FLUID POWER
MACHINERY
SAFETY GUIDEBOOK

ROSS CONTROLS®

<table>
<tr><td>**1**</td><td>INTRODUCTION</td></tr>
</table>

This document outlines the safety requirements for implementing Fluid Power safety solutions. This includes a review of standards requirements, risk assessment methods and risk reduction measures along with an overview of the safety design and implementation process.

<table>
<tr><td>**2**</td><td>REQUIREMENTS</td></tr>
</table>

All machines are unique. The examples in this document may not provide adequate risk reduction in all cases and additional risk reduction measures may be required. However, this guide presents a process to assist with this determination.

Protecting personnel from machinery accidents is the driving factor behind modern machine safety directives. Around the world there are legal requirements for companies to maintain safe workplaces for their employees, not to mention the threat of fines and lawsuits. The **Machinery Directive for the EU and OSHA, for the US**, are two of the most commonly referenced safety requirements.

The Machinery Directive and OSHA requirements differ in specifics due to the differing legal systems but in general both require the OEM and end user to collaborate on machine safeguarding solutions that work best for machine operation, operator tasks, and the risks those interactions possess. The Machinery Directive puts the onus on the machinery supplier while OSHA places ultimate responsibility on the end user.

Use the links below for additional information regarding Machinery Directive requirements or OSHA requirements.

Machinery Directive 2006/42/EC - https://eur-lex.europa.eu

OSHA CFR 29 Part 1910 - https://www.osha.gov
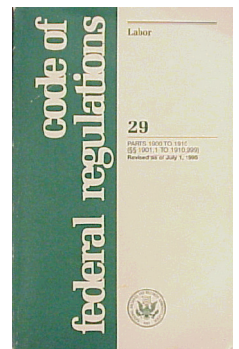
The Machinery Directive ultimately requires specific components and machines to bear a CE mark stating that they meet the requirements of the directive. In order to apply the CE mark the manufacturer must have a technical file containing documentation that shows that specific requirements are met.

Technical Files should include the following information:

- Description of the apparatus, usually accompanied by a block diagram
- Wiring and circuit diagrams
- General arrangement drawings
- List of standards applied
- Records of risk assessments and assessments to standards
- Description of control plan
- Data sheets for critical sub-assemblies
- Parts list
- Copies of any markings and labels
- Copy of instructions (user, maintenance, installation)
- Test reports
- Quality control & commissioning procedures
- Declaration of Conformity

Other published directives that apply to machinery and machine component manufacturers are the "Electric and Electronic Engineering" and "Mechanical Engineering" directives.

Electric and Electronic Engineering	Electromagnetic compatibility Directive (EMC) 2014/30/EU Equipment for explosive atmospheres Directive (ATEX) 2014/34/EU Low Voltage Directive (LVD) 2014/35/EU Radio Equipment Directive (RED) 2014/53/EU Restriction of the use of certain hazardous substances Directive (RoHS) 2011/65/EU
Mechanical Engineering and means of Transport	Equipment for Explosive Atmospheres Directive (ATEX) 2014/34/EU Pressure Equipment Directive (PED) 2014/68/EU Simple Pressure Vessels Directive (SPVD) 2014/29/EU

The terminology of the Machinery Directive and OSHA regulations tends to be vague in nature. In other words, these regulations are not prescriptive, but simply define the processes that should be followed to be in compliance. It is impossible to prescribe a specific solution, device, or method that will work with equal effectiveness in diverse applications such as rail yards, steel plants, paper mills, or food processing facilities where the machines and risks are vastly different. The non-prescriptive nature of these regulations can allow for flexibility in developing solutions but can also be immensely frustrating for companies that are looking for more specific guidance. Safety standards supply this guidance.

The Machinery Directive defines the essential requirements of safety which have influence on the design and construction of the machine. Standards provide the technical specifications needed by professionals to produce the equipment which complies with the requirements for safety and health prescribed by the regulation. Standards which are applicable with European directives are harmonized under the specific directive. Following the harmonized standards will lead to the Presumption of Conformity and the machine builder is allowed to bear the CE mark.

 ROSS CONTROLS®

3	STANDARDS

Standards provide recommended processes, procedures and information on the legal requirements found in the Machinery Directive and OSHA. Standards are created by companies and organizations that have a vested interest in those standards and typically include end users, OEMs, and component suppliers. Commonly referenced standards organizations include:

- ISO (International Standards Organization)
- IEC (International Electrical Commission)
- ANSI (American National Standards Organization)
- NFPA (National Fire Protection Association)
- NFPA (National Fluid Power Association)
- CSA (Canadian Standards Association)
- UL (Underwriters Laboratories)

Other global standards include:
- EN for Europe
- DIN for Germany
- JIS for Japan
- NR for Brazil
- AS for Australia
- GB for China
- and many others for other countries

Before getting into specific standards it is important to understand a few points about reading them.
- An individual standard is often dependent on other standards. For instance, a standard may mention that a risk assessment is required but may reference another standard for specific instructions on how to do it. The standard will include a list of "Normative references" that work hand in hand with that specific standard. There may also be "Informative references". These standards and documents may be useful depending on the specific machine and application.
- The term "shall" indicates that a statement is a requirement and the term "should" means it is a good engineering practice.
- The Annexes provide a great resource to the standard document but are not a binding part of the standard.

Standard Types

The reason standards can be so useful is because they are created to address a specific aspect of a safety system or a specific type of machine allowing them to provide much more detailed requirements and recommendations.

Standards are grouped in three types:
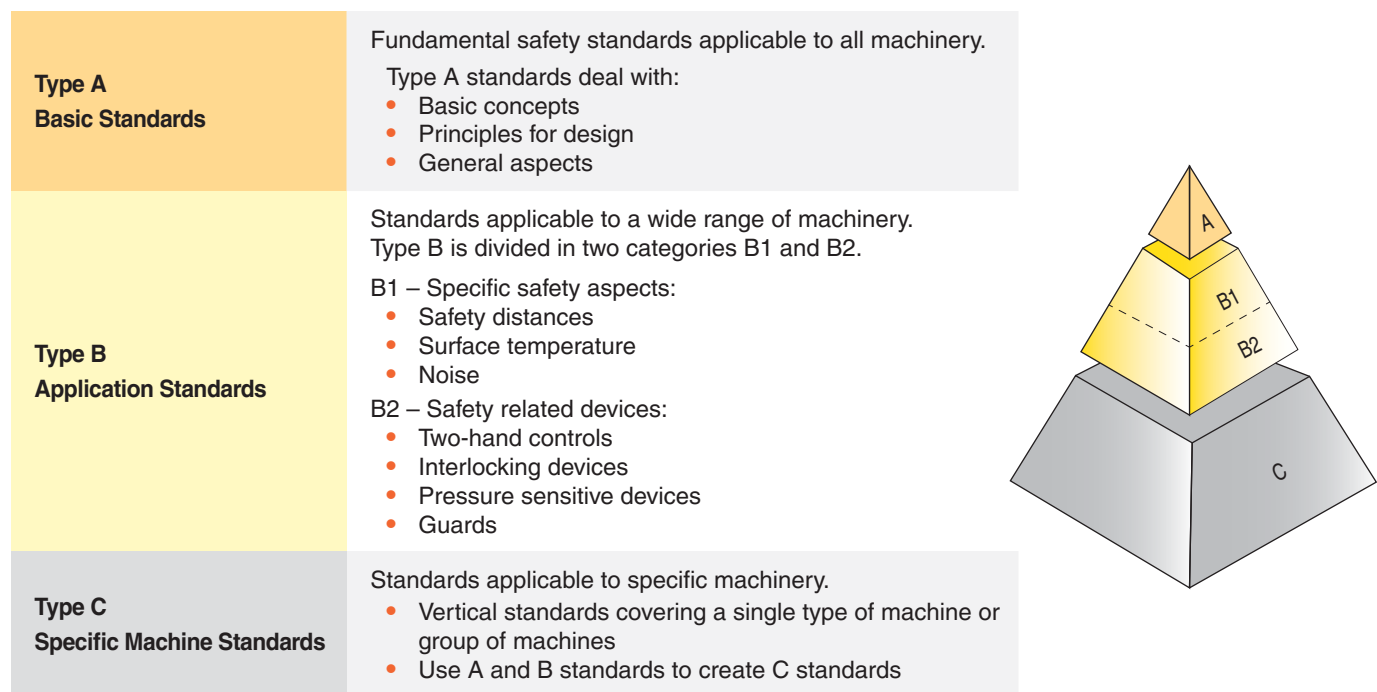
> A, B and C standards

Type-A standards (basis standards) like ISO 12100 and ANSI B11.0 give basic concepts, principles for design, and general aspects that can be applied to all machinery.

Type-B standards (generic safety standards) deal with one or more safety aspect(s), or one or more type(s) of safeguards that can be used across a wide range of machinery:

- Type-B1 standards for particular safety aspects (e.g., safety distances, surface temperature, noise).
- Type-B2 standards for safeguards (e.g., two-hands controls, interlocking devices, pressure sensitive devices, guards)

Type-C standards (machinery safety standards) deal with detailed safety requirements for a particular machine or group of machines like ISO 16092-4 for pneumatic presses.

International Safety Standards Levels		
Type A **Basic Standards**	Fundamental safety standards applicable to all machinery. Type A standards deal with: • Basic concepts • Principles for design • General aspects	
Type B **Application Standards**	Standards applicable to a wide range of machinery. Type B is divided in two categories B1 and B2. B1 – Specific safety aspects: • Safety distances • Surface temperature • Noise B2 – Safety related devices: • Two-hand controls • Interlocking devices • Pressure sensitive devices • Guards	
Type C **Specific Machine Standards**	Standards applicable to specific machinery. • Vertical standards covering a single type of machine or group of machines • Use A and B standards to create C standards	

Type C standards shall be used for specific machines types. Type A & B standards may also be used to help implement some of the requirements of a C type standard. For instance, a safety interlock may be referenced to be used on a plastic blow molding machine which has a type C standard but uses the specifics of a type B standard that show how to implement the safety interlock. Type A & B standards would also be used for any machine where no type C standard exists.

A and B type standards outline the safety development process and are frequently referenced by many other global standards. These standards are often used with other standards listed below to implement complete machinery safety solutions.

OSHA/NFPA/NEMA Standards (If the plant/facility is in the United States)

- 29CFR 1910.212 General Requirements for All Machines
- 29CFR 1910.147 Control of Hazardous Energy
- 29CFR 1910.213-218 Machine specific standards (Type C Standards)
- 29CFR 1910.219 Mechanical Power-transmission Apparatus
- 29CFR 1910.303-308 Electrical Safety
- 29CFR 1910.333 Electrical Safe Work Practices
- 29CFR 1910.95 Occupational Noise Exposure

 ROSS CONTROLS®

ANSI Standards (If the plant/facility is in the United States)

- ANSI/NFPA 70: National Electrical Code - 2020
- ANSI/NFPA 70E: Standard for Electrical Safety in the Workplace - 2021
- ANSI/NFPA 79: Electrical Standard for Industrial Machinery - 2021
- ANSI Z535.1 – 2017: Safety Colors
- ANSI Z535.2 – 2011: Safety Signs
- ANSI Z535.4 – 2011: Product Safety Signs & Labels
- ANSI B11.0 – 2020: Safety of Machinery
- ANSI B11.19 – 2019: Performance Requirements for Risk Reduction Measures: Safeguarding and other Means of Reducing Risk
- ANSI B11.20 – 2017: Safety Requirements for Integrated Manufacturing Systems
- ANSI B11.26 – Functional Safety for Equipment: General Principles for the Design of Safety Control Systems Using ISO 13849-1
- ANSI/ASME B20.1 – 2018: Safety Standard for Conveyors and Related Equipment
- ANSI/PMMI B155.1 – 2016: Safety Requirements of Packaging Machinery
- ANSI/RIA 15.06 – 2012 – Industrial Robots and Robot Systems – Safety Requirements
- ANSI Z244.1 – 2016: Control of Hazardous Energy, Lockout, Tagout, and Alternative Methods

CSA Standards (If the plant/facility is located in Canada)

- CSA Z142:2010 – Code for Power Press Operation: Health, Safety, and Safeguarding Requirements
- CSA Z432:2016 – Safeguarding of Machinery
- CSA Z434:2014 – Industrial Robots and Robot Systems
- CSA Z460:2013 – Control Of Hazardous Energy – Lockout And Other Methods

