs incorporate bifurcated design contacts which may be as low as 2 mA to 10 mA.*
Informative Note 2: *Contacts that are gold flashed to prevent corrosion are especially delicate. On such contacts, the peak current should never exceed the supplier recommended maximum to prevent loss of the flash and subsequently the corrosion protection.*
Informative Note 3: *Many PLC input cards (opto-coupler isolated) may require pull-up or pull-down resistors (e.g., 1KΩ @ 1W in a +24V DC circuit) to ensure a minimum current flow to keep contacts clean and free of corrosion.*

6.4 Fluid Power (Pneumatics and Hydraulics) Design Requirements

Fluid power portions of a safety circuit are subjected to similar design criteria as the electrical portion to satisfy the safety requirements. For example, merely removing control voltage from a directional control valve does not ensure that the SRP/CS will perform as required. The entire circuit, including the MPCE, must be included in the design and analysis. Proper fluid conditioning can increase the mean time to dangerous failure (e.g., filtration, cooling, moisture removal).

6.4.1 Protective Stops in Fluid Power Systems

Typically, protective stop functions within fluid power systems can be realized through one or more of the following methods:

- blocking of the fluid power energy source;
- removal of electrical power from the safety valve(s), conversion source (pump) and/or directional control valves;
- exhausting or removal of energy;
- selective trapping of fluid to maintain actuator position and prevent unintended hazardous movement caused by other energy sources such as gravity, springs, etc.;
- reducing energy to an acceptable level;
- using a mechanical means (e.g., rod locks) to prevent or control hazardous motions.

6.4.2 Reset Function of Safety Valves

The reset of safety valves, with fault detection functions, may be either automatic or manual. The automatic or manual resetting of a valve shall not create a hazard.

Informative Note: *Dual channel safety valves may require the de-energization of the command signal(s) followed by the fault reset command to clear the fault condition.*

6.4.3 Reapplication of Pressure

The reapplication of pressure shall not create a hazard (e.g., rapid or unintended movement). An abrupt change in position due to the reapplication of full pressure to a vented system can cause rapid motion producing a trapping hazard as well as damage the actuators or machine components causing premature mechanical failures. In pneumatic systems, soft start valves or inlet flow controls may be used to prevent this condition.

6.4.4 Fluid Power Valve Crossover

The influence of valve spool shifting crossover conditions on the circuit shall be taken into account for fluid power valves being used in safety applications.

There are two types of crossover conditions; (see crossover position in Annex H):

- Open crossover – fluid pressure (energy) will be open between the supply, an outlet, and an exhaust/return port;
- Closed crossover – fluid pressure (energy) will be trapped at the outlet port with no flow path to supply or exhaust/return port.

These conditions might not be disclosed or only be partially disclosed in supplier information.

Valve functions and schematics typically depict 2 or 3 position valves indicating their normal operating positions. During operation, elements transit from an at-rest condition to one (or two) energized positions. This provides an infinite number of crossover positions as the valve elements shift.

6.5 Mechanical design requirements

Mechanical elements typically form a part of the SRP/CS and play a role in functional safety.

Informative Note: *Examples of safety-related mechanical elements include, but are not limited to:*

- *mounting hardware;*
- *brakes;*
- *couplings;*
- *shafts;*
- *cams;*
- *followers;*
- *chains, belts, cables;*
- *clutches;*
- *screws;*
- *shear pins;*
- *guides;*
- *bearings;*
- *springs;*
- *rupture discs.*

6.5.1 Design Requirements

When used as part of the SRP/CS, mechanical elements shall meet the reliability requirements determined in subclause 5.4.

Where mechanical elements carry a safety performance rating, the rating shall not be lower than the requirement determined in subclause 5.4.

6.5.2 Design Considerations

The following design considerations should be applied as part of the design process for the SRP/CS.

6.5.2.1 General Information

Some of the basic safety principles provided include, but are not limited to:

- use of suitable materials and adequate manufacturing;
- correct sizing and geometry;
- proper selection, combination, arrangements, assembly and installation of components/systems;
- use of the de-energization principle;
- proper fastening/constraint;
- limitation of the generation and/or transmission of force and similar parameters;
- limitation of range of environmental parameters;
- limitation of speed and similar parameters;
- proper reaction time;
- protection against unexpected start-up;
- simplification;
- separation;
- proper lubrication;
- proper prevention of the ingress of contaminants.

In the application of mechanical elements, the following well-tried safety principles shall be considered:

- use of specific materials and manufacturing methods;
- use of components with oriented failure mode;
- over-dimensioning/safety factor;
- safe position;
- increased off force;
- careful selection, combination, arrangement, assembly and installation of components/systems related to the application;
- careful selection of fastening related to the application;
- positive mechanical action;
- redundancy;
- limited range of force and similar parameters;
- limited range of speed and similar parameters;
- limited range of environmental parameters;
- limited range of reaction time;
- limited hysteresis.

7 Fault Consideration

Fault consideration includes the evaluation of failure modes that could affect the ability of a specific circuit to perform its safety function. The acceptance of failure modes and their probability of occurrence is dependent on the required level of circuit reliability. Fault consideration shall be performed as part of the design process. See Annex G for more information on identification and analysis of failures.

Informative Note: *Examples include Fault Tree Analysis, Failure Modes, Effects and Criticality Analysis, Event Tree Analysis and Load-Strength reviews.*

7.1 Common Cause Failure

Common cause failures are failures of multiple devices due to the same cause, and not as consequences of each other. As a part of fault consideration during the design process, susceptibility to common cause failure shall be evaluated for each SRP/CS that includes monitoring and/or two channel structure (i.e., -- Cat 2, 3, and 4). Resistance to common cause failure within a design shall be commensurate with the risk.

Informative Note 1: *For example: Two switches on a rotary cam switch used to monitor the position of a Punch Press crank. A failure of the cam switch drive system, such as a dropping of the coupling chain, will make both switches inoperative, but still in agreement so that the fault will not be detected solely by monitoring the switches, thus losing the ability to determine crank position.*

Informative Note 2: *For examples of means to reduce the risk of common cause failure, see Annex D section 3.*

7.2 Fault Exclusion

During the analysis, certain faults may be uncovered that cannot be detected during operation without undue economic cost(s). Further, the probability that these faults might occur can be made extremely small by using mitigating design, construction and installation techniques. Under these conditions, the faults may be excluded from further consideration. Recommended preventive maintenance procedures shall be included in the justification to ensure that the basis of the exclusions remain valid.

Fault exclusion may be based on but not limited to:

- the low probability of occurrence of some faults;
- well-tried designs (engineering safety practices);
- application-specific technical requirements for the specific hazard.

Justification shall be given in the technical documentation for any excluded faults. See also, Annexes L, M, N, and O for additional information (ISO 13849-2:2012 Annexes A, B, C and D also provide guidance on fault exclusion and its justification).

7.3 Electrical Failure Modes

Failure modes of circuit devices, actuators, and the controller (including interfaces) shall be evaluated. The failure modes to be considered include but are not limited to:

- short circuit of outputs, external wiring, or output devices/actuators, such as the loss of the switching function due to a short to power across the output contacts;
- PES/PLC program alteration (unsecured logic), programming errors or loss of PES/PLC memory;
- failure or fault of the safety device (e.g., internal components);
- false actuator/input signal (noise, external signal error, off-state currents or internal shorted/open PES/PLC input);
- false ON condition of outputs (false trigger, off-state currents);
- uncontrollable oscillating outputs;
- openings in external wiring (e.g., broken wires, corroded terminal contacts);
- complete or partial loss of power;
- increase of device response time;
- common mode failures;
- common cause failures;
- other failures (or combinations of failures) that result in unexpected or unintended operation.
- other failures caused by external electrical influences:
  - rapid changes in applied voltage or current;
  - electrical noise and transients;
  - surge current, over current, or over voltage.

- other failures caused by electrical noise/ transients generated by:
  - large, fast changing, (switching) inductive loads or other energy storing devices;
  - motor starters;
  - welding equipment;
  - variable speed drives;
  - high voltage (e.g., 480 V AC);
  - electromagnetic radiation (e.g., Radio Frequency transceiver – “walkie talkies”);
  - electro-static generators;
  - magnetic fields;
  - environmental (e.g., lightning).

7.4 Fluid Power Failure Modes

7.4.1 General Failure Modes

Failure modes of fluid power components shall be evaluated. The failure modes to be considered include but are not limited to:

- **Seal Failure** – There can be many different seals within a valve or cylinder depending on its design. This failure can be leakage past a seal, expansion of seals due to contaminants, or complete loss of the seal being digested into the system. Leaking or failing seals in valves can result in sluggish behavior thereby slowing or preventing valve response or can initiate valve shifting. Leaking or failing seals in cylinders or holding valves can result in unintended motion due to the release of pressure that should be trapped to maintain cylinder position;

- **Spring Failure** – Spring fracture or complete breakage can slow or prevent valve response. Broken spring parts can also contaminate the valve internal flow paths and prevent complete sealing of the valve. Spring designs that prevent interleaving of the spring halves can eliminate some valve failure modes;

- **Coil Failure** – The physical failure of a coil can result in the valve not functioning or functioning at an unacceptable level. The broken part can result in the element being controlled by the coil being jammed into an unknown position;

- **Complete or Partial Loss of Electrical Power** – The loss of power below the coil operating requirements will result in the valves de-energizing. Due to other valve failure modes, it may not be assumed that the valve will return to its de-energized position;

- **Complete Loss of Fluid Power** – The complete loss of supply pressure to a valve will result in the loss of downstream pressure unless a checking device is utilized downstream. Piloted valves will de-energize as the pilot pressure drops below the minimum operating pressure;

- **Diminished Response Time Fault** – A fault caused by the unacceptable increase in the shift time required for the valve. Non safety-rated power valves can become sluggish thereby increasing shift time. For applications which involve stopping time/distance (safety light curtains, interlocked guards, etc.), an increase in shifting time will void the safety distance previously calculated and can render the safeguarding as no longer adequate. See also, ISO 19973-2;

- **Valve Element Position Failure** – Valve elements can stick at any position within its travel range;

- **Position Fault** – A failure of the valve to completely shift to its intended controlled (energized or de-energized) position is a position fault. See also, crossover position in Annex H;

- **Partial Loss of Fluid Power** – The partial loss of supply pressure to a valve will cause loss of downstream pressure unless a checking device is utilized to specifically prevent this. Air piloted valves can de-energize or partially de-energize resulting in the valve being stuck in a crossover position;

- **Pilot Section Failure** – The pilot portion of a solenoid piloted valve has the same failure modes as the main elements of the valve. The resulting effects of this failure on the main valve elements shall be considered such as unintended main valve element shifting. A failure mode of concern is the ability of a pilot valve to initiate a motion without being given an electrical command signal. A pilot operated valve design should be evaluated to determine if there are failure modes which would initiate a motion, and what additional controls might need to be installed to mitigate this risk. Both main and pilot valves have similar failure modes regarding a valve's inability to return to the de-energized position. The pilot operated valves have an additional potential inability of the valve to exhaust or drain the pilot pressure thereby preventing the main spool from returning;

- **Mounting Orientation** – The effects of gravity on valve and cylinder elements shall be considered and the supplier mounting recommendations followed. Worn out spools, or lapped design spools in a valve mounted in a vertical position could experience a spool shift from vibration if the solenoid moves the spool vertically up and is then de-energized;

- **Inertial Forces** – Valves mounted on moving machine surfaces or subjected to vibration and shock loading can change internal valve position due to these external forces. If these external forces are present, consult the supplier(s) of safety valves for their valve's shock rating. Valve elements shall be mounted perpendicular to the motion to prevent unintended movement;

- **Conductor (hose/tube/pipe) / Connector Failure** – The load can drop, and the conductor can cause injury or damage to equipment (whipping action).

7.4.2 Pneumatic Failure Modes

Failure modes specific to pneumatic circuits shall be evaluated. The failure modes to be considered include but are not limited to:

- **Temperature** – Using pneumatic safety devices outside of their recommended temperature range can result in changed response time or malfunction due to the effect of temperature expansion of different materials used in the valve elements and the temperature effects on valve lubrication;
- **Moisture** – Water extracted from the compressed air in the system due to condensation will affect valve and system response depending on where the water accumulates. Pneumatic systems are sized based on the desired response of the machinery which is based on the volume, pressure, and flow rates throughout the system. The accumulation of water will alter the volume which will in turn affect the pressure, flow, and response of the system. Water can cause varnish to form which can cause the valve to stick;
- **Electrical** – noise and transients can initiate valve operation;
- **Lubrication** – Air line atomized or mist type lubricated circuits require service at frequent intervals. If the lubricators are not maintained and allowed to run dry, the lubrication can become tacky resulting in a decreased level of reliability. Directional control valves, main spools and pilot valves can stick, resulting in failure. Non-lubricated or pre-lubricated systems are preferred because of an inherently higher level of reliability;
- **Line blockage or muffler restriction** – Pneumatic exhaust time can be increased significantly due to line blockages and muffler restrictions due to contamination;
- **Ingress of contaminants**:
  - internally generated – valve and cylinder wear can create contaminants;
  - externally generated – these contaminants can be created by the fluid supply or by the process.

  Informative Note: *See ingress of contaminants in Annex H. Proper fluid conditioning can increase the mean time to dangerous failure (e.g., filtration, cooling, moisture removal).*

7.4.3 Hydraulic Failure Modes

Failure modes specific to hydraulic circuits shall be evaluated. The failure modes to be considered include but are not limited to:

- **Temperature** – temperatures above 55 °C (131 °F) cause a degradation of the oil and its additives reducing its lubrication, and anti-oxidation capability. This leads to increased valve wear, loss of reliability and premature failure;
- **Moisture** – water in the hydraulic fluid, both suspended and dissolved, leads to cavitation, heat damage, and increased corrosion;
- **Air** (bubbles or dissolved) in the hydraulic system leads to cavitation-driven erosion damage. It also reduces the incompressibility of the oil (reduces bulk modulus, making it 'spongy');
- **Particle Contamination** – hydraulic systems are closed systems; contaminants can remain in the fluid unless removed via a filter or other means:
  - internally generated – pump, valve and cylinder wear can create contaminants;
  - externally generated – these contaminants can be created by the supply or by the process.

  Informative Note: *See ingress of contaminants in Annex H. Proper fluid conditioning can increase the mean time to dangerous failure (e.g., filtration, cooling, moisture removal).*

The ability of the components of the hydraulic system to perform their function reliably is primarily dependent on the condition of the fluid.

Listed below are a series of informative design considerations that help ensure that the system will meet the required reliability potential. In the case of hydraulic installations, since they are closed systems, managing wear is important as the byproducts of component wear contaminate the system, thereby becoming the source of further wear and increasing the rate of component degradation. Design considerations include but are not limited to:

- Keep working fluid below 55 ºC;
- Supply electronic temperature monitoring;
- Mount tank away from other heat sources and structures which limit convection cooling;
- Add heat exchanger. Thermal calculations should be based on 38 ºC ambient conditions;
- When using fixed displacement pumps, use low pressure bypass for idle periods instead of dead-heading pump over system pressure relief/reducing valve, or use pressure compensated pumps;
- Keep fluid clean;
- Proper filtration;
- Electronic monitoring of filter pressure drop;
- Tank vent filter element sized 3 µm or less;
- Pre-filter make-up and re-fill oil to 10 µm or less. This is dependent on components;
- For servo valves, add a 10 µm or less in-line filter immediately up-stream of the valve;
- Maintain wipers on cylinder rods;
- In-line particle monitoring or regular laboratory evaluation of fluid;
- Minimize water entry into the fluid;
- Water adsorption element in reservoir vent filter;
- Periodic inspections of heat exchanger, general plumbing and fluid sampling;
- Minimize dispersed and dissolved air in fluid;
- Reduce fluid turbulence in tank;
- Keep tank as large as practicable to reduce fluid cycles per hour;
- Add baffles to control flow and add fluid stationary time;
- Keep fittings and joints tight as they may allow ingress of air;
- Use of power area ventilation can reduce steam, vapors, smog, and airborne dirt particles in the environment and keep them from entering the system.

  Informative Note: *For additional considerations on hydraulic systems, see ISO 4413.*

7.4.4 Avoiding an overly complex design

The pneumatic circuit can become complex, especially Category 3 or 4 and PL d or e, when measures are applied for hazards such as a damaged hose and stored energy (including compressed air in the cylinder and gravity). Pneumatic safety design shall be as simple as possible and avoid over-designing (e.g., achieving a higher PL than PLr).

The consequences of the complex pneumatic circuit include but are not limited to:

- long repair time (poor MTTR, mean time to repair);
- the pneumatic circuit may be more complex than people understand;
- competence/training for CCF (common cause failure) may not be achieved;
- advanced training and skills may be required for troubleshooting and repairs.

When the estimated risk is high, the reliability required for the pneumatic safety system can be Category 3 and/or PL=d. When consequences from the complexity arise, the Category 2 PL=d circuit can be considered over the Category 3 circuit. See Annex Q for more information.

7.5 Mechanical failure modes

7.5.1 Tampering / Defeat

The most common means of tampering with mechanical elements is physical removal or bypassing of an element.

The following shall be considered to reduce the risk of tampering with mechanical elements:

- location of devices / elements within enclosures or guarding;
- tamper resistant fasteners;
- tamper evident fasteners / enclosures;
- safety wire / tab washers.

7.5.2 Failure Modes

Failure modes specific to mechanical elements include but are not limited to:

- wear / corrosion;
- untightening / loosening;
- fracture;
- deformation by overstressing;
- stiffness / sticking;
- contamination.

8 Monitoring / Diagnostic Coverage

Depending on the required reliability for a given safety function, some level of diagnostic coverage or monitoring may be required.

Informative Note 1: *For examples of monitoring methods and their contribution to diagnostic coverage ratings, refer to Annex D.*

Informative Note 2: *Methods of providing the logic for monitoring functionality include a "Safety Interface Module" (SIM) or a safety controller.*

When required by the selected architecture, a redundant device provided to enhance the reliability of the SRP/CS shall be monitored to ensure failures are detected by the safety control system.

Where fault detection by the process is the sole means of monitoring, the fault conditions and appropriate actions shall be provided in the information for use.

Informative Note: *One method of providing Diagnostic Coverage is "fault detection by the process." Typically, this is possible when a failure within elements of the SRP/CS will be evident through a process malfunction, without additional sensors or logic. An example would be a stuck directional valve that serves both process and safety functions will result in machine failure since the driven cylinder will be out of position.*

.

Non safety-rated devices used as part of the monitoring function shall be included in the Fault Considerations and shall be provided with additional means to enhance reliability.

Informative Note: *Examples of such means include but are not limited to:*

- *monitoring of the change of state;*
- *cross monitoring with primary device;*
- *enforced periodic testing.*

8.1 Electrical Monitoring / Diagnostic Coverage Methods

Where monitoring of primary device functionality is provided by additional or auxiliary contacts, such contacts shall be mechanically linked, force guided, or otherwise constructed to ensure that the state of the monitoring contacts correctly indicates the state of the primary device.

8.1.1 Input Masking on Series Connected Devices

Where monitoring is required on input devices connected in a series, means to detect masking or written procedures for sequential testing shall be provided.

Informative Note: *The most commonly effected devices are interlocks and emergency stops.*

When monitoring two or more individually mounted interlocks (see Figure 7), a faulty interlock will be detected if it fails to operate as the guard opens. With at least one channel open, the safety interface module will de-energize its output relays and disable its reset function until the input requirements are met (the faulty interlock is replaced). However, if a fully functional interlock is opened and the faulty interlock is closed before the good one, the failure is not detected.

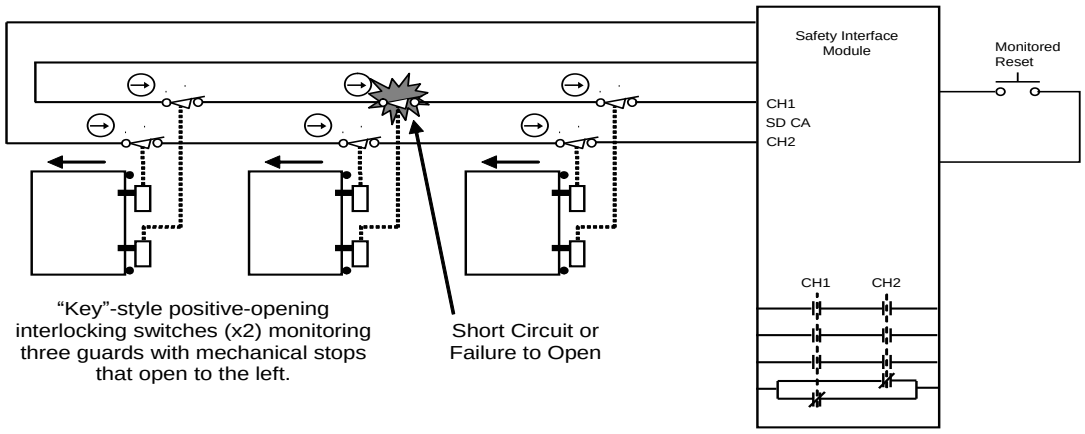


Figure 7 – Input masking on series connected devices

8.2 Fluid Power Monitoring / Diagnostic Coverage Methods

The methods used for fluid power monitoring / diagnostics are:

- Direct monitoring – monitoring the valve spool position with a sensor directly mounted on the valve;
- Indirect monitoring – monitoring the valve operation by a pressure switch, electrical position monitoring of actuators, etc.;
- Monitoring through the process – monitoring the valve operation through the machine cycle.

Non safety-rated devices used as part of the monitoring function shall be included in the Fault Considerations and shall be provided with additional means to enhance reliability.

Informative Note: *Examples of such means include but are not limited to:*

- *monitoring of the change of state;*
- *cross monitoring with primary device;*
- *enforced periodic testing.*

8.2.1 Direct monitoring

Where direct monitoring of the valve internal elements is provided by a limit switch, such contacts shall be mechanically linked, force guided, or otherwise constructed to ensure that the state of the monitoring contacts correctly indicates the state of the primary device. These contacts shall be monitored in the SRP/CS or during the process cycle to verify that the contacts change state with the device being monitored.

Where direct monitoring of the valve internal elements is provided by a non-contact sensor, the change of state shall be monitored in the SRP/CS or during the process cycle to verify that the contacts change state with the device being monitored.

Informative Note 1: *Direct monitoring indicates internal valve component position and may not indicate low flow or leakage in all valve types and designs.*

Informative Note 2: *Low flow or leakage may be a 'safe' or 'dangerous' failure depending on the safety function.*

8.2.2 Indirect monitoring

In some applications, non safety-rated devices can be used to achieve indirect monitoring. See Annex O.

Informative Note: *Indirect monitoring of some fluid power functions using safety-rated devices may not be practicable due to the nature of the device or process. These devices include pressure switches, end of stroke position sensors, linear displacement sensors, flow switches, level switches, and temperature switches.*

Pressure switch settings used for safety monitoring functions shall indicate a safe level of pressure (i.e., not minimum operating pressure).

8.2.3 Monitoring by the process

"Monitoring (fault detection) by the process" can only be applied if the safety-related component is involved in the production process, e.g. a standard PLC or standard sensors are used for workpiece processing and as part of one of the two channels executing the safety function. The appropriate DC level depends on the overlap of the commonly used resources (logic, inputs, outputs).

Informative Note: *An example would be a stuck directional valve that serves both process and safety functions will result in machine failure since the driven cylinder will be out of position.*

8.2.4 Monitoring of three position valves

Where spring-centered valves do not have a monitoring function, or the continued function of the machine does not indicate the ability of the valve to spring center, the centering function shall be tested at suitable intervals. Methods to test spring-centered valves can include the following:

- energize a solenoid and immediately de-energize to center. Monitor actuator position to see if it reaches its end stop or if it halts as expected. This shall be done in both directions;
- with both solenoids de-energized, monitor pressure switches at both ports. This shall be done after a move in each direction and could be part of the normal machine cycle.

8.2.5 Monitoring of response time

Where the stopping time can be affected by the fluid power device response time, the fluid power device response timing or the system stopping time shall be monitored. See safety distance / stopping performance information in ANSI B11.19.

9 Design Requirements – Input Devices (Engineering Control – Devices)

9.1 Emergency Stop Devices

The types of devices for emergency stop (E-stop) include, but are not limited to, the following:

- pushbutton-operated device;
- rope pull (cable pull) operated device;
- foot-operated device without a mechanical guard;
- rod-operated device;
- push-bar-operated device.

9.1.1 Design Requirements

The E-stop function shall not be capable of being muted or manually suspended. E-stop devices shall conform to the requirements in ANSI B11.19.

Informative Note: *See also, NFPA 79, IEC 60204-1 and ISO 13850 for additional information on emergency stop devices.*

9.1.2 Design Considerations

The design considerations in 9.1.2.1 and 9.1.2.2 shall be applied as part of the design process for the SRP/CS.

9.1.2.1 Tampering / Defeat

Emergency stop devices are not typically defeated or tampered with unless unintended actuation occurs. Good design practices that reduce the risk of tampering and defeat include but are not limited to:

- careful consideration in locating devices;
- device selection for vibration resistance;
- location of cable pulls away from moving product/mechanisms.

9.1.2.2 Failure Modes

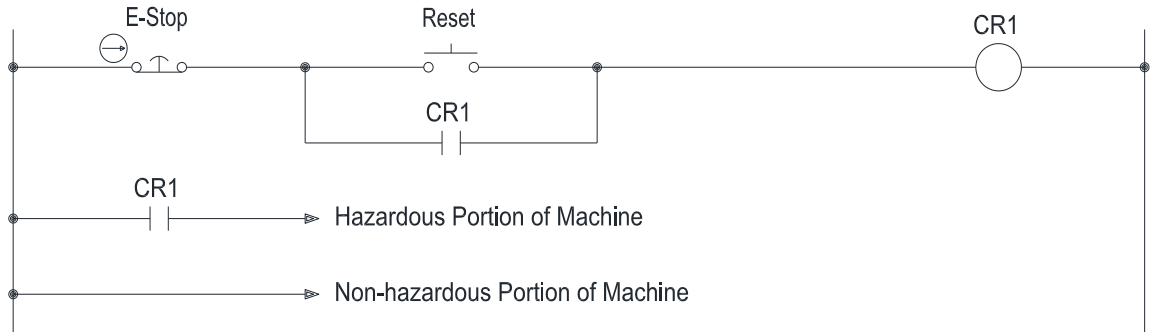
Failure modes specific to emergency stop devices include but are not limited to:

- E-stop contacts falling off the pushbutton actuator - Detection or prevention of a separated contact block on the E-stop device is accomplished by and is specific to the device supplier;

  Informative Note: *Examples include but are not limited to monitored contact blocks, individually mounted contact blocks, and contact blocks mechanically prevented from separating from the actuator.*
- failure of pulleys and similar mechanical elements in cable pull systems resulting in high actuation force, excessive cable slack, or failure to actuate;
- contamination / obstruction preventing operation.

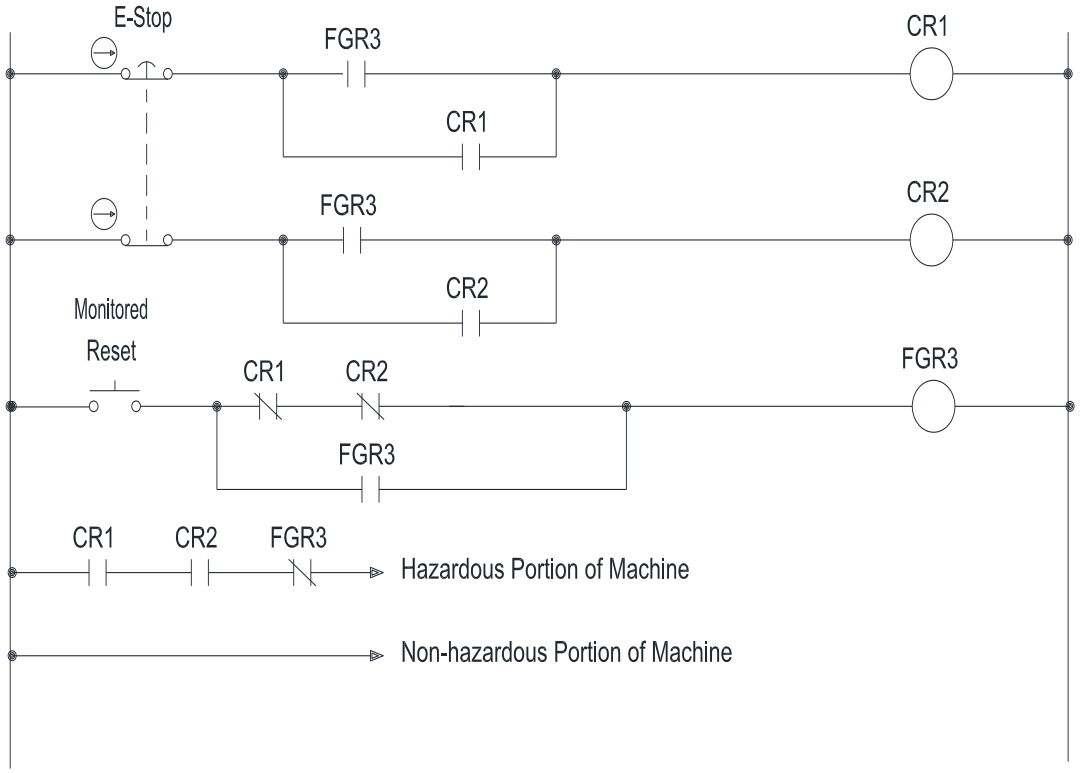
9.1.3 Application Examples

9.1.3.1 Single Channel E-stop Using a Control Relay (Category 1)



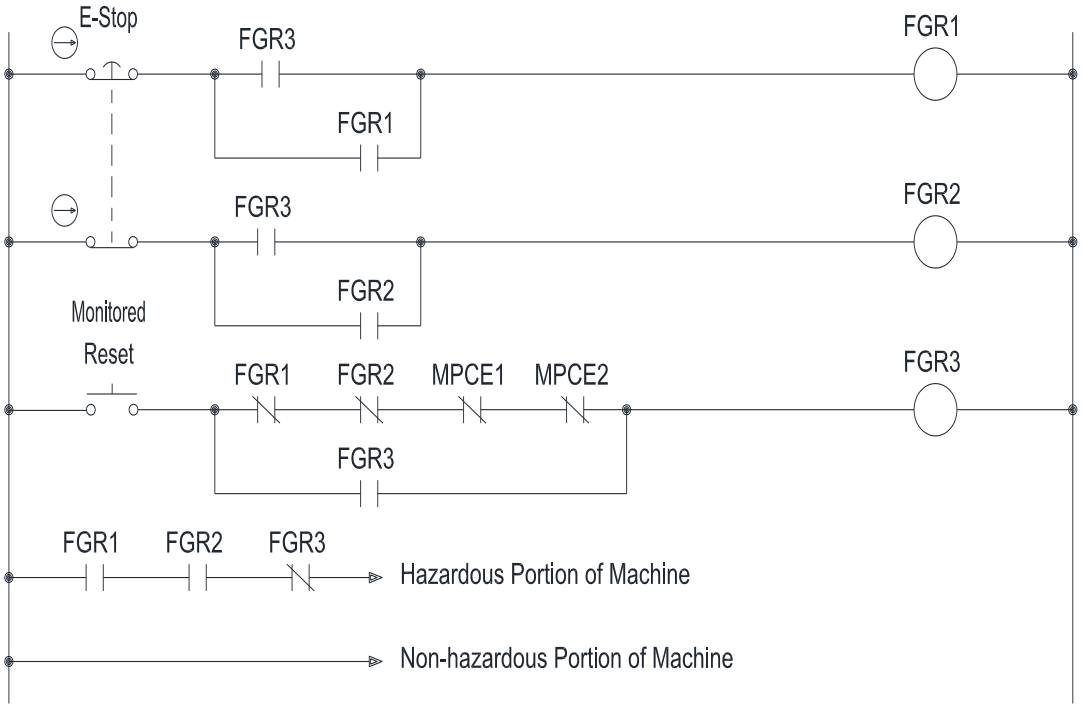
Safety Fxn:	When the E-stop is pressed, the power to the hazardous portion of the machine is removed.
Faults to Consider:	Stuck armature in CR1 or welded contacts of CR1. Wiring short from power to the coil of CR1. Reset contacts are held closed. E-stop contacts falling off the pushbutton actuator.
Fault Exclusion:	Welded E-stop contacts may be excluded since direct opening action contacts are used. Catastrophic failure of the E-stop device may be excluded if designed and installed per ISO 13850 and tested at periodic intervals.
Safety Principles:	When the E-stop is pressed, the power to the coil of CR1 is removed. The normally open contacts of CR1 open and remove power to the hazardous portion of the machine. While the E-stop is in the depressed position, power to the hazardous portion of the machine remains off. When the E-stop is reset, the hazardous portion of the machine will not automatically restart. Restart is accomplished by a separate deliberate action. ***Informative Note:*** *Use of a latching E-stop by itself to replace the CR1 contact in the "hazardous portion of the machine" can reduce the number of failures to consider and is also a common design.*

9.1.3.2 Dual Channel E-stop Using Redundant Control Relays (Category 2)



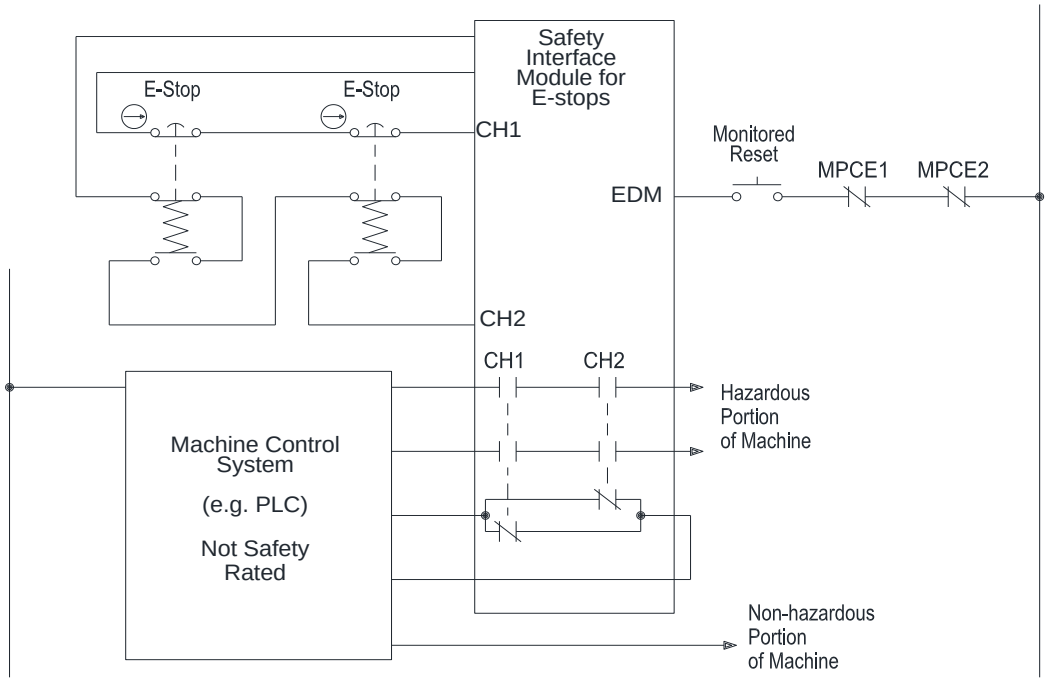
Safety Function:	When the E-stop is pressed, the power to the hazardous portion of the machine is removed.
Faults to Consider:	Stuck armature in CR1 or CR2. Welded contacts of CR1 or CR2. Wiring short from power to the coil of CR1 or CR2. The reset contacts are held closed or shorted. E-stop contacts falling off the pushbutton actuator.
Fault Exclusion:	Welded E-stop contacts may be excluded since direct opening action contacts are used. Catastrophic failure of the E-stop device may be excluded if designed and installed per ISO 13850 and tested at periodic intervals.
Safety Principles:	When the E-stop is pressed, the power to the coils of CR1 and CR2 is removed. The normally open contacts of CR1 and CR2 open and remove power to the hazardous portion of the machine. While the E-stop is in the depressed position, power to the hazardous portion of the machine remains off. When the E-stop is reset, the machine will not automatically restart. Restart is accomplished by a separate deliberate action. Simple redundancy is not adequate to achieve Category 3. An automatic monitor circuit to test for consistency in CR1 and CR2 may provide a warning or a stop command to the non-safety portion of the machine logic.

9.1.3.3 Dual Channel E-Stop Using Force-Guided Relays (FGR) and Cross Monitoring (Category 3)



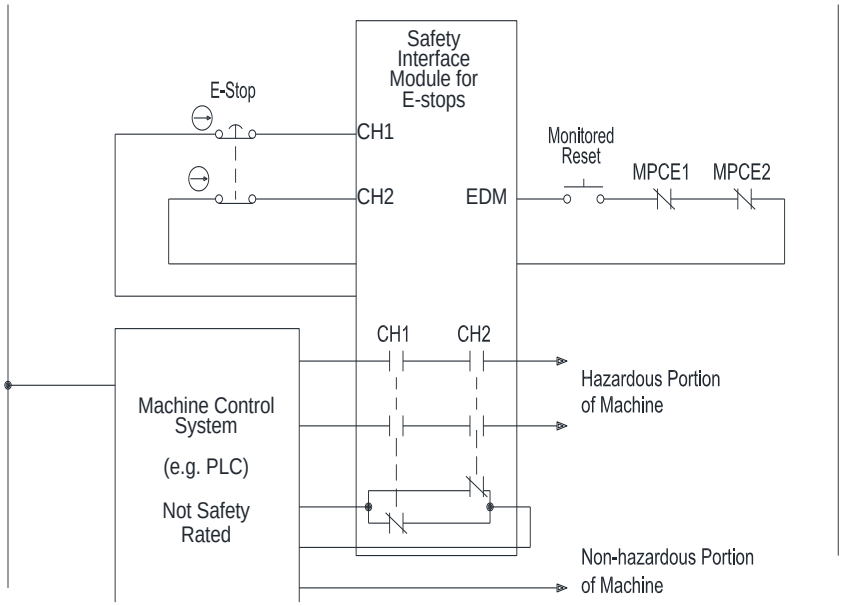
Safety Function:	When the E-stop is pressed, the power to the hazardous portion of the machine is removed.
Faults to Consider:	E-stop contacts falling off the pushbutton actuator. Wire to wire short between the two E-stop N.O. contacts.
Fault Exclusion:	Welded E-stop contacts may be excluded since direct opening action contacts are used. The N.C. and N.O. contacts of FGR1, FGR2 or FGR3 cannot be in the closed state at the same time since mechanically linked contacts are used. Catastrophic failure of the E-stop device may be excluded if designed and installed per ISO 13850 and tested at periodic intervals.
Safety Principles:	When the E-stop is pressed, the power to the coil of FGR1 and FGR2 is removed. The normally open contacts of FGR1 and FGR2 open and remove power to the hazardous portion of the machine. While the E-stop is in the depressed position, power to the hazardous portion of the machine remains off. When the E-stop is reset, the hazardous portion of the machine shall not restart. Restart is accomplished by a separate deliberate action. Category 3 requires redundancy, the addition of MPCE1 and MPCE2 is implied in the diagram. Monitoring all devices is considered best practice. To achieve Category 4 and prevent a short circuit between E-stop contacts, use complementary switching or bi-polar switching.

9.1.3.4 Multiple Dual Channel E-Stop with a Safety Interface Module (SIM)(Category3)



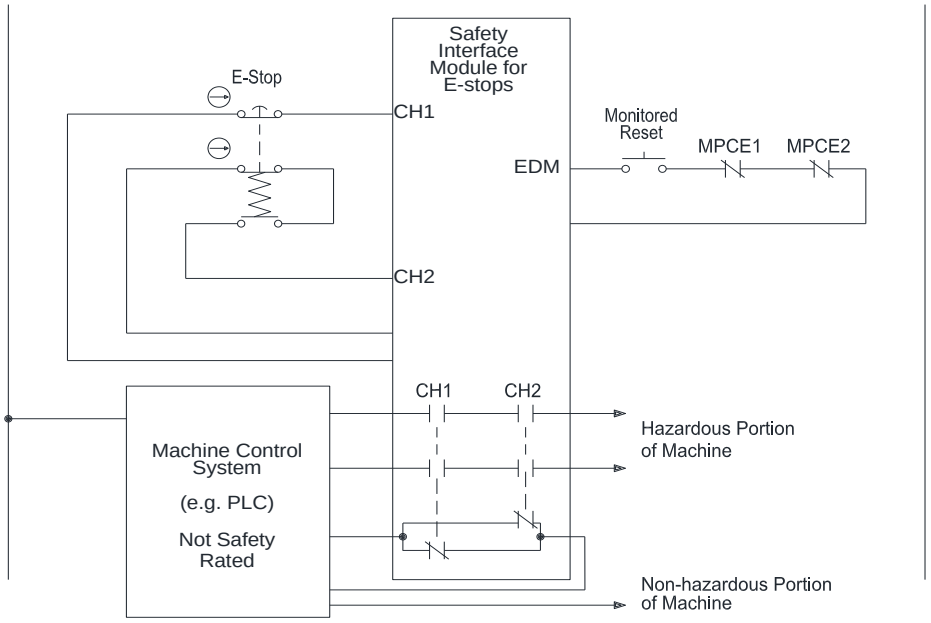
Safety Function:	Pressing the E-stop removes power to the hazardous portion of the machine.
Faults to Consider:	Wiring short across one set of E-stop contacts will be masked by the other E-stop contact.
Fault Exclusion:	Welded E-stop contacts may be excluded since direct opening action contacts are used. Catastrophic failure of the E-stop device may be excluded if designed and installed per ISO 13850 and tested at periodic intervals.
Safety Principles:	While the E-stop is in the depressed position, power to the hazardous portion of the machine remains off. When the E-stop is reset, the hazardous portion of the machine does not automatically restart. Concurrent operation of multiple E-stop devices should be discouraged. Category 3 requires redundancy (MPCE1, MPCE2). Monitoring both devices is considered best practice. The fallen contact solution is diagrammatic as there are many solutions which do not include an additional spring-loaded contact.

9.1.3.5 Single Button Dual Channel E-stop with a SIM (Category 4)



Safety Function:	Pressing the E-stop removes power to the hazardous portion of the machine.
Faults to Consider:	E-stop contacts falling off the pushbutton actuator.
Fault Exclusion:	Welded E-stop contacts may be excluded since direct opening action contacts are used. The N.O. contacts of the monitoring safety relay failing shorted may be excluded because they are redundant and cross monitored. A short across the reset contact or a stuck reset button is excluded because the safety interface relay is looking for a change of state. Catastrophic failure of the E-stop device may be excluded if designed and installed per ISO 13850 and tested at periodic intervals. ***Informative Note:*** *When modifying this diagram by adding multiple pushbuttons in series, concurrent operation of multiple pushbuttons shall be excluded.*
Safety Principles:	While the E-stop is in the depressed position, power to the hazardous portion of the machine remains off. When the E-stop is reset, the hazardous portion of the machine may not restart. Restart shall be accomplished by a separate deliberate action. If the E-stop contact block falls off the panel, the hazardous portion of the machine stops.

9.1.3.6 Single Button Dual Channel E-stop w/ Self-Monitoring and a SIM (Category 4)



Safety Function:	While the E-stop is in the depressed position, power to the hazardous portion of the machine remains off.
Faults to Consider:	None to consider.
Fault Exclusion:	Welded E-stop contacts may be excluded since direct opening action contacts are used. Catastrophic failure of the E-stop device may be excluded if designed and installed per ISO 13850 and tested at periodic intervals. The N.O. contacts of the monitoring safety relay failing shorted may be excluded because they are redundant and cross monitored. A short across the reset contact or a stuck reset button is excluded because the safety interface relay is looking for a change of state.
Safety Principles:	When the E-stop is reset, the hazardous portion of the machine does not automatically restart. If the E-stop contact block falls off the panel, the circuit does not lose the safety function. At a minimum, the E-stop device should be designed and installed per ISO 13850 and tested at periodic intervals. The fallen contact solution is diagrammatic as there are many solutions which do not include an additional spring-loaded contact.

9.2 Mechanical (Contacting) Interlocking Devices

9.2.1 Design Requirements

Safety functions that include guard interlocking extend beyond the SRP/CS to include the mechanical mounting and interface with the guard(s). The reliability of these mechanical functions shall be included in the determination of the overall reliability of the SRP/CS.

Informative Note: *See ANSI B11.19, ISO 14119 and IEC 60947-5-1 for additional design, construction, installation, operation and maintenance requirements.*

9.2.2 Design Considerations

The following design considerations should be applied as part of the design process for the SRP/CS.

9.2.2.1 General Information

9.2.2.1.1 Description of Positively Driven Interlock

Electromechanical switches used for guard interlocking (e.g., key or tongue, roller, hinge, cam, etc.) typically have positively driven N.C. contacts to indicate the state of the guard being monitored.

Positively driven operation is the full separation of the normally closed contact through a non-resilient linkage (e.g., not dependent upon springs) as the direct result of a specified movement of the actuator when it is disengaged or moved from the home position (see Figure 8).

Normally open contacts generally depend on spring action to accomplish the switching action and are not considered “positively driven.” The normally open contacts are typically only used for auxiliary monitoring, not for safety-related purposes.

Another common design characteristic is that positively driven interlocks also have electrically isolated contact pairs.

Informative Note 1: *See IEC 60204-1, ISO 14119, and IEC 60947-5-1 for further information.*
Informative Note 2: *Interlocks are described as in their NORMAL state when the interlocked device is in the CLOSED position, actuator inserted. They are OPERATED when the interlocks are OPENED, or the actuator is withdrawn. The N.C. contacts are closed when the interlocked device is closed i.e., the safe condition.*

9.2.2.1.2 Description of Positive-Mode vs. Negative-Mode Mounting (Actuation)

The proper installation of positively driven interlocks typically results in a positive mode of actuation. Mounting in a positive mode, such that when the actuator is disengaged or moved from the home position, forces a non-resilient linkage (i.e., rigid elements) to open the normally closed contact (see Figure 8). This force ensures that the switching action occurs.

When a single interlock is used to monitor the position of a guard, the interlock should be mounted (actuated) in the positive mode. Mounting in the negative-mode (or non-positive mode) is typically only allowed when a second positively driven interlock is mounted in the positive-mode. This will provide diverse redundancies to minimize common mode failures.

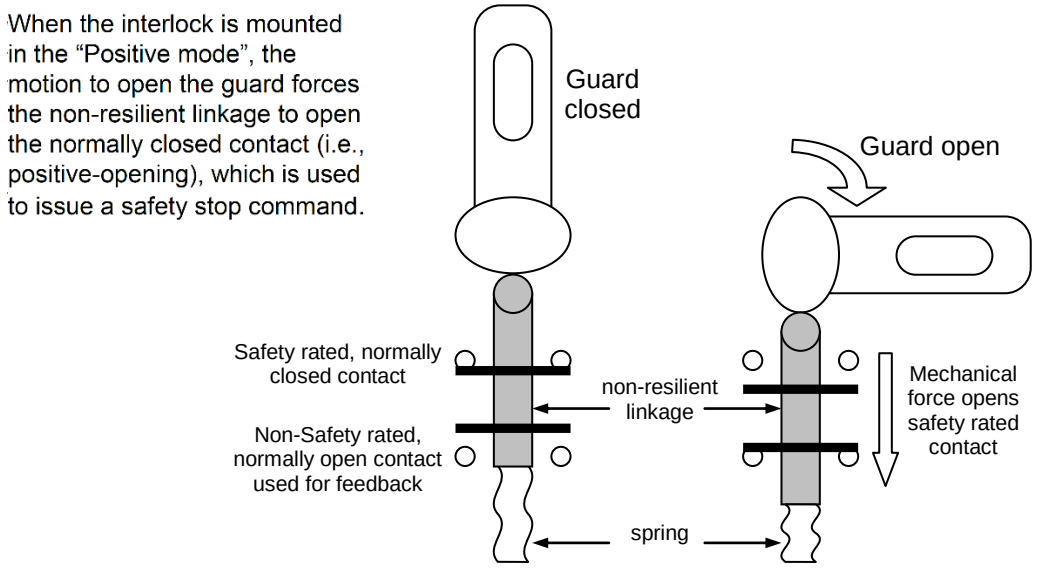


Figure 8: Positive mode operation

9.2.2.1.3 Interlocking device "type" Characteristics

Interlocks are grouped into numeric "types" 1 through 5. Mechanical contact interlocking devices are types 1, 2 and 5. See below for the characteristics of each, as well as tampering/defeat (9.2.2.1.3.2) and failure modes (9.2.2.1.3.3). Interlocks with non-contact related design are types 3 and 4; see also, 9.3.

Type 1 interlocking devices typically exhibit the following characteristics:

- direct mechanical action of the actuator on the actuation system of the position switch;
- direct opening action of the N.C. contact of the position switch due to direct mechanical action;
- fails to danger in case of:
  - failure of the mechanical link between guard and position switch (wear or breaking of the actuator);
  - misalignment between the position switch and the cam;
  - loosening of the limit switch;
  - loosening or breaking of the actuator arm;
  - trip mechanism (cam, machine) falls away.

Type 2 interlocking devices typically exhibit the following characteristics:

- easy principle for integrated guard locking devices;
- especially suitable for use on the opening edge of a movable guard;
- direct mechanical action on the actuator of the position switch;
- direct opening action of the N.C. contact of the position switch due to direct mechanical action;
- can be damaged due to misalignment during the machine life cycle;
- can be degraded by pollution;
- impact from the actuator can cause harm to persons;
- fails to danger in case of:
  - actuator stays in the head (through breakage or use of cheater key);
  - actuator breaks or actuator mounting screws fall off;
  - switch head is broken off the switch body.

Informative Note: *For Type 3 and Type 4 interlocking devices, see 9.3.3.6.*

Type 5 interlocking devices typically exhibit the following characteristics:

- the output system and the trapped key interlocking system are typically physically separated and functionally linked by the transfer of the key;
- keys are coded to only fit into the corresponding locks;
- ensures a sequence of operation;
- the designated sequence results in a safe state of the machine;
- potential failure modes in case of:
  - ingress of particles, chips, or dust exceeding the specified IP rating;
  - spare keys accessible;
  - loosening of the access lock or actuator from the guard.

9.2.2.1.3.1 Design considerations for the application of trapped key interlocking systems

A key transfer plan shall be designed for each trapped key interlocking system. This transfer plan shall detail the key path. Key coding shall be established based on the safety-related specifications. Type 5 interlocking devices shall be in accordance with ANSI B11.19:2019, 10.3.

Informative Note: *A key transfer plan is a drawing, scheme or diagram depicting the trapped key interlocking system with its individual type 5 interlocking devices and the sequence(s) in which they are to be operated.*

Where type 5 interlocking devices are used as part of the SRP/CS, the devices shall meet the behavior requirements of the required safety performance (see 5.4.2). Type 5 interlocking devices are typically single channel architecture for the mechanical parts.

Where type 5 interlocking devices are used within a category 3 or 4 architecture, one of the following shall be implemented:

a) two interlocking devices;
b) one single channel interlocking device achieving the relevant category behavior and requirements;
Informative Note: *The category behavior includes the definition of the category, but not necessarily the designated architecture.*
or
c) one single channel interlocking device where all possible faults are evaluated, and any dangerous failure modes are eliminated or proven to be highly unlikely. In this case, Category 3 behavior may be assumed, and diagnostic coverage is not necessary when all single faults that cause a loss of the safety function are excluded. Non-mechanical aspects of a trapped key interlocking system shall be in accordance with the category requirements.
Informative Note 1: *The category behavior includes the definition of the category, but not necessarily the designated architecture.*
Informative Note 2: *Over-dimensioning of critical parts or designing parts with intentional weak points to create fail-to-safe modes are methods that can be used to address the identified dangerous failure modes.*

Breakage and deformation faults for safety-relevant mechanical components (except for springs) can be excluded if:

- a safety factor of 4 compared to the expected forces is verified by calculation or suitable testing;

or

- a safety factor of 2 compared to the expected forces is verified by calculation or suitable testing;

and

- if the quality of safety-relevant mechanical components is verified by means of continuous quality assurance measures.

9.2.2.1.3.2 Tampering / Defeat

Tampering with interlocks can be a foreseeable misuse of safety functions. Measures to reduce the risk of tampering include but are not limited to:

- use of tamperproof screws for interlock/actuator mounting;
- multiple interlocks with simultaneity test imposed by the logic portion of the circuit;
- automatic, periodic testing;
- function test built into each cycle, e.g., cycle cannot start without logic seeing guard open and close, anti-tie-down for safeguarding.

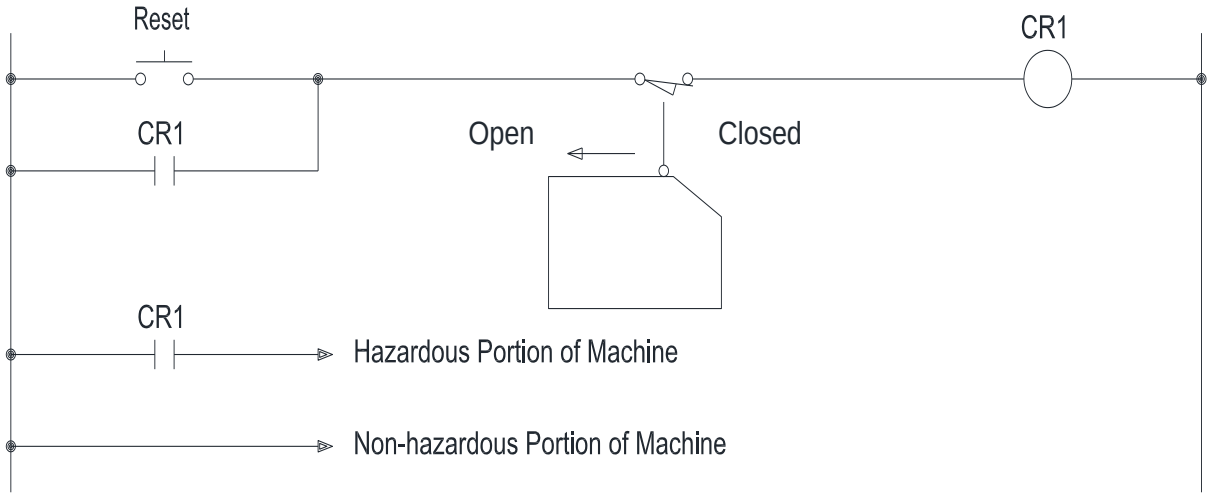
9.2.2.1.3.3 Failure Modes

Failure modes specific to interlocks include but are not limited to:

- exceeding rated opening and closing speed;
- use of the interlock as a mechanical stop or as a mechanical alignment mechanism;
- very slow actuation of the switch can cause issues with monitoring contacts (contact) teasing;
- contamination, corrosion, physical damage;
- failure of mounting interface with guard;
- fatigue and breakage of the actuator;
- failure of spring driven switch functions in Negative-mode mounting.

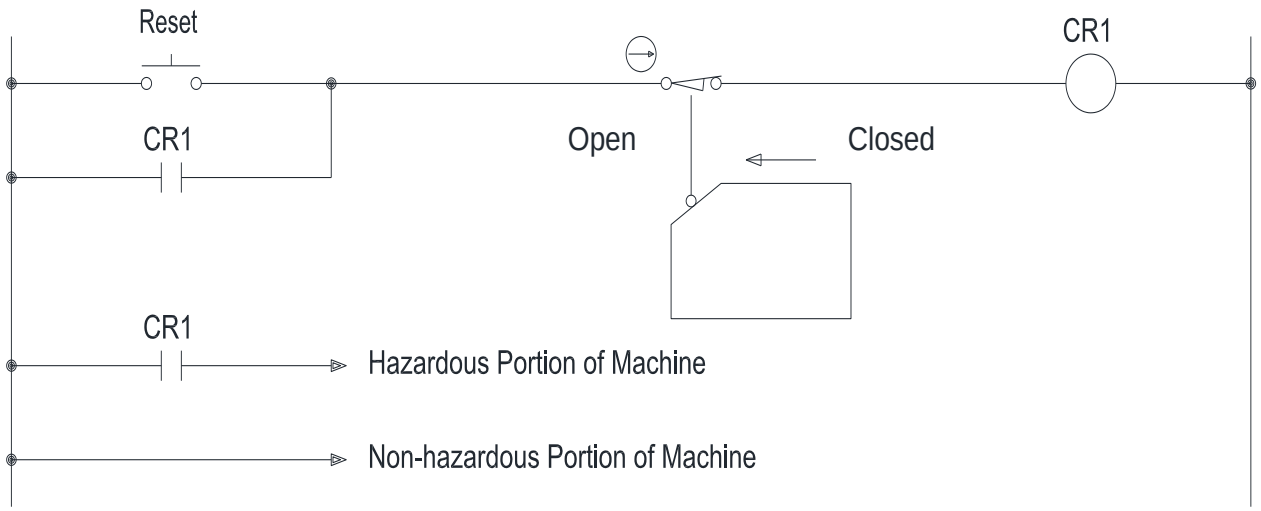
9.2.3 Application Examples

9.2.3.1 Basic Interlocked Guard Circuit (Category B)



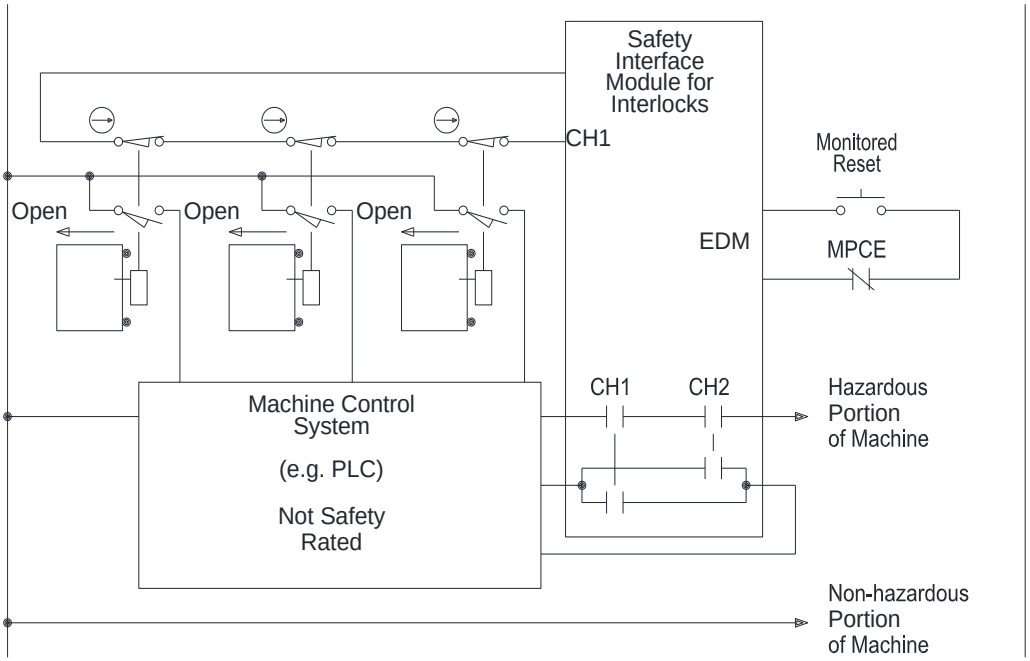
Safety Function:	When the guard is opened, power is removed from the hazardous portion of the machine. ***Informative Note:*** *Guard is shown in the closed position.*
Faults to Consider:	Loss of function of the interlock, including a short circuit and a failure to open (e.g., due to a broken spring). The functional reliability and installation of the Control Relay (CR1) that could result in: - stuck armature in CR1; - welded contacts of CR1; - wiring short from power to the coil of CR1; - wiring short across a contact of CR1; Reset button failing or tied down in a closed condition causing an automatic or unexpected reset. Failure of the spring to open the contacts due to the negative mode mounting of the interlock.
Fault Exclusion:	None (no safety-rated devices employed).
Safety Principles:	The control is designed in accordance with relevant standards. Can withstand the expected influences. The occurrence of a fault can lead to loss of the safety function.

9.2.3.2 Interlocked Guard Circuit – Single Channel (Category 1)



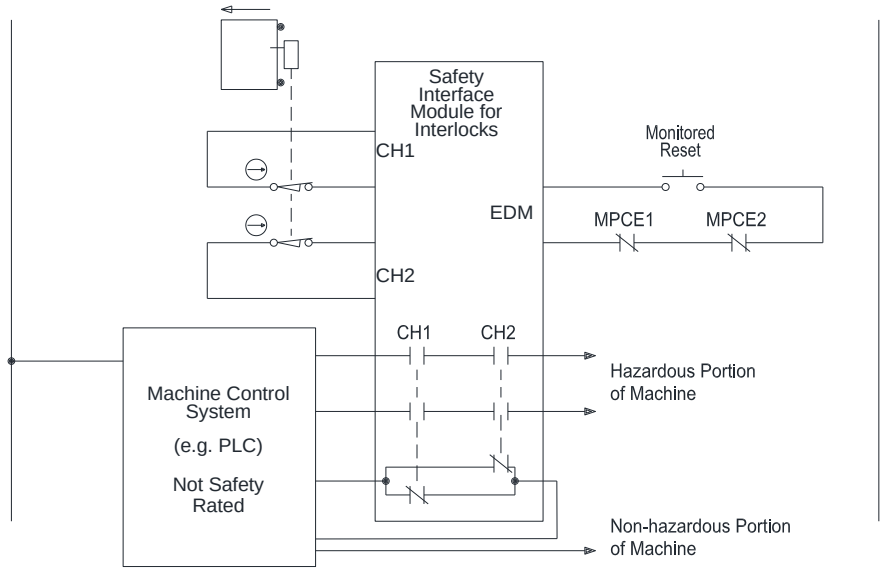
Safety Function:	When the guard is opened, power is removed from the hazardous portion of the machine. ***Informative Note:*** *Guard is shown in the closed position.*
Faults to Consider:	Loss of function of the interlock by a short circuit across the switch or to another source of power. The functional reliability and installation of the Control Relay (CR1) that could result in: - stuck armature in CR1; - welded contacts of CR1; - wiring short from power to the coil of CR1; - wiring short across a contact of CR1; Reset button failing or tied down in a closed condition causing an automatic or unexpected reset.
Fault Exclusion:	Welded contacts are excluded if the positively driven interlock is properly installed (e.g., positive mode). With this exclusion, the opening of the switch contacts may be expected to occur.
Safety Principles:	When the guard is opened power is removed from the Control Relay (CR1) and the hazardous portion of the machine. The risk reduction is improved by adding a positively driven interlock mounted in a positive mode (see 9.2.2.1.1 and 9.2.2.1.2). The control is designed in accordance with relevant standards. Well-tried components and well-tried safety principles are used. The occurrence of a fault can lead to loss of the safety function.

9.2.3.3 Interlocked Guard Monitoring – Single Channel w/ a SIM and PES (Category 2)



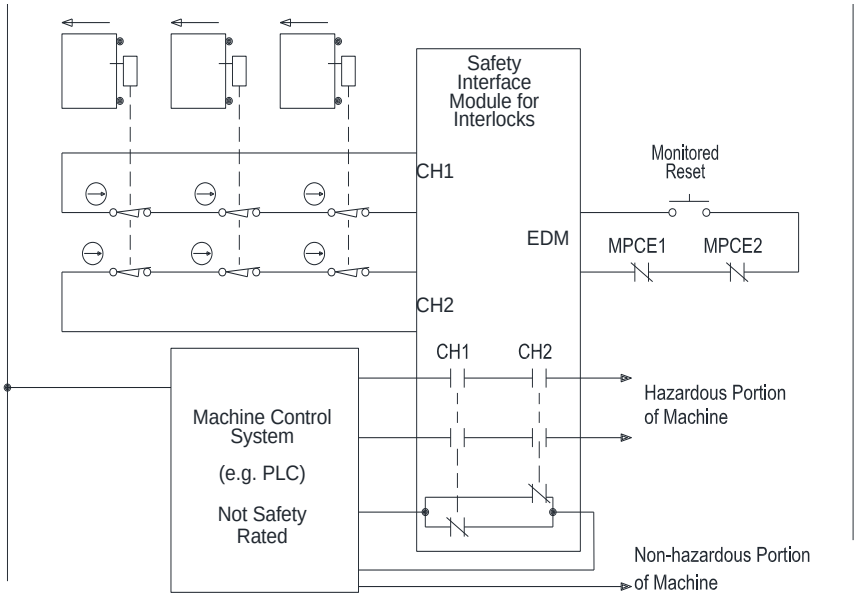
Safety Function:	When one (or more) of the guards is opened, the power is removed from the hazardous portion of the machine. ***Informative Note:*** *Guard is shown in the closed position.*
Faults to Consider:	A catastrophic failure or a short circuit across a set of switch contacts or to another source of power of any of the positively driven interlocking switches (see 8.1.1). Unauthorized or unintended manipulation of the programming that affects the monitoring of the positively driven interlocking switches. The use of type 2 limit switches makes this circuit easy to defeat if extra actuators are available. Faults can be over-ridden or not detected (fault masking, see 8.1.1) when multiple doors are cycled.
Fault Exclusion:	Failure of the interlocking device may be excluded when: • damage to the interlocking device from incorrect actuator engagement is prevented (e.g., overspeed protection, overtravel protection, correct alignment); • the components of the interlocking device (actuator, switch, head) are mechanically mounted per the supplier's information for use; • periodic inspections and testing on the interlocking device and safety function are performed; • the recommended life is not exceeded; • the interlocking device is chosen for the correct environment. If all of the items in the bulleted list are not applied, the reliability may be reduced.
Safety Principles:	When one of the guards is opened, the SIM removes power from its output contacts and the hazardous portion of the machine. The PES/PLC control system is monitoring the safety interface module and the guard interlocks. When a limit switch error occurs, the control system removes the power to the SIM contacts that feed the hazardous portion of the machine. This circuit has the capability of indicating the state of each individual guard, which is accomplished by monitored signals from the normally open (non-safety) contacts (see 9.2.2.1.1). If the positively driven interlocking switch is properly installed, the opening of the switch contacts may be expected to occur. The normally open (non-safety) contact monitored by the PES/PLC control system provides diverse redundancies. A self-monitoring safety interface module is incorporated that is designed, constructed and certified to meet the expected level of safety performance, which provides the monitoring of the interlocking switches and provides protective stop circuits. To achieve Category 2, interlocking device(s) is periodically tested at suitable intervals.

9.2.3.4 Single Interlock to a SIM (Category 3)



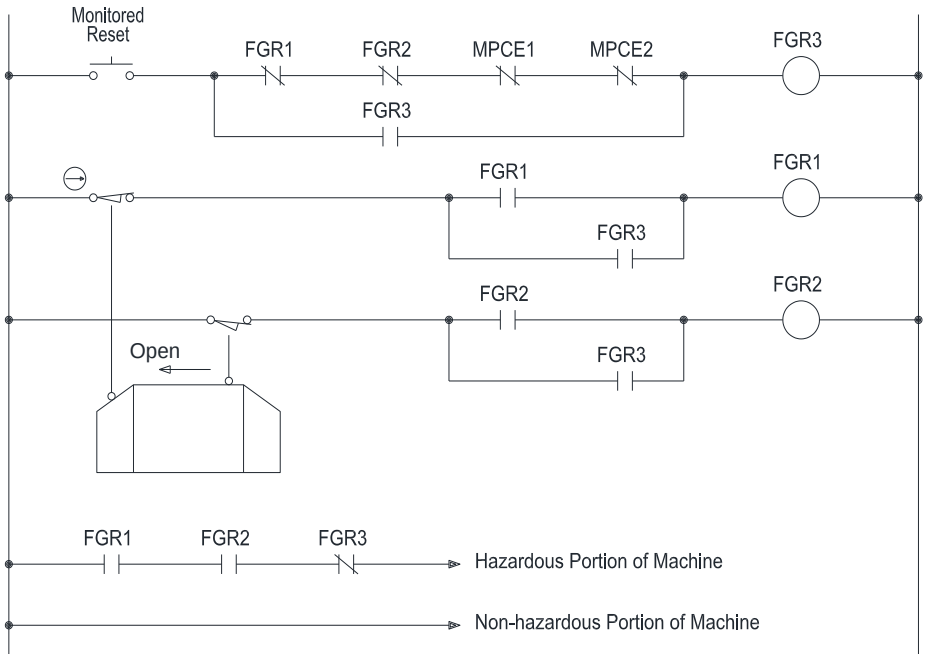
Safety Function:	When the guard is opened, the power is removed from the hazardous portion of the machine. ***Informative Note:*** *Guard is shown in the closed position.*
Faults to Consider:	Mechanical failure of a limit switch or actuator will not be detected. The use of type 2 interlocks makes this circuit easy to defeat if extra actuators are available.
Fault Exclusion:	Failure of the interlocking device may be excluded when: • damage to the interlocking device from incorrect actuator engagement is prevented (e.g., overspeed protection, overtravel protection, correct alignment); • the components of the interlocking device (actuator, switch, head) are mechanically mounted per the supplier's information for use; • periodic inspections and testing on the interlocking device and safety function are performed; • the recommended life is not exceeded; • the interlocking device is chosen for the correct environment. If all of the items in the bulleted list are not applied, the reliability may be reduced.
Safety principles:	When the guard is opened, positively driven contacts of the interlock switch open, and the SIM removes power from its output contacts and the hazardous portion of the machine. To achieve a Category 3, prevent the failure or the loss of the switching function of the single interlocking switch. Category 3 requires redundancy (MPCE1, MPCE2). Monitoring both devices is considered best practice. Undetected failures may be minimized by the correct installation and periodic individual testing of the guard doors.

9.2.3.5 Series Connection of Interlocks to a SIM (Category 3)



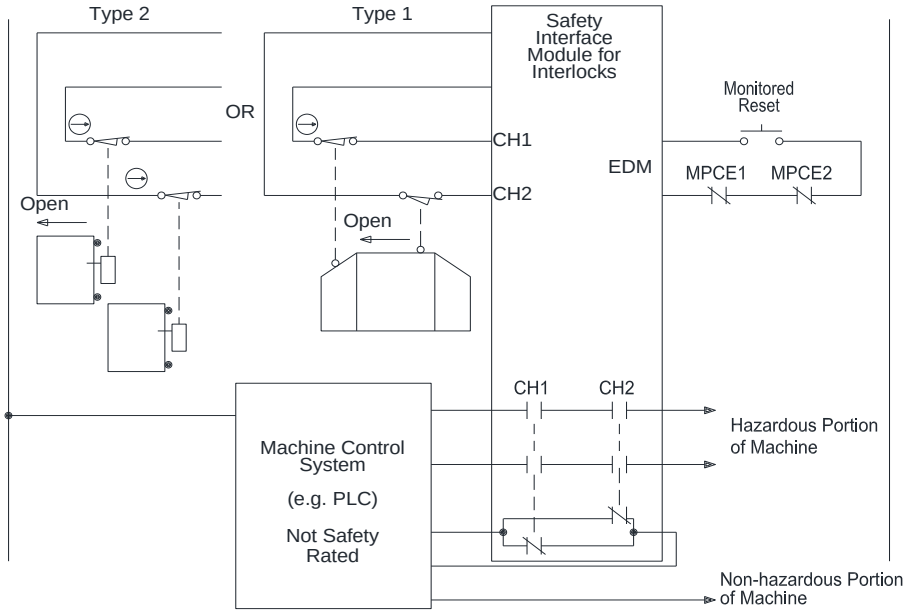
Safety Function:	When any of the guards are opened, power is removed from the hazardous portion of the machine. ***Informative Note:*** *Guard is shown in the closed position.*
Faults to Consider:	Shorts across one of the contacts of any of the interlocking devices can be masked by the opening and closing of another interlocking device. Mechanical failure of the interlocking device or actuator will not be detected. Faults can be over-ridden or not detected (fault masking, see 8.1.1) when multiple doors are cycled. The use of type 2 interlocks makes this circuit easy to defeat if extra actuators are available.
Fault Exclusion:	Failure of the interlocking device may be excluded when: • damage to the interlocking device from incorrect actuator engagement is prevented (e.g., overspeed protection, overtravel protection, correct alignment); • the components of the interlocking device (actuator, switch, head) are mechanically mounted per the supplier's information for use; • periodic inspections and testing on the interlocking device and safety function are performed; • the recommended life is not exceeded; • the interlocking device is chosen for the correct environment. If all of the items in the bulleted list are not applied, the reliability may be reduced.
Safety Principles:	When any of the guards are opened, the SIM removes power from its output contacts and the hazardous portion of the machine. To achieve a Category 3, prevent the failure or the loss of the switching function of any of the interlocking switches. Category 3 requires redundancy (MPCE1, MPCE2). Monitoring both devices is considered best practice. Undetected failures may be minimized by the correct installation and periodic individual testing of the guard doors.

9.2.3.6 Interlocked Guard Monitoring – Dual Channel w/ Relay/Contactor and Reset Button (Category 4)



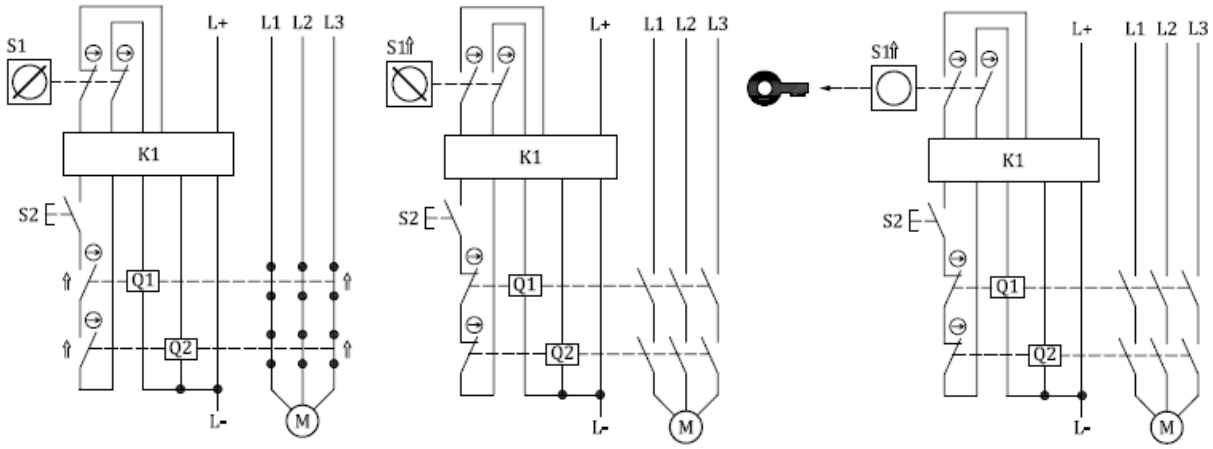
Safety Function:	When the guard is opened, power is removed from the hazardous portion of the machine. ***Informative Note:*** *Guard is shown in the closed position.*
Faults:	None to consider.
Fault Exclusion:	A wire-to-wire short between FGR 1 and FGR 2 when the devices are in the same enclosure. A wire-to-wire short between the two interlocking devices provided wiring to each device is properly protected from damage or the ability to short together. Failure of the interlocking device may be excluded when: • damage to the interlocking device from incorrect actuator engagement is prevented (e.g., overspeed protection, overtravel protection, correct alignment); • the components of the interlocking device (actuator, switch, head) are mechanically mounted per the supplier's information for use; • periodic inspections and testing on the interlocking device and safety function are performed; • the recommended life is not exceeded; • the interlocking device is chosen for the correct environment. If all of the items in the bulleted list are not applied, the reliability may be reduced.
Safety Principles:	When the guard is opened, power is removed from the Force-Guided Relays (FGR1 and FGR2) and the hazardous portion of the machine. Ensure the exclusions. The risk reduction is improved by monitoring those relays via normally closed contacts in the reset circuit. It is further improved by ensuring that the reset button cannot be tied down causing an automatic or unexpected reset. If the positively driven interlock is properly installed, the opening of the switch contacts may be expected to occur. The standard interlock is mounted in a negative mode, which provides diverse redundancy. If one switch fails to function, the other will remove power from the hazardous portion of the machine. If the reset button or FGR3 fails ON, power will be removed from the hazardous portion of the machine. If the wire to wire short between limit switch 1 and limit switch 2, or between FGR 1 and FGR 2, cannot be excluded, this circuit attains only a Category 3 performance.

9.2.3.7 Interlocked Guard Monitoring – Dual Channel w/ a SIM (Category 4)



Safety Function:	When the guard is opened, the power is removed from the hazardous portion of the machine. ***Informative Note:*** *Guard is shown in the closed position.*
Faults to Consider:	None to consider.
Fault Exclusion:	Failure of the interlocking device may be excluded when: • damage to the interlocking device from incorrect actuator engagement is prevented (e.g., overspeed protection, overtravel protection, correct alignment); • the components of the interlocking device (actuator, switch, head) are mechanically mounted per the supplier's information for use; • periodic inspections and testing on the interlocking device and safety function are performed; • the recommended life is not exceeded; • the interlocking device is chosen for the correct environment. If all of the items in the bulleted list are not applied, the reliability may be reduced.
Safety Principles:	When the guard is opened, the dual channel safety interface module detects the opening of the contact of interlock. Power is then removed from the hazardous portion of the machine. The risk reduction is improved by adding the safety interface module, redundant Force-Guided Relays and monitoring those relays via normally closed contacts in the reset circuit. It is further improved by ensuring the reset button cannot be tied down causing an automatic or unexpected reset. If the positively driven interlock is properly installed, the opening of the switch contacts may be expected to occur. The standard interlock is mounted in a negative mode, which provides diverse redundancy. Two positively driven interlocks have the advantage of the positive-mode actuation (see figure on left in above schematic). If one interlock fails to function, or the reset button or one of the Force-Guided Relays fails ON, the safety interface module will prevent a reset. The use of type 2 interlocks makes this circuit easy to defeat if extra actuators are available. A self-monitoring safety interface module is incorporated that is designed, constructed and certified to meet the expected level of safety performance, which provides the monitoring of the interlock and the Force-Guided Relays, and provides protective stop circuits.

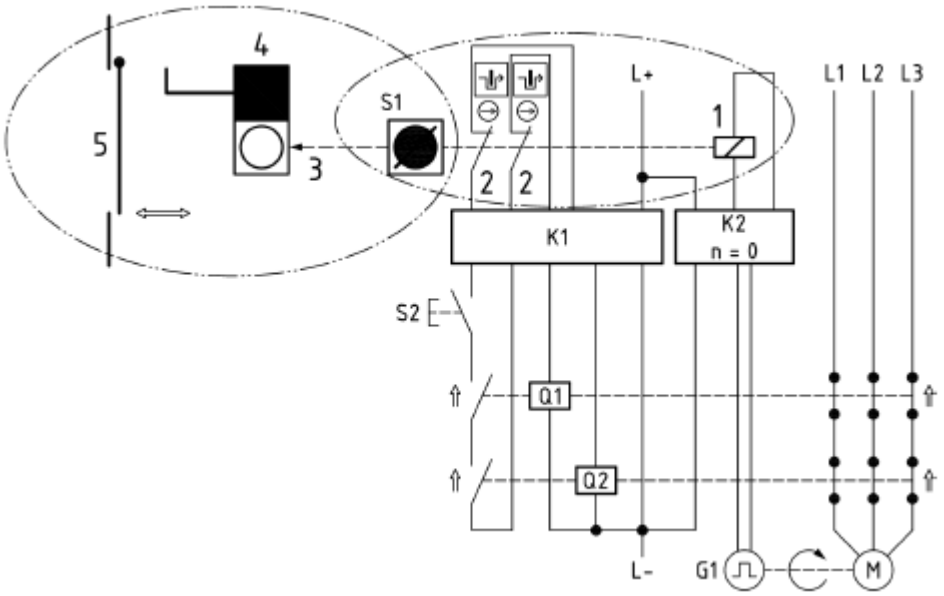
9.2.3.8 Control Interlocking using Trapped Key Interlocking Systems



a) Inputs closed, power contactors on, key releasable;
b) b) Inputs open, contactors off, key inserted and removable;
c) c) Inputs open, power contactors off, key removed.

Safety Function:	When the key is operated to be removable, power is removed from the hazardous portion of the machine (M). The hazardous portion of the machine can only be activated if the key is trapped in the key-operated switch (S1), the reset device (S2) has been operated, and both contactors (Q1 and Q2) are on.
Faults to Consider:	Loss of function of the interlock, including a short circuit and a failure to open (e.g., due to a broken spring). The functional reliability and installation of the logic unit (K1) that could result in: - wiring short from power to the output of K1; - wiring short across outputs of K1; - reset button failing or tied-down in a closed condition causing an automatic or unexpected reset.
Fault Exclusion:	Welded contacts are excluded if the key-operated switch is properly installed since the contacts are positively driven.
Safety Principles:	The risk reduction is improved by using the key-operated switch mounted in a positive mode (see 9.2.2.1.1 and 9.2.2.1.2). The control is designed in accordance with relevant standards. Well-tried components and well-tried safety principles are used. Can withstand the expected influences.

9.2.3.9 Prevention of unexpected start-up using a Trapped Key Interlocking System



Key

Q1	power contactor	1	solenoid
Q2	power contactor	2	solenoid monitoring contact
S1	key-operated solenoid-controlled switch	3	key path
S2	reset device	4	access lock
K1	logic unit	5	movable guard
K2	standstill monitoring logic unit	G1	standstill indicator
M	hazardous portion of the machine		

Safety Function:	When the access lock (4) is unlocked, unexpected start-up is prevented. The hazardous portion of the machine (M) can only be activated if the key is trapped in the key-operated solenoid-controlled switch (S1), the reset device (S2) has been operated, and both contactors (Q1 and Q2) are on.
Faults to Consider:	Loss of function of the interlock, including a short circuit and a failure to open (e.g., due to a broken spring). The functional reliability and installation of the logic unit (K1) that could result in: - wiring short from power to the output of K1; - wiring short across outputs of K1; - reset button failing or tied-down in a closed condition causing an automatic or unexpected reset.
Fault Exclusion:	Welded contacts are excluded if the key-operated solenoid-controlled switch is properly installed since the contacts are positively driven.
Safety Principles:	The risk reduction is improved by using the key-operated solenoid-controlled switch mounted in a positive mode (see 9.2.2.1.1 and 9.2.2.1.2). The control is designed in accordance with relevant standards. Well-tried components and well-tried safety principles are used. Can withstand the expected influences.

9.2.3.10 Single access control procedure using a Trapped Key Interlocking System

Step 1: Machine in operation

1 key-operated switch (key releasable, contacts closed [machine on])

2 access lock (key removed, actuator locked)

Step 2: Operation of the key results in a stop command

1 key-operated switch (key inserted and removable, contacts opened [machine off])

2 access lock (key removed, actuator locked)

Step 3: Key moving between trapped key devices

1 key-operated switch (key removed, contacts opened [machine off])

2 access lock (key removed, actuator locked)

3 key in transfer

Step 4: Key inserted in access lock

1 key-operated switch (key removed, contacts opened [machine off])

2 access lock (key inserted and removable, actuator locked)

Step 5: Access lock unlocked

1 key-operated switch
(key removed, contacts opened [machine off])

2 access lock
(key releasable, actuator unlocked)

Step 6: Actuator removed from access lock, trapping key

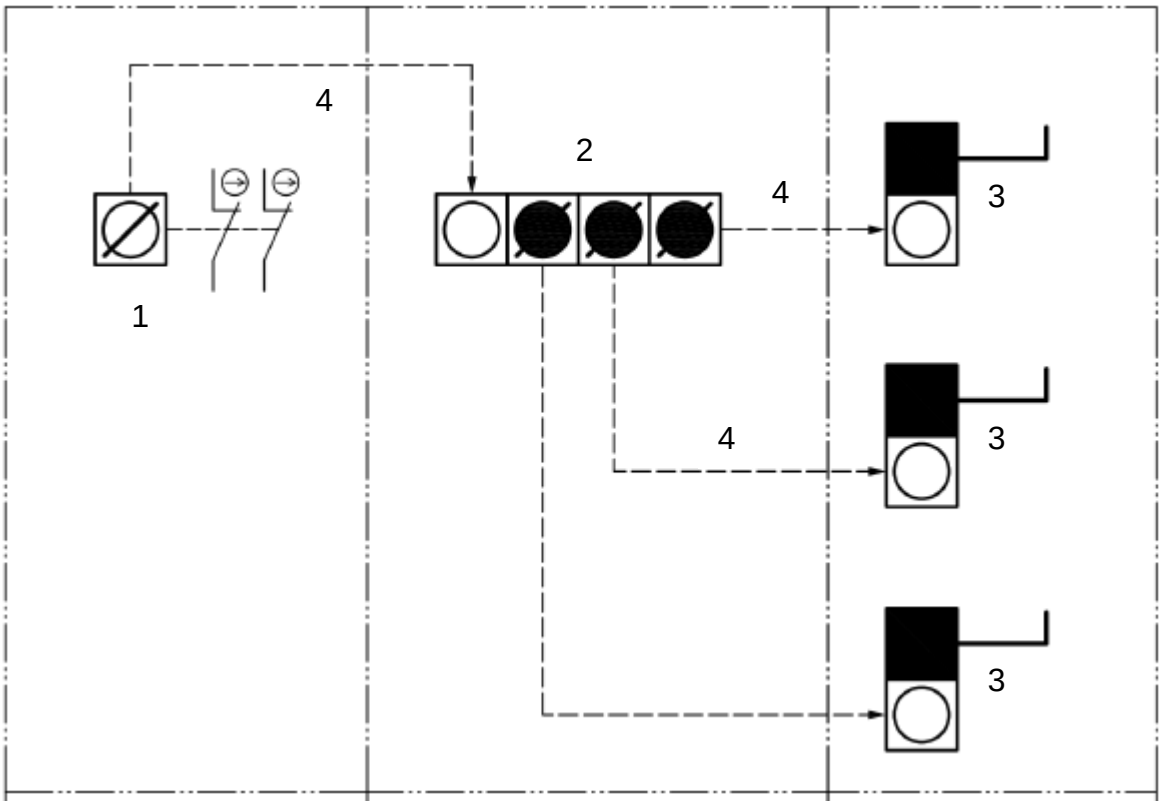
1 key-operated switch
(key removed, contacts opened [machine off])

2 access lock
(key trapped, actuator removed)

Safety Function:	When the key is operated to a removable position, a stop command is initiated for the hazardous portion of the machine. When the key is removed from the key-operated switch it can be used to release the access lock, allowing access to the safeguarded space.
Faults to Consider:	Loss of function of the access lock, including a failure to open (e.g., due to a broken spring). Broken actuator remains in the access lock. If using a logic unit, the functional reliability and installation of the logic unit (K1) could result in: - wiring short from power to the output of K1; - wiring short across outputs of K1; - reset button failing or tied-down in a closed condition causing an automatic or unexpected reset.
Fault Exclusion:	Welded contacts are excluded if the key-operated switch is properly installed since the contacts are positively driven.
Safety Principles:	The risk reduction is improved by using the key-operated solenoid-controlled switch mounted in a positive mode (see 9.2.2.1.1 and 9.2.2.1.2). The control is designed in accordance with relevant standards. Well-tried components and well-tried safety principles are used. Can withstand the expected influences.

9.2.3.11 Access control using a Trapped Key Interlocking System including key exchange

Informative Note: *The safety function, faults to consider, fault exclusions, and safety principles are the same when using one access lock or multiple access locks with a key exchange.*



1 key-operated switch (key releasable, contacts closed [machine on])
2 key exchange (key removed from first position, keys trapped in second through fourth positions)
3 access lock (key removed, actuator locked)
4 key path

Safety Function:	When the key is operated to a removable position, a stop command is initiated for the hazardous portion of the machine. When the key is removed from the key-operated switch, it can be inserted into the key exchange thereby releasing the keys to be inserted into the access locks.
Faults to Consider:	Loss of function of the interlock, including a failure to open (e.g., due to a broken spring). Broken actuator remains in the access lock.
Fault Exclusion:	Welded contacts are excluded if the key-operated switch is properly installed since the contacts are positively driven.
Safety Principles:	The risk is improved by using the key-operated solenoid-controlled switch mounted in a positive mode (see 9.2.2.1.1 and 9.2.2.1.2). The control is designed in accordance with relevant standards. Well-tried components and well-tried safety principles are used. Can withstand the expected influences.

9.3 Non-Contact Interlocking Devices

9.3.1 Design Requirements

Safety functions that include guard interlocking extend beyond the SRP/CS to include the mechanical mounting and interface with the guard(s). The reliability of these mechanical functions shall be included in determining the overall reliability of the SRP/CS.

Informative Note: *See ANSI B11.19 and ISO 14119 for further information.*

For higher levels of safety performance, a non-contact interlocking device whose design complies with an appropriate safety (design) standard(s) shall be used. The design of interlocking devices employing optical technology shall be such that the interlocking device only responds to the appropriate source of light.

For switches utilizing technology affected by the material of the mounting surface (e.g., ferrous, magnetic, or conductive), both the switch and actuator shall be mounted at a minimum distance from such materials, as specified by the supplier.

9.3.2 Design Considerations

The following design considerations represented within the application examples in 9.3.3 should be applied as part of the design process for the SRP/CS.

9.3.3 Application Examples

9.3.3.1 Description of Non-Contact Interlocking Devices

Non-contact interlocking devices come in a variety of styles (e.g., magnetic, inductive, optical, radio frequency tag etc.). The common characteristic of all varieties is that the switch does not necessarily come in physical contact with an actuator, target, or the guard (other than mounting). Non-contact interlocking devices are frequently called "*proximity devices*."

In higher levels of safety performance, the functionality of non-contact interlocking devices should provide the same or greater reliability as positively driven interlocking devices (see 9.2.2.1.1). This is typically accomplished by active monitoring by a Safety Interface Module or the internal design of the device.

9.3.3.2 Inductive Switches

Inductive (proximity) switches rely on the presence or absence of a detectable material for actuation. Standard Inductive switches can be easily defeated and can fail due to common mode failures such as build-up of detectable material on the sensing surface.

For proper operation, the switch sensing surface shall be mounted at a minimum distance from any detectable materials and from other switches if mutual interference (influence) is possible. The supplier typically specifies the distance.

9.3.3.3 Optical Switches

Optical switches rely on the presence or absence of light for actuation. Standard optical switches, frequently called *photoelectric sensors*, can be easily defeated and can fail due to optical effects like "false proxing" where unintended actuation occurs from shiny surfaces reflecting light. Often the path of travel (movement) of the optical switch must be perpendicular to the optical axis to ensure proper switching action.

9.3.3.4 Magnetic Switches

The design of dual channel magnetic switches typically uses complementary switching in which one channel is open, and one channel is closed at all times. This provides redundancy (two contacts) and diversity (different principles of operation) to minimize the possibility of the loss of the switching function due to common mode failures (e.g., secondary or residual magnetic fields and potential short circuit). The circuitry or the safety interface module that is monitoring the magnetic switch will detect and respond to a failure that results in the loss of the complementary state (e.g., a short circuit between the channels, or a short circuit to other sources of power).

Coded and non-coded magnetic switches affect the ability of the switch to be defeated and withstand common mode failures. If either the switch or magnet is mounted on a material that can be magnetized (a ferrous metal, such as iron), the switching distance will be affected. The supplier typically specifies the distance.

9.3.3.5 Transponder Switches

Transponder (e.g., Radio Frequency) switches rely on the presence or absence of a coded actuator that is energized by the switch for actuation. If either the switch or actuator is mounted on any electrically conductive or ferrous materials, switching distance will be affected. The supplier typically specifies the distance.

9.3.3.6 Interlocking Device "type" Characteristics

Non-contact interlocking devices are grouped into numeric "types" 3 and 4. See below for the characteristics of each type as well as tampering/defeat (9.3.3.6.1) and failure modes (9.3.3.6.2).

Informative Note 1: *For types 1 and 2 (mechanical contact interlocking devices), see also, 9.2.2.1.3.*

Informative Note 2: *For type 5 (trapped key) interlocking devices), see also, 9.2.2.1.3.*

Type 3 interlocking devices typically exhibit the following characteristics:

- no moving parts;
- high resistance to dust, liquids;
- easily kept clean;
- due to the lack of coding additional measures against defeating are required;
- may be easily bypassed by a foreign object;
- possible sensitivity to electromagnetic interference;
- additional safety measures required for use in SRP/CS;
- limited application possibilities;
- interlocking device with non-contact actuated position switch with uncoded actuator (e.g., proximity switch).

Type 4 interlocking devices typically exhibit the following characteristics:

- compact, no external moving parts;
- high resistance to dust, liquids;
- easily kept clean;
- medium and high-level coding possible;
- reduces possibility for use of cheater keys;
- tolerance to guard misalignment;
- possible sensitivity to electromagnetic interference;
- interlocking device with non-contact actuated position switch with coded actuator (e.g., Radio Frequency Identification (RFID) uniquely coded tag actuated switches).

9.3.3.6.1 Tampering / Defeat

Tampering with non-contact interlocking devices can be a foreseeable misuse of safety functions. Measures to reduce the risk of tampering include but are not limited to:

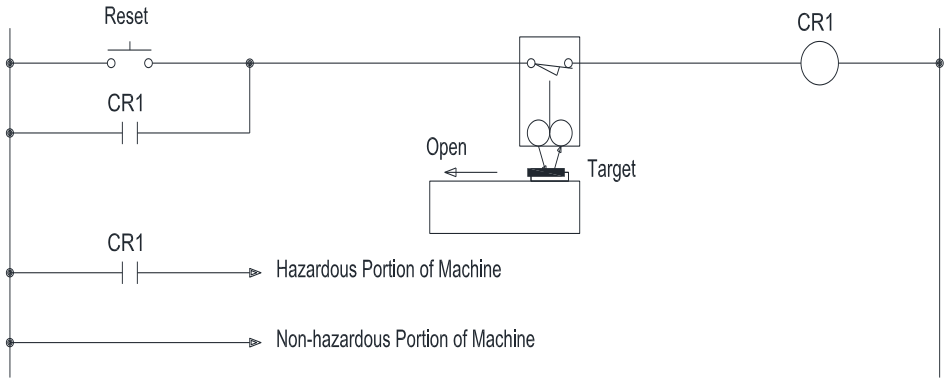
- use of tamper-proof screws for switch/actuator mounting;
- mounting in a protected / concealed location;
- multiple switches with simultaneity test imposed by the logic portion of the circuit;
- automatic, periodic testing;
- switch function test built into each cycle, e.g., cycle cannot start without logic 'seeing' the guard open and close, anti-tie-down for guarding;
- coded actuators.

9.3.3.6.2 Failure Modes

Failure modes specific to non-contact interlocking devices include but are not limited to:

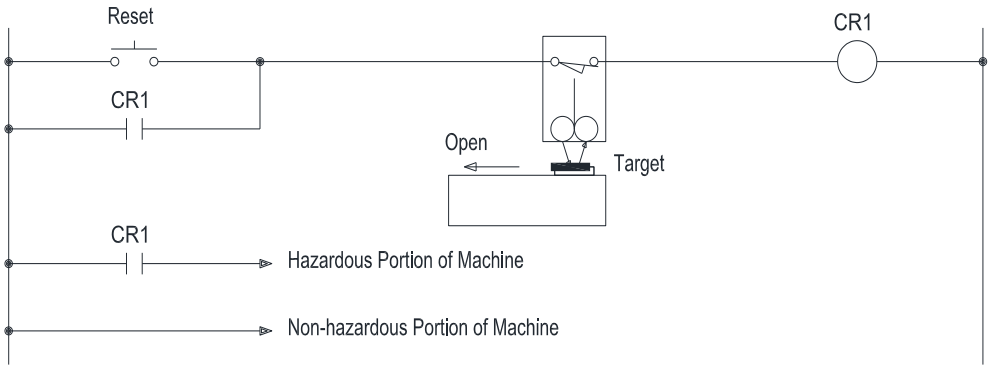
- buildup of detectable material;
- misalignment of interlock components;
- contamination, corrosion, physical damage;
- failure of mounting interface with guard;
- damage to magnetic reed contacts due to excessive current;
- effects from magnetic, radio frequency fields;
- effects from incorrect mounting surfaces (conductive, magnetic, ferrous).

9.3.3.7 Non-Contact Interlocked Guard Monitoring using Standard Retro-Reflective Photo Sensor (Category B)



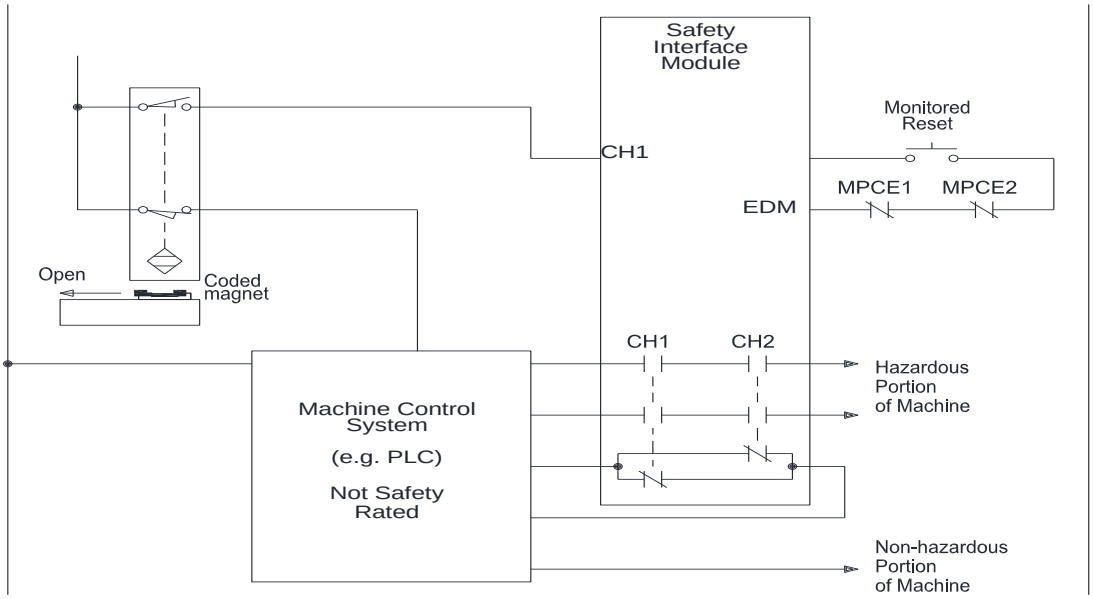
Safety Function:	When the guard is opened, power is removed from the hazardous portion of the machine.
Faults to Consider:	Loss of function of the interlocking device, including a short circuit or a failure to switch (e.g., due to contamination buildup on sensing surface or “false-proxing” due to shiny objects in field of view). The possibility of “false-proxing” may be reduced by using a polarized retro-reflective photoelectric sensor. The functional reliability and installation of the Control Relay (CR1) that could result in: - stuck armature in CR1; - welded contacts of CR1; - wiring short from power to the coil of CR1; - wiring short across a contact of CR1; Reset button failing or tied down in a closed condition causing automatic or unexpected reset.
Fault Exclusion:	None (no safety-rated devices employed).
Safety Principles:	When the guard is opened, power is removed from the Control Relay (CR1) and the hazardous portion of the machine. It is designed in accordance with relevant standards. Can withstand the expected influences. The occurrence of a fault can lead to loss of the safety function.

9.3.3.8 Non-Contact Interlocked Guard Monitoring using Standard Magnetic Sensor (Category B)



Safety Function:	When the guard is opened, power is removed from the hazardous portion of the machine.
Faults to Consider:	Loss of function of the interlocking device, including a short circuit or a failure to switch (e.g., due to external magnetic fields, residual magnetism, or intentional defeat by affixing a magnet to sensor). The functional reliability and installation of the Control Relay (CR1) that could result in: - stuck armature in CR1; - welded contacts of CR1; - wiring short from power to the coil of CR1; - wiring short across a contact of CR1; Reset button failing or tied down in a closed condition causing an automatic or unexpected reset.
Fault Exclusion:	None (no safety-rated devices employed).
Safety Principles:	When the guard is opened, power is removed from the Control Relay (CR1) and the hazardous portion of the machine. It is designed in accordance with relevant standards. Can withstand the expected influences. The occurrence of a fault can lead to loss of the safety function. The use of non-coded limit switches makes this circuit easy to defeat with ordinary magnets.

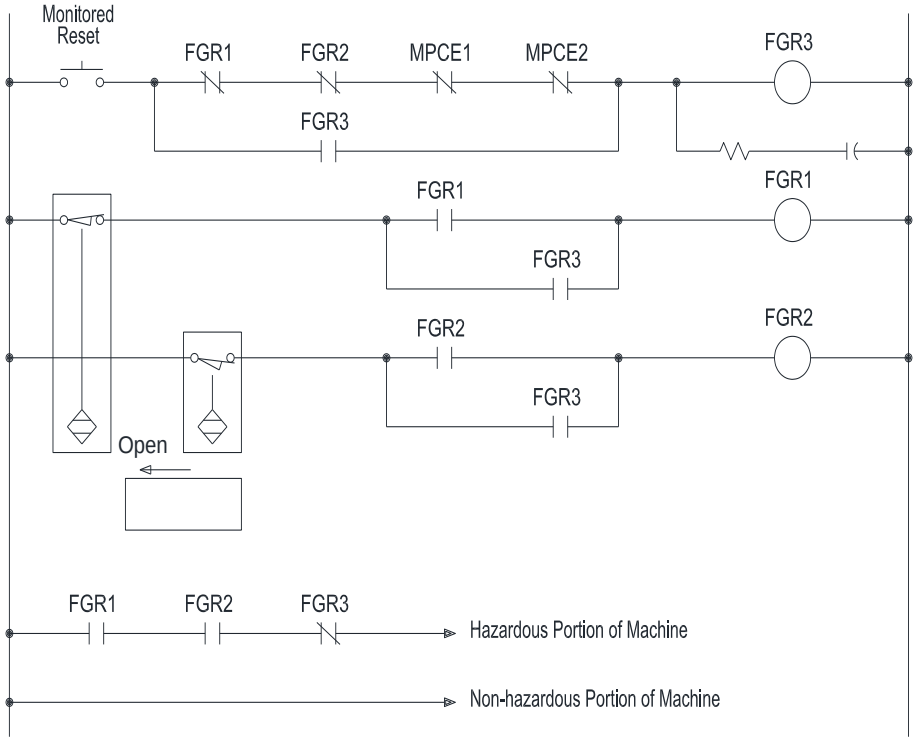
9.3.3.9 Non-Contact Interlocked Guard Monitoring – Single Channel w/ a SIM and PES (Category 2)



Safety Function:	When one (or more) of the guards is opened, the power is removed from the hazardous portion of the machine. ***Informative Note:*** *Guard is shown in the closed position.*
Faults to Consider:	See general failure modes in 7.3 (electrical), 7.4 (fluid power), and specific failure modes in 9.3.3.6.2. Possibility of contamination buildup on sensors' surface. Unauthorized or unintended manipulation of the programming that effects the monitoring of the non-contact interlocking devices.
Fault Exclusion:	Failure of the interlocking device may be excluded when: - damage to the interlocking device from incorrect actuator engagement is prevented (e.g., overspeed protection, overtravel protection, correct alignment); - the components of the interlocking device (actuator, switch, head) are mechanically mounted per the supplier's information for use; - periodic inspections and testing on the interlocking device and safety function are performed; - the recommended life is not exceeded; - the interlocking device is chosen for the correct environment. If all of the items in the bulleted list are not applied, the reliability may be reduced.
Safety Principles:	When one of the guards is opened, the SIM removes power from its output contacts and the hazardous portion of the machine. The PES/PLC control system is monitoring the safety interface module and the interlocks. When a limit switch error occurs, the control system removes the power to the SIM contacts that feed the hazardous portion of the machine. This circuit has the capability of indicating the state of each individual guard, which is accomplished by monitored signals from the second OSSD of the device. A self-monitoring safety interface module is incorporated that is designed, constructed and certified to meet the expected level of safety performance, which provides protective stop circuits. To achieve Category 2, periodically test interlocking device(s) at suitable intervals.

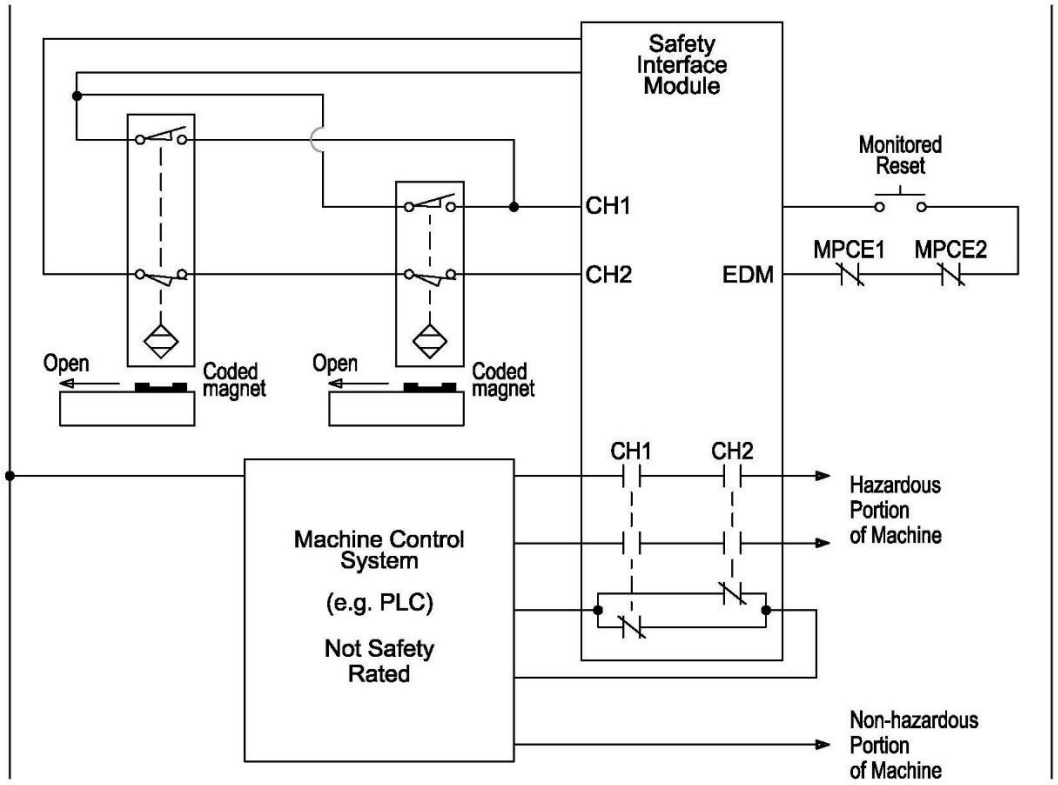
9.3.3.10 Non-Contact Interlocked Guard Monitoring Circuit (Category 3)

Dual Channel with Force-Guided relay monitoring using standard inductive proximity sensors.



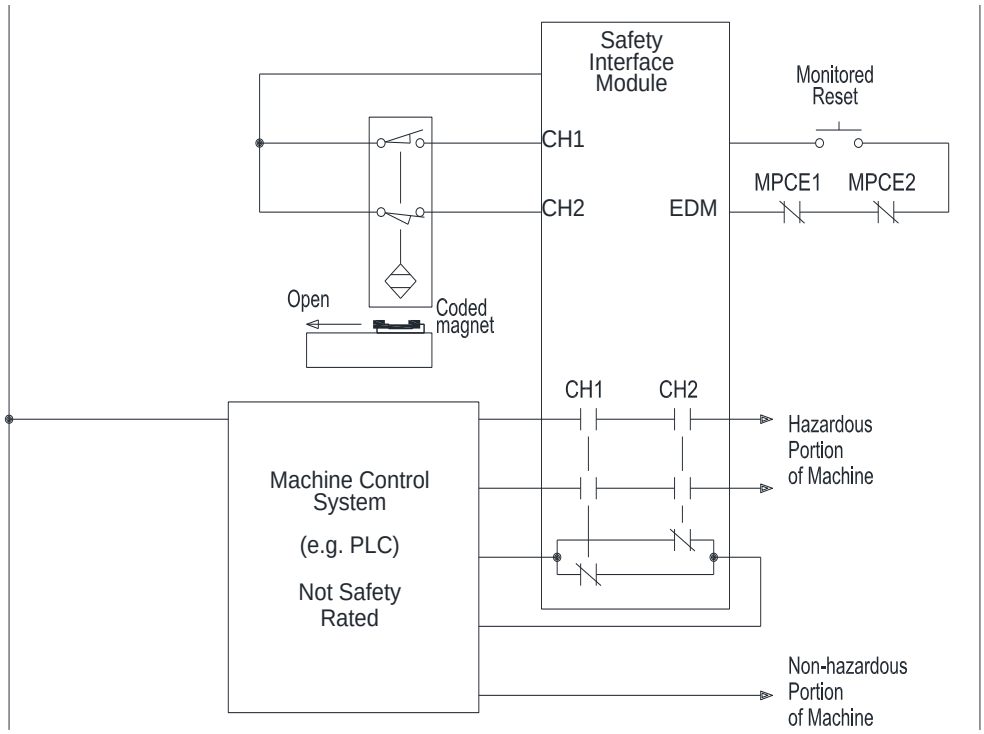
Safety Function:	When the guard is opened, power is removed from the hazardous portion of the machine.
Faults to Consider:	See general failure modes in 7.3 (electrical), 7.4 (fluid power), and specific failure modes in 9.3.3.6.2. Possibility of contamination buildup on sensor's surface. A wire to wire short between sensor 1 and sensor 2 or between FGR 1 and FGR 2. The use of standard proximity switches makes this circuit easy to defeat.
Fault Exclusion:	None to consider
Safety Principles:	When the guard is opened, power is removed from the Force-Guided Relays (FGR1 and FGR2) and the hazardous portion of the machine. The reset button cannot be tied down causing an automatic or unexpected reset by FGR3. FGR1 and FGR2 are monitored via normally closed contacts in the reset circuit. If one switch fails to function, the other will remove power from the hazardous portion of the machine. If the reset button or FGR3 fails ON, power will be removed from the hazardous portion of the machine. Diverse operating modes (N.O. and N.C., one sensing, one not) of the inductive sensors help prevent common mode and common cause failures. This is Category 3 due to the use of standard inductive switches. The use of proximity switches makes this circuit easy to defeat with almost any metallic target. ***Informative Note:*** *See ISO 14119-2024. To achieve Category 4, the proximity sensors:* • *employ the safety principles of short circuit, overload, over voltage, reverse polarity, transient and EMC protections;* • *use methods to reduce or eliminate the probability of common mode failure.*

9.3.3.11 Interlocked Guard Monitoring – Dual Channel with a SIM (Category 3)



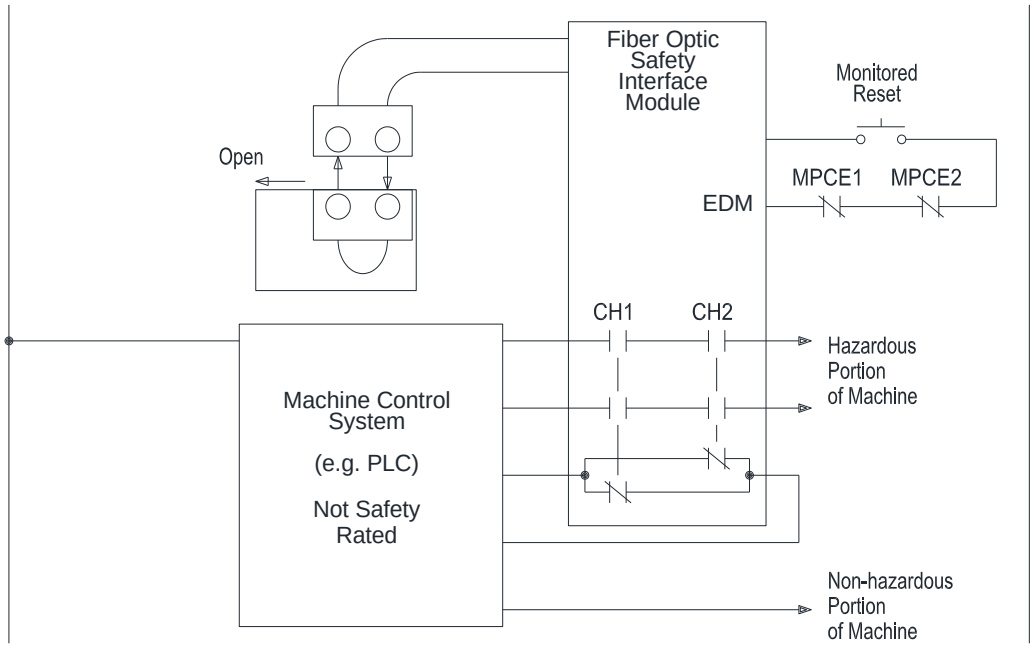
Safety Function:	When the guard is opened, the power is removed from the hazardous portion of the machine.
Faults to Consider:	Faults can be over-ridden or not detected when multiple doors are cycled.
Fault Exclusion:	Catastrophic failure of the sensor resulting in the loss of the safety function (switching) may be excluded due to the design of the magnet and sensor and the complementary switching.
Safety Principles:	When the guard is opened, the dual channel safety interface module detects the opening of the interlocking devices. Power is then removed from the hazardous portion of the machine. The safety interface module monitors the Force-Guided Relays via the normally closed contacts in the reset circuit. The reset button may not be tied down because of the monitored manual reset of the safety interface module. Complementary switching (N.O. and N.C.) of the magnetic sensors helps prevent common mode and common cause failures. The possibility of intentional defeat by affixing a standard magnet to the sensor is reduced by the design of the alternating poles (i.e., coding). Category 3 requires redundancy (MPCE1, MPCE2). Monitoring both devices is considered best practice. This is considered Category 3 due to the use of coded magnets and sensors and the series-parallel connection of multiple sensors. This example uses a special SIM which limits the current drawn from the reed contacts and uses complementary inputs. The use of special reeds and coded magnets makes this interlock difficult to defeat. An additional feature often included in the SIM is a short time window during which both contacts shall change state.

9.3.3.12 Interlocked Guard Monitoring – Dual Channel with a SIM (Category 4)



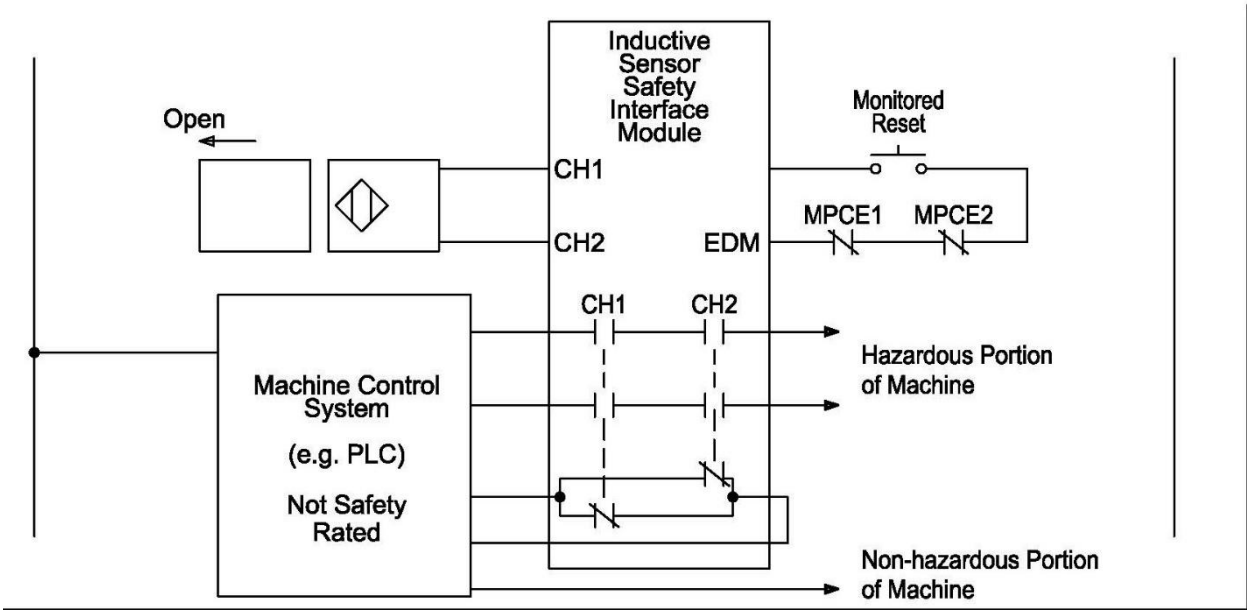
Safety Function:	When the guard is opened, the power is removed from the hazardous portion of the machine.
Faults to Consider:	See general failure modes in 7.3 (electrical), 7.4 (fluid power), and specific failure modes in 9.3.3.6.2. The possibility of intentional defeat by affixing a standard magnet to the sensor is reduced by the design of the alternating poles (i.e., coding).
Fault Exclusion:	Catastrophic failure of the sensor resulting in the loss of the safety function (switching) may be excluded due to the design of the magnet and sensor and the complementary switching.
Safety Principles:	When the guard is opened, the dual channel safety interface module detects the opening of the interlocking devices. Power is then removed from the hazardous portion of the machine. The safety interface module monitors the Force-Guided Contactors via the normally closed contacts in the reset circuit. The reset button may not be tied down because of the monitored manual reset of the safety interface module. Complementary switching (N.O. and N.C.) of the magnetic sensors helps prevent common mode and common cause failures. The possibility of intentional defeat by affixing a standard magnet to the sensor is reduced by the design of the alternating poles (i.e., coding). This is Category 4 due to the use of an individual coded magnet/sensor and the frequency of exercising the guard.

9.3.3.13 Interlocked Guard Monitoring – Dual Channel with a SIM (Category 4)



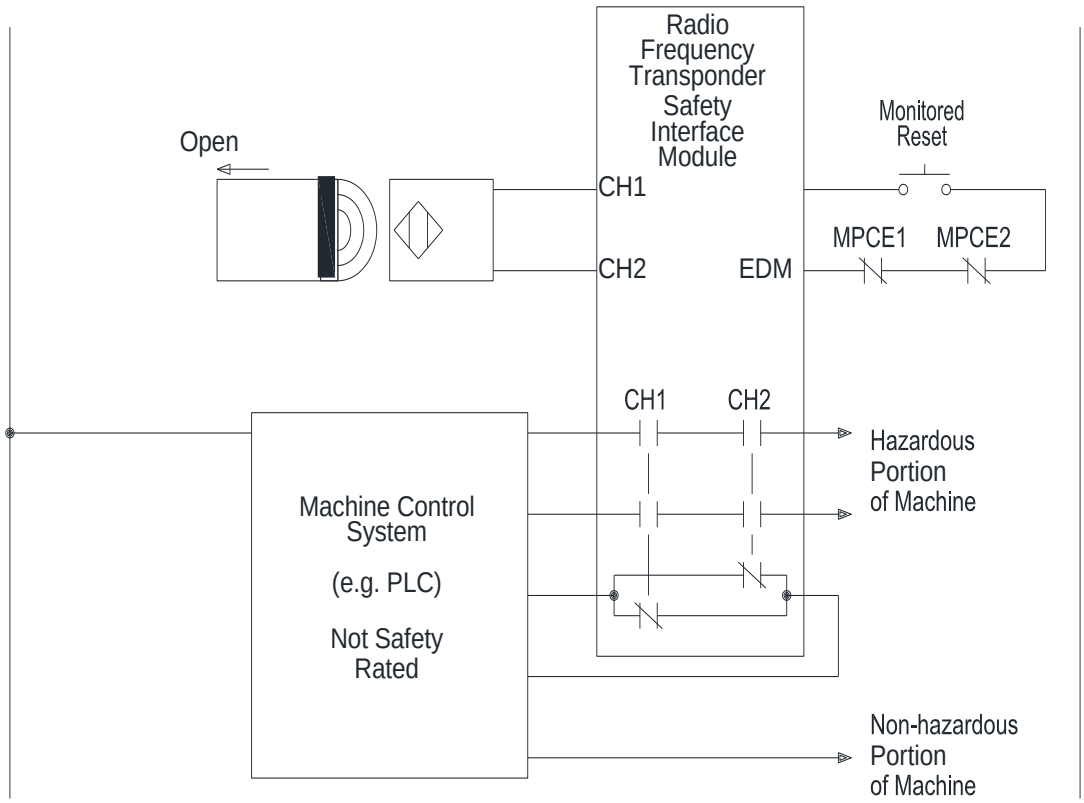
Safety Function:	When the guard is opened, the power is removed from the hazardous portion of the machine.
Faults to Consider:	See general failure modes in 7.3 (electrical), 7.4 (fluid power), and specific failure modes in 9.3.3.6.2.
Fault Exclusion:	Catastrophic failure of the switches resulting in the loss of the safety function (switching) may be excluded due to the design of the optical switches and the Fiber Optic Safety Module. The Fiber Optic Safety Module is specifically designed for the application and to applicable safety standard(s).
Safety Principles:	When the guard is opened, the dual channel safety interface module detects the opening of the interlocking devices. Power is then removed from the hazardous portion of the machine. The safety interface module monitors the Force-Guided Contactors via the normally closed contacts in the reset circuit. The reset button may not be tied down because of the monitored manual reset of the safety interface module. Multiple guards may be monitored on an optical loop without affecting the Category. The possibility of intentional defeat is reduced by the design and installation of the optical devices. This is Category 4 due to the design of the Fiber Optic Safety System.

9.3.3.14 Interlocked Guard Monitoring – Dual Channel with a SIM (Category 4)



Safety Function:	When the guard is opened, the power is removed from the hazardous portion of the machine.
Faults to Consider:	See general considerations in 9.3.2.
Fault Exclusion:	Catastrophic failure of the switch resulting in the loss of the safety function (switching) may be excluded due to the safety design of the dual channel inductive switch and the Inductive Sensor Safety Module. The Inductive Sensor Safety Module is specifically designed for the application and to applicable safety standard(s).
Safety Principles:	When the guard is opened, the dual channel safety interface module detects the opening of the interlocking devices. Power is then removed from the hazardous portion of the machine. The safety interface module monitors the Force-Guided Contactors via the normally closed contacts in the reset circuit. The reset button may not be tied down because of the monitored manual reset of the safety interface module. Multiple guards may be monitored depending on the inductive sensor's OSSD configuration. The possibility of intentional defeat is reduced by the design and installation of the inductive switches. This is Category 4 due to the design of the Inductive Sensor Safety System. ***Informative Note:*** *Due to the ability to intentionally defeat this type of device, it is often not the preferred solution to implement for guard interlock circuits.*

9.3.3.15 Interlocked Guard Monitoring – Dual Channel with a SIM (Category 4)



Safety Function:	An interlocked guard is manually released, removing power from the hazardous portion of the machine which stays de-energized until the guard is closed and reset.
Faults to Consider:	See general considerations in 9.3.2.
Fault Exclusion:	Catastrophic failure of the Dual Channel sensor resulting in the loss of the safety function (switching) may be excluded due to the design of the sensor and the Transponder Safety Module. The Transponder Safety Module is specifically designed for the application and to applicable safety standard(s).
Safety Principles:	When the guard is opened, the dual channel safety interface module detects the opening of the interlocking devices. Power is then removed from the hazardous portion of the machine. The safety interface module monitors the Force-Guided Contactors via the normally closed contacts in the reset circuit. The reset button may not be tied down because of the monitored manual reset of the safety interface module. Multiple guards may be monitored depending on the transponder sensor. The possibility of intentional defeat is reduced by the design and installation of the transponder sensors. This is Category 4 due to the design of the Transponder Safety System.

9.4 Guard Locking Interlocks

9.4.1 Design Requirements

Guard locking functions may be used to protect the process e.g., where opening an interlocked guard during operation will result in machine damage or product loss. Such applications are addressed by normal machine controls. Where guard locking is used to reduce risk to personnel, all elements involved in the function shall be considered as SRP/CS.

Safety functions that include guard locking extend beyond the SRP/CS to include the mechanical mounting and interface with the guard(s). The reliability of these mechanical functions shall be included in the determination of the overall reliability of the SRP/CS.

Informative Note: *See ANSI B11.19, ISO 14119 and IEC 60947-5-1 for additional design, construction, installation, operation and maintenance requirements.*

Entrapment hazards are generated where guard locking is applied and whole-body access to the guarded space is intended. The risks of personnel being trapped in the safeguarded space shall be reduced to an acceptable level.

Informative Note: *The most common means of achieving acceptable risk in this situation is the addition of manual locking override mechanisms readily accessible within the safeguarded space.*

9.4.2 Design Considerations

The following design considerations should be applied as part of the design process for the SRP/CS.

9.4.2.1 General Information

The most commonly used methodology for guard locking is a single integrated device, purposely built for the combined functions of guard interlocking and guard locking. Even when an integrated device is used, the safety functions of interlocking and of locking may be considered separately. Each function may have its own reliability design specification.

Most integrated devices operate in one of two modes: *power to unlock*, where power is applied to a solenoid to release the guard, and *power to lock*, where power is applied to a solenoid to lock the guard.

Guard locking interlock devices can be of type 1, type 2 or type 5 design (see 9.2.2.1.3); for type 3, or type 4 design, see 9.3.3.6.

9.4.2.1.1

9.4.2.1.2 Tampering / Defeat

While integrated devices share many of the same failure modes with the corresponding interlock device types, there are additional factors to be considered. Power to unlock devices may present a significant nuisance to operators, particularly when machines must be locked out frequently, as the removal of power can leave the operator unable to access the machine. In many cases, this results in a higher than normal incidence of tampering for power to unlock devices. This disadvantage must be weighed against the protection provided by power to lock devices should the power to the machine fail.

Informative Note: *Upon loss of power, the stopping time of the machine is often lengthened. If loss of power also results in release of the locking element, it can be possible to access the hazard before the motions have been stopped*.

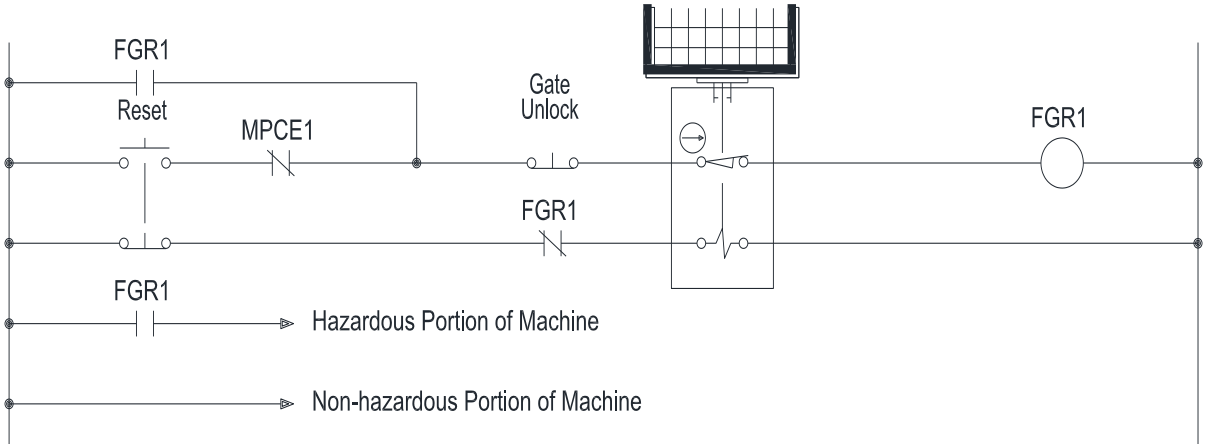
9.4.2.1.3 Failure Modes

Failure modes specific to guard locking interlock devices include but are not limited to:

- use of the interlocking devices as a mechanical stop or as a mechanical alignment mechanism;
- contamination, corrosion, physical damage;
- failure of mounting interface with the guard;
- fatigue and breakage of the interlock actuator;
- failure of the spring mechanism to engage the lock mechanism.

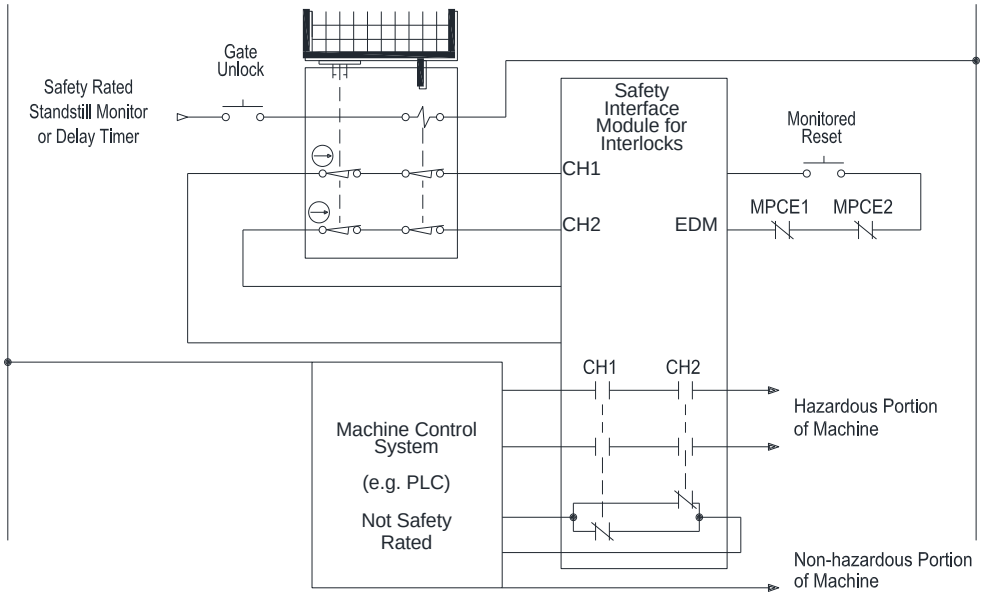
It is very important to note that several failure modes can yield an undetectable loss of the locking function. The interlock function of the device may be positively driven, but the locking functionality is typically spring driven, and thus cannot be considered positively driven.

9.4.2.2 Power to Release, Inline Guard locking Interlock (Category 2)



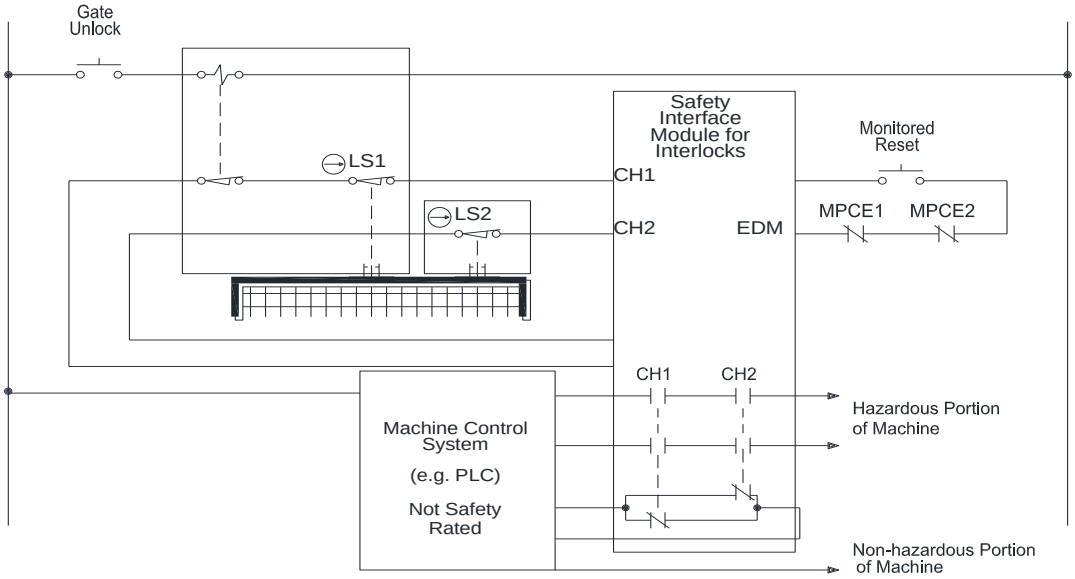
Safety Function:	An interlocked guard is manually released, removing power from the hazardous portion of the machine which stays de-energized until the guard is closed and reset.
Faults to Consider:	Wiring short across the Reset button.
Fault Exclusion:	Failure of the interlocking device may be excluded when: • damage to the interlocking device from incorrect actuator engagement is prevented (e.g., overspeed protection, overtravel protection, correct alignment); • the components of the interlocking device (actuator, switch, head) are mechanically mounted per the supplier's information for use; • periodic inspections and testing on the interlocking device and safety function are performed; • the recommended life is not exceeded; • the interlocking device is chosen for the correct environment. If all of the items in the bulleted list are not applied, the reliability may be reduced.
Safety Principles:	The guard is closed to allow the Reset button to energize the Force-Guided Relay and to de-energize the solenoid (which locks the guard closed) and energize the hazardous portion of the machine. When shut down by the release of the guard, the hazard must be capable of being neutralized before the hazard can be reached. The guard cannot be opened when the solenoid is de-energized. While the guard remains unlocked and open, power to the hazardous portion of the machine remains off. Closing the guard does not supply power to the hazardous portion of the machine without a manual reset. To achieve Category 2, periodically test the guard interlock circuit at suitable intervals.

9.4.2.3 Power to Release, Dual Axis Guard Locking Interlock (Category 3)



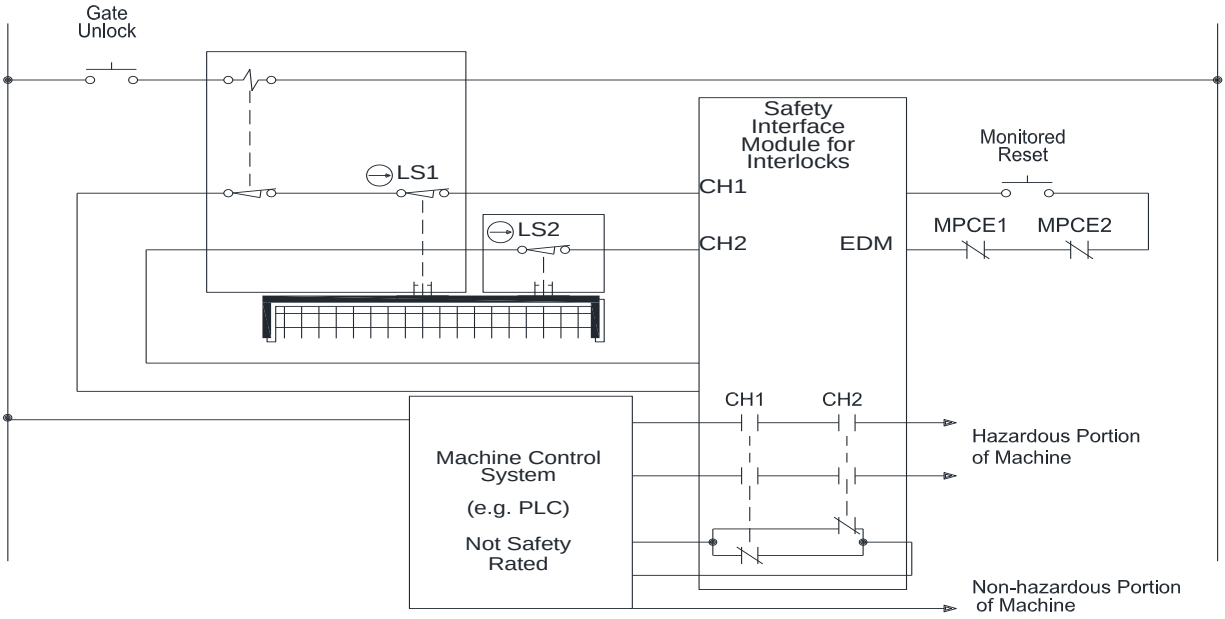
Safety Function:	When the hazardous motion has stopped, an interlocked guard may be released thereby removing power from the hazardous portion of the machine which shall stay de-energized until the guard is closed and reset.
Faults to Consider:	Failure of both limit contacts between use (test). Mechanical failure of the switch or actuator will not be detected. Both the solenoid contacts and the interlock contacts can mask a fault in each other; see 8.1.1 and informative note below.
Fault Exclusion:	Wiring short from power to the solenoid. Failure of the interlocking device may be excluded when: • damage to the interlocking device from incorrect actuator engagement is prevented (e.g., overspeed protection, overtravel protection, correct alignment); • the components of the interlocking device (actuator, switch, head) are mechanically mounted per the supplier's information for use; • periodic inspections and testing on the interlocking device and safety function are performed; • the recommended life is not exceeded; • the interlocking device is chosen for the correct environment. If all of the items in the bulleted list are not applied, the reliability may be reduced.
Safety Principles:	The timer or zero-speed switch prevents release of the guard until the hazard has been neutralized. While the guard remains unlocked and open, power to the hazardous portion of the machine remains off with the hazard in a safe state. The guard remains locked until the Guard Unlock button is pressed. Pressing the Guard Unlock button allows the guard to open and de-energizes the SIM outputs. Opening the guard and releasing the Guard Unlock button maintains the SIM safety outputs in the de-energized state. Closing the guard does not cause the SIM safety output to change state. The safety performance of the standstill (zero-speed) device feeding the Guard Unlock is equal to or greater than the system safety performance requirement. With the guard closed and the solenoid de-energized, the SIM safety outputs can be energized by pressing the Reset button. ***Informative Note:*** *Some suppliers of Solenoid Interlocks prewire the Solenoid Armature Lock mechanism contacts in series with the Guard Interlock, while others do not. To ensure that common cause failures are not hidden by this series connection, the user should consult the supplier's Information for Use. If the contacts are available individually, the design should have one Solenoid Contact in one channel and one Guard Interlock Contact in the other.*

9.4.2.4 Power to Release, Dual Axis Interlock Connected with secondary guard interlock switch to a SIM (Category 4)



Safety Function:	An interlocked guard is manually released, removing power from the hazardous portion of the machine which remains de-energized until the guard is closed and reset.
Faults to Consider:	Wiring short across the Guard Unlock button. Reset contacts are held closed. Wiring short across the Guard Unlock button, or shorted solenoid armature monitor contact.
Fault Exclusion:	Wiring short from power to the solenoid. Failure of the interlocking device may be excluded when: • damage to the interlocking device from incorrect actuator engagement is prevented (e.g., overspeed protection, overtravel protection, correct alignment); • the components of the interlocking device (actuator, switch, head) are mechanically mounted per the supplier's information for use; • periodic inspections and testing on the interlocking device and safety function are performed; • the recommended life is not exceeded; • the interlocking device is chosen for the correct environment. If all of the items in the bulleted list are not applied, the reliability may be reduced.
Safety Principles:	The guard remains locked until the Guard Unlock button is pressed. Pressing the Guard Unlock button allows the guard to open and de-energizes the SIM outputs. Opening the guard and releasing the Guard Unlock button maintains the SIM safety outputs in the de-energized state. Closing the guard does not cause the SIM safety output to change state. With the guard closed and the solenoid de-energized, the SIM safety outputs can be energized by pressing the Reset button. When shut down by the release of the guard, the hazard must be capable of being neutralized before the hazard can be reached. The addition of the separate, monitored safety-rated limit switch on the guard ensures that no common cause failure in the solenoid lock and switch assembly can lead to the loss of the safety function. ***Informative Note 1:*** *Some suppliers of Solenoid Interlocks prewire the Solenoid Armature Lock mechanism contacts in series with the Guard Interlock, while others do not. To ensure that common cause failures are not hidden by this series connection, the user should consult the supplier's Information for Use. If the contacts are available individually, the design should have one Solenoid Contact in one channel and one Guard Interlock Contact in the other.* ***Informative Note 2:*** *Additional safety circuitry may be required between the pushbutton (device) and the solenoid, depending on the application.*

9.4.2.5 Power to Release, Dual Axis Interlock Connected with Secondary Guard Interlocking Device to a SIM (Category 4)



Safety Function:	An interlocked guard is manually released, removing power from the hazardous portion of the machine which remains de-energized until the guard is closed and reset.
Faults:	Wiring short across the Guard Unlock button, or shorted solenoid armature monitor contact.
Fault Exclusion:	Wiring short from power to the solenoid. Failure of the interlocking device may be excluded when: • damage to the interlocking device from incorrect actuator engagement is prevented (e.g., overspeed protection, overtravel protection, correct alignment); • the components of the interlocking device (actuator, switch, head) are mechanically mounted per the supplier's information for use; • periodic inspections and testing on the interlocking device and safety function are performed; • the recommended life is not exceeded; • the interlocking device is chosen for the correct environment. If all of the items in the bulleted list are not applied, the reliability may be reduced.
Safety Principles:	The guard remains locked until the Guard Unlock button is actuated. Actuating the Guard Unlock button allows the guard to open but does not change the state of the SIM outputs. Opening the guard and releasing the Guard Unlock button maintains the SIM safety outputs in the de-energized state. Closing the guard does not cause the SIM safety output to change state. With the guard closed and the solenoid de-energized, the SIM safety outputs can be energized by pressing the Reset button. When shut down by the release of the guard, the hazard must be capable of being neutralized before the hazard can be reached. The addition of the separate, monitored safety-rated limit switch on the guard ensures that no common cause failure in the solenoid lock and switch assembly can lead to loss of the safety function. ***Informative Note 1:*** *Some suppliers of Solenoid Interlocks prewire the Solenoid Armature Lock mechanism contacts in series with the Guard Interlock, while others do not. To ensure that common cause failures are not hidden by this series connection, the user should consult the supplier's Information for Use. If the contacts are available individually, the design should have one Solenoid Contact in one channel and one Guard Interlock Contact in the other.* ***Informative Note 2:*** *Additional safety circuitry may be required between the pushbutton (device) and the solenoid, depending on the application.*

9.5 Optical Presence Sensing Devices

9.5.1 Design Requirements

See ANSI B11.19 for design/performance requirements for Optical Presence Sensing Devices.

9.5.2 Design Considerations

The following design considerations should be applied as part of the design process for the SRP/CS.

9.5.2.1 General Information

The three styles of electro-optical presence-sensing devices are:

- safety light curtains (safety light screen);
- single and multiple safety beams (point and grid systems);
- safety area scanners (diffuse reflection devices).

An electro-optical presence-sensing device function relies on the presence or absence of light for actuation. Typical methods are:

- through-beam principle, where the light beam(s) traverses the detection zone once, and an interruption (blockage) of one or more beams detects an object;
- retro-reflective principle, where the light beam(s) traverses the detection zone twice, and an interruption (blockage) of one or more beams detects an object;
- diffuse reflection, where the light beam strikes an object, and a portion of the light is reflected to a receiving element(s) whereby the presence or location of the object is determined;
- vision-based, where a receiving element(s) detects changes in the ambient light or the presence or absence of an object.

Some designs have electromechanical relay outputs. Other designs provide solid-state OSSD outputs, which provide fault monitoring of the outputs.

9.5.2.2 Light Curtains

Light Curtains are typically micro-processor based products that are designed and constructed to meet IEC 61496-2. Primarily, they use the through-beam principle of sensing, but systems are available that use the retro-reflective principle. In either design, an interruption of a beam of light (a “dark” condition) causes the outputs to go to an OFF-state, sending an immediate stop command to the machine control.

IEC 61496-2 describes two “types” of Light Curtains that differ in their performance in the presence of faults and under influences from environmental conditions. The requirements for a Type 2 system are less stringent than for a Type 4 system. Thus, a Type 2 rating generally limits usage to Category 2 applications, while a Type 4 rating is allowed in Category 4 applications.

9.5.2.3 Single/Multiple Beam Devices (Point or Grid Devices)

Single/Multiple Beam Devices are typically micro-processor based products that are designed and constructed to meet IEC 61496-2. They primarily use the through-beam principle of sensing and are typically mounted to detect the torso of an individual entering an area. As with a Light Curtain, an interruption of a beam of light (a “dark” condition) causes the outputs to go to an OFF-state, sending an immediate stop command to the machine control.

IEC 61496-2 describes two “types” of Single/Multiple Beam Devices that differ in their performance in the presence of faults and under influences from environmental conditions. The requirements for a Type 2 system are less stringent than for a Type 4 system. Thus, a Type 2 rating generally limits usage to Category 2 applications, while a Type 4 rating is allowed in Category 4 applications.

9.5.2.4 Scanners

Scanners are micro-processor based products designed and constructed to meet IEC 61496-3. Scanners use a diffuse reflection, time-of-flight principle to detect an object. A pulsing beam of light rotates to create a safety plane. The size of the object detected typically depends on the distance and configuration of the scanner. For example, the time-of-flight technique measures the time it takes the scanner to receive the beam reflected by the object. This principle allows the scanner to establish a warning zone and a safety zone.

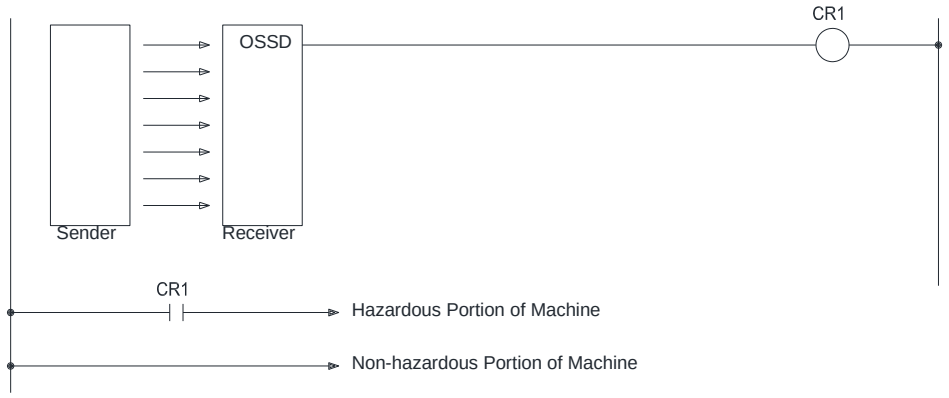
Informative Note: *The warning zone may or may not be safety-rated.*

The diffuse reflection principle and Type 3 rating typically limits their usage to Category 3 applications.

9.5.3 Application Examples

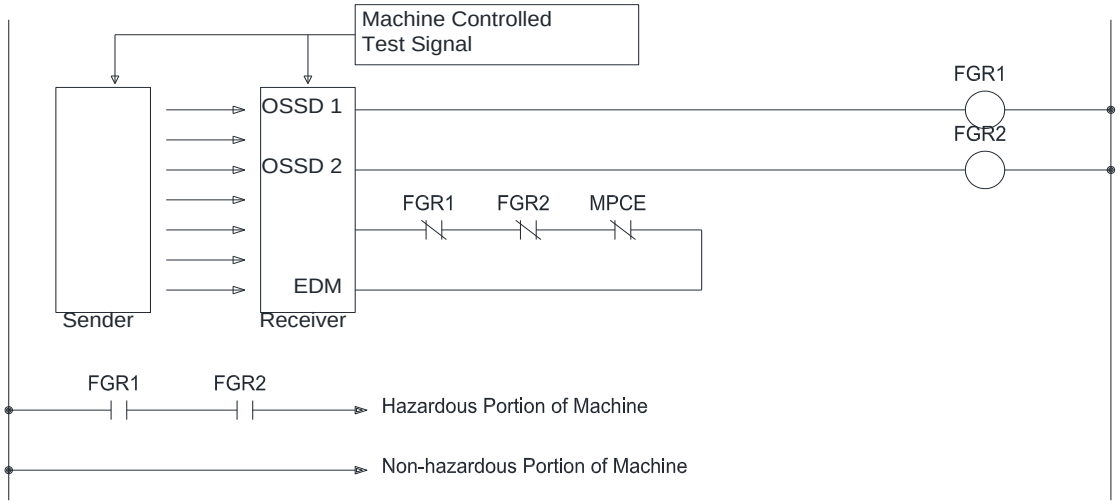
The following circuits are depicted as Light Curtains but may be applied to any presence sensing device(s) described in this subclause.

9.5.3.1 IEC 61496 Type 2 Presence Sensing Device with Control Relay (Category 1)



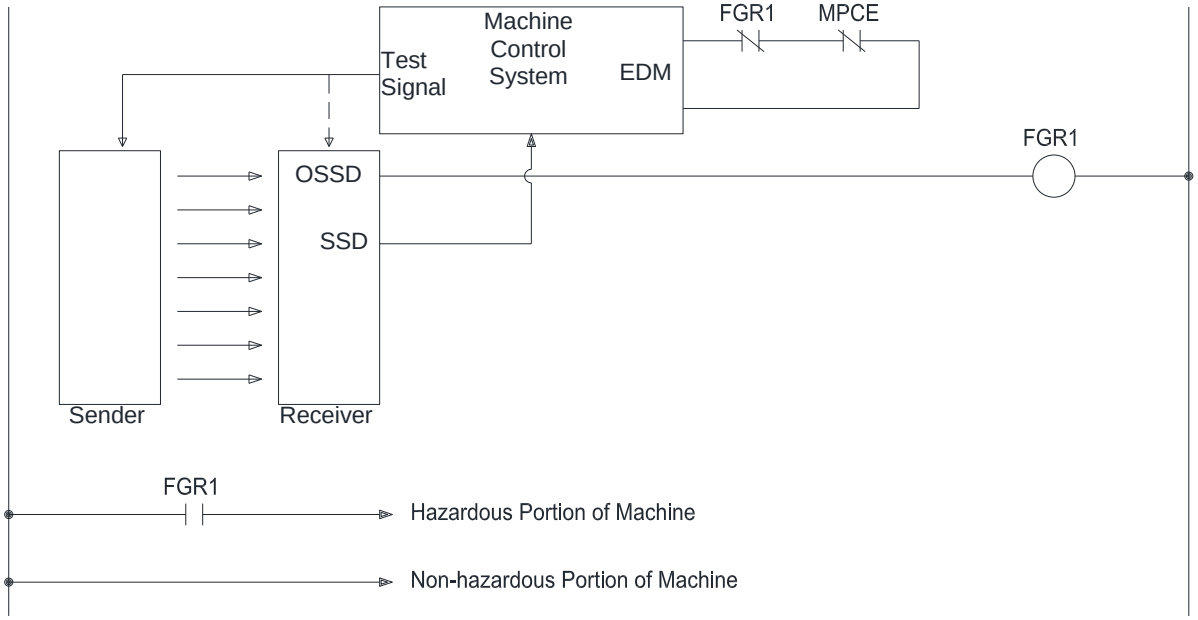
Safety Function:	When the Light Curtain is interrupted, the relay removes power from the hazardous portion of the machine.
Faults to Consider:	Type 2 presence sensing devices do not detect all internal failures. Failure of the OSSD to “ON.” Failure of CR1 to drop or its contact to open. Wiring short from power to the relay coil of CR1.
Fault Exclusion:	None to consider.
Safety Principles:	The safety distance is established for placement of the OSSD such that the hazardous portion of the machine stops before personnel can reach the hazard. For point of operation guarding, the Light Curtain may be configured to automatic reset depending on the application; see ANSI B11.19. For perimeter guarding applications, the Light Curtain should be manually reset.

9.5.3.2 IEC 61496 Type 2 Presence Sensing Device with Force-Guided Relay (Category 2)



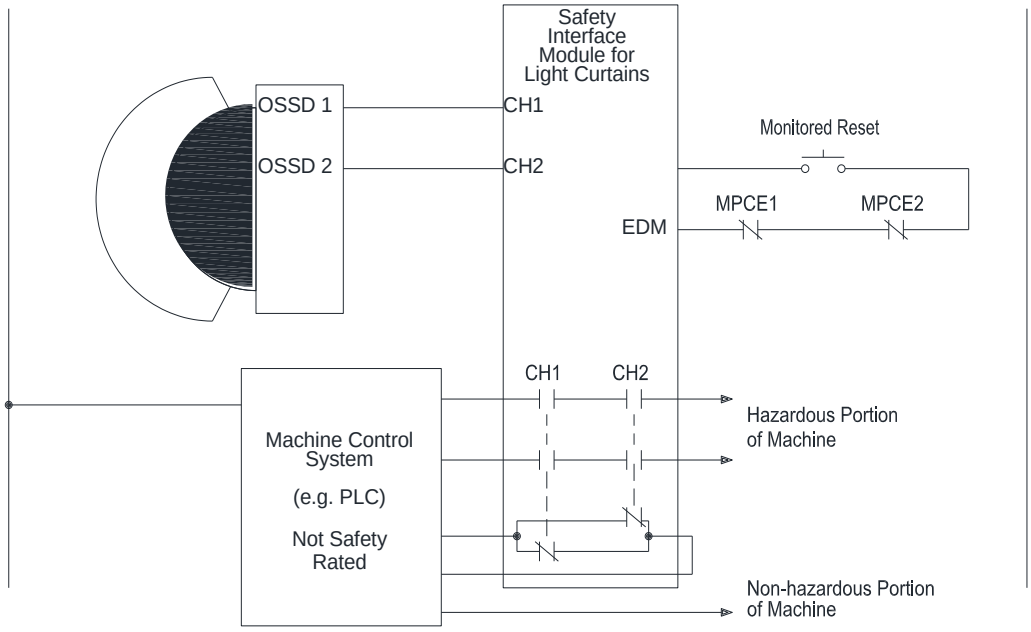
Safety Function:	When the Light Curtain is interrupted, the Force-Guided Relays remove power from the hazardous portion of the machine.
Faults to Consider:	Type 2 presence sensing devices do not detect all internal failures. Wiring short from power to the relay coil of CR1.
Fault Exclusion:	None to consider.
Safety Principles:	To achieve Category 2, periodic testing is required. The safety distance is established for placement of the OSSD such that the hazardous portion of the machine stops before personnel can reach the hazard. For point of operation guarding, the Light Curtain may be configured to automatic reset depending on the application; see ANSI B11.19. For perimeter guarding applications, the Light Curtain should be manually reset. The mechanically linked contacts of the Force-Guided Relays provide checking on each energization and de-energization of the safety circuit.

9.5.3.3 IEC 61496 Type 2 Presence Sensing Device with Force-Guided Relay (Category 2)



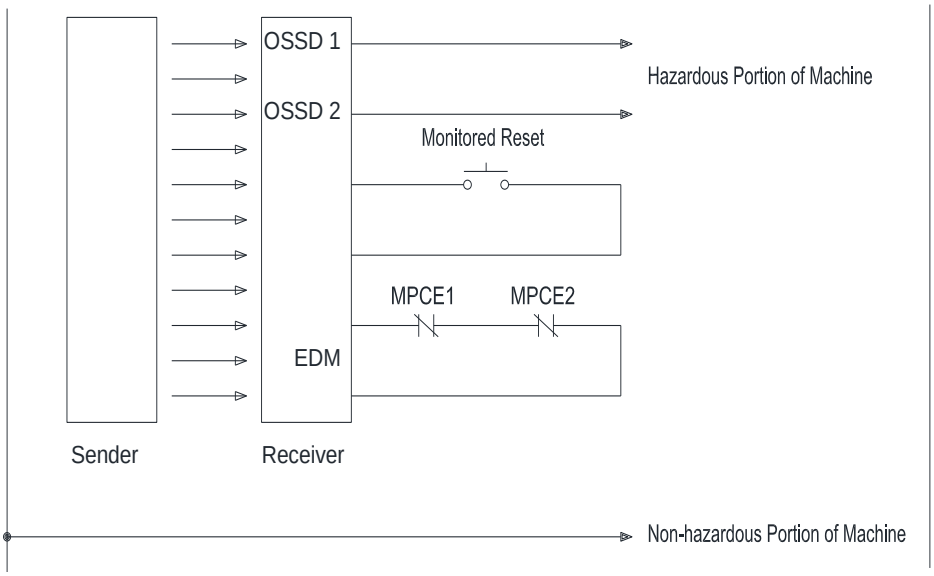
Safety Function:	When the Light Curtain is interrupted, the Force-Guided Relay FGR1 removes power from the hazardous portion of the machine.
Faults to Consider:	Type 2 presence sensing devices do not detect all internal failures. Wiring short from power to the relay coil of CR1.
Fault Exclusion:	None to consider.
Safety Principles:	The safety distance is established for placement of the OSSD such that the hazardous portion of the machine stops before personnel can reach the hazard. The machine-controlled test signal shall be configured to check the operation of the Light Curtain at periodic intervals. The mechanically linked contacts of the Force-Guided Relay and MPCE provide checking on each energization of the safety circuit. The SSD output sends a signal to the machine control system if a fault is detected. Upon detection of the SSD signal, the machine control system executes a stop function. To achieve Category 2, periodic testing is required. For point of operation guarding, the Light Curtain may be configured to automatic reset depending on the application; see ANSI B11.19. For perimeter guarding applications, the Light Curtain should be manually reset.

9.5.3.4 IEC 61496 Type 3 Presence Sensing Device with Safety Interface Module (Category 3)



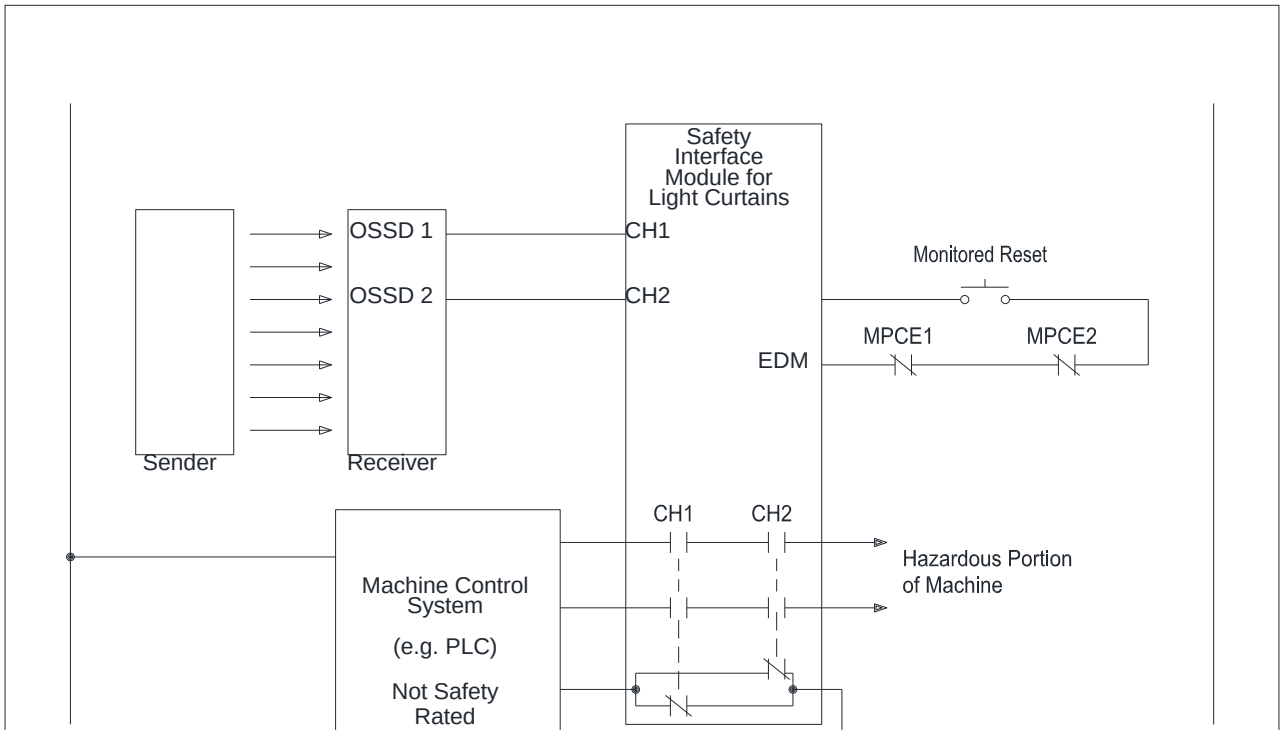
Safety Function:	When light from the scanner is reflected by an object which is determined by the receiver to be in the safety zone, the OSSD should go to a low state and the safety interface module removes power from the hazardous portion of the machine.
Faults to Consider:	None.
Fault Exclusion:	None to consider.
Safety Principles:	The safety distance is established for placement of the OSSD such that the hazardous portion of the machine stops before personnel can reach the hazard. For point of operation guarding, the monitored reset may be changed to automatic reset. For perimeter guarding applications, the SIM should be manually reset. The Type 3 Electro Sensitive Device limits this circuit to Category 3. Category 3 requires redundancy (MPCE1, MPCE2). Monitoring both devices is considered best practice. ***Informative Note:*** *Due to the triangular "shadow" cast by the rotating beam source, a small object close to the scanner can hide a potentially large object such as an individual approaching the scanner.*

9.5.3.5 IEC 61496 Type 4 Presence Sensing Device with OSSD (Category 4)



Safety Function:	When the Light Curtain is interrupted, power is removed from the MPCEs and the hazardous portion of the machine.
Faults to Consider:	None.
Fault Exclusion:	None to consider.
Safety Principles:	The safety distance is established for placement of the presence sensing device such that the hazardous portion of the machine stops before personnel can reach the hazard. For point of operation guarding, the Light Curtain may be configured to automatic reset depending on the application; see ANSI B11.19. For perimeter guarding applications, the Light Curtain should be manually reset. The contactors can be energized from the OSSD. The Light Curtain is self-contained with OSSD output monitoring and external device monitoring.

9.5.3.6 IEC 61496 Type 4 Presence Sensing Device with Safety Interface Module (Category 4)



Safety Function:	When the Light Curtain is interrupted, the safety interface module removes power from the hazardous portion of the machine.
Faults to Consider:	None.
Fault Exclusion:	Short from power to the output of the SIM if the final switching elements are located in the same control panel, wiring meets NFPA 79. Shorts validated during commission or other equivalent measures are used.
Safety Principles:	The safety distance is established for placement of the OSSD such that the hazardous portion of the machine stops before personnel can reach the hazard. For point of operation guarding, the monitored reset may be changed to automatic reset. For perimeter guarding applications, the SIM should be manually reset.

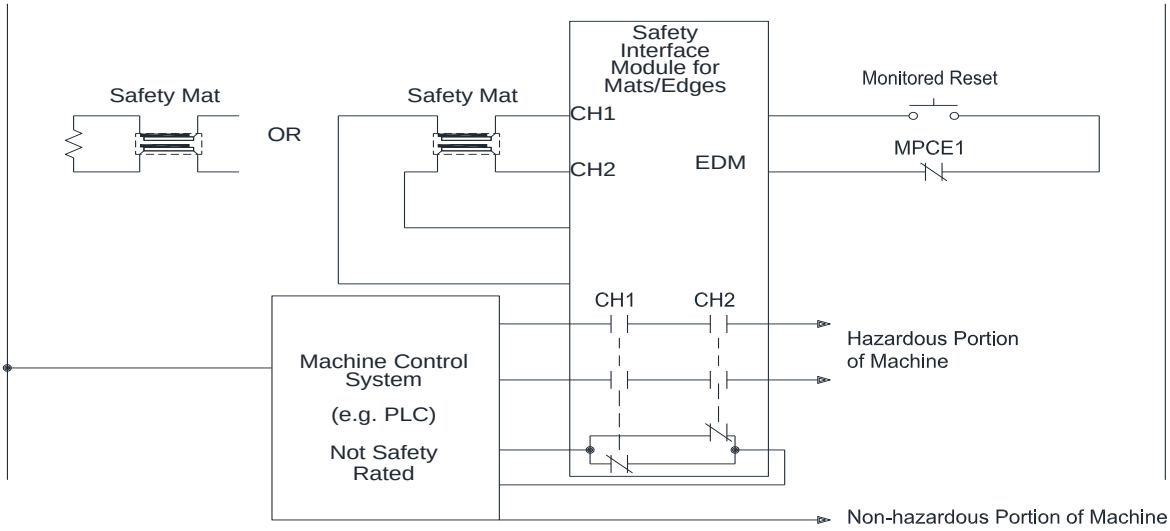
9.6 Safety Mats / Edges

9.6.1 Design Requirements

Most safety mats come in two basic types: 4-wire or 2-wire, with a terminating resistor. Both offer the same level of safety performance. The control unit shall be selected to accommodate the selected type. Edges using safety mat technology are applicable.

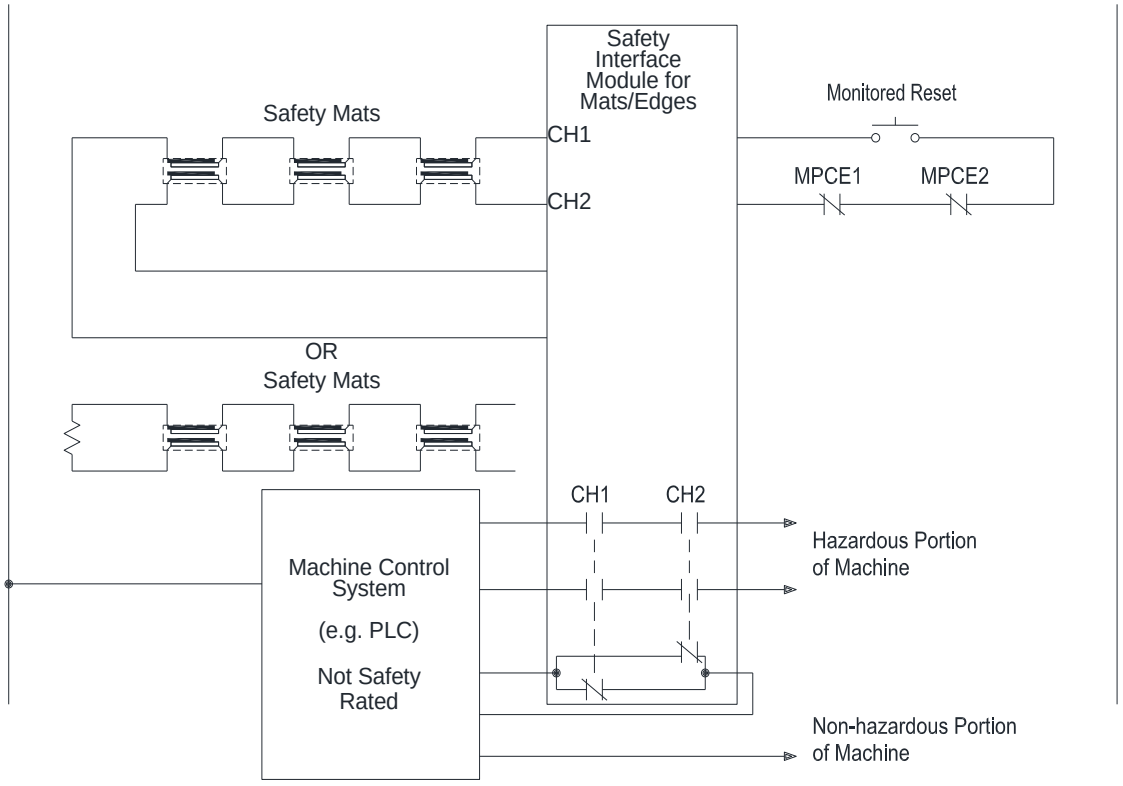
9.6.2 Application Examples

9.6.2.1 Single Safety Mat using a Safety Interface Module (Category 2)



Safety Function:	Stepping on the mat causes the outputs of the safety interface module to turn off.
Faults to Consider:	Failure of the mat to detect an individual due to mechanical damage.
Fault Exclusion:	None to consider.
Safety Principles:	While standing on the mat, the power to the hazardous portion of the machine remains off. The hazardous portion of the machine will not restart after stepping off the mat. Press and release the Reset button to close the safety contacts of the safety interface module. Safety interface modules for mats/edges are designed for specific mat/edge connection; refer to supplier specifications. This design is limited to Category 2 due to the capability of the SIM depicted. ***Informative Note:*** *Select an appropriate safety mat/edge controller for the mat configuration. The same controller cannot be used for both of the configurations shown above.*

9.6.2.2 Multiple Safety Mats using a Safety Interface Module (Category 3)



Safety Function:	Stepping on any part of the mats causes the outputs of the safety interface module to turn off.
Faults to Consider:	Failure of any mat to detect an individual due to mechanical damage.
Fault Exclusion:	None to consider.
Safety Principles:	While standing on any of the mats, the power to the hazardous portion of the machine remains off. The hazardous portion of the machine will not restart after stepping off the mat. Press and release the Reset button to close the safety contacts of the safety interface module. To achieve a Category 3 requires redundancy (MPCE1, MPCE2). Monitoring both devices is considered best practice. Use of multiple safety mats does not change the safety performance of the system since the active circuit is common to each. ***Informative Note 1:*** *Select an appropriate safety mat/edge controller for the mat configuration. The same controller cannot be used for both of the configurations shown above.* ***Informative Note 2:*** *The second safety mat configuration shown uses two four-wire mats in conjunction with one two-wire resistance mat. For multiple two-wire resistor mats, the mats are connected in parallel at the resistive safety mat controller, and the termination resistor of each mat is increased to n times R, where n is the number of parallel mats and R is the resistance used for an individual mat.*

9.7 Two-Hand Control

9.7.1 Design Requirements

Type I and type II two-hand control devices are not intended for safety applications; therefore, this standard only addresses Type III two-hand control devices.