International Standards

- ISO 12100:2010: Safety of Machinery; General Principles for Design, Risk Assessment and Risk Reduction
- ISO 13850:2015 Safety of Machinery; Emergency Stop Equipment - Functional Aspects & Principles for Design
- ISO 13851:2019 Safety of Machinery; Two hand Control Devices – Functional Aspects & Principles of Design
- ISO 13854:2017 Minimum gaps to avoid crushing of parts of the human body
- ISO 13857:2019 Safety of Machinery; Safe Distances to Prevent Hazardous Zones Being Reached by Upper and Lower Limbs
- ISO 13849-1:2015 Safety Related Parts of Control Systems Part 1: General Principles for Design
- ISO 13849-2:2012 Safety Related Parts of Control Systems Part 2: Validation
- ISO 13855:2010 Safety of Machinery – The Positioning of Protective Equipment in Respect of Approach Speeds of the Human Body
- ISO 13856:2015 Safety of machinery – Pressure Sensitive Protective Devices
    › Part 1: Mats and Floors
    › Part 2: Edges and Bars
    › Part 3: Bumpers
    › Part 4: Pressure Sensitive Barriers
- ISO 14118:2017 Safety of Machinery – Prevention of Unexpected Start-up
- ISO 14119:2013 Safety of Machinery – Interlocking Devices Associated with Guards – Principles for Design and Selection
- ISO 14120:2015 Design and Construction of Fixed and Movable Guards
- EN 61496:2020 Safety of Machinery – Electro-Sensitive Protective Equipment (Parts 1, 2, 3, 7)
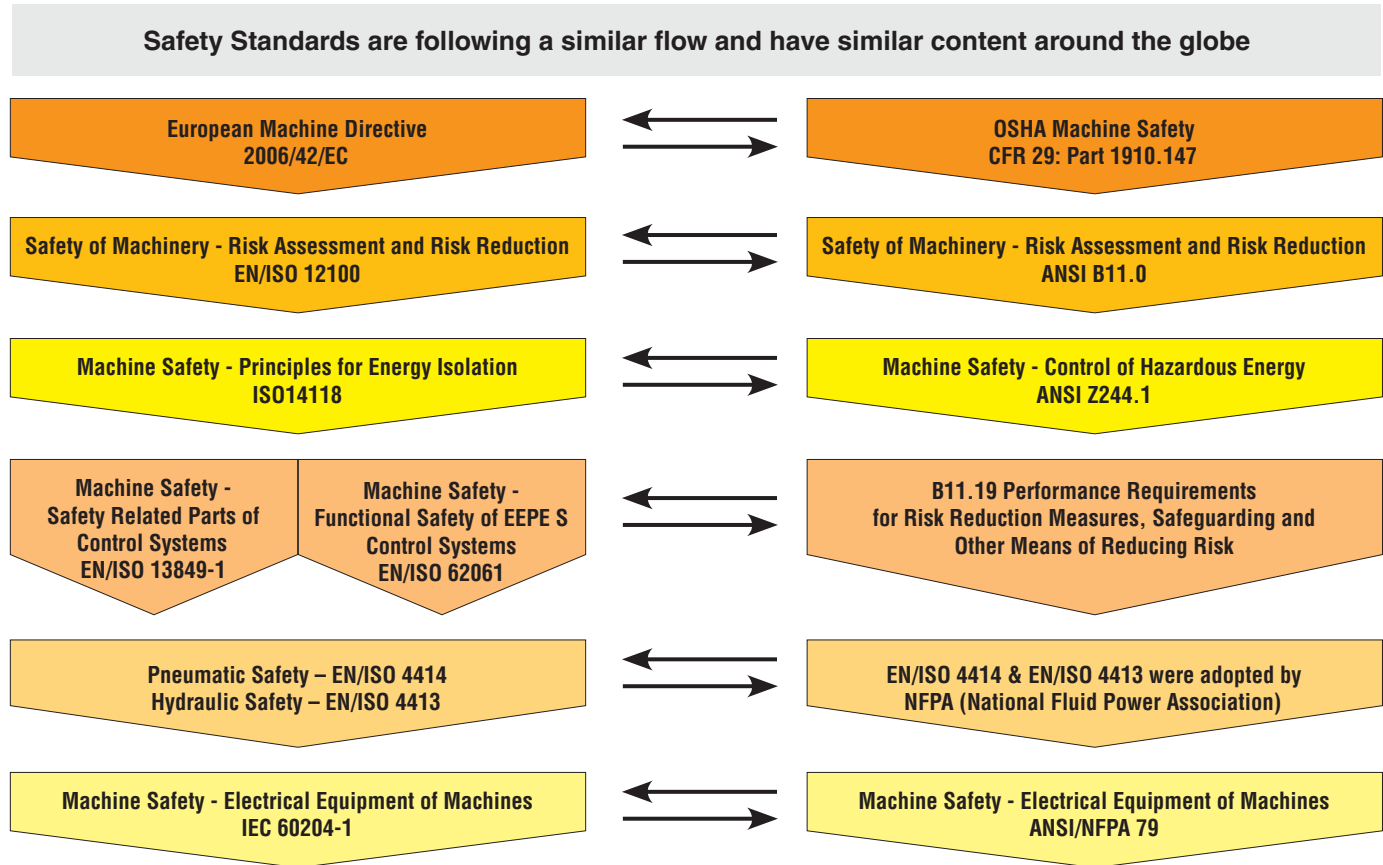
International Electro-Technical Commission Standards (IEC)

- IEC 60204-1:2016 Safety of Machinery – Electrical Equipment of Machines
- IEC 60529:1989/AMD2:2013/COR1:2019 Degrees of protection Provided by Enclosures
- IEC 61508:2010 Functional Safety Electrical, Electronic and Programmable Electronic Safety Related Systems
- IEC 62061:2016 Safety of Machinery: Functional Safety of Safety Related electrical, electronic and programmable electronic control systems

Harmonization and Differences of Standards

While the list of standards can seem confusing it is important to understand that following a standard means following a process that guides you through the process of achieving acceptable risk within a machine that will meet the local regulations. The Machinery Directive and OSHA require a risk assessment but do not mention how to do it. Using standards that are harmonized under the Machinery Directive provides for the presumption of conformity. However, you could choose ISO 12100 or ANSI B11.0 to meet either regulation's requirement. The Machinery Directive does not require you to use ISO nor does OSHA require you to follow ANSI.

With that said, the standards are using the same terminology and have many of the same requirements. In fact, many of the same companies and individuals sit on multiple standards committees because they believe is it is critical to make the standards more uniform while still meeting local legal requirements. Below is an example of how several standards are becoming more and more similar and some like ISO 4413 & 4414 are globally harmonized.

Safety Standards are following a similar flow and have similar content around the globe

European Machine Directive 2006/42/EC	**OSHA Machine Safety CFR 29: Part 1910.147**
Safety of Machinery - Risk Assessment and Risk Reduction EN/ISO 12100	**Safety of Machinery - Risk Assessment and Risk Reduction ANSI B11.0**
Machine Safety - Principles for Energy Isolation ISO14118	**Machine Safety - Control of Hazardous Energy ANSI Z244.1**
Machine Safety - Safety Related Parts of Control Systems EN/ISO 13849-1 / **Machine Safety - Functional Safety of EEPE S Control Systems EN/ISO 62061**	**B11.19 Performance Requirements for Risk Reduction Measures, Safeguarding and Other Means of Reducing Risk**
Pneumatic Safety – EN/ISO 4414 Hydraulic Safety – EN/ISO 4413	**EN/ISO 4414 & EN/ISO 4413 were adopted by NFPA (National Fluid Power Association)**
Machine Safety - Electrical Equipment of Machines IEC 60204-1	**Machine Safety - Electrical Equipment of Machines ANSI/NFPA 79**

   ROSS CONTROLS®

Fluid Power Specific Standards

The two basic standards for fluid power safety design are:

➢ ISO 4413 Hydraulic fluid power — General rules and safety requirements for systems and their components
➢ ISO 4414 Pneumatic fluid power — General rules and safety requirements for systems and their components

The standards above have been adopted by the NFPA (National Fluid Power Association). Following these standards helps users meet the requirements of EU, U.S., and some other countries' regulations. However, these are basic standards that define well tried practices. These standards do not specify anything regarding the design of a fluid power safety component or system. However, they do provide a normative reference to ISO 12100 for risk assessment and risk reduction and ISO 13849-1 for design and implementation.

ISO 4414:2010 and ISO 4413:2010 have the same general requirements

5 General rules and safety requirements

5.1 General

5.1.1 When designing pneumatic or hydraulic systems for machinery, all intended operations and use of systems shall be considered. Risk assessment, e.g., in accordance with ISO 14121-1 (replaced by ISO 12100:2010), shall be carried out to determine the foreseeable risks associated with systems when they are used as intended. Reasonably foreseeable misuse shall not cause hazards. The risks identified shall be eliminated by design and, where this is not practicable, safeguards (first preference) or warnings (second preference) against such risks shall be incorporated, in accordance with the hierarchy established in ISO 12100.

NOTE: This International Standard provides requirements for components of fluid power systems; some of these requirements are dependent on the hazards associated with the machine in which the system is installed. Therefore, the final specification and construction of the pneumatic or hydraulic system could need to be based on risk assessment and agreement between purchaser and supplier.

5.1.2 The control systems shall be designed in accordance with the risk assessment. This requirement is met when ISO 13849-1 is used.

ISO 13849-1 has two specific statements about Fluid Power safety

1 Scope

Pneumatics and Hydraulics are part of the safety related part of the control system (SRP/CS).

5.1 Specification of Safety Functions

Where necessary, the requirements for characteristics and safety functions shall be adapted for use with different energy sources. As most of the references in Tables 8 and 9 relate to electrical standards but the applicable requirements will need to be adapted in the case of other technologies (e.g., hydraulic, pneumatic).

Per ANSI B11.0

7.2 Control systems performing a safety function

Some risk reduction measures involve safety functions which are performed/executed by a system of controls. The control system elements responsible for the safety function are considered the safety-related parts of the control system (SRP/CS).

Informative Note 1: SRP/CS can be electrical, electronic, hydraulic, and/or pneumatic or any combination thereof (see ISO 13849-1 and ANSI B11.26). The SRP/CS may be composed of sensors, logic solvers and actuators.

7.2.3 Stop functions

When pneumatic, hydraulic, or mechanical elements are incorporated into a safety stopping function, the circuit design and component selection shall be appropriate for the required level of safety performance.

It is clear that fluid power output devices are part of the safety related parts of the control system and must meet the risk reduction level required by the hazard that the safety function is addressing. ISO 12100, ANSI B11.0, ISO 13849-1, ANSI B11.19, and ANSI Z244 will be used below to introduce the process of designing a safety system.

| **4**	**SAFETY DEVELOPMENT PROCESS**

Many global component and equipment suppliers provide a suggested safety development process or lifecycle to guide customers/users through a systematic approach of developing and implementing machine safety solutions. Below is a 6-step development process that follows the requirements of the applicable safety standard.

	Machinery Safety Development : A Systematic Development Process	
Step 1	**Risk Assessment**	• Risk Assessment for all task and hazard pairs • Pressure and Force Analysis for fluid power risks • Identifying the system Performance Level required (PLr) for each hazard
Step 2	**Functional Specification Development**	• Determination of job task types for each hazard • Determination of functionality needs • Determination of mitigation techniques • Determination of required safety functions
Step 3	**Selection of Mitigation Devices**	• For electrical power, mechanical power, fluid power, and all sources of hazardous energy
Step 4	**Safe Design**	• For electrical power, mechanical power, and fluid power design • Design verification calculations to ensure that the Performance Level achieved (PLa) exceeds or meets the Performance Level required (PLr)
Step 5	**Installation & Validation**	• Installation process & procedures according to manufacturer • Validation that each safety function operates as intended • Validation should include fault injection and functional testing
Step 6	**Periodic Testing and Maintenance of the Safety Components**	• Maintenance according to manufacturer requirements • Annual testing of each safety function

ROSS CONTROLS®

ANSI B11.0 takes the approach of defining responsibilities for component suppliers, machine suppliers, and end users and encourages collaboration throughout the lifecycle of the machine. This collaboration helps ensure that risk is properly assessed and, ultimately, is reduced to an acceptable level. Collaboration lets the parties involved plan and implement the process to ensure that all residual risk is effectively communicated throughout the chain of design and implementation to the end-user so that they may deal with it properly.

ANSI B11.0 Figure 5: Sample of Machinery Lifecycle Responsibilities
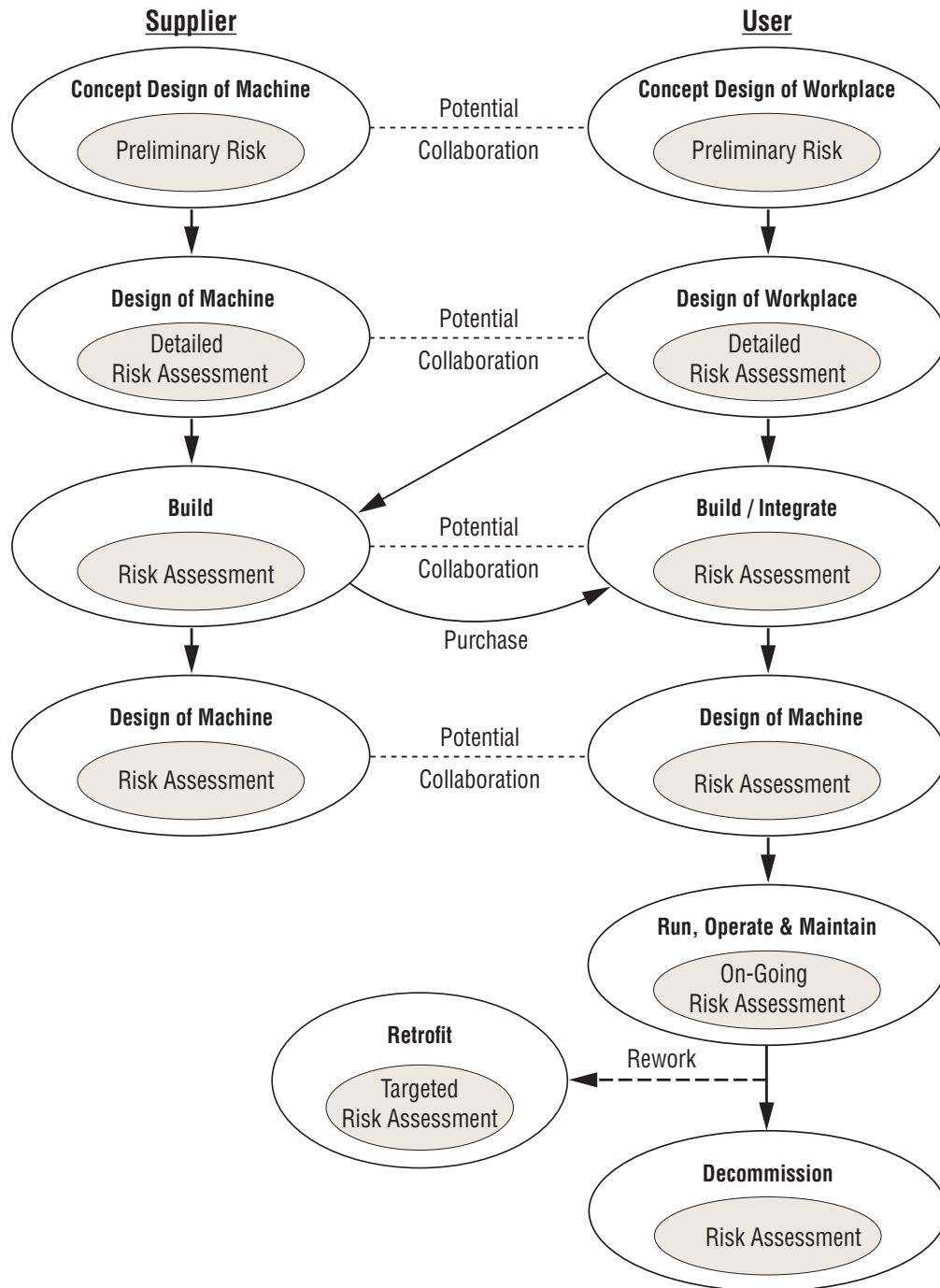
5	RISK ASSESSMENT

- Risk assessment for all task and hazard pairs
- Pressure and force analysis for fluid power risks
- Identifying the required system Performance Level (PLr) for each hazard

Risk assessment is fundamental to machine safeguarding. The goal of a safety system is to reduce risk to an acceptable level with risk being defined as a task & hazard pair. If the risk assessment and the risk reduction are implemented properly, the safety system will be integral with the machine and allow employees safe access to perform their required tasks in a safe, yet, unencumbered way. A safety system that is burdensome is likely to be bypassed or circumvented in the name of expediency and productivity. Also, the risk reduction measure should not create new hazards.

The risk assessment process includes the steps of analyzing the inherent risks of the machine, tasks that cause people to be exposed to those inherent risks, and ultimately includes the application of risk reduction methods as well as documenting the results. The whole process should also be considered as an iterative process in which all task & hazard pairs are assessed for severity, frequency, and possibility of avoidance. The risk assessment result would be a category and/or performance level recommendation that risk reduction measures must meet.

If the residual risk is not deemed to be acceptable (tolerable), then the process should be repeated to determine what additional reduction measures need to be applied. However, risk assessment also allows that not all risks can be eliminated or reduced within reasonable economic limits. Whether or not the residual risk is determined to be acceptable is ultimately the responsibility of the end user.

The best approach to performing a risk assessment is as a team, allowing the input of different opinions as to what tasks need to be performed and what hazards exist. Operators, as well as maintenance staff, should be included along with engineers, management, safety staff, and other employees that can offer useful opinions and information. You should also consider bringing "outsiders" to the team for these people can bring specific safety expertise to the process that, otherwise, may be lacking on your team. ANSI B11.0: 2020 now includes a list of responsibilities for the supplier and user of machinery and recommends points of potential collaboration. The machine manufacturer is now responsible for sharing the assessment with the user (for new or rebuilt machines). The user, in the past, was solely responsible for machine safety. If the assessment program is properly structured initially, a risk assessment will result in the identification of hazards that were overlooked previously or allowed to exist because they were not covered by any standard. The assessment should be expanded beyond human injury to cover damage to the machine and other company assets as well as damage to the environment. This will result in a safer and more efficient workplace. This does not mean that the manufacturer can eliminate all risk. The manufacturer must identify and communicate any residual risk to the end user.

 ROSS CONTROLS®

Risk Estimation Steps According to ISO 12100 and ANSI B11.0

ISO 12100 and ANSI B11.0 provide guidance for the risk assessment process which consists of risk estimation and risk reduction. The flow charts below outline the risk assessment processes for ISO 12100 and ANSI B11.0. While appearing slightly different, the two processes are near identical.

ISO 12100 – Risk Assessment Process

ANSI B11.0 – Risk Assessment Process
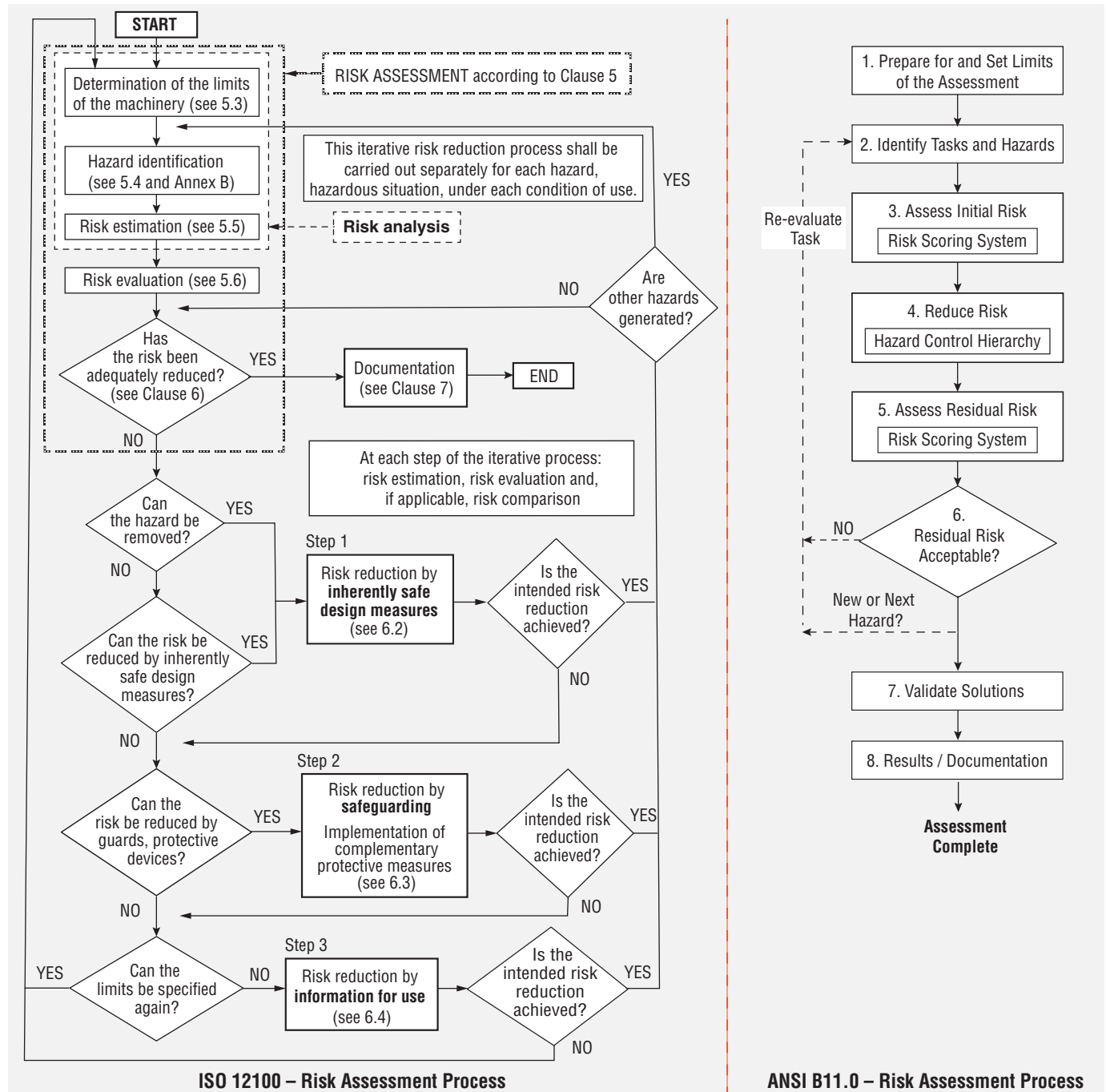
Step 1 is to determine the limits and scope of the machinery and assessment.

Step 2 is to identify tasks and associated hazards. This includes the affected persons, the tasks they perform, and hazards they are exposed to. It is important to not overlook hazards associated with fluid power portions of the safety system.

Step 3 includes initial risk estimation in order to determine what level of risk reduction is required.

There are numerous risk assessment estimation tools available. Selecting one that is best for you is a critical step. The following sections present examples of several widely used risk estimation tools.

ANSI B11.0 Risk Estimation Example

The ANSI B11.0 risk estimation matrix shown below uses Severity and Probability in order to score identified risks. There are four choices each for both severity of harm and probability of occurrence. These are defined in ANSI B11.0 section 6.4.2.

Severity	• Catastrophic – death or permanently disabling injury or illness (unable to return to work); • Serious – severe debilitating injury or illness (able to return to work at some point); • Moderate – significant injury or illness requiring more than first aid (able to return to same job); • Minor – no injury or slight injury requiring no more than first aid (little or no lost work time).
Probability	• Very likely – near certain to occur; • Likely – may occur; • Unlikely – not likely to occur; • Remote – so unlikely as to be near zero.

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

ISO13849-1 Risk Estimation Example

ISO 13849-1 has its own method for determining the performance level required. It has three factors instead of two; severity of injury, frequency of exposure, and possibility to avoid; but only provides two choices for each factor. This risk estimation tool provides a required Performance Level (PLr) a, b, c, d, or e.
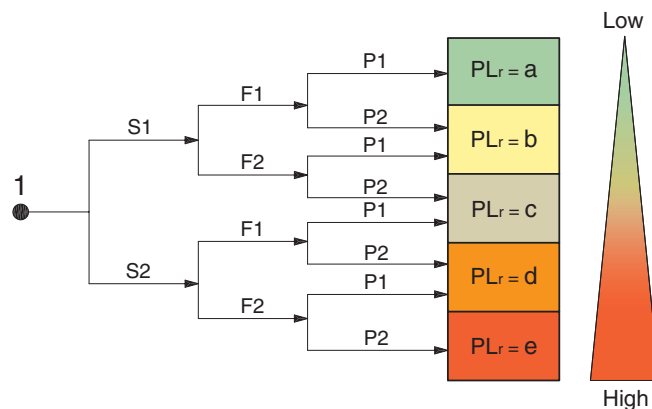
Risk graph for determining required PLr for safety function ISO 13849-1

Key:

1   Starting Point
L   Low Risk
H   High Risk
PLr Performance Level required

Risk Parameters:

S   Severity of the damage
    S1   minor injury (reversible)
    S2   serious injury (irreversible or death)
F   Frequency of the risk
    F1   rare up to frequent, short duration
    F2   frequent up to continuous, long duration
P   Possibility of avoiding the risk or limiting the damage
    P1   possible under certain conditions
    P2   rarely possible

ROSS CONTROLS®

ANSI/RIA TR15.306 Risk Estimation Example

ANSI/RIA TR15.306 uses a hybrid approach that is similar to both the ANSI B11.0 and ISO13849-1 methods for determining the performance level and category that is required. It has three factors like the ISO13849-1 methodology but it results in terms similar to the ANSI B11.0 approach.