Informative Note 1: *See ANSI B11.19 and ISO 13851 for additional design, construction, installation, operation and maintenance requirements.*

Informative Note 2: *See ANSI B11.TR1 Annex K for ergonomic considerations in two-hand control device applications.*

Informative Note 3: *Both electric and pneumatic controls should conform to the requirements in ISO 13851.*

See ANSI B11.19 for design requirements for two-hand control devices. In addition, Two-Hand control circuits shall:

- require synchronous actuation by both hands within 500 ms;
- where the synchronous actuation time limit is exceeded, require both hand controls to be released before operation is initiated;
- require continuous actuation during hazardous condition;
- inhibit hazardous condition if either hand control is released once operation begins;
- require release and re-actuation of both hand controls to re-initiate the hazardous operation (i.e., “anti-tie down”).

9.7.2 Design Considerations

The following design considerations should be applied as part of the design process for the SRP/CS.

9.7.2.1 General Information

The reliability and the safety of the circuitry for two-hand control devices primarily, but not exclusively, rely on the physical installation and the electrical or pneumatic interfacing of the hand controls (actuating devices).

Informative Note: *ISO 13851 describes the functional and safety requirements of two-hand control devices and the relationship of the Type designation to the Category requirements of ISO 13849-1. ISO 13851 segments the Type III designation into three sub-classifications: Type IIIa, Type IIIb, and Type IIIc. While all three sub-classifications have the same functional requirements as described above, ISO 13851 requires at a minimum that Type IIIa meets a Category 1, Type IIIb meets a Category 3, and Type IIIc meets a Category 4 per ISO 13849-1.*

These devices typically exhibit the following characteristics:

- Type IIIa, Category 1: A single failure can result in the loss of the safety function (e.g., a short circuit across a single normally open contact in one palm button results in no stop signal when a hand is removed from that palm button);
- Type IIIb, Category 3: A single failure does not result in the loss of the safety function, but an accumulation of undetected failures can result in the loss of the safety function (e.g., a palm button that has two independent normally open contacts can resist a single failure, but can fail unsafe if two shorts across the redundant contacts occur);
- Type IIIc, Category 4: A single failure does not result in the loss of the safety function. This is typically accomplished with a palm button that has two independent contacts, one normally open and one normally closed.

9.7.2.2 Tampering / Defeat

Mounting location and orientation must be designed specifically to avoid defeat through actuation by any body parts other than two hands.

9.7.2.3 Failure Modes

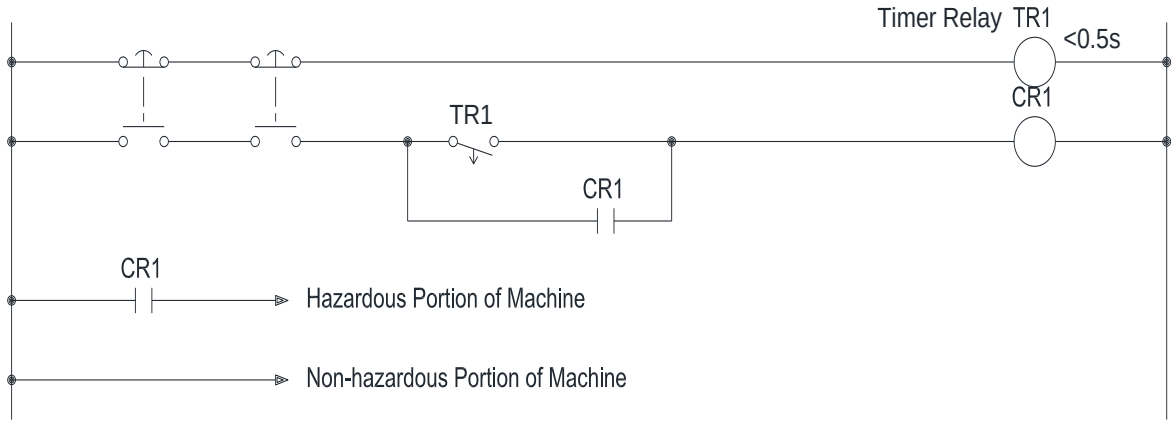
Failure modes specific to two-hand control devices include but are not limited to:

- a broken spring, mechanical seizure, etc., that would result in not detecting the release of a hand control;
- severe contamination or other environmental influences that can cause slow response when released or a false ON condition of the hand control(s), e.g., sticking of mechanical linkages;
- the functional reliability and installation of the logic devices (e.g., Timer Relays (TR), Control Relays (CR) Two-Hand Control Safety Interface Modules (SIM)).

Routine functional checks and maintenance may be required to address some failure modes.

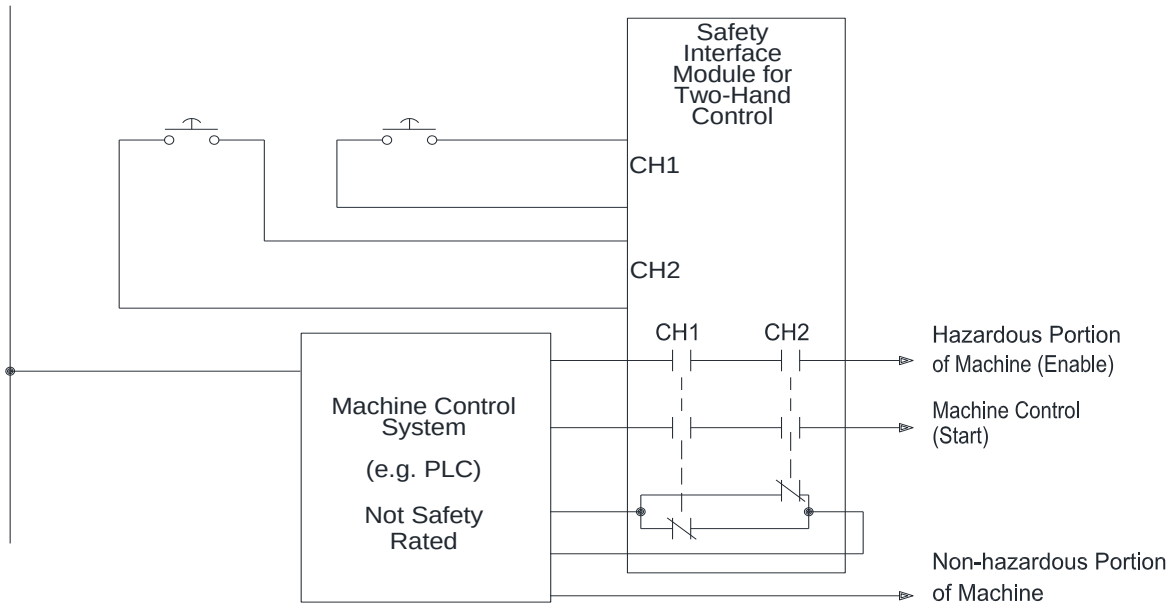
9.7.3 Application Examples

9.7.3.1 Two-Hand Control Device (Type IIIa Category 1)



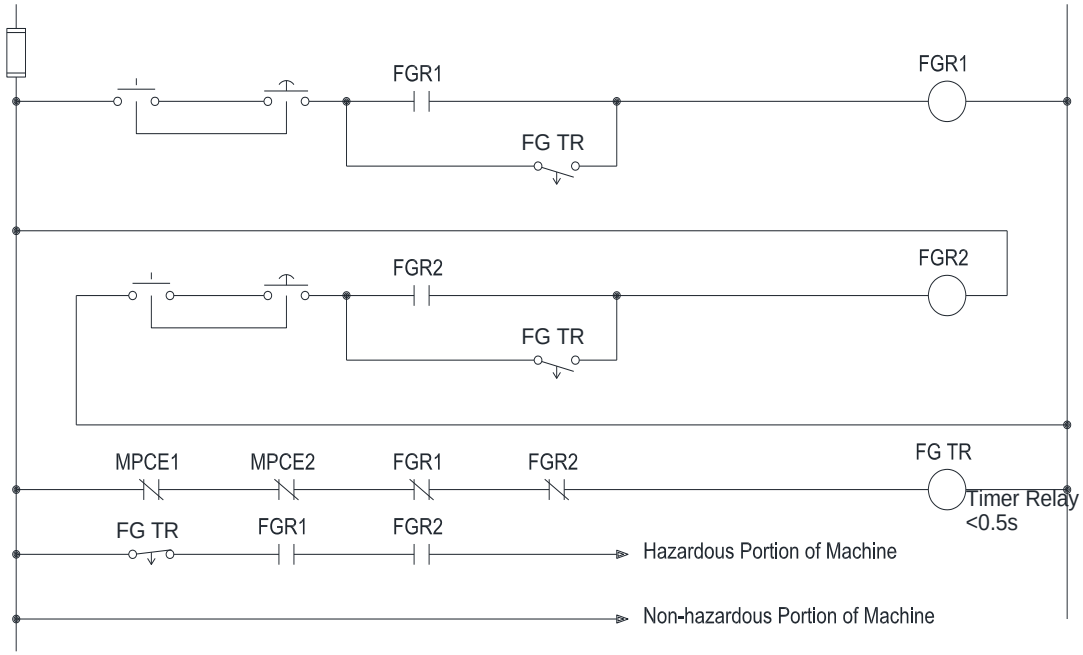
	Power will not be supplied to the hazardous portion of the machine until both switches are released and then are re-actuated within 0.5 seconds of each other, and then maintained throughout the hazardous portion of the cycle.
Faults to Consider:	The functional reliability and installation of the Timer Relay (TR) and the Control Relay (CR) that could result in: - stuck armature in CR1; - welded contacts of CR1 or TR1; - wiring short from power to the coil or across a contact of CR1 or TR1; - a change in the drop out time of TR1.
Fault Exclusion:	Failure of either button to return when released (i.e., open the circuit).
Safety Principles:	Well-tried devices are used. Complies with basic functional requirements of a two-hand control per NFPA 79 and IEC 60204-1. ***Informative Note:*** *FG TR is a normally open held closed off delay timer contact with a delayed drop out of less than 500 ms.*

9.7.3.2 Two-Hand Control Device (Type IIIa Category 1)



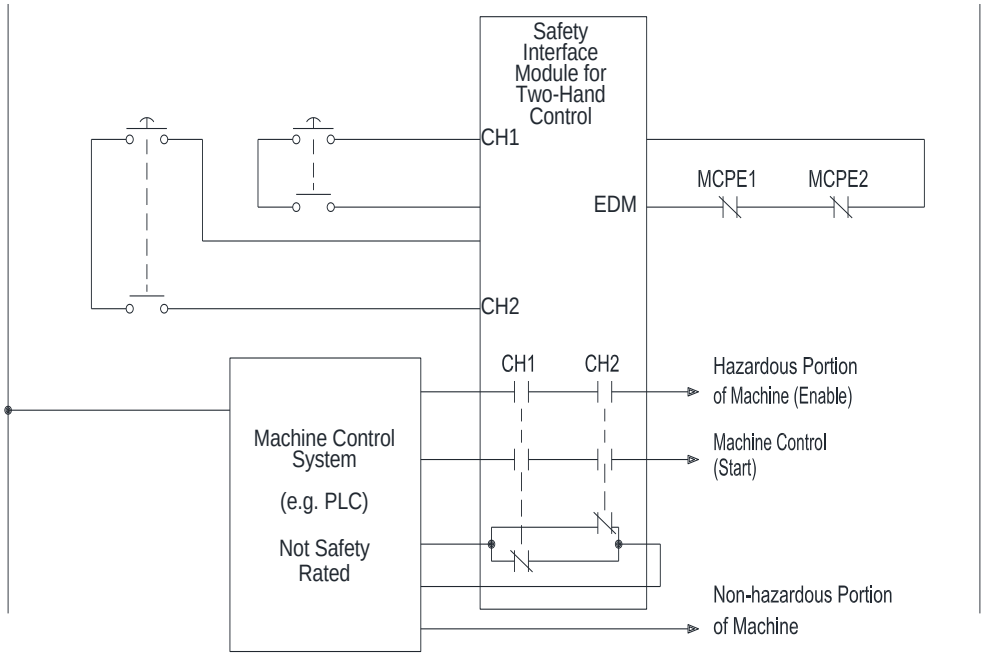
Safety Function:	Power will not be supplied to the hazardous portion of the machine until both switches are released and then are re-actuated within 0.5 seconds of each other, and then maintained throughout the hazardous portion of the cycle.
Faults to Consider:	A short circuit in the interconnect wiring for a two-hand control and the safety interface module will result in the loss of the stop command.
Fault Exclusion:	Failure of either button to return when released (i.e., open the circuit).
Safety Principles:	The primary limitation of this circuit is the method with which the hand controls are being monitored. Since each button only provides a single normally open contact, a short circuit, a broken spring, or a mechanical seizure, etc. can result in the safety module not detecting the release of the button. A free hand could result without cessation of the hazardous condition. Under these fault conditions, another cycle is prevented. Complies with basic functional requirements of a two-hand control per NFPA 79 and IEC60204-1. ***Informative Note:*** *At a minimum, this circuit complies with requirements of a Type IIIa Two-hand Control Device per ISO 13851.*

9.7.3.3 Two-Hand Control Device (Type IIIb Category 3)



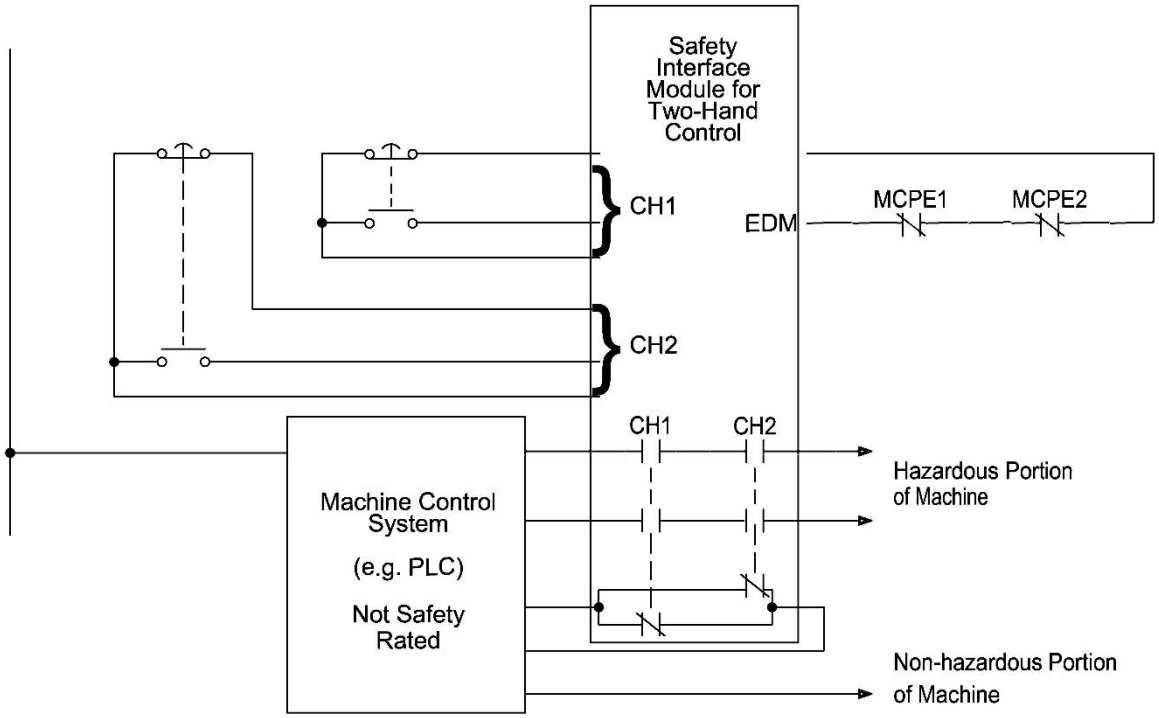
Safety Function:	Power will not be supplied to the hazardous portion of the machine until both switches are released and then are re-actuated within 0.5 seconds of each other, and then maintained throughout the hazardous portion of the cycle.
Faults to Consider:	The functional reliability and installation of the Timer Relay (TR) that could result in a change in the drop-out time of TR1.
Fault Exclusion:	Failure of either button to return when released (i.e., open the circuit).
Safety Principles:	Complies with basic functional requirements of a two-hand control per NFPA 79 and IEC 60204-1. The risk reduction is improved by adding redundant Force-Guided Relays and monitoring those relays via normally closed contacts in the timer relay circuit. ***Informative Note:*** *TR1 is a normally open held closed off delay timer contact with a delayed drop out of less than 500 ms.* Input wire to wire shorts are detected by switching both sides of the circuit, causing a short and opening of the fuse (typically done on low voltage ungrounded circuits). Category 3 requires redundancy (MPCE1, MPCE2). Monitoring both devices is considered best practice. Periodically test the circuit to ensure the function of each pushbutton.

9.7.3.4 Two-Hand Control Device (Type IIIb Category 3)



Safety Function:	Power will not be supplied to the hazardous portion of the machine until both switches are released and then are re-actuated within 0.5 seconds of each other, and then maintained throughout the hazardous portion of the cycle.
Faults to Consider:	The safety interface module meets the required level of safety performance for the expected level of risk reduction. A short circuit between input channels is detected and an immediate stop command is issued. The design, construction, and installation of the palm buttons have redundant contacts that have separate mechanical linkages and springs. An accumulation of failures or a short circuit in the interconnect wiring for a hand control and the safety interface module will result in the loss of the stop command.
Fault Exclusion:	Failure of either button to return when released (i.e., open the circuit).
Safety Principles:	Complies with basic functional requirements of a two-hand control per NFPA 79 and IEC 60204-1. ***Informative Note:*** *At a minimum, this circuit complies with requirements of a Type IIIb Two-hand Control Device per ISO 13851.* The method that the hand controls are being monitored is similar to the Type IIIa circuit (i.e., “four-wire” hookup), but to overcome the possibility of certain single failures, a second normally open contact per button is required. The redundant contact configuration eliminates or minimizes failures that can include a short circuit across a single contact, a single broken spring, and some mechanical seizure issues. While these failures are not detected, this reduces the chance of a free hand without cessation of hazardous conditions. Category 3 requires redundancy (MPCE1, MPCE2). Monitoring both devices is considered best practice.

9.7.3.5 Two-Hand Control Device (Type IIIc Category 4)



Safety Function:	Power will not be supplied to the hazardous portion of the machine until both switches are released and then are re-actuated within 0.5 seconds of each other, and then maintained throughout the hazardous portion of the cycle.
Faults to Consider:	The safety interface module meets the required level of safety performance as determined by the risk assessment for the expected level of risk reduction. A short circuit between input channels is detected and an immediate stop command is issued. The design, construction, and installation of the palm buttons have redundant contacts that have separate mechanical linkages and springs.
Fault Exclusion:	Failure of either button to return when released (i.e., open the circuit).
Safety Principles:	Complies with basic functional requirements of a two-hand control per NFPA 79 and IEC 60204-1. ***Informative Note:*** *At a minimum, this circuit complies with requirements of a Type IIIc Two-Hand Control Device per ISO 13851.* This method of monitoring the hand controls is superior to the “four-wire” hook-up of Type IIIa and Type IIIb Two-Hand Control Device circuits. Hand Controls in a Type IIIc Two-Hand Control Device not only offers redundant contacts (or outputs), but also detect reasonably foreseeable failure modes that would lead to not detecting the release of a hand control. The “six-wire” N.O./N.C. hook up further eliminates or minimizes failures that Type IIIb addresses by monitoring for a short circuit in the interconnect wiring. This further reduces the chance of a free hand without cessation of hazardous condition.

9.8 Speed Detection

9.8.1 Design Requirements

Speed detection in a safety function shall determine when hazardous motion has ceased or is at a specific safe velocity / RPM.

Informative Note: *Safe velocity / RPM may be determined by a risk assessment or applicable machine-specific "base" safety standard(s).*

9.8.2 General Information and Design Considerations

A common application example for speed detection is where an engineering control – device is too close to the hazardous motion to ensure that the motion has ceased before the hazard can be reached. Under these conditions, access is permitted to the hazard only after the velocity is below the defined value. Access control is commonly accomplished through the use of solenoid operated locks or key release which enable access through physical barrier(s). The following design considerations should be applied as part of the design process for the SRP/CS.

Common means of determining speed are given in 9.8.2.1 – 9.8.1.3.

Informative Note: *Time delay as a means of speed detection has not been included in the methods due to the large variation in stopping times that may occur. Such designs must be evaluated for both physical stop time variations and timer variations/ faults. Means to ensure that the prime mover has been de-energized may also be required.*

9.8.2.1 Back EMF Sensing

The speed detection device measures the phase to phase voltage at the motor leads after the supply power has been removed. The voltage (back EMF) generated by the revolving rotor decreases as its RPM slows. When the voltage has reached a sufficiently low value and indicates an almost stopped state, the speed detection device(s) energizes the output. Some devices may sense the inverse voltage spike which is generated at stop. The use of these devices with variable frequency drives or servo drives can generate false outputs. Consult the suppliers' application data regarding compatibility with various drive systems.

9.8.2.2 Encoder Sensing

The speed detection device(s) monitors an encoder pulse train to determine the speed and direction of the hazardous motion. The encoder is usually mounted on the motor but may be attached to any drive train rotating shaft. Safety-rated encoders are also available.

9.8.2.3 Proximity Switch Sensing

The sensor detects a mechanical feature on a moving portion of the drivetrain. Most systems use inductive proximity switches counting pulses, but see-through or opposed mode photo-electric sensors are also used. The speed detection device(s) monitors sensor pulses to determine the velocity. The number of features (targets) determines the relative sensitivity of the speed sensing. Comparison to the set point may be time between pulses or pulse train frequency. Higher safety Category systems will use multiple sensors and sensing points.

The Proximity Switch and Encoder Sensing technologies may also be used to monitor any given "safe" speed, not just zero. Back EMF sensing is typically only applied for zero speed.

9.8.2.4 Tampering / Defeat

As speed detection is commonly integrated in the drivetrain of machinery, tampering or defeat is less common.

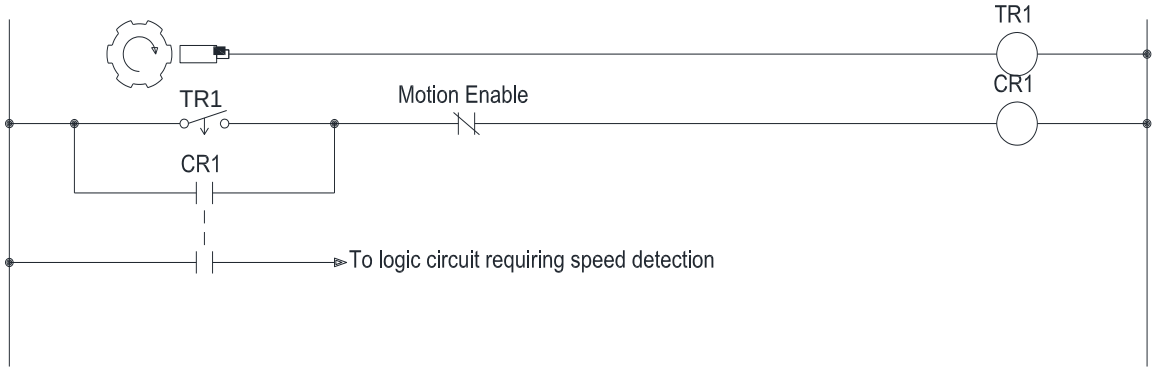
9.8.2.5 Failure Modes

Failure modes specific to speed detection devices include but are not limited to:

- failure of drive train components such that the speed monitoring elements "see" no motion when the hazard is still moving, e.g., monitoring the motor speed on a belt drive output hazard such as a saw blade. In this case, the belt could fail during the braking torque allowing the saw blade to continue to spin even though the motor has ceased all motion;
- failures related to the application of Back EMF type devices on Variable Frequency Drive or other incompatible drive systems.

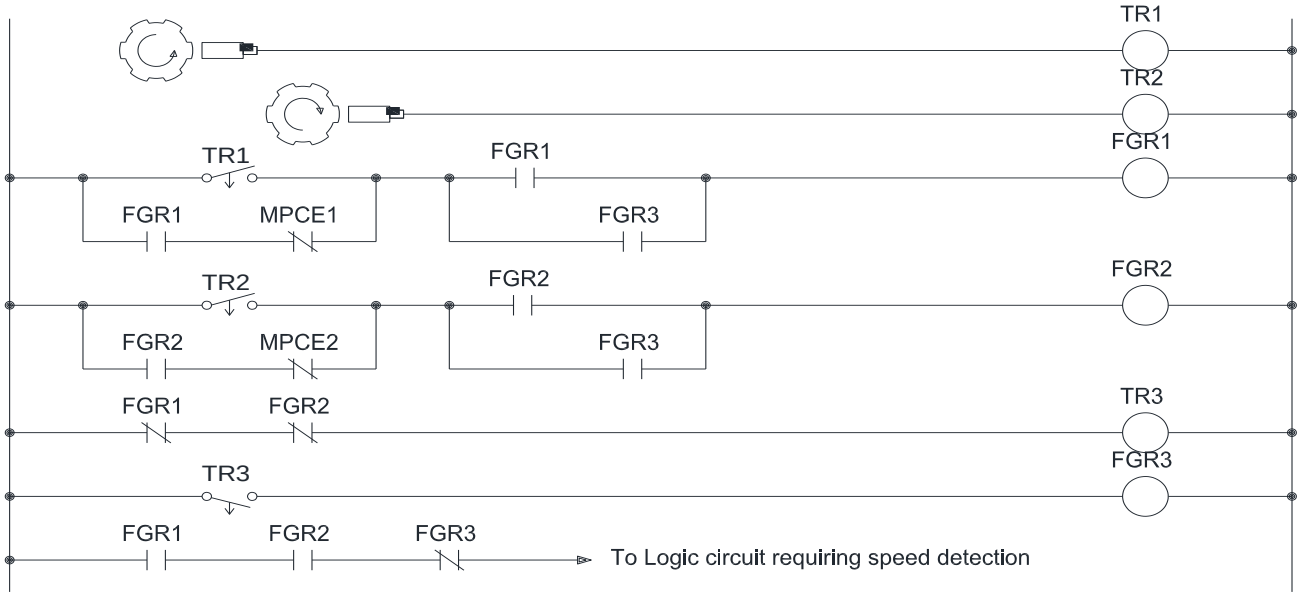
9.8.3 Application Examples

9.8.3.1 Single Proximity Sensing (Category 1)



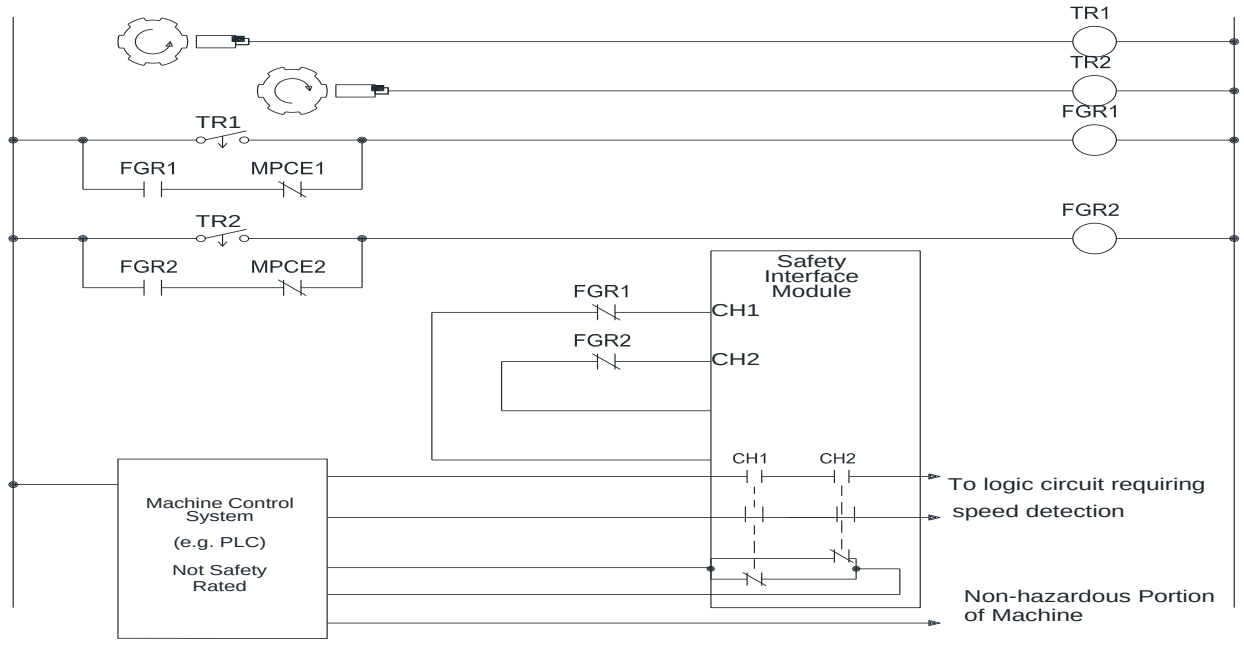
Safety Function:	The output of this circuit supplies power when the rotating part of the machine comes to a stop.
Faults to Consider:	Failure of the sensor to detect the pulse train causing immediate “zero-speed” indication. Failure of the sensor in the off mode causing immediate “zero-speed” indication. Failure of the sensing object coupling. Loss of drive integrity between motor and hazardous motion. Failure of timer TR1. Failure of CR1 armature. Welded contacts. Power supply brown-out causing false sensor output. Failure of the Motion Enable contact to open during the machine run time.
Fault Exclusion:	Failure of the sensor to detect the speed may be excluded when robustly mounted on the hazardous motion with minimum slippage between components and use of vibration tolerant fastening systems. Power supply brown out may be excluded if the relay drop-out voltage is higher than the sensor’s sensing failure voltage.
Safety Principles:	The circuit STOPPED output supplies power when the rotation of the pulse train has approached zero motion. The STOPPED signal is used in the safety portion of the control circuit to gain access to the safeguarded space when motion has ceased. The proximity switch resets the off-delay timer at each sensing pulse. When the interval between pulses exceeds the off-delay setting, the N.C. contact closes and pulls in holding relay CR1. The pulse train interval allows the relays to have time to cycle between lobes at the last transition. “Motion Enable” is a force guided contact from the contactor that controls the hazardous motion. The normally closed auxiliary contact resets the holding circuit when the hazard is under power. The actual speed of the pulse train at “zero” speed is a function of the number of pulses as well as the timer setting. An error in setting the timer too short can produce an output even though the object is still moving. To make this Category 2, provide cyclic monitoring of the speed detection output within the machine control.

9.8.3.2 Dual Proximity Sensors to Timers and Force-Guided Relay Monitoring (Category 3)



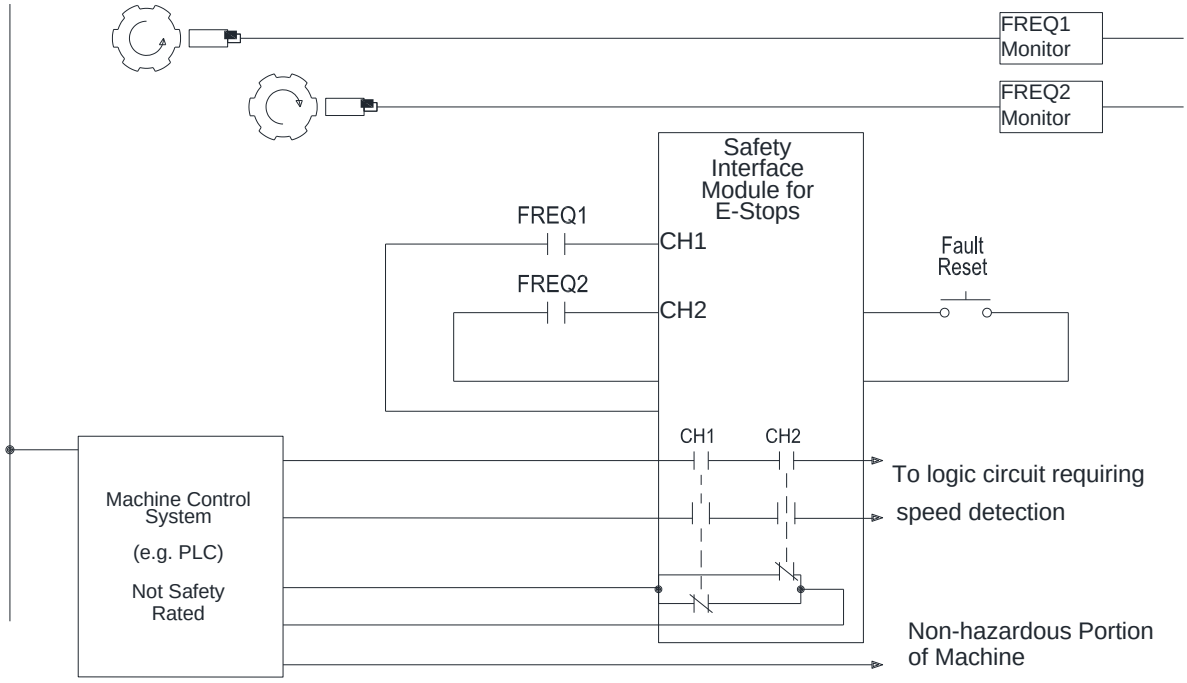
Safety Fxn:	The output of this circuit supplies power when the rotating part of the machine comes to a stop.
Faults to Consider:	Loss of drive to the sensor objects. Loss of drive integrity between motor and hazardous motion.
Fault Exclusion:	If the two objects are mounted separately, the loss of the pulse train may be excluded. Welded contacts or stuck armatures can be excluded with the use of force-guided relays and contactors. Power supply brown out may be excluded if the FGR drop out voltage is higher than the sensor sensing failure.
Safety Principles:	The circuit STOPPED output supplies power when the rotation of the objects approaches zero motion. The STOPPED signal is used in the safety portion of the control circuit to gain access to the safeguarded space when motion has ceased. The MPCE motor starters are not directly part of the safety function as failure to stop does not present a hazardous situation because there will be no access. However, the failure of the N.C. contacts to open when the machine is in motion can cause a failure to reset and this leads to a failure to danger of the sensing circuit. Category 3 requires redundancy (MPCE1, MPCE2). Monitoring both devices is considered best practice. Proximity sensors 1 and 2 each pulse reset their own off-delay timer. When the pulse interval exceeds the timer settings of each timer, their respective relay pulls in, setting each holding circuit. TR3 is to cover timing differences in the timers and to bridge the interval when one FGR is energized but the other is not, as well as the angular difference in sensor trip points. The hazardous motion MPCEs Force-Guided auxiliary contacts drop the holding circuits when the hazard is under power assuring that the timer contacts open and their FGRs drop out during hazard energization, pulling in FGR3 for the next cycle. The pulse train interval allows the relays to have time to cycle between lobes at the last transition. Failure of a sensor to detect the pulse train will be detected by the circuit which requires both timers to cycle for each zero-speed cycle. The failure of any of the timers will be detected by the circuit. On flexible drives, it might not be possible to ensure that there is minimum slippage between the components. Whenever possible, the sensing objects should be mounted on the hazardous motion. The use of individual mounting of both sensors and objects can remove common cause failures. Only one contact per timer is used since electronic timers typically do not contain Force-Guided contacts. By having the timer drive Force-Guided Relays, the timer function can be reliably monitored in the circuit.

9.8.3.3 Dual Proximity Sensors to Timers and Force-Guided Relay Monitored by a SIM (Category 3)



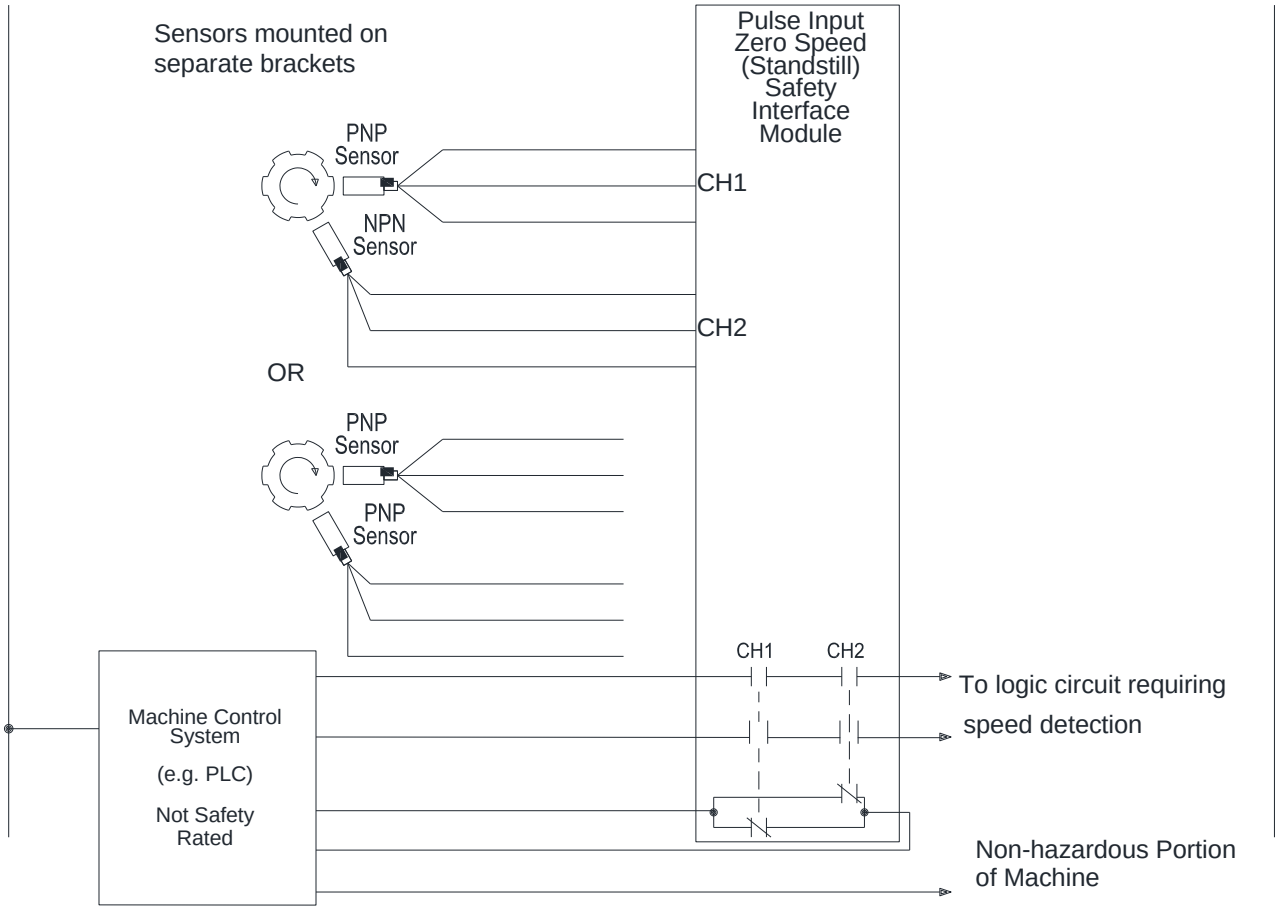
Safety Fxn:	The output of this circuit supplies power when the rotating part of the machine comes to a stop.
Faults to Consider:	Loss of drive to the sensor objects. Loss of drive integrity between motor and hazardous motion.
Fault Exclusion:	If the two objects are mounted separately, the loss of the pulse train may be excluded. Welded contacts or stuck armatures can be excluded with the use of force-guided relays and contactors. Power supply brown out may be excluded if the FGR drop out voltage is higher than the sensor sensing failure.
Safety Principles:	The circuit output goes high when the rotation of the objects has approached zero motion. The STOPPED signal is used in the safety portion of the control circuit to gain access to the safeguarded space when motion has ceased. Proximity sensors 1 and 2 each pulse reset an off-delay timer. When the pulse interval exceeds the off-delay timer settings of each timer, the respective relay pulls in. The hazardous motion MPCEs Force-Guided N.C. auxiliary contacts drop the holding circuits when the hazard is under power assuring that the timer contacts open and their FGRs drop out during hazard energization. The pulse train interval allows the relays to have time to cycle between lobes at the last transition. Failure of a sensor to detect the pulse train will be detected by the circuit which requires both timers to cycle for each zero-speed cycle. The failure of any of the timers will be detected by the circuit. The SIM monitors for single faults in the sensing circuit. The MPCE motor starters are not directly part of the safety function as failure to stop does not present a hazardous situation because there will be no access. However, the failure of the N.C. contacts to open when the machine is in motion can cause a failure to reset and leads to a failure to danger of the sensing circuit. Category 3 requires redundancy (MPCE1, MPCE2). Monitoring both devices is considered best practice. On flexible drives, it might not be possible to ensure that there is minimum slippage between the components. Whenever possible, the sensing objects should be mounted on the hazardous motion. The use of individual mounting of both sensors and objects can remove common cause failures. Only one contact per timer is used since electronic timers typically do not contain Force-Guided contacts. By having the timer drive Force-Guided Relays, the timer function can be reliably monitored in the circuit.

9.8.3.4 Dual Proximity Sensors to Dual Frequency Counters Monitored by a SIM (Category 3)



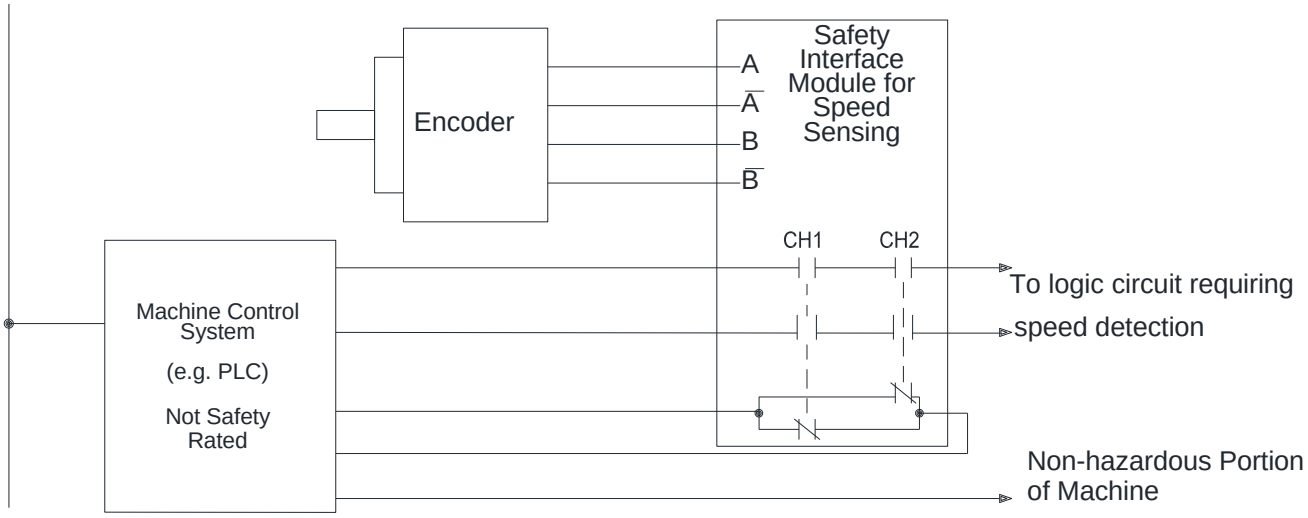
Safety Function:	The output of this circuit supplies power when the rotating part of the machine comes to a stop. Other safety functions monitor the MPCE.
Faults to Consider:	Loss of drive to the sensor pulse train device. Loss of drive integrity between motor and hazardous motion.
Fault Exclusion:	If the two pulse train devices are mounted separately, the loss of the pulse train may be excluded. Welded contacts or stuck armatures can be excluded with the use of force-guided relays and contactors. Power supply brown out may be excluded if the SIM drop out voltage is higher than the sensor sensing failure.
Safety Principles:	The circuit output goes high when the pulse train has approached zero motion as defined by the frequency (Rate) monitor set points. Proximity sensors 1 and 2 each feed an OVERSPEED frequency counter. When the pulse frequency is below the counter settings of each frequency monitor, their respective output contacts are closed. Failure of a sensor to detect the pulse train will be detected by the circuit which requires both timers to cycle for each zero-speed cycle. The failure of any of the timers will be detected by the circuit. The SIM monitors for single faults in the sensing circuit. The STOPPED signal is used in the safety portion of the control circuit to gain access to the safeguarded space when motion has ceased. On flexible drives, it might not be possible to ensure that there is minimum slippage between the components. Whenever possible, the sensing object should be mounted on the hazardous motion. The use of individual mounting of both sensors and objects can remove common cause failures. Take care in setting and monitoring the set points for unauthorized changes as a high frequency set point could enable the circuit “zero” speed output at an unacceptable velocity.

9.8.3.5 Dual Proximity Sensors Plus Zero-speed or Stand Still SIM (Category 3 or 4)



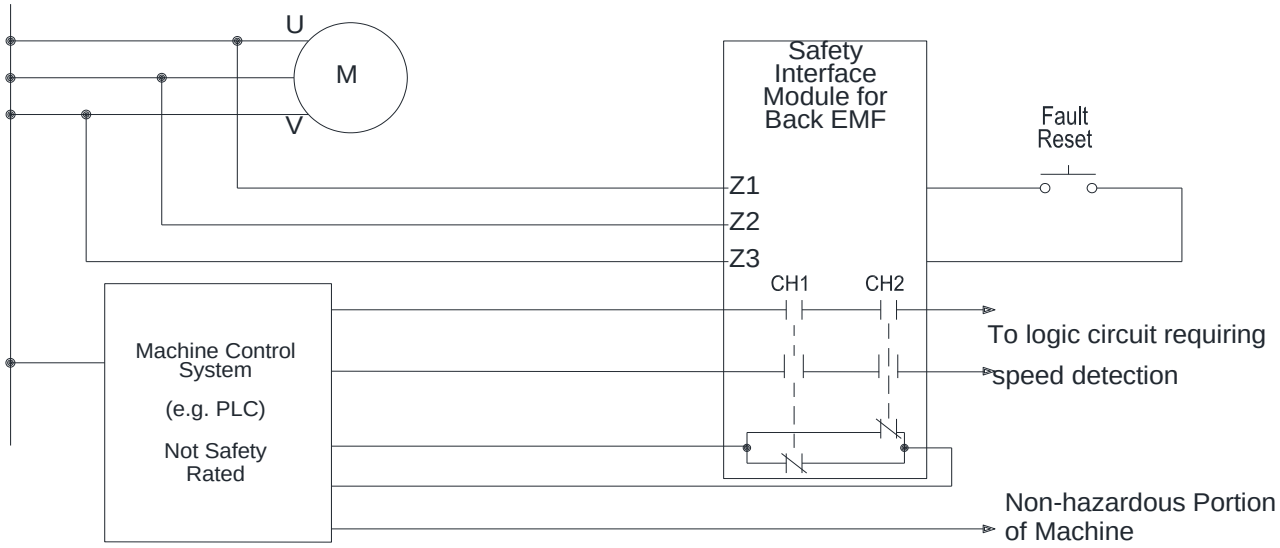
Safety Function:	The output of this circuit supplies power when the rotating part of the machine comes to a stop. Other safety functions monitor the MPCE.
Faults to Consider:	Loss of drive to the sensor pulse train device. Loss of drive integrity between motor and hazardous motion.
Fault Exclusion:	If the two pulse trains are mounted separately, then the loss of pulse train may be excluded. The failure of either of the frequency counters will be detected by the circuit. Power supply brown out may be excluded if the SIM drop out voltage is higher than the sensor sensing failure.
Safety Principles:	The circuit output goes high when the rotation has slowed, and the sensor pulse train frequency drops below the set frequency, indicating acceptable speed. The STOPPED signal is used in the safety portion of the control circuit to gain access to the safeguarded space when motion has ceased. Proximity sensors 1 and 2 each feed pulses into a dual channel Zero-speed (Stand Still) SIM which monitors the sensors and internal faults. The failure of a sensor to detect the pulse train will be detected by the circuit which requires both frequency monitors to sense a low frequency, approaching zero, to obtain an output. Use of the Safety Interface Module ensures that welded contacts or a stuck armature will be detected. On flexible drives, it might not be possible to ensure that there is minimum slippage between the components. Whenever possible, the sensing objects should be mounted on the hazardous motion. The use of individual mounting of both sensors and objects can remove common cause failures. Take care in setting and monitoring the set points for unauthorized changes as a high frequency set point could enable the circuit “zero” speed output at an unacceptable velocity.

9.8.3.6 Encoder Speed Monitoring (Category 3)



Safety Function:	The output of this circuit supplies power when the rotating part of the machine comes to a stop.
Faults to Consider:	Loss of drive to the encoder. Loss of drive integrity between motor and hazardous motion. Failure of the encoder output pulse. If the encoder is also used as the feedback to the drive control, some failure modes will be detected by the drive system. The user evaluates the impact of two devices on the encoder on performance and mean time to failure.
Fault Exclusion:	None to consider.
Safety Principles:	Use of an encoder as input to the encoder speed monitor SIM. The circuit output goes high when the rotation of the encoder has approached zero RPM or when it is below a safe speed. The STOPPED signal is used in the safety portion of the control circuit to gain access to the safeguarded space when motion has ceased. Use of the Safety Interface Module ensures that welded contacts or a stuck armature will be detected. On flexible drives, it might not be possible to ensure that there is minimum slippage between the components. If the encoder is mounted on the motor, belt drives or other non-direct drives, then the encoder might not detect zero-speed.

9.8.3.7 Motor Drive Back EMF Detection (Category 3 or 4)



Safety Function:	The output of this circuit supplies power when the rotating part of the machine comes to a stop. Other safety functions monitor the MPCE.
Faults to Consider:	Loss of drive integrity between motor and hazardous motion. False Zero due to noise induced negative voltage pulses at low drive frequency, especially on voltage reversal sensors.
Fault Exclusion:	If the drive is direct or gear train, the loss of drive integrity may be excluded.
Safety Principles:	The circuit output goes high when the rotation of the drive motor has stopped. Monitor the back EMF of the motor while coasting down. This is done either by monitoring the level of the voltage induced in the open motor windings by the rotor motion during coast down which is inversely proportional to the rotor RPM, or by using the voltage reversal spike generated at rotor stop. The STOPPED signal is used in the safety portion of the control circuit to gain access to the safeguarded space when motion has ceased. On flexible drives, it might not be possible to ensure that there is minimum slippage between the components. Belt drives and other non-direct drives should not be monitored for zero speed in this manner. Back EMF SIMs to be used on variable frequency drives are specifically approved by a statement by the supplier. Use of a unit not suited for Variable Frequency Drive can produce false “zero-speed” at low drive frequencies while the motor is still under power. Use of the Safety Interface Module ensures that welded contacts or a stuck armature will be detected. Manufacturer may have certification for a Category 3 or 4.

9.9 Enabling Devices

9.9.1 Design Requirements

An enabling device is a manually operated control device. The enabling safety function has two parts:

1) when continuously held in the enabled position, the enabling device allows machine operation;
2) when released or depressed beyond the enabled state, the enabling device initiates a stop command or prevents machine operation.

Means shall be provided to activate/deactivate enabling devices.

Informative Note: *Examples of such means include but are not limited to:*

- *special machine mode or cycle that activates the enabling device and requires its use;*
- *key switch;*
- *plugging in an enabling device equipped with a pluggable connector that indicates to the control system that the enabling device is active.*

When more than one person needs to access the hazard area, multiple enabling devices may be required. All active enabling devices shall be required to be actuated to initiate the hazard.

9.9.2 Design Considerations

Enabling devices may be 2 or 3 position style. In the event of an unexpected incident, the 2-position switch is designed to open when released. The 3-position switch provides additional functionality as it is designed to open when either released or when depressed beyond the enabled state.

The design and performance requirements of 3-position switches are established by ANSI B11.19 and IEC 60947-5-8 (see Figure 9). The enabling device has three sequential actuator positions. The contacts are closed when the actuator is in the mid-position (position 2). The contacts are open when the actuator is at rest (position 1) and when fully depressed (position 3). When transitioning from position 3 to position 1, the contacts shall remain open while passing through the middle (enabled) position (position 2). The following design considerations should be applied as part of the design process for the SRP/CS.

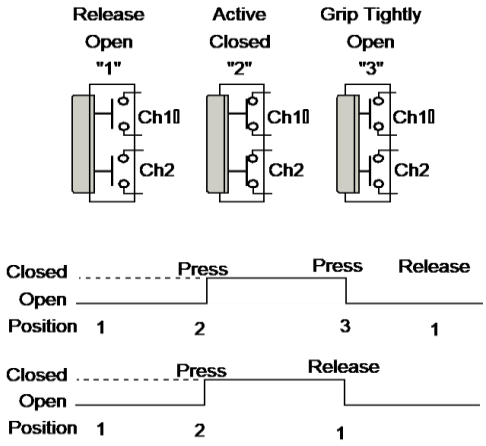


Figure 9: Enabling device contact functions

9.9.2.1 Tampering / Defeat

Tampering or defeat commonly occurs when enabling devices are overly burdensome to operate e.g., – two hands are required for a task while the machine is enabled or a 3-position enabling device is applied where the ergonomics of such a device cause operator fatigue. In some applications, anti-tie-down or plausibility logic may be employed to detect tampering. Partial body and whole body access to the hazard area may require different functionality.

9.9.2.2 Failure Modes

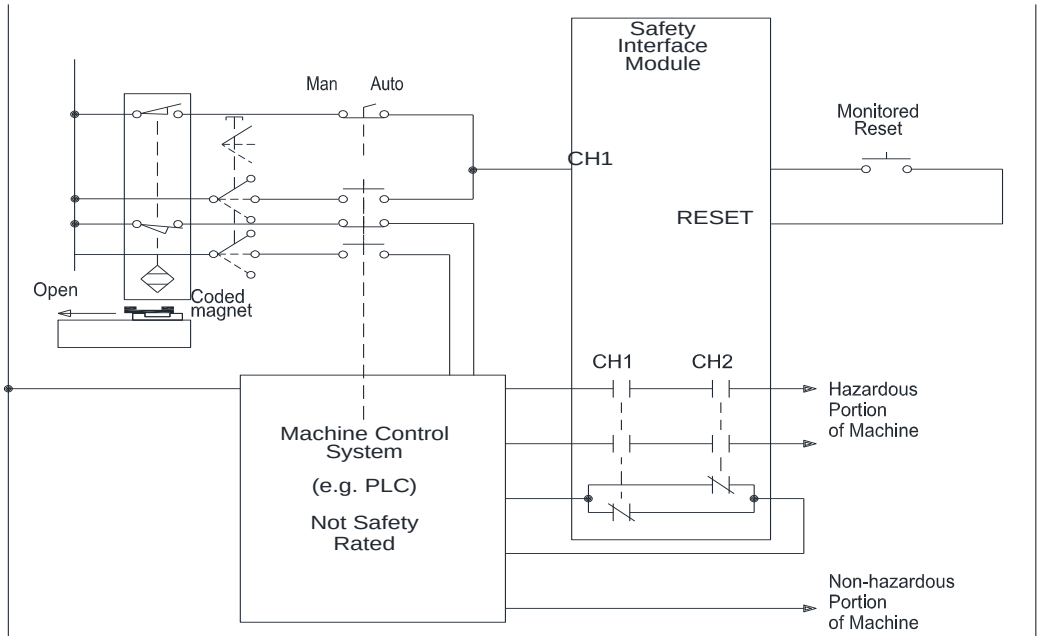
Failure modes specific to enabling devices include but are not limited to:

- broken spring or mechanical seizure that would result in not detecting the release of the enabling control;
- severe contamination or other environmental influences that can cause slow response when released;
- accidental activation of simple button style devices.

9.9.3 Application Examples

9.9.3.1 Non-Contact Interlocked Guard Monitoring – Single Channel w/ a SIM and PES (Category 2)

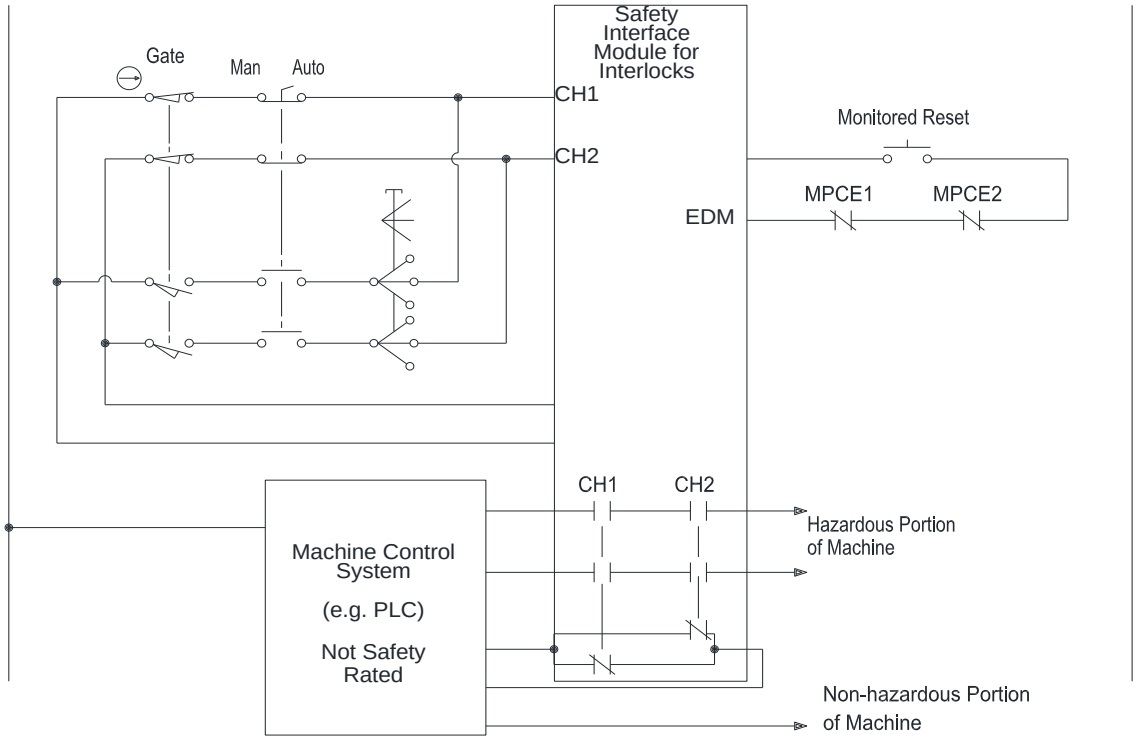
This enabling device allows manual operation of hazard with the use of an enabling device and Jog / Inch control. No monitored reduction of rate of hazardous motion.



Safety Function:	In the manual mode, the hazard may not be initiated unless the enabling device has been operated and held in the center position. The hazardous situation may be enabled when the protected zone guard is closed and the Automatic Mode has been selected, OR the guard is open, Manual Mode has been selected and the enabling device is held in the enable mid-position. When the enabling device is in the mid-position, the manual JOG/INCH button in the control logic may produce motion.
Faults to Consider:	Due to the series connection of guard interlock, mode selector, and enabling device, some failures of the interlock, mode selector, and/or enabling device are not detected. Single faults on the input channel which cannot be detected by the SIM, are masked and/or reset by the off/on cycling of any other device in series with the fault. Unauthorized or unintended manipulation of the programming that effects the monitoring of the non-contact interlocking device and the enabling device.
Fault Exclusion:	Faults related to the interlock device may be excluded as long as the installation and use follows the guidelines detailed in 9.3.3.1.
Safety Principles:	When the guard is opened, the SIM removes power from its output contacts and the hazardous portion of the machine unless the enabling device is being operated while in manual mode. Robust design and testing prior to use may reduce the risk of undetected faults. Alternate protective means, such as enabling device cable length, location of JOG/INCH device may be utilized to further reduce operator exposure. The PES/PLC control system monitors the safety interface module, the guard interlocks and the enabling device. When an error occurs, the control system removes the power to the SIM contacts that feed the hazardous portion of the machine. This circuit has the capability of indicating the state of each individual device, which is accomplished by monitored signals from the second OSSD/interlocking contact of the device. A self-monitoring safety interface module is incorporated that is designed, constructed and certified to meet the expected level of safety performance, which provides protective stop circuits. To achieve Category 2, periodically test the guard interlocking device(s) and the enabling device at suitable intervals.

9.9.3.2 Enabling device with an interlock for manual operation (Category 3)

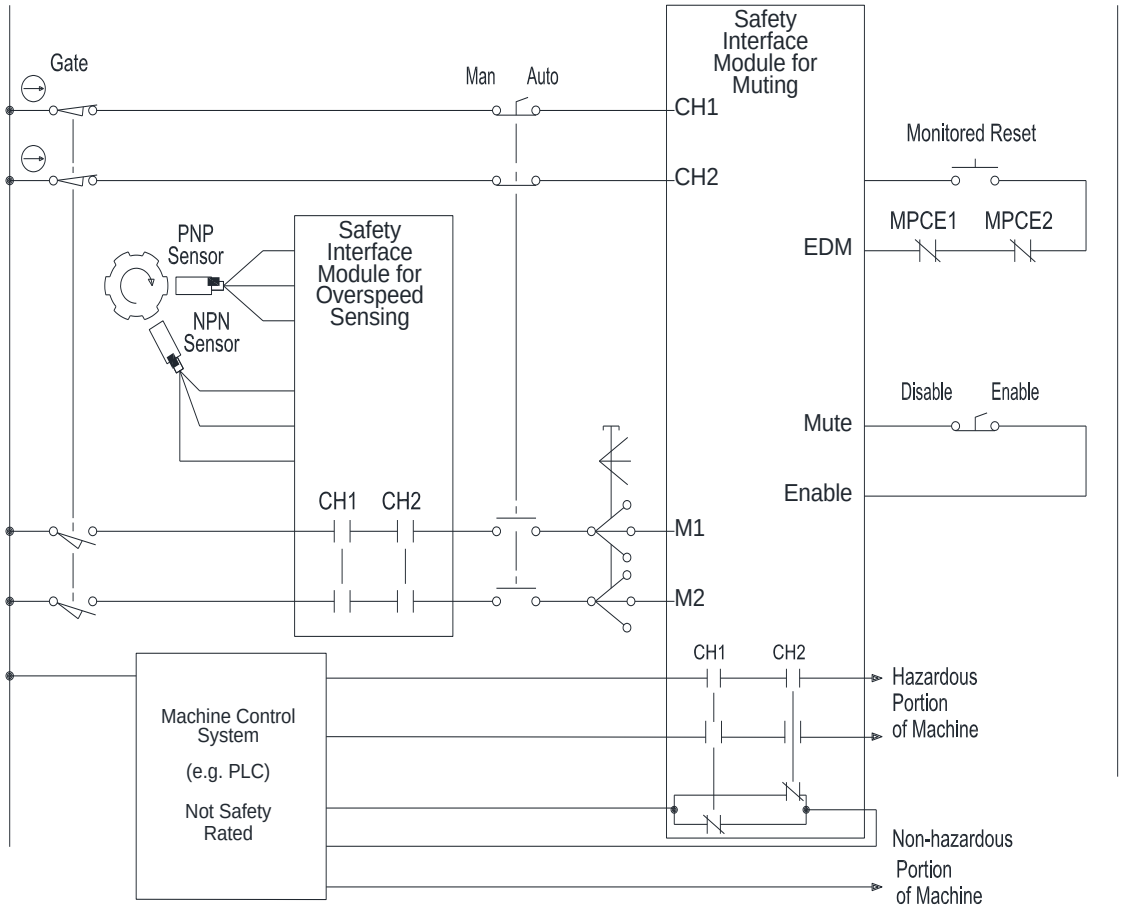
This enabling device allows manual operation of hazard with the use of an enabling device and JOG / INCH control. No monitored reduction of rate of hazardous motion.



Safety Function:	In the manual mode, the hazard may not be initiated unless the enabling device has been operated and held in the center position. The hazardous situation may be enabled when the protected zone guard is closed and the Automatic Mode has been selected, OR the guard is open, Manual Mode has been selected and the enabling device is held in the enable mid-position. When the enabling device is in the mid-position, the manual JOG/INCH button in the control logic may produce motion.
Faults to Consider:	Due to the series connection of guard interlock, mode selector and enabling device, some failures of the guard, mode selector, and/or enabling device are not detected.
Fault Exclusion:	Welded contacts and relay failures can be excluded when force-guided devices are used, and the SIM can monitor for and detect the welded contacts.
Safety Principles:	Robust design and testing prior to use may reduce the risk of undetected faults. Single faults on the input channel, which can be detected by the SIM, are masked and/or reset by the off/on cycling of any other device in series with the fault. Alternate protective means, such as enabling device cable length, location of JOG/INCH device may be utilized to further reduce operator exposure. Category 3 requires redundancy (MPCE1, MPCE2). Monitoring both devices is considered best practice.

9.9.3.3 Enabling Device with Manual/Auto Switch (Category 3)

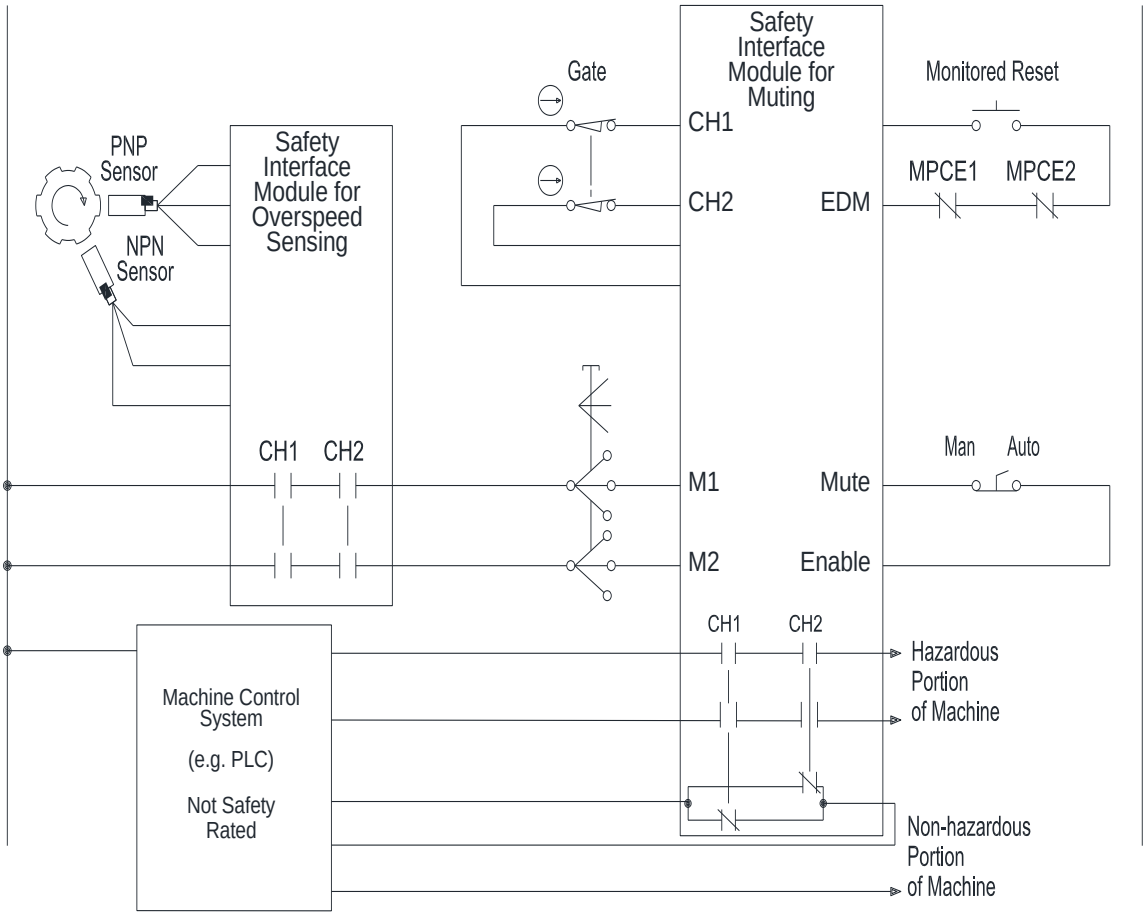
A manual suspension module is used to permit manual operation of an engineering control – device for a reduced speed hazard with the use of an enabling device.



Safety Function:	Manual function is enabled when the protected zone guard is open, and Manual Mode has been selected. When the enabling device is centered, the manual JOG/INCH button may produce motion. The hazardous motion RPM remains below the set point to enable the manual motion.
Faults to Consider:	Due to the series connection of guard interlock and enabling device, some failures of the guard and/or enabling device are not detected. Any of the faults of the zero-speed monitor can enable the JOG/INCH function to an unsafe speed.
Fault Exclusion:	Welded contacts and relay failures can be excluded when force-guided devices are used, and the SIM can monitor for and detect the welded contacts.
Safety Principles:	Robust design and testing prior to use may reduce the risk of undetected faults. Single faults on the input channel, which may be detected by the SIM, are masked and/or reset by the off/on cycling of any other device in series with the fault. Category 3 requires redundancy (MPCE1, MPCE2). Monitoring both devices is considered best practice. Use of speed limiting may help reduce risk by increasing the possibility to escape the hazardous motion and is most commonly used in Manual Mode with enabling devices and JOG/INCH devices. The enabling device is functional only when the hazardous motion is below the value determined by the risk assessment, usually in the range of 250 mm/sec (~10 in/sec) or less. Due to the nature of the hazard, this method is usually used in High/Intermediate to High risk reduction applications.

9.9.3.4 Enabling Device with Manual Suspension Enable (Category 3)

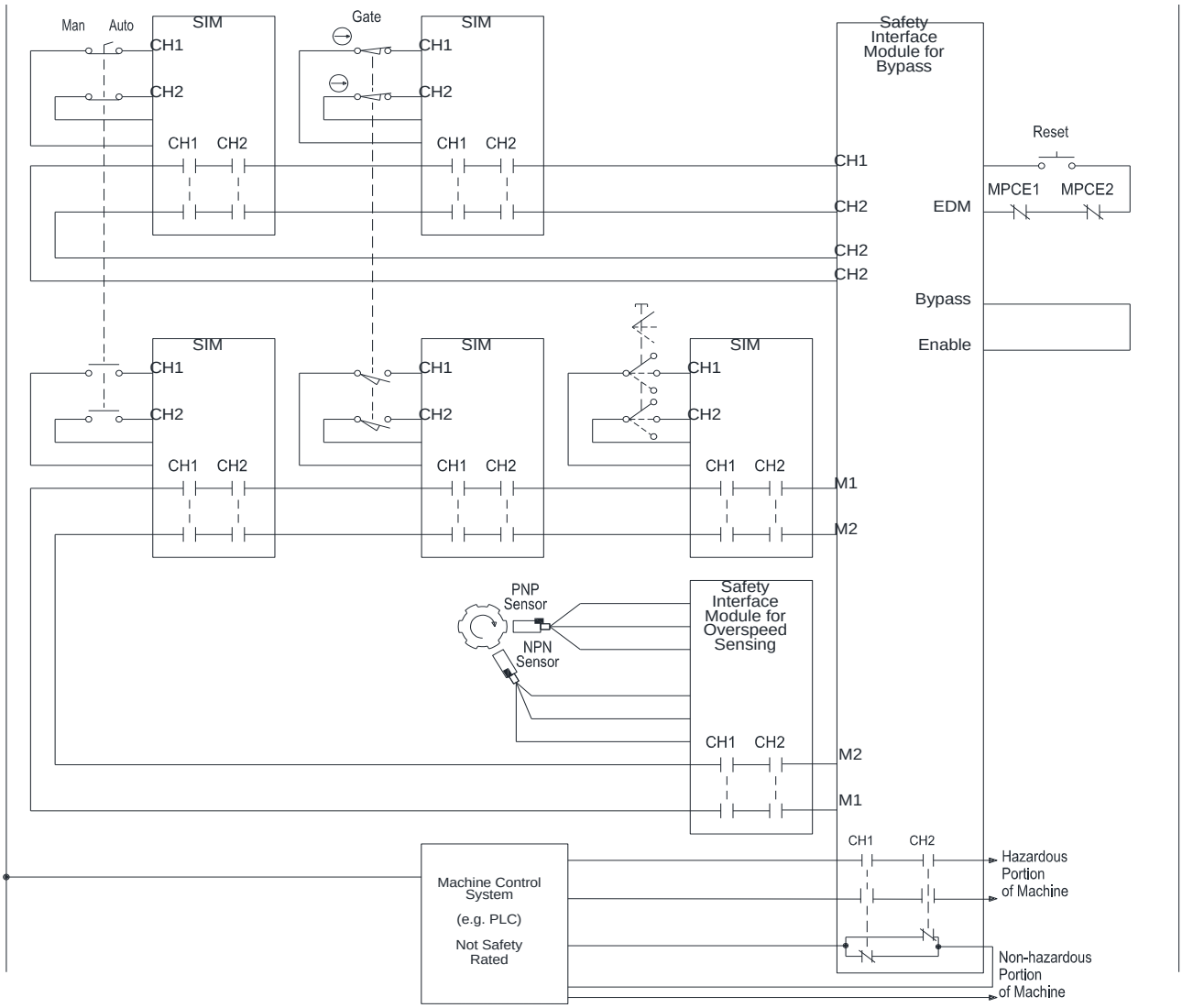
A manual suspension module is used to permit manual operation of an engineering control – device of a reduced speed hazard using an enabling device.



Safety Function:	In manual mode, when the enabling device is centered, the manual JOG/INCH button may produce motion with the partial access door open. The hazardous motion RPM remains below the set point to enable the manual motion.
Faults to Consider:	Due to the series connection of the enabling device some failures are not detected. Change of mode selector from Manual may not inhibit the enable function once initiated. Any of the faults of the zero-speed monitor can enable the JOG/INCH function to an unsafe speed.
Fault Exclusion:	None to consider.
Safety Principles:	Robust design and testing prior to use may reduce the risk of undetected faults. Due to the partial entry construction of the guarding, it is not required for the guard to be open in order to utilize the enabling device Use of the manual suspension module allows limiting the duration of an enable cycle based on module design. Welded contacts and relay failure are detected by the SIM. Category 3 requires redundancy (MPCE1, MPCE2). Monitoring both devices is considered best practice. The manual suspension enabled in Manual Mode is not a safety input but a control input.

9.9.3.5 Enabling Device with Manual Suspension and Reduced Speed (Category 4)

A manual suspension module is used to permit manual operation at a reduced speed with the use of an enabling device. To ensure the highest possibility of detecting a device failure, each device is interfaced with its own SIM. The use of a Category 3 rating of the overspeed SIM would limit the system overall performance level to Category 3.



Safety Function:	Manual function is enabled when the door of the whole body access guard is open, and Manual Mode has been selected. When the enabling device is centered, a manual JOG/INCH button may produce motion. The hazardous motion RPM shall remain below set point to enable the manual motion.
Faults to Consider:	The system performance is limited in the Manual Mode by the performance of the Over-Speed SIM. Performance in the Automatic Mode has not been compromised and is considered high risk reduction. Any of the faults of the zero-speed monitor can enable the JOG/INCH function to an unsafe speed.
Fault Exclusion:	Welded contacts and relay failures can be excluded when force-guided devices are used, and the SIM can monitor for and detect the welded contacts.
Safety Principles:	Use of the manual suspension module allows limiting the duration of an enable cycle based on module design. Category 4 requires redundancy and monitoring of both MPCEs is required. Detection of failure modes of individual devices has not been compromised by the addition of series connected contacts in the SIM input channels. A manual reset is used to prevent semi-automatic hunting around the maximum speed.

10 Design Requirements - Logic Devices

10.1 General

Logic devices provide the relationship between the inputs and outputs of the SRP/CS, and they also monitor for faults.

The logic circuits may use designs incorporating discrete component logic, Safety Interface Modules (SIMs), or Safety Programmable Electronic System (SPES).

Informative Note: *While the examples shown in this standard make use of SIMS to provide logic and monitoring functions, properly applied and rated PES can also be utilized. See ISO 13849-1 and ANSI B11.TR4 for additional information on the software requirements for such systems.*

10.1.1 Design Requirements

When used as part of the SRP/CS, safe logic devices shall provide a level of reliability commensurate with the requirement determined in 5.4.

Where the logic device carries a safety performance rating, the rating shall not be lower than the requirement determined in 5.3.

10.1.2 Design Considerations

The following design considerations (10.1.2.1 through 10.1.2.4) should be applied as part of the design process for the SRP/CS.

10.1.2.1 Safety Interface Module General Information

A Safety Interface Module (also known as a *Safety Relay*) is a combination of individual components that provides a safety-related function(s) in a distinct system. Some of the safety-related functions provided include, but are not limited to:

- protective stop;
- emergency stop;
- guard interlocking;
- presence sensing device interface;
- safe speed monitoring / zero speed monitoring;
- safe timing;
- two-hand control;
- limited inch/jog.

Safety Interface modules also provide additional functionality including diagnostics and monitoring, and can include but not be limited to:

- auxiliary (non-safety) outputs;
- monitored manual reset functions;
- self-monitoring for internal faults;
- input channel monitoring (for short circuits or proper function);
- external device monitoring.

Input device examples in this standard that use SIMs assume that the rated performance level of the SIM is equal to or greater than the Category shown in the subclause heading.

The term “Safety Relay” is sometimes used to describe Safety Interface Modules. This term is also used to refer to individual Force-Guided Relays. The user is cautioned not to confuse the functional capabilities of each.

Informative Note: *See EN 61810-1:2015 for other guidance on design of Force-Guided Relays.*

10.1.2.2 Tampering / Defeat

The most common means of tampering with logic devices is tie-down of the reset function. Refer to 10.1.2.4 for methods to reduce the risk of reset tampering.

The typical mounting location of logic devices within the control enclosure can significantly reduce the risk of tampering with wiring or configuration settings.

10.1.2.3 Failure Modes

Failure modes specific to safety interface modules include but are not limited to:

- damage to output contacts caused by overcurrent (follow supplier's specifications for loading and overcurrent protection);
- damage to output contacts caused by inductive transients (follow good design practice for Transient Voltage Surge Suppression (TVSS) on loads driven by safe logic devices);
- software/configuration errors on programmable devices (SPES).

10.1.2.4 Reset Function of the Safety Circuit

The reset function shall not initiate hazardous machine motion or operation. The reset function may be automatic, manual or monitored manual.

The reset function of the safety circuit is included when determining the reliability (performance) provided by a circuit.

Automatic reset does not require human intervention to execute the reset function. Non-Monitored manual reset allows human intervention, however, a short or a tie-down of the reset device can cause an unintended reset.

Monitored manual reset requires human intervention such that a shorted or tied down reset device may not cause a reset (e.g., open-close-open action).

Automatic reset may be used in situations where an individual is continually detected by an engineering control – device or the reset function is provided by some other portion of the safety-related machine control.

Manual reset shall be used in situations where an individual can pass through an engineering control – device and is no longer detected, or the reset function is required to prevent hazardous situations. Manual reset without monitoring may be used when lower levels of reliability are appropriate.

In the presence of a failure, the user shall be responsible to be certain that repetitive manual reset of the system or device is not used for production operation.

Informative Note 1: *The diagrams shown within this document typically show the reset function as a manual reset, but this is not intended to be an absolute requirement depending upon the application.*

Informative Note 2: *For more detailed information on reset, see also ANSI B11.19.*

10.2 Software and Programming

10.2.1 General

The SRP/CS may contain software as a part of a machine controller, a separate external system, or a combination of multiple methodologies. The requirements of 10.2 shall be used for specifying, developing, and verifying application software intended for safety applications.

Machine safety-related application software (SRASW) may include, but is not limited to:

- predefined functions of an external safety-rated controller (e.g., safety function blocks);
- safety features of the specific systems (i.e., safety-rated soft axis on robots);
- safety features of machines (i.e., safe motion).

SRASW may also be known as limited variability language (LVL). It may be expressed as a pre-defined function block which contains the logic sequence, limits, and expressions for entered input and output information.

Informative Note 1: *See also, ISO 13849-1 or IEC 62061.*

Informative Note 2: *Use of Performance Level methodology for SRASW should conform to the requirements of 7.4 in ISO 13849-1.*

SRASW programming shall be performed by qualified personnel proficient in the safety programmable controller being used and the proper implementation of its function blocks.

10.2.2 Software Safety Requirements Specifications (SSRS)

The SSRS describes the required reliability of the software aspect for the safety function and defines its objective.

In creating the SSRS, the following factors at a minimum shall be considered:

- which input(s) triggers which output(s);
- the required reliability of the software aspect for each safety function;
- response time of the software aspect of the safety function;
- conditions under which the safety function is manually suspended through software;
- the requirement has captured the right information;
- writing the SSRS using plain language instead of technical language to ensure it is understandable.

10.2.3 Components

10.2.3.1 Inputs

Safety-rated input modules or devices shall be used for inputs that are part of the safety function and shall be wired or installed according to manufacturer specifications. This includes hard-wired inputs or networked inputs.

10.2.3.2 Logic

Safety-rated programmable controllers shall be used for logic solvers that are part of the safety function.

Where SRASW and non-SRASW are combined in one component:

- SRASW and non-SRASW shall be coded in different function blocks with well-defined interfaces;
- there shall be no logical combination of non safety-related and safety-related data which can lead to downgrading of the integrity of safety-related signals. For example, combining safety-related and non safety-related signals by a logical “OR” where the result controls safety-related signals.