An additional table is used to define the performance requirements, much like the ANSI B11.0 methodology.

Table 12 – RIA TR R15.306 Risk Level Decision Matrix

Severity of Injury	Exposure to the Hazard	Avoidance of the Hazard	Risk Level
S1 - Minor	E0 - Prevented		Negligible
	E1 - Low	A1 - Likely	Negligible
		A2/A3 - Not Likely/Possible	Low
	E2 - High		Low
S2 - Moderate	E0 - Prevented		Low
	E1 - Low		Low
		A1 - Likely	Medium
	E2 - High		Medium
		A2/A3 - Not Likely/Possible	High
S3 - Serious	E0 - Prevented		Low
	E1 - Low		High
		A1/A2 - Likely/Not Likely	High
	E2 - High		High
		A3 - Not Possible	Very High

Risk Level	Minimum SRP/CS Requirements	
	PL_r	Structure Category
Negligible	c	1
Low	c	2
Medium	d	2
High	d	3
Very High	e	4

ANSI B11.26 Risk Estimation Comparison

Table 16 in ANSI B11.26 can be used to compare the required system performance in terms of ANSI B11.0 and ISO 13849-1 Category and Performance Level.

RISK LEVEL	RISK REDUCTION			
	ANSI B11.26	ANSI B11.0	Category (ISO 13849-1:1999)	Performance Level (ISO 13849-1: 2015)
Highest	Requirements of B and the use of well-tried safety principles shall apply. Safety-related parts shall be designed, so that a single fault in any of these parts does not lead to a loss of the safety function, and the single fault is detected at or before the next demand upon the safety function, but that if this detection is not possible, an accumulation of undetected faults shall not lead to loss of the safety function.	Redundancy w/continuous self-checking (e.g., Dual channel w/continuous monitoring)	3 or 4	d or e
Intermediate/High	Requirements of B and the use of well-tried safety principles shall apply. Safety-related parts shall be designed, so that a single fault in any of these parts does not lead to the loss of the safety function, and whenever reasonably practicable, the single fault is detected.	Redundancy w/self-checking upon start-up (e.g., Dual channel w/monitoring at cycle/start-up)	3	c or d
Low/Intermediate	Requirements of B and the use of well-tried safety principles shall apply. Safety function shall be checked at suitable intervals by the machine control system.	Redundancy that may be manually checked (e.g., Dual channel w/optional manual monitoring)	2	b, c, or d
Lowest	Requirements of B shall apply. Well-tried components and well-tried safety principles shall be used.	Single channel	1	b
Negligible	SRP/CS and/or their protective equipment, as well as their components, shall be designed, constructed, selected, assembled and combined in accordance with relevant standards so that they can withstand the expected influence. Basic safety principles shall be used.		B	a

Fluid Power Risk Assessment

In order to do a complete, thorough risk estimation, fluid power devices must be considered. Fluid power devices are the final control elements in most systems and must be taken into account because they have the potential to create hazards when a fault occurs.

Consider:

- Does pneumatic or hydraulic system cause motion?
- Could the pneumatic or hydraulic system cause pinching, shearing or puncture points?
- Can turning off pneumatic or hydraulic pressure cause things to move?
- Could gravity have an effect?

If there are pinch points, shearing points, and puncture points that are caused by fluid power devices, these hazards must be addressed. Take time to understand the potential failure modes of the valves used in the system; and the severity associated with the particular hazards based on the pressures and forces being used in the pneumatic or hydraulic system.

Each fluid power actuator (cylinder or otherwise) in the machine's system must be evaluated as to how it is controlled and what pressures are applied in order to determine the forces that may be generated. The control scheme of the valves in the system must also be examined in order to determine both normal and faulted conditions of the fluid power circuit. It is also important to consider what happens when a safety event occurs. Therefore, it is crucial to determine what the actuators will do when the valves are de-energized or if a fault occurs at that time.

Even though most pneumatic systems operate in the 80 to 100 psi (5.5 to 6.8 bar) range, there are many variations to this, both higher and lower. Examples that follow will be based on this common pressure range. However, it is important to consider the actual system pressure when doing a risk assessment on your own equipment. Although it may be obvious to most, it is important to note that the pressures and forces associated with hydraulics are typically much greater than those associated with pneumatics. Therefore, this evaluation is equally, if not more, important with regard to hydraulic systems.

 ROSS CONTROLS®

In order to help determine severity, ANSI B11.0 provides additional references to allowable force and pressure. Annex E presents Table 8 - Estimation of Injury Severity. This includes references for values of catastrophic, serious, moderate, and minor for various injuries including burns, lacerations/amputations, fracture, sound, and electrical shock. Fracture references both force and pressure as follows:

Table 8 — Estimation of Injury Severity				
Table 8 illustrates one way that forces and energies can be used to estimate increasing severity potential. This informative table provides guidance on evaluating severity and has been developed based on "post incident" and test data. The values in the table (which have been determined from literature referenced below the table) should not be used as strict definitions of severity. Values may differ based on application specific data or individual susceptibilities. Some detailed injury information presented below may be useful in evaluating historical data with known hazardous events. The reader should be notified that variations to this table are acceptable.				
Injury Type	**Catastrophic**	**Serious**	**Moderate**	**Minor**
Lacerations or Amputations** 2 5	Lacerations or amputations* that could result in death or a permanently disabling injury such as blindness. *For example, amputations of: Hand Foot Arm Leg Eye	Lacerations of the head or face requiring sutures or other closure in lieu of sutures or partial blindness typically caused by: • flying projectiles; • stationary sharp edges; • blunt, sharp edges. Amputation of finger(s) or toe(s), typically caused by: • sharp edges mechanically in motion (e.g. rotating, reciprocating, shearing);	Lacerations, not involving the face, requiring sutures or other closure in lieu of sutures typically caused by: • stationary sharp edges; • blunt, sharp edges. External (deep) Lacerations (> 10 cm long on body; > 5 cm long on	Minor/superficial cuts requiring bandaging treatment; typically caused by: • stationary blunt surfaces; • offset, blunt edges with loads less than 28 kPa (4 psi).
Fracture 2 5 Fracture forces are derived from literature search that identified pain and fracture thresholds at 150 N (33.7 lbf), 400 N (89.9 lbf) and 2000 N (449.6 lbf) using an 80mm (3.15 in) diameter load cell.	399.9 kPa (58 psi) For example, fracture of spinal column.	Fracture of long bones in arms, legs or fracture of the skull or spine*, typically caused by loads exceeding 297 kPa (43 psi) and 399.9 kPa (58 psi) under certain test conditions. * For example: • Ankle • Leg (femur and lower leg) • Hip • Thigh • Skull • Spine (minor compression fracture) • Jaw (severe) • Larynx • Multiple rib fractures • Blood or air in chest	Fracture of small bones*, typically caused by loads between 297 kPa (43 psi) and 399.9 kPa (58 psi) under certain test conditions. * For example: • Extremities (finger, toe, hand, foot) • Wrist • Arm • Rib • Sternum • Nose • Tooth • Jaw • Bones around eye	Contusions and skin abrasions typically caused by loads between 83 kPa (12 psi) and 297 kPa (43 psi) under certain test conditions. No physical signs typically caused by dynamic loads less than 83 kPa (12 psi) under certain test conditions.

The color coding in the chart below corresponds to ANSI B11.0 risk levels based on pressure and force.

Catastrophic	Serious	Moderate	Minor

The pressure supplied to an actuator is literally the driving force and the higher the pressure, the higher the force the actuator can apply to the work piece (and to an associated pinch point, etc.). The chart below indicates how much force can be generated by standard size cylinders at various pressures.

Cylinder Bore Diameter inch	Area inch^2	Force Newtons lbf					
		15 psi	30 psi	45 psi	80 psi	100 psi	150 psi
0.75	0.44	7	13	20	35	44	66
1	0.79	12	24	35	63	78	118
1.25	1.23	18	37	55	98	123	184
1.5	1.77	27	53	80	141	177	265
2	3.14	47	94	141	251	314	471
2.5	4.91	74	147	221	393	491	736
3	7.07	106	212	318	565	707	1060
4	12.57	188	377	565	1005	1257	1885
4.5	15.90	239	477	716	1272	1590	2386
5	19.63	295	589	884	1571	1963	2945

Cylinder Bore Diameter mm	Area mm^2	Force Newtons (N)					
		1 Bar	2 Bar	3 Bar	5.5 Bar	7 Bar	10 Bar
20	314.16	31	63	94	173	220	314
25	490.87	49	98	147	270	344	491
32	804.25	80	161	241	442	563	804
40	1256.64	126	251	377	691	880	1257
50	1936.49	196	393	589	1080	1374	1963
63	3117.24	312	623	935	1714	2182	3117
80	5026.54	503	1005	1508	2765	3519	5027
100	7853.98	785	1571	2356	4320	5498	7854
125	12271.84	1227	2454	3682	6750	8590	12272
150	17671.44	1767	3534	5301	9719	12370	17671

In many cases a non-monitored or single-channel valve is an unacceptable solution because any malfunction in the valve that allows pressure to continue to flow downstream could result in pinch-point forces exceeding these standards' allowances due to a fully pressurized cylinder or a cylinder with a high gravitational load. Thus, in most cases redundancy and monitoring are required in the system which raises your minimum control category to at least 3.

A simple chart shows the forces and pressures in ANSI B11.0, and how they align with performance levels.

ANSI B11.0 Table 8	Units	Catastrophic	Serious	Moderate	Minor
Force	lbf	449.6	89.9	**33.7**	
Force	N	2000	400	**150**	
Pressure	psi	59	59	**43**	12
Pressure	N/cm^2	40	40	**29.6**	8.3
PLr	–		e	d	**c**	b

ISO/TS 15066:2016 Robots and robotic devices – Collaborative robots Table A.2 contains biometric limit values for various parts of the body.

2 Table A.2 – Biomechanical Limits					
		Quasi-static contact		Transient contact	
Body Region	Specific Body Area	Maximum permissible pressure [a] N/cm²	Maximum permissible force [b] N	Maximum permissible pressure multiplier [c] P_T	Maximum permissible force multiplier [c] F_T
Skull and Forehead[d]	1 Middle of forehead	130	130	not applicable	not applicable
Skull and Forehead[d]	2 Temple	110	130	not applicable	not applicable
Face[d]	3 Masticatory muscle	110	65	not applicable	not applicable
Neck	4 Neck muscle	140	150	2	2
Neck	5 Seventh neck muscle	210	150	2	2
Back and Shoulders	6 Shoulder joint	160	210	2	2
Back and Shoulders	7 Fifth lumbar vertebra	210	210	2	2
Chest	8 Sternum	120	140	2	2
Chest	9 Pectoral muscle	170	140	2	2
Abdomen	10 Abdominal muscle	140	110	2	2
Pelvis	11 Pelvic bone	210	180	2	2
Upper Arms and Elbow Joints	12 Deltoid muscle	190	150	2	2
Upper Arms and Elbow Joints	13 Humerus	220	150	2	2
Lower Arms and Wrist Joints	14 Radial bone	190	160	2	2
Lower Arms and Wrist Joints	15 Forearm muscle	180	160	2	2
Lower Arms and Wrist Joints	16 Arm nerve	180	160	2	2
Hands and Fingers	17 Forefinger pad D	300	140	2	2
Hands and Fingers	18 Forefinger pad ND	270	140	2	2
Hands and Fingers	19 Forefinger end joint D	280	140	2	2
Hands and Fingers	20 Forefinger end joint ND	220	140	2	2
Hands and Fingers	21 Thenar eminence	200	140	2	2
Hands and Fingers	22 Palm D	260	140	2	2
Hands and Fingers	23 Palm ND	260	140	2	2
Hands and Fingers	24 Back of the hand D	200	140	2	2
Hands and Fingers	25 Back of the hand ND	190	140	2	2
Thighs and Knees	26 Thigh muscle	250	220	2	2
Thighs and Knees	27 Kneecap	220	220	2	2
Lower Legs	28 Middle of shin	220	130	2	2
Lower Legs	29 Calf muscle	210	130	2	2

ROSS CONTROLS®

It is easy to see that forces higher than these threshold values are attainable in most typical machine operations depending on actuator size and supplied pressure. In cases where these force threshold values are exceeded, additional measures must be utilized to provide adequate machine safeguarding. Other factors, such as tooling, may result in much lower force threshold values being used in the risk assessment. For instance, a cylinder with blunt tooling attached could pose a lower risk than a cylinder with sharp tooling under the same amount of force. Likewise, a cylinder stuck in the extended position would not have the same risks as a cylinder with a heating element (in a heat seal application) stuck in the engaged melting mode. In a clamping application the cylinder's force may be exerted over a clamping area smaller than the bore area. This acts as a multiplier creating a much higher force at the point of contact. ANSI B11.0 Annex Q includes data from IRRST R-956 Safe Reduced Speed and Force which lists a wide variety of acceptable speeds, force, kinetic energy, and pressures cited from various sources based on industry.