10.2.3.3 Outputs

Safety-rated output modules or devices shall be used for outputs that are part of the safety function and shall be wired or installed according to manufacturer specifications. This includes hard-wired outputs or networked outputs.

10.2.4 Structure

Programs should be sequenced in a logical order. Inputs should be processed, logic applied using the inputs, then outputs executed/triggered. Processing data in other sequences can adversely affect reaction time, which may affect the safety distance calculation.

Variables describing the safety-rated I/O and used as part of the certified safety functions shall be dedicated safety variables. Variables should be labeled in an understandable manner. For example, the format may include, but is not limited to:

- function (i.e., input or output);
- device type or name;
- location (i.e., node, controller).

Non-safety I/O variables shall not be used as safety variables when their manipulation will compromise the safety function (variables in non-safety I/O can be forced with minimal security and can facilitate unauthorized changes of the safety function).

Non-safety variables used in the safety-related application software should be limited to safety devices for diagnostics and the reset device. They should have unique names in the safety and standard controller.

Non-safety variables may be known as “exposed variables.”

10.2.5 Programming

The SRASW program shall be readable, understandable, testable, and maintainable. SRASW programming should begin after the following information has been reviewed:

- industry standards relevant to the application: (i.e., ANSI B11.0, ANSI B11.19);
- requirements, recommendations, or guidelines from the component manufacturer;
- Safety Requirement Specification: the description of all safety functions;
- end-user/machine supplier programming specifications (if applicable).

Certified safety function blocks shall be used for their intended application when provided for use with the safety-rated controller. A Safety function block is considered certified if it has been evaluated per relevant standard(s) and approved by an independent third-party organization such as a Nationally Recognized Testing Laboratory (NRTL). User-created logic may be considered after confirming that certified safety function blocks for the application do not exist. Modifying certified safety function block code invalidates the certification.

SRASW design shall:

- use modular and structured programming to enable ease of reading and testing;
- execute code inside function block with only one entry and one exit point;
- use techniques for detection and control of hardware failure and for defensive programming within input, processing and output blocks which lead to safe state;
- assign a safety output at only one program location.
  Informative Note: *Under certain circumstances, it may be permissible to assign a safety output at more than one program location.*

10.2.6 Software validation

SRASW, including any modifications, shall be validated as part of the safety function validation (see clause 12).

Informative Note: *Additional information on validating SRASW can be found in ISO 13849-2 and IEC 62061.*

After validation is completed, the safety-related programmable controller shall be locked, signed, or password protected to prevent unauthorized changes and the checksum, signature, or other equivalent value shall be recorded as the final state of the SRASW.

Changes to the SRASW shall follow the requirements regarding change management (see clause 13).

10.2.7 Cybersecurity

Failure modes from cybersecurity risks shall be identified and addressed according to ANSI B11.0.

Informative Note: *For information and requirements about cybersecurity, see (ANSI) B11.TR9.*

Methods shall be in place to monitor for necessary firmware updates that address safety or cybersecurity vulnerabilities. Implementation of these updates shall take place as soon as reasonably practicable.

10.2.8 Remote access

SRASW shall not be modifiable by remote access unless the local validation of the safety function is performed.

If a machine is capable of remote access (remotely controlled by personnel who are physically away from the machine), the following requirements shall be fulfilled:

a) remote changes shall not override local selection and cause any local hazardous situation(s);
b) loss of connection of the remote access shall not cause a hazardous situation(s);
c) remote changes to safety-related parameters shall not be possible without local action to confirm the acceptability of the change and that the change(s) does not create any hazardous situations.

11 Design Requirements – Output Devices (MPCE)

Where the logic devices in the SRP/CS do not directly control the hazard, a supplemental device shall be used. Such devices include, but are not limited to relays, contactors, and fluid power valves. This supplemental device that directly controls the hazard is referred to in this document as the Machine Primary Control Element (MPCE).

Informative Note: *Devices such as SIMs are typically limited in switching capacity to less than 10 amps and 230 VAC. In addition, many potentially hazardous motions are generated by fluid power actuators such as cylinders and fluid motors and must be controlled by fluid power valves acting as a part of the SRP/CS.*

11.1 Relays and Contactors

11.1.1 Design Requirements

Where monitoring of relays/contactors is required to achieve the required level of circuit reliability, the monitoring contacts shall be force guided.

11.1.2 Design Considerations

The following design considerations (11.1.2.1 – 11.1.2.2) should be applied as part of the design process for the SRP/CS.

11.1.2.1 Tampering / Defeat

The most common means of tampering with MPCE relays and contactors is manual manipulation of the override plunger on the device. The typical mounting location within the control enclosure can significantly reduce the risk of manipulation, however some suppliers also offer devices with tamper resistant covers or no override function.

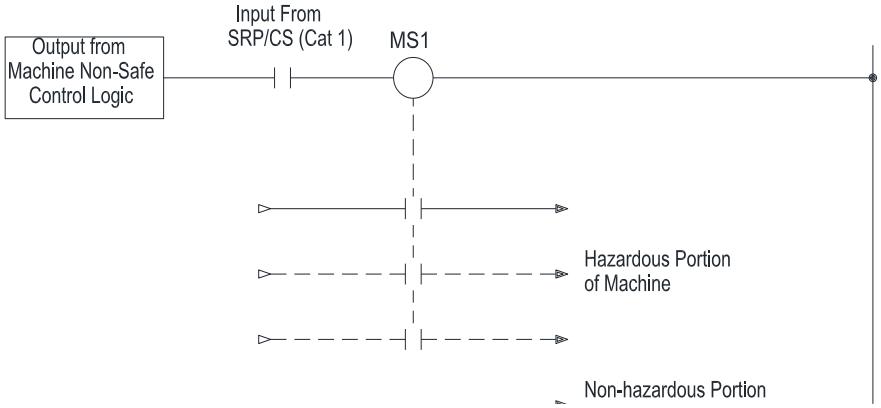
11.1.2.2 Failure Modes

Failure modes specific to relays and contactors include but are not limited to:

- welding of contacts;
- sticking of mechanisms/magnets preventing opening of circuit(s).

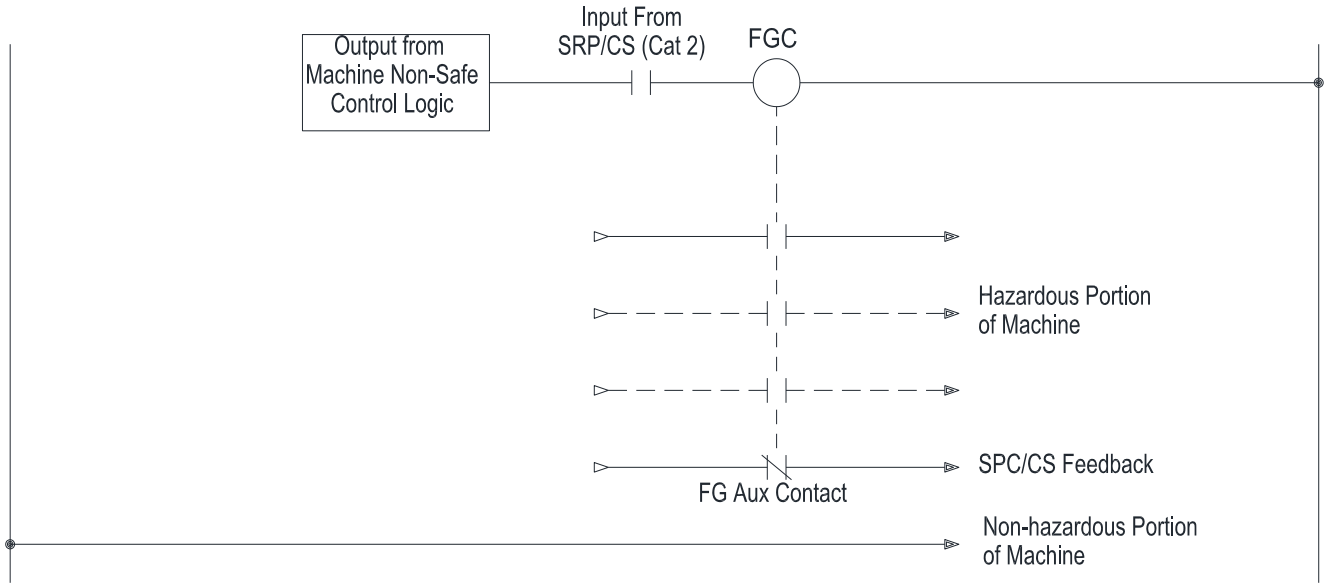
11.1.3 Application Examples

11.1.3.1 Contactor (Category 1)



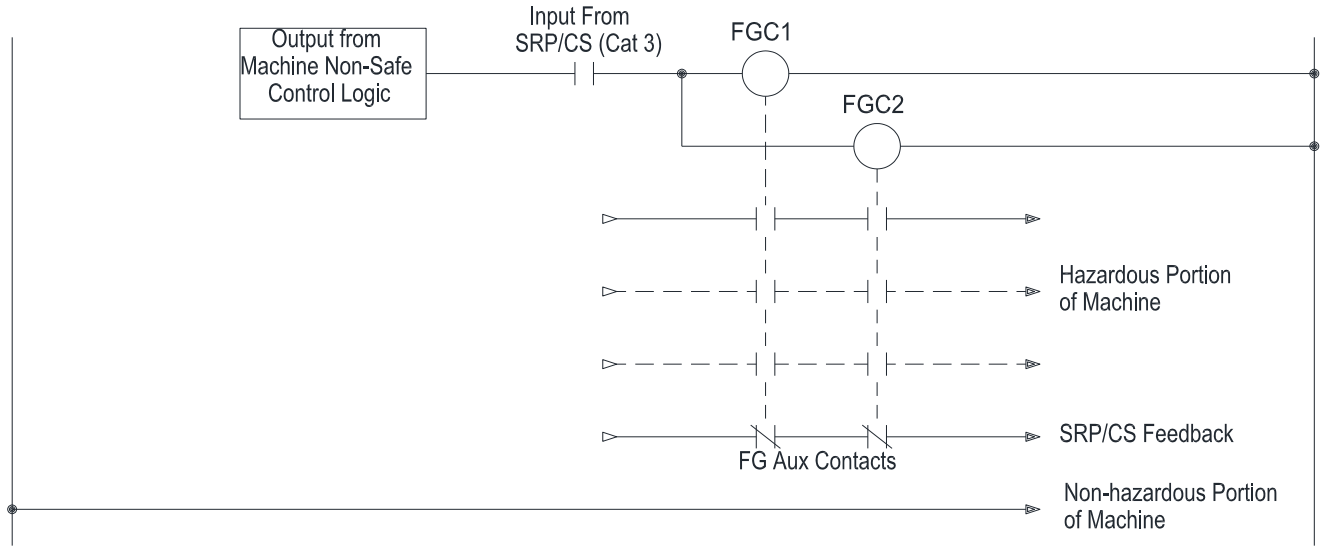
Safety Function:	When the input from the SRP/CS goes low, the MS1 contactor drops and power to the hazardous portion of the machine is removed.
Faults to Consider:	Failure of the armature to drop due to jamming, residual magnetism or worn/broken springs. Welded contacts fail to disconnect all load connections. Short of the contactor coil wire to another power source.
Fault Exclusion:	None to consider.
Safety Principles:	Proper installation (e.g., gravity dependent devices). The mean time between failures can be extended by correct load design and proper over current protection. Contacts should be inspected at a regular interval. The contactor should be replaced when approaching their cycle life expectancy. Shorting of the coil wire to another power source may be excluded if the SRP/CS source and the contactor are in the same cabinet, or precautions taken to prevent such a short through isolation of the wire example; in separate conduit on a remotely located contactor.

11.1.3.2 Force-Guided Contactor (Category 2)



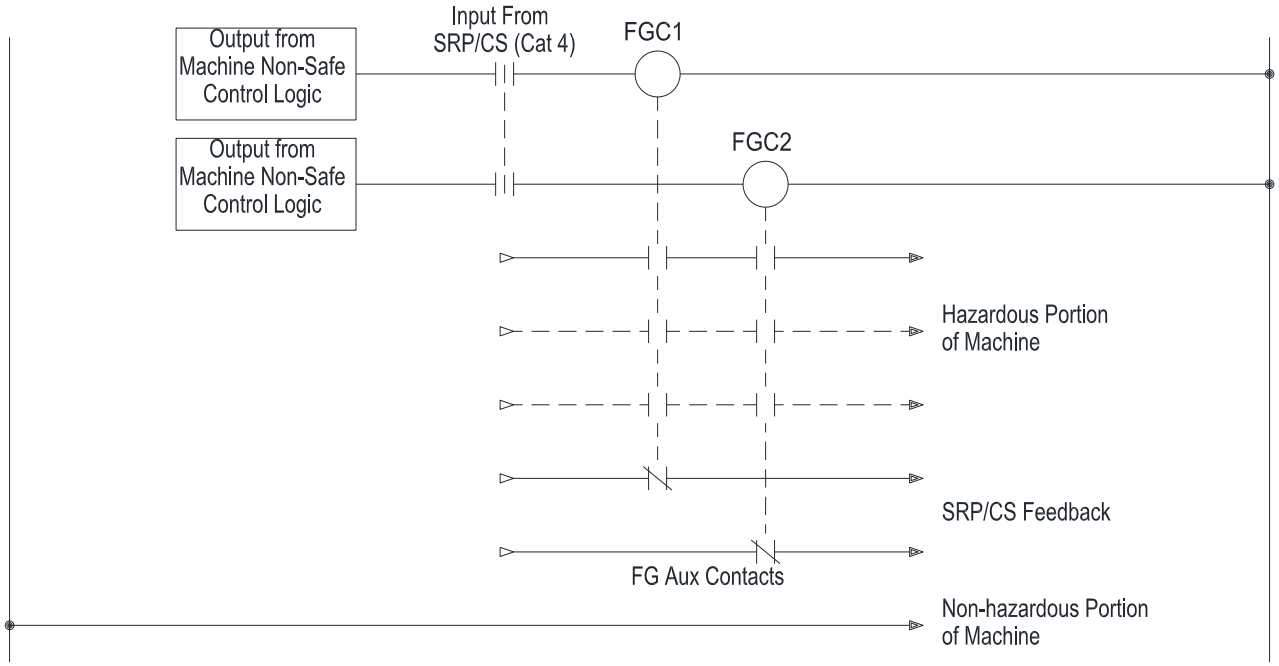
Safety Function:	When the input from the SRP/CS goes low, the contactor drops and power to the hazardous portion of the machine is removed.
Faults to Consider:	Shorting of the feed wire to another source of power will prevent the contactor from dropping. Shorting of the feedback auxiliary contact to another power source.
Fault Exclusion:	Welded contacts failing to disconnect all load connections can be excluded through the over-dimensioning of contact rating.
Safety Principle:	Proper installation (e.g., gravity dependent devices). The mean time between failures can be extended by correct load design and proper over current protection. Contacts should be inspected at a regular interval. The contactor should be replaced when approaching their cycle life expectancy. Shorting of the coil wire to another power source may be excluded if the SRP/CS source and the contactor are in the same cabinet, or precautions taken to prevent such a short through isolation of the wire example; in separate conduit on a remotely located contactor. The auxiliary contact may be used as input to a warning or separate shut down if the contactor does not drop as expected. Failure of the armature to drop due to jamming, residual magnetism or worn/broken springs failing to disconnect all load connections can be detected through the use of the Force-Guided auxiliary contact as feedback to the SRP/CS, preventing re-energization of another hazardous cycle.

11.1.3.3 Dual Force-Guided Contactor (Category 3)



Safety Function:	When the inputs from the SRP/CS go low, power to the hazardous portion of the machine is removed. ***Informative Note:*** *This "single" contact shown in the diagram is for simplification of the drawing only. As it is noted as a Cat 3 input, it must meet the typical requirements of that circuit architecture.*
Faults to Consider:	Since the contacts to the load are in series, over current damage during one run cycle is a common cause failure mode which could cause simultaneous welded contact failure.
Fault Exclusion:	Welded contacts failing to disconnect all load connections can be excluded through the over-dimensioning of contact rating. Failure of both coils to drop due to a short to another power source can be excluded when two channel supply, one per coil is used. The common coil connection to the SRP/CS as shown in the diagram may be excluded as this type of fault is made in the same cabinet
Safety Principles:	Contacts from dual contactors in series with the hazardous portion of the machine increase the probability of a hazard disconnect. If one contactor fails to disconnect the hazard's power, the other contactor will. Conservative fusing and contactor sizing can reduce the probability of damage to both contactors during the same overload or load short. Proper installation (e.g., gravity dependent devices). Overload-protect the power to the hazard and conservatively size the contactor to prevent common cause failures of welded contacts due to over current in the same stop cycle. Category 3 requires redundancy (MPCE1, MPCE2). Monitoring both devices is considered best practice. The type of failures in the feedback from the MPCE which may be detected is a function of the SIM's design. Some monitoring of the cycling of the inputs, or the concurrent state of the two feedback channels. Those SIMs which only monitor the presence of voltage might not detect certain faults such as a short to another power source even though dual channel feedback is used. For full advantage of the cycling monitoring the auxiliary contacts should NOT be connected in series as this presents a point of common failure. Use of continuity instead of a power source feedback SIM may eliminate false feedback signals due to shorting to another source of power. The single source failure mode of common wiring of coils and feedback may be excluded when the SRP/CS source and monitoring are in the same cabinet and in close proximity to the MPCE. If this is not the case, take special precautions to prevent shorting of these wires to a second power source, such as separate conduit(s) or sourcing each FGR from a separate SRP/CS contact.

11.1.3.4 Dual Force-Guided Contactor (Category 4)



Safety Function:	When the inputs from the SRP/CS go low, power to the hazardous portion of the machine is removed.
Faults to Consider:	Since the contacts to the load are in series, over current damage during one run cycle is a common cause failure mode which could cause simultaneous welded contact failure.
Fault Exclusion:	Welded contacts failing to disconnect all load connections can be excluded through the over-dimensioning of contact rating. Failure of both coils to drop due to a short to another power source can be excluded by use of two channel supply, one per coil (fault exclusion based on location in the same cabinet is also possible).
Safety Principles:	Contacts from dual contactors in series with the hazardous portion of the machine increase the probability of a hazard disconnect. If one contactor fails to disconnect the hazard's power, the other contactor will. Proper installation (e.g., gravity dependent devices). Overload-protect power to the hazard and conservatively size the contactor to prevent common cause failures of welded contacts due to over current in the same stop cycle. The type of failures in the feedback from the MPCE which may be detected is a function of the SIMs design. Some monitoring of the cycling of the inputs, or the concurrent state of the two feedback channels. Those SIMs which only monitor the presence of voltage might not detect certain faults such as short to another power source even though dual channel feedback is used. Use of individual auxiliary contact feedback rather than series, eliminate one point of common cause failure.

11.2 Power Drive Systems for Safe Torque Off

This section covers the use of Variable Frequency Drives or other drive systems related to rotational or linear motor power.

11.2.1 Design Considerations

The following design considerations should be applied as part of the design process for the SRP/CS.

11.2.1.1 General Information

Power drive systems rated for safety applications, PDS (SR), may be used as an alternative to contactors to remove power from motors to achieve safety functions.

Informative Note: *IEC 61800-5-2 describes a set of safety functions and sets out the design, development, integration and validation requirements for drives to achieve a safety rating that meets the requirements of IEC 61508. The safety functions set out in IEC 61800-5-2 are listed below. For the purposes of this standard, only Safe Torque Off is considered, as this standard does not consider programmable devices. The example circuits in this standard achieve Safe Torque Off by hardware signals only.*

- *Safe Torque Off: Rotational or linear motor power is not applied or is removed; a Category 0 Stop.*
- *Safe Stop 1: Controls and monitors the motor deceleration rate within set limits to stop the motor, then executes the Safe Torque Off function; a Category 1 Stop.*
- *Safe Stop 2: Controls and monitors the motor deceleration rate within set limits to stop the motor and then executes the Safe Operating Stop function; a Category 2 Stop.*
- *Safe Operating Stop: Power is used to hold motor in a stopped condition. Mechanical brakes may not be needed.*
- *Safely Limited Speed: Prevents the motor from exceeding the specified speed limit.*
- *Safely Limited Torque: Prevents the motor from exceeding the specified torque or linear force limit.*
- *Safely Limited Position: Prevents the motor shaft from exceeding the specified position limit(s).*
- *Safely Limited Increment: Prevents the motor shaft from exceeding the specified increment – a jog.*
- *Safe Direction: Ensures that the motor shaft can move only in the specified direction.*
- *Safe Motor Temperature: Prevents the motor temperature from exceeding a specified limit.*
- *Safe Brake Control: Provides a safe output signal to control an external brake.*
- *Safe Cam: Provides a safe output signal to indicate whether the motor shaft position is within a specified range.*
- *Safe Speed Monitor: Provides a safe output signal to indicate whether the motor speed is below a specified limit.*

For the purpose of this standard, the operation of the drive is as follows. Drives from various suppliers may operate differently than described here. Two block diagrams are used: one for standard rated drives and one for safety-rated drives (see Figure 10). For both types of drives, pressing the Stop button initiates a programmed deceleration of the motor to a stop condition with power remaining available to the motor. This is a Category 2 stop. This deceleration is not safety-rated.

For the standard drive, opening the enable signal executes a coast-to-stop. This coast-to-stop does not meet the requirements of a Category 0 stop as power is still available at the output drive transistors.

Safety-rated drives, often referred to as “Safe Stand Still” or “Safe Torque Off” drives are typically offered with a safety Category rating. The safety-rated drive has additional high integrity circuitry that inhibits modulation of the power transistors. Some drive designs may have two external safety-related signals (Ch1 and Ch2), while others use only one channel. A monitoring signal may be used to indicate that the High Integrity Disable is active. At the time of publication of this standard, these drives are typically rated as Category 3.

The Start and Stop signals are usually not part of the safety-related portion of the control system but are used in normal stopping as well as to provide an orderly shutdown or deceleration stop prior to the protective stop signal being issued. See NFPA 79.

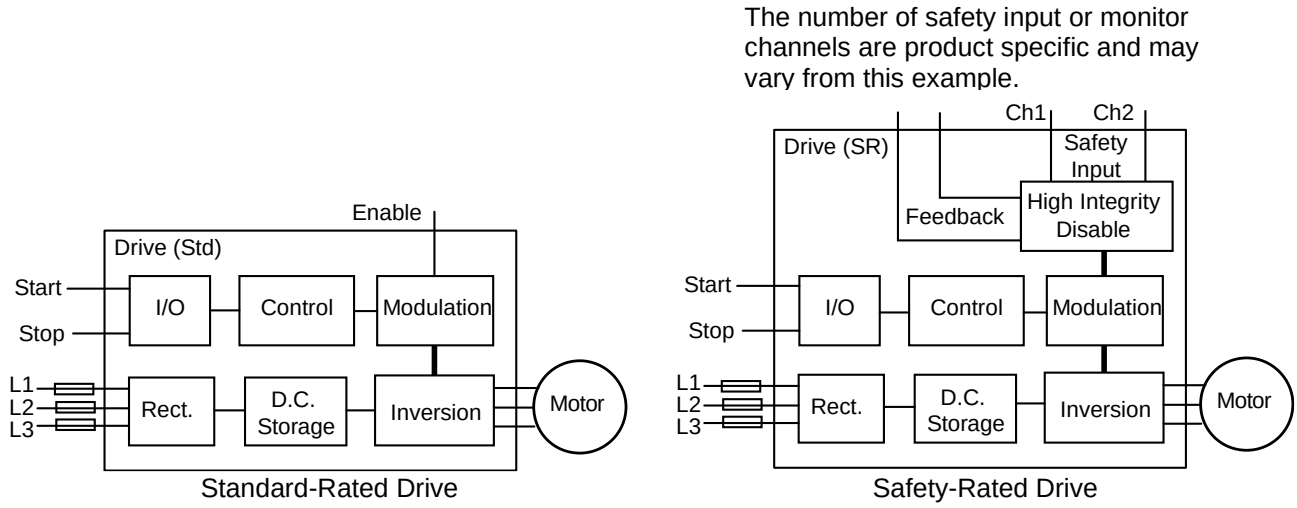
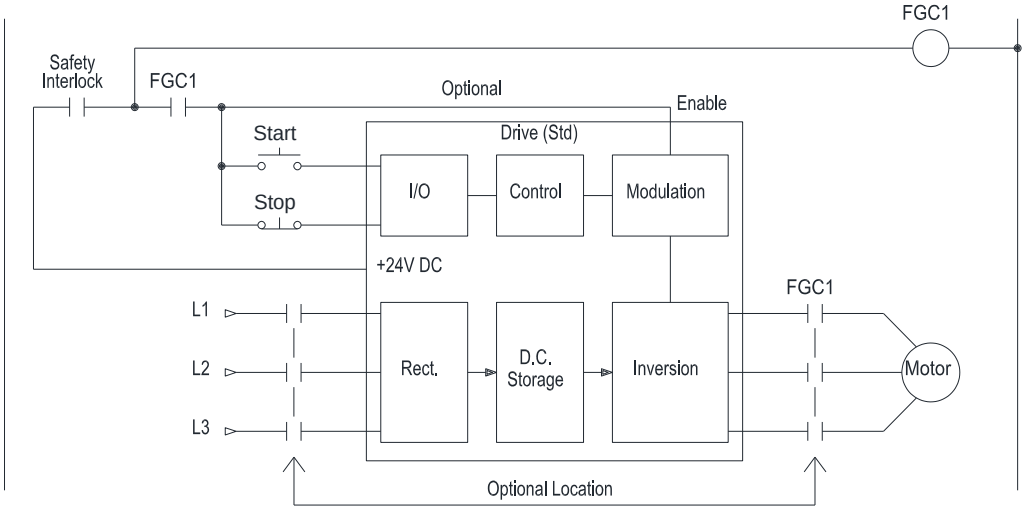


Figure 10: Drive comparison

For this subclause of the standard, only the motor drive and a generic start/stop connection are shown. If the motor control signal is part of the safety-related portion of the control system, its functionality may be chosen from the many examples in the previous clauses. The input and logic elements together with the drive design will determine the performance of the safety-related portion of the control system.

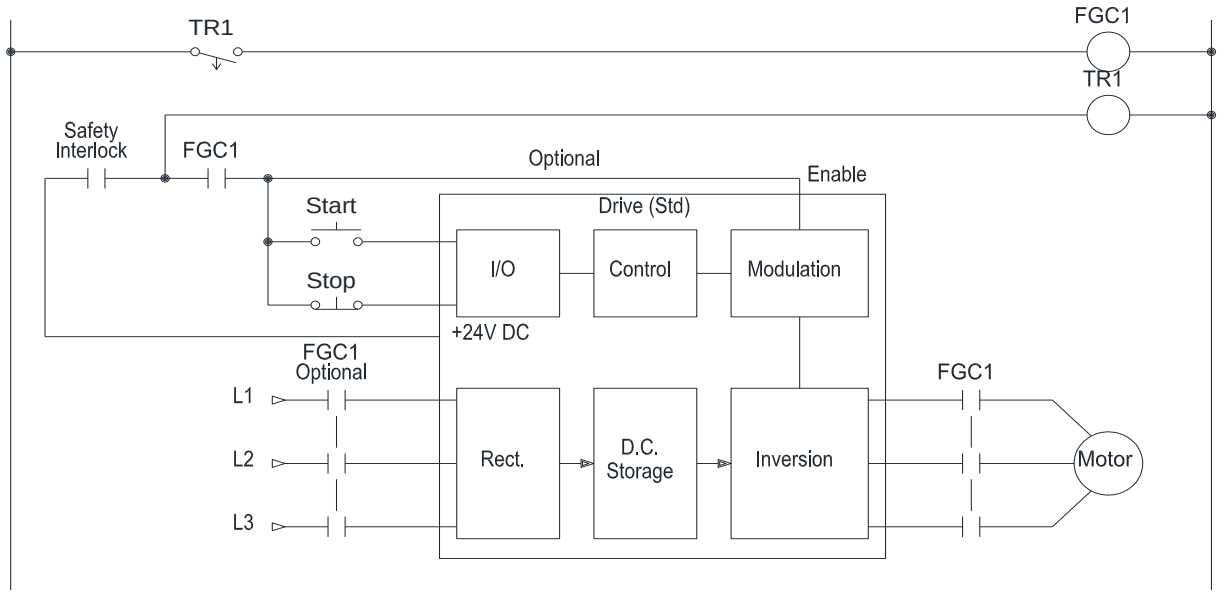
11.2.2 Application Examples

11.2.2.1 Single Channel Interlock Functional Stop Category 0 (per NFPA 79) of an AC Motor using Standard Rated AC Drive (Category 1)



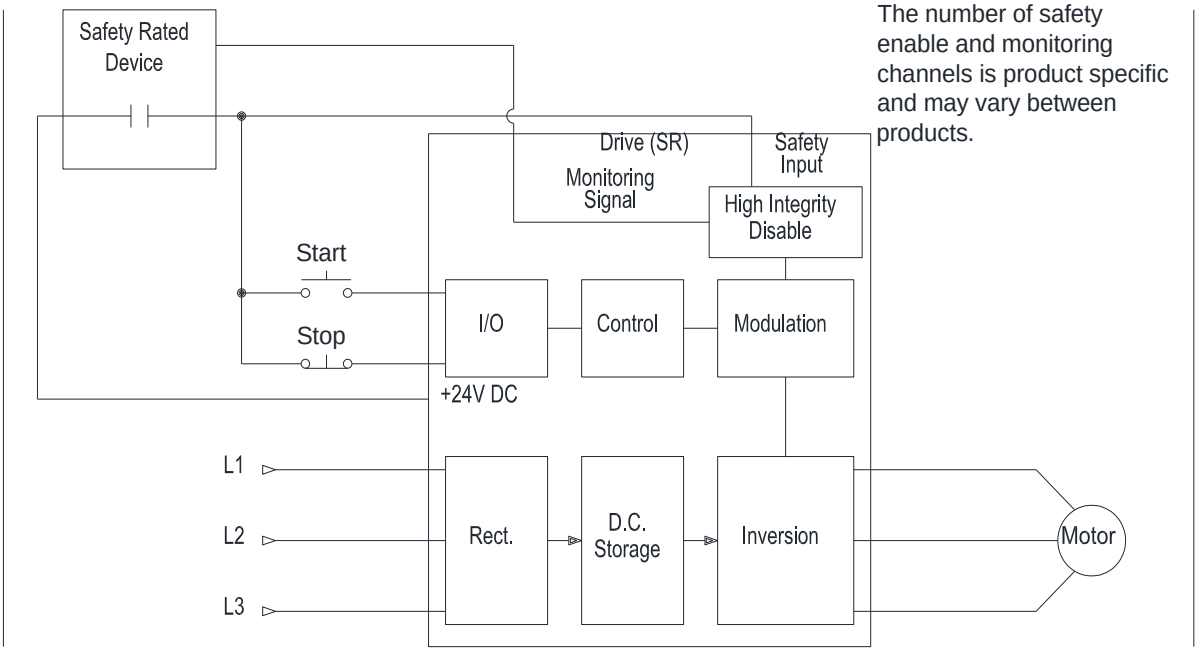
Safety Fxn:	When the safety interlock control goes low, the drive coasts to a stop with zero torque.
Faults to Consider:	The drive for this application is considered as a single solid-state device with a single point of failure. Wiring fault (short) to 24V DC at the safety interlock will keep the drive enabled and cause the contactor to remain energized. The contactor can weld or remain stuck in the closed state, failing to isolate the motor from the drive.
Fault Exclusion:	None to consider
Safety Principles:	The drive is stopped by both the logic input and disabling of the Enable line. The latter forces all output transistors to shut off immediately. The motor is disconnected from the drive by the power poles of FGC1, and will coast to a stop, with no torque. While the safety interlock remains open, the power to the drive guard control circuitry in the drive remains off. When the safety interlock is closed, the power to the guard control circuitry in the AC drive is restored, and the motor is connected to the drive by FGC1. The motor will not rotate. Restart is accomplished by a separate deliberate action (e.g., pressing the start button of the drive). The N.O. contact of FGC1 in the enabling circuit prevents enabling the drive into an open load The time required to reach the motion hazard is longer than the coast down time of the motor. Robust design can reduce the likelihood of a contactor failure. Construction techniques may reduce the likelihood of a short to 24V DC. The failure mode of the safety interlock may be managed by applying the safety principles of the previous clauses. The safety level performance of the safety interlock is controlled by its design. Use of a Force-Guided Contactor in conjunction with the safety interlock may detect a non-operative contactor. If detected before a drive control failure, machine run-on may be avoided. Failure of the drive to shut off at the logic level, may typically be detected by a resulting motor to command following error or drive over voltage when the drive's active output is connected to an open load. The direct acting auxiliary contacts of the contactor are monitored in the safety interlock circuit as shown in the SIM diagrams as MPCE 1. This type of monitoring may promote this motor connection to a Category 2 performance. ***Informative Note:*** *Consult the drive supplier for the preferred location of the safety contactor (before the drive or before the motor). The designer should review with the drive supplier, any specific requirements to take into account the reflected load when power is interrupted.*

11.2.2.2 Single Channel Interlock Functional Stop Category 1 (per NFPA 79) of an AC Motor using Standard Rated AC Drive (Category 1)



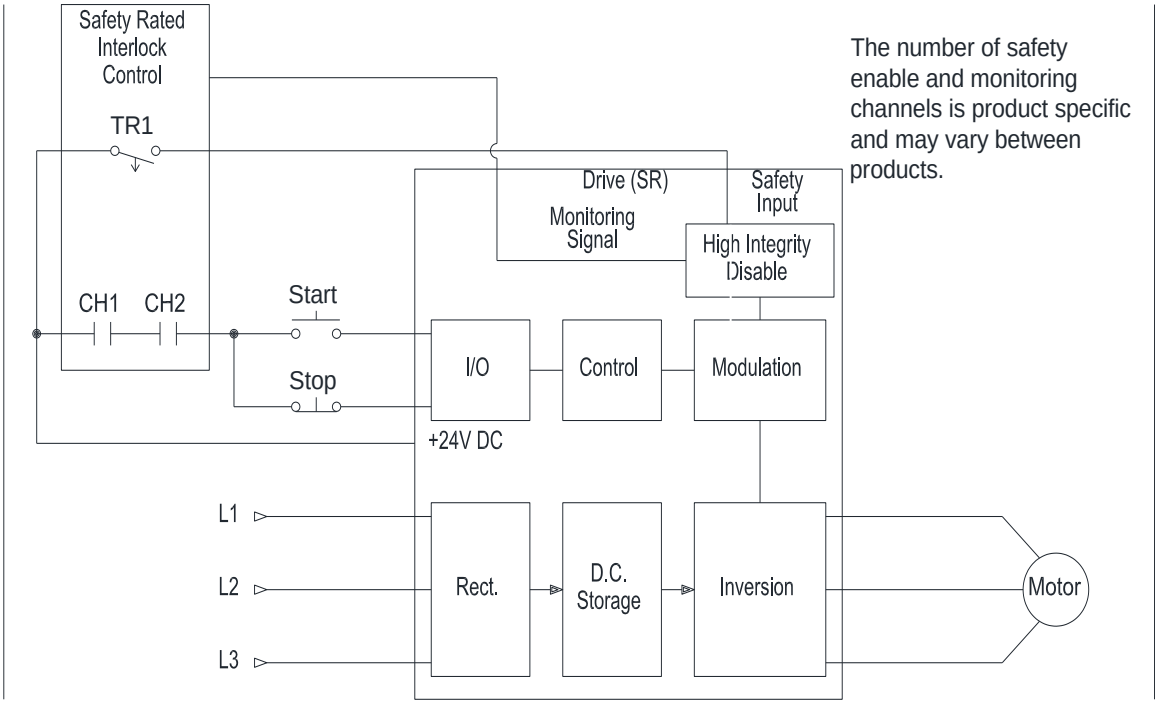
Safety Function:	When the interlock circuit goes low the motor decelerates under control of the drive. After a time delay sufficient to decelerate the motor to a stop, it is disconnected from power.
Faults to Consider:	The drive for this application is considered as a single solid-state device with a single point of failure. The time set on timer TR1 is sufficient to bring the motor to a controlled stop under all reasonable load conditions. Wiring fault (short) to 24V DC at the safety interlock will keep the drive enabled and cause the contactor to remain energized. Failure of the timer to time accurately or fail to drop out will leave power available to the motor. The contactor can weld or remain stuck in the closed state, failing to isolate the motor from the drive.
Fault Exclusion:	None to consider.
Safety Principles:	When the interlock circuit goes low, the drive receives a logic level stop. The motor decelerates under control of the drive. After a time delay TR1 sufficient to decelerate the motor to a stop, the enabling signal is removed forcing all output transistors to shut off with no torque. The motor is disconnected from the drive power by FGC1. While the interlock remains open, the power to the guard control circuitry in the drive remains off. When the interlock is closed, the power to the guard control circuitry in the AC drive is restored, and the motor is connected to the drive by FGC1. The motor will not rotate. Restart is accomplished by a separate deliberate action (e.g., pressing the start button of the drive). The N.O. contact of FGC1 in the enabling circuit prevents enabling the drive into an open load. Robust design can reduce the likelihood of a contactor failure. Construction techniques may reduce the likelihood of a short to 24V DC. The failure mode of the interlock may be managed by applying the safety principles of the previous clauses. The safety level performance of the interlock is controlled by its design. Use of a Force-Guided Contactor in conjunction with the interlock may detect a non-operative contactor. If detected before a drive control failure, machine run-on may be avoided. Failure of the drive to shut off at the logic level may typically be detected by a resulting motor to command following error or drive over voltage when the drive's active output is connected to an open load. The direct acting auxiliary contacts of the contactor are monitored in the interlock circuit as shown in the SIM diagrams as MPCE 1. This type of monitoring may promote this motor connection to a Category 2 performance. ***Informative Note:*** *Consult the drive supplier for the preferred location of the safety contactor (before the drive or before the motor). The designer should review with the drive supplier, any specific requirements to take into account the reflected load when power is interrupted.*

11.2.2.3 A Functional Stop Category 0 (per NFPA 79) of an AC Motor using Safety-related AC Drive (Category 3)



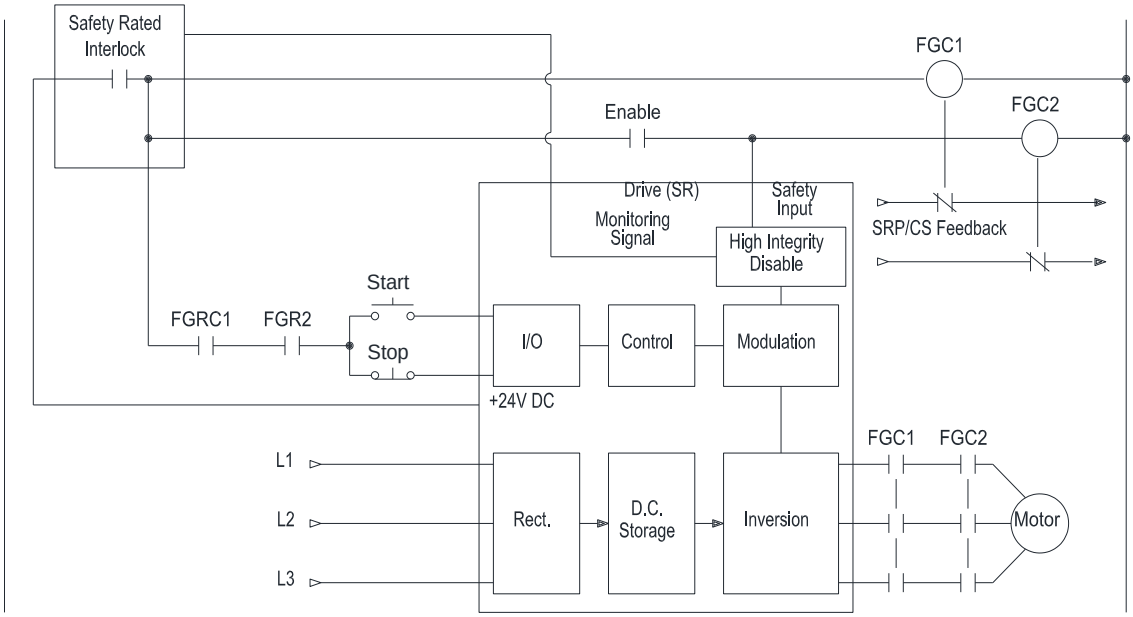
Safety Function:	When the interlock circuit goes low, the drive is shut off immediately. The motor will coast to a stop, with no torque.
Faults to Consider:	Short to 24V DC of the safety interlock circuit can keep the drive enabled.
Fault Exclusion:	None to consider.
Safety Principles:	When the interlock circuit goes low, the drive receives both a logic level stop and the power to guard control circuitry of the AC Drive is removed, through the High Integrity disable circuit, forcing all output transistors to shut off immediately. The motor will coast to a stop, with no torque. The time required to reach the motion hazard is longer than run coast time of the motor. While the safety interlock circuit remains open, the power to the guard control circuitry in the drive remains off. A single fault in the safety-rated drive will not cause the motor to rotate. When the safety interlock circuit is closed and reset, the power to the guard control circuitry in the AC drive is restored, but the motor does not rotate. Restart is accomplished by a separate deliberate action (e.g., pressing the start button of the drive). Any failure modes of the safety interlock circuit are determined by the circuit design. The designer follows the drive supplier's instructions to maintain the drive's safety capability. As an example, some drives may require dual channel guard drive enable signals, self-monitored inputs or provide dual channel monitoring. These shall be strictly adhered to, and their integrity shall be maintained. If these dual channel means are not provided, other methods are used to prevent a loss of the safety function or monitoring by excluding a short to a source of 24V DC through the use of other design and construction methods.

11.2.2.4 Functional Stop Category 1 (per NFPA 79) of an AC Motor using Safety-rated AC Drive (Category 3)



Safety Function:	When the interlock control circuit goes low, the motor decelerates to a stop under control of the drive. After a time delay sufficient to decelerate the motor to a stop, power is removed resulting in zero torque.
Faults to Consider:	Short to 24V DC of the safety interlock circuit can keep the drive enabled. The time required to reach the motion hazard is longer than the deceleration time of the motor.
Fault Exclusion:	None to consider.
Safety Principles:	When the safety-rated interlock control circuit goes low, the drive receives a logic level stop. The motor decelerates under control of the drive. After a time delay TR1 sufficient to decelerate the motor to a stop, the power to the guard control circuitry of the AC Drive is removed, through the High Integrity disable circuit, forcing all output transistors to shut off immediately While the safety interlock circuit remains open, the power to the guard control circuitry in the drive remains off. A single fault in the safety-rated drive will not cause the motor to rotate. When the safety interlock circuit is closed and reset, the power to the guard control circuitry in the AC drive is restored, but the motor does not rotate. Restart is accomplished by a separate deliberate action (e.g., pressing the start button of the drive). Any failure modes of the safety interlock circuit are determined by the circuit design. The designer follows the drive supplier's instructions to maintain the drive's safety capability. As an example, some drives may require dual channel guard drive enable signals, self -monitored inputs or provide dual channel monitoring. If these means are not provided, other methods are used to prevent a loss of the safety function or monitoring by excluding a short to a source of 24V DC through the use of other design and construction methods. ***Informative Note:*** *The designer should review with the drive supplier, any specific requirements to take into account the reflected load when power is interrupted.*

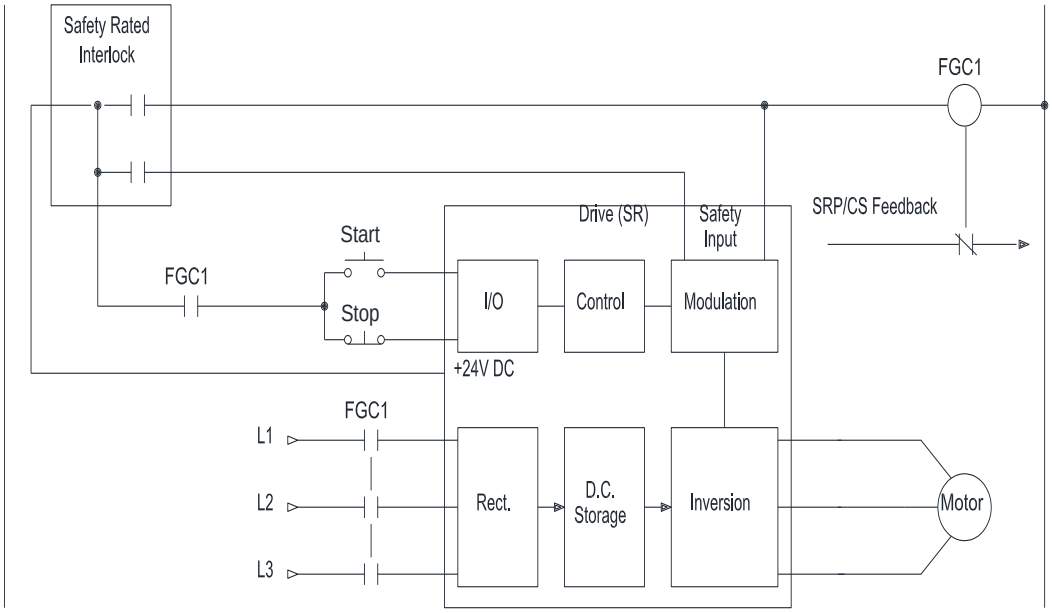
11.2.2.5 Dual Channel Interlock Functional Stop Category 0 (per NFPA 79) of an AC Motor using Standard Rated AC Drive with Checking (Category 4)



See Informative Note 1 below on proper placement of contactors.

Safety Function:	When the safety interlock circuit switch goes low, the drive AC 3-Phase power is removed. The motor will coast to a stop, with no torque.
Faults to Consider:	The drive may not be considered part of the safety system. The time required to reach the motion hazard is longer than run down time of the motor.
Fault Exclusion:	Welded contacts in the relays can be excluded by the use of force-guided relays.
Safety Principles:	When the safety interlock circuit switch goes low, then two contactors in the supply drop and the drive receives a logic level stop and the power to guard control circuitry. The latter forces all output transistors to shut off immediately. The motor will coast to a stop, with no torque. The motor is isolated from the line power by the two Force-Guided contactors FGC1 and 2. While the safety interlock circuit remains open, the power to the guard control circuitry in the drive and the two contactors remain off. When the safety interlock circuit is closed, the power to the guard control circuitry in the AC drive is restored, and the motor reconnected to the drive power by FGC1 and 2, but the motor will not rotate. Restart is accomplished by a separate deliberate action (e.g., pressing the start button of the drive). A safety-rated motor drive may be used to help prevent the opening of the contactors while the drive output is high. As shown in other circuits, a time delay or zero-speed switch may be used to provide active power for deceleration prior to dropping the FGC. The direct acting auxiliary contacts of the contactor are monitored in the safety interlock circuit as shown in the SIM diagrams as MPCE 1 and MPCE 2. Any failure modes of the safety interlock circuit are determined by the circuit design. Some suppliers may provide an L1, L2, L3 disconnect option which keeps power on the controller. ***Informative Note 1:*** *Stop Category 1 may be constructed by using a time delay for the contactors FGC1 and FGC2.* ***Informative Note 2:*** *The designer reviews with the drive supplier, any specific requirements to take into account the reflected load when power is interrupted.*

11.2.2.6 Dual Channel Interlock Functional Stop Category 0 (per NFPA 79) of an AC Motor using Safety-rated AC Drive with Checking and one Force Guided Contactor (Category 4)



See Informative Note 1 below on proper placement of contactors

Safety Function:	When the safety interlock circuit switch goes low, the drive AC 3-Phase power is removed by the contactor and the drive performs its Category 3 level control stop. The motor will coast to a stop, with no torque.
Faults to Consider:	The drive may not be considered part of the safety system. The time required to reach the motion hazard is longer than run down time of the motor.
Fault Exclusion:	None to Consider.
Safety Principles:	When the safety interlock circuit switch goes low, the contactor in the supply drop and the drive receives a safety-rated logic level stop removing the power to the guard control circuitry. The latter forces all output transistors to shut off immediately. The motor will coast to a stop, with no torque. The motor is isolated from the line power by the Force-Guided contactor FGC1. While the safety interlock circuit remains open, the power to the guard control circuitry in the drive and the contactor remains off. When the safety interlock circuit is closed, the power to the guard control circuitry in the AC drive is restored, and the motor reconnected to the drive power by FGC1, but the motor will not rotate. Restart is accomplished by a separate deliberate action (e.g., pressing the start button of the drive). Some suppliers may provide an L1, L2, L3 disconnect option which keeps power on the controller. Any failure modes of the safety interlock circuit are determined by the circuit design. The failure of either of the FGR to disconnect the motor or the drive control shut down will be detected by the safety interlock circuit, preventing further operation. A Safety Stop 1 drive may be used if the drop of FGC1 is delayed until the motor has reached a stop. As shown in other circuits, a time delay or zero-speed switch may be used to provide active power for deceleration prior to dropping the FGC. The motor will come to a controlled stop using the safety-rated drive Category 1 stop. ***Informative Note 1:*** *Stop Category 1 may be constructed by using a time delay for the contactors FGC1 .* ***Informative Note 2:*** *The designer reviews with the drive supplier, any specific requirements to take into account the reflected load when power is interrupted.*

11.3 Pneumatic Systems

11.3.1 Design Requirements

When used as part of an SRP/CS, pneumatic elements shall meet the reliability requirements determined in subclause 5.4.

11.3.2 Design Considerations

The pneumatic safety system may consist of a number of safety functions to address different pneumatic risks. Each individual safety function may have different risk levels and the required reliability levels may not be the same. This is especially true for residual risk.

Informative Note: *The risk level of an actuator under full supply pressure may require a category 3 or 4 safety function. The residual risk due to gravity may only require a category 1 solution.*

11.3.3 Supply Circuit

The example shown after 11.3.9 contains a safety lockout valve, safety valve, filters, regulator and gauge.

11.3.4 Energy Isolation/Lockout Valve

A manual energy isolation device shall be provided to block supply and release downstream pressure. It shall meet the requirements of ANSI Z244.1 and ANSI B11.0. Considerations include supply & exhaust capacity, verification of energy removal, and tamper resistance.

11.3.5 Air Preparation (Contamination Control)

A fluid power circuit's reliability is influenced by contamination, also known as its cleanliness level. Care must be taken to select fluid conditioning components appropriate for the intended level of reliability. Strict adherence to the proper conditioning of the fluid power source can increase the mean time to dangerous failure.

11.3.6 Filtration

Filters shall meet or exceed the filtration requirements of the pneumatic safety devices as described by the manufacturer in accordance with ISO 8573. Filters with automatic drains are encouraged.

11.3.7 Regulator

Control shall be provided to maintain the system pressure within safe limits, e.g., where pressure regulators are used, they should be of the self-relieving type. Relieving type regulators are not safety relief devices and shall not be the sole device to prevent excess pressure where its relief capability may be inadequate.

The preferred means of protection against excessive pressure are one or more pressure relief valves located to limit the pressure in all parts of the system.

Loss of pressure or critical drops in pressure shall not expose personnel to a hazard.

Regulators with a bypass check valve should be considered to reduce exhaust times.

Informative Note: *Over pressurizing can result in premature wear due to an increase in forces created by pneumatic devices above what is required by the manufacturer.*

11.3.8 Lubrication

11.3.8.1 Non-Lubricated (preferred)

Non-lubricated pneumatic systems, also known as *pre-lubricated* because the actuators are pre-lubricated for the intended life of the equipment, are preferred because of an inherently higher level of reliability and reduced operational costs and should be used wherever possible.

11.3.8.2 Lubricated (not recommended)

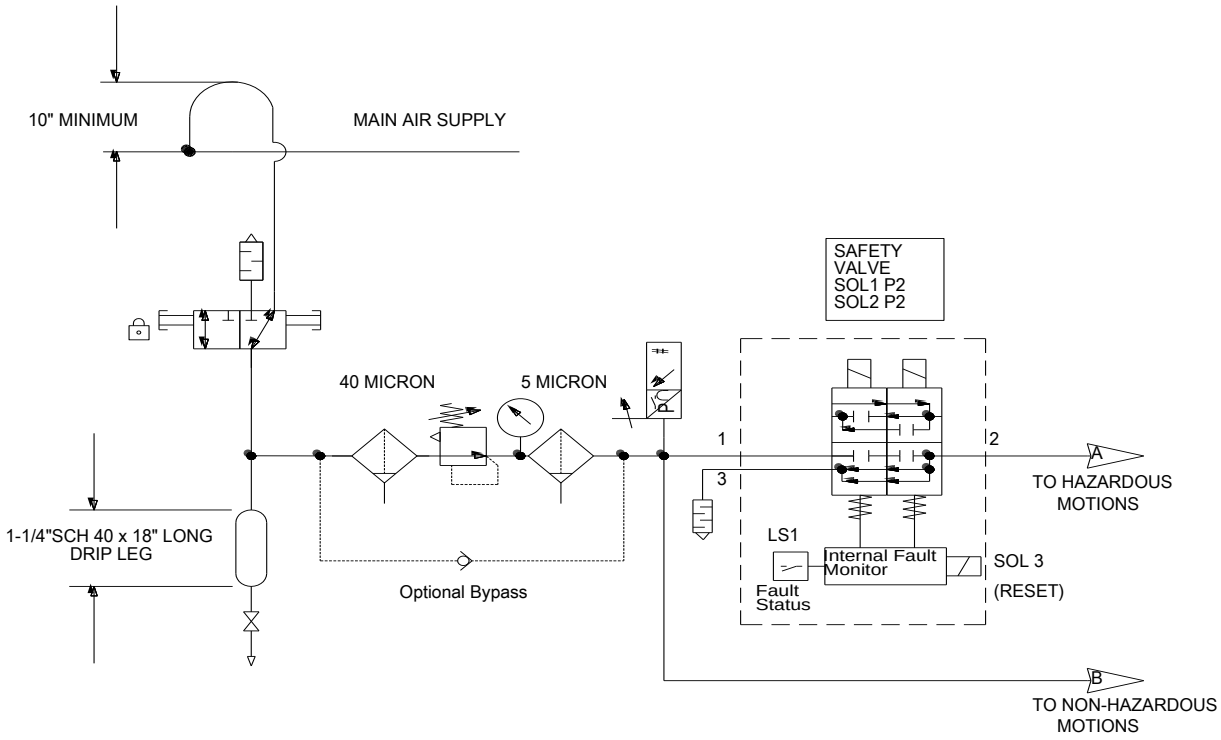
Air-line atomized or mist type lubricated circuits and components must be serviced at frequent intervals. If the lubricators are not maintained and allowed to run dry, the lubrication will quickly dry out and become tacky resulting in a decreased level of reliability of the pneumatic systems control components. Motion control

valves, main spools and pilot valves can stick in a number of positions thereby preventing the ability of the valve from returning to a de-energized position and stop a hazardous motion as intended.

11.3.9 Air Valve Mufflers

Air mufflers for safety systems and air dumps shall have sufficient capacity so as not to restrict the exhausting of the system. Sintered bronze or paper mufflers shall not be used.

Pneumatic exhaust ports shall not create a jet concern. Exhausts without a muffler shall be provided with a shield or other device so as to guard from direct exposure to the exhausting air and eliminate the potential blocking of the exhaust. Exhaust may be plumbed to hollow structural machine members with a drain valve at the low point.



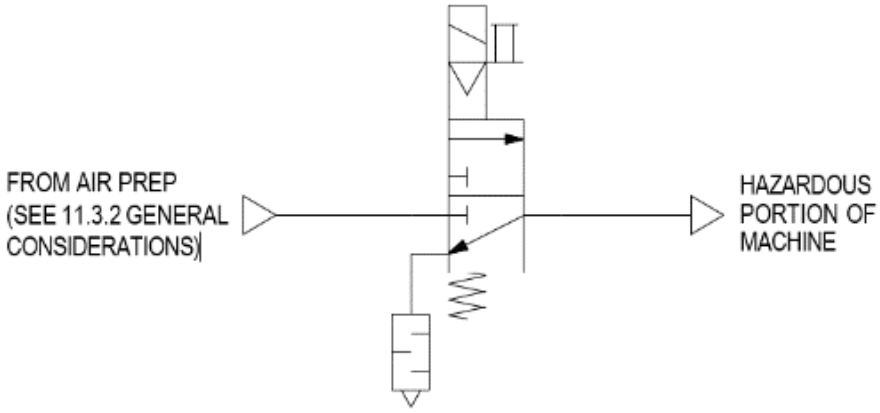
Safety Function:	Proper air preparation conditions the incoming fluid supply thereby increasing the circuit life, reliability and performance.
Faults to Consider:	Filter failure, high liquid level or poor maintenance will pass contamination to the system. Regulator failure or improper adjustment can cause excessive pressures in the system.
Fault Exclusion:	None to consider.
Safety Principles:	The air drop header connection to the top of the main header minimizes contamination transfer to equipment increasing the overall system reliability. Connections to the bottom of the header will act as a drain, increasing the level of contamination to the machine and is not permitted. Safety exhaust lockout valve - Installation in vertical drop allows for convenient lockout placement close to and at the same height as the electrical disconnect. This saves time in removing energy in a hazardous situation. The valve may also be located next to the filter. Air Preparation-Drip leg acts as a collector for the majority of supply contaminants thereby greatly increasing filter life. Filtration requirements as defined by ISO 8573. System regulator is set to the minimum pressure required for proper operation. Pressures set above minimum requirements unnecessarily increase operational costs and increase component wear, which can lead to a decrease in overall reliability. Safety valve(s) - Performance requirements are to be determined by the risk assessment.

11.3.10 Pneumatic Safety Functions

11.3.10.1 Exhaust (Blocking/Dump) Safety Function

11.3.10.1.1 Design requirements

When the electrical command signal is removed, fluid supply pressure shall be blocked and vented from the hazardous portion of the machine.



11.3.10.1.2 Design considerations

Potential hazardous failures include the failure to block and vent, a slow response causing the venting to take longer than usual due to valve delay or muffler contamination, or a failure which allows residual pressure to remain downstream.

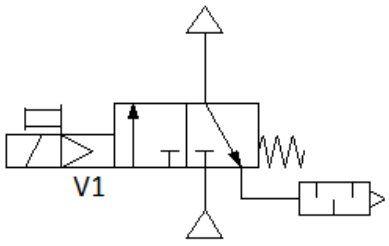
Additional hazards caused by gravity or the reapplication or pressure shall be considered.

Informative Note 1: *Gravity issues can be addressed with pilot operated checks or rod locks/brakes.*
Informative Note 2: *Reapplication of pressure can be addressed with soft start valves or flow controls.*

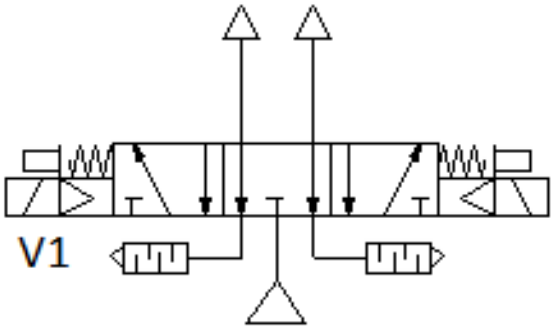
Monitoring can be done via direct monitoring of the internal element, indirect monitoring of the downstream pressure, or monitoring of the process if the valve is controlling a single actuator such as an air motor or single acting cylinder.

Informative Note: *A minimum operating pressure switch may not indicate that a safe pressure level has been reached.*

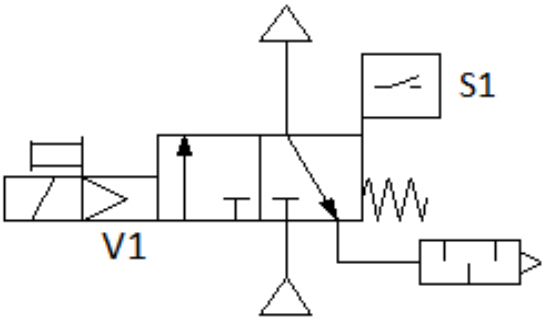
11.3.10.2 Exhaust (blocking/Dump) – 3/2 Normally Closed Valve (Category 1)

Circuit:	
Safety Function:	When the electrical command signal is removed, fluid supply pressure is blocked and vented from the hazardous portion of the machine.
Faults to Consider:	Leakage or improper sealing of components. Valve element not actuating or de-actuating properly. A slow or sticking valve can affect response time of the safety system.
Fault Exclusion:	None to consider.
Safety principles:	When the electrical command signal is removed, the valve shifts to the spring returned position thereby blocking fluid power from flowing downstream and exhausts fluid power from the hazardous portion of the machine.

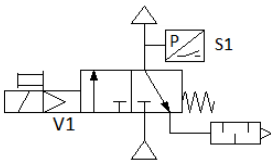
11.3.10.3 Exhaust (Blocking/Dump) – 5/3 Open Center Valve (Category 1)

Circuit:	
Safety Function:	When the electrical command signal is removed, fluid supply pressure is blocked and vented from the hazardous portion of the machine.
Faults to Consider:	Leakage or improper sealing of components. Valve element not actuating or de-actuating properly. A slow or sticking valve can affect response time of the safety system.
Fault Exclusion:	None to consider.
Safety principles:	When the electrical command signal is removed, the valve shifts to the spring returned position thereby blocking fluid power from flowing downstream and exhausts fluid power from the hazardous portion of the machine.

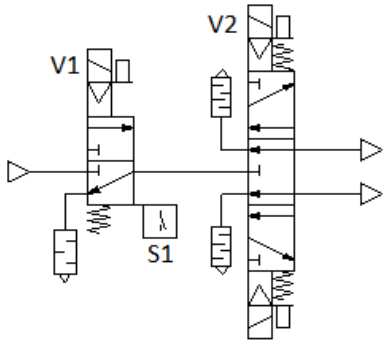
11.3.10.4 Exhaust (blocking/Dump – 3/2 Normally Closed Valve with Integrated Sensor (Category 2)

Circuit:	
Safety Function:	When the electrical command signal is removed, fluid supply pressure is blocked and vented from the hazardous portion of the machine.
Faults to Consider:	Leakage or improper sealing of components. Valve element not actuating or de-actuating properly. A slow or sticking valve can affect response time of the safety system.
Fault Exclusion:	None to consider.
Safety Principles:	When the electrical command signal is removed, the valve shifts to the spring returned position thereby blocking fluid power from flowing downstream and exhausts fluid power from the hazardous portion of the machine. S1 indicates the position of the valve element in the flow to output state. S1 is monitored by the SRP/CS at regular intervals to ensure that the valve has shifted. S1 changes state prior to allowing flow. When response time is critical, monitor the timing between solenoid actuation/de-actuation and sensor response.

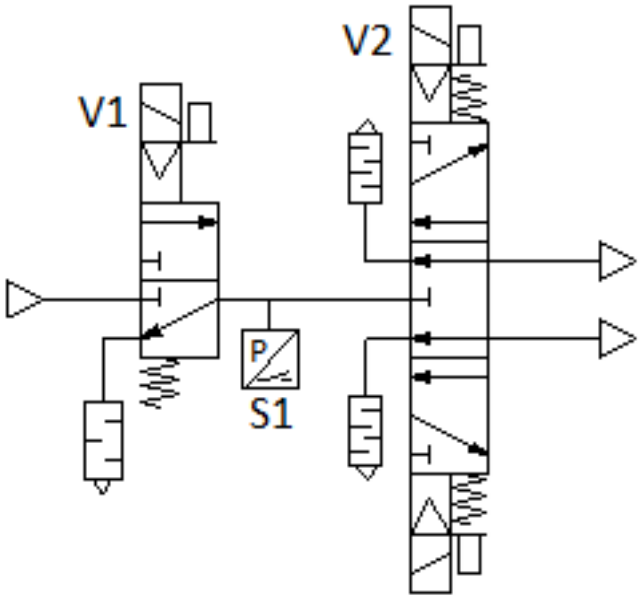
11.3.10.5 Exhaust (Blocking/Dumping) – 3/2 Normally Closed Valve with Pressure Sensor (Category 2)

Circuit:	
Safety Function:	When the electrical command signal is removed, fluid supply pressure is blocked and vented from the hazardous portion of the machine.
Faults to Consider:	Leakage or improper sealing of components. Valve element not actuating or de-actuating properly. A slow or sticking valve can affect response time of the safety system.
Fault Exclusion:	None to consider.
Safety Principles:	When the electrical command signal is removed, the valve shifts to the spring returned position thereby blocking fluid power from flowing downstream and exhausts fluid power from the hazardous portion of the machine. S1 indicates the position of the valve element in the flow to output state. S1 is monitored by the SRP/CS at regular intervals to ensure that the valve has shifted. When response time is critical, monitor the timing between solenoid actuation/de-actuation and sensor response.

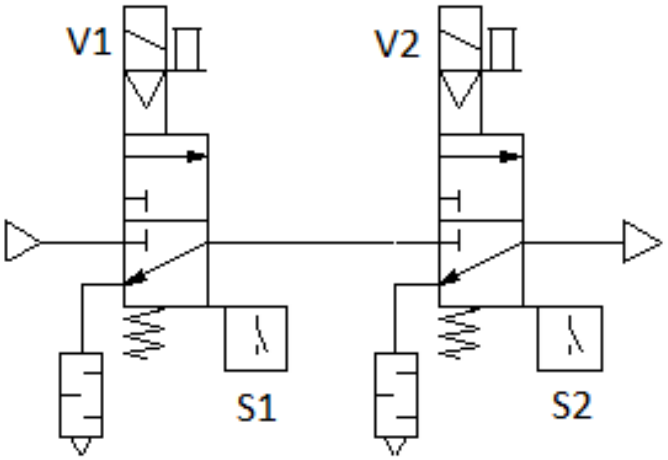
11.3.10.6 Exhaust (Blocking/Dump) – 3/2 Normally Closed Valve with Integrated Sensor in Series with 5/3 Open Center Valve (Category 3)

Circuit:	
Safety Function:	When the electrical command signal is removed, fluid supply pressure is blocked and vented from the hazardous portion of the machine.
Faults to Consider:	Leakage or improper sealing of components. A slow or sticking valve can affect response time of the safety system.
Fault Exclusion:	None to consider.
Safety Principles	When the electrical command signal is removed, the valve shifts to the spring returned position thereby blocking fluid power from flowing downstream and exhausts fluid power from the hazardous portion of the machine. S1 indicates the position of the valve element V1 in the flow to output state. S1 is monitored by the SRP/CS at regular intervals to ensure that the valve has shifted. S1 changes state prior to allowing flow. 5/3 Open Center valve is monitored indirectly or by the process (monitoring not shown). The continued function of the machine may not indicate the ability of the valve V2 to spring center and remove energy. The ability for the directional valve V2 to stop the motion by centering is tested at regular intervals. When response time is critical, monitor the timing between solenoids actuation/de-actuation sensor response, and process response.

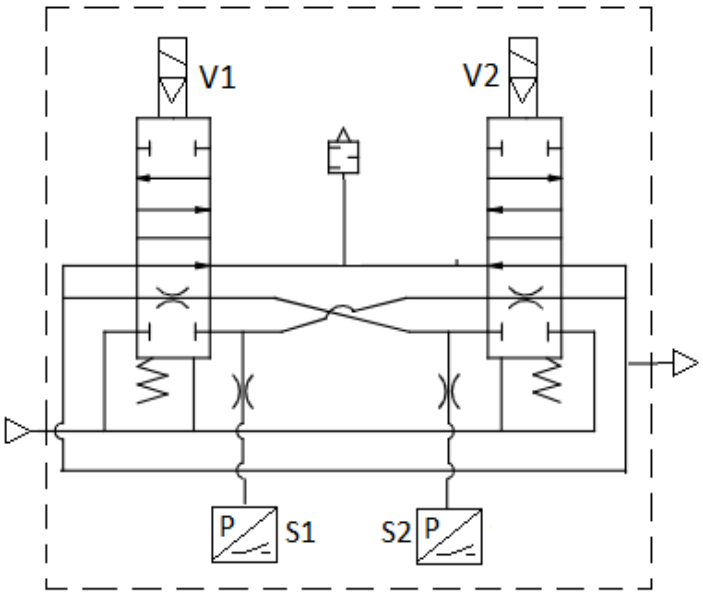
11.3.10.7 Exhaust (Blocking/Dump) – 3/2 Normally Closed Valve with Pressure Sensor in Series with 5/3 Open Center Valve (Category 3)

Circuit:	
Safety Function:	When the electrical command signal is removed, fluid supply pressure is blocked and vented from the hazardous portion of the machine.
Faults to Consider:	Leakage or improper sealing of components. A slow or sticking valve can affect response time of the safety system.
Fault Exclusion:	None to consider.
Safety Principle:	When the electrical command signal is removed, the valve shifts to the spring returned position thereby blocking fluid power from flowing downstream and exhausts fluid power from the hazardous portion of the machine. S1 indicates the position of the valve element V1 in the flow to output state. S1 is monitored by the SRP/CS at regular intervals to ensure that the valve has shifted. S1 changes state prior to allowing flow. 5/3 Open Center valve is monitored indirectly or by the process (monitoring not shown). The continued function of the machine may not indicate the ability of the valve V2 to spring center and remove energy. The ability for the directional valve V2 to stop the motion by centering is tested at regular intervals. When response time is critical, monitor the timing between solenoids actuation/de-actuation sensor response, and process response.

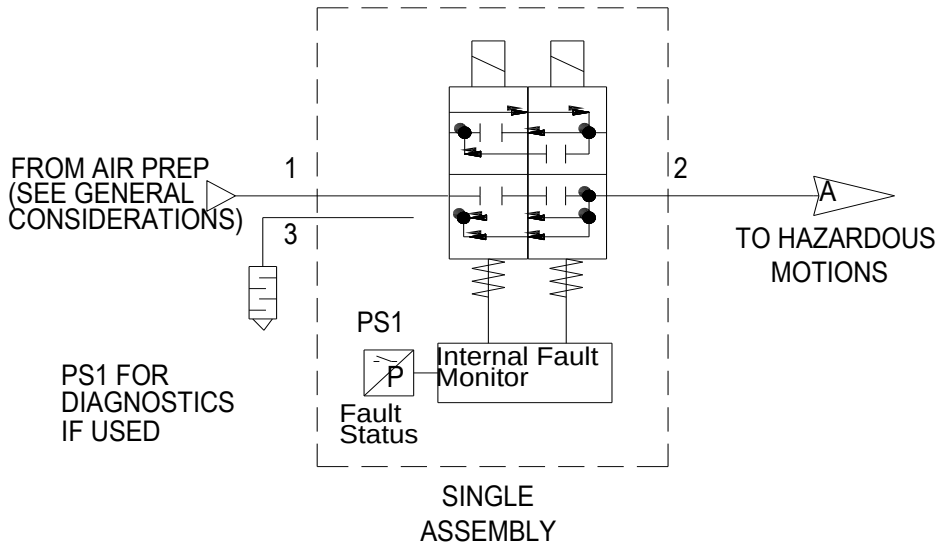
11.3.10.8 Exhaust (Blocking/Dump) 3/2 Normally Closed Valves with Integrated Sensors in Series (Category 3 or 4)

Circuit:	
Safety Function:	When the electrical command signal is removed, fluid supply pressure is blocked and vented from the hazardous portion of the machine.
Faults to Consider:	Leakage or improper sealing of components. A slow or sticking valve can affect response time of the safety system.
Fault Exclusion:	None to consider.
Safety Principle:	When the electrical command signal is removed, the valve shifts to the spring returned position thereby blocking fluid power from flowing downstream and exhausts fluid power from the hazardous portion of the machine. Sensors which indicate the position of the valve elements, are directly operated by the elements in the flow to output state. Sensors are monitored by the SRP/CS at regular intervals or when there is a demand of the safety function to ensure that the valves have shifted. A single fault is detected at or before the next demand upon the safety function. Non-synchronous movement of the independent elements while actuating or de-actuating is monitored by the SRP/CS and results in a fault condition (diminished performance fault). Sensors change state prior to allowing flow. To achieve up to Category 3, sensors may be monitored in series. To achieve up to Category 4, monitor sensors in parallel.

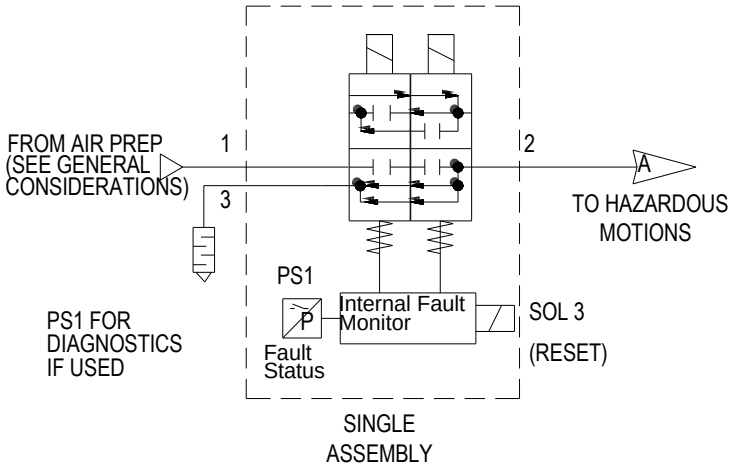
11.3.10.9 3/2 Exhaust (Blocking Dump) – Normally Closed Safety-Rated Dual Valve with Sensors, Automatic Reset (Category 4)

Circuit:	
Safety Function:	When the electrical command signal is removed, fluid supply pressure is blocked and vented from the hazardous portion of the machine.
Faults to Consider:	A slow or sticking valve can affect response time of the safety system.
Fault Exclusion:	None to consider.
Safety Principle	When the electrical command signal is removed, the valve shifts to the spring returned position thereby blocking fluid power from flowing downstream and exhausts fluid power from the hazardous portion of the machine. Sensors indicate the pressure supplied by the independent valve elements. Sensors are monitored by the SRP/CS at regular intervals or when there is a demand of the safety function to ensure that the valves have shifted. A single fault is detected at or before the next demand upon the safety function. Non-synchronous movement of the independent elements while actuating or de-actuating is monitored by the SRP/CS and results in a fault condition (diminished performance fault). When response time is critical, monitor the timing between solenoids actuation/de-actuation and sensors response. To achieve up to Category 3, sensors may be monitored in series. To achieve up to Category 4, monitor sensors in parallel.

11.3.10.10 Exhaust (Blocking/Dump) – 3/2 Normally Closed Safety-Rated Dual Valve with Internal Monitoring and Feedback Sensor, Automatic Reset (Category 4)

Circuit:	
Safety Function:	When the electrical command signal is removed, fluid supply pressure is blocked and vented from the hazardous portion of the machine.
Faults to Consider:	None to consider.
Fault Exclusion:	None to consider.
Safety Principle:	When the electrical command signal is removed, the valve shifts to the spring returned position thereby blocking fluid power from flowing downstream and exhausts fluid power from the hazardous portion of the machine. Monitoring is performed internally by the valve assembly. A valve internal malfunction will result in a safe condition. When a faulted condition exists, PS1 can provide status feedback to a PLC input. PS1 is provided for status indication purposes and is not considered as part of the SRP/CS. The internal dynamic monitoring ensures both independent valve elements function simultaneously. Non-synchronous movement of the independent elements while actuating or de-actuating results in a fault condition (diminished performance fault). Auto-Reset of the valve does not cause the valve to shift and provide pressure downstream.

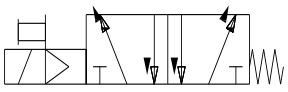
11.3.10.11 Exhaust (Blocking Dump) 3/2 Normally Closed Safety-Rated Dual Valve with Internal Monitoring, Feedback Sensor, Manual Reset (Category 4)

Circuit:	
Safety Function:	When the electrical command signal is removed, fluid supply pressure is blocked and vented from the hazardous portion of the machine.
Faults to Consider:	None to consider.
Fault Exclusion:	None to consider.
Safety Principle:	When the electrical command signal is removed, the valve shifts to the spring returned position thereby blocking fluid power from flowing downstream and exhausts fluid power from the hazardous portion of the machine. Monitoring is performed internally by the valve assembly. A valve internal malfunction will result in a safe condition. When a faulted condition exists, PS1 can provide status feedback to a PLC input. PS1 is provided for status indication purposes and is not considered as part of the SRP/CS. The internal dynamic monitoring ensures both independent valve elements function simultaneously. Non-synchronous movement of the independent elements while actuating or de-actuating results in a fault condition (diminished performance fault). Resetting of the valve does not cause the valve to shift and provide pressure downstream.

11.3.11 Safe Valve Position/Direction (Safe Return)

11.3.11.1 Design Requirements

When the electrical command signal is removed, the hazardous motion shall reverse and continue until the end of stroke is reached.



11.3.11.2 Design Considerations

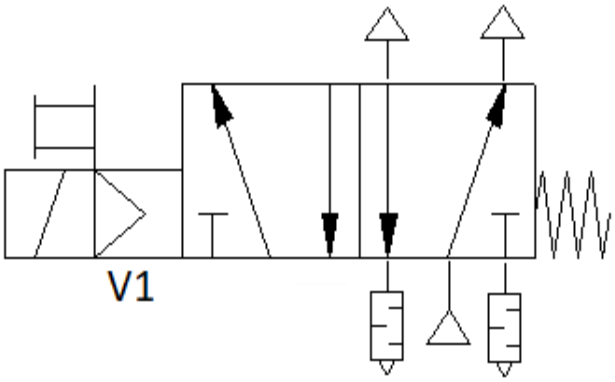
Potential hazardous failures include failure to unshift continuing motion in the hazardous direction, or a slow response causing motion to continue in the hazardous direction for a short period of time.

Additional hazards including pinch points on the return stroke or motion caused by the loss of supply pressure due to gravity shall be considered.

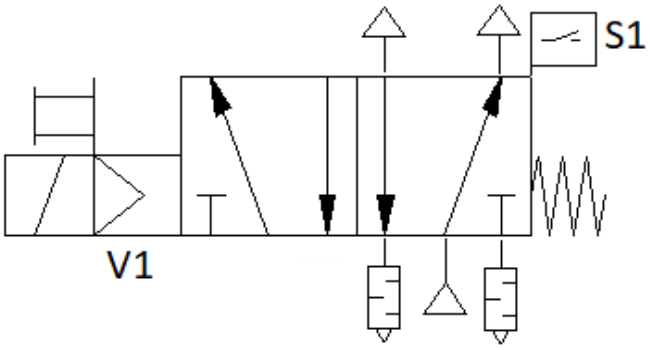
Monitoring can be done via direct monitoring of the internal element, indirect monitoring of the downstream pressures or cylinder position, or monitoring by process of the actuator being controlled.

Informative Note: *End of stroke monitoring will not indicate a hazardous failure until the cylinder reaches the end of stroke and the potentially hazardous event has occurred.*

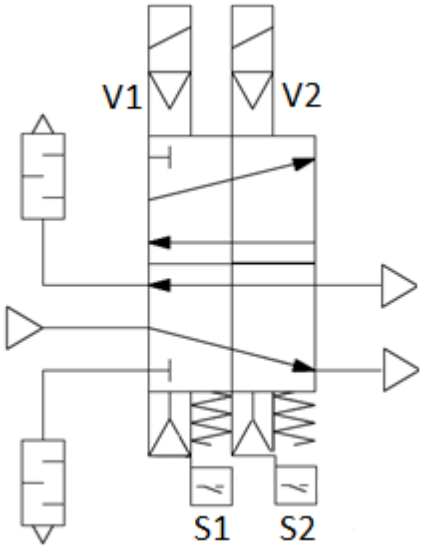
11.3.11.3 Safe Valve Position/Direction (Safe Return) – 5/2 Valve (Category 1)

Circuit:	
Safety Function:	When the electrical command signal is removed, the hazardous motion reverses and continues until the end of stroke is reached.
Faults to Consider:	Valve element not actuating or de-actuating properly. A slow or sticking valve can affect response time of the safety system. Loss of supply pressure allows movement.
Fault Exclusion:	None to consider.
Safety Principles	The spring returns the valve to the home position.

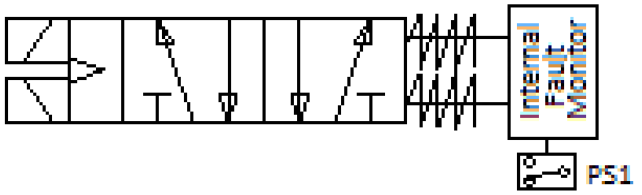
11.3.11.4 Safe Valve Position/Direction (Safe Return) – 5/2 Valve with Integrated Sensor (Category 2)

Circuit:	
Safety Function:	When the electrical command signal is removed, the hazardous motion reverses and continues until the end of stroke is reached.
Faults to Consider:	Valve element not actuating or de-actuating properly. A slow or sticking valve can affect response time of the safety system. Loss of supply pressure allows movement.
Fault Exclusion:	None to consider.
Safety Principles:	The spring returns the valve to the home position. S1 indicates the position of the valve element. S1 shall be monitored by the SRP/CS at regular intervals to ensure that the valve has shifted. S1 changes state prior to changing flow path. When response time is critical, monitor the timing between solenoid actuation/de-actuation and sensor response.

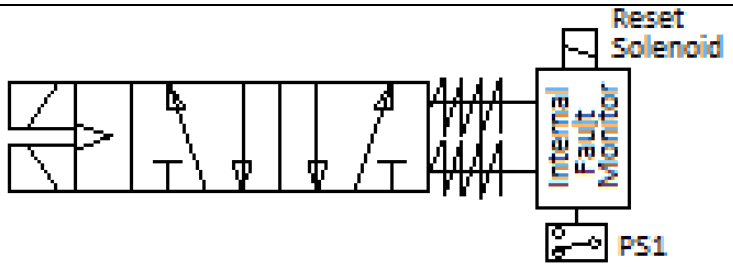
11.3.11.5 5/2 Safe Valve Position/Direction (Safe Return) – Safety-Rated Dual Valve with Integrated Sensors, Automatic Reset (Category 3 or 4)

Circuit:	
Safety Function:	When the electrical command signal is removed, the hazardous motion reverses and continues until the end of stroke is reached.
Faults to Consider:	Loss of supply pressure allows movement.
Fault Exclusion:	None to consider.
Safety Principles	The spring returns the valve to the home position. Sensors which indicate the position of the valve elements. Sensors are monitored by the SRP/CS at regular intervals or when there is a demand of the safety function to ensure that the valves have shifted. A single fault is detected at or before the next demand upon the safety function. Non-synchronous movement of the independent elements while actuating or de-actuating is monitored by the SRP/CS and results in a fault condition (diminished performance fault). Sensors change state prior to changing flow path. To achieve up to Category 3, sensors may be monitored in series. To achieve up to Category 4, monitor sensors in parallel.

11.3.11.6 Safe Valve Position/Direction(Safe Return) – Dual Safety-Rated 5/2 Valve with Internal Monitoring, Feedback Sensor, Automatic Reset (Category 4)

Circuit:	
Safety Function:	When the electrical command signal is removed, the hazardous motion reverses and continues until the end of stroke is reached.
Faults to Consider:	Loss of supply pressure allows movement.
Fault Exclusion:	None to consider.
Safety Principles	The spring returns the valve to the home position. Monitoring is performed internally by the valve assembly. A valve internal malfunction will result in a safe condition. When a faulted condition exists, PS1 can provide status feedback to a PLC input. PS1 is provided for status indication purposes and is not considered as part of the SRP/CS. The internal dynamic monitoring ensures both independent valve elements function simultaneously. Non-synchronous movement of the independent elements while actuating or de-actuating and results in a fault condition (diminished performance fault). Auto-Reset of the valve does not cause the valve to shift and allow actuator motion.