The chart below shows the change in force and pressure based on bore size, high and low pressure, and tooling contact area. It then provides a PLr based on force and pressure.

A pressure/force calculator can be found at www.rosscontrols.com, see Support and Downloads, Technical Tools page.

Instructions: 1. Enter data for bore size, contact area, high, and low pressures.
  2. The pounds of force and pressure will be calculated.
  3. The estimated PLr based on standard anthropomorphic data will be shown.

This chart is based on other standards, including ANSI B11.0 Annex E, Table 8 - Estimation of Injury Severity Fracture Data.

System Data	Imperial		Metric	
Bore	1.5	in	3.81	mm
Tooling Contact Area	1.5	in^2	967.74	mm^2
High Pressure	80	psi	0.5516	mpa
Low Pressure	20	psi	0.1379	mpa
Bore Area	1.767	in^2	1140	mm^2

Calculations	Units	High Pressure	Low Pressure	PLr High	PLr Low
Force	lbf	141.4	35.5	d	c
	N	628.9	157.2		
Pressure at Tool	psi	94.2	23.6	d	b
	N/cm^2	65.0	16.2		

6	FUNCTIONAL SPECIFICATION DEVELOPMENT

- Determination of job task types for each hazard
- Determination of functionality needs
- Determination of mitigation techniques
- Determination of required safety functions

Risk Reduction processes follow a hierarchy of risk reduction measures to determine what risk reduction method(s) will be used. The hierarchy represents the different types of measures that may be available and lists them from most preferred to least preferred - ranging from Inherently Safe Design to Administrative Controls. It is important to realize that, even though the most preferred type of risk reduction measure is to design out the hazard, it may be difficult or impossible to use that method because of how the machine functions and/or, especially, if the machine has already been designed and built. Quite often, the most feasible option is to use a combination of the different types of risk reduction measures such as guards, control devices, procedures, and personal protective equipment (PPE).

	Classification	Risk Reduction Measures	Examples	Influence on Risk Factors
Most Preferred	Inherently Safe by Design	Design Out (Elimination or Substitution)	• eliminate pinch points (increase clearance) • intrinsically safe (energy containment) • automated material handling (robots, conveyors, etc.) • redesign the process to eliminate or reduce human interaction • reduce force, speed, etc. through selection of inherently safe components • substitute less hazardous chemicals	• impact on overall risk (elimination) by affecting severity and probability of harm • may affect severity of harm, frequency of exposure to the hazard under consideration, and/or the possibility of avoiding or limiting harm depending on which method of substitution is applied.
	Engineering Controls	Guards, Control Functions and Devices	• guards • interlock devices • presence sensing devices (light curtains, safety mats, area scanners, etc.) • two-hand control and two-hand trip devices • alternative methods to lockout to control hazardous energy	• greatest impact on the probability of harm (occurrence of hazardous events under certain circumstance) • minimal if any impact on severity of harm
	Administrative Controls	Awareness Means	• lights, beacons, and strobes • computer warnings • signs and labels • beepers, horns, and sirens	• potential impact on the probability of harm (avoidance) • no impact on severity of harm
		Information for Use (Training and Procedures)	• safe work procedures • training	• potential impact on the probability of harm (avoidance and/or exposure) • no impact on severity of harm
		Administrative Safeguarding Methods	• safe-holding safeguarding method	• potential impact on the probability of harm (avoidance and/or occurrence) • no impact on severity of harm
		Supervision	• supervisory control of configurable elements	
		Control of Hazardous Energy	• lockout / tagout	
		Tools	• workholding equipment • hand tools	• potential impact on the probability of harm (avoidance and/or occurrence) • potential impact on severity of harm
Least Preferred		Personal Protective Equipment (PPE)	• safety glasses and face shields • ear plugs • gloves • protective footwear • respirators	• potential impact on the probability of harm (avoidance) • potential impact on severity of harm

Inherently safe design measures include elimination or substitution. Elimination could include things like redesigning the machine, automating a portion of the machine to eliminate a dangerous task, or changing the sequence to completely do away with the potential hazard. Substitution could include implementing measures that reduce speed, pressure, force, and direction to reduce the hazard to an acceptable level rendering it safe. Engineering controls (safety systems) reduce risk or eliminate the frequency of exposure to the hazard. This can be done through the use of physical guarding and/or safety systems that control the electrical, pneumatic, hydraulic, and other energy sources in a way that meets the safety level determined by the risk assessment for that task/hazard pair.

 ROSS CONTROLS®

Selecting the most appropriate risk reduction measures will be application specific and may take multiple steps. ANSI B11.19 and many ISO Type B standards provide performance requirements. They include information on the use of fixed and moveable guards, control functions, and control devices as well as administrative controls.

Below is an example list of recognized safety functions for electrical control systems from ISO 13849-1. See Tables 8 & 9 below for details:

Table 8 — Some International Standards applicable to typical machine safety functions and certain of their characteristics			
Safety function/characteristic	Requirement(s)		For additional information, see:
	This part of ISO 13849	ISO 12100:2010	
Safety-related stop function initiated by safeguard [a]	5.2.1	3.28.8, 6.2.11.3	IEC 60204–1:2005, 9.2.2, 9.2.5.3, 9.2.5.5 ISO 14119 ISO 13855
Manual reset function	5.2.2	–	IEC 60204–1:2005, 9.2.5.3, 9.2.5.4
Start/restart function	5.2.3	6.2.11.3, 6.2.11.4	IEC 60204–1:2005, 9.2.1, 9.2.5.1, 9.2.5.2, 9.2.6
Local control function	5.2.4	6.2.11.8, 6.2.11.10	IEC 60204–1:2005, 10.1.5
Muting function	5.2.5	–	IEC/TS 62046:2008, 5.5
Hold-to-run function	–	6.2.11.8 b)	IEC 60204–1:2005, 9.2.6.1
Enabling device function	–	–	IEC 60204–1:2005, 9.2.6.3,10.9
Prevention of unexpected start-up	–	6.2.11.4	ISO 14118 IEC 60204–1:2005, 5.4
Escape and rescue of trapped persons	–	6.3.5.3	–
Isolation and energy dissipation function	–	6.3.5.4	ISO 14118 IEC 60204–1:2005, 5.3, 6.3.1
Control modes and mode selection	–	6.2.11.8, 6.2.11.10	IEC 60204–1: 2005, 9.2.3, 9.2.4
Interaction between different safety-related parts of control systems	–	6.2.11.1 (last sentence)	IEC 60204–1:2005, 9.3.4
Monitoring of parameterization of safety-related input values	–	–	–
Emergency stop function [b]	–	6.3.5.2	ISO 13850 IEC 60204–1:2005, 9.2.5.4

[a] Including interlocked guards and limiting devices (e.g., over-speed, over-temperature, over-pressure).
[b] Complementary protective measure, see ISO 12100:2010.
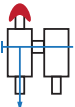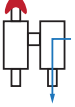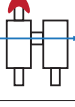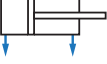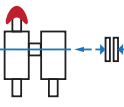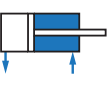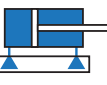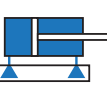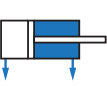
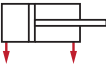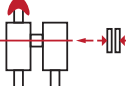| Table 9 — Some International Standards applicable to typical machine safety functions and certain of their characteristics			
Safety function/characteristic	Requirement(s)		For additional information, see:
	This part of ISO 13849	ISO 12100:2010	
Response time	5.2.6	–	ISO 13855:2010, 3.2, A.3, A.4
Safety-related parameter such as speed, temperature or pressure	5.2.7	6.2.11.8 e)	IEC 60204–1:2005, 7.1, 9.3.2, 9.3.4
Fluctuations, loss and restoration of power sources	5.2.8	6.2.11.8 e)	IEC 60204–1:2005, 4.3, 7.1, 7.5
Indications and alarms	–	6.2.8	ISO 7731 ISO 11428 ISO 11429 IEC 61310–1 IEC 60204–1:2005, 10.3, 10.4 IEC 61131 IEC 62061
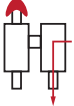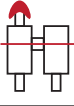
Potential safety functions for pneumatics include:

- Energy Isolation – This is the same as "Prevention of unexpected start-up" from Table 8.
- Safe Exhaust – This is the same as "Isolation and energy dissipation function from Table 8 but is also tied to the 3 top safety functions. Safety related stop initiated by a safeguard, manual reset, and start/restart functions.
- Safe Return – This is a local control function per Table 8 and is also tied to other safety functions from Table 8. Safety related stop initiated by a safeguard, manual reset, start/restart and control modes, and mode selection functions.
- Safe Stop - This is a local control function per Table 8 and is also tied to other safety functions from Table 8. Safety related stop initiated by a safeguard, manual reset, start/restart and control modes, and mode selection functions. Safe stop can be accomplished with 2 different types of solutions.
    a. Pilot Operated Check Valves
    b. Safe Control and Stop valves
- Safe Pressure/Force – This is a safety related parameter function from Table 9. It is also used with other safety functions from Table 8. Safety related stop initiated by a safeguard, manual reset, start/restart and control modes, and mode selection functions.

PNEUMATICS						
Safety Function Type	Energy Isolation	Safe Exhaust	Safe Return	Safe Return "Dual Pressure"	Safe Control and Safe Load Holding	Safe Pressure Select
PUS - Prevention of Unexpected Start-up (Lockout -Tagout) B11.26 11.3.3.1	✓					
SDE - Safe Deenergization (Safe Exhaust) B11.26 11.3.3.2		✓				
SEZ - Safe Energization (Safe Exhaust with Soft-Start) B11.26 11.3.3.2		✓				
STO - Safe Torque Off (Safe Exhaust) B11.26 11.3.3.2		✓				
SBC - Safe Brake Control B11.26 11.3.3.3 B11.26 11.3.3.2		✓	✓			
SDI - Safe Direction (Safe Return) B11.26 11.3.3.3				✓		
SS1 - Safe Stop 1 (Controlled Stop) (Safe Stop with Holding) B11.26 11.3.3.4					✓	
SS2 - Safe Stop with Blocking (Safe-Holding) B11.26 11.3.3.4					✓	
SLP - Safe Limited Pressure (Torque) B11.26 11.3.3.3						✓

 ROSS CONTROLS®

Potential safety functions for hydraulics include:

- Energy Isolation - This is the same as "Prevention of unexpected start-up" from Table 8
- Block and Bleed - This is the same as "Isolation and energy dissipation function from Table 8 but is also tied to the 3 top safety functions. Safety related stop initiated by a safeguard, manual reset, and start/restart functions.
- Block and Stop - This is a local control function per Table 8 and is also tied to other safety functions from Table 8. Safety related stop initiated by a safeguard, manual reset, start/restart and control modes, and mode selection functions.

HYDRAULICS			
Safety Function Type	Energy Isolation	Block & Bleed	Block & Stop
SDE - Safe Deenergization (Block & Bleed) B11.26 11.4.3.1		✓	
SEZ - Safe Energization (Block & Bleed) B11.26 11.4.3.1		✓	
STO - Safe Torque Off (Block & Bleed) B11.26 11.4.3.1		✓	
SBC - Safe Brake Control B11.26 11.4.3.1		✓	
SS1 - Safe Stop 1 (Controlled Stop) (Safe Stop with holding) B11.26 11.4.3.4			✓
SS2 - Safe Stop with Blocking (Safe-Holding) B11.26 11.4.3.4			✓

Safety Functions

Complete safety functions are made of input devices, logic devices, and output devices. The safety input device is the trigger for the safety function. The safety logic device monitors the input device and makes a decision on how to control the output devices. The safety logic device also monitors the feedback signals from the output device/devices. For specific design requirements, see section 10 of this document.

Safety Input	+	Safety Logic	+	Safety Output	=	Complete Safety Function

Safety reaction tables can be used to determine how individual actuators are to be controlled based on safety triggering events (the table below is just an example).

Actuator List				
Triggering Device	Clamp Cylinder	Press Cylinder	Riveting Motor	Slide Cylinder
Emergency Stop	Safe Exhaust	Safe Exhaust	Power Isolation	Safe Exhaust
Light Curtain	Safe Pressure	Safe Control & Stop	Power Isolation	Safe Return
Door Switch				

7	SAFETY FUNCTION SELECTION

- Electrical Power, Mechanical Power, Fluid Power, and all other sources of hazardous energy

Choosing the most appropriate safety function will depend on the risks, desired outcome, the potential failure modes, and residual risks. In all cases the safety logic device will drop power to the output devices. The circuit is dependent upon the output device performing the safety function when signaled to do so. Choosing the right valve requires an understanding of the operation and failure modes of the valves that might be used to implement the safety function.

Failure Modes

Understanding failure modes of the devices chosen is very important in the design process when you want to fail to a safe condition. The most common valve failure is a when a valve does not shift properly, either energizing or de-energizing, and the valve's function is not performed. This can cause unexpected motion - either at the wrong time or even in the wrong direction. Depending on the application, this could lead to a critical situation.

There are, however, many other common valve failure modes and reasons for the failures. The tables below list common fluid power valve failure modes and also some failure modes that are specific to certain valve functions.

STANDARD FLUID POWER VALVE FAILURE MODES		
PROBLEM	**RESULT**	**CONSIDERATIONS**
Pilot pressure is reduced or lost.	Valve will return to mechanically offset (OFF) position.	Ensure offset (OFF) position is the fail to safe position.
Internal wear causing leakage.	Not possible to pre-define as depends on valve design.	Ensure valve design does not allow for unsafe condition.
Dirt, grit, or rust enters valve.	Valve may stick (see valve sticking).	Make sure pipes are clean, pipe tape not used, filter hydraulic oil and air.
Valve spool sticks.	Valve will not return to mechanically offset (OFF) position. Valve can be in any number of crossover conditions.	*Requires that 2nd valve be used and placed in a circuit that allows both to function properly.
Failure of valve actuator.	If actuator fails in de-actuated position valve will return to mechanically offset (OFF) position. If actuator fails in actuated position valve will stay actuated.	*Requires that 2nd valve be used and placed in a circuit that allows both to function properly.
Failure of solenoid coil.	Valve will return to mechanically offset (OFF) position.	Ensure offset (OFF) position is the fail to safe position.
Failure subject to excessive flow.	Valve may shift without a signal.	Ensure valve is designed to prevent such from causing accidental shifting, particularly in hydraulics.

FAILURE MODES ASSOCIATED WITH CERTAIN VALVE FUNCTIONS		
Valve Type	**Faults**	**Worst Case Faulted Outcome**
3/2 Normally Closed Spring Return		Air continues to be supplied
5/2 Spring Return		Motion continues at full force, does not reverse
5/2 Detented	Pilot or spool stick, Broken components (spring, seals, detent), Contamination	Motion will continue until end of stroke or reverse
5/3 Open Center, Closed Center, or Power Center		Motion continues at full force or reverses
Pilot Operated Check		Motion due to opposite end pressure or gravity
Flow Control		Speed control not effective, exhaust restricted.
Soft start		Speed control not effective, exhaust restricted.
Figure 5-1 *Same as a control-reliable valve except you must also design in monitor		

Category 3 and 4 valves are used to prevent these types of failures from causing the loss of the safety function. The redundancy (or structure) and the monitoring create fail-to-safe devices. If one valve element malfunctions, the second valve element can still perform the safety function. However, there are other factors that will affect when a dual safety valve has a fault such as increased stopping time. A change in the normal flow path of a faulted valve will affect the time it takes to exhaust the pressure or add pressure in a safe return function. This should be considered in any safe distance calculations.

 ROSS CONTROLS®

Residual Risk

Quite often, risk mitigation attempts can result in unacceptable levels of residual risk. Because of this, the risk assessment process is iterative. The first attempt may leave residual risk that is deemed unacceptable, and, therefore, requires at least a second attempt to reach an acceptable level of risk. The process must be repeated until an acceptable level of risk is achieved. The table below represents a list of common hazards and associated residual risks for each of the four safety functions. Other safety functions may be available that can be used to address the residual risks until an acceptable level of risk is achieved.

Cause of Hazard	Safety Function	Advantage	Residual Risk
Cylinder motion/point of operation	Safe Exhaust	Remove motive force from actuators Can supply a zone or cell	Reapplication of pressure, gravity
	Safe Cylinder Return	Single actuator control	Retract motion, loss of supply pressure
	Safe Control Stop	Single actuator control	Trapped pressure, leakage
Clamp (Pinch point)	Safe Reduced Pressure/Force	Reduce force from actuators Can supply a zone or cell	Pinch points remain at reduced force/pressure

Residual Risk	Safety Function	New Residual Risk
Reapplication of pressure	Soft-Start	Entire system may not be pressurized (i.e., downstream of 5/3 CC)
Reapplication of pressure	Flow Control	No back pressure for first stroke
Gravity	Load Holding	Leakage, slow motion, must be blocked for maintenance
Loss of supply pressure	Check Valve on supply	Leakage, slow motion, must be blocked for maintenance
Leakage	Periodic testing of safety circuit	Slow motion
Trapped pressure	Trapped pressure	Leakage, slow motion, must be blocked for maintenance

Based on the tasks and their associated risks, the available safety function options, and the potential residual risks, select the most appropriate safety function, accordingly.

There are four primary solutions for abating pneumatic actuator associated risks:

1. Block the air supply to the control valve and, therefore, to the actuators, with a 3/2 control reliable exhaust valve (Category-3 or -4). Use a safety-rated valve matched to the control category determined by your risk assessment. The advantage of this method is that one safety-rated exhaust valve can be used to remove the supply pressure from one or more directional control valves and actuators while helping maintain safety system control integrity. A safety-rated exhaust valve can supply a machine, cell, or zone.

   In some cases, removing the supply pressure alone can leave a load free to fall or continue moving due to gravity or momentum. In addition to safe exhaust you must consider the gravitational force and momentum operating on the mass of the load and apply a suitable solution to stop and hold the load in place. With the motive force removed, the suitable solution will be dependent upon the mass, the tooling, and the failure modes of the devices being used to maintain a safe state. Solutions may include the use of pilot-operated check valves to trap pressure beneficially, and/or safety catchers or rod locks to mechanically hold the actuator(s) without trapping pressure in the system.

2. Reverse the cylinder motion to a safe position by using a 5/2 control-reliable double valve. This will result in a safe state, provided a return stroke of the actuator does not pose any additional risk. In the case of heat sealing applications, this could be a very good solution. It would remove the heating element from the work piece (fuel) as well as reverse the cylinder direction away from the pinch point.

3. Stopping motion by trapping pressure in both ends of the cylinder can be accomplished with a safety-rated 4/3 or 5/3 closed-center valve. Only a safety-rated closed center valve can be used to reach higher level control reliable safety-rated systems without the addition of other components mentioned in solution 1.

4. Reduce the force or pressure to an acceptable level using a pressure select solution. This will supply higher pressure during normal operations but reduced pressure when safe operator access is required. This can be used to supply downstream valves. It is important to note that higher pressure may still be downstream depending on the type of actuator valve in the circuit. For example, a 5/3 closed-center valve will maintain the higher pressure until shifted allowing the lower pressure into the system.

While all machines are different the following flow chart might provide some overall guidance to the best first step option.
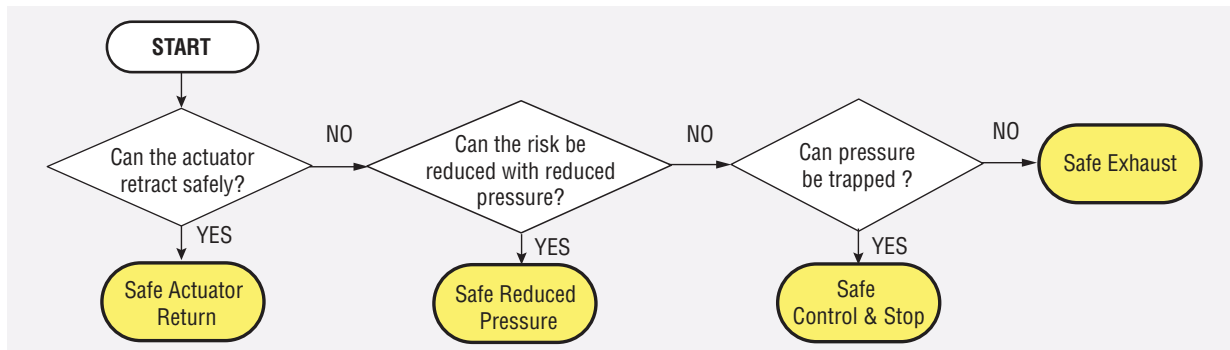
Fault Exclusion

Both ISO 13849-1 and ANSI B11.26 reference fault exclusions for safety functions, from ISO 13849-1

7.3 Fault Exclusion

It is not always possible to evaluate SRP/CS without assuming that certain faults can be excluded. For detailed information on fault exclusions, see ISO 13849-2.

Fault exclusion is a compromise between technical safety requirements and the theoretical possibility of occurrence of a fault.

Fault exclusion can be based on:

– *the technical improbability of occurrence of some faults,*
– *generally accepted technical experience, independent of the considered application, and*
– *technical requirements related to the application and the specific hazard.*

If faults are excluded, a detailed justification shall be given in the technical documentation.

Many of these are simply based on good engineering practices that are required in other standards. These ISO 13849-2 Annexes A - D provide information on fault exclusions for mechanical, pneumatic, hydraulic, and electrical systems respectively. Each of these sections looks at basic safety principles, well tried safety principles, and then faults and fault exclusions which are broken into valve function and specific failure modes. For the sake of brevity, the figures shown below are excerpts of the tables and not the complete tables.

One example of a fault exclusion is that you can exclude that a valve will burst when it is used within its specifications. The manufacturer will have undergone the design, and testing of the product. If the valve is third party certified, this testing would be part of the documentation package and the technical file required for CE marking. This is an entirely reasonable fault exclusion.

Hose breakage is a commonly discussed fault exclusion. ISO 13849-2 allows fault exclusion for hoses manufactured to ISO 4079-1 provided they are inspected and maintained. However, many end users require hard pipe or tubing because they have experienced hoses breaking on machinery. ISO 13849-2 does not allow fault exclusion of hydraulic hose breakage.

An additional hydraulic issue of note includes proper fastening. It specifically mentions manufacturers' application notes and proper torque. The notes will frequently mention a specific grade of bolt and torque requirement that is crucial to meet the pressure rating of the devices.

There are some fault exclusions that could lead to unsafe design decisions being made. Table B3 ISO 13849-2 for pneumatic directional control valves lists "Change in Switching Time" and "Non-Switching" (i.e., sticking) as items that can be excluded based on Table A2 in ISO 13849-2, Well Tried Safety Principles. While these principles are typically used by manufacturers there are many factors that would influence the actual outcomes.

Table C.3 in ISO 13849-2, for hydraulic directional control valves lists the same fault considerations as Table B3 for pneumatic directional control valves as well as leakage considerations, but has very specific details in the remarks. These specific details may be known to the valve manufacturer but would not be easily understood by the typical safety system designer. Creating the required detailed justification would require obtaining and documenting the level of detail listed in the remarks.

Tables B.4 and C.4 in ISO 13849-2, are specifically for shut off, check, quick exhaust, and shuttle valves and has a similar list of fault exclusions including leakage. The only purpose of a check valve is to trap pressure by shutting off completely with no leakage. The remarks mention that filtration must be provided and that the manufacturer's conditions must be met as well. Having clean, dry air will improve the life of all pneumatic systems but the reality is that there will be condensation and ingression of contaminants that will affect life and potentially induce failure modes such as leakage at the check valve seat.

 ROSS CONTROLS®

ANSI B11.26 also contains a list of common potential failure modes in sections 7.3.2 and 7.3.3.

7.3.2   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;*

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 supply or by the process.

Informative Note: *See ingress of contaminants in Annex H. Proper conditioning of the fluid power source can increase the mean time to dangerous failure.*

7.3.3   Hydraulic Failure Modes

Failure modes specific to hydraulic circuits shall be evaluated. The failure modes to be considered include but are no 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:
– 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 1: *See Ingress of contaminants in Annex H. Proper conditioning of the fluid power source can increase the mean time 10 dangerous failure.*

Annex H of ANSI B11.26 explains a bit further what is meant by ingression

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.

All valves will fail at some point in time. The concept of functional safety is that a control reliable safety system will fail safe and the failure will be detected before the next demand of the safety function. Because of this, fault exclusions should be used with great care, and the justification must be part of the technical documentation. A well designed safety system using well tried principles, a dual channel system, and a high level of diagnostics will not require fault exclusions and will lead to the safest solution.

8	PNEUMATIC SAFETY VALVE SELECTION

When choosing specific valves to address primary and residual risk, the choice will be dependent on a number of factors including flow rate, pipe sizes, voltage, soft start requirements, and the type of safety relay or safety controller being used to control the valve.