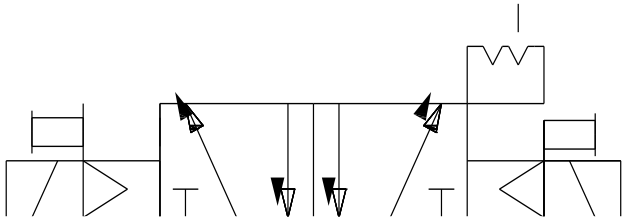
11.3.11.7 Safe Valve Position/Direction (Safe Return) – Dual Safety-Rated Valve with Internal Monitoring, Feedback Sensor, Manual Reset (Category 4)

Circuit:	
Safety Function:	When the electrical command signal is removed, the hazardous motion reverses and continues until the end of stroke is reached.
Faults to Consider:	Loss of supply pressure allows movement.
Fault Exclusion:	None to consider.
Safety Principles:	Monitoring is performed internally by the valve assembly. A valve internal malfunction will result in a safe condition. When a faulted condition exists, PS1 can provide status feedback to a PLC input. PS1 is provided for status indication purposes and is not considered as part of the SRP/CS. The internal dynamic monitoring ensures both independent valve elements function simultaneously. Non-synchronous movement of the independent elements while actuating or de-actuating is monitored by the SRP/CS and results in a fault condition (diminished performance fault). Resetting of the valve does not cause the valve to shift and provide pressure downstream.

11.3.12 Maintain End of Stroke Position (Safe Last Position)

11.3.12.1 Design Requirements

When the electrical command signal is removed, the hazardous motion shall continue in the direction initiated, or dwell in its current end of travel location. Designs should be limited to short strokes or actuators where a loss of pressure would not lead to a safety hazard.



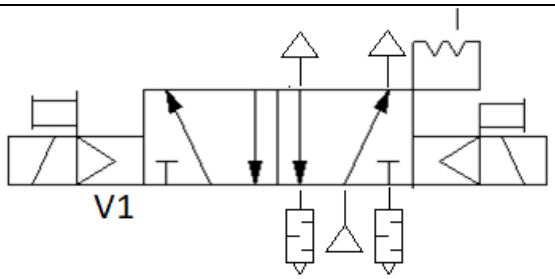
11.3.12.2 Design Considerations

Potential hazards include continued motion or reversal of motion without stopping.

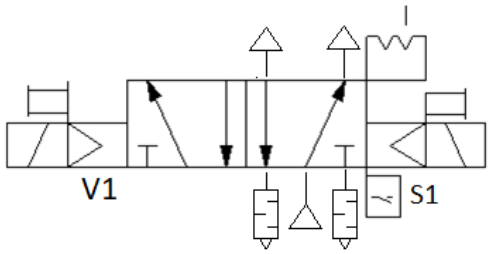
Additional hazards including motion in either direction creating pinch points or dropping of clamped parts shall be considered. Loss of supply pressure can result in loss of actuator (i.e., clamping) force.

Monitoring can be done via direct monitoring of the internal element, indirect monitoring of the downstream pressures, or monitoring by process of the actuator being controlled.

11.3.12.3 Maintain End of Stroke Position (Safe Last Position) - 5/2 Detented Valve (Category 1)

Circuit:	
Safety Function:	When the electrical command signal is removed, the hazardous motion continues in the direction initiated, or dwells in its current end of travel location.
Faults to Consider:	Valve element not actuating or de-actuating properly. A slow or sticking valve can affect response time of the safety system. Loss of supply pressure allows movement.
Fault Exclusion:	None to consider.
Safety Principles:	Limit to short strokes.

11.3.12.4 5/2 Maintain End of Stroke Position (Safe Last Position) - Detented Valve with Integrated Sensor (Category 2)

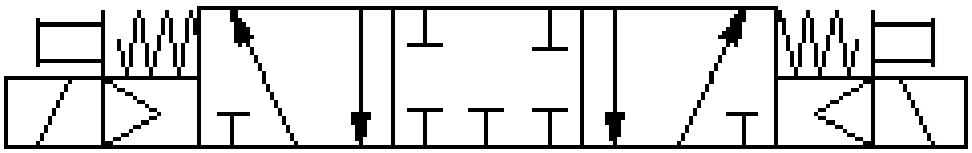
Circuit:	
Safety Function:	When the electrical command signal is removed, the hazardous motion continues in the direction initiated, or dwells in its current end of travel location.
Faults to Consider:	Valve element not actuating or de-actuating properly. A slow or sticking valve can affect response time of the safety system. Loss of supply pressure allows movement.
Fault Exclusion:	None to consider.
Safety Principles:	S1 indicates the position of the valve element. S1 is monitored by the SRP/CS at regular intervals to ensure that the valve has shifted. Sensor changes state prior to changing flow path. When response time is critical, monitor the timing between solenoid actuation/de-actuation and sensor response.

11.3.13 Safe Stopping (Load Holding)

11.3.13.1 Control and Stop/Hold

11.3.13.1.1 Design Requirements

When the electrical command signal is removed, the hazardous motion shall be halted and the actuator held in its present position.



11.3.13.1.2 Design Considerations

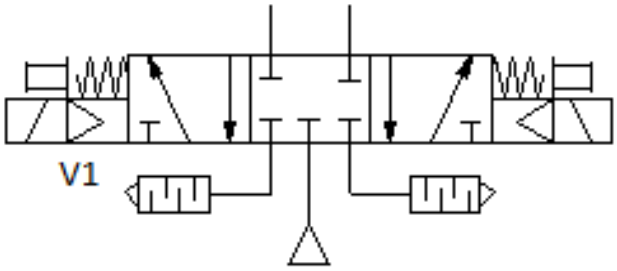
Potential hazards include continuing motion or the reversal of motion.

Additional hazards including motion in either direction creating pinch points, drifting motion due to system leakage, and trapped pressure in the system shall be considered.

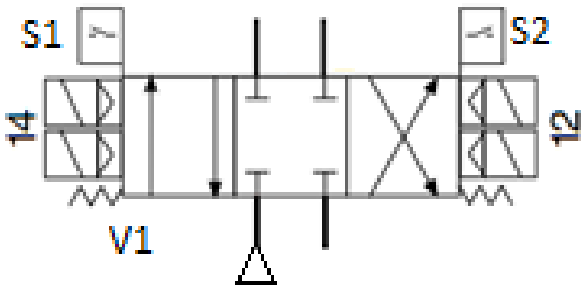
Monitoring can be done via direct monitoring of the internal element, indirect monitoring of the actuator, or monitoring by process of the actuator being controlled.

Informative Note: *End of stroke monitoring will not indicate a hazardous failure until the potentially hazardous event has occurred.*

11.3.13.2 Control and Stop/Hold 5/2 Closed Center Valve (Category 1)

Circuit:	
Safety Function:	When the electrical command signal is removed, the hazardous motion stops, and the actuator is held in its present position.
Faults to Consider:	Valve element not actuating or de-actuating properly. A slow or sticking valve can affect response time of the safety system. Leakage or improper sealing of components including downstream devices will cause motion.
Fault Exclusion:	None to consider.
Safety Principles:	Monitoring the position of the valve can improve reliability.

11.3.13.3 Control and Stop/Hold – 5/3 Closed Center Safety-Rated Dual Valve with Integrated Sensors, Automatic Reset (Category 3 or 4)

Circuit:	
Safety Function:	When the electrical command signal is removed, the hazardous motion stops, and the actuator is held in its present position.
Faults to Consider:	Leakage or improper sealing of components including downstream devices will cause motion.
Fault Exclusion:	None to consider.
Safety Principles	Sensors which indicate the pressure supplied by the independent valve elements. Sensors are continuously monitored by the SRP/CS at regular intervals to ensure that the valves have shifted. Non-synchronous movement of the independent elements while actuating or de-actuating is monitored by the SRP/CS and results in a fault condition (diminished performance fault). When response time is critical, monitor the timing between solenoid actuation and sensor response. To achieve up to Category 3, sensors may be monitored in series. To achieve up to Category 4, monitor sensors in parallel.

11.3.14 Stop (Load Holding)

Pilot operated (P.O.) checks or blocking valves are used to trap or store energy (pneumatic pressure) in the actuator(s) to maintain force or position. This energy is typically not removed by turning off the air supply safety lockout exhaust valve.

Spring return blocking valves on the exhaust side of a vertical actuator maintain the actuator position by trapping air under the actuator piston. Solenoid or P.O. Check valves may also be used to trap or store energy (pneumatic pressure) in the actuator(s) to maintain position. This energy is typically not removed by the blocking valve, nor by venting the compressed air supply. Note that the check valve functions only in the exhaust flow path. When the directional control valve shifts to pressurize the line into the check valve, it will cause the actuator to move in the upward direction. Thus, the check valve provides fluid control only in the exhaust mode.

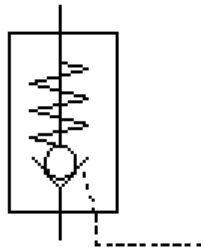
P.O. checks maintain the vertical actuator position by trapping air between the valve and the actuator piston. To ensure quick response, the entrained volume between the valve and the actuator should be kept to a minimum. P.O. checks, piston, rod seal, fittings or line leaks can cause a lowering motion that needs to be considered during the risk assessment.

Caution: The use of dual P.O. checks used to trap pressure (stored energy) on both sides of the actuator shall consider that leaks will cause an unintended movement of the actuator towards the leak. The pilot pressure supply can directly affect the closing of the check which can impact the stopping time/distance of the actuator. The supply shall be connected downstream of the safety blocking/dump valve.

When the exhaust or drain end of a cylinder at the rod end can be blocked due to failure in the control or valve while system pressure can still be supplied to the piston, the design shall be capable of withstanding the pressure intensification due to the rod area differential between the supply and exhaust/drain sides of the cylinder piston.

For the check valves with external pilot control to be dual channel when controlled by their pilot only, each shall have its own individual pilot control valve or be piloted by a category 3 or 4 exhaust (blocking/dump) valve, or else they will have a common failure mode, which is not acceptable for a dual channel design.

11.3.14.1 Stop (Load Holding) Pilot Operated (P.O.) Check



11.3.14.1.1 Design Requirements

Removal of the command signal results in stoppage of hazardous motion and the actuator held in position.

11.3.14.1.2 Design Considerations

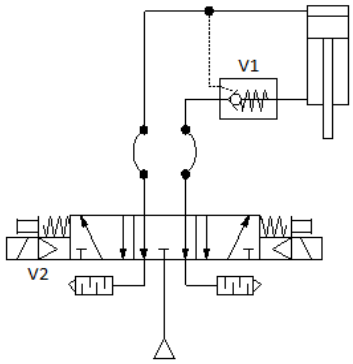
Potential hazards include continuing motion or potential drift.

Additional Hazards including motion in either direction creating pinch points and trapped pressure in the system shall be considered.

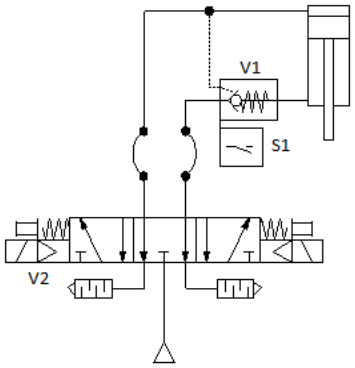
Monitoring can be done via direct monitoring of the internal element, indirect monitoring of the downstream pressures, or monitoring by process of the actuator being controlled.

Informative Note: *Direct position sensing may not indicate leakage in the valve or system.*

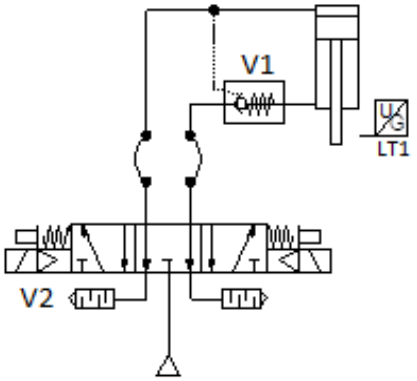
11.3.14.2 Stop (Load Holding) – Pilot Operated Check Valve (Category 1)

Circuit:	
Safety Function:	Removal of the command signal results in stoppage of hazardous motion and the actuator held in position.
Faults to Consider:	Valve element not actuating or de-actuating properly. A slow or sticking valve can affect response time of the safety system. Leakage or improper sealing of components including downstream devices will cause motion.
Fault Exclusion:	None to consider.
Safety Principles:	Monitoring the position of the valve can improve reliability.

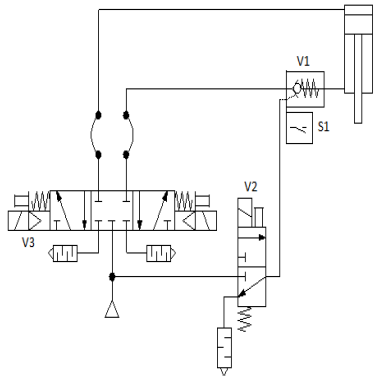
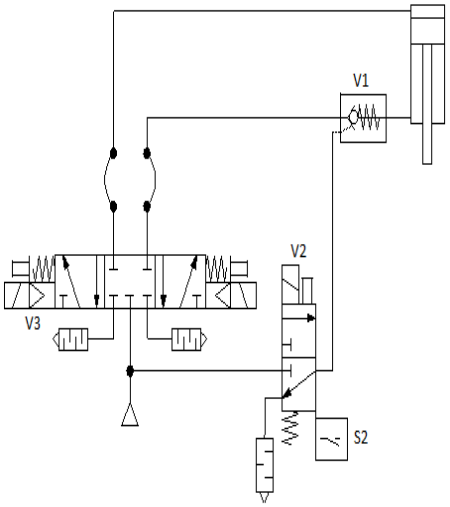
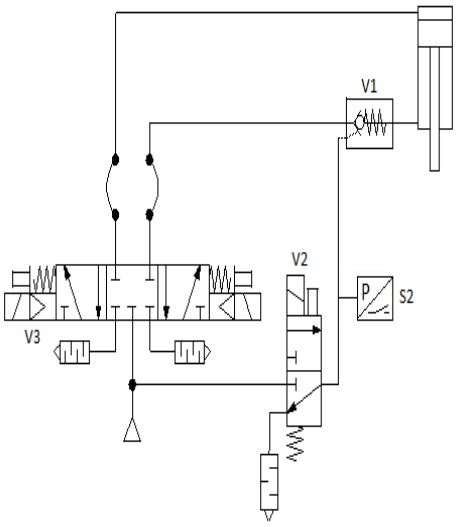
11.3.14.3 Stop (Load Holding) Pilot Operated Check Valve with Integrated Sensor (Category 2)

Circuit:	
Safety Function:	Removal of the command signal results in stoppage of hazardous motion and the actuator held in position.
Faults to Consider:	Valve element not actuating or de-actuating properly. A slow or sticking valve can affect the response time of the safety system. Leakage or improper sealing of components including downstream devices will cause motion.
Fault Exclusion:	None to consider.
Safety Principles:	S1 indicates the position of the valve element V1. S1 is monitored by the SRP/CS at regular intervals to ensure that the valve has shifted. When response time is critical, monitor the timing between solenoid actuation/de-actuation and sensor response. Sensor changes state prior to changing flow path. (Leakage cannot be detected).

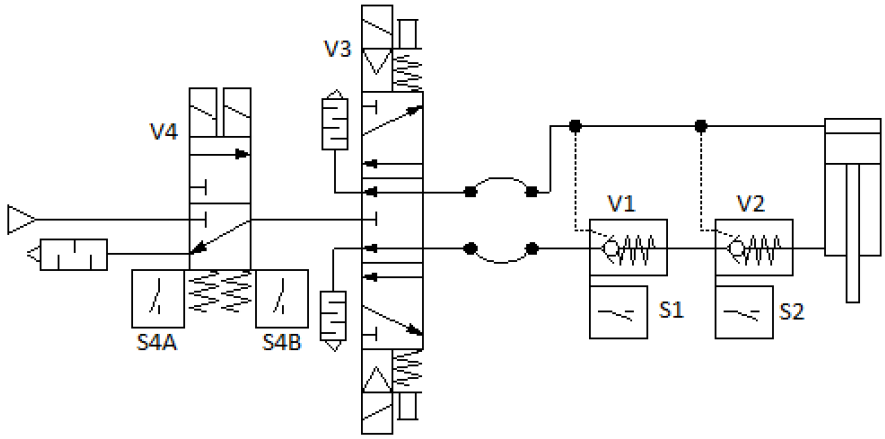
11.3.14.4 Stop (Load Holding) Pilot Operated Check Valve with Actuator Sensor Feedback (Category 2)

Circuit:	
Safety Function:	Removal of the command signal results in stoppage of hazardous motion and the actuator held in position.
Faults to Consider:	Failure of the 3-Position valve to center when solenoid is released. Pilot operated check valve element not actuating or de-actuating properly. A slow or sticking valve can affect the response time of the safety system. Leakage or improper sealing of components including downstream devices will cause motion.
Fault Exclusion:	None to consider.
Safety Principles:	LT1 indicates the position of the cylinder. LT1 is monitored by the SRP/CS at regular intervals to ensure that the valve has shifted. When response time is critical, monitor the timing between solenoid actuation/de-actuation and sensor response.

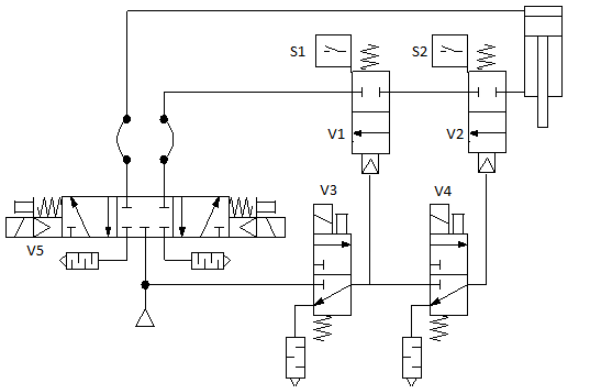
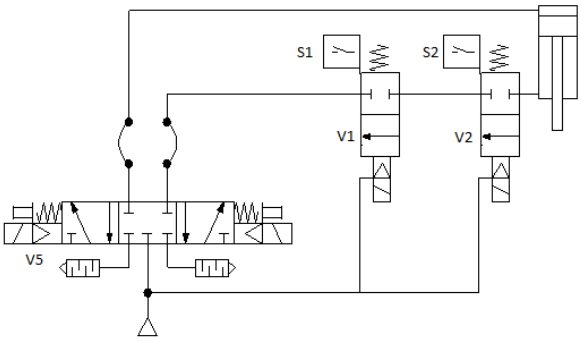
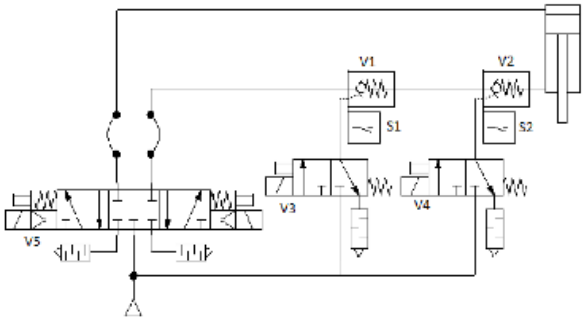
11.3.14.5 Stop (Load Holding) 5/3 Closed Center Valve with Pilot Operated Check Valve with Integrated Sensor (Category 3)

Circuit:	 A  B  C
Safety Function:	Removal of the command signal results in stoppage of hazardous motion and the actuator held in position.
Faults to Consider:	Valve element not actuating or de-actuating properly. A slow or sticking valve can affect the response time of the safety system. Leakage or improper sealing of components including downstream devices will cause motion. 5/3 closed center valves may be subject to internal leakage.
Fault Exclusion:	Example A: none to consider. Example B and Example C: check valve failure.
Safety Principles:	Example A: S1 indicates the position of the valve element V1. Sensors should change state prior to changing flow path. Example B: S2 indicates the position of the valve element V2. Sensors should change state prior to changing flow path. Example C: S2 indicates the position of the valve element V2.The sensor is monitored by the SRP/CS at regular intervals to ensure that the valve has shifted. Sensor changes state prior to changing flow path. When response time is critical, monitor the timing between solenoid actuation/de-actuation and sensor response. V1 Leakage cannot be detected; V3 Monitoring by process

11.3.14.6 Stop (Load Holding) – 5/3 Open Center Valve with Redundant Pilot Operated Check Valve with Integrated Sensors and Safety-Rated Exhaust Valve (Category 3)

Circuit:	 Control valve V3 is not part of the safety function.
Safety Function:	Removal of the command signal results in stoppage of hazardous motion and the actuator held in position.
Faults to Consider:	Valve element not actuating or de-actuating properly. A slow or sticking valve can affect the response time of the safety system. Leakage or improper sealing of components including downstream devices will cause motion.
Fault Exclusion:	None to consider.
Safety Principles:	S1 and S2 indicate the position of the valve elements. S1 and S2 are monitored by the SRP/CS at regular intervals to ensure that the valves have shifted. When response time is critical, monitor the timing between solenoid actuation and sensor response. Sensors change state prior to changing flow path. Leakage cannot be detected. Monitoring to detect the faults of V4.

11.3.14.7 Stop (Load Holding) – 5/3 Open Center Valve with Redundant Pilot Operated Check Valve with Integrated Sensors and Redundant Control Valves (Category 3)

Circuit:	 A  B  C Control valve V5 is not part of the safety function.
Safety Function:	Removal of the command signal results in stoppage of hazardous motion and the actuator held in position.
Faults to Consider:	Valve element not actuating or de-actuating properly. A slow or sticking valve can affect the response time of the safety system. Leakage or improper sealing of components including downstream devices will cause motion.
Fault Exclusion:	None to consider.
Safety Principles:	S1 and S2 indicate the position of the valve elements V1 and V2. S1 and S2 are monitored by the SRP/CS at regular intervals to ensure that the valves have shifted. Sensors change state prior to changing flow path. When response time is critical, monitor the timing between solenoid actuation and sensor response. Leakage cannot be detected.

11.3.15 Rod locks / brakes

11.3.15.1 Design Requirements

When the control signal is removed, the pressure will be removed from the rod lock / brake and the spring will engage the mechanism to hold the actuator rod in place.

Informative Note: *For the purposes of this standard, "rod lock" and "rod brake" are used interchangeably.*

11.3.15.2 Design Considerations

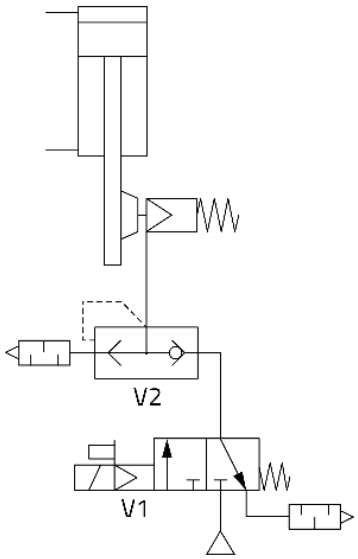
Potential hazards include continuing motion and potential drift.

Potential hazard severity can be reduced to an acceptable level but not eliminated.

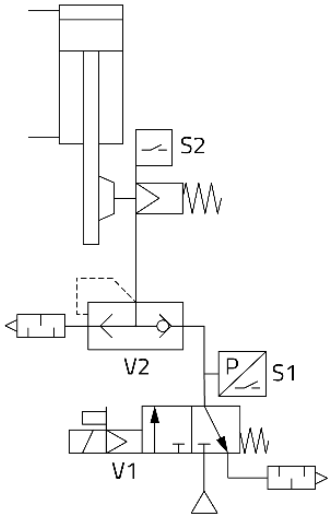
Monitoring can be done via direct monitoring of the internal element or monitoring actuator motion.

The components selected shall be rated by the manufacturer for the intended application, i.e., dynamic stopping, static load holding, or cylinder force vs. gravity load.

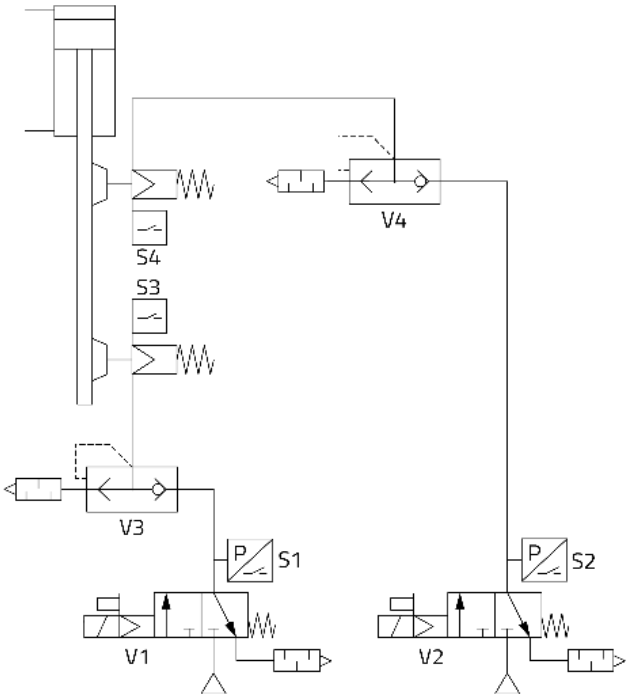
11.3.15.3 Rod Locks / brakes – 3/2 Normally Closed Valve (Category 1)

Circuit:	 Quick exhaust valve V2 (Optional) Recommended if improved response time is required.
Safety Function:	When the electrical command signal is removed, the pressure will be removed from the rod lock / brake and the spring will engage the mechanism to hold the actuator rod in place.
Faults to Consider:	Valve element not actuating or de-actuating properly. Rod Lock element not actuating or de-actuating properly. A slow or sticking valve can affect response time of the safety system. Leakage or improper sealing of components including downstream devices will cause motion.
Fault Exclusion:	None to consider.
Safety Principles:	Monitoring can improve the reliability.

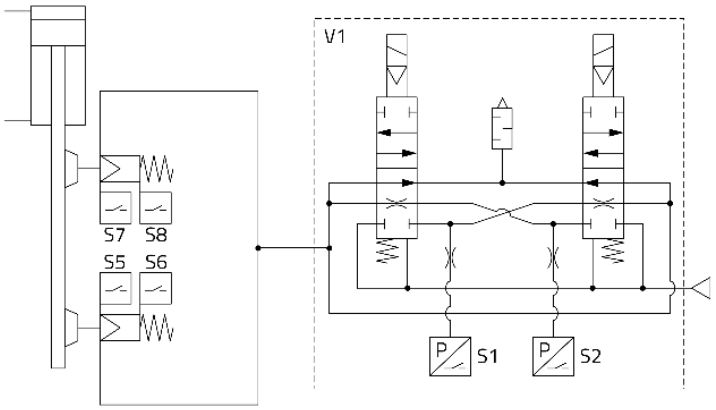
11.3.15.4 Rod Locks / Brakes – 3/2 Normally Closed Valve with Pressure feedback and Safety-Rated Rod Lock with position feedback (Category 2)

Circuit:	 Quick exhaust valve V2 (Optional) Recommended if improved response time is required.
Safety Function:	When the electrical command signal is removed, the pressure will be removed from the rod lock / brake and the spring will engage the mechanism to hold the actuator rod in place.
Faults to Consider:	Valve element not actuating or de-actuating properly. Rod Lock elements are not actuating or de-actuating properly. A slow or sticking valve can affect response time of the safety system. Leakage or improper sealing of components including downstream devices will cause motion.
Fault Exclusion:	None to consider.
Safety Principles:	S2 indicates the position of the rod lock. S1 and S2 indicate the position of the valve elements V1 and V2. S1 and S2 are monitored by the SRP/CS at regular intervals to ensure that the valves have shifted.

11.3.15.5 Rod locks / brakes – Redundant 3/2 Normally Closed Valve with Pressure feedback and Redundant Safety-Rated Rod Lock with position feedback (Category 3)

Circuit:	 Quick exhaust valves V3, V4 (Optional) Recommended if improved response time is required.
Safety Function:	When the electrical command signal is removed, the pressure will be removed from the rod lock / brake and the spring will engage the mechanism to hold the actuator rod in place.
Faults to Consider:	Valve element not actuating or de-actuating properly. Rod Lock elements are not actuating or de-actuating properly. A slow or sticking valve can affect response time of the safety system. Leakage or improper sealing of components including downstream devices will cause motion.
Fault Exclusion:	None to consider.
Safety Principles:	S3 and S4 indicate the position of the rod lock. S1, S2, S3 and S4 indicate the position of the valve elements V1, V2, V3 and V4. S1, S2, S3 and S4 are monitored by the SRP/CS at regular intervals to ensure that the valves have shifted.

11.3.15.6 Rod Locks / Brakes – Redundant 3/2 Normally Closed Safety-Rated Dual Valve with Sensors, Automatic Reset and Redundant Safety-Rated Rod Lock with Dual position feedback (Category 4)

Circuit:	 V1 to be mounted as close as possible to Rod Locks to minimize response time degradation.
Safety Function:	When the electrical command signal is removed, the pressure will be removed from the rod lock / brake and the spring will engage the mechanism to hold the actuator rod in place.
Faults to Consider:	Valve element not actuating or de-actuating properly. Rod Lock elements are not actuating or de-actuating properly. A slow or sticking valve can affect response time of the safety system. Leakage or improper sealing of components including downstream devices will cause motion.
Fault Exclusion:	Trapping of air to the brakes through the use of appropriate pipes and fittings for the application.
Safety Principles:	S5 - S8 indicates the position of the rod locks. S1 – S2 indicate the pressure supplied by V1. All sensors are monitored by the SRP/CS at regular intervals or when there is a demand of the safety function to ensure that the valves and rod locks have shifted. A single fault is detected at or before the next demand upon the safety function. Non-synchronous movement of the independent valve elements while actuating or de-actuating is monitored by the SRP/CS and results in a fault condition (diminished performance fault). To achieve up to Category 4, monitor sensors in parallel.

11.3.16 Flow Control

11.3.16.1 Design Requirements

Flow controls are used to control the actuator speed. They can be used to limit the flow into a port causing the actuator to build pressure and move at a limited rate. The flow control can also be used to limit the flow out of an actuator when being exhausted. This only reduces speed when air pressure is present on the downstream side of the actuator.

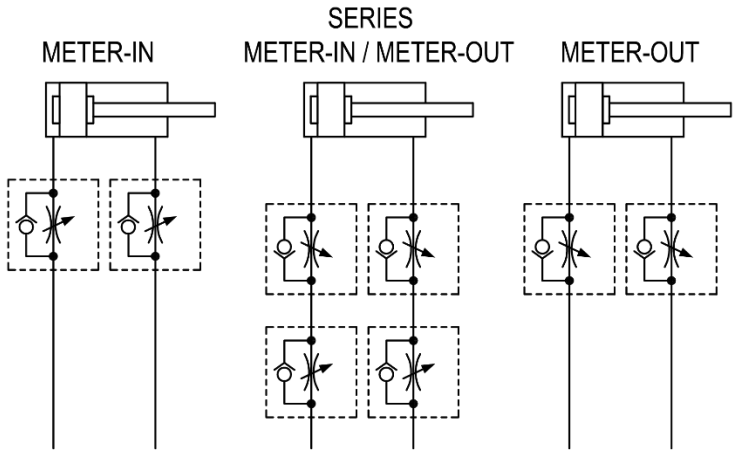
When the reapplication of pressure occurs after an energy isolation event, meter-in flow controls can be used to limit the flow into the cylinder to prevent the rapid acceleration that will occur when there is an absence of pressure in the opposite end of the actuator.

11.3.16.2 Design Considerations

On applications with over running loads, limiting the flow both into and out of an actuator may be the most appropriate solution. This reduces or eliminates the rapid advance caused by lack of air in an exhausted meter-out circuit and allows for braking of fast-moving applications where inertia is a factor.

Meter-in flow controls shall be used on all applications where the cylinder lines are exhausted, either by the safety valve, or by the directional control valve.

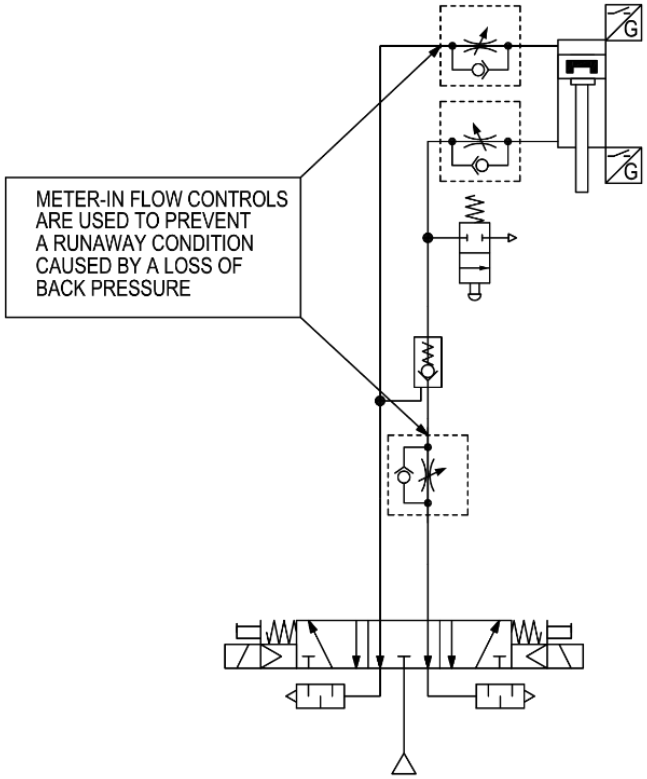
Meter-out flow controls are used to prevent rapid movement (extension or retraction) of the cylinder rod in the event of a mechanical jam or loss of supply air, either of which would vent the back pressure on an exhaust speed control.



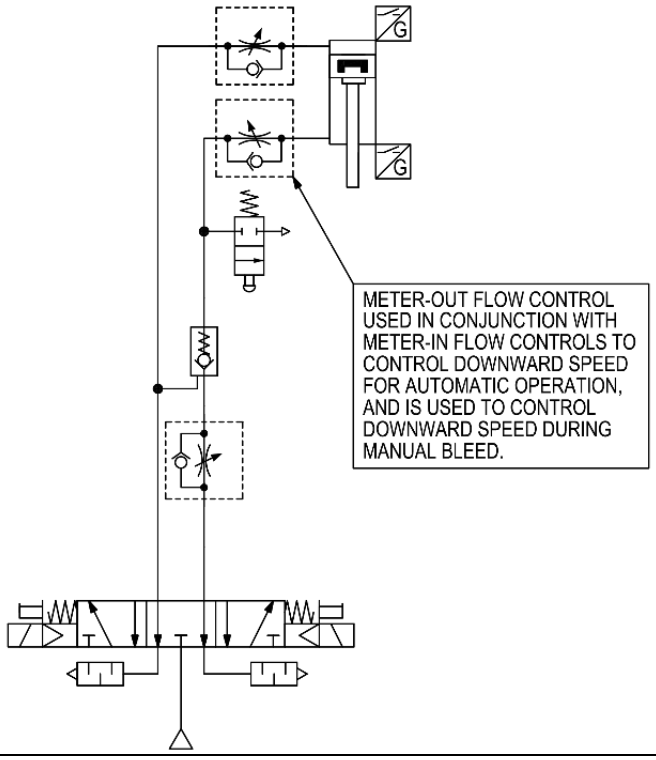
Meter-IN – Controls the fluid flow going into the cylinder after air has been exhausted from both actuator lines. This method can result in slip-stick or jerky motions while moving large bore actuators slowly.

Meter-OUT – Controls the fluid flow coming out of the cylinder with a slightly better control of slow-moving actuators. The actuator velocity can be extremely fast if both cylinder lines have been exhausted, or if the cylinder motion has been stalled while under pressure, as the compressed air that is normally used for speed control has been removed.

11.3.16.3 Flow Control – Meter Out Flow Control Example

Circuit:	
Safety Function:	Control the flow causing the actuator to move at a limited rate.
Faults to Consider:	Operator adjustment. Flow control check valve can get stuck open due to contamination, resulting in an increase in actuator speed. Due to the air compressibility and depending on differences between friction and sliding friction forces, flow-in only can result in intermittent incremental advance until full stroke is reached. Rapid unexpected motion can occur when the downstream air has been removed from the actuator.
Fault Exclusion:	None to consider.
Safety Principles:	Meter-IN and/or Meter-OUT prevent rapid movement of the cylinder rod.

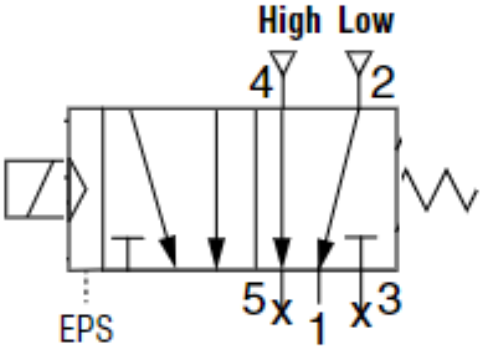
11.3.16.4 Flow Control – Meter Out Flow Control Example

Circuit:	
Safety Function:	Control the flow causing the actuator to move at a limited rate.
Faults to Consider:	Operator adjustment. Flow control check valve can get stuck open due to contamination, resulting in an increase in actuator speed. Due to the air compressibility and depending on differences between friction and sliding friction forces, flow-in only can result in intermittent incremental advance until full stroke is reached.
Fault Exclusion:	None to consider.
Safety Principles	Meter-OUT prevents rapid movement of the cylinder rod.

11.3.17 Safe Pressure (force) Selection

11.3.17.1 Design Requirements

When the electrical command signal is removed, the pressure at the application shall be reduced to an acceptable level.



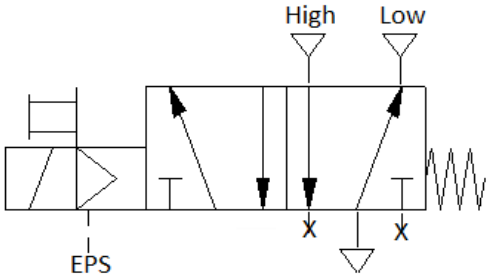
11.3.17.2 Design Considerations

Potential hazard severity can be reduced to an acceptable level but not eliminated.

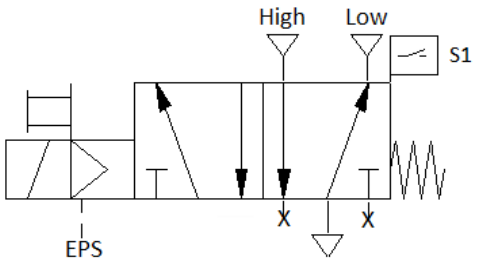
Additional hazards shall be considered including higher pressure is maintained in the system.

Monitoring can be done via direct monitoring of the internal element or indirect monitoring of the downstream pressures.

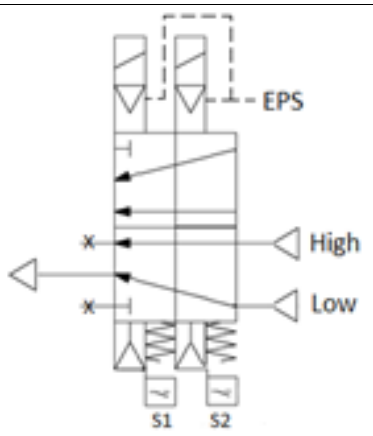
11.3.17.3 Safe pressure (force) selection - 5/2 Valve (Category 1)

Circuit:	
Safety Function:	When the electrical command signal is removed, the pressure at the application will be reduced to an acceptable level.
Faults to Consider:	Valve element not actuating or de-actuating properly. A slow or sticking valve can affect response time of the safety system. Higher pressure is maintained downstream.
Fault Exclusion:	None to consider.
Safety Principles:	Monitoring safety position can improve reliability.
Residual Risk:	Higher pressure is maintained downstream.

11.3.17.4 Safe pressure (force) selection - 5/2 Valve with Integrated Sensor (Category 2)

Circuit:	
Safety Function:	When the electrical command signal is removed, the pressure at the application will be reduced to an acceptable level.
Faults to Consider:	Valve element not actuating or de-actuating properly. A slow or sticking valve can affect response time of the safety system. Higher pressure is maintained downstream.
Fault Exclusion:	None to consider.
Safety Principles:	S1 indicates the position of the valve element. S1 is monitored by the SRP/CS at regular intervals to ensure that the valve has shifted. Sensor changes state prior to changing flow path. When response time is critical, monitor the timing between solenoid actuation/de-actuation and sensor response.

11.3.17.5 5/2 Safe Valve Position/Direction (Safe Return) – Safety-Rated Dual Valve with Integrated Sensors (Category 4)

Circuit:	
Safety Function:	When the electrical command signal is removed, the pressure at the application will be reduced to an acceptable level.
Faults to Consider:	Loss of supply pressure.
Fault Exclusion:	None to consider.
Safety Principles:	The spring returns the valve to the home position. Sensors which indicate the position of the valve elements. Sensors are monitored by the SRP/CS at regular intervals or when there is a demand of the safety function to ensure that the valves have shifted. A single fault is detected at or before the next demand upon the safety function. Non-synchronous movement of the independent elements while actuating or de-actuating is monitored by the SRP/CS and results in a fault condition (diminished performance fault). Sensors change state prior to changing flow path. To achieve up to Category 3, sensors may be monitored in series. To achieve up to Category 4, monitor sensors in parallel.

11.3.18 Velocity Fuse

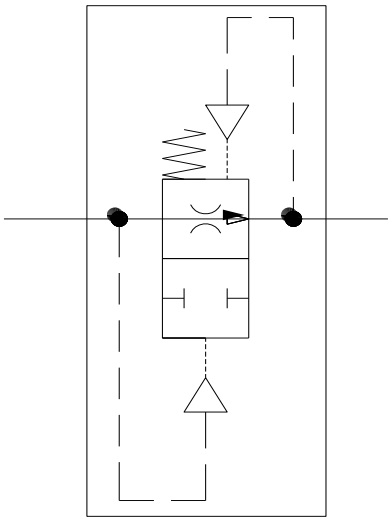
11.3.18.1 Design Requirements

A velocity fuse is a device that will automatically react to the sudden loss of pressure that occurs when a downstream hose or fitting is disconnected or broken. The sudden loss of pressure will result in an unsecured hose whipping around, potentially causing injuries or damage unless a velocity fuse is installed.

11.3.18.2 Design Considerations

The device shall be installed on the supply side of the hose to prevent whipping action from occurring. When used on vertical loads to prevent rapid lowering during a conductor failure, the device shall be installed directly into the actuator port.

11.3.18.3 Velocity fuse (Category 1)

Circuit:	
Safety Function:	A velocity fuse is a device that will automatically react to the sudden loss of pressure that occurs when a downstream hose or fitting is disconnected or broken.
Faults to Consider:	Valve element can stick causing a failure to stop the whipping as intended.
Fault Exclusion:	None to consider.
Safety Principles:	Well-tried components suitable for the application.

11.4 Hydraulic Systems

11.4.1 Hydraulic Design Requirements

Hydraulic circuits use hydraulic fluid to transfer energy to perform work. This energy must be properly managed and conditioned to minimize or eliminate hazards associated with component failures and the release of stored energy. To effectively mitigate these hazards, risk assessment of the hydraulic design process shall include the following steps:

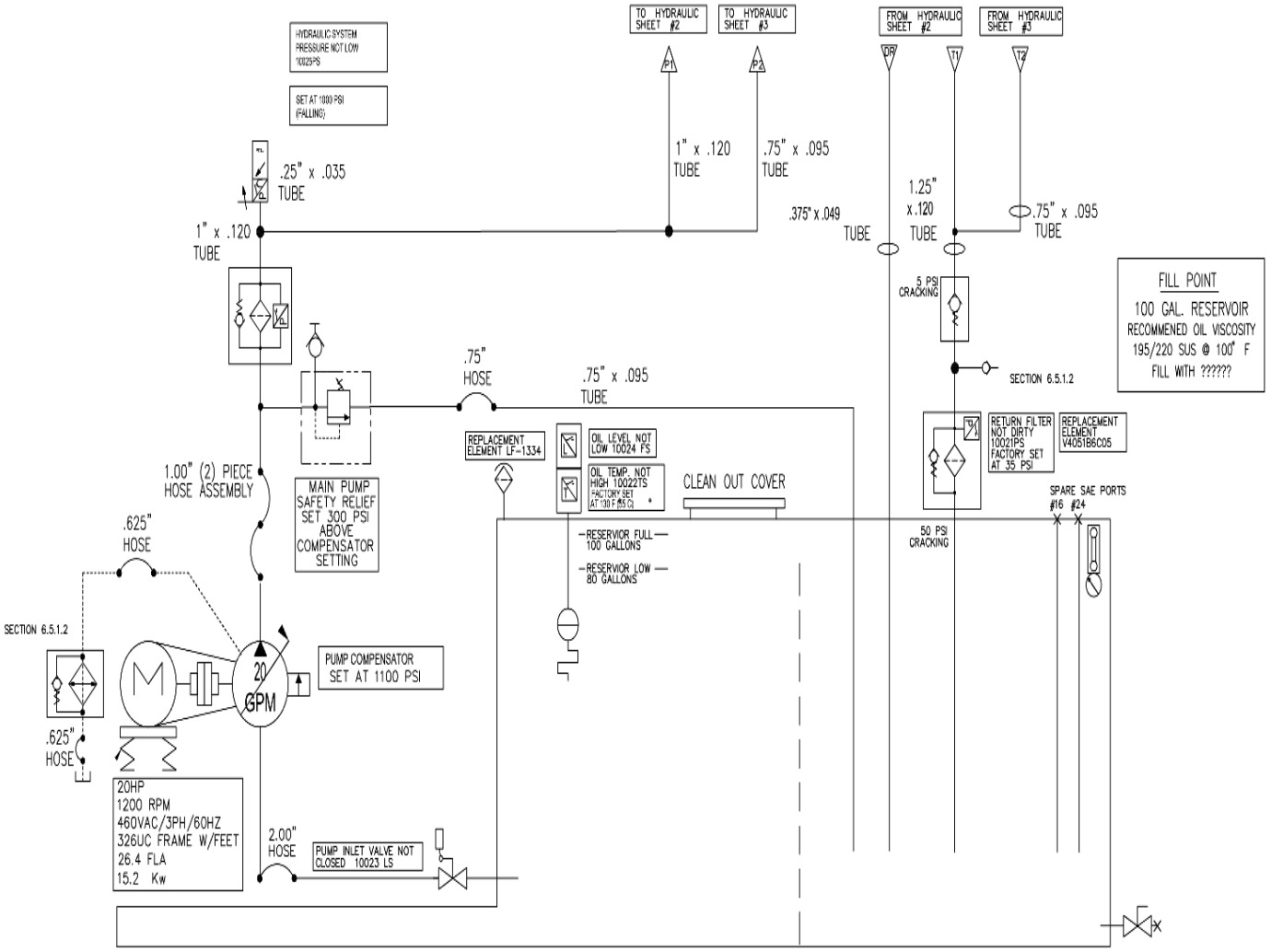
- Determine hazards presented by motions powered by hydraulic energy and other hazards associated with a fluid under pressure;
- Select the appropriate fluid preparation components based on the required contamination control filtration level required;
- Determine if a blocking valve is required to isolate or remove energy;
- Select the appropriate valve performance based on the risk Category requirements;
- Select the motion valve most appropriate for the application(s);
- If a vertical load needs to be held in place, select a pilot operated check or counter-balance valve;
- If the load needs to be stopped or held by mechanical means, select the appropriate lock, brake, or equivalent mechanical device;
- Additional hydraulic support means may also be required;
- If speed control is required or the re-application of pressure can create a hazard, select the appropriate flow control solution;
- Evaluate each remaining risk to determine whether or not it is tolerable.

The following hydraulic examples use direct acting valves which represent the majority of valves used in industry for flows less than 20 GPM. Direct acting valves have fewer failure modes than pilot operated valves regarding a valve's ability to initiate a motion without being given an electrical command signal.

11.4.2 Fluid Preparation (Contamination Control)

A fluid power circuit‘s reliability is influenced by contamination, also known as its cleanliness level. Select fluid conditioning components appropriate for the intended level of reliability. Strict adherence to the proper conditioning of the fluid power source can increase the mean time to dangerous failure.

A pilot operated valves design should be evaluated to determine if there are failure modes which would initiate a motion and what addition controls might need to be installed to mitigate this risk. Both valve types have similar failure modes regarding a valve’s inability to return to the de-energized position, but the pilot operated valves have an additional concern and that is the potential inability of the valve to exhaust or drain the pilot pressure preventing the main spool from returning.

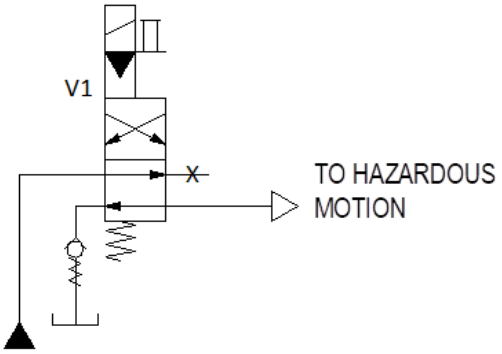


Safety Function:	Proper pre-filtering conditions the incoming fluid supply increasing the circuit‘s reliability. Filtration requirements as defined by ISO 4406. Safety valve(s) - Use and implement as determined by the risk assessment.
Faults to Consider:	Filter failure, high fluid temperature, ingression or poor maintenance will pass contamination to the system causing premature failure of components and potentially invalidate the vendor‘s mean time to failure data. Regulator failure or improper adjustment can cause excessive pressures in the system.
Fault Exclusion:	None to consider.
Safety Principles:	The application of the principles above will greatly increase the mean time to dangerous failure and are applicable to all levels of design.

11.4.3 Dump and Block Fluid to the Hazardous Motion

11.4.3.1 Design Requirements

When the electrical command signal is removed, fluid supply pressure shall be blocked, and pressure dissipated from the hazardous motion.



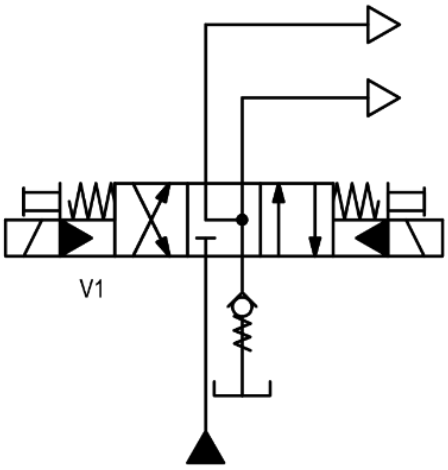
11.4.3.2 Design Considerations

Potential hazardous failures include the failure to block and dissipate pressure.

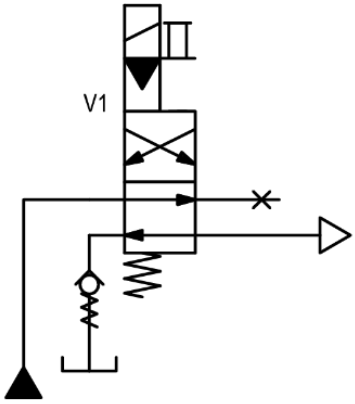
Residual risk including motion caused by gravity or the reapplication of pressure shall be considered.

Monitoring can be done via direct monitoring of the internal element, indirect monitoring of the downstream pressure, or monitoring of the process if the valve is controlling a single actuator such as a single acting cylinder.

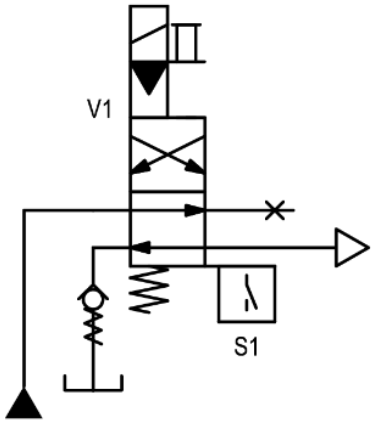
11.4.3.3 Dump and Block - 5/3 Open Center (Float Center) Valve (Category 1)

Circuit:	
Safety Function:	When the electrical command signal is removed, fluid supply pressure is blocked, and pressure is dissipated from the hazardous motion.
Faults to Consider:	Leakage or improper sealing of components. Valve element not actuating or de-actuating properly. A slow or sticking valve can affect response time of the safety system.
Fault Exclusion:	None to consider.
Safety Principles:	The continued function of the machine may not indicate the ability of the valve to spring center and remove energy. Test the ability for the directional valve to stop the motion by centering at regular intervals.

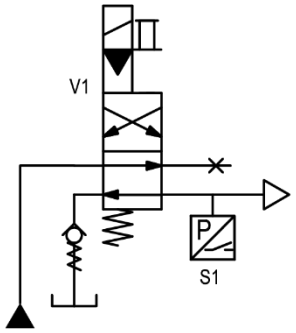
11.4.3.4 Dump and Block - 4/2 Valve (Category 1)

Circuit:	
Safety Function:	When the electrical command signal is removed, fluid supply pressure is blocked, and pressure is dissipated from the hazardous motion.
Faults to Consider:	Leakage or improper sealing of components. Valve element not actuating or de-actuating properly. A slow or sticking valve can affect response time of the safety system.
Fault Exclusion:	None to consider.
Safety Principles:	Monitoring can improve reliability.

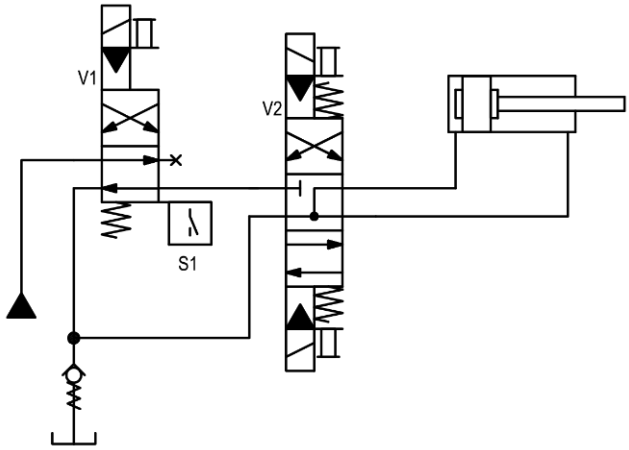
11.4.3.5 Dump and Block - 4/2 Valve with Integrated Sensor (Category 2)

Circuit:	
Safety Function:	When the electrical command signal is removed, fluid supply pressure is blocked, and pressure is dissipated from the hazardous motion.
Faults to Consider:	Leakage or improper sealing of components. Valve element not actuating or de-actuating properly. A slow or sticking valve can affect response time of the safety system.
Fault Exclusion:	None to consider.
Safety Principles:	S1 indicates the position of the valve element in the flow to output state. S1 is monitored by the SRP/CS at regular intervals to ensure that the valve has shifted. Sensor changes state prior to allowing flow. When response time is critical, monitor the timing between solenoid actuation/de-actuation and sensor response.

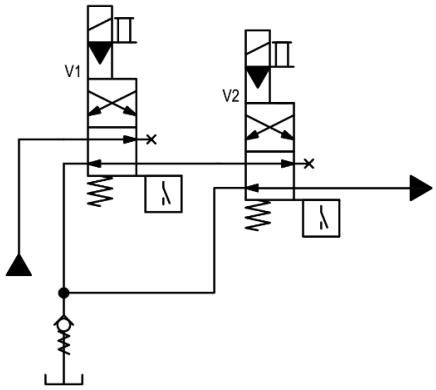
11.4.3.6 Dump and Block - 4/2 Valve with Pressure Sensor (Category 2)

Circuit:	
Safety Function:	When the electrical command signal is removed, fluid supply pressure is blocked, and pressure dissipated from the hazardous motion.
Faults to Consider:	Leakage or improper sealing of components. Valve element not actuating or de-actuating properly. A slow or sticking valve can affect response time of the safety system.
Fault Exclusion:	None to consider.
Safety Principle:	S1 indicates downstream pressure and shall be set to a safe pressure level. S1 is monitored by the SRP/CS at regular intervals to ensure that the valve has shifted. When response time is critical, monitor the timing between solenoid actuation/de-actuation and sensor response.

11.4.3.7 Dump and Block – 3/2 Normally Closed Valve with Integrated Sensor in Series with 5/3 Open Center (Float Center) Valve (Category 3)

Circuit:	
Safety Function:	When the electrical command signal is removed, fluid supply pressure is blocked, and pressure is dissipated from the hazardous motion.
Faults to Consider:	Leakage or improper sealing of components.
Fault Exclusion:	None to consider.
Safety Principles:	S1 indicates the position of the valve element V1 in the flow to output state. S1 is monitored by the SRP/CS at regular intervals to ensure that the valve has shifted. S1 changes state prior to allowing flow. 5/3 Open Center valve is monitored indirectly or by the process (monitoring not shown). The continued function of the machine may not indicate the ability of the valve to spring center and remove energy. Test the ability of the directional valve to stop the motion by centering at regular intervals.

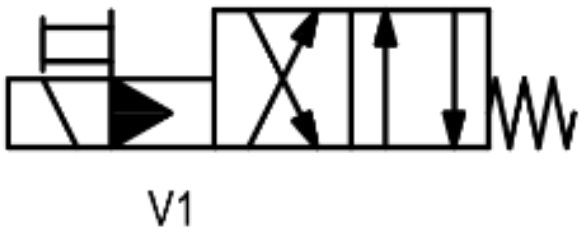
11.4.3.8 Dump and Block – Redundant 4/2 Valve with Integrated Sensor in Series (Category 3 or 4)

Circuit:	
Safety Function:	When the electrical command signal is removed, fluid supply pressure is blocked, and pressure is dissipated from the hazardous motion.
Faults to Consider:	Leakage or improper sealing of components.
Fault Exclusion:	None to consider.
Safety Principles	Sensors which indicate the position of the valve elements, are directly operated by the elements in the flow to output state. Sensors are monitored by the SRP/CS at regular intervals or when there is a demand of the safety function to ensure that the valves have shifted. A single fault is detected at or before the next demand upon the safety function. Non-synchronous movement of the independent elements while actuating or de-actuating is monitored by the SRP/CS and results in a fault condition (diminished performance fault). Sensors change state prior to allowing flow. When response time is critical, monitor the timing between solenoid(s) actuation/de-actuation and sensor(s) response. To achieve up to Category 3, sensors may be monitored in series. To achieve up to Category 4, monitor sensors in parallel.

11.4.4 Return

11.4.4.1 Design Requirements

When the electrical command signal is removed, the hazardous motion shall reverse and continue until the end of stroke is reached.



11.4.4.2 Design Considerations

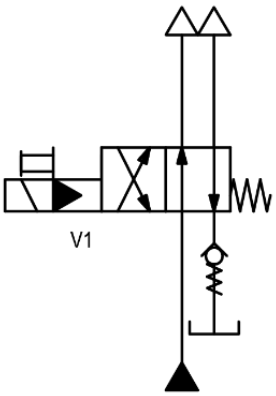
Potential hazardous failures include failure to unshift continuing motion in the hazardous direction, or a slow response causing motion to continue in the hazardous direction for a short period of time.

Additional hazards including pinch points on the return stroke or motion caused by the loss of supply pressure shall be considered.

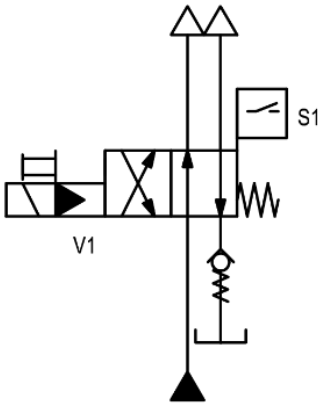
Monitoring can be done via direct monitoring of the internal element, indirect monitoring of the downstream pressures, or monitoring by process of the actuator being controlled.

Informative Note: *End of stroke monitoring will not indicate a hazardous failure until the potentially hazardous event has occurred.*

11.4.4.3 4/2 Valve (Category 1)

Circuit:	
Safety Function:	When the electrical command signal is removed, the hazardous motion reverses and continues until the end of stroke is reached.
Faults to Consider:	Valve element not actuating or de-actuating properly. A slow or sticking valve can affect response time of the safety system. Hazardous motion continues. Loss of supply pressure allows movement.
Fault Exclusion:	None to consider.
Safety Principles:	Monitoring can improve the reliability.

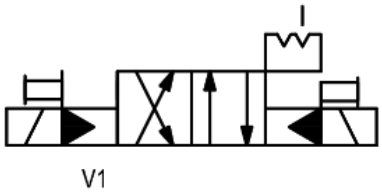
11.4.4.4 4/2 Valve with Integrated Sensor (Category 2)

Circuit:	
Safety Function:	When the electrical command signal is removed, the hazardous motion reverses and continues until the end of stroke is reached.
Faults to Consider:	Valve element not actuating or de-actuating properly. A slow or sticking valve can affect response time of the safety system.
Fault Exclusion:	None to consider.
Safety Principles:	S1 indicates the position of the valve element. S1 is monitored by the SRP/CS at regular intervals to ensure that the valve has shifted. S1 changes state prior to changing flow path. When response time is critical, monitor the timing between solenoids actuation/de-actuation and sensors response.

11.4.5 Maintain End of Stroke Position

11.4.5.1 Design Considerations

When the electrical command signal is removed, the hazardous motion shall continue in the direction initiated, or dwell in its current end of travel location. Designs should be limited to short strokes or actuators where a loss of pressure would not lead to a hazard.

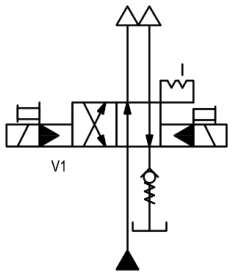


11.4.5.2 Design Considerations

Potential hazards include continued motion or reversal of motion without stopping. Additional hazards including motion in either direction creating pinch points shall be considered.

Monitoring can be done via direct monitoring of the internal element, indirect monitoring of the downstream pressures, or monitoring by process of the actuator being controlled.

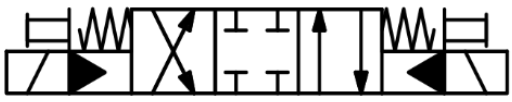
11.4.5.3 4/2 Detented Valve (Category 1)

Circuit:	
Safety Function:	When the electrical command signal is removed, the hazardous motion continues in the direction initiated, or dwells in its current end of travel location.
Faults to Consider:	Valve element not actuating or de-actuating properly. A slow or sticking valve can affect response time of the safety system.
Fault Exclusion:	None to consider.
Safety Principles:	Monitoring can improve reliability.

11.4.6 Control and Stop/Hold

11.4.6.1 Design Requirements

When the electrical command signal is removed, the hazardous motion shall be halted and the actuator held in its present position.



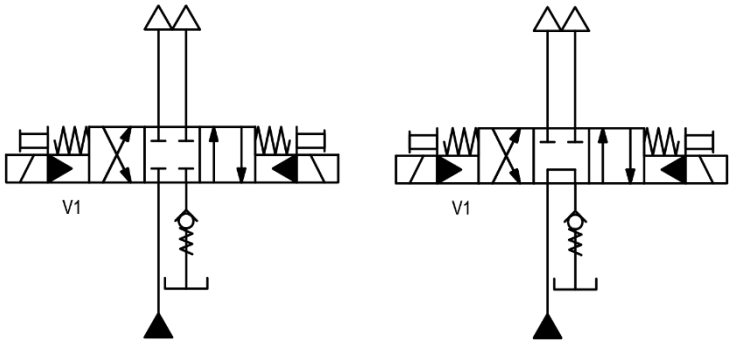
11.4.6.2 Design Considerations

Potential hazards include continuing motion or the reversal of motion and potential drift. Additional hazards, including motion in either direction creating pinch points and trapped pressure in the system, shall be considered.

Monitoring can be done via direct monitoring of the internal element, indirect monitoring of the downstream pressures, or monitoring by process of the actuator being controlled.

Informative Note: *End of stroke monitoring will not indicate a hazardous failure until the potentially hazardous event has occurred.*

11.4.6.3 Control and Stop/Hold – 4/3 Closed Center or Tandem Center Valve (Category 1)

Circuit:	
Safety Function:	When the electrical command signal is removed, the hazardous motion stops, and the actuator is held in its present position.
Faults to Consider:	Valve element not actuating or de-actuating properly. A slow or sticking valve can affect response time of the safety system.
Fault Exclusion:	None to consider.
Safety Principles	Monitoring can improve reliability.

11.4.7 Load Holding - Spring Return Blocking and Pilot Operated Check Valves

Solenoid blocking valves are used to trap or store energy (hydraulic pressure) in the actuator(s) to maintain position. This energy typically is not removed by turning off the hydraulic power unit.

Spring return blocking valves on the exhaust side of a vertical actuator maintain the actuator position by trapping fluid under the actuator piston. Seal leaks, piston seal, rod seal, fittings or line leaks can cause a lowering motion that needs to be considered during the risk assessment.

Solenoid or Pilot Operated Check valves may also be used to trap or store energy (hydraulic pressure) in the actuator(s) to maintain position. This energy is typically not removed by the check valve, nor by turning off the power unit. Note that the check valve functions only in the exhaust flow path. When the directional control valve shifts to pressurize the line into the check valve, it will cause the actuator to move in the opposite direction. Thus, the check valve provides fluid control only in the exhaust mode. See the example circuit in 11.4.7.5.

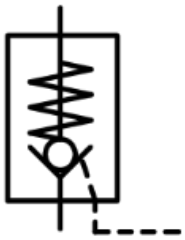
Pilot operated checks maintain a vertical actuator position by trapping fluid between the actuator piston and the check. Their application should be limited to light loads. PO check seal leaks, piston seal, rod seal, fittings or line leaks can cause a lowering motion that needs to be considered during the risk assessment.

The pilot pressure supply can directly affect the closing of the check which can impact the stop time/distance of the actuator. The pilot supply shall be connected downstream of the safety blocking valve.

When the rod end line of a cylinder can be blocked (due to a failure in any of the components in that line) or restricted, the design shall be capable of withstanding the pressure intensification from supply pressure at the cap end acting on the differential area. Hydraulic intensification on single rod cylinders and pressure spikes caused by quickly stopping a moving load shall also be considered as one of the failure modes. Where these conditions exist, consider the use of a counter-balance valve since it may safely reduce the pressure by venting the intensified pressure to drain. See 11.4.8.

11.4.7.1 Design Requirements

When the command signal is removed, the hazardous motion shall be halted and the actuator held in its present position.



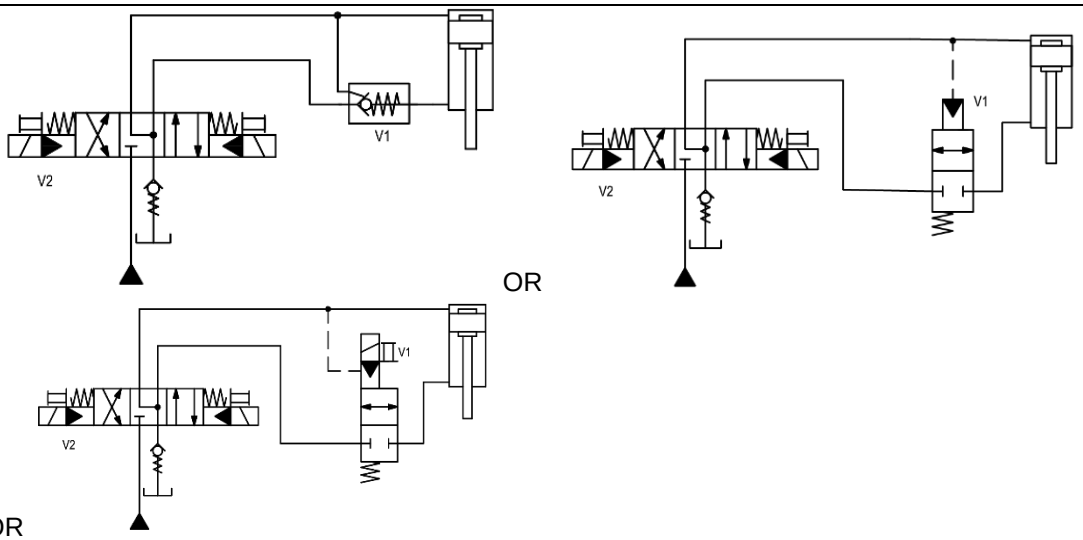
11.4.7.2 Design Requirements

Potential hazards include motion continuing or the reversal of motion and potential drift. Additional hazards include motion in either direction creating pinch points and trapped pressure in the system shall be considered.

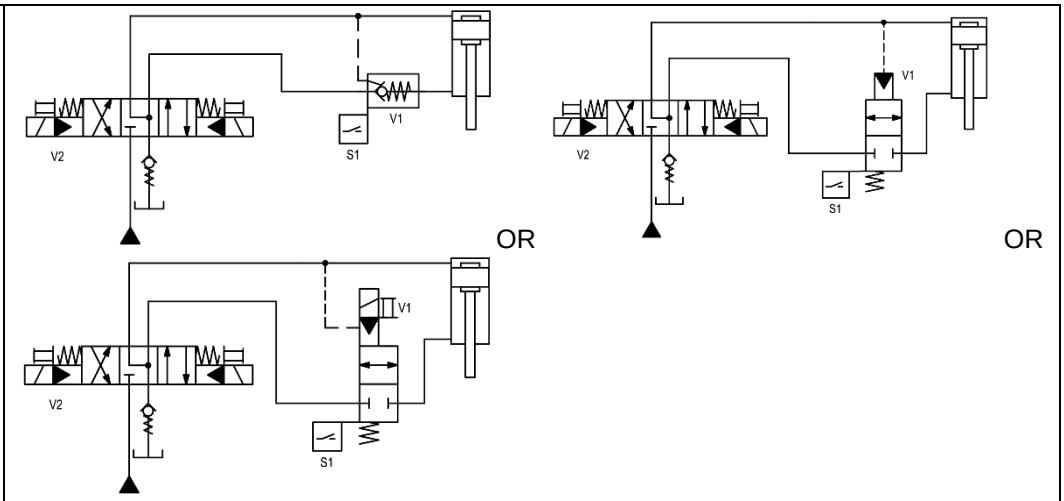
Monitoring can be done via direct monitoring of the internal element, indirect monitoring of the downstream pressures, or monitoring by process of the actuator being controlled.

Informative Note: *Direct position sensing may not indicate leakage in the valve or system.*

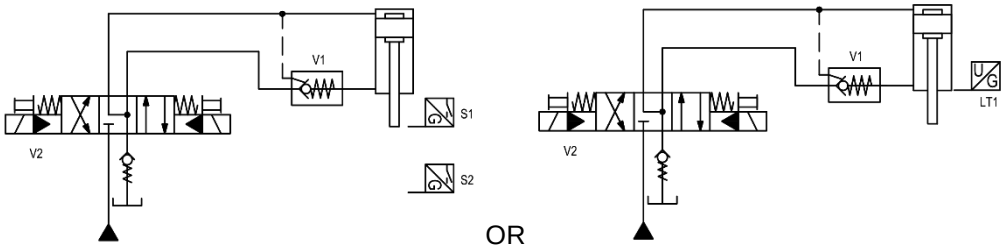
11.4.7.3 Load Holding – Pilot Operated Check Valve or 2/2 Normally Closed Valve (Category 1)

Circuit:	
Safety Function:	When the command signal is removed, the hazardous motion stops, and the actuator is held in its present position.
Faults to Consider:	Valve element not actuating or de-actuating properly. A slow or sticking valve can affect response time of the safety system. Leakage or improper sealing of components including downstream devices will cause motion. Stored energy can cause unexpected motion when released during service.
Fault Exclusion:	None to consider.
Safety Principles	Monitoring can improve reliability.

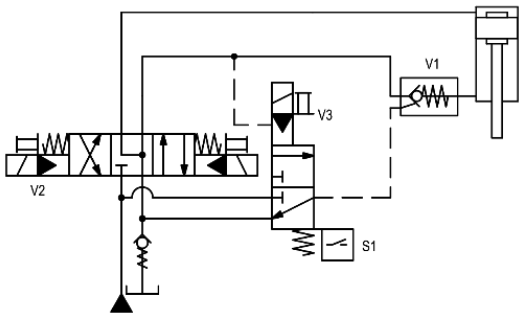
11.4.7.4 Load Holding – Pilot Operated Check Valve or 2/2 Normally Closed with Integrated Sensor (Category 2)

Circuit:	
Safety Function:	When the command signal is removed, the hazardous motion stops, and the actuator is held in its present position.
Faults to Consider:	Valve element not actuating or de-actuating properly. A slow or sticking valve can affect the response time of the safety system. Leakage or improper sealing of components including downstream devices will cause motion. Stored energy can cause unexpected motion when released during service.
Fault Exclusion:	None to consider.
Safety Principles:	S1 indicates the position of the valve element V1. S1 is monitored by the SRP/CS at regular intervals to ensure that the valve has shifted. S1 changes state prior to changing flow path. When response time is critical, monitor the timing between solenoids actuation/de-actuation and sensors response. Leakage cannot be detected.

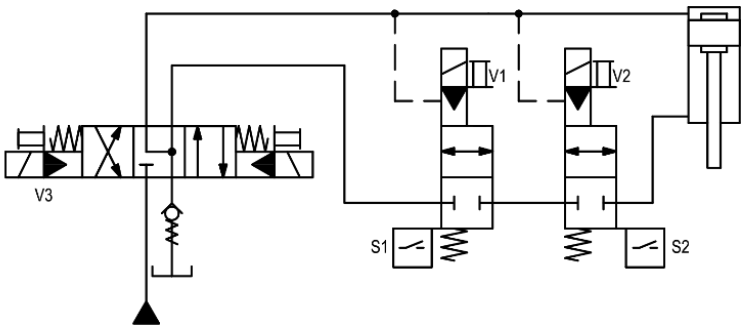
11.4.7.5 Load Holding – Low / Intermediate Risk Reduction Pilot Operated Check Valve or 2/2 Normally Closed with Actuator Sensor Feedback (Category 2)

Circuit:	
Safety Function:	When the command signal is removed, the hazardous motion stops, and the actuator is held in its present position.
Faults to Consider:	Valve element not actuating or de-actuating properly. A slow or sticking valve can affect the response time of the safety system. Leakage or improper sealing of components including downstream devices will cause motion. Stored energy can cause unexpected motion when released during service.
Fault Exclusion:	None to consider.
Safety Principles:	S1 and S2 (or LT1) indicate the position of the actuator. S1 and S2 (or LT1) are monitored by the SRP/CS at regular intervals to ensure that the valve has shifted. The continued function of the machine may not indicate the ability of the valve to spring center and remove energy. The ability of the directional valve to stop the motion by centering is tested at regular intervals.

11.4.7.6 Load Holding – Pilot Operated Check Valve or 2/2 Normally Closed with Integrated Sensor (Category 2)

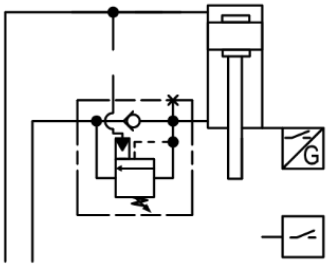
Circuit:	
Safety Function:	When the command signal is removed, the hazardous motion stops, and the actuator is held in its present position.
Faults to Consider:	Valve element not actuating or de-actuating properly. A slow or sticking valve can affect the response time of the safety system. Leakage or improper sealing of components including downstream devices will cause motion. Stored energy can cause unexpected motion when released during service.
Fault Exclusion:	Check valve failure.
Safety Principles:	S1 indicates the position of the valve element V3. S1 is monitored by the SRP/CS at regular intervals to ensure that the valve has shifted. S1 changes state prior to changing flow path. When response time is critical, monitor the timing between solenoids actuation/de-actuation and sensors response.

11.4.7.7 Load Holding – 5/3 Closed Center Valve with Redundant Pilot Operated Check Valves or 2/2 Normally Closed Valves w/ Integrated Sensors and Redundant Control Valves (Category 3)

Circuit:	
Safety Function:	When the command signal is removed, the hazardous motion stops, and the actuator is held in its present position.
Faults to Consider:	A slow or sticking valve can affect the response time of the safety system. Leakage or improper sealing of components including downstream devices will cause motion.
Fault Exclusion:	None to consider.
Safety Principles:	S1 and S2 indicate the position of the valve elements V1 and V2. S1 and S2 are monitored by the SRP/CS at regular intervals to ensure that the valves have shifted. Sensors change state prior to changing flow path. When response time is critical, monitor the timing between solenoids actuation/de-actuation and sensors response.

11.4.8 Load Holding – Counter-balance Valves

In addition to trapping the fluid in the actuator, the counter-balance valve has a relief function that will prevent pressure intensification and allow for braking. Since the pressure relief setting is adjustable, the valve shall be set 300 PSI above that required to suspend the load. The load shall be supported or lowered before releasing the trapped pressure. A means of relieving the trapped pressure shall be provided. Some counter-balance valves are provided with the manual override. The ability of the counter-balance valve to hold the load is directly influenced by the ability of the remainder of the fluid circuit to remove pressure from the pilot line.

Circuit:	
Safety Function:	The load is held when the system supply pressure is removed.
Faults to Consider:	A slow or sticking valve can affect the response time of the safety system. Leakage or improper sealing of components including downstream devices will cause motion. Stored energy can cause unexpected motion when released during service.
Fault Exclusion:	None to consider.
Safety Principles:	Relief function that will prevent pressure intensification and allow for braking.

11.4.9 Rod Locks and Rod Brakes

11.4.9.1 Design Requirements

When the control signal is removed, the hazardous motion shall be stopped and the actuator held in its present position.

Informative Note: *For the purposes of this standard, rod lock and rod brake are used interchangeably.*

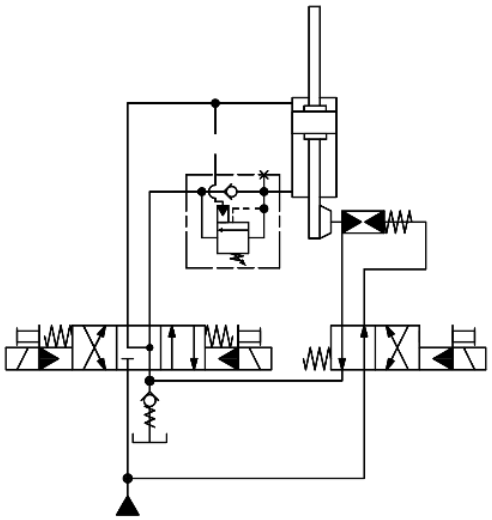
11.4.9.2 Design Considerations

Potential hazards include continuing motion and potential drift. Potential hazard severity can be reduced to an acceptable level but not eliminated.

Monitoring can be done via direct monitoring of the internal element or monitoring actuator motion.

The components selected shall be rated by the manufacturer for the intended application, i.e., dynamic stopping, static load holding, or cylinder force vs. gravity load.

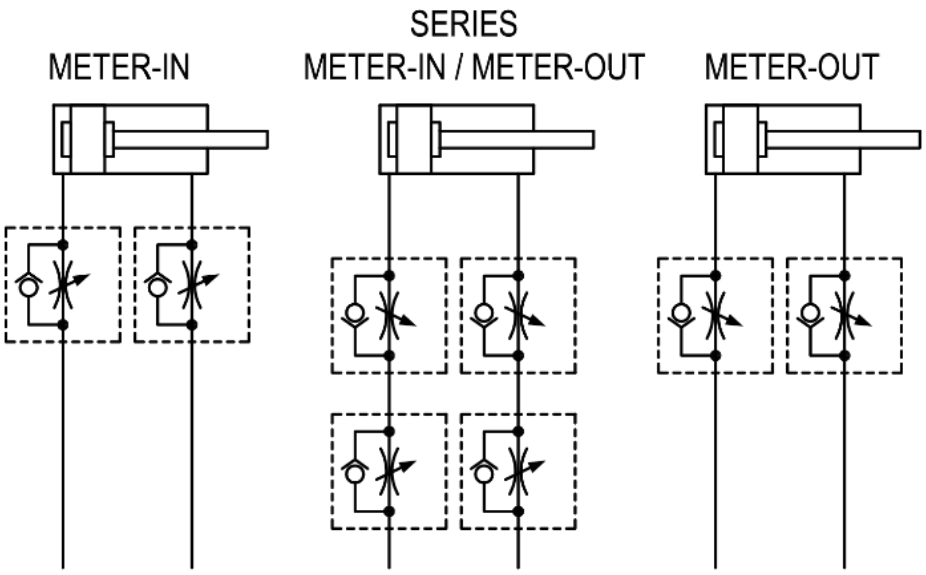
11.4.9.3 Rod Lock/Brake (Category 1)

Circuit:	
Safety Function:	When the electrical command signal is removed, the pressure will be removed from the rod lock / brake and the spring will engage the mechanism to hold the actuator rod in place.
Faults to Consider:	Valve element not actuating or de-actuating properly. A slow or sticking valve can affect response time of the safety system. Hazardous motion can continue.
Fault Exclusion:	None to consider.
Safety Principles:	Well-tried components suitable for the application.

11.4.10 Speed Control Flow Controls

Flow controls are used to control the actuator speed. They can be used to limit the flow into a port causing the actuator to build pressure and move at a limited rate. The flow control can also be used to limit the flow out of an actuator.

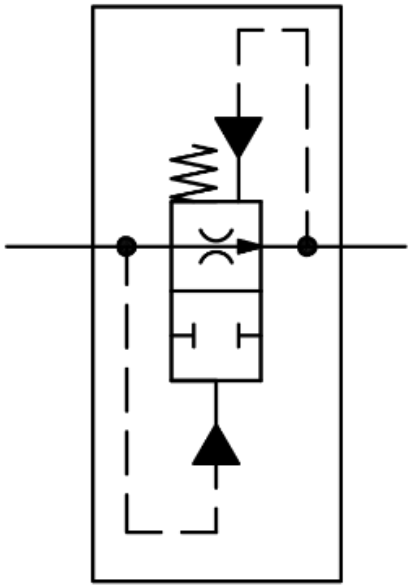
Meter-in flow controls may be used to prevent intensification on the rod end of the cylinder but will not quickly stop an over-running load. Meter-out flow controls shall be used where braking is required, and intensification is not an issue.

Circuit:	
Safety Function:	Control the flow causing the actuator to move at a limited rate.
Faults to Consider:	Operator adjustment. Contamination will change actuator speed influencing stop distance formulas and placement of safeguarding devices. Flow control check can get stuck open due to contamination resulting in an increase in actuator speed. Increased speed.
Fault Exclusion:	None to consider.
Safety Principles:	Well-tried components suitable for the application.

11.4.11 Velocity Fuse

A velocity fuse is a device that will automatically react to the sudden loss of pressure that occurs when a downstream hose or fitting is disconnected or broken. The sudden loss of pressure will result in an unsecured hose whipping action or a sudden drop of a vertical load, potentially causing injuries or damage.

The device shall be installed on the supply side of the hose to prevent the whipping action from occurring or directly at the cylinder port on vertical applications. When used on vertical loads to prevent rapid lowering during a conductor failure, the device shall be installed directly into the actuator port.

Circuit:	
Safety Function	A velocity fuse is a device that will automatically react to the sudden loss of pressure that occurs when a downstream hose or fitting is disconnected or broken.
Faults to Consider:	Pilot or main spool can stick in any position causing a failure of the flow to stop as intended. Valve element not actuating or de-actuating properly due to fluid contamination or internal wear. Load not being held in place.
Fault Exclusion:	None to consider.
Safety Principles:	Well-tried components suitable for the application.