Fluid Power Risk Reduction Process

The chart below represents a general overview of the fluid power risk reduction process and highlights the parameters that should be considered. Detailed information on selecting safety functions and appropriate valve types are presented in the following chapters. A more detailed flowchart can be found in Annex A.

```
                    ┌──────────┐
                    │  START   │
                    └────┬─────┘
                         │
                ┌────────▼────────┐
                │     Select      │
                │  Lockout Valve  │
                └────────┬────────┘
                         │
   ┌─────────────────────▼─────────────────────────────┐
   │ Determine fluid power hazards based on your        │
   │ risk assessment.                                   │
   │ Must consider pressure, forces, and failure modes. │
   │ Select most appropriate risk reduction method.     │
   │ For assistance see Select Safety Function.         │
   └──┬─────────────┬──────────────┬─────────────┬──────┘
      │             │              │             │
 ┌────▼────┐  ┌─────▼─────┐  ┌─────▼─────┐  ┌────▼──────┐
 │  Safe   │  │   Safe    │  │   Safe    │  │   Safe    │
 │ Exhaust │  │ Actuator  │  │ Control   │  │ Reduced   │
 │         │  │  Return   │  │  & Stop   │  │ Pressure  │
 └────┬────┘  └─────┬─────┘  └─────┬─────┘  └────┬──────┘
      │             │              │             │
 ┌────▼─────────────▼──────────────▼─────────────▼──────┐
 │              Determine Residual risk.                │
 └──────────────────────┬───────────────────────────────┘
                        │
                ┌───────▼────────┐
                │   Does the     │          NO
                │ solution reduce├────────────────┐
                │  the risk to   │                │
                │ acceptable     │                │
                │    level?      │                │
                └───────┬────────┘                │
                     YES│                         │
            ┌───────────▼─────────────┐           │
            │ Wiring, Programming &    │           │
            │ Validation              │           │
            └───────────┬─────────────┘           │
                        │                         │
                ┌───────▼────────┐                │
                │   COMPLETE     │                │
                └────────────────┘                │
```

© 2021, All Rights Reserved.
ROSS CONTROLS®

Lockout/Energy Isolation

The first step is to choose the lockout valve that is needed. Each machine is required to have an energy isolation valve, and, in fact, there may also be other lockout valves for individual machines or zones of a line.

Lockout/Energy Isolation Valve Selection Flow Chart with ROSS Valve Series
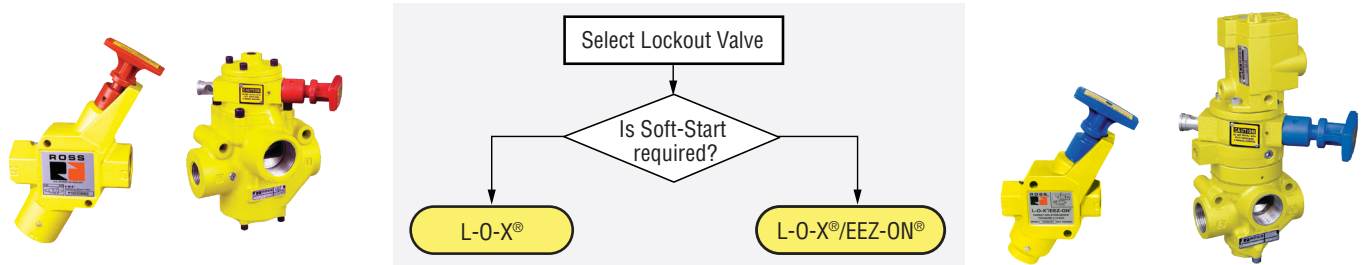
The concerns when selecting a lockout valve would be port size, flow rate to supply, flow rate to exhaust, and if soft start is needed. When soft-start is used on the lockout valve, please note that the soft-start function will only work up to the point where flow is blocked by some other device such as a directional valve that is closed at start-up, for example a safe exhaust valve or a 5/3 closed or open center valve. More information on soft-start selection can be found in Annex C.

Exhaust flow rate can be an important factor when looking at uptime if lockout occurs with any regularity. A ball valve with a bleed port, which can take up to 25 times longer to exhaust, may meet OSHA's broad requirements but does not meet ANSI machinery requirements. In fact ANSI B11.0 & B155.1 requirements for lockout include a number of best practices to address shortfalls with devices used for energy isolation (LOTO).

LOTO Requirements and Best Practices

- Valve not used for any other function
- Located outside of the hazardous area
- Valve should be well marked
- Valve should be differentiated by its appearance
- Easily identified and operated

- Full diameter exhaust (rapid release of stored energy)

Locked ON   Locked in between   Locked ON/OFF?
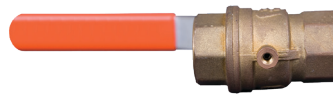
- Tamper resistant
- Should only be able to be locked in the off position
- "Positive action" which would indicate only two positions (ON and OFF)

- A method for the employee to verify that the energy has dissipated after initiating lock out process.

Pop-up Pressure Indicator

The LOTO/Energy Isolation device is not an E-Stop device.

This chart shows the time difference to exhaust 8 cubic feet (226 liters) of compressed air using a ROSS L-O-X® valve with full size exhaust versus a ball valve with a bleed port. The chart shows that there is an additional 10 minutes of waiting for the pressure to be exhausted when using the ball valve. This results in increased downtime. Additionally, there is the risk of someone entering the machine before it is fully de-energized.

Exhausting 8 Cubic Feet at 100 psi

Pressure (PSIG) vs Time (Minutes)

— Ball Valve   — LOX® Valve
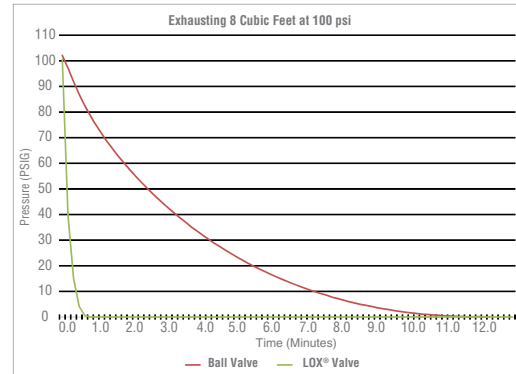
Pneumatic Energy Isolation Example 1 – With standard Lockout valve without Soft-Start
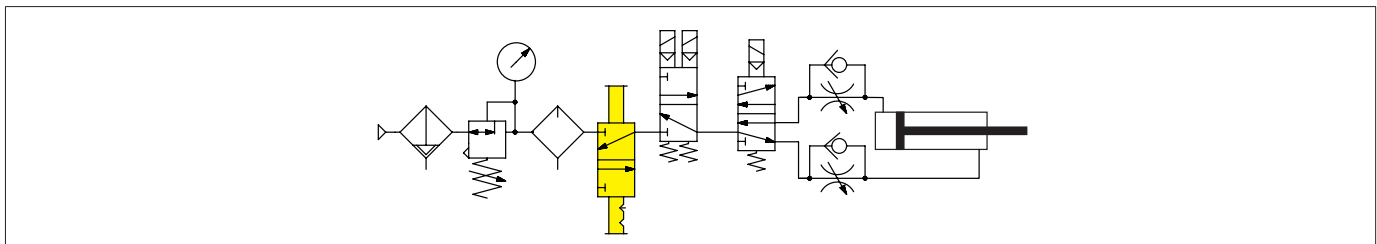
Pneumatic Energy Isolation Example 2 – With standard Lockout valve with Soft-Start
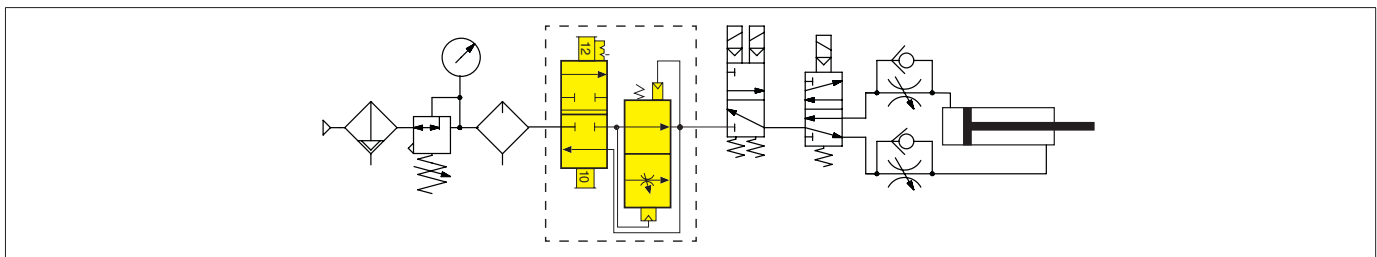
Lockout valves are often used in air entry systems that have drip legs, filters, regulators, lubricators, and safe exhaust valves as shown below. Sometimes users may require a soft-start function which could be included in the lockout valve, safe exhaust valve, or added to the air entry system as an additional component. Below are images of typical safe air entry systems with soft-start.

Where the lockout valve is placed in the overall system is application dependent. The example on the left shows the lockout prior to the filter and regulator. In general, filters, regulators, and lubricators are not designed for backflow. If these devices can flow backwards, debris and oil can be blown back upstream. In the example below, on the left, it is assumed that the electrically controlled exhaust valve would exhaust the main volume of system air, and the lockout valve would be used only to remove air from the filter and regulator. The example on the right side shows the lockout valve after the filter and regulator and prior to a distribution block and the electrical exhaust valve. This may be preferred when, due to machine design and/or procedures, the lockout valve may be used while the electrically controlled exhaust valve is still energized. In this case a large volume of air is prevented from back flowing through the filter regulator and back into the lockout valve. There must be a way to lockout and service the filter and regulator which is not shown in this example.

 ROSS CONTROLS®
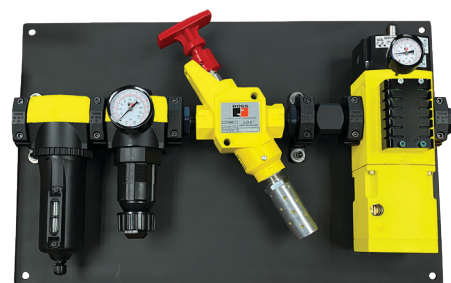
Safe Exhaust

Safe Exhaust valves are used to block supply pressure and exhaust downstream pressure from an entire machine. Safe exhaust valves can also be used to isolate individual actuators and/or zones depending on requirements of the risk assessment. Safe exhaust valves are available for use in systems that require up to Performance Level e with a variety of voltages and sizes to meet specific customer needs. The safe exhaust valve selection flow chart below is meant to help users select the most appropriate safe exhaust valve.

Safe Exhaust Valve Selection Flow Chart with ROSS Valve Series (Part 1)
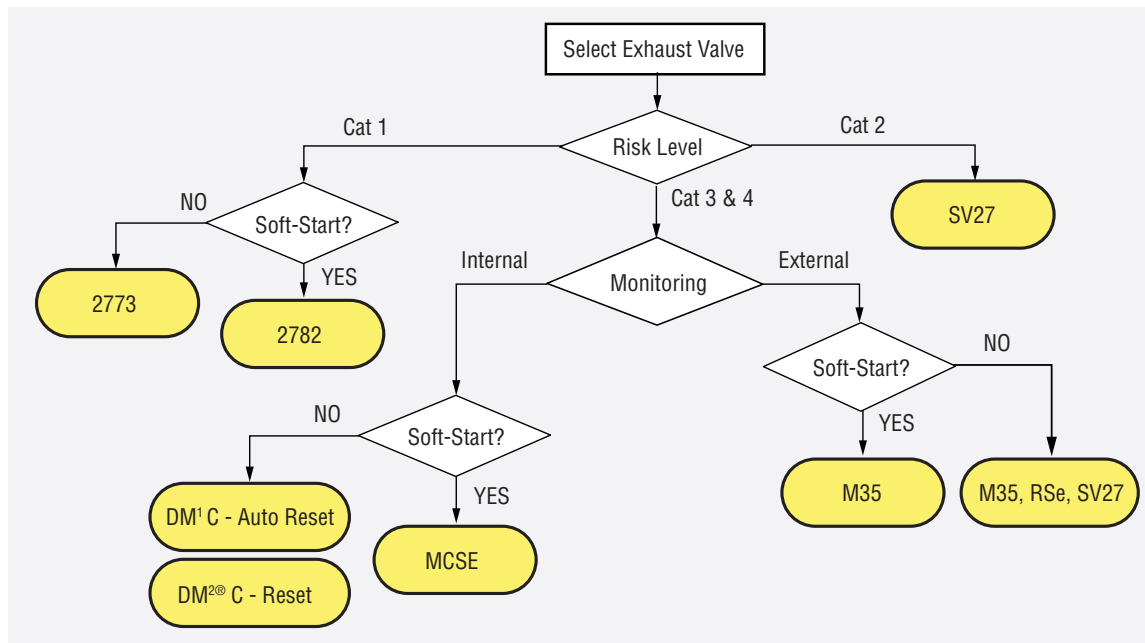
It is important to match the safety valve type with the type of safety controller being used. If the controller is a simple, hard-wired safety relay, internally-monitored valves can be integrated quite easily. If the controller is programmable, an externally monitored valve might be the best choice. Internal monitoring simply means the valve monitors its function itself, fails to the safe mode, and prevents further operation as long as the fault exists. External monitoring means there are sensors that detect pressure and/or valve position sensors that provide feedback to the safety controller to detect a discordance, indicate a fault, and stop the machine until the fault is cleared. More detailed information on internal versus external can be found in Annex B.