12 Validation

The purpose of validation is to confirm that the SRP/CS supports the specified safety requirements given in clause 6.

Informative Note 1: *In this standard, the validation is limited to the designed SRP/CS or a part of it supporting the safety functions required from the risk reduction strategy at the machine level given in ANSI B11.0 and ISO 12100. The SRP/CS validation result is intended to be part of the overall validation of the machine.*

Informative Note 2: *For additional information on validation, see Annexes L – O and ISO 13849-2.*

The fundamental principles of validation include the elements of checking (e.g., analysis, inspection) and testing. The design of the safety function(s) shall be validated to answer three questions (at a minimum):

	Questions:	
CHECK	1	Are we doing the right things?
	2	Are we doing things right?
TEST	3	Do the safety functions work correctly?

Validation of software should be done with personnel highly proficient in the safety programmable controller being used and the proper implementation of its function blocks. Validation shall be carried out by persons who are independent from the design of the SRP/CS.

Informative Note: *"Independent person" does not necessarily mean that a third-party test is required.*

Software checks/tests that shall be done include but are not limited to checking and/or testing that:

- function blocks selected for engineering control devices / functions are correctly allocated and configured;
- the logic of the function blocks in relation to the machine's span of control, which inputs trigger which outputs per the SSRS (see subclause 10.2.2);
- the E-stop function block has priority over other functions and is not capable of manual suspension;
- any safety functions manually suspended in the software are in line with the SSRS and risk assessment;
- the software was locked following the completion of the validation;
- the safety programmable controller is designed with an internal safety related software simulation / validation tool, and that it shall be used as part of the software validation.

Each safety function specified in the SRP/CS requirements specification and all the SRP/CS operation and maintenance procedures shall be validated by checking and/or testing. When discrepancies occur, corrective action and re-testing shall be carried out as necessary and shall be documented. Validation activities shall be clearly communicated as to which level(s) of validation apply.

Informative Note: *There are different 'levels' of validation that impact the safety function including:*

- *component level (a simple component that performs the safety function by itself without the machine builder modifying the safety function);*
- *subsystem level (complex components e.g., safety PLC, for which the machine builder can define its own safety function by parameterization, programming, or other means);*
- *machine level.*

The validation shall demonstrate that the SRP/CS meets the ability to perform a safety function under expected environmental conditions.

Informative Note: *In some cases, validation should be carried out by persons who are independent of the design of the SRP/CS. By "independent person," that does not necessarily mean that a third-party test is required.*

For Categories 2, 3 and 4 or PLd or PLe, the validation of the safety function shall also include testing under fault conditions (to demonstrate that the fault reaction will be initiated by the implemented diagnostic function). If the validation cannot be successfully completed, changes in the design are necessary. The validation of the modified parts of the SRP/CS should then be repeated. This process should be iterated until the SRP/CS for each safety function is successfully validated.

The validation shall be conducted using a written document which includes:

- what test should be conducted (functional operation in use and/or reasonably foreseeable failures);
- how the tests may be done safely;
- what the expected and required results/reaction of each test should be;
- a record of the results.

13 Change Management

The change management process is the sequence of steps to ensure any modification to the equipment will not adversely affect the safety functions of the machine. The activities that a change management team follows to properly track requirements are still being met after a change ensures that personnel are not at increased risk after a change than prior to a change.

Informative Note 1: *Changes can be needed due to process changes, equipment changes, environmental changes, application changes, new features, bugs, etc.*

Informative Note 2: *The change management process is in place to ensure that all modifications are implemented in a deliberate manner. This process may be governed by a policy or procedure to ensure that only trained individuals are responsible for change implementation.*

Where changes are made to any safety function (e.g., hardware or software), a risk assessment shall be repeated for those parts of the machinery being modified or affected. See ANSI B11.0.

Changes, repairs, or modifications to any part of a safety function shall be implemented by authorized personnel (see also, Annex P).

Changes or modifications to a safety function shall be documented (see also, Annex P).

Changes, repairs, or modifications to any part of a safety function shall be tested to confirm proper functionality of the affected safety function(s) and that other safety functions are not adversely affected.

Access to the software shall be limited to authorized personnel. Any unauthorized changes or modifications to the safety software shall be prevented.

14 Information for Use

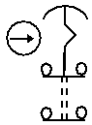
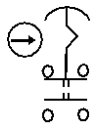
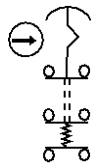
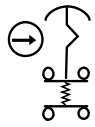
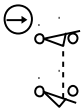
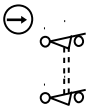
Information for use shall meet the requirements of ANSI B11.0 and include specific design limitations related to the functional safety system. Examples include:

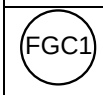
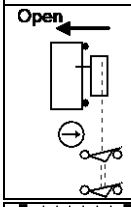
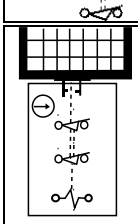
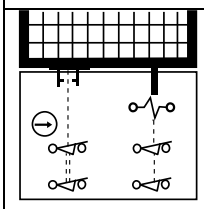
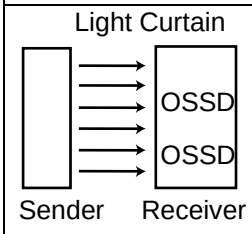
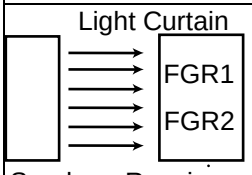
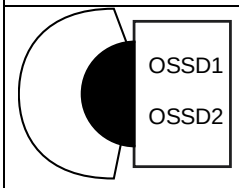
- fault exclusions;
- factors affecting component life (e.g., mission time);
- residual risk related to functional safety;
- safety function description(s);
- functional safety check, test, and confirm requirements.

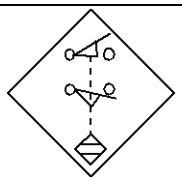
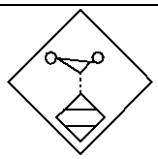
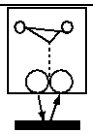
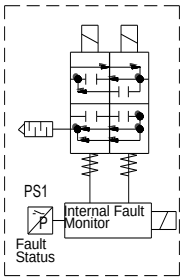
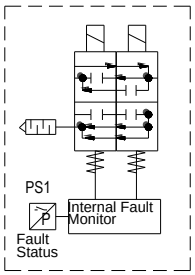
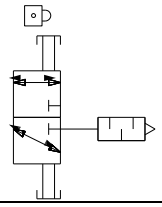
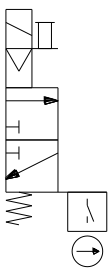
Informative Note: *For additional material on Information for Use, see ISO 20607.*

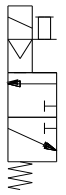
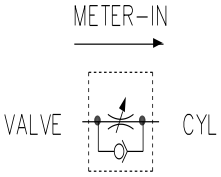
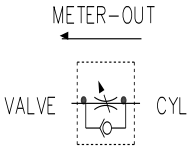
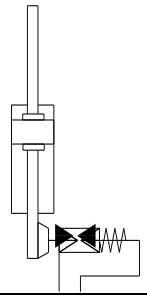
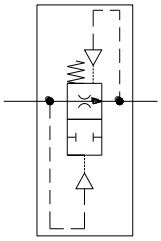
Annex A – Symbols
(Informative)

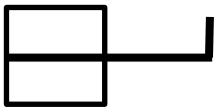
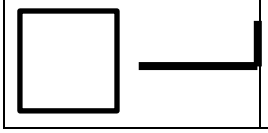
Table 5 — Table of Symbols

Symbol	Name	Symbol Description
	E-stop	Emergency stop switch with a mushroom head latching pushbutton with terminals and single, positively driven, normally closed contact.
	E-stop	Emergency stop switch with a mushroom head latching pushbutton with terminals and dual, positively driven, normally closed contacts that are electrically isolated and mechanically linked. The double dotted line indicates that both contacts are mechanically linked.
	E-stop	Emergency stop switch with a mushroom head latching pushbutton with terminals and dual, positively driven contacts with one normally closed and one normally open. The contacts are electrically isolated and mechanically linked. The double dotted line indicates that both contacts are mechanically linked.
	E-stop	Emergency stop switch with a mushroom head latching pushbutton with terminals and dual, positively driven, normally closed contacts that are electrically isolated and mechanically linked, with contact block sensing contact. The double dotted line indicates that both contacts are mechanically linked, and the spring indicates a normally open contact that is intended to be used for the monitoring circuit. In this case, the normally open held closed contact is used to detect if the contact block separates from the button.
	E-stop	Emergency stop switch with a mushroom head latching pushbutton with terminals and single, positively driven, normally closed contacts that are electrically isolated and mechanically linked, with contact block sensing contact. The spring indicates a normally open contact that is intended to be used for the monitoring circuit. In this case, the normally open contact held closed is used to detect if the contact block separates from the button.
	Switch, Interlock	Switch with one direct (positive) opening normally closed contact with its guard closed (limit switch released).
	Switch, Interlock	Switch with one direct (positive) opening normally closed contact and one non-direct (positive) opening normally open contact with its guard closed.
	Switch, Interlock	Switch with direct (positive) opening normally closed contacts with its guard door closed. The double dotted line indicates that both contacts are connected by non-resilient members.
FGR1 	Contact, Force-Guided Control Relay	Normally closed contact that is mechanically linked to the other contacts of the control relay, in this example, designated FGR1.
FGR1 	Contact, Force-Guided Control Relay	Normally open contact that is mechanically linked to the other contacts of the control relay, in this example, designated FGR1.
CR1 	Contact, Control Relay	Normally closed contact that is not mechanically linked to the other contacts of the control relay, in this example, designated CR1.
CR1 	Contact, Control Relay	Normally open contact that is not mechanically linked to the other contacts of the control relay, in this example, designated CR1.

Symbol	Name	Symbol Description
SIM1 	Contact, Safety Interface Module	Normally closed contact from a safety interface module. See also, ANSI B11.19.
SIM1 	Contact, Safety Interface Module	Normally open contact from a safety interface module. See also, ANSI B11.19.
	Coil, Force-Guided Control Relay	Control relay with all contacts electrically isolated and mechanically linked (positive-driven, force-guided).
	Coil, Force guided Contactor	Contactor with all contacts electrically isolated and mechanically linked (positive-driven, force-guided).
	Interlock	Type 2 interlocking device with two normally closed direct acting contacts. The double dotted line indicates that both contacts are mechanically linked. The removal of the actuator is direct acting to these safety-related contacts.
	Guard locking Interlock (Dependent)	Solenoid safety contact is mechanically interlocked to actuator safety contacts. The double dotted line indicates that both contacts are mechanically linked. The removal of the actuator is direct acting to the safety-related contacts.
	Guard locking Interlock (Independent)	Solenoid and actuator are independent. The double dotted line indicates that both contacts are mechanically linked. The removal of the actuator is direct acting to the safety-related contacts.
	Safety Light Curtain	Light Curtain has two OSSD (solid-state) outputs.
	Safety Light Curtain	Light Curtain has two FGR (Force-Guided) outputs.
	Safety Scanner	Safety Laser Scanner with two OSSD (solid-state) outputs.

	Safety Mat	A device, consisting of a sensing surface and control, which detects the presence of an individual(s) on its surface.
	Inductive Proximity Sensor	A switch, capable of detecting an appropriate target, based on inductive technology.
	Magnetic Sensor	A switch, capable of detecting an appropriate target, based on magnetic technology.
	Non-contact interlock Photoelectric Sensing	A switch, capable of detecting an appropriate target, based on optical technology.
	Pneumatic Safety Valve (dual channel)	Redundant internally monitored cross flow valve with solenoid reset. The valve will inhibit further operation should an internal fault occur and will maintain the faulted condition until the reset action takes place. The status switch provides optional feedback and is not required for the valve's safety function.
	Pneumatic Safety Valve (dual channel)	Redundant internally monitored cross flow valve with automatic reset and a status switch. Because the device resets automatically, the status switch should be externally monitored to detect faults and prevent further operation.
	Energy Isolation Device	Valve intended to block incoming pneumatic energy and relieve downstream pneumatic energy.
	Valve (single channel) with sensing	This valve has three ports (inlet, outlet, and exhaust) and two positions (de-energized and energized). When de-energized, the valve blocks the inlet supply and exhausts the downstream pneumatic energy. The switch monitors the position of internals providing feedback regarding valve position.

	Valve (single channel)	This valve has three ports (inlet, outlet, and exhaust) and two positions (de-energized and energized). When de-energized, the valve blocks the inlet supply and exhausts the downstream pneumatic energy.
	Flow control – Meter-IN	Device controls the flow going into the cylinder, also known as meter-IN.
	Flow control – Meter-OUT	Device controls the flow coming out of the cylinder, also known as meter-OUT.
	Rod Lock (Brake)-	A device that mechanically engages the rod to stop or hold motion.
	Velocity fuse	A device that blocks flow if the pressure differential exceeds its design limits.
	Key	
	Lock	Lock without a key
	Lock	Lock with a key inserted but removable
	Lock	Lock with a key inserted and releasable
	Lock	Lock without a key.

	Lock	Lock with a key inserted but removable.
	Lock	Lock with a key inserted and releasable.
	Lock	Lock with a key trapped.
	Actuator	Actuator inserted and locked in a trapped key interlocking device.
	Actuator	Actuator inserted in and removable from a trapped key interlocking device.
	Actuator	Actuator removed from an unlocked trapped key interlocking device.

Nomenclature for Labeling a SIM

1) The module should be labeled “Safety Interface Module” (see Figure 11) or in special applications, the label should include the “function” and then “Safety Interface Module” (e.g., Two-hand Control Safety Interface Module).
2) Input Channels are labeled “CH1” “CH2” (etc.) for input Channel One, Channel Two.
3) Output Channels are labeled “CH1” “CH2” (etc.) for input Channel One, Channel Two, though they may not have a relation to input channels.
4) The Reset button when used should be labeled “Reset”
    a) “Monitored Reset” when monitored manual reset function is required;
    b) For auto reset, a reset button is not shown and there is no label.
5) Between the input channel labels is a function description:
    a) “SD” = Short-circuit Detection;
    b) “SA” = Synchronous Actuation;
    c) “CA” = Concurrent Actuation.
6) External Device Monitoring (EDM) - if used, an EDM is shown between the connections.
    a) MPCE1 = Machine primary control element;
    b) MPCE2 = Machine primary control element.

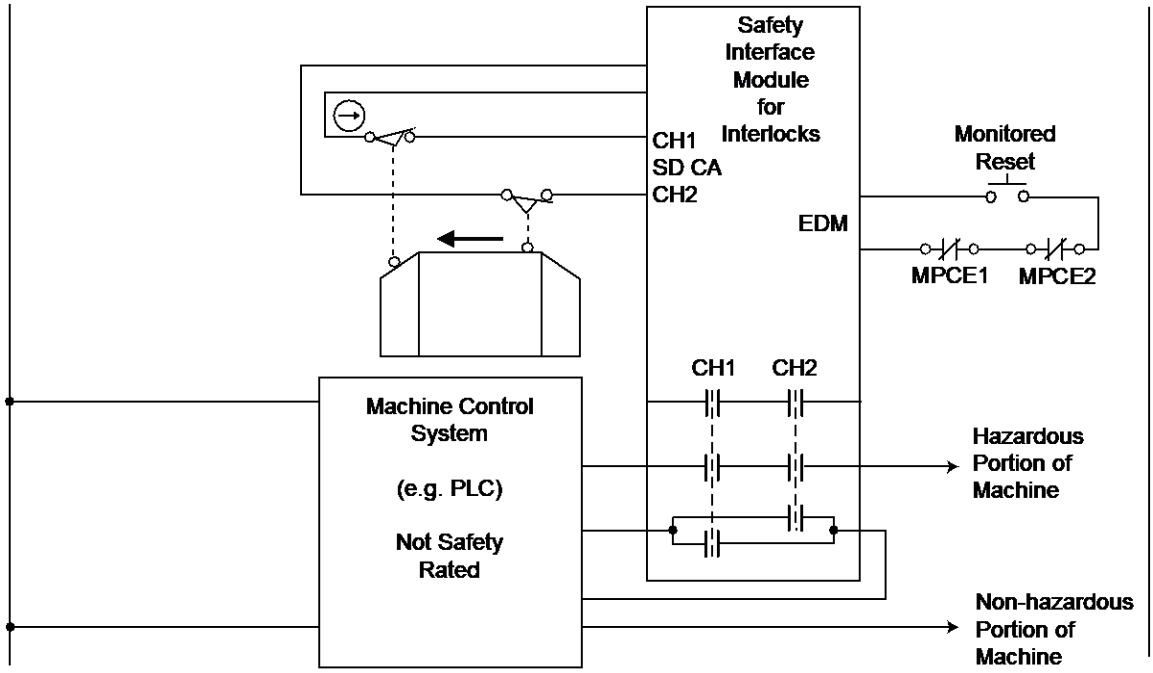


Figure 11: Example of labeling a SIM

Annex B – Performance Levels and Safety-Related Block Diagrams
(Informative)

This annex describes the five performance levels of the SRP/CS and how to select a performance level (PL). In addition, guidance is provided for developing safety-related block diagrams used in determining the safety performance level attained by a proposed functional safety circuit.

B.1 Performance Levels (PL)

The PL levels are defined in terms of Probability of Dangerous Failure per Hour PFH. Each PL has, as part of its performance requirement, a maximum dangerous failure per hour rate (PFH) requirement which is given in the Table 6 below.

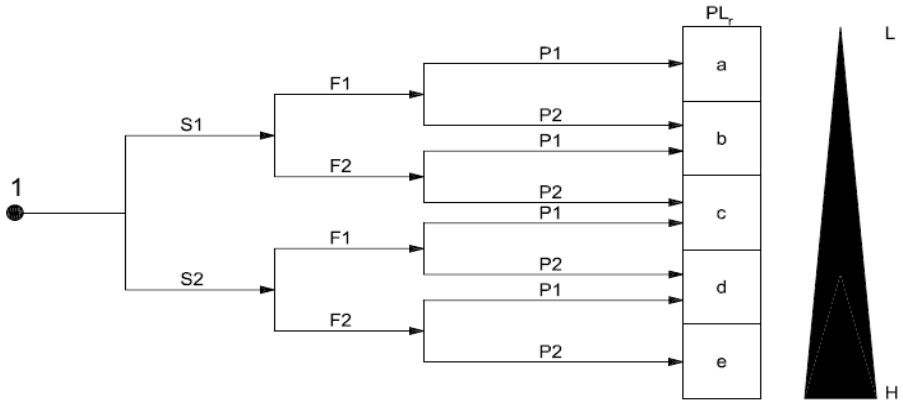
Table 6 — PL and PFH relationship
(from ISO 13849-1:2023 Table 2)

PL	**Average frequency of a dangerous failure per hour** (PFH) 1/h
a	$10^{-5} \leq PFH < 10^{-4}$
b	$3 \times 10^{-6} \leq PFH < 10^{-5}$
c	$10^{-6} \leq PFH < 3 \times 10^{-6}$
d	$10^{-7} \leq PFH < 10^{-6}$
e	$PFH < 10^{-7}$
NOTE: The PFH value is considered to be identical to the PFH according to IEC 62061:2021 and the IEC 61508 series.	

For individual components and channels, a term of λ_d, or the reciprocal of Mean Time To Dangerous Failure ($1/MTTF_D$) is used, although $MTTF_D$ is typically stated in terms of years rather than hours.

B.2 How to select a PL

The selection of a required PL for each safety function is based on the severity of injury, the frequency and/or exposure to a hazard, and the possibility of avoiding the hazard or limiting harm. These factors are combined as in Figure 12.



Key

1 starting point for evaluation of safety function's contribution to risk reduction
L low contribution to risk reduction
H high contribution to risk reduction
PL_r required performance level

Risk parameters:

S severity of injury
S1 slight (normally reversible injury)
S2 serious (normally irreversible injury or death)
F frequency and/or exposure to hazard
F1 seldom-to-less-often and/or exposure time is short
F2 frequent-to-continuous and/or exposure time is long
P possibility of avoiding hazard or limiting harm
P1 possible under specific conditions
P2 scarcely possible

Figure 12: Risk Graph for Performance Levels
(from ISO 13849-1 Annex A Figure A.1)

B.3 Developing the Safety-Related Block Diagram

The first task in determining the safety performance level attained by a proposed functional safety circuit is to develop its Safety-Related Block Diagram. It is critical that this step be done correctly, as an error here leads to an invalid determination of the PL achieved. The following steps are to be performed in the sequence given below:

Step 1 Identify the circuit components

Identify the circuit components whose failure will result in the loss of the safety function. Determine which components directly impact the ability of the others to perform their safety function. A failure to danger of any component in the string will result in the loss of the safety function. This identifies a channel and is shown in a series block connection as in the example in Figure 13. Note the inclusion of the components' interconnection means in the diagram.

Caution: A muting or manual suspension function, which in the electric diagram is a parallel function, is a series element in the safety-related block diagram, since an invalid activation or a failure of the muting/manual suspension function to exit that mode constitutes a failure to danger of the SRP/CS.

Any failure modes to danger in the interconnection i_{ix} between subsystems shall be included in one of its subsystems, or as an individual component (see Step 3).

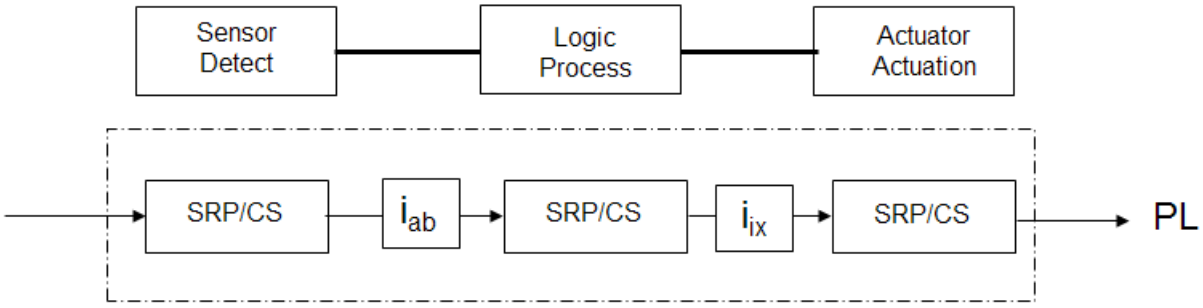


Figure 13: Safety-related part(s) of the control system, subsystem or channel

Step 2 Identify the circuit inputs, logic and outputs

There are three basic functions which control the safety circuit performance which must be identified: Input (sensors); Logic; and Output. Each of these may be a simple component or a complex subsystem also comprised of its own input, logic, and output as illustrated in Figure 14.

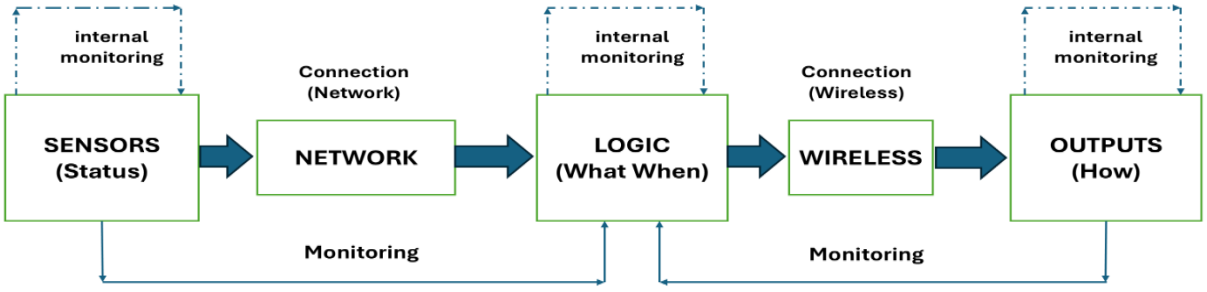


Figure 14: Example of components in the series failure loop

For example:

- Input Sensors:
  - detect status of possible trigger of the safety function;
  - for Safety PLC, it may be connected to separate input devices.
- Logic:
  - evaluate status of Input, Output and system faults, and establish appropriate SRP/CS response;
  - Safety PLC may have optional variations in I/O components with different fault tolerance capability which shall be matched to the total system performance requirements;
  - internal feedback may be present in more complicated devices such as safety light curtains, safety interface module, safety PLC, etc.
- Outputs Power Isolation:
  - isolate power from the hazardous devices and provide feedback to the logic components;
  - for safety logical devices with 24V DC safety output channels, there may be additional separate intermediate devices to drive hazard isolation devices.

Step 3 Identify the interconnections between components or subsystems

The interconnection between components or subsystems shall be identified and included in the safety-related block diagram since their failure can also lead to the loss of the safety function. This is especially true when such complex communication as networks and wireless links are used between components or subsystems.

Interconnections can include communications means between control components. Each technology has specific failure modes which are either addressed by the supplier, or shall be considered by the SRP/CS designer such as:

- point-to-point hardwire;
- networks;
- wireless;
- fiber-optic.

Step 4 Arrange / re-arrange the block diagram

The block diagram shall be created by arranging the components (such as in Figure 15). The order of the series components of a safety-related block diagram is not significant. Components and sub-assemblies may be re-arranged for simplification of the structure analysis

Informative Note: *If multiple individual components which are being evaluated as their own subsystems will be capped at their maximum $MTTF_D$, grouping them into one subsystem will result in the more capable channel PFH calculation. This is because the maximum $MTTF_D$ cap, of 100 years is applied only once to the grouped subsystem instead of to each individual component in their individual subsystems. See Table 14 (E.5 of Annex E).*

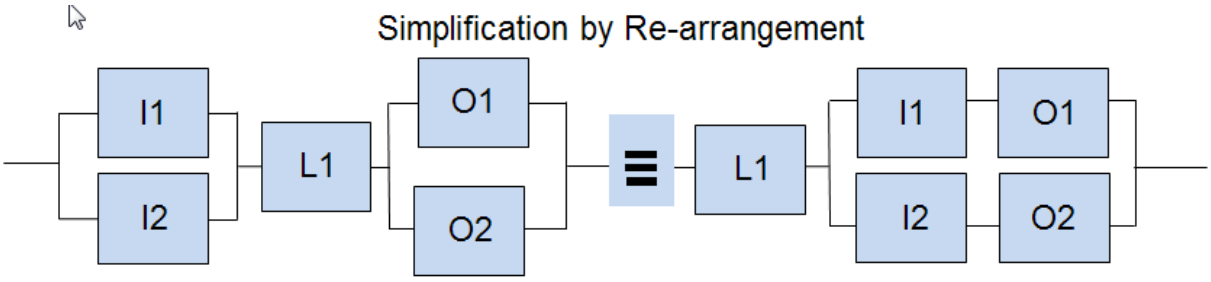


Figure 15: Re-arrangement of components of a safety-related block diagram
(from BGIA Report 2-2008e)

Step 5 Apply the analysis to components and subsystems
The block diagram analysis should be applied to components and subsystems (see Figures 15 and 16).

One of the advantages of the SRP/CS performance analysis by the use of ISO 13849-1 is the ability to utilize and analyze both components and subsystems of varying complexities and performance levels in the same safety function.

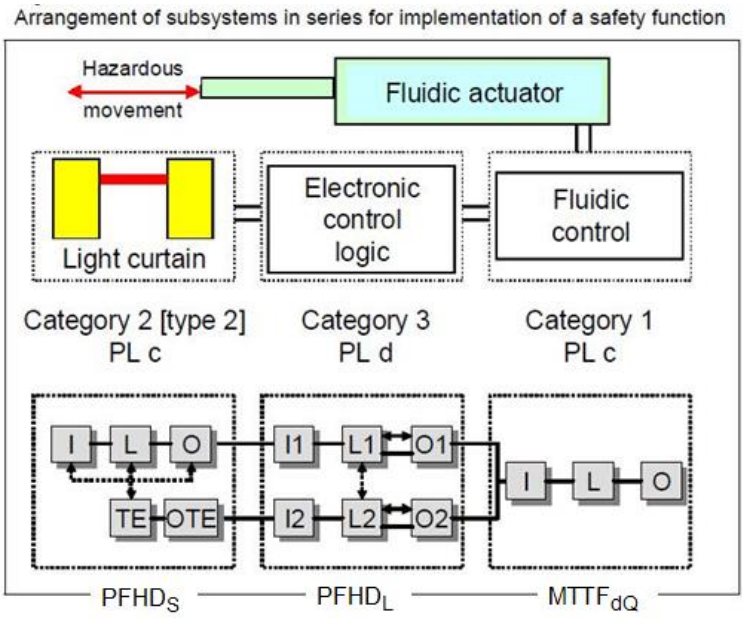


Figure 16: Various subsystems in one SRP/CS
(from BGIA Report 2-2008e)

Step 6 Identify monitoring elements
Components, subsystems, or channels which monitor shall also be identified. These elements monitor but do not directly perform a safety function; i.e., their failure does not lead directly to the loss of the safety function. If their interconnection serves to provide a warning or a secondary shut-down of the hazard (which functions only upon the detection of a fault), they are identified as Monitoring Devices and potentially as part of a structure two channel. Except as part of the Monitoring Channel of a Structure 2, multiple monitoring devices are not shown in the series safety-related block diagram, since although their failure may lead to the loss of the monitoring function, it does not directly lead to the loss of the safety function.

Step 7 Use the category structures for calculations
Calculations have been developed for the category structures described in Annex C. Use those structures to avoid detailed calculations.

If the proposed safety circuit cannot be resolved into one of the five structures of Annex C, the simplified calculations of ISO 13849-1 for PFH may not be used.

Informative Note: *Deviation from these structures requires full analysis using FMEA and full statistical methods and either IEC 62061 or IEC 61508 calculations shall be applied.*

Step 8 Examples
The example designs below are used to demonstrate the conversion of the SRP/CS's schematic to a safety-related block diagram which may be used to verify the circuit's appropriate performance using the simplified statistical methods utilized by ISO 13849-1.

Informative Note: *Circuit conversion to Series Safety-related Logic Block diagrams may be applied to totally fluid power designs as illustrated in Figure 17 or mixed systems as illustrated in Figure 18.*

For simplification of the fluid power circuit conversion to a safety-related block diagram, the control function of the solenoids has been left out for clarity. The performance of the sensor and the logic function safety-related block diagram performance level is added later to that of the fluid power (see a combined circuit example in Figure 17).

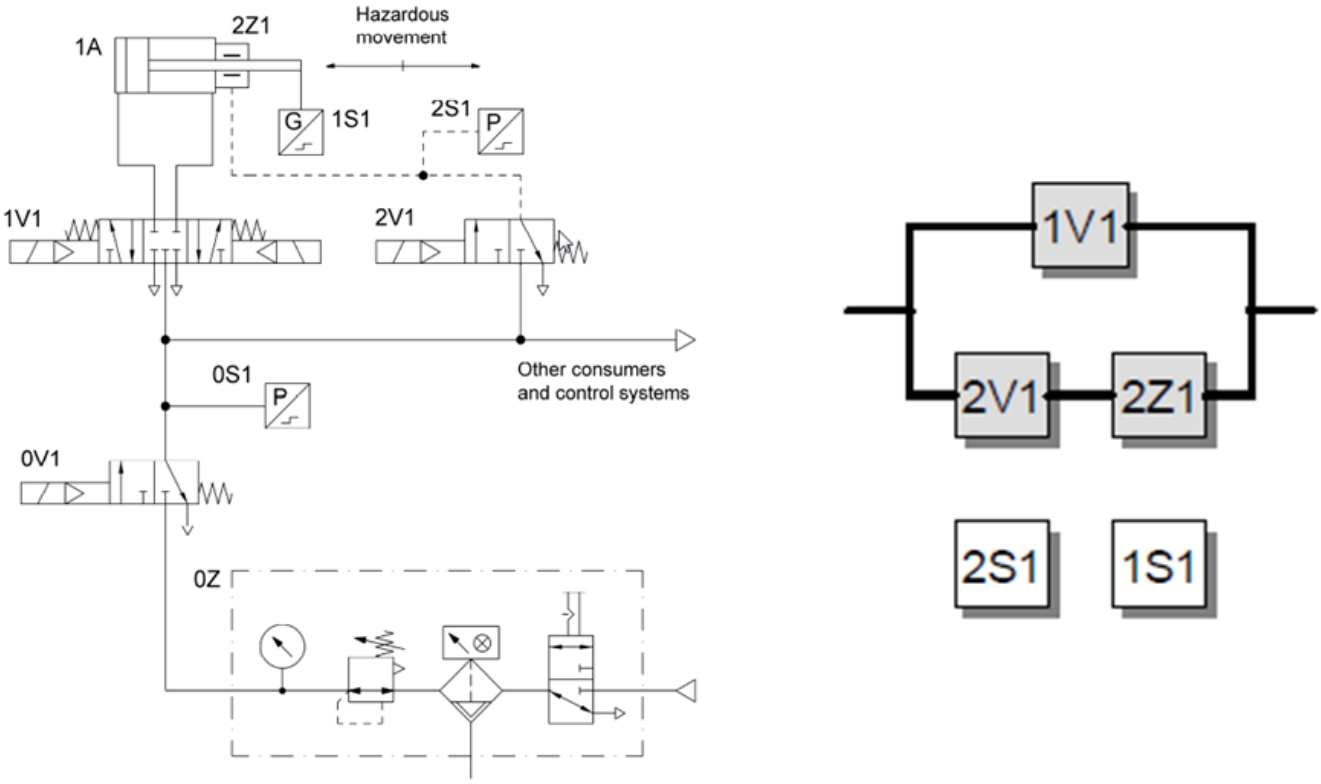


Figure 17: Fluid power segment of the SRP/CS
(from BGIA Report 2-2008e 8.2.14)

Safety Function: When the safety sensor device is triggered, power is removed from solenoids on valves 1V1 and 2V1 resulting in the removal of line pressure and blocking both cylinder ports, and in venting and thereby applying the spring-loaded rod brake of the cylinder whose motion presents the hazardous situation.

The rod brake shall be capable of holding the rod under full supply pressure to be considered as a channel of the safety-related block diagram, as it will not stop hazardous motion if 1V1 fails to shift. If this cannot be verified, the circuit is only a single channel while line pressure is applied to the system, as the brake will provide a safety function only against a load dropping due to gravity.

Due to other system manufacturing requirements, the operation of this safety function does NOT block and vent the system supply with 0V1, which is used in other safety functions such as emergency stop. In that case, OV1 would vent the rod brake even if 2V1 failed to spring return.

Monitoring devices (here, 2S1 and 1S1), are not shown in the series safety-related block diagram, since although their failure may lead to the loss of the monitoring function, it does not directly lead to the loss of the safety function. Their function is to increase the circuit reliability performance by detecting other components' functional failures. These devices shall be checked to verify that they are cycling with each application of the safety function, in the SRP/CS, if possible, but at a minimum in the process sequence control.

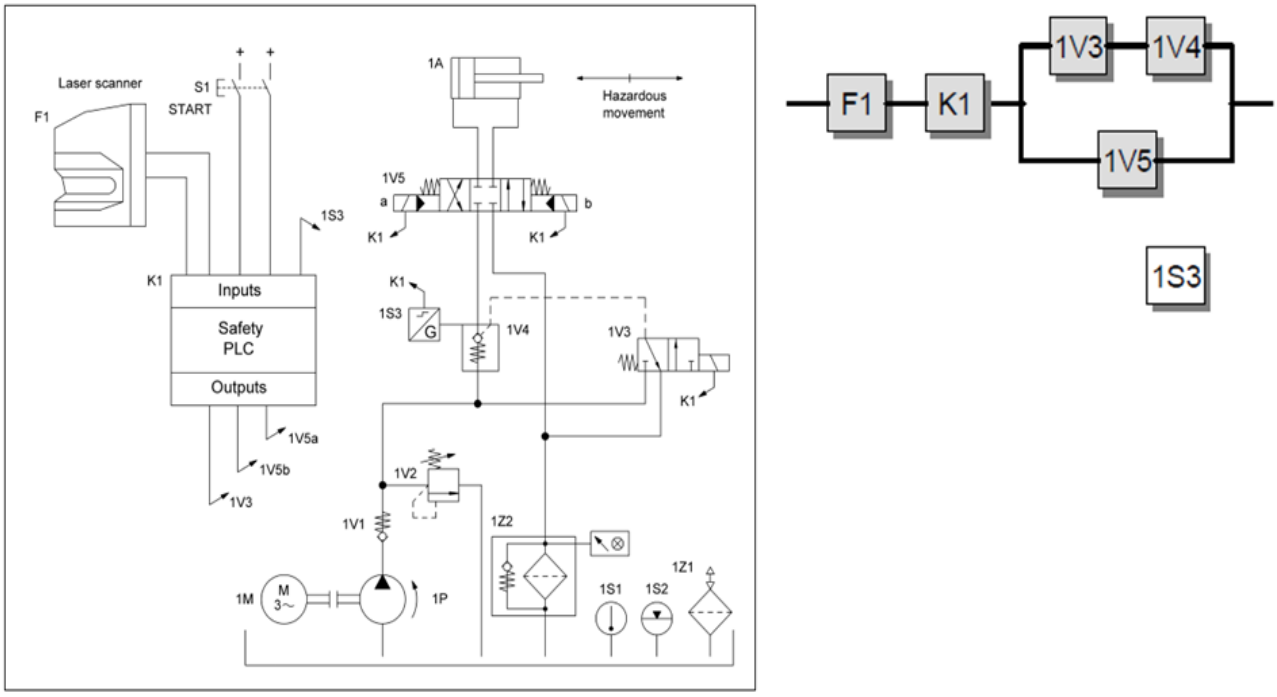


Figure 18: Detection zone monitoring by laser scanner with electro-hydraulic de-activation of hazardous movement (from BGIA Report 2/2008e 8.2.15)

Safety Function: When intrusion is detected by the Laser Scanner, the Safety PLC removes power from the dual channel valves of 1V3 and 1V5, removing pilot pressure at 1V4, blocking supply flow and blocking both cylinder ports at 1V5.

Informative Note: *This fluid power configuration has dual channel control of both cylinder direction motions.*

Monitoring devices (here, 1S3), are not shown in the series safety-related block diagram, since although its failure may lead to the loss of the monitoring function, it does not directly lead to the loss of the safety function. Their function is to increase circuit performance by detecting component functional failures. These devices shall be checked to verify that they are cycling with each application of the safety function, in the SRP/CS, if possible, but at a minimum in the process sequence control.

Annex C – Categories and How to Make a Selection
(Informative)

This annex describes the five structure categories of the SRP/CS and how to select a category.

C.1 Structure Categories

There are five structure categories (B, 1, 2, 3 and 4), along with their functional descriptions that were originally defined in EN 954-1. These categories were retained in ISO 13849-1 and are defined using the following terms:

a) **Structure Category:** the structure category (or simply, *Category*) plays a significant role in the determination of the Performance Level;
b) **$MTTF_D$:** the 'components' or 'channels' mean time to dangerous failure;
c) **DC** (Diagnostic Coverage)**:** the SRP/CS's ability to detect failures to danger;
d) **CCF** (common cause failure)**:** the level of reduction of common cause failures.

Structure Category B

The SRP/CS shall be designed, constructed, selected, assembled and combined in accordance with the relevant standards and using basic safety principles able to withstand:

- the expected operating stresses;
- the influence of the processed material;
- other relevant external influences.

Structure Category B shall exhibit the following features:

- there is no diagnostic coverage, DC_{avg} = None;
- $MTTF_D$ of the channel may be LOW to MEDIUM;
- CCF is not relevant.

Fault Reaction: When a fault occurs, it may lead to the loss of the safety function.
The designated architecture of structure Category B is depicted in this single channel figure below:

Key

i_m interconnecting means
I input device, e.g. sensor
L logic
O output device, e.g. main contactor

Figure 19: Category B
(Figure 7 from ISO 13849-1)

Structure Category 1

The requirements of structure Category B shall apply to structure Category 1, and in addition:

- The SRP/CS shall be designed and constructed using well-tried components and well-tried safety principles.

With Structure Category 1:

- there is no diagnostic coverage, DC_{avg} = None;
- $MTTF_D$ of the channel shall be HIGH;
- CCF is not relevant.

Fault Reaction: When a fault occurs, it may lead to the loss of the safety function; the probability of the loss of the safety function is lower than that for structure Category B.

The designated architecture of structure Category 1 is depicted in this single channel figure below:

Key

i_m interconnecting means
I input device, e.g. sensor
L logic
O output device, e.g. main contactor

Figure 20: Category 1
(Figure 8 from ISO 13849-1)

Structure Category 2

The requirements of structure Category B shall apply to structure Category 2, and in addition:

- Well-tried safety principles shall be used;
- The SRP/CS shall be designed so that the safety function can be checked at suitable intervals by the machine control system:
  - the initiation of this check may be automatic;
  - the check shall allow operation if no faults have been detected;
  - the check shall generate an output which initiates appropriate control action if a fault is detected:
    - whenever possible, that output shall initiate a safe state, and that safe state shall be maintained until the fault is cleared;
    - when it is not possible to generate a safe state, the output shall provide a warning of the hazard.

With Structure Category 2:

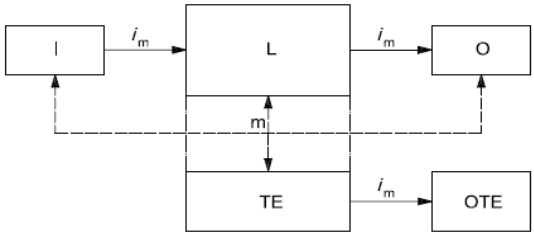
- DC_{avg} may be Low;
- $MTTF_D$ of the channel may be LOW to MEDIUM;
- CCF shall meet the minimum score.

Fault Reaction:

- When a fault occurs, it may lead to the loss of the safety function between checks;
- The loss of safety function is detected by the check;
- A fault in the monitoring circuit may lead to the loss of monitoring capability, resulting in a safety performance degradation to Category B or 1 depending on the $MTTF_D$ of the safety channel.
  Informative Note: *For Category 2, the PL of the channel (TE, OTE) is not required, however, $MTTF_{D,TE}$ of the TE channel shall be ≥ ½ $MTTF_{D,L}$ (if the logic $MTTF_D$ can be determined individually) or ≥ ½ $MTTF_D$ of the single channel capable of eliminating the hazard. Note that all failures which could cause the loss of the monitoring function shall be included. These may be different than those if the same device is used in a safety channel.*

- *A relay failing to energize is typically not a failure to danger in the safety channel. It may, however, cause a monitoring failure when applied in a monitoring channel and therefore failure of either function to drop out or to pull in may need to be counted in the $MTTF_{D,TE}$ or $MTTF_{D,TEO}$ as well as the DC of the TE or OTE.*
- *In some cases, structure Category 2 is not applicable, because the checking of the safety function cannot be applied to all components.*
- *The test frequency shall be at least 100 times greater than the demand placed upon a safety function.*

The designated architecture of structure Category 2 is depicted in Figure 21 (single channel with monitoring) below:



Dashed lines represent reasonably practicable fault detection.

Key

i_m interconnecting means
I input device, e.g. sensor
L logic
m monitoring
O output device, e.g. main contactor
TE test equipment
OTE output of TE

Figure 21: Category 2
(Figure 9 from ISO 13849-1)

Structure Category 3:

The requirements of structure Category B shall apply to structure Category 3, and in addition:

- Well-tried safety principles shall be used;
- The SRP/CS shall be designed so that:
  - a single fault in any of these parts does not lead to the loss of the safety function;
  - whenever reasonably feasible, the single fault shall be detected at or before the next demand upon the safety function.

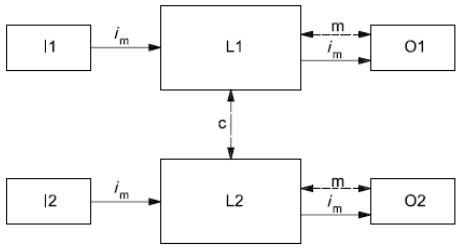
With structure Category 3:

- DC_{avg} may be Low;
- $MTTF_D$ of each channel may be LOW to MEDIUM;
- CCF shall meet the minimum score.

Fault Reaction:

- When a single fault occurs, the safety function is still always performed;
- Some, but not all faults will be detected;
- Accumulation of undetected faults may lead to the loss of the safety function.

The designated architecture of structure Category 3 is depicted in Figure 22 (dual channel monitoring):



Dashed lines represent reasonably practicable fault detection.

Key

i_m	interconnecting means
c	cross monitoring
I1, I2	input device, e.g. sensor
L1, L2	logic
m	monitoring
O1, O2	output device, e.g. main contactor

Figure 22: Category 3
(Figure 10 from ISO 13849-1)

Structure Category 4:

The requirements of structure Category B shall apply to structure Category 4, and in addition:

- Well-tried safety principles shall be used;
- The SRP/CS shall be designed so that:
  - a single fault in any of these parts does not lead to the loss of the safety function;
  - a single fault is detected at or before the next demand upon the safety functions:
    - if this detection is not possible, then the accumulation of faults shall not lead to the loss of the safety function.

With Structure Category 4:

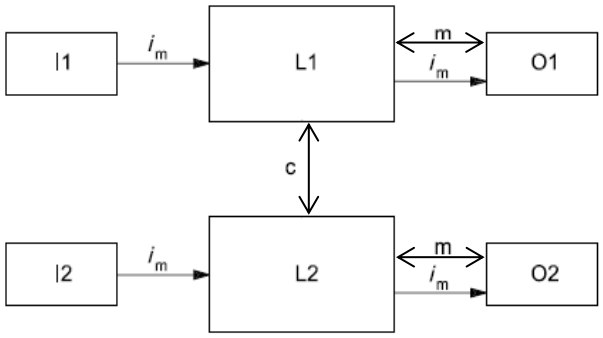
- DC_{avg} shall be HIGH;
- $MTTF_D$ of each channel shall be HIGH;
- CCF shall meet the minimum score.

Fault Reaction:

- When a single fault occurs, the safety function is still always performed;
- The faults will be detected in time to prevent the loss of the safety function;
- Accumulation of undetected faults shall not lead to the loss of the safety function.

The designated architecture of structure Category 4 is depicted in Figure 23 (dual channel monitoring).

Informative Note: *The change from dotted to solid lines for the monitoring function m and c illustrates the higher level of fault to danger discovery capability (DC), of this structure.*



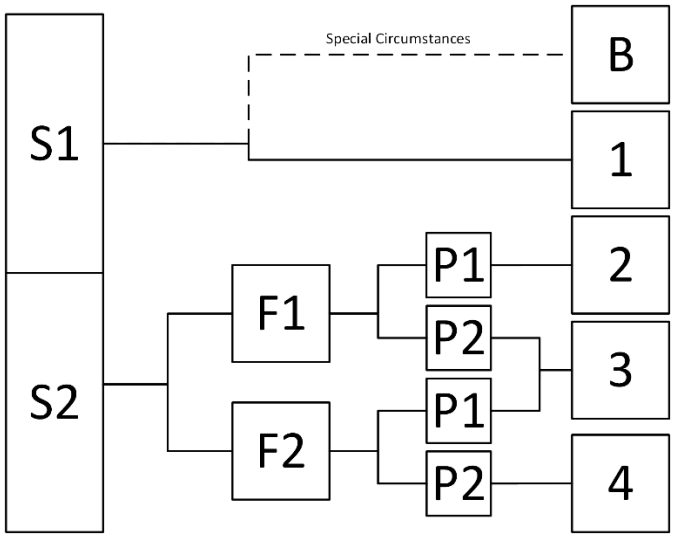
Key

i_m	interconnecting means
c	cross monitoring
I1, I2	input device, e.g. sensor
L1, L2	logic
m	monitoring
O1, O2	output device, e.g. main contactor

Figure 23: Category 4
(Figure 11 from ISO 13849-1)

C.2 How to select a category

The selection of a category is based on the severity of potential injury, the frequency and/or exposure to a hazard, and the possibility of avoiding the hazard or limiting harm. These factors are combined as in Figure 24.



Key

S	Severity of injury
S1	Slight injury (normally reversible)
S2	Serious injury or death
F	Frequency and/or exposure to hazard
F1	Low frequency or short duration of exposure
F2	High frequency or continuous exposure
P	Possibility of avoiding hazard or limiting harm
P1	High possibility of avoidance or limit of harm under specific conditions
P2	Scarcely possible of avoidance or limit of harm

Figure 24: Risk Graph for Categories

The category of the SRP/CS may also be determined using the flow chart below (Figure 25).

Informative Note: *An identified failure may be excluded if the probability of occurrence is extremely low and is justified by well-tried design principles. Document all exclusions and their justification.*

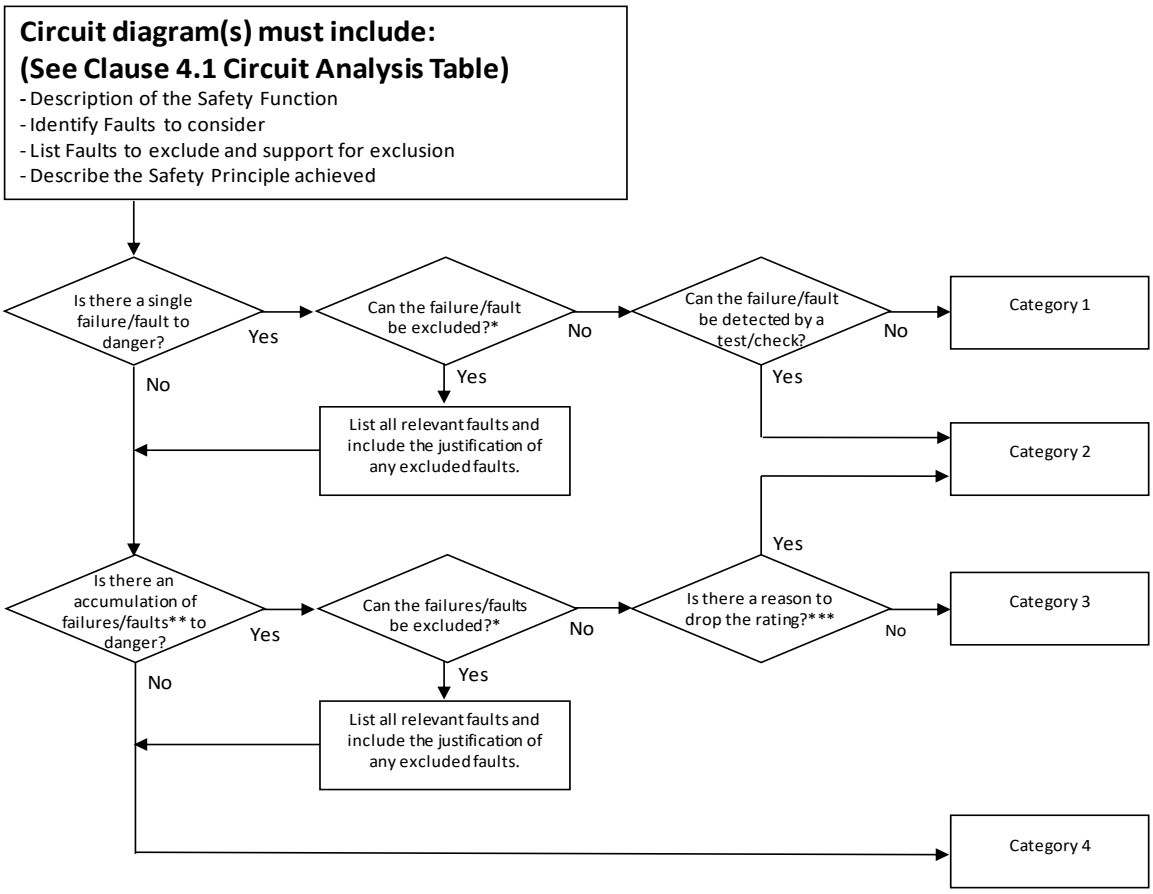


Figure 25: Flow chart to determine which Category may be achieved by the circuit.

** If a failure is not detected, it shall be assumed that, with further utilization, additional failures will occur. The combination of these failures shall be detected before the SRP/CS can fail to danger.

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

$MTTF_D$ of a component or subsystem is the operation time at which the probability of failure to danger reaches 63.2%. B_{10D} is the number of cycles until 10% of the components of a group under test fail to danger. B_{10D} is used to calculate a component $MTTF_D$ using the number of operations of the component per year. Since the component's number of cycles per year is application specific, $MTTF_D$ is typically not available from suppliers for types of components that are wear failure driven.

The sequence for finding the $MTTF_D$ values is in the following order:

1) Suppliers Data:
   - Suppliers offer $MTTF_D$ values for:
     a. electronic components;
     b. subsystems.
   - Suppliers offer B_{10D} values for:
     a. mechanical components;
     b. electromechanical components;
     c. pneumatic components;
     d. hydraulic components.
2) Use well-tried values as described in the methods in Annexes C or D in ISO 13849-1:2023;
3) Choose 10 years.

D1.1 Evaluating the $MTTF_D$

There are three methods for evaluating the $MTTF_D$ of components and subsystems used in the construction of the SRP/CS. They are ranked here by preference:

1) Supplier data that is supplied in most cases.
   Suppliers may supply either the $MTTF_D$ value of their components and subsystems or the B_{10D} value of their components. $MTTF_D$ may be calculated from the B_{10D} as shown in D1.2 below.

2) If neither the $MTTF_D$ nor B_{10D} values are available from the supplier, the following method of evaluating the $MTTF_D$ using data from Table 7 below may be applied. This method is called *Good Engineering Method*, and it may be used if:
   - it is expected that the supplier of the component has used basic and well-tried safety principles referenced in the table during the design and manufacture of the product (see also ISO 13849-2, A through D sub-clauses 1 through 4);
   - the supplier of the component has specified the appropriate application and operating conditions under which their product may be used;
   - the design of the SRP/CS fulfills the basic and well-tried principles for the implementation and operation of the component described in Annexes A through D of ISO 13849-2;
   - the user complies with the application and conditions of the supplier. This is of particular importance in the control of the operating environment such as temperature and humidity, and specifically:
     a) hydraulic fluid maintenance;
     b) compress air and system maintenance;
     c) electrical power systems in terms of transients, EMI and RFI.

3) If no other practical information on a component is available, use 10 years for the $MTTF_D$.

Table 7 — International Standards dealing with $MTTF_D$ or B_{10D} for Components

(from ISO 13849-1:2023 Annex C Table C.1)

	Basic and well-tried safety principles according to ISO 13849-2	**Relevant standards**	**Typical values: $MTTF_D$ (years) $B1_{0D}$ (cycles)**
mechanical components	Table A.1 and Table A.2	—	$MTTF_D$ = 150
hydraulic components with n_{op} ≥ 1 000 000 cycles per year [a]	Table C.1 and Table C.2	ISO 4413	$MTTF_D$ = 150
hydraulic components with 1 000 000 cycles per year > n_{op} ≥ 500 000 cycles per year [a]	Table C.1 and Table C.2	ISO 4413	$MTTF_D$ = 300
hydraulic components with 500 000 cycles per year > n_{op} ≥ 250 000 cycles per year [a]	Table C.1 and Table C.2	ISO 4413	$MTTF_D$ = 600
hydraulic components with n_{op} < 250 000 cycles per year [a]	Table C.1 and Table C.2	ISO 4413	$MTTF_D$ = 1 200
pneumatic components	Table B.1 and Table B.2	ISO 4414	B_{10D} = 20 000 000 [c]
relays and contactor relays with small load	Table D.1 and Table D.2	IEC 61810-3 IEC 60947 series	B_{10D} = 20 000 000
relays and contactor relays with nominal load	Table D.1 and Table D.2	IEC 61810-3 IEC 60947 series	B_{10D} = 400 000
proximity switches with small load	Table D.1 and Table D.2	IEC 60947 series ISO 14119	B_{10D} = 20 000 000
proximity switches with nominal load	Table D.1 and Table D.2	IEC 60947 series ISO 14119	B_{10D} = 400 000
contactors with small load [d]	Table D.1 and Table D.2	IEC 60947 series	B_{10D} = 20 000 000
contactors with nominal load [d]	Table D.1 and Table D.2	IEC 60947 series	B_{10D} = 1 300 000
position switches [b]	Table D.1 and Table D.2	IEC 60947 series ISO 14119	B_{10D} = 20 000 000
position switches (with separate actuator, guard-locking) [b]	Table D.1 and Table D.2	IEC 60947 series ISO 14119	B_{10D} = 2 000 000
emergency stop devices [b]	Table D.1 and Table D.2	IEC 60947 series ISO 13850	B_{10D} = 100 000
pushbuttons (e.g., enabling switches) [b]	Table D.1 and Table D.2	IEC 60947 series	B_{10D} = 100 000

Note 1 – For the definition and use of B_{10D}, see C.4 (of ISO 13849-1).
Note 2 – B_{10D} is estimated as 2X $B10$ (50 % dangerous failure) if no other information (e.g., product standard) is available.
Note 3 – Emergency stop devices according to IEC 60947-5-5 and ISO 13850 and enabling switches according to IEC 60947-5-8 can be estimated as a category 1 or category 3/4 subsystem depending on the number of electrical output contacts and on the fault detection in the subsequent subsystem. Each contact element (including the mechanical actuation) can be considered as one channel with a respective B_{10D} value. For enabling switches according to IEC 60947-5-8, this implies the opening function by pushing through or by releasing. In some cases, it is possible that the machine builder can apply fault exclusion according to ISO 13849-2:2012, Table D.8, considering the specific application and environmental conditions of the device.
Note 4 – Reduction of switching cycles can lead to an increasing probability of sticking of the switching elements in spool valves (see ISO 4413).
Note 5 – The $MTTF_D$ for mechanical components refers exclusively to mechanically moving components/parts (not to housing).
[a] B_{10D} calculation for hydraulic components is not permitted as a reverse calculation from standard $MTTF_D$ values.

[b] If fault exclusion for direct opening action is possible.
[c] In general, this value can be assumed for most pneumatic components. However, depending on the application and type, e.g., shut-off valve, this value can be significantly lower.
[d] "Nominal load" or "small load" should take into account safety principles described in ISO 13849-2:2012, such as over-dimensioning of the rated current value. "Small load" means, for example, 20 %.

D1.2 Calculating the $MTTF_D$ from the B_{10D}

For hydraulic, pneumatic, mechanical and electromechanical components, suppliers typically supply the B_{10d} or B_{10} value, not the $MTTF_D$ because the time to attain B_{10D} cycles is application specific. The B_{10D} is the number of cycles until 10% of the components in a test fail to danger.

The Mean number of Cycles to Dangerous Failure MCF_D is equal to 10 x B_{10D}. $MTTF_D$ for a specific application may be calculated from the B_{10D} value by dividing 10 x B_{10D} cycles by the number of operating cycles per year. In the equation below, the times-10 factor is shown as 0.1 in the denominator.

$$MTTF_D = \frac{B_{10D}}{0.1 \times n_{op}} \quad \text{where} \quad n_{op} = \frac{d_{op} \times h_{op} \times 3600}{t_{cycle}}$$

- n_{op} is the mean number of annual operations
- d_{op} is the mean operation, in days per year
- h_{op} is the mean operation in hours per day
- t_{cycle} is the mean time in seconds per cycle
- T_{10D} is the mean time until 10% of the components fail dangerously (test Interval)
- B_{10D} may be estimated as 2x B_{10} on the assumption that ½ the device failures are to danger. If further well-tried information is available on the ratio between all failures and failures to danger, that number may be used. These can vary as much as from 20 to over 70 %.

B_{10D} = B_{10} / the ratio between all failues and failures to danger

- typically, MCF_D may be estimated as 2x10xB_{10} or $MTTF_D$= 2x10xB_{10}/n_{op}

$$Where \quad T_{10D} = \frac{B_{10D}}{nop} \qquad hence \qquad MTTF_D = \frac{B_{10D}}{0.1 \times nop} = \frac{T_{10D}}{0.1}$$

Encapsulated subsystems which have cycle dependent wear components, such as safety channel output relays of Safety Interface Modules or Safety PLC outputs, are typically supplied by the supplier with system performance PL and PFH data. These data are valid only as long as the T_{10D} time (also known as Proof Test Interval) of the wear component has not been exceeded, at which time the subsystem or the wear components should be replaced.

D1.3 Example on calculating the $MTTF_D$ from the B_{10D}

Problem: A machine's mechanical interlock switch has a B_{10D} of 2,000,000 cycles and the machine runs one 8-hour shift, 270 days per year. The interlock is activated six times per shift.
Calculate the $MTTF_D$ of the interlock switch.

Solution: Using the formula below to calculate the $MTTF_D$

$$MTTF_D = \frac{B_{10D}}{0.1 \times nop} \qquad where \qquad nop = \frac{dop \times hop \times 3600}{tcycle}$$

Calculate the nop in order to calculate the interlock switch $MTTF_D$. *for this application* given that:

- d_{op} = 270 days
- h_{op} = 1 shift = 8hrs
- interlock is activated 6 times/shift = 6 times every 8 hours = 6 times every 8x60x60 seconds = 6 times every 28800 seconds = 1 time each 4800 seconds
    - hence t_{cycle} = 4800 seconds

$$\boldsymbol{nop = \frac{dop \times hop \times 3600}{tcycle} = \frac{270 \times 8 \times 3600}{4800} = 1620}$$

$$\boldsymbol{MTTF_D = \frac{B_{10D}}{0.1 \times nop} = \frac{2{,}000{,}000}{0.1 \times 1620} = 1.2\ E4\ years}$$

D1.4 Calculating the $MTTF_D$ for each channel

The formula is: $\frac{1}{MTTF_D} = \sum_{i=0}^{N} \frac{1}{MTT_{Di}}$

- $MTTF_D$ is the $MTTF_D$ for the complete channel
- $MTTF_{Di}$ is the $MTTF_D$ for each component which has a contribution to the safety function

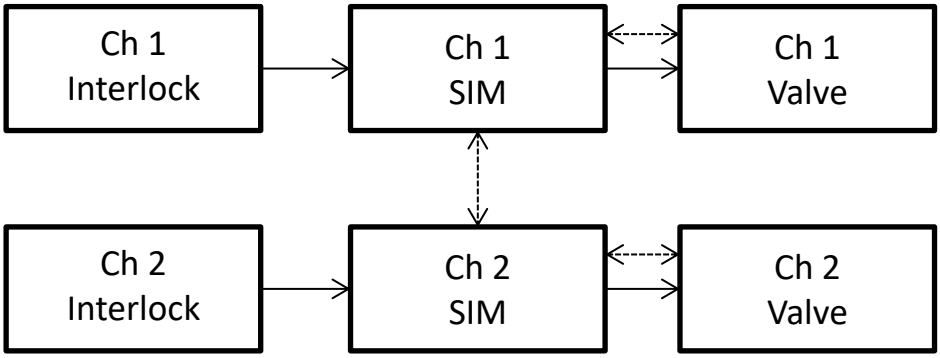


Figure 26: $MTTF_D$ channel example

In the above structure, an interlock switch is wired to a SIM and then to dual valves. In order to calculate the $MTTF_D$ of the system, calculate the $MTTF_D$ for each channel. Since both channels are made of the same components, the $MTTF_D$ of Channel 2 is equal to $MTTF_D$ of channel 1. The $MTTF_D$ for Ch1 and Ch2 is therefore:

$$\frac{1}{\mathrm{MTTF}_D} = \frac{1}{\mathrm{MTTF}_D(\mathrm{interlock})} + \frac{1}{\mathrm{MTTF}_D(\mathrm{SIM})} + \frac{1}{\mathrm{MTTF}_D(\mathrm{Valve})}$$

then:

$$MTTF_D = \frac{1}{\frac{1}{\mathrm{MTTF}_D(\mathrm{interlock})} + \frac{1}{\mathrm{MTTF}_D(\mathrm{SIM})} + \frac{1}{\mathrm{MTTF}_D(\mathrm{Valve})}}$$

Symmetrization of the channels is the combination of the $MTTF_D$ of the two channels and is calculated below. This symmetrized value is used for the channel $MTTF_D$ of the safety function for Category 3 and Category 4.

If: $MTTF_{D(ch1)} = MTTF_{D(ch2)}$
Then: $MTTF_{D(\text{safety function})} = MTTF_{D(ch1)} = MTTF_{D(ch2)}$

D1.5 Example Calculation of the $MTTF_D$ of a channel

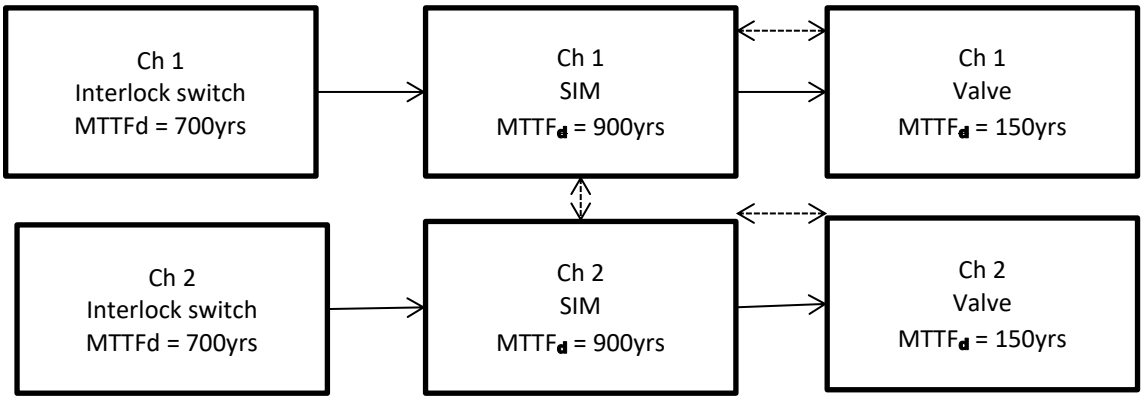


Figure 27: Example $MTTF_D$ channel

Problem: Calculate the $MTTF_D$ of the safety function given the schematic below**:**

$$MTTF_D(SF) = MTTF_D(ch1) = MTTF_D(ch2) = \frac{1}{\frac{1}{\mathrm{MTTF}_D(\mathrm{interlock})} + \frac{1}{\mathrm{MTTF}_D(\mathrm{SIM})} + \frac{1}{\mathrm{MTTF}_D(\mathrm{Valve})}}$$

$$= \frac{1}{\frac{1}{700} + \frac{1}{900} + \frac{1}{150}} = 108.62\ years = \ 100\ \mathrm{years}$$

where $MTTF_{D\ ch1}$ and $MTTF_{D\ ch2}$ are the values for two different redundant channels, each limited to a maximum value of either 100 years (categories B, 1, 2 and 3) or 2,500 years (category 4) before the formula above is applied.

D1.6 Calculation of the symmetrized $MTTF_D$ for channels with different $MTTF_D$ values

When the $MTTF_D$ of the channels differ, there are two methods available:

1- Take the worst-case channel $MTTF_D$, as the symmetrized value. This understates the symmetrized value which otherwise will be larger than the smallest symmetrized value;
2- Use the formula below to calculate the $MTTF_D$ for the safety function.

$$MTTF_D = 2/3\left[MTTF_D(ch1) + MTTF_D(ch2) - \frac{1}{\frac{1}{MTTF_D(ch1)} + \frac{1}{MTTF_D(ch2)}}\right]$$

Example on calculating the $MTTF_D$ of two different channels:

Problem: Given a safety function that has two channels, channel 1 has an $MTTF_D$ of 95 yrs and channel 2 has an $MTTF_D$ of 112 yrs. Calculate the $MTTF_D$ of the safety function:

Solution: Cap the $MTTF_D$ at 100 years for channel 2

$$2/3\left[95 + 100 - \frac{1}{\frac{1}{95} + \frac{1}{100}}\right] = \ 97\ yrs$$

For a structure Category 2, each channel (safety and monitoring) is evaluated separately. The $MTTF_D$ of the monitoring channel should be equal to or greater than ½ of the $MTTF_D$ of the safety channel. If this is not the

case, $MTTF_D$ safety channel is capped at 2($MTTF_D$) of the monitoring channel.

Mean time to dangerous failure of each channel ($MTTF_D$):
The value of the $MTTF_D$ of each channel is grouped into three levels: LOW, MEDIUM and HIGH. $MTTF_D$ is the Mean Time to Dangerous Failure of a component or channel and is generally measured in years.

Table 8 — $MTTF_D$
(from ISO 13849-1 Table 5)

$MTTF_D$	
Denotation of each channel	**Range of each channel**
Low	3 years < $MTTF_D$ < 10 years
Medium	10 years < $MTTF_D$ < 30 years
High	30 years < $MTTF_D$ < 100 years

Annex D – Section 2: Diagnostic Coverage
(Informative)

D2.1 Example values of the Diagnostic Coverage

I. Input devices:

Table 9 — DC for input devices
(from ISO 13849-1 2023 Annex E Table E.1)

Measure	Diagnostic Coverage (DC) [a,b]
Input device	
Cyclic test stimulus by dynamic change of the input signals	90%
Plausibility check, e.g., use of normally open and normally closed mechanically linked contacts	99%
Cross monitoring of inputs without dynamic test	Percentage to be defined depending on the specific application, e.g., depending on how often a signal change is done by the application (see NOTE 4)
Cross monitoring of input signals with dynamic test if short circuits are not detectable (for multiple I/O)	90%
Cross monitoring of input signals and intermediate results within the logic (L), and temporal and logical software monitor of the program flow and detection of static faults and short circuits (for multiple I/O)	99%
Indirect monitoring (e.g., monitoring by pressure switch, electrical position monitoring of actuators)	90% to 99%, depending on the application
Direct monitoring (e.g., electrical position monitoring of control valves, monitoring of electromechanical devices by mechanically linked contact elements)	99%
Fault detection by the process	Percentage to be defined depending on the specific application; this measure alone is not sufficient for the required performance level - (PL_r) e (see NOTES 2, 3 and 5)
Monitoring some characteristics of the sensor (response time, range of analog signals, e.g., electrical resistance, capacitance)	60%

II. Logic Devices:

Table 10 — DC values for Logic Devices

(from ISO 13849-1 2023 Annex E Table E.1 (continued))

Measure	Diagnostic Coverage (DC) [a,b]
Logic	
Indirect monitoring (e.g., monitoring by pressure switch, electrical position monitoring of actuators)	90% to 99%, depending on the application (see NOTE 2)
Direct monitoring (e.g., electrical position monitoring of control valves, monitoring of electromechanical devices by mechanically linked contact elements)	99%
Simple temporal time monitoring of the logic (e.g., timer as watchdog, where trigger points are within the program of the logic)	60%
Temporal and logical monitoring of the logic by the watchdog, where the test equipment does plausibility checks of the behavior of the logic	90%
Start-up self-tests to detect latent faults in parts of the logic (e.g., program and data memories, input/output ports, interfaces)	60% to 90% (depending on the testing technique - see NOTE 2)
Checking the monitoring device reaction capability (e.g., watchdog) by the main channel at start-up or whenever the safety function is demanded or whenever an external signal demands it (e.g., through an input facility)	90%
Dynamic principle (all components of the logic are required to change the state ON-OFF-ON when the safety function is demanded), e.g., interlocking circuit implemented by relays	99%
Invariable memory: signature of one word (single bus width)	90%
Invariable memory: signature of double word (double bus width)	99%
Variable memory: RAM-test by use of redundant data e.g., flags, markers, constants, timers and cross comparison of these data	60%
Variable memory: check for readability and write ability of used data memory cells	60%
Variable memory: self-test (e.g., “galpat” or “Abraham”) or double RAM with hardware or software comparison and read/write test	99%
Processing unit: self-test by software (see IEC 61508-7:2010, A.3)	60% to 90%
Processing unit: coded processing (see IEC 61508-7:2010, A.3)	90% to 99%

Fault detection by the process	Percentage to be defined depending on the specific application; this measure alone is not sufficient for the required performance level (PL_r) e (see NOTES 2, 3 and 5)

III. Output Devices:

Table 11 — DC for Output devices
(from ISO 13849-1 2023 Annex E Table E1)

Measure	Diagnostic Coverage (DC) [a,b]
Output Device	
Monitoring of outputs by one channel without dynamic test	Percentage to be defined depending on the specific application, e.g., depending on how often a signal change is done by the application (see NOTE 4)
Cross monitoring of outputs without dynamic test	Percentage to be defined depending on the specific application, e.g., depending on how often a signal change is done by the application (see NOTE 4)
Cross monitoring of output signals with dynamic test without detection of short circuits (for multiple I/O)	90%
Cross monitoring of output signals and intermediate results within the logic (L) and temporal and logical software monitor of the program flow and detection of static faults and short circuits (for multiple I/O)	99%
Redundant shut-off path with monitoring of the outputs by logic and test equipment, see example ISO 13849-2:2012, Annex E	99%
Indirect monitoring (e.g., monitoring by pressure switch, electrical position monitoring of actuators)	90% to 99%, depending on the application (see NOTE 2)
Fault detection by the process	Percentage to be defined depending on the specific application; this measure alone is not sufficient for the required performance level (PL_r) e (see NOTES 2, 3 and 5)
Direct monitoring (e.g., electrical position monitoring of control valves, monitoring of electromechanical devices by mechanically linked contact elements)	99%

Note 1 – For additional estimations for DC, see, e.g., IEC 61508-2:2010, Table A.2 to Table A.14.

Note 2 – For measures where a DC range is given (e.g., fault detection by the process), the correct DC value can be determined by considering all dangerous failures and then deciding which of them are detected by the DC measure. In case of any doubt, an FMEA should be the basis for the estimation of the DC.

Note 3 – For the DC measure "Fault detection by the process," the demand rate of the safety function (rd) and the process diagnostic (test) rate (rt) can be considered together with a limitation of the effective DC of the tested component:

a) *rt*/rd > 1 DC is limited to 60 %
b) *rt*/rd > 10 DC is limited to 90 %
c) *rt*/rd > 100 DC is limited to 99 %

Note 4 – For the DC measure "Cross monitoring of inputs or outputs without dynamic test," the effect of the test rate can be incorporated using the following limitations for the effective DC of the tested component:

For Category 3 and Category 4:

— *r*t < 1/year DC is 0 %

— *r*t ≥ 1/year DC is limited to 90 %
— *r*t ≥ 1/month DC is limited to 99 %

Note 5 – When the DC measure "fault detection by the process" is combined with other DC measures as listed in Annex E this measure can still be included in the DC estimation of the block, even for PLr e.

[a] DC measures can be combined to achieve a higher DC.

[b] If medium or high DC is claimed for the logic, at least one measure for each of variable memory, invariable memory and processing unit with each DC at least 60 % shall be applied. Other measures can be used than those listed in this table.

For the application of Table E.1 see the indicative examples below.

EXAMPLE 1: ISO 13849-2:2012, Annex E presents a complete worked example (which is very detailed) for the validation of fault behavior and diagnostic means on an automatic assembly machine.

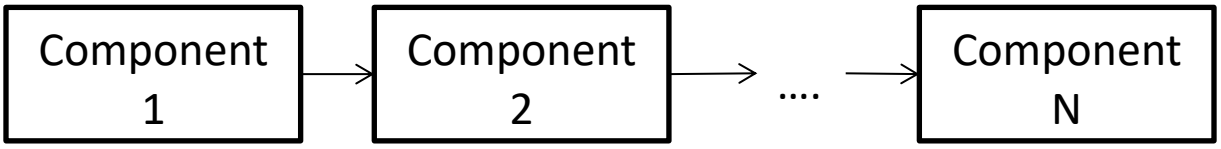
Note – ISO/TR 24119 describes a pragmatic step-by-step table-based methodology for evaluation of DC for series connected interlocking devices with potential free contacts.

EXAMPLE 2: The DC measure "fault detection by the process" can only be applied if the safety-related component is involved in the production process, e.g., a standard PLC or standard sensors are used for workpiece processing and as part of one of two channels executing the safety function. The appropriate DC level depends on the overlap of the commonly used resources (logic, inputs/outputs). For example, when all faults of a rotary encoder on a printing machine lead to highly visible interruption of the printing process, the DC for this sensor used to monitor a safely limited speed can be estimated as between 90 % up to 99 %.

D2.2 Calculating the DC_{avg} for a safety function or SRP/CS

The components of both channels are included for Category 3 and Category 4, as this is a system average DC.

The $MTTF_D$ is included with the DC of each component in the DC_{avg} to give proper weight to a component which might have a low individual DC but a high $MTTF_D$. This device would not add materially to the total of undiscovered failures to danger of the total system, as the failures which may not be discovered have a very slight probability of occurrence.



$$DCavg = \frac{\frac{DC1}{MTTFd1} + \frac{DC2}{MTTFd2} + \cdots + \frac{DCN}{MTTFdN}}{\frac{1}{MTTFd1} + \frac{1}{MTTFd2} + \cdots + \frac{1}{MTTFdN}}$$

Some faults are difficult to detect while other faults are extremely rare. If a known fault to danger is not detected and is also extremely rare, it may be excluded, and its occurrence is not included in the DC calculation. Any such exclusion shall be documented, and its rationale fully explained.

Informative Note 1: *For well-tried Safety Principles of Exclusion, see also Annexes L - O.*

Informative Note 2: *For additional information on fault exclusion, see section 5 of Annex A, B, C, and D, of ISO 13849-2:2012 and Annexes L, M, N and O of ANSI B11.26.*

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

Table 12 —Estimation of the measures against CCF for example B

(from ISO 13849-1:2023 Annex I, Table I.1)

No.	Item	Implemented measures	Score for control circuit	Max. possible score
1	**Separation/segregation**			
	physical separation between signal paths	• separate wiring to PLC between SW1B and SW2 (signal cables routed separately) • separation of both functional channels in the cabinet, e.g., between K1B and CC (separate components) • cross-connection of both channels limited to diagnostic testing	15	15
2	**Diversity**			
	different technologies/ design or physical principles are used	• position switch SW1B is operated when the safety guard is opened and has a break-contact element with direct opening action while position switch SW2 is operated when the safety guard is closed and uses a make-contact element • one functional channel uses electromechanical components, while the other functional channel uses programmable electronic components	20	20
3	**Design/application/experience**			
3.1	protection against over-voltage, over-pressure, over-current, and over-temperature	• additional protection against over-voltage and over-current on system level using external protection components where needed, i.e., diodes, fuses on inputs and outputs and a free-wheeling diode on relay K1B • over-voltage and under-voltage detection in the PLC	15	15
3.2	components used are well-tried	Only switch SW1B and relay K1B are well-tried components	none (only partly fulfilled, see F.2)	5
4	**Assessment/analysis**			
	For each part of SRP/ CS a failure mode and effect analysis has been carried out and its results taken into account to avoid common cause failures in the design	• not completely implemented • (FMEA with focus on CCF has been carried out but not in a formalized and completely documented way)	None	5
5	**Training**			
	Training of designers to understand the causes and consequences of CCFs	not completely implemented	None	5

No.	Item	Implemented measures	Score for control circuit	Maximum possible score
6	**Environmental**			
6.1	For electrical/electronic systems, prevention of contamination and EMIs to protect against CCFs in accordance with appropriate standards (e.g., IEC 61326-3-1)	— additional protection against electro-magnetic disturbances on a system level using external protection components, such as diodes, fuses, filters and shielding on all inputs and outputs (appropriate measures of Table L.1 implemented with focus on CCF) — signal and power cables are routed separately	25	25
6.2	Other Influences: Consideration of the requirements for immunity to all relevant environmental influences such as, temperature, shock, vibration, humidity (e.g., as specified in relevant standards)	— choice of both position switches to withstand all expected environmental influences with sufficient over-dimensioning and consideration of possible CCF causes — K1B, PLC and CC installed in the cabinet with temperature control	10	10
	Total		85	Max. 100

Annex E – Calculation Aids for Determination of SRP/CS PFH & PL (Informative)

The Performance Level calculation is applied within the SRP/CS as part of the design verification process. If the risk reduction solution is dependent on the correct functioning of the control system, the PL calculation applies.

The safety performance level of the output circuit should meet the level of safety performance of the input circuit, and vice versa. If safety performance levels are not the same, then the actual safety function will only meet the lower level of safety performance.

E.1 Determining the PL (achieved)

The first step in determining the PL is to develop a safety-rated function block diagram from the circuit design to identify the structure and all Fail To Danger elements. All elements whose failure can lead to the loss of the safety function shall be shown in the series blocks. Refer to Annex B for further detail.

For structure Categories 1, 2, 3 and 4, the following applies:

- Mission time is 20 years;
  - Any device which reaches its B_{10D} life in less than the mission life of the safety function shall be replaced at that time, or the mission life of the safety function limited to that value;
- For Category 2; demand rate ≤ 1/100 test rate;
- For Category 2; $MTTF_{D,TE}$ for the testing channel shall be ≥ 1/2 $MTTF_{D,L}$ of the safety channel;
  - If this requirement is initially not met and the testing $MTTF_{D,TE}$ cannot be increased, the calculated value of $MTTF_{D.L}$ or $MTTF_D$ of the safety channel shall be capped at ≤ 2 x $MTTF_{D,TE}$ of the Test Channel.

E.2 Determine the safety function to be verified

- Determine the PL_r from Figure11 for the safety function;
- Identify the SRP/CS that will constitute the safety function;
- Use the proposed SRP/CS to develop a Safety-Related block diagram for the safety function. This diagram will:
  - identify the structure of the SRP/CS;
  - all devices in the SRP/CS whose failure can cause the loss of that safety function shall be identified. These are shown as a series connection in the structure examples.
- Include the i_M physical connection(s) between blocks as their failure can lead to the loss of the safety function;
  - wire, fiber-optic, network, wireless.

Using the safety-related block diagram, calculate or evaluate the:

- $MTTF_D$ of the symmetrized channels or single channel (Annex D Section 1);
- DC_{avg} if required (Annex D Section 2);
- CCF if required (Annex D Section 3).

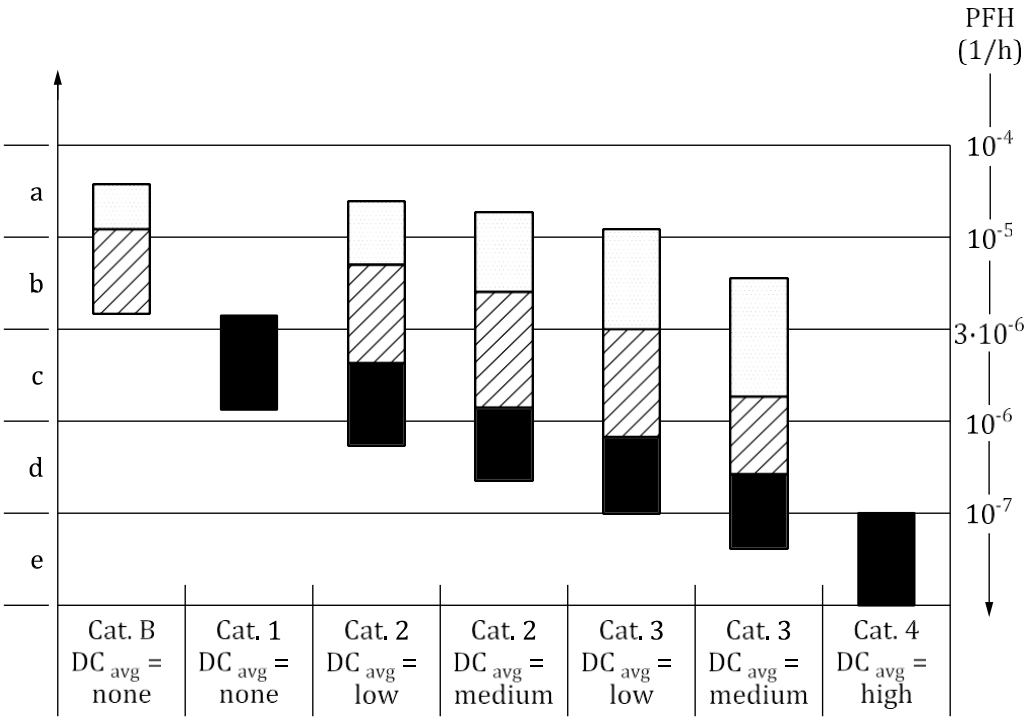
E.3 Simplified procedure for estimating PL

The PL may be estimated by taking into account all relevant parameters and the appropriate methods for their calculation. Table 13 shows one method. On the chart below, select the category and its appropriate DC_{avg} and draw a vertical line that meets the $MTTF_D$ levels.

Informative Note: *Ensure that CCF mode requirement has been met if required by the category.*

Depending on the symmetrized channel $MTTF_D$ group (LOW, MEDIUM or HIGH), draw a horizontal line from the top of that block intersecting the y-axis to determine the PL value. This is the most conservative value since all combinations of $MTTF_D$ in that group will attain at least its lower PL.

To meet the required safety function specification, the PL achieved shall be ≥ PL_r.



Key

PFH average frequency of dangerous failure per hour

PL performance level

low $MTTF_D$ of each channel

medium $MTTF_D$ of each channel

high $MTTF_D$ of each channel

Figure 28: Relationship between categories, DC_{avg}, $MTTF_D$ of each channel and PL
(from ISO 13849-1:2023 Fig 12).

Table 13 — Simplified procedure for evaluating Performance Level achieved by the SRP/CS
(This table is a tabular representation of Figure 28 [from ISO 13849-1:2015 Table 6])

Category	B	1	2	2	3	3	4
DC_{avg}	NONE	NONE	LOW	MEDIUM	LOW	MEDIUM	HIGH
$MTTF_D$ of each channel							
LOW	a	Not covered	a	b	b	c	Not covered
MEDIUM	b	Not covered	b	c	c	d	Not covered
HIGH	Not covered	c	c	d	d	d	e

E.4 Example on estimating the Performance Level using the simplified graph method

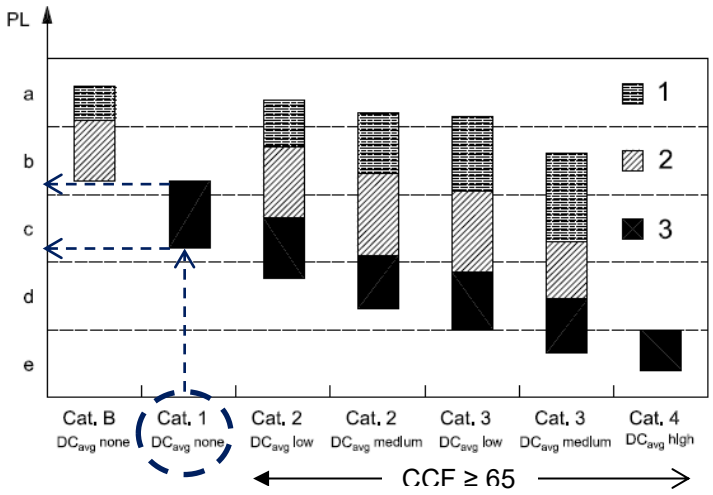
Problem:

Find the Performance Level of a safety function, that has a:

- Structure Category 1
- Channel $MTTF_D$ = High

Solution:

- Locate Structure Category 1, on the x-axis and select the Category 1 with DC_{avg} = None
- Draw a vertical line to the top of the $MTTF_D$ rectangle. Note that only a channel $MTTF_D$ = HIGH may achieve a Category 1 structure
- Project over to the y-axis and read the PL Note that the channel may reach either a PL_b or a PL_c, depending on the actual value of the channel's $MTTF_D$. However, with this level of granularity in information, only reaching PL_b may be ensured. That is the most conservative performance level, and the penalty for using the simplified graphical approach.



Key: Performance Level

1. $MTTF_D$ of systemized channel – LOW
2. $MTTF_D$ of systemized channel – MEDIUM
3. $MTTF_D$ of systemized channel – HIGH

Figure 7.7.1-2 Example Simplified Graph from ISO 13849-1 Figure 5

For a more granular evaluation of the system performance based on numerical value of symmetrized channel $MTTF_D$, use Table 14 to locate the $MTTF_D$ and establish PL as shown below.

E.5 Numerical evaluation using Table 14

This method is more accurate than the simplified graphical method and it requires the same data, however instead of using the group $MTTF_D$, a design specific value lookup table is used. The table provides a finer granulation of the $MTTF_D$ of the symmetrized channels than is possible with the grouping in the graph.

a) Symmetrized Channel $MTTF_D$;
b) DC_{avg};
c) Structure Category;
d) CCF (depending on the structure category).

The following sequence is used:

- Select the row that contains the closest, lower calculated $MTTF_D$ value of the symmetrized channels. For example, if $MTTF_D$ is 25 years, select the 24-year row;
- Select the column that matches the Category and DC_{avg} of the SRP/CS. Project the $MTTF_D$ row location to the left and read the PFH and PL of the SRP/CS or safety function in the selected column.

Informative Note 1: *The horizontal gray bars identify the break point between the $MTTF_D$ groupings used in the graph.*
Informative Note 2: *PFH is the average frequency of a dangerous failure of an SRP/CS to perform the specified safety function over a given period of time.*

Table 14 — Numerical Representation Table K.1 (from ISO 13849-1 2023 Annex K)

	Average probability of a dangerous failure per hour (1/h) and corresponding performance level (PL)															
$MTTF_d$ for each channel years	Cat. B DC_{avg} = none	PL	Cat. 1 DC_{avg} = none	PL	Cat. 2 DC_{avg} = low	PL	Cat. 2 DC_{avg} = medium	PL	Cat. 3 DC_{avg} = low	PL	Cat. 3 DC_{avg} = medium	PL	Cat. 4 DC_{avg} = high	PL
3	$3{,}80 \times 10^{-5}$	a			$2{,}58 \times 10^{-5}$	a	$1{,}99 \times 10^{-5}$	a	$1{,}26 \times 10^{-5}$	a	$6{,}09 \times 10^{-6}$	b		
3,3	$3{,}46 \times 10^{-5}$	a			$2{,}33 \times 10^{-5}$	a	$1{,}79 \times 10^{-5}$	a	$1{,}13 \times 10^{-5}$	a	$5{,}41 \times 10^{-6}$	b		
3,6	$3{,}17 \times 10^{-5}$	a			$2{,}13 \times 10^{-5}$	a	$1{,}62 \times 10^{-5}$	a	$1{,}03 \times 10^{-5}$	a	$4{,}86 \times 10^{-6}$	b		
3,9	$2{,}93 \times 10^{-5}$	a			$1{,}95 \times 10^{-5}$	a	$1{,}48 \times 10^{-5}$	a	$9{,}37 \times 10^{-6}$	b	$4{,}40 \times 10^{-6}$	b		
4,3	$2{,}65 \times 10^{-5}$	a			$1{,}76 \times 10^{-5}$	a	$1{,}33 \times 10^{-5}$	a	$8{,}39 \times 10^{-6}$	b	$3{,}89 \times 10^{-6}$	b		
4,7	$2{,}43 \times 10^{-5}$	a			$1{,}60 \times 10^{-5}$	a	$1{,}20 \times 10^{-5}$	a	$7{,}58 \times 10^{-6}$	b	$3{,}48 \times 10^{-6}$	b		
5,1	$2{,}24 \times 10^{-5}$	a			$1{,}47 \times 10^{-5}$	a	$1{,}10 \times 10^{-5}$	a	$6{,}91 \times 10^{-6}$	b	$3{,}15 \times 10^{-6}$	b		
5,6	$2{,}04 \times 10^{-5}$	a			$1{,}33 \times 10^{-5}$	a	$9{,}87 \times 10^{-6}$	b	$6{,}21 \times 10^{-6}$	b	$2{,}80 \times 10^{-6}$	c		
6,2	$1{,}84 \times 10^{-5}$	a			$1{,}19 \times 10^{-5}$	a	$8{,}80 \times 10^{-6}$	b	$5{,}53 \times 10^{-6}$	b	$2{,}47 \times 10^{-6}$	c		
6,8	$1{,}68 \times 10^{-5}$	a			$1{,}08 \times 10^{-5}$	a	$7{,}93 \times 10^{-6}$	b	$4{,}98 \times 10^{-6}$	b	$2{,}20 \times 10^{-6}$	c		
7,5	$1{,}52 \times 10^{-5}$	a			$9{,}75 \times 10^{-6}$	b	$7{,}10 \times 10^{-6}$	b	$4{,}45 \times 10^{-6}$	b	$1{,}95 \times 10^{-6}$	c		
8,2	$1{,}39 \times 10^{-5}$	a			$8{,}87 \times 10^{-6}$	b	$6{,}43 \times 10^{-6}$	b	$4{,}02 \times 10^{-6}$	b	$1{,}74 \times 10^{-6}$	c		
9,1	$1{,}25 \times 10^{-5}$	a			$7{,}94 \times 10^{-6}$	b	$5{,}71 \times 10^{-6}$	b	$3{,}57 \times 10^{-6}$	b	$1{,}53 \times 10^{-6}$	c		
10	$1{,}14 \times 10^{-5}$	a			$7{,}18 \times 10^{-6}$	b	$5{,}14 \times 10^{-6}$	b	$3{,}21 \times 10^{-6}$	b	$1{,}36 \times 10^{-6}$	c		
11	$1{,}04 \times 10^{-5}$	a			$6{,}44 \times 10^{-6}$	b	$4{,}53 \times 10^{-6}$	b	$2{,}81 \times 10^{-6}$	c	$1{,}18 \times 10^{-6}$	c		
12	$9{,}51 \times 10^{-6}$	b			$5{,}84 \times 10^{-6}$	b	$4{,}04 \times 10^{-6}$	b	$2{,}49 \times 10^{-6}$	c	$1{,}04 \times 10^{-6}$	c		
13	$8{,}78 \times 10^{-6}$	b			$5{,}33 \times 10^{-6}$	b	$3{,}64 \times 10^{-6}$	b	$2{,}23 \times 10^{-6}$	c	$9{,}21 \times 10^{-7}$	d		

	Average probability of a dangerous failure per hour (1/h) and corresponding performance level (PL)															
$MTTF_d$ for each channel years	Cat. B DC_{avg} = none	PL	Cat. 1 DC_{avg} = none	PL	Cat. 2 DC_{avg} = low	PL	Cat. 2 DC_{avg} = medium	PL	Cat. 3 DC_{avg} = low	PL	Cat. 3 DC_{avg} = medium	PL	Cat. 4 DC_{avg} = high	PL
15	$7{,}61 \times 10^{-6}$	b			$4{,}53 \times 10^{-6}$	b	$3{,}01 \times 10^{-6}$	b	$1{,}82 \times 10^{-6}$	c	$7{,}44 \times 10^{-7}$	d		
16	$7{,}13 \times 10^{-6}$	b			$4{,}21 \times 10^{-6}$	b	$2{,}77 \times 10^{-6}$	c	$1{,}67 \times 10^{-6}$	c	$6{,}76 \times 10^{-7}$	d		
18	$6{,}34 \times 10^{-6}$	b			$3{,}68 \times 10^{-6}$	b	$2{,}37 \times 10^{-6}$	c	$1{,}41 \times 10^{-6}$	c	$5{,}67 \times 10^{-7}$	d		
20	$5{,}71 \times 10^{-6}$	b			$3{,}26 \times 10^{-6}$	b	$2{,}06 \times 10^{-6}$	c	$1{,}22 \times 10^{-6}$	c	$4{,}85 \times 10^{-7}$	d		
22	$5{,}19 \times 10^{-6}$	b			$2{,}93 \times 10^{-6}$	c	$1{,}82 \times 10^{-6}$	c	$1{,}07 \times 10^{-6}$	c	$4{,}21 \times 10^{-7}$	d		
24	$4{,}76 \times 10^{-6}$	b			$2{,}65 \times 10^{-6}$	c	$1{,}62 \times 10^{-6}$	c	$9{,}47 \times 10^{-7}$	d	$3{,}70 \times 10^{-7}$	d		
27	$4{,}23 \times 10^{-6}$	b			$2{,}32 \times 10^{-6}$	c	$1{,}39 \times 10^{-6}$	c	$8{,}04 \times 10^{-7}$	d	$3{,}10 \times 10^{-7}$	d		
30			$3{,}80 \times 10^{-6}$	b	$2{,}06 \times 10^{-6}$	c	$1{,}21 \times 10^{-6}$	c	$6{,}94 \times 10^{-7}$	d	$2{,}65 \times 10^{-7}$	d	$9{,}54 \times 10^{-8}$	e
33			$3{,}46 \times 10^{-6}$	b	$1{,}85 \times 10^{-6}$	c	$1{,}06 \times 10^{-6}$	c	$5{,}94 \times 10^{-7}$	d	$2{,}30 \times 10^{-7}$	d	$8{,}57 \times 10^{-8}$	e
36			$3{,}17 \times 10^{-6}$	b	$1{,}67 \times 10^{-6}$	c	$9{,}39 \times 10^{-7}$	d	$5{,}16 \times 10^{-7}$	d	$2{,}01 \times 10^{-7}$	d	$7{,}77 \times 10^{-8}$	e
39			$2{,}93 \times 10^{-6}$	c	$1{,}53 \times 10^{-6}$	c	$8{,}40 \times 10^{-7}$	d	$4{,}53 \times 10^{-7}$	d	$1{,}78 \times 10^{-7}$	d	$7{,}11 \times 10^{-8}$	e
43			$2{,}65 \times 10^{-6}$	c	$1{,}37 \times 10^{-6}$	c	$7{,}34 \times 10^{-7}$	d	$3{,}87 \times 10^{-7}$	d	$1{,}54 \times 10^{-7}$	d	$6{,}37 \times 10^{-8}$	e
47			$2{,}43 \times 10^{-6}$	c	$1{,}24 \times 10^{-6}$	c	$6{,}49 \times 10^{-7}$	d	$3{,}35 \times 10^{-7}$	d	$1{,}34 \times 10^{-7}$	d	$5{,}76 \times 10^{-8}$	e
51			$2{,}24 \times 10^{-6}$	c	$1{,}13 \times 10^{-6}$	c	$5{,}80 \times 10^{-7}$	d	$2{,}93 \times 10^{-7}$	d	$1{,}19 \times 10^{-7}$	d	$5{,}26 \times 10^{-8}$	e
56			$2{,}04 \times 10^{-6}$	c	$1{,}02 \times 10^{-6}$	c	$5{,}10 \times 10^{-7}$	d	$2{,}52 \times 10^{-7}$	d	$1{,}03 \times 10^{-7}$	d	$4{,}73 \times 10^{-8}$	e
62			$1{,}84 \times 10^{-6}$	c	$9{,}06 \times 10^{-7}$	d	$4{,}43 \times 10^{-7}$	d	$2{,}13 \times 10^{-7}$	d	$8{,}84 \times 10^{-8}$	e	$4{,}22 \times 10^{-8}$	e
68			$1{,}68 \times 10^{-6}$	c	$8{,}17 \times 10^{-7}$	d	$3{,}90 \times 10^{-7}$	d	$1{,}84 \times 10^{-7}$	d	$7{,}68 \times 10^{-8}$	e	$3{,}80 \times 10^{-8}$	e
75			$1{,}52 \times 10^{-6}$	c	$7{,}31 \times 10^{-7}$	d	$3{,}40 \times 10^{-7}$	d	$1{,}57 \times 10^{-7}$	d	$6{,}62 \times 10^{-8}$	e	$3{,}41 \times 10^{-8}$	e
82			$1{,}39 \times 10^{-6}$	c	$6{,}61 \times 10^{-7}$	d	$3{,}01 \times 10^{-7}$	d	$1{,}35 \times 10^{-7}$	d	$5{,}79 \times 10^{-8}$	e	$3{,}08 \times 10^{-8}$	e
91			$1{,}25 \times 10^{-6}$	c	$5{,}88 \times 10^{-7}$	d	$2{,}61 \times 10^{-7}$	d	$1{,}14 \times 10^{-7}$	d	$4{,}94 \times 10^{-8}$	e	$2{,}74 \times 10^{-8}$	e
100			$1{,}14 \times 10^{-6}$	c	$5{,}28 \times 10^{-7}$	d	$2{,}29 \times 10^{-7}$	d	$1{,}01 \times 10^{-7}$	d	$4{,}29 \times 10^{-8}$	e	$2{,}47 \times 10^{-8}$	e

	Average probability of a dangerous failure per hour (1/h) and corresponding performance level (PL)															
$MTTF_d$ for each channel years	Cat. B DC_{avg} = none	PL	Cat. 1 DC_{avg} = none	PL	Cat. 2 DC_{avg} = low	PL	Cat. 2 DC_{avg} = medium	PL	Cat. 3 DC_{avg} = low	PL	Cat. 3 DC_{avg} = medium	PL	Cat. 4 DC_{avg} = high	PL
15	$7{,}61 \times 10^{-6}$	b			$4{,}53 \times 10^{-6}$	b	$3{,}01 \times 10^{-6}$	b	$1{,}82 \times 10^{-6}$	c	$7{,}44 \times 10^{-7}$	d		
16	$7{,}13 \times 10^{-6}$	b			$4{,}21 \times 10^{-6}$	b	$2{,}77 \times 10^{-6}$	c	$1{,}67 \times 10^{-6}$	c	$6{,}76 \times 10^{-7}$	d		
18	$6{,}34 \times 10^{-6}$	b			$3{,}68 \times 10^{-6}$	b	$2{,}37 \times 10^{-6}$	c	$1{,}41 \times 10^{-6}$	c	$5{,}67 \times 10^{-7}$	d		
20	$5{,}71 \times 10^{-6}$	b			$3{,}26 \times 10^{-6}$	b	$2{,}06 \times 10^{-6}$	c	$1{,}22 \times 10^{-6}$	c	$4{,}85 \times 10^{-7}$	d		
22	$5{,}19 \times 10^{-6}$	b			$2{,}93 \times 10^{-6}$	c	$1{,}82 \times 10^{-6}$	c	$1{,}07 \times 10^{-6}$	c	$4{,}21 \times 10^{-7}$	d		
24	$4{,}76 \times 10^{-6}$	b			$2{,}65 \times 10^{-6}$	c	$1{,}62 \times 10^{-6}$	c	$9{,}47 \times 10^{-7}$	d	$3{,}70 \times 10^{-7}$	d		
27	$4{,}23 \times 10^{-6}$	b			$2{,}32 \times 10^{-6}$	c	$1{,}39 \times 10^{-6}$	c	$8{,}04 \times 10^{-7}$	d	$3{,}10 \times 10^{-7}$	d		
30			$3{,}80 \times 10^{-6}$	b	$2{,}06 \times 10^{-6}$	c	$1{,}21 \times 10^{-6}$	c	$6{,}94 \times 10^{-7}$	d	$2{,}65 \times 10^{-7}$	d	$9{,}54 \times 10^{-8}$	e
33			$3{,}46 \times 10^{-6}$	b	$1{,}85 \times 10^{-6}$	c	$1{,}06 \times 10^{-6}$	c	$5{,}94 \times 10^{-7}$	d	$2{,}30 \times 10^{-7}$	d	$8{,}57 \times 10^{-8}$	e
36			$3{,}17 \times 10^{-6}$	b	$1{,}67 \times 10^{-6}$	c	$9{,}39 \times 10^{-7}$	d	$5{,}16 \times 10^{-7}$	d	$2{,}01 \times 10^{-7}$	d	$7{,}77 \times 10^{-8}$	e
39			$2{,}93 \times 10^{-6}$	c	$1{,}53 \times 10^{-6}$	c	$8{,}40 \times 10^{-7}$	d	$4{,}53 \times 10^{-7}$	d	$1{,}78 \times 10^{-7}$	d	$7{,}11 \times 10^{-8}$	e
43			$2{,}65 \times 10^{-6}$	c	$1{,}37 \times 10^{-6}$	c	$7{,}34 \times 10^{-7}$	d	$3{,}87 \times 10^{-7}$	d	$1{,}54 \times 10^{-7}$	d	$6{,}37 \times 10^{-8}$	e
47			$2{,}43 \times 10^{-6}$	c	$1{,}24 \times 10^{-6}$	c	$6{,}49 \times 10^{-7}$	d	$3{,}35 \times 10^{-7}$	d	$1{,}34 \times 10^{-7}$	d	$5{,}76 \times 10^{-8}$	e
51			$2{,}24 \times 10^{-6}$	c	$1{,}13 \times 10^{-6}$	c	$5{,}80 \times 10^{-7}$	d	$2{,}93 \times 10^{-7}$	d	$1{,}19 \times 10^{-7}$	d	$5{,}26 \times 10^{-8}$	e
56			$2{,}04 \times 10^{-6}$	c	$1{,}02 \times 10^{-6}$	c	$5{,}10 \times 10^{-7}$	d	$2{,}52 \times 10^{-7}$	d	$1{,}03 \times 10^{-7}$	d	$4{,}73 \times 10^{-8}$	e
62			$1{,}84 \times 10^{-6}$	c	$9{,}06 \times 10^{-7}$	d	$4{,}43 \times 10^{-7}$	d	$2{,}13 \times 10^{-7}$	d	$8{,}84 \times 10^{-8}$	e	$4{,}22 \times 10^{-8}$	e
68			$1{,}68 \times 10^{-6}$	c	$8{,}17 \times 10^{-7}$	d	$3{,}90 \times 10^{-7}$	d	$1{,}84 \times 10^{-7}$	d	$7{,}68 \times 10^{-8}$	e	$3{,}80 \times 10^{-8}$	e
75			$1{,}52 \times 10^{-6}$	c	$7{,}31 \times 10^{-7}$	d	$3{,}40 \times 10^{-7}$	d	$1{,}57 \times 10^{-7}$	d	$6{,}62 \times 10^{-8}$	e	$3{,}41 \times 10^{-8}$	e
82			$1{,}39 \times 10^{-6}$	c	$6{,}61 \times 10^{-7}$	d	$3{,}01 \times 10^{-7}$	d	$1{,}35 \times 10^{-7}$	d	$5{,}79 \times 10^{-8}$	e	$3{,}08 \times 10^{-8}$	e
91			$1{,}25 \times 10^{-6}$	c	$5{,}88 \times 10^{-7}$	d	$2{,}61 \times 10^{-7}$	d	$1{,}14 \times 10^{-7}$	d	$4{,}94 \times 10^{-8}$	e	$2{,}74 \times 10^{-8}$	e
100			$1{,}14 \times 10^{-6}$	c	$5{,}28 \times 10^{-7}$	d	$2{,}29 \times 10^{-7}$	d	$1{,}01 \times 10^{-7}$	d	$4{,}29 \times 10^{-8}$	e	$2{,}47 \times 10^{-8}$	e

Informative Note: *With the charts above in the Simplified Procedure, the single channel structure may be either Category B or Category 1 depending on the $MTTF_D$ of the channel. In this example, the $MTTF_D$ did not meet the requirement of Category 1 since the value was below 30 years. To reach this category, either the number of components in the channel shall be reduced (as shown in the Safety Logic Diagram), or the individual components' $MTTF_D$ shall be increased to attain a minimum channel $MTTF_D$ of at least 30 years, which is the minimum requirement for Category 1. The content of Table 14 is also available in the form of a circular calculator shown as in Figure 29.*

The circular calculator is available through https://www.dguv.de/ifa/praxishilfen/practical-solutions-machine-safety/performance-level-calculator/index.jsp

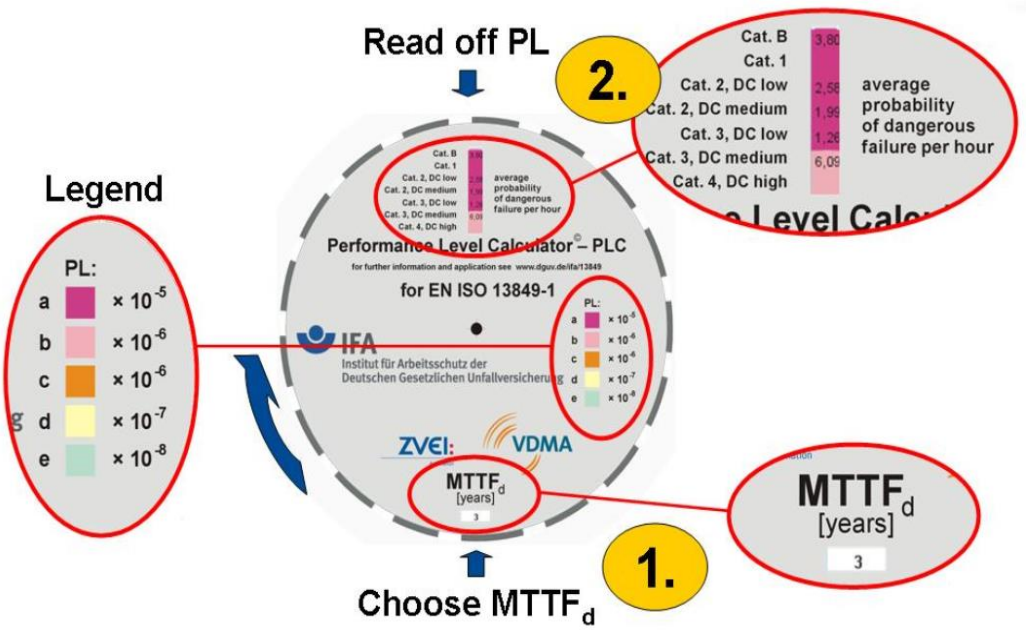


Figure 29: IFA Circular PL Calculator

1) Locate the $MTTF_D$ of the symmetrized channel by rotating the wheel until the closest lower year appears in the $MTTF_D$ bottom window.
2) Select the Category and Diagnostic Coverage (DC_{avg}) values from the top window. Read the mantissa and identify the power of ten multiplier color code from the color-coded Legend.
3) The mantissa and multiplier provide the $MTTF_D$ of the SRP/CS = Category B, which equals 3.00 x 10^{-5} failures to danger per hour.

E.6 Example of calculating the channel PL of a single channel with multiple subsystems

The SRP/CS for a given safety function may be comprised of individual components or of subsystems, each of which may also have one to more inputs, logic blocks and/or outputs (e.g., simple components are limit switches, PE sensors, contactors, valves, etc.). See Figure 30.

Subsystems may be:

- simple components with multiple varying specifications such as the mechanical and electrical life of a contactor;
- simple components grouped together for the sake of the computation;
- complete unto themselves with PL and PFH provided by the supplier and typically referred to as “encapsulated” subsystems, such as safety light curtains, laser scanners, and safety capable drives;
- CCF is achieved.

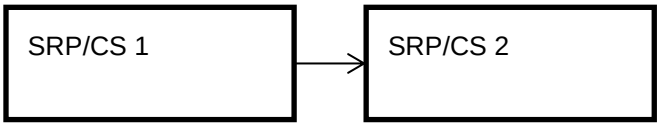


Figure 30: Example single channel, multiple systems

Problem: Given the following values for encapsulated subsystem SRP/CS 1 and encapsulated subsystem SRP/CS 2, calculate the PFH and PL of the safety function SRP/CS:
Subsystem SRP/CS 1:

- Structure Category 3;
- $MTTF_D$ = 15yrs;
- DC_{avg} = 90%;
- CCF is achieved.

Subsystem SRP/CS 2:

- Structure Category 2;
- $MTTF_D$ = 12yrs;
- DC_{avg} = 90%.

Solution:
For Subsystem SRP/CS 1

- A DC_{avg} of 90% is a Medium $DC_{avg;}$
- Locate 15 years in the $MTTF_D$ column and draw a horizontal line into the Category 3 DC_{avg} Medium column (from table K.1 ISO 13849-1:2023).

	Average probability of a dangerous failure per hour (PRF) (1/h) and corresponding performance level (PL)						
MTTFD for each channel years	**Cat.B** DC_{avg} = none	**Cat.1** DC_{avg} = none	**Cat.2** DC_{avg} = low	**Cat.2** DC_{avg} = medium	**Cat.3** DC_{avg} = low	**Cat.3** DC_{avg} = medium	**Cat.4** DC_{avg} = high
15	7.61×10^{-6} b		4.53×10^{-5} b	3.01×10^{-5} b	1.82×10^{-5} c	7.44×10^{-7} d	

Informative Note: *The channels’ symmetrized $MTTF_D$ value is used for system evaluation in Structure 3 and 4. See Annex D Section 1.IV*

PFH(1) = 7.44×10^{-7} and a PL_d

For Subsystem SRP/CS 2

- A DC_{avg} of 90% is a Medium DC_{avg}
- Locate 12 years in the $MTTF_D$ column, and draw a horizontal line into the Category 2 DC_{avg} Medium column:
  - from Table 14, PFH (2) = 4.04×10^{-6} and a PLb

To calculate the PL of the total system or safety function, add the PFH of its components.
Here, PFH(1) + PFH(2).

The System PFH = $(4.04 + 0.744) \times 10^{-6} = 4.784 \times 10^{-6}$

Determine the PL level from Table 6. Since 4.78×10^{-6} lies between 3×10^{-6} and 1×10^{-5} the system is PLb.
The total system structure is Category 2 as a system structure may not be higher than its lowest subsystem.

E.7 Combination method to estimate the PL of a safety function

If a safety function that is made of multiple Encapsulated Subsystem SRP/CS, from multiple input devices, logic devices and output devices, the PL of the total SRP/CS may be estimated using just their individual PL.

With the PL value of each of the subsystems' SRP/CS, the PL of the safety function is estimated from Table 15. This method identifies the subsystem with the lowest PL of the safety function, and the number of subsystems of the same PL value.

PL_{Low} is the lowest subsystem PL in a safety function
N_{Low} is the number of subsystems with the same PL_{Low}

Table 15 — Calculation of PL for series alignment of SRP/CS
(from ISO 13849-1:2023 Table 11)

PL_{low}	N_{low}	→	PL
a	> 3	→	None, not allowed
	≤ 3	→	a
b	> 2	→	a
	≤ 2	→	b
c	> 2	→	b
	≤ 2	→	c
d	> 3	→	c
	≤ 3	→	d
e	> 3	→	d
	≤ 3	→	e

Note: The values calculated for this look-up table are based on reliability values at the mid-point for each PL.

Calculate the PL for each subsystem of the SRP/CS, as in the example above, or use the PL provided by the supplier of the subsystem:

1. $MTTF_{D;}$
2. DC_{avg};
3. Structure Category;
4. CCF (depending on the structure category);
5. Calculate the PL for each subsystem SRP/CS.

E.8 Example on estimating the Safety Function PL from a combination of the SRP/CS

The SRP/CS with several combined subsystems is shown in Figure 31.

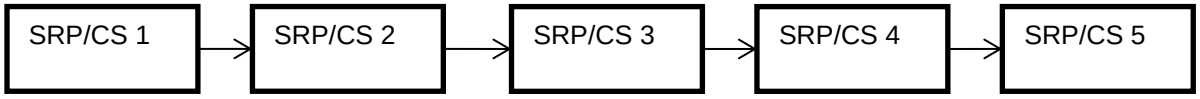


Figure 31: Example of combination of SRP/CS's

PL_{Low} = b and N_{Low} = 3

From Table 15 above, a PL_{Low} of b with an N_{Low} of 3, which is > 2, results in a PL_a for the safety function.

Informative Note: *This method is not very accurate as it uses the median PFH of each subsystem PLs' category in its evaluation. More accurate total system PL values may be achieved by using the actual PFH of each subsystem using the method of Annex D Section 1 D1.4 for a single channel. However, many of the commercially available subsystems provide ONLY the PL or SIM CL values not their actual PFH. This may in part be due to their design assumptions whether wear items such as output relays are included. This PLs is valid only for the duration of the mission life of the subsystem and only when applied per supplier installation and use. If the PL of only some of the subsystems is known, the PFH of subsystems comprised of the individual remaining components may be calculated and their combined PFH determined to form a composite PL. This PL is then combined with the PL of the commercial subsystems as above.*

E.9 Evaluating the PL_r and calculating the PL through 3rd party software

The use of third party software to calculate the PL is the most accurate method and the most convenient.

Informative Note: *These are available from various sources both as freeware and as purchased software. Additionally, safety system design and ISO 13849 application rules may be embedded in the program, potentially preventing errors. Many suppliers supply libraries which can be imported directly into the calculator of their safety products' performance and specification. See Figure 30 as an example.*

Free software for calculating the PL is the international IFAs SISTEMA software; the link below is to the source site. Many of the major safety product suppliers have posted a library of their products' performance levels and some specification and application data on their websites. The IFA source also contains links to SISTEMA 'cookbooks' for operational instructions.

Link: https://www.dguv.de/ifa/praxishilfen/practical-solutions-machine-safety/software-sistema/index.jsp

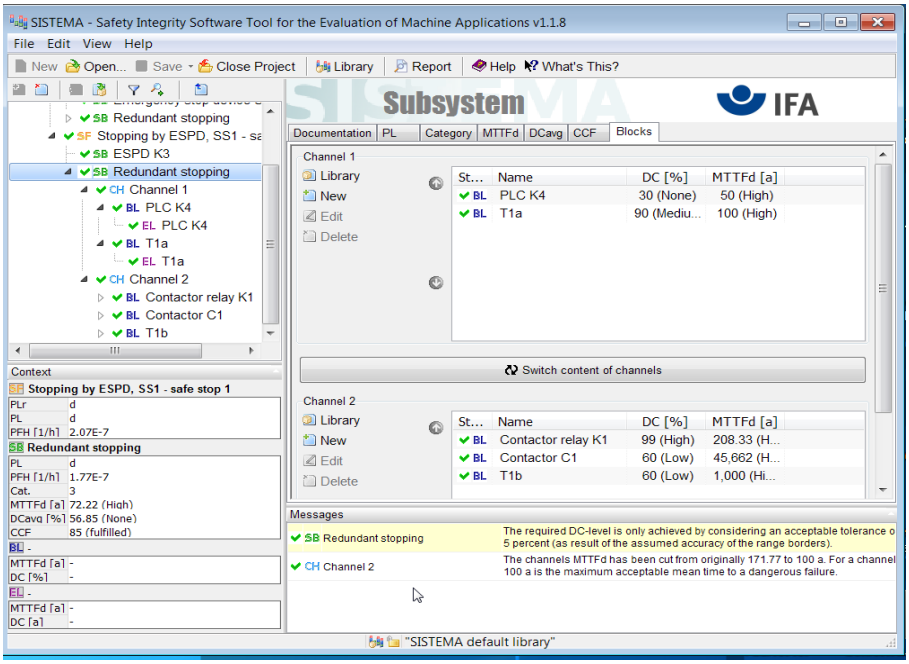


Figure 32: Calculation of PL using IFA SISTEMA computer program

These deliver the most accurate (and typically higher) $MTTF_D$ and PL values because each subsystem SRP/CS or channel is being calculated via its specific PFH or $MTTF_D$. Therefore, the combination of different subsystems' SRP/CS's will add up their individual PFH and will not use the combination method which uses the median of the PFH of their PL. Similarly, the DC_{avg} actual value is used, giving credit to an 89% which in the table evaluation is degraded to "low" or 60% since it is below the "medium" value of 90%. It should be remembered, however, that any of the calculations are based on numerous assumptions of component construction, installation, and application specifics which may render the assumptions to be inappropriate. The apparent accuracy of a five-digit PFH resultant should not mislead. When comparing competitive designs, no real value should be placed on the resultant PFH beyond the most significant digit of the characteristic and the times 10 exponent.

The convenience of the software is due to:

- Manufacturer libraries; generally 3rd party software contains libraries that can be populated with values for each supplier's components or subsystems, for example:
  - Structure category;
  - $MTTF_D$ and B_{10D} values;
  - PL for subsystems SRP/CS in some cases.
- PFH values for subsystems SRP/CS in some cases;
- The software usually generates a report with the required PL_r for each safety function along with the achieved PL and details of the components used.

One of the most valuable features of such a program is the ability to calculate "what if" scenarios which permit the evaluation of the impact of changing the specification of one component or subsystem with another, on the overall performance of the entire SRP/CS for that safety function.

Annex F – Analysis of Circuit Considerations
(Informative)

F.1 Component / Equipment Failures

The component / equipment failures to be addressed in the design of the system isolation equipment include but are not limited to:

1) Power contactor failures:
   a) Power contact(s) broken or welded, won't open;
   b) Auxiliary contact won't change state due to mechanical link failure;
   c) Auxiliary contact(s) welded;
   d) Auxiliary contact(s) are not making a circuit due to corrosion or other foreign material.

2) Connection from monitored circuit to voltage check component (e.g., relays) failures:
   a) One wire open;
   b) Multiple wires open.

3) Voltage check (e.g., relays) failures:
   a) Open coil;
   b) Contact won't change state due to mechanical link failure;
   c) Contact(s) welded;
   d) Contact(s) not making a circuit due to corrosion or other foreign material.

4) Component failure:
   a) Example failures to consider:
      i) Open coil;
      ii) Other internal failure of the respective component.
   b) Contact failures:
      i) Circuit to switch shorted;
      ii) Circuit to switch open;
      iii) N.O. contacts will not open;
      iv) N.O. contacts will not close;
      v) N.C. contacts will not open;
      vi) N.C. contacts will not close;
      vii) Contacts won't change state due to mechanical link failure;
      viii) N.C. auxiliary contact will not open;
      ix) N.C. auxiliary contact will not close.
   c) Verification light at disconnect station failures:
      i) Light burn out.

The results for each failure event need to be addressed in the design of the system isolation equipment include but are not limited to:

1) effect on verification light;
2) detection of the failure;
3) overall design of the system isolation equipment such that any failure will not diminish the required Category 4 safety performance.

F.2 Failure Analysis Techniques

Failure Mode and Effect Analysis (FMEA) is a qualitative analysis that uses inductive reasoning (or “bottom-up” logic) that evaluates the occurrence of a single failure (or fault) on the components, modules, devices and systems. The consequences of each failure are documented individually and those resulting in a situation that does not comply with the performance requirement or otherwise create a hazardous condition should be corrected. Failure Modes, Effects and Criticality Analysis (FMECA) add to FMEA by including a method to evaluate the probability of a failure versus the severity of its consequences. Several FMEA methodologies are available including, but not limited to the following:

- **AIAG FMEA-4** - Potential Failure Mode and Effects Analysis;
- **AIAG MFMEA** - FMEA for Tooling and Equipment (Machinery FMEA);
- **IEC 60812** - Analysis Techniques for System Reliability – Procedure for FMEA;

- **MIL–HDBK–338B** - Electronic Reliability Design Handbook – section 7.8;
- **SAE J1739** - Potential Failure Mode and Effects Analysis in Design (DESIGN FMEA), Potential Failure Mode and Effects Analysis in Manufacturing and Assembly Processes (PROCESS FMEA).

For additional examples to consider, refer to ISO 13849-2 Annexes A through D and ANSI B11.TR4.

The failure mode analysis techniques that may be used include but are not limited to:

1) Failure mode and effects analysis (FMEA for hardware and FMECA for the consequences – see Informative Note below) as appropriate to:
   a) evaluate the effects and the sequences of events caused by each identified failure;
   b) determine the significance or criticality of each failure to the system's correct function or performance;
   c) classify identified failures according to their detect ability and any other relevant characteristic;
   d) estimate the significance and probability of failure.

Informative Note: *The FMEA and FMECA are methods of reliability analysis intended to identify failures that have significant consequences affecting the system performance in the application considered. For more information about FMEA methodology, see IEC 60812 "Analysis Techniques for System Reliability - Procedure for Failure Mode and Effects Analysis (FMEA)."*

2) Fault Tree Analysis (FTA) is a process that uses deductive reasoning (or "top-down" logic) that uses models, such as Boolean logic, to diagram combinations of failures, faults and other events that can result in a hazardous situation. Several FTA methodologies are available including, but are not limited to:

- **ANSI / AIAA S-102-2-18** - Performance-Based Fault Tree Analysis Requirements;
- **IEC 61025** - Fault Tree Analysis;
- **MIL–HDBK–338B** - Electronic Reliability Design Handbook – subclause 7.9.

Fault tree analysis is used (as appropriate) for the:

   a) identification of the causes or combinations of causes leading to the hazard;
   b) determination of whether a particular reliability measure meets the stated requirement;
   c) demonstration that assumptions made in other analyses, regarding the independence of systems and non-relevance of failures, are not violated;
   d) identification of common events or common cause failures.

Informative Note: *The fault tree analysis is particularly well suited to the analysis of complex systems comprising several functionally related or dependent subsystems with different performance objectives. The fault tree itself is an organized graphical representation of the conditions or other factors causing or contributing to the occurrence of a defined undesirable event, referred to as the "top event." Fault tree analysis is a deductive (top-down) method of analysis aimed at pinpointing the causes or combinations of causes that can lead to the defined top event.*

F.3 System or Component Failures

System or component failures to be considered and managed include, but are not limited to:

1) Engineering controls – devices and other inputs:
   a) failure of the output devices;
   b) failure to detect the individual(s) at the hazard zone;
   c) EMC interference;
   d) improper response time;
   e) power source failure.

2) Interfaces:
   a) failure to respond due to short or open;
   b) indeterminate response;
   c) failure to perform its safety-related function(s).

3) Control elements of the machine actuators:
   a) failure to turn off / release / stop;
   b) indeterminate output.

4) Failure of the programmable electronic device (PED):
   a) Input:
      i) no response to input signal;
      ii) indeterminate response.
   b) Output:
      i) output stays on or off;
      ii) indeterminate output.
   c) Memory:
      i) loss or corruption;
      ii) bit failure;
      iii) not easily alterable;
      iv) security procedure;
      v) address or data gate failures.
   d) Internal communications links and busses:
      i) loss of connection;
      ii) I / O failures;
      iii) response time;
      iv) data corruption.
   e) Central Processing Unit:
      i) improper response to commands;
      ii) I / O failures;
      iii) response time.
   f) Environmental considerations. The following environmental conditions can cause faults to occur in those items described above:
      i) EMC (EMI, RFI, ESD), burst, fast transient, conductive induced, surge;
      ii) EMC emissions, RF, line conducted, EMI;
      iii) temperature / humidity;
      iv) pollution, dust, water, oil, corrosives;
      v) shock / vibration.
   g) Input power (variations and interruptions):
      i) See NFPA 79 for additional information.

F.4 Example of System Fault Analysis

Figure 33 below shows a schematic of a dual channel safety system using a safety interface module (SIM). Two dual channel interlocks are connected in series to the input of the SIM. The SIM turns on two Force-Guided Relays, which in turn energize the hazardous portion of the machine.

A basic understanding of the SIM is required to help with the system fault analysis. The figure shows the basic parts of a typical SIM. Power enters the SIM and goes through a Short Circuit Protection (SCP) device. The power is “conditioned” and fed to the other internal parts of the SIM. The power exits the SIM to go to one of the contacts of the interlock. After passing through the interlocks, the power is connected to a Force-Guided Relay driving Channel 1. Channel 1 is pulled-up to power. The SIM power is connected to the Force-Guided Relay driving Channel 2. The negative side of Channel 2 goes out to the interlock. After passing through the interlocks, the signal goes back into the SIM and connects Channel 2 to ground. Channel 2 is pulled down to ground. Although there are other techniques used by SIMs, this figure is intended to show the principles of fault detection. The following queries address wiring short circuit faults. Other faults (such as open circuit, mechanical, component) should also be considered to complete the analysis.

The safety system designer should answer these questions about potential faults:

1. Can the fault be detected?
2. When can the fault be detected?
3. How does the system react to the fault?
4. Can the fault be masked or reset?
5. If the fault cannot be detected, how does the system respond if an additional fault occurs?
6. Can alternative measures be employed or may fault exclusion be justified?

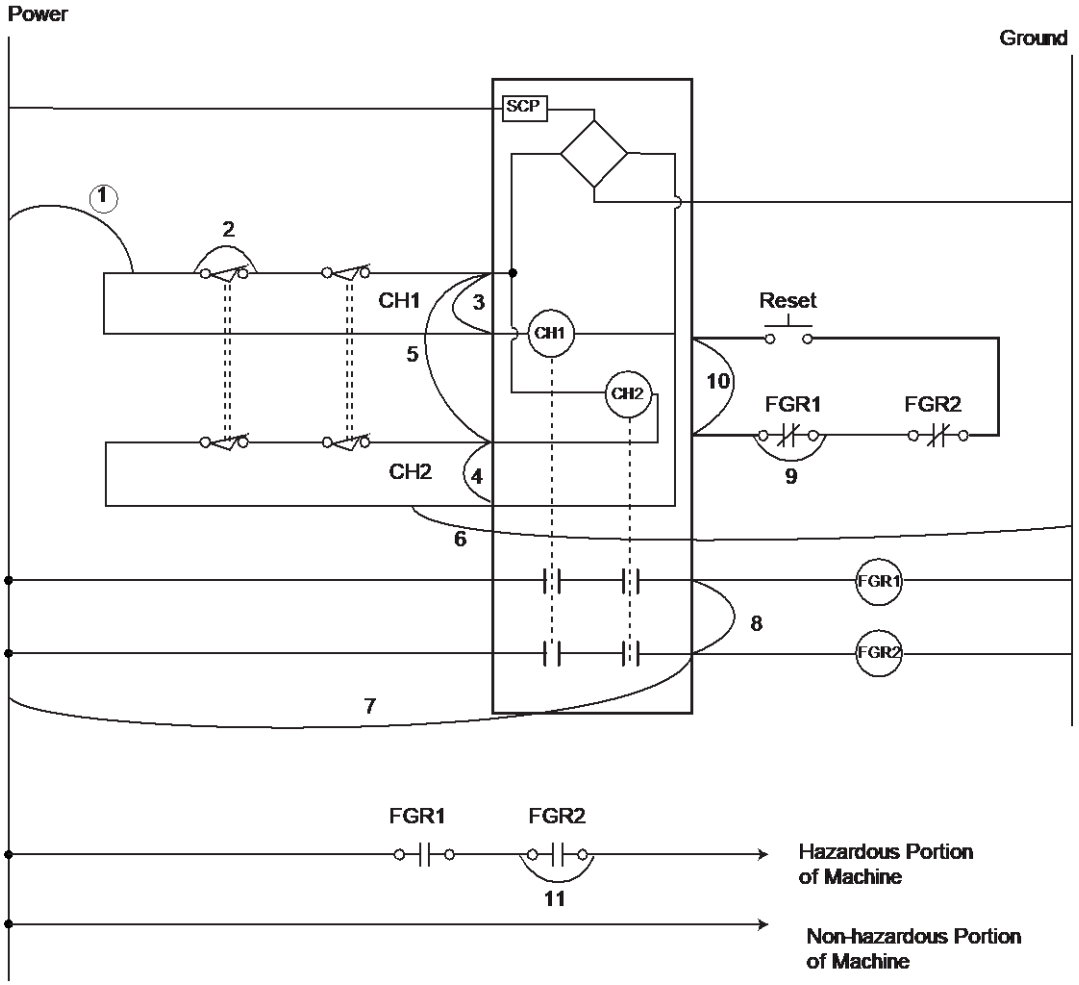


Figure 33: Typical dual channel safety system using a SIM

Fault analysis:

1. Fault from power to CH1:
    a. This fault is detected by the SIM;
    b. When the interlock is open, the SIM de-energizes the hazardous portion of the machine. When the interlock is closed, the fault is detected by the SIM;
    c. The SIM prevents energization of the hazardous portion of the machine;
    d. This fault cannot be masked by opening and closing the interlocks. The fault can be reset by cycling power to the SIM.
2. Fault across one of the interlock contacts:
    a. This fault is detected by the SIM;
    b. When the interlock is open, the SIM de-energizes the hazardous portion of the machine. When the interlock is closed, the fault is detected by the SIM;
    c. The SIM prevents energization of the hazardous portion of the machine;
    d. This fault can be masked by opening and closing the other interlock. The fault can be reset by cycling power to the SIM;
    e. If masked or reset, a second fault across the other interlock contact leads to the loss of the safety function.
3. Fault across CH1 at the SIM terminals:
    a. Same as Fault 1.

4. Fault across CH1 at the SIM terminals:
    a. The results are similar to Faults 1 and 3.
5. Fault from CH1 to CH2 at the SIM:
    a. This fault is detected by the SIM;
    b. This fault is detected immediately by the SCP of the SIM;
    c. The outputs of the SIM de-energize and remove power to the hazardous portion of the machine;
    d. This fault cannot be masked or reset.
6. Short from CH2 to ground:
    a. This fault is detected by the SIM;
    b. When one of the interlocks is opened, the SIM de-energizes the hazardous portion of the machine. When the interlock is closed, the fault is detected by the SIM;
    c. The SIM prevents energization of the hazardous portion of the machine;
    d. This fault cannot be masked by opening and closing the interlocks. The fault can be reset by cycling power to the SIM.
7. Short from Power to Output 2 of the SIM:
    a. This fault is detected by the SIM;
    b. When one of the interlocks is opened, the SIM de-energizes the hazardous portion of the machine by turning off FGC1. When the interlock is closed, the fault is detected by the reset circuit of the SIM;
    c. The SIM prevents re-energization of the hazardous portion of the machine;
    d. This fault cannot be masked by opening and closing the interlocks. The fault can be reset by cycling power to the SIM.
8. Short circuit from FGR1 to FGR2:
    a. This fault cannot be detected by the SIM. This fault should be considered for exclusion;
    b. A second fault (fault #7) will lead to the loss of the safety function.
9. Short across one of the FGR1 feedback contacts:
    a. This fault cannot be detected by the SIM. This fault should be considered for exclusion.
10. Short across the reset connections of the SIM:
    a. If the SIM is designed or configured for automatic reset, this fault can only be detected by observation by the machine user. The safety system will be reset as soon as the interlocks are closed. This fault is not detected by the SIM. If the SIM is designed or configured for monitored reset, this fault will be detected by the SIM.
    b. If the reset is monitored, the SIM will not re-energize its outputs.
11. Fault across one of the output contacts of the FGR1:
    a. This fault cannot be detected by the safety system. This fault should be considered for exclusion.

Fault Exclusion

During the analysis, certain faults may be uncovered that cannot be detected during operation without undue economic cost(s). Further, the probability that these faults might occur may be made extremely small by using mitigating design, construction and installation. Under these conditions, the faults may be excluded from further consideration. Recommended preventive maintenance procedures should be included in the justification so that the basis of the exclusions remains valid.

Fault exclusion can be based on, but not limited to the following factors:

- the low probability of occurrence of some faults;
- tried and true (sound) engineering safety practices;
- application-specific technical requirements for the specific hazard.

Detailed justification should be given in the technical documentation for any excluded faults. See ISO 13849-2, Annexes A through D which provide guidance on fault exclusion and its justification.

Annex G – Failures, Systemic
(Informative)

G.1 General
ISO 13849-2 gives a comprehensive list of measures against systematic failure which should be applied, such as basic and well-tried safety principles.

G.2 Measures for the Control of Systematic Failures
The following measures should be applied:

a) Use of de-energization (see ISO 13849-2);
   - the SRP/CS should be designed so that with loss of its power supply, a safe state of the machine can be achieved or maintained.

b) Measures for controlling the effects of voltage breakdown, voltage variations, overvoltage, under voltage;
   - SRP/CS behavior in response to voltage breakdown, voltage variations, overvoltage, and under voltage conditions should be predetermined so that the SRP/CS can achieve or maintain a safe state of the machine (see also IEC 60204-1 and IEC 61508-7:2010, A.8).

c) Measures for controlling or avoiding the effects of the physical environment (for example, temperature, humidity, water, vibration, dust, corrosive substances, electromagnetic interference and its effects);
   - SRP/CS behavior in response to the effects of the physical environment should be predetermined so that the SPR/CS can achieve or maintain a safe state of the machine (see also, for example, IEC 60529, IEC 60204-1).

d) Program sequence monitoring should be used with SPR/CS containing software in order detect defective program sequences;
   - a defective program sequence exists if the individual elements of a program (e.g., software modules, subprograms or commands) are processed in the wrong sequence or period of time or if the clock of the processor is faulty (see IEC 61508-7:2010, A.9).

e) Measures for controlling the effects of errors and other effects arising from any data communication process (see IEC 61508-2:2010, 7.4.11).

In addition, one or more of the following measures should be applied, taking into account the complexity of the SRP/CS and its PL:

- failure detection by automatic tests;
- tests by redundant hardware;
- diverse hardware;
- operation in the positive mode;
- mechanically linked contacts;
- direct opening action;
- oriented mode of failure;
- over-dimensioning by a suitable factor, where the supplier can demonstrate that de-rating will improve reliability; where over-dimensioning is appropriate, an over-dimensioning factor of at least 1.5 should be used.

G.3 Measures for Avoidance of Systematic Failures

The following measures should be applied:

a) Use of suitable materials and adequate manufacturing;
   - selection of material, manufacturing methods and treatment in relation to, e.g., stress, durability, elasticity, friction, wear, corrosion, temperature, conductivity, and dielectric rigidity.

b) Correct dimensioning and shaping;
   - consideration of, e.g., stress, strain, fatigue, temperature, surface roughness, tolerances, and manufacturing.

c) Proper selection, combination, arrangements, assembly and installation of components, including cabling, wiring and any interconnections;
   - apply appropriate standards and supplier application notes, e.g., catalogue sheets, installation instructions, specifications, and use of good engineering practice.

d) Compatibility;
   - use components with compatible operating characteristics.

e) Withstanding specified environmental conditions;
   - design the SRP/CS so that it is capable of working in all expected environments and in any foreseeable adverse conditions, e.g., temperature, humidity, vibration and electromagnetic interference (EMI) (see IEC 61508-7:2010, B.3.3).

In addition, one or more of the following measures should be applied, taking into account the complexity of the SRP/CS and its PL:

a) Hardware design review (e.g., by inspection or walk-through);
   - to reveal, by reviews and analysis, discrepancies between the specification and implementation (see IEC 61508-7:2010, B.3.7 and B.3.8).

b) Computer aided design tools capable of simulation or analysis;
   - perform the design procedure systematically and include appropriate construction elements that are already available and tested (see IEC 61508-7:2010, B.3.5).

c) Simulation;
   - perform a systematic and complete inspection of an SRP/CS design in terms of both the functional performance and the correct dimensioning of their components (see IEC 61508-7:2010, B.3.6).

G.4 Measures for Avoidance of Systematic Failures During SRP/CS Integration

The following measures should be applied during integration of the SPR/CS:

- functional testing;
- project management;
- documentation.

In addition, black-box testing should be applied, taking into account the complexity of the SPR/CS and its PL.

Annex H – General Overview of Valves
(Informative)

This annex provides a general primer on valve components, types of valves, and the reliability of valves.

Actuator
Component (for example, motor, cylinder) that transforms fluid energy into mechanical energy.

Direct Acting
A valve whose main spool or elements position is controlled by generating a force through a coil to a push pin or rod which pushes or pulls on the spool to control valve position.

Pilot operated
A valve whose main spool or elements position is controlled by a secondary valve that delivers or vents pressure to the ends of the main element to control valve position.

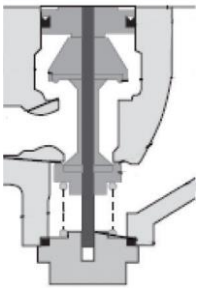
Interleaving Spring
A spring designed such that a break will not allow the two sections to coil into themselves, thereby resulting in a shorter spring length. Springs should be installed around a rod or mounted in a hole.

Ingression
A means or place where contamination is generated or enters the system. Contamination can come from the supply, can be generated internally due to wear of metal or rubber components, or can come from the process, typically from material that has collected on the cylinder rods or ingested through the reservoir breather.

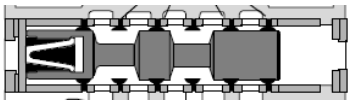
Fluid
Hydraulic, pneumatic, lubrication or other liquids or gasses.

Valve Element
The internal portion of a valve which moves to cause changes in the flow paths of the air or fluid. This may be a spool, poppet, slide, or other design. This may also include pilot sections of pilot operated valves.

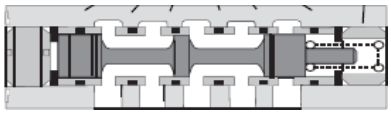
Poppet Valve (Hydraulic or Pneumatic)
A type of element construction in which the element moves perpendicular to the sealing surface (similar to the exhaust poppet in an automobile engine). When applied to machines supplied with industrial quality air or hydraulics, the poppet design is the most dependable due to the internal force balances on the elements. The internal valve forces are biased towards the un-energized condition. The fluid also flows over the sealing surface which helps prevent contaminants from being deposited. It typically requires component failure or severe contamination to cause an unsafe fault condition.



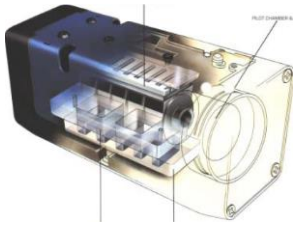
Resilient Seal Spool Valve (Pneumatic Only)
A type of element construction incorporating a spool which slides inside of soft seals (such as O-rings) which provide sealing between the ports in the body and the spool. Failure modes: resilient seal wear due to high cycles or contamination causing leakage which can lead to unintended motion. Failure is normally slow over the life of the product but *can* be sudden and catastrophic. Contamination can also lead to a delay in shift time, failure to shift at all and stopping at any point in its travel. This design is the least sensitive to sticky contamination but most prone to wear from solid particulate.



Spool Valves
A type of element construction incorporating a spool which slides on a thin film of the pressurized media (air or oil). Failure modes: normal leakage and metal to metal seal wear resulting in leakage. Wear is gradual over time and does not normally result in unintended motion. Contamination can also lead to a delay in shift time, failure to shift at all and stopping at any point in its travel. In pneumatic systems, this design is particularly sensitive to lubrication that has been allowed to dry. This design is the most sensitive to sticky contamination but least prone to wear from solid particulate.



Slide Valve (Pneumatic Only)
A type of element construction incorporating a plate which slides on a thin film of the pressurized air.
Failure modes: plate-to-plate seal wear resulting in leakage. Wear is gradual over time and does not normally result in unintended motion. Contamination can also lead to a delay in shift time, failure to shift at all and stopping at any point in its travel. In pneumatic systems, this design is particularly sensitive to lubrication that has been allowed to dry.



Relative Valve Dependability Guide

Crossover Valve	Poppet Construction	"O" ring spool Construction	Air Bearing spool Construction	Slide/plate Construction
HIGH				**LOW**

Valve Cross Over and "Ghost" Positions
Valve elements transit over various conditions as they shift. The published schematics are not able to convey this valve shifting position information. These conditions might not be disclosed or only partially disclosed in catalog information. The typical valve can be described as having an open crossover or a closed crossover. In an open crossover position, the fluid path is open between the three ports instead of the typical two, which can result in a port not being fully pressurized. In a closed crossover position, the fluid path is blocked thereby trapping pressure that is expected to be fully pressurized or exhausted.

The designer is cautioned to investigate these conditions in safety and non-safety valving within the circuit and to ensure that they do not create an unsafe condition. Images A through E display some potential spool and sleeve valve positions. These are meant to illustrate the potential crossover hazards that can exist within a 5/3 close center valve. Crossover position concerns are not limited to a particular valve design or supplier.

Image A:
An un-energized spool and sleeve valve has one port open from IN to OUT with the exhaust blocked. The other potential outlet port is open to exhaust.

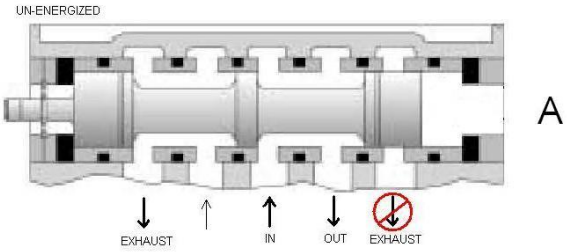


Image B:
An energized spool and sleeve valve has the second outlet port open to the inlet and the initial outlet port open to exhaust.

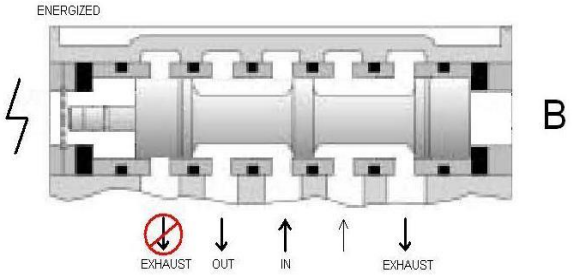


Image C:
This image depicts a spool and sleeve valve that is stuck in a mid-position that blocks all ports. The outlet pressure is trapped and cannot be exhausted.

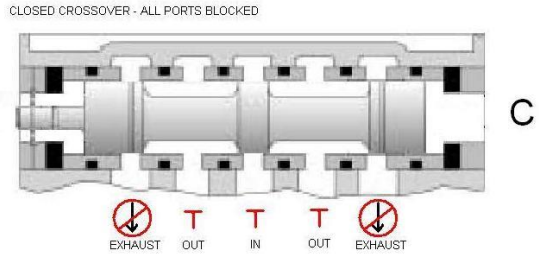


Image D:
This image depicts a spool and sleeve valve that is stuck in a mid-position that supplies inlet pressure to both outlet ports and the exhaust is blocked.

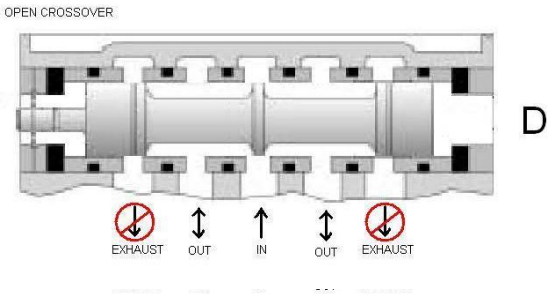
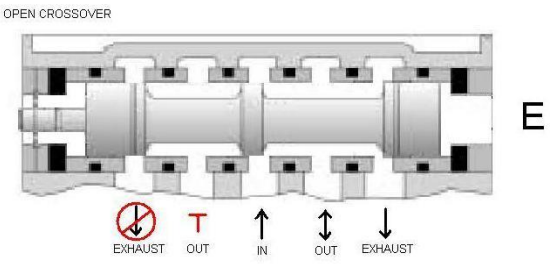


Image E:
This image depicts a spool and sleeve valve that is stuck in a mid-position that has the supply open to an outlet and exhaust port while the second outlet port exhaust path is blocked.



Internal Safety Valve Monitoring
A means to determine the required safety level of the valve is present. Detection of a fault (diminished performance or traditional) of one element in a dual channel device indicates a reduction in the level of safety protection previously provided due to the loss of the redundant feature. In single channel devices, detection of a fault indicates the possible inability of the valve to operate properly and the complete loss of any safety level previously present. The monitoring should also inhibit further operation of the machine upon fault detection until the valve is reset. The valve reset shall be consistent with 6.4.2.

External Valve Monitoring
Electrical devices external to a sensing type valve that provide for safety valve monitoring. A safety PLC or an appropriate safety interface module (SIM) can be programmed to detect diminished performance and standard faults.

Standard Industrial Quality Solenoid Valves
These are not safety devices and shall not be used as such. However, they may be used as directional control valves provided that their energy supply comes from a safety valve whose rating meets the appropriate safety level determined during the risk assessment.

Soft Start Valves
A valve which gradually reapplies the pneumatic pressure to avoid shock. When the risk assessment determines that the reapplication of the pneumatic supply causes dangerous undesirable rapid movement of components such as cylinders, the designer should consider incorporating a soft start type valve to gradually re-pressurize the system, providing slow gradual movement. The soft start valve should not inhibit the exhaustion of the downstream air.

Velocity Fuse (Hose Failure Automatic Shut Off Valve)
A device which senses the change in flow which occurs upon failure of a hose end and automatically reduces or shuts off the flow so as to avoid hose whip. Currently, 29 CFR 1926.302(b)(7) (OSHA construction industry regulatory standards) only requires these on hoses greater than ½ inch, and only when used with hand tools.

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

The purpose of the requirements of this standard is to prevent exposure to hazardous motion (or situations) by mitigating the risk of failure, faults and inadequate design practices and by improving the integrity, reliability, and the performance of the safety-related functions. The level of performance of the safety-related function(s) depends on the level of risk associated with the hazard. See clause 5.

There are various design strategies that may be used so that failures of components, modules, devices or systems meet the required level of performance. Some design strategies may allow an accumulation of single failures and yet still stop (or prevent the re-initiation of) hazardous motion (or situations) when the next critical failure would cause loss of the safety-related function. Other strategies include self-diagnosis to determine and respond to failures. Still other strategies use tried and proven components and design principles to reduce the probability of a failure to an acceptable level of risk.

Control reliability is a design strategy, method or feature that separates the safety-related functions of a system into components, modules, devices or systems that may be monitored or checked by other components, modules, devices or systems. It is axiomatic that protection from the loss of safety-related functions due to multiple, simultaneous failures (common cause) of components, sometimes referred to as "fail-safe," is not practically achievable. Catastrophic failure of the machine actuator (electrical, mechanical or fluidic) may result in the loss of the safety-related function.

The use of redundant components, modules, devices or systems (with or without monitoring or checking) is frequently used in process control systems where the goal is to maintain the process in the event of a failure. Aircraft systems, chemical processing plants and electrical power transmission systems are just a few examples of applications where the process must continue in the presence of a failure.

The goal of control reliability is to create a safety-related function(s) such that a reasonably foreseeable, single failure does not lead to the loss of the safety function or does not prevent a normal or immediate stop from occurring. The failure or the resulting fault must be detected at or before the next demand of safety (e.g., at the beginning or end of a cycle, or when an engineering control – device is actuated). The safety-related part of the control system then must initiate an immediate stop command or prevent the next machine cycle or hazardous situation until the failure is corrected.

In addition to the use of well-tried, robust components and generally accepted principles, reasonably foreseeable single failures that can result in the loss of the safety function shall be detectable, or those that are not detectable shall be designed out, or the probability minimized to an acceptable level of risk (see Fault Exclusion below and ANSI B11.0).

Control reliability is not provided by simple redundancy. There must be monitoring to verify that redundancy is maintained. Control reliability uses monitoring and checking to determine that a discernable component, module, device or system has failed and that the hazardous motion (or situation) is stopped or is prevented from starting or restarting.

Informative Note: *Because some failures cannot be detected until the completion of a cycle or a portion of the cycle, the loss of safety-related functions may occur for a portion of the cycle.*

Control reliability of electrical, electronic, pneumatic, or hydraulic systems or devices frequently consists of monitored, multiple and independent parallel or series components, modules, devices or systems. Control reliability of machine control systems or devices may be achieved by the use of, but not limited to, one or both of the following:

- the use of two or more dissimilar components, modules, devices or systems, with the proper operation of each being verified (monitored) by the other(s);
- the use of two or more identical components, modules, devices or systems, with the proper operation of each being verified (monitored) by the other(s).

These methods require that the engineering control – device, its interface to the control system (or directly to the actuator control) and actuator control meet the requirements listed in subclause 6.1.

Another control reliability strategy may be used when the machine motion is stopped and reinitiated at least once per cycle. This strategy requires that the control system and the actuator control utilize the design methods above. The engineering control – device and its interface may or may not be control reliable. The control system must be designed to require that the device and its interface is exercised automatically or by the operator (e.g., releasing hand controls or interrupting an electro-optical device) before a subsequent machine cycle may be initiated so that these elements do not lead to the loss of the safety-related function(s) beyond one cycle.

In any strategy, "*Fault Exclusion*" is an important tool. If the design eliminates the possibility of various failures, the designer can justify a fault exclusion through the risk assessment process. The principle of fault exclusion must be incorporated into the design and installation to either eliminate, or reduce to an acceptable level of risk, the possibility of catastrophic/common mode failures that could result in loss of the safety function.

Many methods exist to determine if the safety-related functions meet the required performance requirements; three principal examples include:

a) Failure Modes & Effects Analysis (FMEA)
b) Fault Tree Analysis (FTA)
c) Probabilistic determination

Annex F covers FMEA (a) and FTA (b).

Probabilistic determination covers methodologies that use statistical analysis to determine the probability of a failure that will result in a loss of the safety function. Several methodologies are available including, but are not limited to:

- **IEC 61508** - Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems
- **IEC 62061** - Functional Safety of Safety-Related Electrical, Electronic, and Programmable Electronic Control Systems
- **ISO 13849-1** - Safety of machinery - Safety-related parts of control systems - Part 1: General principles for design

The achievement of control reliability is dependent upon the selection and integration of components, modules, devices and systems that have been specifically designed and intended for use in safety-related functions. A disciplined design process, including design guidelines, peer review and other elements, is important for achieving completeness and accuracy of the design, and should be implemented so that control reliability is achieved.

Annex J – External Device Monitoring by the Safety-Related Function
(Informative)

J.1 External Device Monitoring

Depending on the level of risk, it may be critical to verify the normal functioning of control elements (such as Force-Guided Relays) between the safety-related function(s) and the machine actuators. A common method of accomplishing this is a monitoring feedback function, which is typically called External Device Monitoring (EDM).

For this monitoring to be reliable, the system should include a normally closed feedback contact that can accurately reflect the status of the control elements. For proper monitoring, the control element should typically have a mechanically linked design (see EN 50205). This ensures that their normally open contacts used for controlling hazardous motion have a positive relationship with the normally closed monitoring contacts.

In a Force-Guided Relay, the mechanically linked design ensures that if the normally open contact welds closed (or otherwise loses its ability to control hazardous motion), the monitor contact will not return to a closed state when the relay coil de-energizes; see Figure 34. This open monitor contact signals a fault to the EDM function. This is not always the case with standard “ice cube” or IEC-style relays; because they cannot detect a welded contact, they should not be used in a high-risk safety circuit.

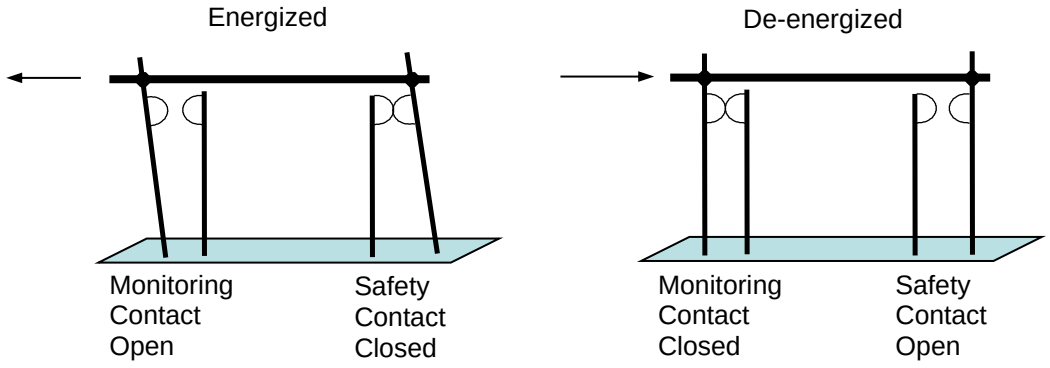


Figure 34 – Mechanically linked contacts

In a redundant circuit, when the fault is detected (immediately or at the next demand on the safety system), the second output channel opens to signal the stop command, and the reset function is prevented.

The EDM function can take several forms, but is typically described as “Single-Channel,” “Dual-Channel,” or “Power-Monitoring.” The following general descriptions are generic only, not all encompassing, and are only intended to highlight the common concepts of the EDM function.

J.2 Single-Channel Monitoring

Single-channel monitoring is a common method in which normally closed contacts from each control element are fed back to the safety-related function (e.g., Safety Interface Module) monitoring input in a series connection. The input should be closed before the run cycle can begin and should re-close after each stop command before another run cycle can begin.

With more sophisticated systems, the timing may be checked to verify that not only does the monitor input close, but that it switches within a specified period of time before another run cycle can begin. This is to detect slowing or sticking control elements that can increase response time which can affect the safe positioning (safety distance) of some engineering controls.

Single channel monitoring is typically accomplished where the safety-related function supplies a return path for current flow (Figure 35, below), where the signal is generated by the supply voltage (Figure 36), or where both the manual reset, and external device monitoring are combined into one input (Figure 37).

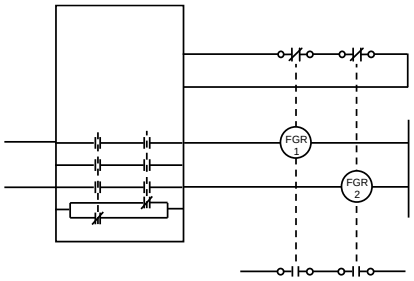


Figure 35

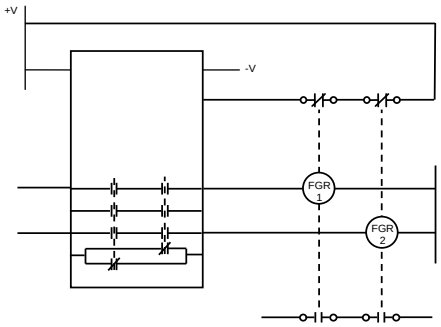


Figure 36

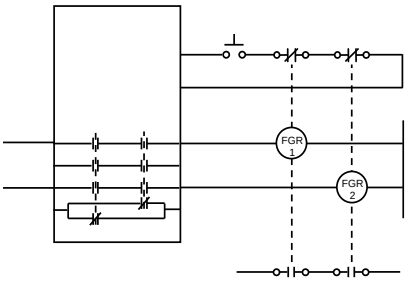


Figure 37

J.3 Dual-Channel Monitoring

In redundant systems, dual-channel monitoring verifies the operation of each control element separately. The monitoring function is similar to single channel monitoring such that the input should be closed before the run cycle can begin and should re-close after each stop command before another run cycle can begin. One difference is that a fault condition is generated if the two inputs are ever in different states (i.e., one open and one closed). This gives dual-channel monitoring the ability to detect additional faults (e.g., a short across a monitoring contact). Depending on the sophistication of the system, diagnostics can also identify which specific element has slowed by checking timing or has completely failed. Dual-channel monitoring is typically accomplished where the safety-related function supplies a return path for current flow (Figure 38), or where the signal is generated by the supply voltage (Figure 39).

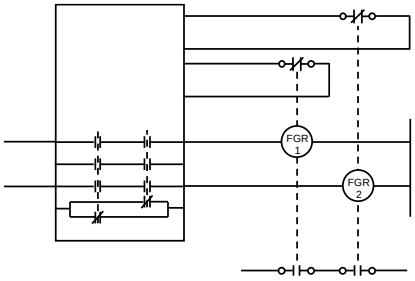


Figure 38

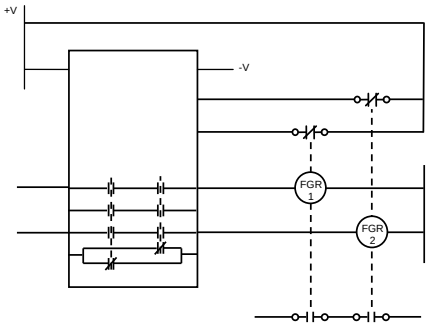


Figure 39

J.4 Power Monitoring

The EDM function is accomplished through the power supply feed and is called a Power Monitoring Circuit. One is normally closed and one normally open contact from each of the control elements are arranged in a series-parallel monitoring circuit (Figure 40). If either control element should experience a failure (such as a welded normally open contact), the difference in states is detected in the power monitoring circuit and will remove power from the safety circuit or safety device. The power supply for the safety device should be designed to tolerate normal transitions of the control elements as they change states. This design can also be configured to detect slowing or sticking control elements if the time of the transition extends beyond a predetermined time.

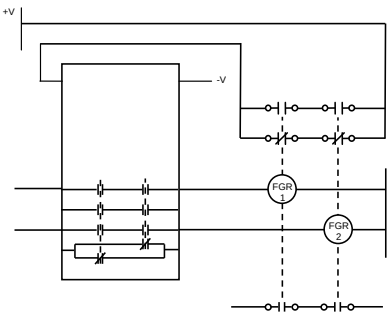


Figure 40: Power Monitoring Circuit

Annex K – Validation Tools for Mechanical Systems

[Annex A of ISO 13849-2:2012]

(Informative)

When mechanical systems are used in conjunction with other technologies, then relevant tables for basic safety and well–tried safety principles should also be taken into account.

K.1 List of basic safety principles

Table 17 — Basic safety principles

Basic safety principles	Remarks
Use of suitable materials and adequate manufacturing	Selection of material, manufacturing methods and treatment in relation to, stress, durability, elasticity, friction, wear, corrosion, temperature, etc.
Correct dimensioning and shaping	Consider factors such as stress, strain, fatigue, surface roughness, sticking tolerances, and manufacturing.
Proper selection, combination, arrangements, assembly and installation of components/system	Apply supplier application notes, for example, catalogue sheets, installation instructions, specifications, and use of good engineering practice in similar components/systems.
Use of de–energization principle	The safe state is obtained by the release of energy. See primary action for stopping in ANSI/ISO 12100. Energy is supplied for starting the movement of a mechanism. See primary action for starting ANSI/ISO 12100. Consider different modes, for example, operation mode, maintenance mode. This principle shall not be used in special applications, for example, to keep energy for clamping devices.
Proper fastening	For the application of screw locking consider supplier application notes. Overloading can be avoided by applying adequate torque loading technology.
Limitation of the generation and/or transmission of force and similar parameters	Examples are break pin, break plate, torque limiting clutch.
Limitation of range of environmental parameters	Examples of parameters are temperature, humidity, and pollution at the installation place. Consider supplier application notes.
Limitation of speed and similar parameters	Consider factors such as speed, acceleration, deceleration required by the application.
Proper reaction time	Consider factors such as spring tiredness, friction, lubrication, temperature, inertia during acceleration and deceleration, combination of tolerances.
Protection against unexpected start–up	Consider unexpected start-up caused by stored energy and after power "supply" restoration for different modes such as operation mode, maintenance mode etc. Special equipment for the release of stored energy may be necessary. Special applications, for example, to keep energy for clamping devices or ensure a position, need to be considered separately.
Simplification	Reduce the number of components in the safety-related system.
Separation	Separation of safety-related functions from other functions.
Proper lubrication	
Proper prevention of the ingress of fluids and dust	Consider IP rating (see IEC 60529).

K.2 List of well-tried safety principles

Table 18 — Well–tried safety principles

Well–tried safety principles	Remarks
Use of carefully selected materials and manufacturing	Selection of suitable material, adequate manufacturing methods and treatments related to the application.
Use of components with oriented failure mode	The predominant failure mode of a component is known in advance and is always the same, see ANSI/ISO 12100.
Over–dimensioning/safety factor	The safety factors are given in standards or by good experience in safety-related applications.
Safe position	The moving part of the component is held in one of the possible positions by mechanical means (friction only is not enough). Force is needed for changing the position.
Increased OFF force	A safe position/state is obtained by an increased OFF force in relation to ON force.
Careful selection, combination, arrangement, assembly and installation of components/system related to the application	-
Careful selection of fastening related to the application	Avoid relying only on friction.
Positive mechanical action	Dependent operation (e.g., parallel operation) between parts is obtained by positive mechanical link(s). Springs and similar "flexible" elements should not be part of the link(s) (see ANSI/ISO 12100).
Multiple parts	Reducing the effect of faults by multiplying parts, e.g., where a fault of one spring (of many springs) does not lead to a dangerous condition.
Use of well–tried spring	A well–tried spring requires: • use of carefully selected materials, manufacturing methods (e.g., presetting and cycling before use) and treatments (e.g., rolling and shot–peening); • sufficient guidance of the spring, and; • sufficient safety factor for fatigue stress (i.e., with high probability a fracture will not occur). Well–tried pressure coil springs may also be designed by: • use of carefully selected materials, manufacturing methods (e.g., presetting and cycling before use) and treatments (e.g., rolling and shot-peening); • sufficient guidance of the spring, and; • clearance between the turns less than the wire diameter when unloaded, and; • sufficient force after a fracture(s) is maintained (i.e., a fracture(s) will not lead to a dangerous condition).
Limited range of force and similar parameters	Decide the necessary limitation in relation to the experience and application. Examples for limitations are break pin, break plate, torque limiting clutch.
Limited range of speed and similar parameters	Decide the necessary limitation in relation to the experience and application. Examples for limitations are centrifugal governor; safe monitoring of speed or limited displacement.
Limited range of environmental parameters	Decide the necessary limitations. Examples on parameters are humidity, temperature, and pollution at the installation. Consider supplier application notes.
Limited range of reaction time, limited hysteresis	Decide the necessary limitations. Consider factors such as spring tiredness, friction, lubrication, temperature, inertia during acceleration and deceleration, combination of tolerances.

K.3 List of well–tried components

Well–tried components for a safety–related application in the following list is based on the application of well–tried safety principles and/or a standard for their particular applications. A well–tried component for some applications can be inappropriate for other applications.

Table 19 — Well–tried components

Well-tried components	Conditions for "well–tried"	Standard or specification
Screw	All factors influencing the screw connection and the application are to be considered.	Mechanical jointing such as screws, nuts, washers, rivets, pins, bolts etc. are standardized.
Spring	See Table K.2 "Use of a well–tried spring".	Technical specifications for spring steels and other special applications are given in ISO 4960.
Cam	All factors influencing the cam arrangement (e.g., part of an interlocking device) are to be considered.	See ISO 14119 (interlocking devices).
Break–pin	All factors influencing the application are to be considered.	-----

K.4 Fault lists and fault exclusions

K.4.1 Introduction

The lists express some fault exclusions and their rationale. The precise instant that the fault occurs can be critical.

K.4.2 Various mechanical devices, components and elements

Table 20 — Mechanical devices, components and elements

(For example: cam, follower, chain, clutch, brake, shaft, screw, pin, guide, bearing)

Fault considered	Fault exclusion	Remarks
Wear / corrosion	Yes, in the case of carefully selected material, (over)-dimensioning, manufacturing process, treatment and proper lubrication, according to the specified lifetime.	See ISO 13849-1.
Untightening / loosening	Yes, in the case of carefully selected material, manufacturing process, locking means and treatment, according to the specified lifetime.	
Fracture	Yes, in the case of carefully selected material, (over)-dimensioning, manufacturing process, treatment and proper lubrication, according to the specified lifetime.	
Deformation by overstressing	Yes, in the case of carefully selected material, (over)-dimensioning, treatment and manufacturing process, according to specified lifetime.	
Stiffness / sticking	Yes, in the case of carefully selected material, (over)-dimensioning, manufacturing process, treatment and proper lubrication, according to specified lifetime.	

K.4.3 Pressure coil springs

Table 21 — Pressure coil springs

Fault considered	Fault exclusion	Remarks
Wear / corrosion	Yes, in the case of the use of well-tried spring(s) and carefully selected fastening(s)	See ISO 13849-1.
Force reduction by setting and fracture		
Fracture		
Stiffness / sticking		
Loosening		
Deformation by overstressing		

Annex L – Validation Tools for Pneumatic Systems

[Annex B of ISO13849-2:2012]

(Informative)

When pneumatic systems are used in conjunction with other technologies, then relevant tables for basic safety and well-tried safety principles should also be taken into account. Where pneumatic components are electrically connected/controlled, the appropriate fault lists in Annex D should be considered.

Informative Note: *Requirements of specific directives could apply such as simple pressure vessels and pressure equipment.*

L.1 List of basic safety principles

Table 22 — Basic safety principles

Basic safety principles	Remarks
Use of suitable materials and adequate manufacturing	Selection of material, manufacturing methods and treatment in relation to, e.g., stress, durability, elasticity, friction, wear, corrosion, temperature.
Correct dimensioning and shaping	Consider e.g., stress, strain, fatigue, surface roughness, tolerances, manufacturing.
Proper selection, combination, arrangements, assembly and installation of components / system	Apply supplier application notes, e.g., catalogue sheets, installation instructions, specifications and use of good engineering practice in similar components/systems.
Use of de–energization principle	The safe state is obtained by the release of energy to all relevant devices. See primary action for stopping in ANSI/ISO 12100. Energy is supplied for starting the movement of a mechanism. See primary action for starting in ANSI/ISO 12100. Consider different modes, e.g., operation mode, maintenance mode. This principle shall not be used in some applications, e.g., where the loss of pneumatic pressure will create an additional hazard.
Proper fastening	For the application of e.g., screw locking, fittings, gluing, clamp ring, consider supplier application notes. Overloading can be avoided by applying adequate torque loading technology.
Pressure limitation	Examples are pressure relief valve, pressure reducing/control valve.
Speed limitation / speed reduction	An example is the speed limitation of a piston by a flow valve or a throttle.
Sufficient avoidance of contamination of the fluid	Consider filtration and separation of solid particles and water in the fluid.
Proper range of switching time	Consider, e.g., the length of pipework, pressure, exhaust capacity, force, spring tiredness, friction, lubrication, temperature, inertia during acceleration and deceleration, combination of tolerances.
Withstanding environmental conditions	Design the equipment so that it is capable of working in all expected environments and in any foreseeable adverse conditions, e.g., temperature, humidity, vibration, pollution. Consider supplier specification/application notes.
Protection against unexpected start–up	Consider unexpected start–up caused by stored energy and after power supply restoration for different modes, e.g., operation mode, maintenance mode. Special equipment for the release of stored energy may be necessary (see ISO 14118). Special applications (e.g., to keep energy for clamping devices or ensure a position) need to be considered separately.
Simplification	Reduce the number of components in the safety–related system.
Proper temperature range	To be considered throughout the whole system.
Separation	Separation of the safety–related functions from other functions.

L.2 List of well–tried safety principles

Table 23 — Well–tried safety principles

Well–tried safety principles	Remarks
Over–dimensioning / safety factor	The safety factor is given in standards or by good experience in safety–related applications.
Safe position	The moving part of the component is held in one of the possible positions by mechanical means (friction only is not enough). Force is needed to change the position.
Increased OFF force	One solution can be that the area ratio for moving a valve spool to the safe position (OFF position) is significantly larger than for moving the spool to ON position (a safety factor).
Valve closed by load pressure	These are generally seat valves, e.g., poppet valves, ball valves. Consider how to apply the load pressure in order to keep the valve closed even if for example, the spring closing the valve breaks.
Positive mechanical action	The positive mechanical action is used for moving parts inside pneumatic components.
Multiple parts	See list of basic safety principles.
Use of well-tried spring	See list of basic safety principles.
Speed limitation / speed reduction by resistance to defined flow	Examples are fixed orifice, fixed throttle.
Force limitation / force reduction	This may be achieved by a well-tried pressure relief valve which is, for example, equipped with a well-tried spring, correctly dimensioned and selected.
Appropriate range of working conditions	The limitation of working conditions, for example, pressure range, flow rate and temperature range should be considered.
Proper avoidance of contamination of the fluid	Consider high degree of filtration and separation of solid particles and water in the fluid.
Sufficient positive overlapping in piston valves	The positive overlapping ensures the stopping function and prevents un-allowed movements.
Limited hysteresis	For example, increased friction will increase hysteresis. Combination of tolerances will also influence the hysteresis.

L.3 List of well–tried components

At present, no list of well-tried components is given. The status of being well-tried is mainly application specific. Components may be stated as being well-tried if they conform to the description given in ISO 13849-1.
A well-tried component for some applications can be inappropriate for other applications.

L.4 Fault lists and fault exclusions

The lists express some fault exclusions and their rationale. The precise instant that the fault occurs can be critical.

L.5 Valves

L.5.1 Directional control valves

Table 24 — Directional control valves

Fault considered	Fault exclusion	Remarks
Change of switching times	Yes, in the case of positive mechanical action of the moving components as long as the actuating force is sufficiently large.	-----
Non–switching (sticking at the end or zero position) or incomplete switching (sticking at a random intermediate position)	Yes, in the case of positive mechanical action of the moving components as long as the actuating force is sufficiently large.	
Spontaneous change of the initial switching position (without an input signal)	Yes, in the case of positive mechanical action of the moving components as long as the holding force is sufficiently large, or Yes, if well–tried springs are used and if normal installation and operating conditions apply (see remark 1), or Yes, in the case of spool valves with elastic sealing and if normal installation and operating conditions apply (see remark 1).	1) Normal installation and operating conditions apply when: • the conditions specified by the supplier have been observed and; • the weight of the moving component is not acting in an unfavorable sense in terms of safety (e.g., horizontal installation) and; • no special inertial forces affect the moving components (e.g., direction of motion takes into account the orientation of the moving machine parts) and; • no extreme vibration and shock stresses occur.
Leakage	Yes, in the case of spool type valves with elastic seal in so far as a sufficient positive overlap is present (see remark 2) and if normal conditions of operation apply and adequate treatment and filtration of the compressed air is provided, or Yes, in the case of seat valves if normal conditions of operation apply (see remark 3) and adequate treatment and filtration of the compressed air is provided.	2) In the case of spool type valves with elastic seal, the effects due to leakage may usually be excluded. However, a small amount of leakage may occur over a long period of time. 3) Normal conditions of operation apply when the conditions specified by the supplier are being observed.
Change in the leakage flow rate over a long period of use	None	-----
Bursting of the valve housing or breakage of the moving component(s) as well as breakage / fracture of the mounting or housing screws	Yes, if construction, dimensioning and installation are in accordance with good engineering practice.	
For servo and proportional valves: pneumatic faults which cause uncontrolled behavior	Yes, in the case of servo and proportional directional valves if these can be assessed, in terms of technical safety, as conventional directional control valves due to their design and construction.	
Informative Note: *If the control functions are realized by a number of single function valves, then a fault analysis should be carried out for each valve. The same procedure should be carried out in the case of piloted valves.*		

L.5.2 Shutoff and check valves

Table 25 — Stop (shut-off) valves/non-return (check) valves/quick-action venting valves/shuttle valves

Fault considered	Fault exclusion	Remarks
Change of switching times	None	
Non-opening, incomplete opening, non-closure or incomplete closure (sticking at an end position or at an arbitrary intermediate position)	Non-closure or incomplete closure (sticking at an end position or at an arbitrary intermediate position). Yes, if the guidance system for the moving component(s) is designed in a manner similar to that for a non–controlled ball seat valve without a damping system (see remark 1) and if well-tried springs are used.	1) For a non–controlled ball seat valve without damping system, the guidance system is generally designed in a manner such that any sticking of the moving component is unlikely.
Spontaneous change of the initial switching position (without an input signal)	Yes, for normal installation and operating conditions (see remark 2) and if there is sufficient closing force on the basis of the pressures and areas provided.	2) Normal installation and operating conditions are being met when: • the conditions specified by the supplier are being followed; and • no special inertial forces affect the moving components, e.g., direction of motion takes into account the orientation of the moving machine parts; and • no extreme vibration or shock stresses occur.
For shuttle valves: simultaneous closing of both input connections	Yes, if, on the basis of the construction and design of the moving component, simultaneous closing is unlikely.	-----
Leakage	Yes, if normal conditions of operation apply (see remark 3) and there is adequate treatment and filtration of the compressed air.	3) Normal conditions of operation apply when the conditions specified by the supplier are being observed.
Change in the leakage flow rate over a long period of use	None	-----
Bursting of the valve housing or breakage of the moving component(s) as well as breakage/fracture of the mounting or housing screws	Yes, if construction, dimensioning and installation are in accordance with good engineering practice.	-----

L.5.3 Flow valves

Table 26 — Flow valves

Fault considered	Fault exclusion	Remarks
Change in flow rate without any change in setting device	Yes, for flow control valves without moving parts (see remark 1), e.g., throttle valves, if normal operating conditions apply (see remark 2) and adequate treatment and filtration of the compressed air is provided.	1) The setting device is not considered to be a moving part. Changes in flow rate due to changes in pressure differences are physically limited in this type of valve and are not covered by this assumed fault. 2) Normal operating conditions apply when the conditions specified by the supplier are being observed.
Change in the flow rate in the case of non–adjustable, circular orifices and nozzles	Yes, if the diameter is 0.8 mm, normal operating conditions apply (see remark 2), and if adequate treatment and filtration of the compressed air is provided.	
For proportional flow valves: change in the flow rate due to an unintended change in the set value.	None	-----
Spontaneous change in the setting device	Yes, where there is an effective protection of the setting device adapted to the particular case, based upon technical safety specification(s).	
Unintended loosening of operating element(s) of the setting device	Yes, if an effective positive locking device against loosening (unscrewing) is provided.	
Valve housing bursting; breakage or fracture of mounting/housing screw or moving component(s)	Yes, if construction, dimensioning and installation are in accordance with good engineering practice.	

L.5.4 Pressure valves

Table 27 — Pressure valves

Fault considered	Fault exclusion	Remarks
Non–opening or insufficient opening (spatially and temporarily) when exceeding the set pressure (sticking or sluggish movement of the moving component; see remark 1)	Yes, if: • the guidance system for the moving component(s) is similar to the case of a non– controlled ball seat or membrane valve (see remark 2), e.g., for a pressure reducing valve with secondary pressure relief, and • the installed springs are well-tried springs.	1) This fault applies only when the pressure valve(s) is used for forced actions, e.g., clamping. This fault does not apply to its normal function in the pneumatic systems, e.g., pressure limitation, pressure decrease. 2) For a non–controlled ball seat valve or for a membrane valve, the guidance system is generally designed in such a manner that any sticking of the moving component is unlikely.
Non–closing or insufficient closing (spatially and temporarily) if pressure drops below the set value (sticking or sluggish movement of the moving component; see remark 1)		
Change of the pressure control behavior without changing the setting device (see remark 1)	Yes, for directly actuated pressure limiting valves and pressure switching valves if the installed spring(s) are well–tried.	
For proportional pressure valves: change in the pressure control behavior due to unintended change in the set value (see remark 1)	None	
Spontaneous change in the setting device	Yes, where there is effective protection of the setting device within the requirements of the application, e.g., lead seals.	-----
Unintended unscrewing of the operating element of the setting device	Yes, if an effective positive locking device against unscrewing is provided.	
Leakage	Yes, for seat valves, membrane valves and spool valves with elastic sealing in normal operating conditions (see remark 3) and if adequate treatment and filtration of the compressed air is provided.	3) Normal operating conditions are being met when the conditions specified by the supplier are being followed.
Change of the leakage flow rate, over a long period of use	None	-----
Valve housing bursting; breakage or fracture of mounting/housing screw or moving component(s)	Yes, if construction, dimensioning and installation are in accordance with good engineering practice.	

L.5.5 Pipework

Table 28 — Pipework

Fault considered	Fault exclusion	Remarks
Bursting and leakage	Yes, if the dimensioning, choice of materials and fixing are in accordance with good engineering practice (see remark 1).	1) When using plastic pipes, it is necessary to consider the supplier's data, in particular with respect to operational environmental influences, e.g., thermal influences, chemical influences and influences due to radiation. When using steel pipes that have not been treated with a corrosion resistant medium, it is particularly important to provide sufficient drying of the compressed air.
Failure at the connector (e.g., tearing off, leakage)	Yes, if using bite type fittings or threaded pipes (i.e., steel fittings, steel pipes) and if dimensioning, choice of materials, manufacture, configuration and fixing are in accordance with good engineering practice.	-----
Clogging (blockage)	Yes, for pipework in the power circuit. Yes, for the control and measurement pipework if the nominal diameter is 2 mm.	
Kinking of the plastic pipes with a small nominal diameter	Yes, if properly protected and installed, taking into account the relevant supplier data, e.g., minimum bending radius.	

L.5.6 Hose assemblies

Table 29 — Hose assemblies

Fault considered	Fault exclusion	Remarks
Bursting, tearing off at the fitting attachment and leakage	Yes, if hose assemblies using hoses manufactured to EN 854 (ISO 4079-1) or similar hoses (see remark 1) with the corresponding hose fittings.	1) Fault exclusion is not considered when: • the intended lifetime is expired; • fatigue behavior of reinforcement can occur; • external damage is unavoidable.
Clogging (blockage)	Yes, for hose assemblies in the power circuit. Yes, for the control and measurement hose assemblies if the nominal diameter is 2mm.	-----

L.5.7 Connectors

Table 30 — Connectors

Fault considered	Fault exclusion	Remarks
Bursting, breaking of screws or stripping of threads	Yes, if dimensioning, choice of material, manufacture, configuration and connection to the piping and/or to the fluid technology components are in accordance with good engineering practice.	-----
Leakage (loss of airtightness)	None (see remark 1)	1) Due to wear, aging, deterioration of elasticity, etc., it is not possible to exclude faults over a long period. A sudden major failure of the airtightness is not assumed.
Clogging (blockage)	Yes, for applications in the power circuit. Yes, in the case of the control and measurement connectors if the nominal diameter is 2 mm.	-----

L.5.8 Pressure transmitters and pressure medium transducers

Table 31 — Pressure transmitters and pressure medium transducers

Fault considered	Fault exclusion	Remarks
Loss or change of air/oil-tightness of pressure chambers	None	-----
Bursting of the pressure chambers as well as fracture of the attachment or cover screws	Yes, if dimensioning, choice of material, configuration and attachment are in accordance with good engineering practice.	-----

L.5.9 Compressed air treatment

Table 32 — Filters

Fault considered	Fault exclusion	Remarks
Blockage of the filter element	None	-----
Rupture or partial rupture of the filter element	Yes, if the filter element is sufficiently resistant to pressure.	
Failure of the dirt indicator or dirt monitor	None	
Bursting of the filter housing or fracture of the cover or connecting elements	Yes, if dimensioning, choice of material, arrangement in the system and fixing are in accordance with good engineering practice.	

M5.10 Oilers

Table 33 — Oilers

Fault considered	Fault exclusion	Remarks
Change in the set value (oil volume per unit time) without change to the setting device	None	-----
Spontaneous change in the setting device	Yes, if effective protection of the setting device is provided and adapted to the particular case.	
Unintended unscrewing of the operating element of the setting device	Yes, if an effective positive locking device against unscrewing is provided.	
Bursting of the housing or fracture of the cover, fixing or connecting elements.	Yes, if the dimensioning, choice of materials, arrangement in the system and fixing are in accordance with good engineering practice.	

M5.11 Silencer

Table 34 — Silencer

Fault considered	Fault exclusion	Remarks
Blockage (clogging) of the silencer	Yes, if the design and construction of the silencer element fulfils remark 1.	1) Clogging of the silencer element and/or an increase in the exhaust air back pressure above a certain critical value is unlikely if the silencer has a suitably large diameter and is designed to meet the operating conditions.

L.5.12 Accumulators and pressure vessels

Table 35 — Accumulators and pressure vessels

Fault considered	Fault exclusion	Remarks
Fracture / bursting of the accumulator / pressure vessel or connectors or stripping of the threads of the fixing screws	Yes, if construction, choice of equipment, choice of materials and arrangement in the system are in accordance with good engineering practice.	-----

L.5.13 Sensors

Table 36 — Sensors

Fault considered	Fault exclusion	Remarks
Faulty sensor (see remark 1)	None	1) Sensors in this table include signal capture, processing and output in particular for pressure, flow rate, temperature, etc.
Change of the detection or output characteristics	None	-----

L.5.14 Information processing

Table 37 — Logical elements

Fault considered	Fault exclusion	Remarks
Faulty logic element (e.g., AND element, OR element, Logic–storage–element) due to, e.g., change in the switching time, failing to switch or incomplete switching	For corresponding fault assumptions and fault exclusions, see lists of well-tried safety principles.	-----

L.5.15 Time-delay devices

Table 38 — Time-delay devices

Fault considered	Fault exclusion	Remarks
Faulty time delay device, e.g., pneumatic and pneumatic / mechanical time and counting elements	Yes, for time delay devices without moving components, e.g., fixed resistance, if normal operating conditions (see remark 1) apply and adequate treatment and filtration of the compressed air is provided.	1) Normal operating conditions are being met when the conditions specified by the supplier are being followed.
Change of detection or output characteristics		
Bursting of the housing or fracture of the cover or fixing elements	Yes, if construction, dimensioning and installation are in accordance with good engineering practice.	-----

L.5.16 Converters

Table 39 — Converters

Fault considered	Fault exclusion	Remarks
Faulty converter (see remark 1)	Yes, for converters without moving components, e.g., reflex nozzle, if normal operating conditions apply (see remark 2) and adequate treatment and filtration of the compressed air is provided.	1) This covers e.g., the conversion of a pneumatic signal into an electrical one, the position detection (cylinder switch, reflex nozzle), the amplification of pneumatic signals. 2) Normal operating conditions are being met when the conditions specified by the supplier are being followed.
Change of detection or output characteristics		
Bursting of the housing or fracture of the cover or fixing elements	Yes, if construction, dimensioning and installation are in accordance with good engineering practice.	-----

Annex M – Validation Tools for Hydraulic Systems

[Annex C of ISO 13849-2:2012]

(Informative)

When hydraulic systems are used in conjunction with other technologies, then relevant tables for basic safety and well-tried safety principles should also be taken into account. Where hydraulic components are electrically connected/controlled the appropriate fault lists in Annex D should be considered.

M.1 List of basic safety principles

Air bubbles and cavitation in the hydraulic fluid should be avoided because they can create additional hazards, e.g., unintended movements.

Table 40 — Basic safety principles

Basic Safety Principles	Remarks
Use of suitable materials and adequate manufacturing	Selection of material, manufacturing methods and treatment in relation to e.g., stress, durability, elasticity, friction, wear, corrosion, temperature, hydraulic fluid.
Correct dimensioning and shaping	Consider e.g., stress, strain, fatigue, surface roughness, tolerances, manufacturing.
Proper selection, combination, arrangements, assembly and installation of components/system	Apply supplier application notes, e.g., catalog sheets, installation instructions, specifications, and use of good engineering practice in similar components/ systems.
Use of de–energization principle	The safe state is obtained by the release of energy to all relevant devices. See primary action for stopping in ANSI/ISO 12100. Energy is supplied for starting the movement of a mechanism. See the primary action for starting in ANSI/ISO 12100. Consider different modes, e.g., operation mode, maintenance mode. This principle shall not be used in some applications, e.g., where the loss of hydraulic pressure will create an additional hazard.
Proper fastening	For the application of e.g., screw locking, fittings, gluing, clamp ring, consider supplier application notes. Overloading can be avoided by applying adequate torque loading technology.
Pressure limitation	Examples are pressure relief valve, pressure reducing / control valve.
Speed limitation / speed reduction	An example is the speed limitation of a piston by a flow valve or a throttle.
Sufficient avoidance of contamination of the fluid	Consider filtration/separation of solid particles / water in the fluid. Consider also an indication of the need of filter–service.
Proper range of switching time	Consider e.g., the length of pipework, pressure, evacuation relief capacity, spring tiredness, friction, lubrication, temperature/viscosity, inertia during acceleration and deceleration, combination of tolerances.
Withstanding environmental conditions	Design the equipment so that it is capable of working in all expected environments and in any foreseeable adverse conditions, e.g., temperature, humidity, vibration, pollution. Consider supplier specifications and application notes.
Protection against unexpected start–up	Consider unexpected start–up caused by stored energy and after power supply restoration for different modes, e.g., operation mode, maintenance mode. Special equipment for the release of stored energy may be necessary. Special applications, (e.g., keeping energy for clamping devices or ensure a position) need to be considered separately.
Simplification	Reduce the number of components in the safety–related system.
Proper temperature range	To be considered throughout the whole system.
Separation	Separation of safety–related functions from other functions.

M.2 List of well–tried safety principles

Table 41 — Well–tried safety principles

Well-tried Safety Principles	Remarks
Over–dimensioning / safety factor	The safety factor is given in standards or by good experience in safety–related applications.
Safe position	The moving part of the component is held in one of the possible positions by mechanical means (friction only is not enough). Force is needed to change the position.
Increased OFF force	One solution can be that the area ratio for moving a valve spool to the safe position (OFF position) is significantly larger than for moving the spool to the ON position (a safety factor).
Valve closed by load pressure	Examples are seat and cartridge valves. Consider how to apply the load pressure in order to keep the valve closed even if, e.g., the spring closing the valve, breaks.
Positive mechanical action	The positive mechanical action is used for moving parts inside hydraulic components.
Multiple parts	See list of basic safety principles
Use of well–tried spring	See list of basic safety principles
Speed limitation/speed reduction by resistance to defined flow	Examples are fixed orifice, fixed throttle.
Force limitation/force reduction	This may be achieved by a well–tried pressure relief valve which is, e.g., equipped with a well–tried spring, correctly dimensioned and selected.
Appropriate range of working conditions	The limitation of working conditions, e.g., pressure range, flow rate and temperature range should be considered.
Monitoring of the condition of the fluid	Consider the high degree of filtration/separation of solid particles/water in the fluid. Consider also the chemical/physical conditions of the fluid. Consider an indication of the need of filter–service.
Sufficient positive overlapping in piston valves	The positive overlapping ensures the stopping function and prevents un-allowed movements.
Limited hysteresis	For example, increased friction will increase hysteresis. Combination of tolerances will also influence the hysteresis.

M.3 List of well–tried components

At this time, no list of well–tried components is given. The status of being well–tried is mainly application specific. Components may be stated as being well–tried if they conform to the description given in ISO 13849-1. A well–tried component for some applications can be inappropriate for other applications.

M.4 Fault lists and fault exclusions

The lists express some fault exclusions and their rationale. The precise instant that the fault occurs can be critical.

M.4.1 Valves

Table 42 — Directional control valves

Fault considered	Fault exclusion	Remarks
Change of switching times	Yes, in the case of positive mechanical action of the moving components as long as the actuating force is sufficiently large; or Yes, with respect to the non–opening of a special type of cartridge seat valve, when used with at least one other valve, to control the main flow of the fluid (see remark 1).	1) Special type of cartridge seat valve is achieved if: • the active area for initiating the safety–related switching movement is at least 90% of the total area of the moving component (poppet); and • the effective control pressure on the active area, can be increased up to the maximum operating pressure in line with the behavior of the seat valve in question; and • the effective control pressure on the area opposite to the active area of the moving component is vented to a very low value compared with the maximum operating pressure, e.g., return pressure in case of pressure dump valves or supply pressure in case of suction / fill valves; and • the moving component (poppet) is provided with peripheral balancing grooves; and • the pilot valve(s) to this seat valve is designed together in a manifold block (i.e., without hose assemblies and pipes for the connection of these valves).
Non–switching (sticking at an end or zero position) or incomplete switching (sticking at a random intermediate position)	Yes, in the case of positive mechanical action of the moving components as long as the actuating force is sufficiently large; or Yes, with respect to the non–opening of a special type of cartridge seat valve, when used with at least one other valve, to control the main flow of the fluid (see remark 1).	
Spontaneous change of the initial switching position (without an input signal)	Yes, in the case of positive mechanical action of the moving components as long as the holding force is sufficiently large; or Yes, if well–tried springs are used and if normal installation and operating conditions apply (see remark 2); or Yes, with respect to the non–opening of a special type of cartridge seat valve, when used with at least one other valve, to control the main flow of the fluid (see remark 1) and if normal installation and operating conditions apply (see remark 2).	2) Normal installation and operating conditions apply when: • the conditions specified by the supplier are being observed; and • the weight of the moving component is not acting in an unfavorable sense in terms of safety, e.g., horizontal installation; and • no special inertial forces affect the moving components, e.g., direction of motion takes into account the orientation of the moving machine parts; and • no extreme vibration or shock stresses occur.
Leakage	Yes, in the case of seat valves, if normal Installation and operating conditions apply (see remark 3) and an adequate filtration system is provided.	3) Normal installation and operating conditions apply when the conditions specified by the supplier are being observed.
Change in the leakage flow rate over a long period of use	None	-----
Valve housing bursting; breakage or fracture of mounting/housing screw or moving component(s)	Yes, if construction, dimensioning and installation are in accordance with good engineering practice.	
For servo and proportional valves: hydraulic faults which cause uncontrolled behavior	Yes, in the case of servo and proportional directional valves if these can be assessed, in terms of safety, as conventional directional control valves due to their design and construction.	
Informative Note: *If the control functions are realized by a number of single function valves, then a fault analysis should be carried out for each valve. The same procedure should be carried out in the case of piloted valves.*		

M.4.2 Shutoff and check valves

Table 43 — Stop (shut–off) valves/non–return (check) valves/shuttle valves, etc.

Fault considered	Fault exclusion	Remarks
Change of switching times	None	---
Non–opening, incomplete opening, non–closure or incomplete closure (sticking at an end position or at an arbitrary intermediate position)	Yes, if the guidance system for the moving component(s) is designed in a manner similar to that for a non–controlled ball seat valve without a damping system (see remark 1) and if well–tried springs are used.	1) For a non–controlled ball seat valve without damping system, the guidance system is generally designed in a manner such that any sticking of the moving component is unlikely.
Spontaneous change of the initial switching position (without an input signal)	Yes, for normal installation and operating conditions (see remark 2) and if there is sufficient closing force on the basis of the pressures and areas provided.	2) Normal installation and operating conditions are being met when: • the conditions specified by the supplier are being followed; and • no special inertial forces affect the moving components, e.g., direction of motion takes into account the orientation of the moving machine parts; and • no extreme vibration or shock stresses occur.
For shuttle valves: simultaneous closing of both input connections	Yes, if on the basis of the construction and design of the moving component this simultaneous closing is unlikely.	-----
Leakage	Yes, if normal conditions of operation apply (see remark 3) and an adequate filtration system is provided.	3) Normal conditions of operation apply when the conditions specified by the supplier are being observed.
Change in the leakage flow rate over a long period of use	None	-----
Bursting of the valve housing or breakage of the moving component(s) as well as breakage/fracture of the mounting or housing screws	Yes, if construction, dimensioning and installation are in accordance with good engineering practice.	

M.4.3 Flow valves

Table 44 — Flow valves

Fault considered	Fault exclusion	Remarks
Change in the flow rate without change in the setting device	Yes, in the case of flow valves without moving parts (see remark 1), e.g., throttle valves, if normal operating conditions apply (see remark 2) and an adequate filtration system is provided (see remark 3).	1) The setting device is not considered to be a moving part. Changes in flow rate due to changes in the pressure differences and viscosity are physically limited in this type of valve and are not covered by this assumed fault. 2) Normal operating conditions are being met when the conditions specified by the supplier are being followed. 3) Where a non–return valve is integrated into the flow valve, then in addition, the fault assumptions for non-return valves have to be observed.
Change in the flow rate in the case of non–adjustable, circular orifices and nozzles	Yes, if the diameter is > 0,8 mm, normal operating conditions apply (see remark 2) and if an adequate filtration system is provided.	
For proportional flow valves: Change in the flow rate due to an unintended change in the set value	None	
Spontaneous change in the setting device	Yes, where there is an effective protection of the setting device adapted to the particular case, based upon technical safety specification(s).	
Unintended loosening of the operating element(s) of the setting device	Yes, if an effective positive locking device against loosening (unscrewing) is provided.	
Valve housing bursting; breakage or fracture of mounting/housing screw or moving component(s)	Yes, if construction, dimensioning and installation are in accordance with good engineering practice.	

M.4.4 Pressure valves

Table 45 — Pressure valves

Fault considered	Fault exclusion	Remarks
Non–opening or insufficient opening (spatially and temporarily) when exceeding the set pressure (sticking or sluggish movement of the moving component; see remark 1)	Yes, with respect to the non–opening of a special type of cartridge seat valve, when used with at least one other valve, to control the main flow of the fluid (see remark 1), or Yes, if the guidance system for the moving component(s) is similar to the case of a non–controlled ball seat valve without a damping device (see remark 2) and if the installed springs are well–tried.	1) This fault applies only when the pressure valve(s) is used, for forced actions, e.g., clamping, and for the control of hazardous movement, e.g., suspension of loads. This fault does not apply to its normal function in hydraulic systems, e.g., pressure limitation, pressure decrease. 2) For a non–controlled ball seat valve without a damping device the guidance system is generally designed in such a manner that any sticking of the moving component is unlikely.
Non–closing or insufficient closing (spatially and temporarily) if the pressure drops below the set value (sticking or sluggish movement of the moving component; see remark 1)		
Change of the pressure control behavior without changing the setting device (see remark 1)	Yes, in the case of directly actuated pressure relief valves, if the installed spring(s) are well–tried.	
For proportional pressure valves: change in the pressure control behavior due to unintended change in the set value (see remark 1)	None	
Spontaneous change in the setting device	Yes, where there is an effective protection of the setting device adapted to the particular case in relation to technical safety specifications (e.g., lead seals).	-----
Unintended unscrewing of the operating element of the setting device	Yes, if an effective positive locking device against unscrewing is provided.	
Leakage	Yes, for seat valves if normal operating conditions apply (see remark 3) and if an adequate filtration system is provided.	3) Normal operating conditions apply when the conditions specified by the supplier are being observed.
Change of the leakage flow rate over a long period of use	None	-----
Bursting of the valve housing or breakage of the moving component(s) as well as breakage/ fracture of the mounting or housing screws	Yes, if construction, dimensioning and installation are in accordance with good engineering practice.	

M.4.5 Metal pipework, hose assemblies and connectors

Table 46 — Metal pipework

Fault considered	Fault exclusion	Remarks
Bursting and leakage	Yes, if the dimensioning, choice of materials and fixing are in accordance with good engineering practice.	-----
Failure at the connector (e.g., tearing off, leakage)	Yes, if using welded fittings or welded flanges or flared fittings and if dimensioning, choice of materials, manufacture, configuration and fixing are in accordance with good engineering practice.	
Clogging (blockage)	Yes, for pipework in the power circuit. Yes, for the control and measurement pipework if the nominal diameter is 3 mm.	

M.4.6 Hose assemblies

Table 47 — Hose assemblies

Fault considered	Fault exclusion	Remarks
Bursting, tearing off at the fitting attachment and leakage	None	-----
Clogging (blockage)	Yes, for hose assemblies in the power circuit. Yes, for the control and measurement hose assemblies if the nominal diameter is 3 mm.	

M.4.7 Connectors

Table 48 — Connectors

Fault considered	Fault exclusion	Remarks
Bursting, breaking of screws or stripping of threads	Yes, if dimensioning, choice of material, manufacture, configuration and connection to the piping and/or to the fluid technology component are in accordance with good engineering practice.	-----
Leakage (loss of the leak–tightness)	None (see remark 1)	1) Due to wear, aging, deterioration of elasticity, etc., it is not possible to exclude faults over a long period. A sudden major failure of the leak-tightness is not assumed.
Clogging (blockage)	Yes, for applications in the power circuit. Yes, in the case of the control and measurement connectors if the nominal diameter is 3 mm.	-----

M.4.8 Filters

Table 49 — Filters

Fault considered	Fault exclusion	Remarks
Blockage of the filter element	None	-----
Rupture of the filter element	Yes, if the filter element is sufficiently resistant to pressure and an effective bypass valve or effective monitoring of dirt is provided.	
Failure of the bypass valve	Yes, if the guidance system of the bypass valve is designed in a manner similar to that for a non–controlled ball seat valve without a damping device and if well–tried springs are used.	
Failure of the dirt indicator or dirt monitor	None	
Bursting of the filter housing or fracture of the cover or connecting elements	Yes, if dimensioning, choice of material, arrangement in the system and fixing are in accordance with good engineering practice.	

M.4.9 Energy storage

Table 50 — Energy storage

Fault considered	Fault exclusion	Remarks
Fracture/bursting of the energy storage vessel or connectors or cover screws as well as stripping of the screw threads	Yes, if construction, choice of equipment, choice of materials and arrangement in the system are in accordance with good engineering practice.	-----
Leakage at the separating element between the gas and the operating fluid	None	-----
Failure/breakage of the separating element between the gas and the operating fluid	Yes, in the case of cylinder/piston storage (see remark 1).	1) A sudden major leakage is not to be considered.
Failure of the filling valve on the gas side	Yes, if the filling valve is installed in accordance with good engineering practice and if adequate protection against external influences is provided.	-----

M.4.10 Sensors

Table 51 — Sensors

Fault considered	Fault exclusion	Remarks
Faulty sensor (see remark 1)	None	1) Sensors in this Table include signal capture, processing and output, in particular for pressure, flow rate, temperature, etc.
Change of the detection or output characteristics	None	-----

Annex N – Validation Tools for Electrical Systems

[Annex D of ISO 13849-2:2012]

(Informative)

When electrical systems are used in conjunction with other technologies, then relevant tables for basic safety and well–tried safety principles should also be taken into account.

Informative Note 1: *Electronic components may not be considered as well-tried.*

Informative Note 2: *The environmental conditions of IEC 60204-1 do not apply to the validation process if other environmental conditions are specified.*

N.1 List of basic safety principles

Table 52 — Basic safety principles

Basic Safety Principles	Remarks
Use of suitable materials and adequate manufacturing	Selection of material, manufacturing methods and treatment in relation to factors such as stress, durability, elasticity, friction, wear, corrosion, temperature, conductivity, dielectric rigidity.
Correct dimensioning and shaping	Consider factors such as stress, strain, fatigue, surface roughness, tolerances, manufacturing.
Proper selection, combination, arrangements, assembly and installation of components/system	Apply supplier application notes, for example, catalogue sheets, installation instructions, specifications, and use of good engineering practice.
Correct protective bonding	One side of the control circuit, one terminal of the operating coil of each electromagnetic operated device or one terminal of some other electrical device is connected to the protective bonding circuit (for full text, see IEC 60204-1).
Insulation monitoring	Use of an isolation monitoring device which either indicates an earth fault or interrupts the circuit automatically after an earth fault (see IEC 60204-1).
Use of de–energization principle	A safe state is obtained by de–energizing all relevant devices by, for example, use of normally closed (NC) contact for inputs (pushbuttons and position switches) and normally open (NO) contact for relays (see also, ANSI/ISO 12100). Exceptions may exist in some applications where, as an example, the loss of the electrical supply will create an additional hazard. Time delay functions may be necessary to achieve a system safe state (see IEC 60204-1).
Transient suppression	Use of a suppression device (RC, diode, varistor) parallel to the load, but not parallel to the contacts. ***Informative Note:*** *A diode increases the switch off time, more than the other energy absorption surge suppression devices listed.*
Reduction of response time	Minimize delay in de–energizing of switching components.
Compatibility	Use components compatible with the voltages and currents used.
Withstanding environmental conditions	Design the equipment so that it is capable of working in all expected environments and in any foreseeable adverse conditions, e.g., temperature, humidity, vibration and electromagnetic interference (EMI).
Secure fixing of input devices	Secure input devices, for example, interlocking switches, position switches, limit switches, proximity switches, so that position, alignment and switching tolerance is maintained under all expected conditions, e.g., vibration, normal wear, ingress of foreign bodies, temperature. See ISO 14119.
Protection against unexpected start–up	Prevent unexpected start–up, for example, after power supply restoration (see ANSI/ISO 12100, ISO 14118 and IEC 60204-1.
Protection of the control circuit	The control circuit should be protected in accordance with IEC 60204.
Sequential switching for circuit of serial contacts of redundant signals	To avoid the common mode failure of the welding of both contacts, the switching on and off does not happen simultaneously, so that one contact always switches without current.

N.2 List of well–tried safety principles

Table 53 — Well–tried safety principles

Well-tried Safety Principles	Remarks
Positive mechanically linked contacts	Use of positively mechanically linked contacts, for example, monitoring function (see ANSI/ISO 12100).
Fault avoidance in cables	To avoid short circuit between two adjacent conductors: • use cable with shield connected to the protective bonding circuit on each separate conductor; or • in flat cables, use of one earthed conductor between each signal conductors.
Separation distance	Use of sufficient distance between position terminals, components and wiring to avoid unintended connections.
Energy limitation	Use of a capacitor for supplying a finite amount of energy, for example, in a timer application.
Limitation of electrical parameters	Limitation in voltage, current, energy or frequency resulting, for example, in torque limitation, hold–to–run with displacement/time limited, reduced speed, to avoid leading to an unsafe state.
No undefined states	Avoid undefined states in the control system. Design and construct the control system so that during normal operation and all expected operating conditions its state, for example, its output(s) can be predicted.
Positive mode actuation	Direct action is transmitted by the shape (and not by the strength) with no elastic elements, for example, spring between actuator and the contacts (see ISO 14119).
Failure mode orientation	Wherever possible, the device/circuit should fail to the safe state or condition.
Oriented failure mode	Oriented failure mode components or systems should be used wherever practicable (see EN 292–2: [ISO/TR 12100-2]):
Over–dimensioning	De-rate components when used in safety circuits, for example, by: • current passed through switched contacts should be less than half their rated current; • the switching frequency of components should be less than half their rated value; and • total number of expected switching operations shall be ten times less than the device's electrical durability. ***Informative Note:*** *De-rating can depend on the design rationale.*
Minimize possibility of faults	Separate safety–related functions from the other functions.
Balance complexity/simplicity	Balance should be made between combining functions for efficiency and simplifying to have better reliability.

N.3 List of well–tried components

The components listed in ISO 13849-2:2012, Table D.3 are considered to be well–tried if they conform to the description given in ISO 13849-1:2023, 6.1.11. The standards listed in Table 54 can demonstrate their suitability and reliability for a particular application. A well–tried component for some applications can be inappropriate for other applications.

Table 54 — Well–tried components

Well-tried component	Additional conditions for "well-tried"	Standard or specification
Switch with positive mode actuation (direct opening action), e.g.: • push-button; • position switch; • cam-operated selector switch for mode of operation.	—	IEC 60947-5-1:2003, Annex K
Emergency stop device	—	ISO 13850 and IEC 60947-5-5
Fuse	—	IEC 60269-1
Circuit-breaker	—	IEC 60947-2
Switches, disconnectors	—	IEC 60947-3
Differential circuit-breaker/RCD (residual current device)	—	IEC 60947-2:2006, Annex B
Well–tried component	Additional conditions for well–tried	Standard or specification
Main contactor	Only well-tried if: • other influences are taken into account, e.g., vibration; • failure is avoided by appropriate methods, e.g., over-dimensioning (see Table D.2); • the current to the load is limited by the thermal protection device; and • the circuits are protected by a protection device against overload. ***Informative Note:*** *Fault exclusion is not possible.*	IEC 60947-4-1
Control and protective switching device or equipment (CPS)	—	IEC 60947-6-2
Auxiliary contactor (e.g., contactor relay)	Only well-tried if: • other influences are taken into account, e.g. vibration; • there is positively energized action; • failure is avoided by appropriate methods, e.g., over-dimensioning (see Table D.2); • the current in the contacts is limited by a fuse or circuit-breaker to avoid the welding of the contacts; and • contacts are positively mechanically guided when used for monitoring. ***Informative Note:*** *Fault exclusion is not possible.*	EN 50205 IEC 60947-5-1 IEC 60947-4-1:2001, Annex F
Relay	Only well-tried if: • other influences are taken into account, e.g., vibration; • positively energized action; • failure avoided by appropriate methods; e.g., over-dimensioning (see Table D.2); and • the current in the contacts is limited by fuse or circuit-breaker to avoid the welding of the contacts. ***Informative Note:*** *Fault exclusion is not possible.*	IEC 61810-1 IEC 61810-2
Transformer	—	IEC 61558
Cable	Cabling external to enclosure should be protected against mechanical damage (including, e.g., vibration or bending).	IEC 60204-1:2005, Clause 12
Plug and socket	—	According to an electrical standard relevant for the intended application. For interlocking, see also ISO 14119.
Temperature switch	—	For the electrical side, see EN 60730-1

N.4 Fault lists and fault exclusions

N.4.1 Introduction

The lists express some fault exclusions and their rationale. For validation, both permanent faults and transient disturbances should be considered. The precise instant that the fault occurs can be critical.

N.4.2 Conductors and connectors

Table 55 — Conductors/cables

Fault considered	Fault exclusion	Remarks
Short–circuit between any two conductors	Short circuits between conductors which are: • permanently connected (fixed) and protected against external damage, e.g., by cable ducting, armoring; *or* • separate multicore cables; *or* • within an electrical enclosure (see remark 1); *or* • individually shielded with earth connection.	1) Provided both the conductors and enclosure meet the appropriate requirements (see IEC 60204-1).
Short circuit of any conductor to an exposed conductive part or to earth or to the protective bonding conductor	Short circuits between conductor and any exposed conductive part within an electrical enclosure (see remark 1).	
Open circuit of any conductor	None	-----
Short circuit between two adjacent tracks/pads	Short circuits between adjacent conductors in accordance with remarks 1 to 3.	1) The base material used is according to IEC 60249 and the creepage distances and clearances are dimensioned at least to IEC 60664–1, with at least a pollution degree 2/installation category III. 2) The printed side(s) of the assembled board is covered with an aging–resistant varnish or a protective layer covering all conductor paths in accordance with IEC 60664–3. 3) All enclosures of the SRP/CS, including those mounted remotely, should provide a degree of protection of at least IP 54 (see IEC 60529), when mounted as specified.
Open–circuit of any track	None	-----

N.4.3 Printed circuit boards/assemblies

Table 56 — Printed circuit boards/assemblies

Fault considered	Fault exclusion	Remarks
Short circuit between two adjacent tracks / pads	Short circuits between adjacent conductors in accordance with remarks 1 to 3.	1) The base material used is according to IEC 60249 and the creepage distances and clearances are dimensioned at least to IEC 60664–1, with at least a pollution degree installation category III. 2) The printed side(s) of the assembled board is covered with an aging–resistant varnish or a protective layer covering all conductor paths in accordance with IEC 60664–3. 3) All enclosures of the safety–related parts of the control system, including those mounted remotely, should provide a degree of protection of at least IP 54 (see IEC 60529), when mounted as specified.
Open–circuit of any track	None	-----

N.4.4 Terminal block

Table 57 — Terminal block

Fault considered	Fault exclusion	Remarks
Short circuit between adjacent terminals	Short circuit between adjacent terminals in accordance with remarks 1) or 2).	1) The terminals used and the requirements of IEC 60204-1are satisfied. 2) The design by itself ensures that short circuit is avoided, e.g., by shaping shrink down plastic tubing over connection point.
Open–circuit of individual terminals	None	-----

N.4.5 Multi–pin connector

Table 58 — Multi–pin connector

Fault considered	Fault exclusion	Remarks
Short circuit between any two adjacent pins	Short circuit between adjacent pins in accordance with remarks 1 and 2.	1) By using ferrules or other suitable means for multi–stranded wires. Creepage distances and clearances and all gaps should be dimensioned to at least IEC 60664 with installation category III. 2) The assembled board should be mounted in an enclosure of at least IP 54 (see IEC 60529) and the printed side(s) of the assembled board is covered with an aging–resistant varnish or a protective layer covering all conductor paths in accordance with IEC 60664–3.
Interchanged or incorrectly inserted connector when not prevented by mechanical means	None	-----
Short circuit of any conductor (see remark 3) to earth or a conductive part or to the protective conductor	None	3) The core of the cable is considered as a part of the multi–pin connector.
Open circuit of individual connector pins	None	-----

N.4.6 Switches

Table 59 — Electromechanical position switch, manually operated switch

(e.g., pushbutton, reset actuator, DIP switch, magnetically operated contacts, reed switch, pressure switch, temperature switch)

Fault considered	Fault exclusion	Remarks
Contact will not close	None	-----
Contact will not open	Contacts in accordance with IEC 60947-5-1 are expected to open.	-----
Short circuit between adjacent contacts insulated from each other	Short circuit may be excluded for switches in accordance with IEC 60947-5-1 (see remark 1).	1) Conductive parts which become loose should not be able to bridge the insulation between contacts.
Simultaneous short circuit between three terminals of changeover contacts	Simultaneous short circuits may be excluded for switches in accordance with IEC 60947-5-1 (see remark 1).	
Informative Note: *The fault lists for the mechanical aspects are considered in Annex A.*		

N.4.7 Electromechanical devices

Table 60 — Electromechanical devices

(e.g., relay, contactor relays)

Fault considered	Fault exclusion	Remarks
All contacts remain in the energized position when the coil is de–energized (e.g., due to mechanical fault)	None	-----
All contacts remain in the de–energized position when power is applied (e.g., due to mechanical fault, open circuit of coil)	None	
Contact will not open	None	
Contact will not close	None	
Simultaneous short circuit between the three terminals of a changeover contact	Simultaneous short circuit may be excluded if remarks 1 and 2 are fulfilled.	1) The creepage and clearance distances are dimensioned to at least IEC 60664–1, with at least pollution degree 2/installation category III. 2) Conductive parts which become loose cannot bridge the insulation between contacts and the coil.
Short circuit between two pairs of contacts and/or between contacts and coil terminal	Short circuit may be excluded if remarks 1 and 2 are fulfilled.	
Simultaneous closing of normally open and normally closed contacts	Simultaneous closing of contacts may be excluded if remark 3 is fulfilled.	3) Positively driven (or mechanically linked) contacts are used.

N.4.8 Proximity switches

Table 61 — Proximity switches

Fault considered	Fault exclusion	Remarks
Permanently low resistance at output	None (see remark 1).	1) See IEC 60947-5-3.
Permanently high resistance at output	None (see remark 2).	2) Fault prevention measures should be described.
Interruption in power supply	None	-----
No operation of switch due to mechanical failure	No operation due to mechanical failure when remark 3 is fulfilled.	3) All parts of the switch should be sufficiently well fixed.
Short–circuit between the three connections of a change–over switch	None	-----

N.4.9 Solenoid valves

Table 62 — Solenoid valves

Fault considered	Fault exclusion	Remarks
Does not energize	None	-----
Does not de–energize	None	
***Informative Note**: Fault lists for mechanical aspects of pneumatic and hydraulic valves are considered in Annexes B and C respectively.*		

N.4.10 Transformers

Table 63 — Transformers

Fault considered	Fault exclusion	Remarks
Open circuit of individual winding	None	-----
Short circuit between different windings	Short circuit between different windings may be excluded if remark 1 is fulfilled.	1) The requirements of IEC 60742 should be met. Additionally, for rated voltages below 500 V, the insulation should meet the requirements for a 2 500 V AC test voltage. Short circuits in coils and windings need to be avoided by taking appropriate steps, e.g., by: • impregnating the coils so as to fill all the cavities between individual coils and the body of the coil and the core; and • using winding conductors well within their insulation and high temperature ratings. 2) In the event of a secondary short circuit, heating above a specified operating temperature should not occur.
Short circuit in one winding	Short circuit in one winding may be excluded if remark 1 is fulfilled.	
Change in effective turns ratio	Change in effective turns ratio may be excluded if remark 1 is fulfilled. See also the guidance in remark 2.	

N.4.11 Inductances

Table 64 — Inductances

Fault considered	Fault exclusion	Remarks
Open circuit	None	-----
Short circuit	Short circuit may be excluded if remark 1 is fulfilled.	1) Coil is single layered, enameled or potted and with axial wire connections and axial mounted.
Random change of value 0.5 LN < L < LN + tolerance, where LN is the nominal value of inductance (see remark 2).	None	2) Depending upon the type of construction other ranges can be considered.

N.4.12 Resisters

Table 65 — Resistors

Fault considered	Fault exclusion	Remarks
Open circuit	None	-----
Short circuit	Short circuit may be excluded if remark 1 is fulfilled. No exclusions for resistors used in surface–mounting technology.	1) The resistor is of the film type, or wire-wound type with protection to prevent unwinding of wire in the event of breakage, with axial wire connections, axial mounted and varnished.
Random change of value 0.5 RN < R < 2 RN, where RN is the nominal value of resistance (see remark 2).	None	2) Depending upon the type of construction other ranges may be considered.

N.4.13 Resister networks

Table 66 — Resistor networks

Fault considered	Fault exclusion	Remarks
Open circuit	None	-----
Short circuit between any two connections	None	-----
Short circuit between any connections	None	-----
Random change of value 0.5 RN < R < 2 RN, where RN is the nominal value of resistance (see remark 1)	None	1) Depending upon the type of construction, other ranges may be considered.

N.4.14 Potentiometers

Table 67 — Potentiometers

Fault considered	Fault exclusion	Remarks
Open circuit of individual connection	None	-----
Short circuit between all connections	None	
Short circuit between any two connections	None	
Random change of value 0.5 Rp < R < 2 Rp, where Rp = nominal value of resistance (see remark 1).	None	1) Depending upon the type of construction, other ranges may be considered.

N.4.15 Capacitors

Table 68 — Capacitors

Fault considered	Fault exclusion	Remarks
Open circuit	None	-----
Short circuit	None	
Random change of value 0.5 CN < C < CN + tolerance, where CN = nominal value of capacity (see remark 1)	None	1) Depending upon the type of construction, other ranges may be considered.
Changing value for loss tangent (tan δ)	None	-----

N.4.16 Discrete semiconductors

Table 69 — Discrete semiconductors

(e.g., diodes, Zener diodes, transistors, triacs, voltage regulators, quartz crystals, phototransistors, light–emitting diodes [LEDs])

Fault considered	Fault exclusion	Remarks
Open circuit of any connection	None	-----
Short circuit between any two connections	None	
Short circuit between all connections	None	
Change in characteristics	None	

N.4.17 Optocouplers

Table 70 — Optocouplers

Fault considered	Fault exclusion	Remarks
Open circuit of individual connection	None	-----
Short circuit between any two input connections	None	
Short circuit between any two output connections	None	
Short circuit between any two connections of input and output	Short circuit between input and output may be excluded if remark 1 is fulfilled.	1) The base material used should be according to IEC 60249 and the creepage distances and clearances should be dimensioned at least to IEC 60664–1, with at least pollution degree installation category III.

N.4.18 Non–programmable integrated circuits

Table 71 — Non–programmable integrated circuits

Fault considered	Fault exclusion	Remarks
Open circuit of each individual connection	None	-----
Short circuit between any two connections	None	
Stuck–at–fault (i.e., short–circuit to 1 and 0 with isolated input or disconnected output)	None	
Static "0" and "1" signal at all inputs and outputs, either individually or simultaneously	None	
Parasitic oscillation of outputs	None	
Changing values (e.g., input/ output voltage of analog devices)	None	

Informative Note: *In this standard, ICs with less than 1,000 gates and/or less than 24 pins, operational amplifiers, shift registers and hybrid modules are considered to be non-complex. This definition is somewhat arbitrary.*

N.4.19 Programmable and/or complex integrated circuits

Table 72 — Programmable and/or complex integrated circuits

Fault considered	Fault exclusion	Remarks
Faults in all or part of the function including software faults	None	-----
Open circuit of each individual connection	None	
Short circuit between any two connections	None	
Stuck–at–fault (i.e., short–circuit to 1 and 0 with isolated input or disconnected output)	None	
Static "0" and "1" signal at all inputs and outputs, either individually or simultaneously	None	
Parasitic oscillation of outputs	None	
Changing values (e.g., input/output voltage of analog devices)	None	
Undetected faults in the hardware which go unnoticed because of the complexity of the integrated circuit	None	

Informative Note: *In this standard, an IC is considered to be complex if it consists of more than 1,000 gates and/or more than 24 pins. This definition is somewhat arbitrary. The analysis should identify additional faults which should be considered if they influence the operation of the safety function.*

Annex O – Consideration for Fluid Power DC (Diagnostic Coverage)
(Informative)

This Annex explains DC on fluid power circuits with pneumatic example circuits.

3-position valve – Indirect monitoring:

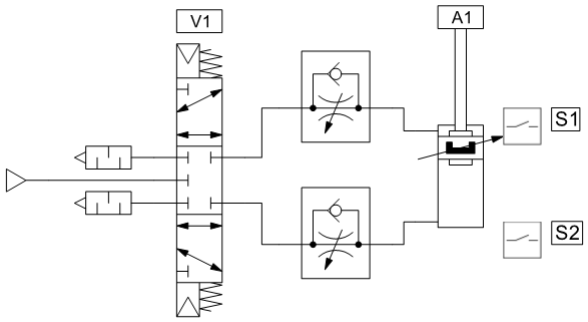


Figure O.1 – 3-position center blocked valve

Where:

V1: the 3-position center blocked valve is controlled by the safety controller.
V1e: V1 valve extend output.
V1r: V1 valve retract output.
S1: a cylinder extended position switch wired to logic.
S2: a cylinder retracted position switch wired to logic.

DC software description:

Software parameter:

- T1e: expected time for cylinder A1 to start extending.
- T2e: expected time for cylinder A1 to extend.
- T3e: expected time for cylinder A1 to start retracting.
- T4e: expected time for cylinder A1 to retract.
- T5e: expected time for cylinder A1 to stop while extending.
- T6e: expected time for cylinder A1 to stop while retracting.
- T7e: expected time for cylinder A1 to hold at stopped mid position.
- T8e: expected time for cylinder A1 to hold at extended position.
- T9e: expected time for cylinder A1 to hold at retracted position.
- The expected time (T1e through T9e) can be slightly greater than the measured average time.

Testing and measurements:

1) **T1m**: While cylinder A1 is retracted and S2 is on. Logic to measure the time from V1e turning on to S2 turning off.

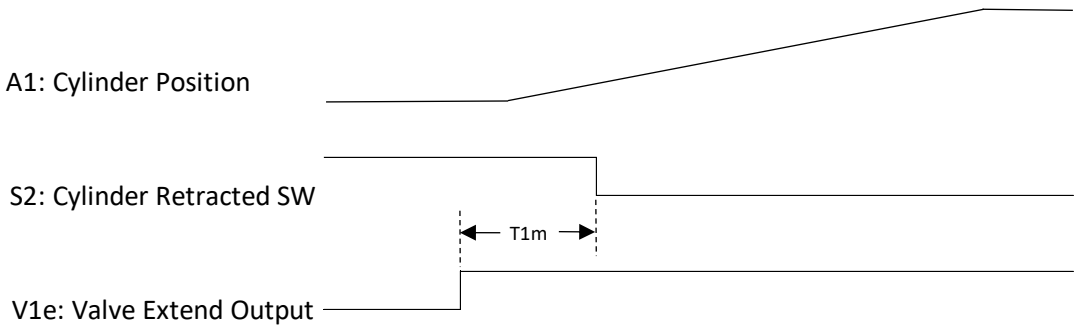


Figure O.2 – Timing diagram for T1m

2) **T2m**: Logic to measure the time from V1e turning on to S1 turning on.

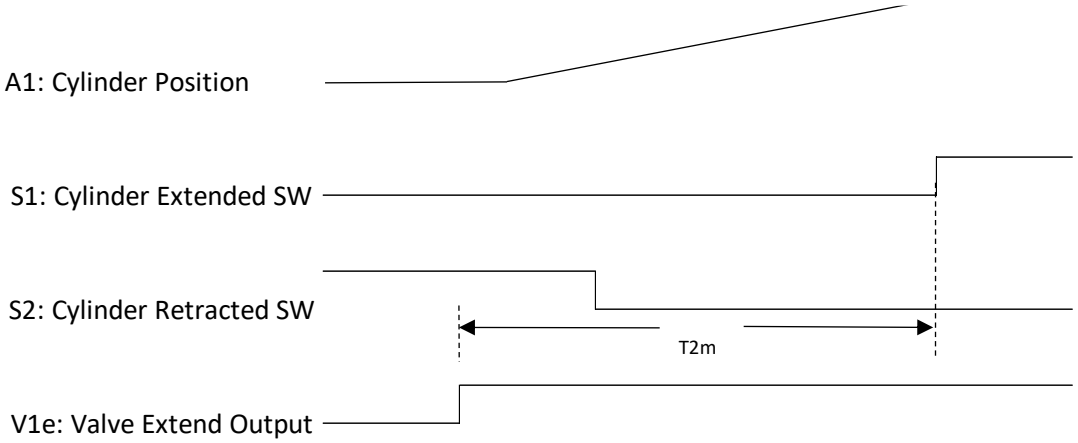


Figure O.3 – Timing diagram for T2m

3) **T3m**: While cylinder A1 is extended and S1 is on, logic measures the time from V1r turning on to S1 turning off.

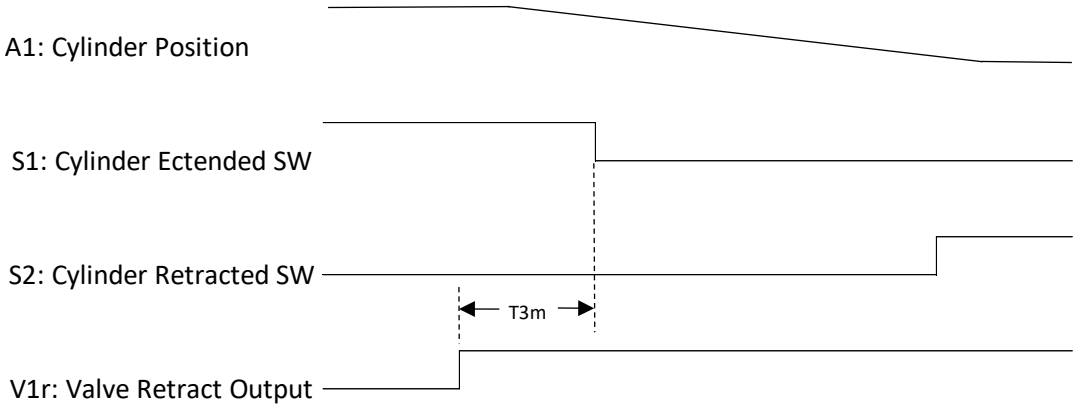


Figure O.4 – Timing diagram for T3m

4) **T4m**: Logic to measure the time from V1r turning on to S2 turning on.

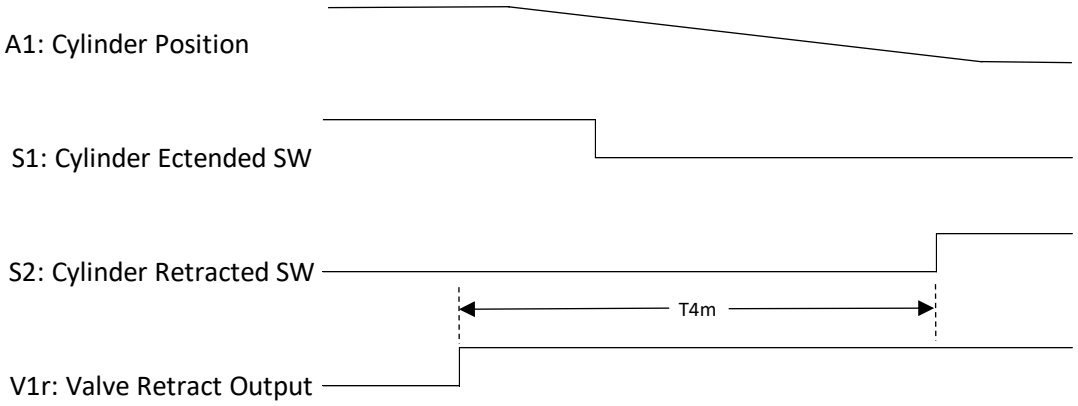


Figure O.5 – Timing diagram for T4m

5) Stop while cylinder A1 is moving: This has to be tested mid-stroke and is difficult to measure without a linear displacement transducer on cylinder A1. This test can also be performed by a person with manual control.
   a) **T5m**: While V1e is on and cylinder A1 is extending and mid-stroke, turn off V1e and logic to measure the time to stop.

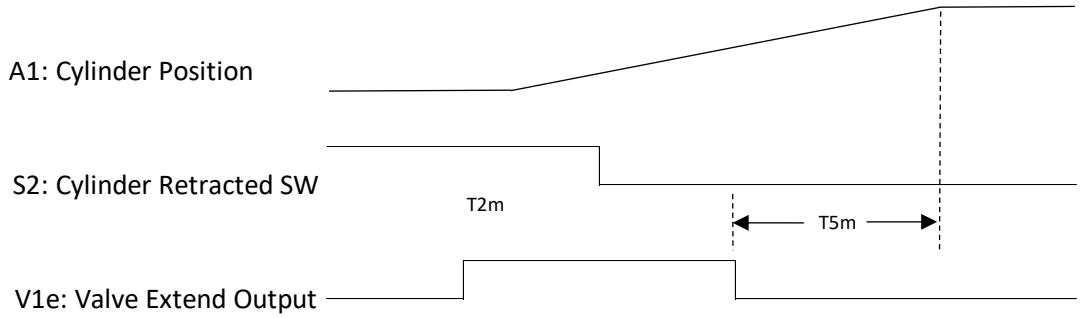


Figure O.6 – Timing diagram for T5m

   b) **T6m**: While V1r is on and cylinder A1 is retracting and mid-stroke, turn off V1r and logic to measure the time to stop.

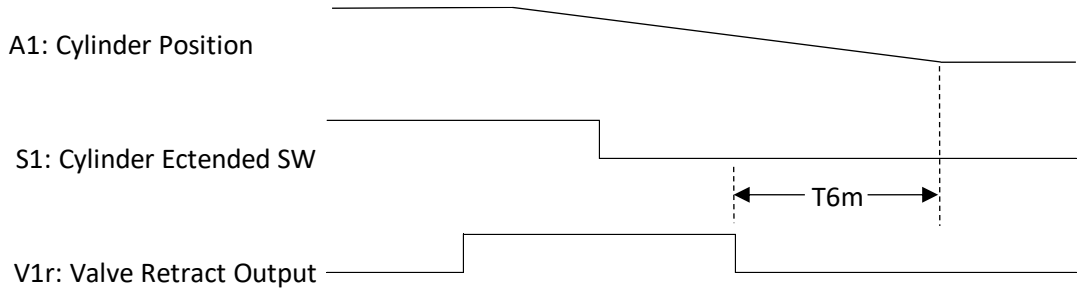


Figure O.7 – Timing diagram for T6m

   c) **T7m**: While cylinder A1 is stopped at the mid-stroke, measure the time the cylinder drifts a predetermined distance or the amount of drift in a given time.

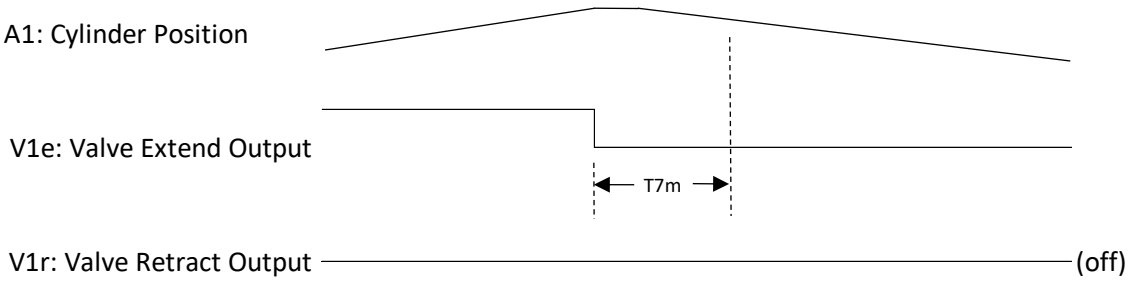


Figure O.8 – Timing diagram for T7m

6) **T8m**: While V1e is on and cylinder A1 is extended and S1 is on, turn off V1e and logic to measure the time to S1 to turn off (cylinder to drift).

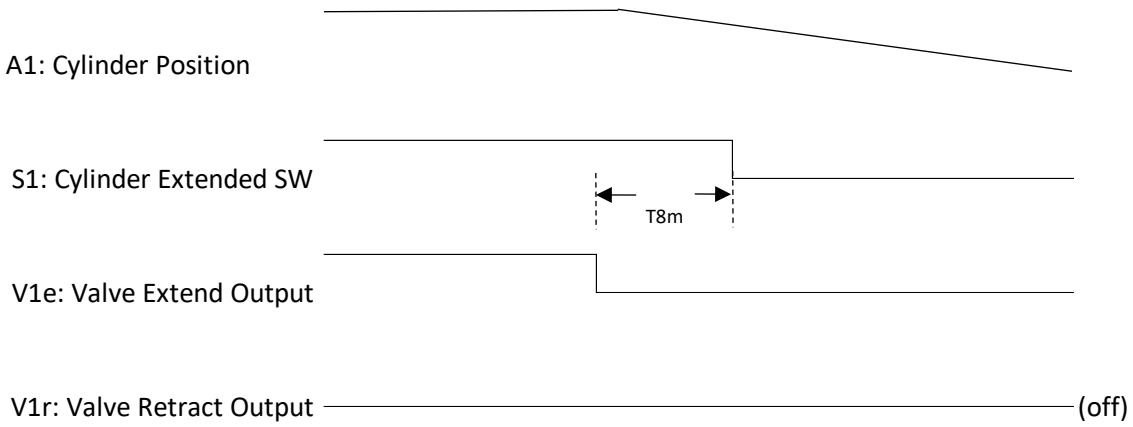


Figure O.9 – Timing diagram for T8m

7) **T9m**: While V1r is on and cylinder A1 is retracted and S2 is on, turn off V1r and logic to measure the time to S2 to turn off (cylinder to drift).

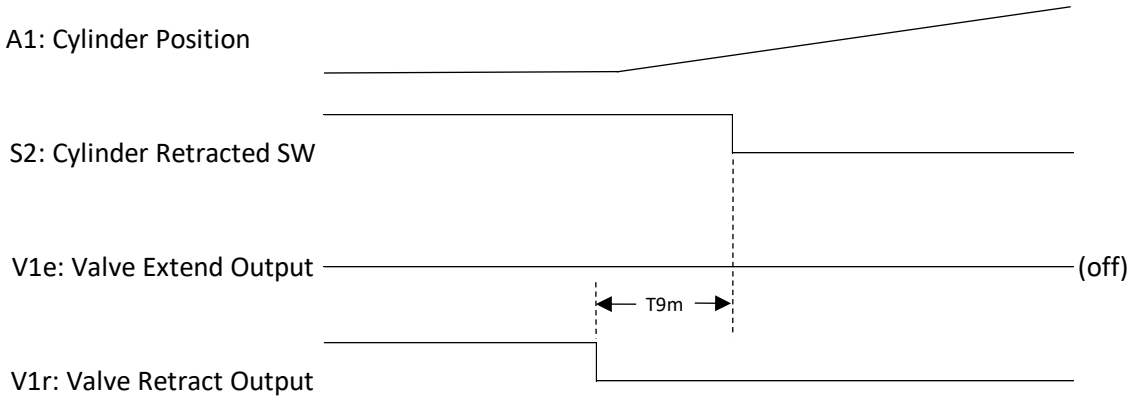


Figure O.10 – Timing diagram for T9m

Fault condition:

- T1m > T1e, T2m > T2e, T3m > T3e, etc.,

Remark:

- If flow control is used, the expected time (T1e, T2e, T3e, etc.) shall be adjusted after the flow adjustment. Tamper-proof flow control, fixed orifice, or proportional valve shall be considered.

Table 73 – FMEA example for 5/3 valve with position sensors

Valve Failure	Safe	Dangerous Detected	Dangerous Undetected
Solenoid burns out	T1m, T2m, T3m, T4m		
Solenoid spring breaks		T5m, T6m, T7m	
Exhaust seat failure	X		
Seal failure		T8m, T9m, T5m, T6m, T7m	
Return spring failure		T5m, T6m, T7m	
Valve sticks shifted		T1m, T2m, T3m, T4m, T5m, T6,m, T7m	
Valve sticks in mid-position		T1m, T2m, T3m, T4m	
Valve sticks unshifted	T1m, T2m, T3m, T4m		

When all tests are performed for each failure, the maximum DC can be achieved.

2-position exhaust valve and POC (pilot operated check) valve - Indirect monitoring:

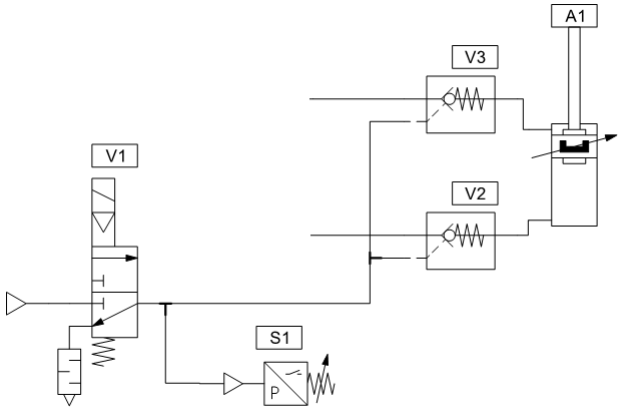


Figure O.11 – 2-position exhaust valve and POC (pilot operated check) valve

Where:

V1:	2-position exhaust valve is controlled by the safety controller.
S1:	The pressure sensor is connected to the Logic
V2, V3:	POC valves
DC_1	DC for V1
DC_2	DC for V2 and V3

DC software description:
Software parameter:

- T1e: Expected time for V1 to complete the exhaust of the air

Testing and measurements:

- T1m: While V1 is energized and S1 is off, de-energize V1 and measure time to S1 to turn on. DC_1 can be up to 90%
- T2m: While V1 is de-energized, the Logic tries to extend/retract the cylinder A1 (make sure the cylinder does not move). DC_2 can be up to 90%

Fault condition:

- T1m > T1e
- T2m cylinder can be moved while V1 is de-energized

Table 74 – FMEA example for 3/2 NC valve with a series pressure sensor

Valve Failure	Safe	Dangerous Detected	Dangerous Undetected
Solenoid burns out	X		
Solenoid spring breaks		T1m	
Exhaust seal failure	X		
Exhaust seat failure	X		
Inlet seal failure		T1m	
Inlet seat failure		T1m	
Return spring failure		T1m	
Valve sticks shifted			X
Valve sticks in mid-position			X
Valve sticks unshifted	X		

Table 75 – FMEA example for pilot operated check valves tested through testing

Valve Failure	Safe	Dangerous Detected	Dangerous Undetected
Exhaust seal failure	X		
Exhaust seat failure	X		
Inlet seal failure			X
Inlet seat failure			X
Return spring failure		T2m	
Valve sticks shifted		T2m	
Valve sticks in mid-position		T2m	
Valve sticks unshifted	X		

Annex P – Change Management System
(Informative)

The key elements for a successful change management process have been identified below. The documentation requirements for each step may differ and may be part of an overarching change management process that may include non-safety elements or may be specific to the safety system architecture.

A robust change management system should provide a clear description of why the change is needed, what the change encompasses, and a description of the tasks to be performed in order to implement the change.

The key elements of a change management system are identified in the list below:

- **Change Description:**
  - The need for the change must be well understood by the individual(s) responsible for developing and implementing the change.
  - A requirements document could be the Change Description.

- **Impact Analysis:**
  - An evaluation should be conducted to determine what elements of the safety architecture could be potentially impacted.
  - Testing strategy should be developed as an output of the Impact Analysis.

- **Review:**
  - The proposed solution should be reviewed by authorized individuals with the skills to identify any foreseeable issues with the change.
  - When the solution contains multiple elements, e.g., wiring changes, component changes, sequence changes, configuration/software changes, then multiple individuals may be required to review the proposed solution.

- **Deployment/Implementation:**
  - The implementation of the solution must be done in a manner that does not result in a heightened level of risk to personnel not associated with the implementation.
  - A process to ensure the equipment is “Out of Service” should be executed to prohibit anyone from trying to use the equipment while the modification is in the process of being implemented.

- **Testing/Ready for Use Verification:**
  - The testing strategy that was developed during the Impact Assessment phase should be re-evaluated once the modification has been completed to ensure that all areas impacted by the solution are tested. There could be a situation where not everything could be foreseen during the Impact Assessment phase.
  - Regression testing to ensure that any safety function that should not have been impacted by the change is still intact and functional.
  - The testing should conform with the guidance provided in ANSI B11.0.

Annex Q – Example of avoiding an overly complex pneumatic design
(Informative)

Q.1 A pneumatic circuit without a safety function
A safety upgrade process for an existing pneumatic circuit (Figure Q.1) is explained.

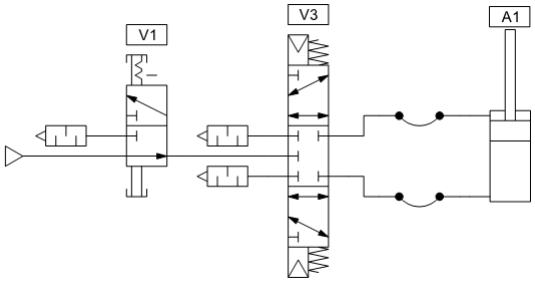


Figure Q.1 Existing Pneumatic Circuit Before a Safety Upgrade

Where:	V1	LOTO valve
	V3	3 position center closed control valve, wired to a standard PLC
	A1	Cylinder with a vertically suspended load. Extending the cylinder is a downward motion

Q.2 A pneumatic circuit with a Category 2 PL=d
Safety Functions:
Based on a risk assessment, the following safety functions are identified:

- Protection against unexpected start-ups, PLr=d
- Stopping, PLr=d
- Holding, PLr=d
  (the PLr for each safety function can be different)

Measure Against Damaged Hose:
The existing design has plastic hoses. The safety function can get lost when a hose gets loose or damaged. The plastic hose that holds the vertical load must be replaced with a hydraulic type or pilot-operated check valves must be added. In this example, pilot-operated check valves, V4 and V5 are selected. The above safety functions are implemented in Figure Q.2 as Category 2 PL=d.

DC, Diagnostics Coverage:
V2, V4, and V5 are output devices. Operation of the V2 is indirectly monitored by a pressure sensor S2. The V4 and V5 operation is indirectly monitored with the cylinder position sensors S4 and S5. In the safety PLC, the time required for the cylinder to extend and retract is checked every motion cycle.

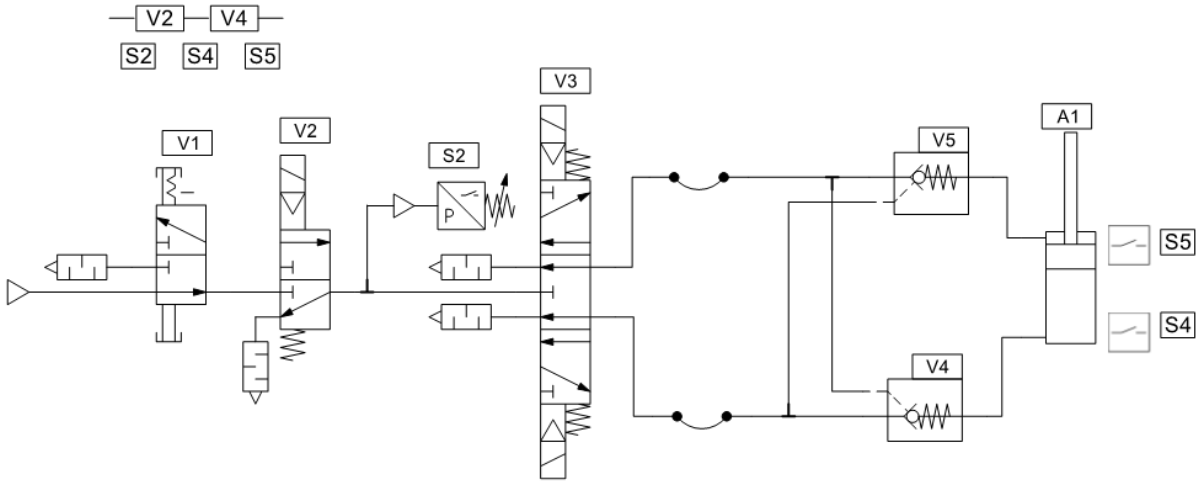


Figure Q.2A Targeting Category 2 PL=d Pneumatic Circuit

Where:

V1	LOTO valve
V2	Safety exhaust valve, wired to a safety PLC
V3	3 position center closed control valve, wired to a standard PLC
V4 / V5	Pilot operated check valves, directly mounted on the cylinder A1
A1	Cylinder with a vertically suspended load. Extending the cylinder is a downward motion.
S2	Pressure switch to indirectly monitor the operation of V2, wired to a safety PLC
S4 / S5	Cylinder position sensors to indirectly monitor the operation of V4 and V5, wired to a safety PLC

Category 2 PL=d:
To achieve Category 2 PL=d, demand rate ≤ 1/100 test rate for V2, S2, V5, V4, S5 and S4 is not possible, but the testing can occur immediately upon demand of the safety function. The time to detect the fault and bring the machine to a non-hazardous condition (stop the machine) should be shorter than the time to reach the hazard.

For example:

- When V2 is de-energized, but S2 does not change the state, V3 shifts to the center and stops the hazardous motion.
- When the time for A1 cylinder extending and retracting measured by S4 and S5 changed over the threshold, V2 gets de-energized and stops hazardous motion.

$MTTF_D$ of the testing channel ($MTTF_D$ of the S2, S4, S5, and safety controller) should be greater than $MTTF_D$/2 of the functional channel.

Measure Against Stored Energy:
In the above design, after locking out V2, the stored energy (gravity from the vertically suspended load) exists between pilot-operated check valves V4, V5, and cylinder A1. It can cause unexpected motion during maintenance activities. A measure against the unexpected motion is added in Figure Q.3. V6 is a manual pressure relief control valve located in the safe space, and V7 is a pressure relief valve. Actuating V6 allows the suspended load to be moved down safely after locking out the machine.

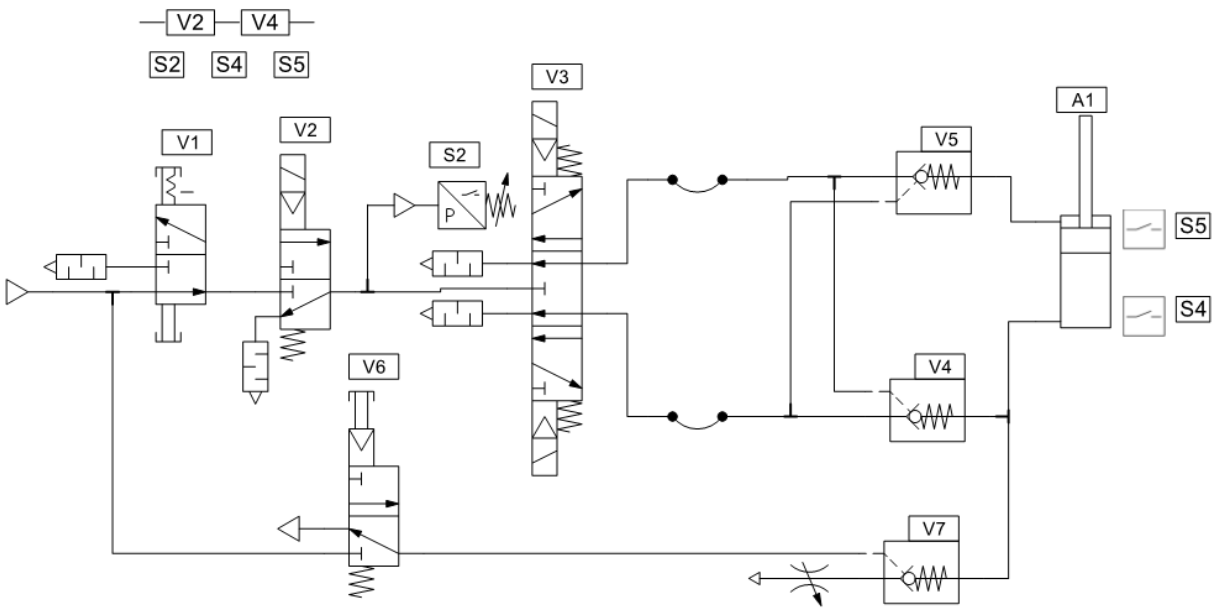


Figure Q.2B Category 2 PL=d with Manual Pressure Relief

Where:

V1	LOTO valve
V2	Safety exhaust valve
V3	3 position center closed control valve, wired to a standard PLC
V4, V5	Pilot operated check valves, directly mounted on the cylinder A1
V6	Manual pressure relief control valve located in the safe space
V7	Pressure relief valve
A1	Cylinder with a vertically suspended load. Extending the cylinder is a downward motion
S2	Pressure switch to indirectly monitor the operation of V2, wired to a safety PLC
S4, S5	Cylinder position sensors to indirectly monitor the operation of V4 and V5, wired to a safety PLC

Q.3 A Pneumatic Circuit with a Category 3 PL=d

The pneumatic circuit from Figure Q.3 is redesigned to a Category 3 PL=d circuit (Figure Q.4) by connecting V3 to a safety PLC and adding redundant pilot-operated check valves, V8 and V9. A Category 3 pneumatic circuit can get overly complicated. A designer should consider the following questions:

- Is this circuit simple enough for your maintenance team?
- Is your average maintenance team can troubleshoot and maintain this circuit?
- Does the complicated circuit motivate people to defeat or modify the safety circuit?

A simpler Category 2 PL=d circuit (Figure Q.3) can be a better choice considering the maintainability.

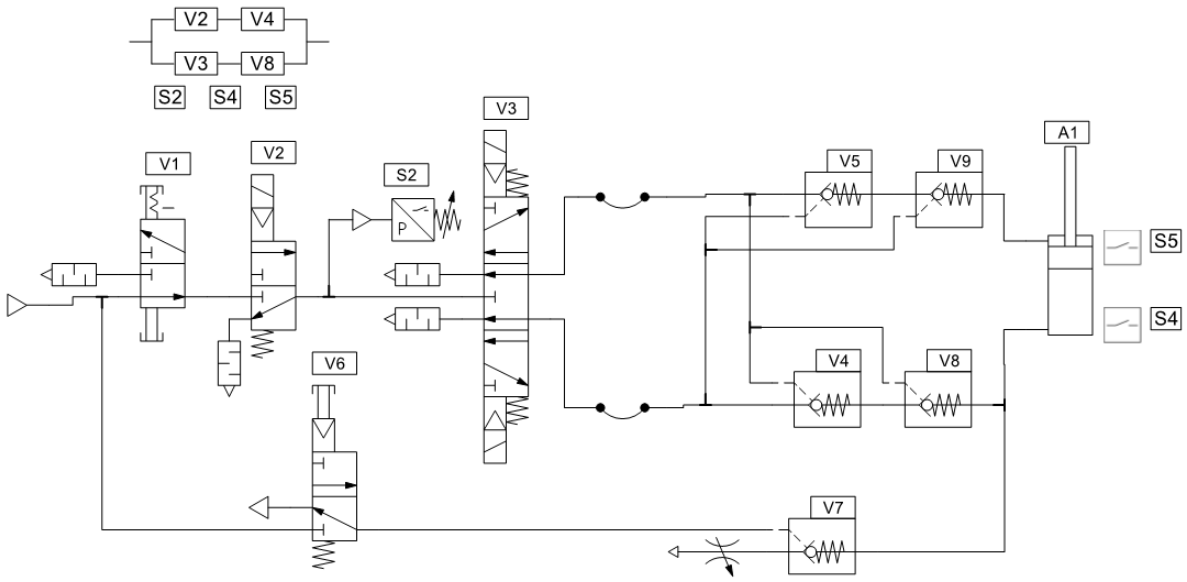


Figure Q.3 Category 3 PL=d with Manual Pressure Relief

Where:

V1	LOTO valve
V2	Safety exhaust valve, wired to a safety PLC
V3	3 position center closed control valve, wired to a safety PLC
V4, V5	Pilot operated check valves, directly mounted on the cylinder A1 via V8 and V9
V6	Manual pressure relief control valve located in the safe space
V7	Pressure relief valve
V8, V9	Pilot operated check valves, directly mounted on the cylinder A1
A1	Cylinder with a vertically suspended load. Extending the cylinder is a downward motion
S2	Pressure switch to indirectly monitor the operation of V2, wired to a safety PLC
S4, S5	Cylinder position sensors to indirectly monitor the operation of V4 and V5, wired to a safety PLC