The next potential decision is whether or not a soft-start function is needed. A soft-start type valve will slowly build up pressure but only to the next part of the circuit that prevents flow.

Once a valve type is defined, the residual risk involved with exhausting air pressure must be considered. Shutting off and removing air pressure can result in motion due to gravitational forces which could create an additional hazard. Load holding valves may be needed to prevent motion (see the Safe Load Holding section).

Safe Exhaust Valve Selection Flow Chart (Part 2)

Note: This chart can be used if exhausting air causes additional motion.
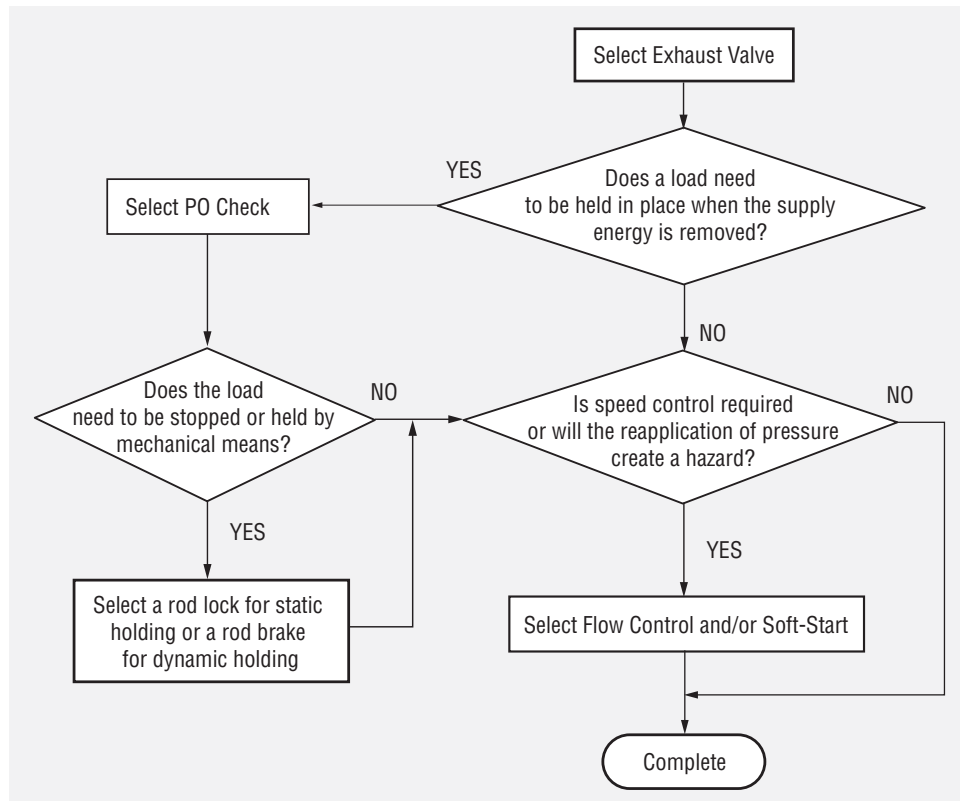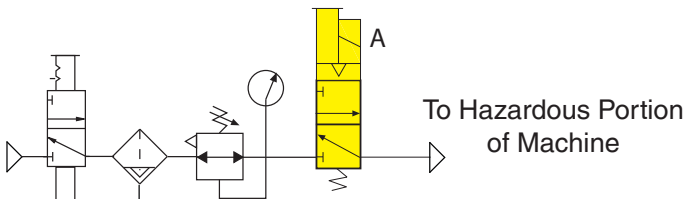
Blocking valves, PO check valves, and mechanical devices can be used to eliminate motion caused by exhausting the air in the system. Pilot operated check valves are often used in conjunction with mechanical devices. Mechanical devices could be rod locks, rod brakes, or catchers that work on the actuator or connecting rod, or they could be ratchet type devices or cylinders acting as pins to hold the platen in place. It is important to understand that these devices must be rated to the safety level required. If the devices are air-operated, the safe exhaust valve should control the air supply to the rod locks or catchers to meet the control integrity requirements of the system.

The residual risk of re-application of pressure may require the addition of soft-start valves on each cylinder to prevent "slamming" action upon the re-energization process.

     ROSS CONTROLS®
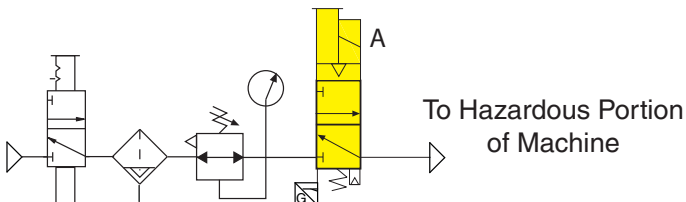
Pneumatic Safe Exhaust Example 1 – Category 1

3/2 single channel solenoid-operated spring return control valve with no feedback. A Category 1 control system may not require a safe exhaust valve for general operation but may be needed for emergency stop or removing the air supply to vacuum systems or other air driven devices.

|	
Safety Function	Pneumatic energy is removed from downstream when de-energized
Residual Risk	Motion due to gravity or other residual energy (i.e., spring force, trapped pressure) Reapplication of energy may create rapid motion
Faults to Consider	A single channel circuit can fail dangerously
Diagnostics	None
ANSI B11.26 Reference	11.3.3.2.1
ISO 13849-1 Reference	Safety related Stop function initiated by a safeguard Start/restart function Prevention of unexpected startup Isolation and Energy dissipation Emergency Stop function
VDMA 24584 Reference	6.1 Safe Torque OFF (STO) 6.2 Safe Stop 1 (SS1) 6.17 Safe De-energization (SDE)
Solution Valve Series	A) Various

Pneumatic Safe Exhaust Example 2 – Category 2

3/2 single channel solenoid-operated spring return control valve with feedback - must be monitored by the safety controller**.**

Safety Function	Pneumatic energy is removed from downstream when de-energized
Residual Risk	Motion due to gravity or other residual energy (i.e., spring force, trapped pressure) Reapplication of energy may create rapid motion
Faults to Consider	A single channel circuit can fail dangerously, but can be detected A fault of the feedback can lead to the loss of the safety function between checks
Diagnostics	Feedback sensing
ANSI B11.26 Reference	11.3.3.2.2.1
ISO 13849-1 Reference	Safety related Stop function initiated by a safeguard Start/restart function Prevention of unexpected startup Isolation and Energy dissipation Emergency Stop function
VDMA 24584 Reference	6.1 Safe Torque OFF (STO) 6.2 Safe Stop 1 (SS1) 6.17 Safe De-energization (SDE)
Solution Valve Series	A) SV 3/2

Pneumatic Safe Exhaust Example 3 – Category 3 or 4

Two 3/2 single channel solenoid-operated spring return control valves with feedback - must be monitored by the safety controller.

Safety Function	Pneumatic energy is removed from downstream when de-energized
Residual Risk	Motion due to gravity or other residual energy (i.e., spring force, trapped pressure) Reapplication of energy may create rapid motion
Faults to Consider	Increased exhaust time if second valve sticks in energized position For Category 3 some dangerous faults may not be detected
Diagnostics	Feedback sensing
ANSI B11.26 Reference	11.3.3.2.4, 11.3.3.2.5.1
ISO 13849-1 Reference	Safety related Stop function initiated by a safeguard Start/restart function Prevention of unexpected startup Isolation and Energy dissipation Emergency Stop function
VDMA 24584 Reference	6.1 Safe Torque OFF (STO) 6.2 Safe Stop 1 (SS1) 6.17 Safe De-energization (SDE)
Solution Valve Series	A) SV 3/2 (2)

To Hazardous Portion of Machine

Pneumatic Safe Exhaust Example 4 – Category 4

3/2 dual channel solenoid-operated spring return control valve – monitoring may be internal or external depending on valve series selected.

Safety Function	Pneumatic energy is removed from downstream when de-energized
Residual Risk	Motion due to gravity or other residual energy (i.e., spring force, trapped pressure) Reapplication of energy may create rapid motion
Faults to Consider	None
Diagnostics	Feedback sensing or internally monitored
ANSI B11.26 Reference	11.3.3.2.5.2, 11.3.3.2.5.3
ISO 13849-1 Reference	Safety related Stop function initiated by a safeguard Start/restart function Prevention of unexpected startup Isolation and Energy dissipation Emergency Stop function
VDMA 24584 Reference	6.1 Safe Torque OFF (STO) 6.2 Safe Stop 1 (SS1) 6.17 Safe De-energization (SDE)
Solution Valve Series	A) M35, RSe, MCSE, DM2®, DM1

with Soft-Start

To Hazardous Portion of Machine

ROSS CONTROLS®
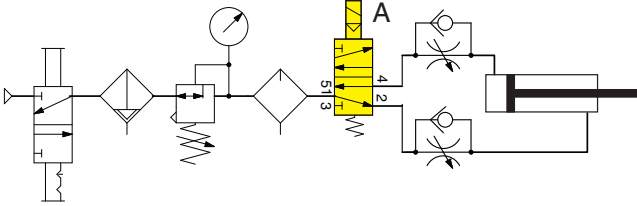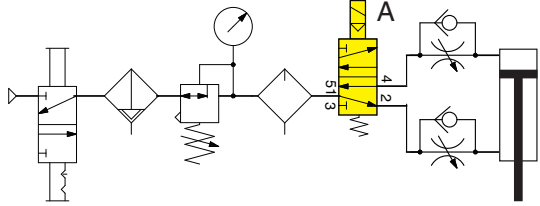
Safe Return

Safe Return valves are used to return a cylinder or other actuator to its home position when the valve is switched off or when there is a fault within the valve. If gravity is a hazard with loss of supply pressure, a check valve may need to be added to the supply of the safe return valve. If a check valve is added to the supply line, trapped pressure can occur during lockout.

Safe Return Valve Selection Flow Chart with ROSS Valve Series
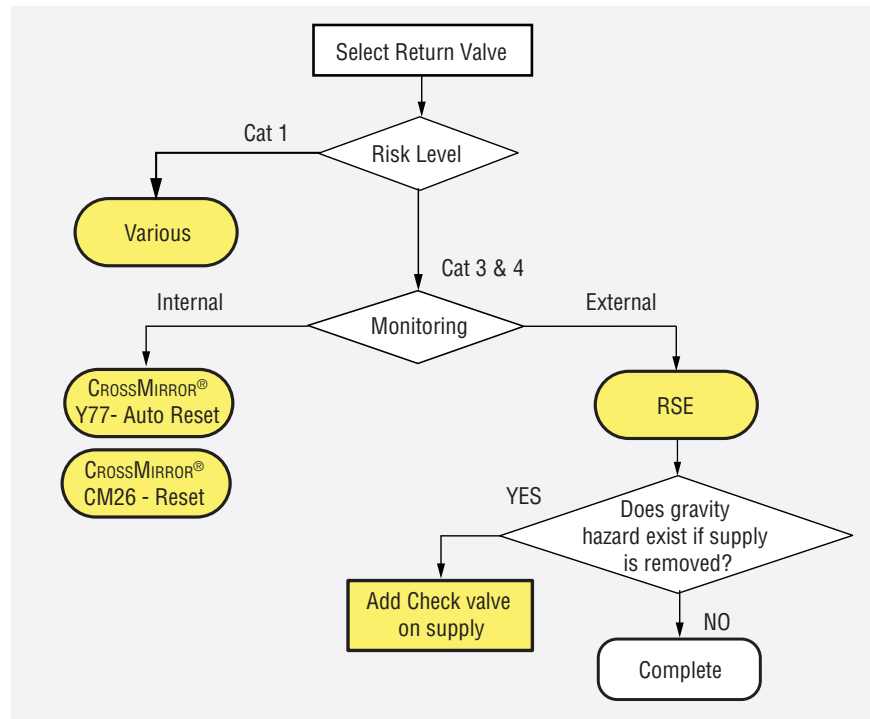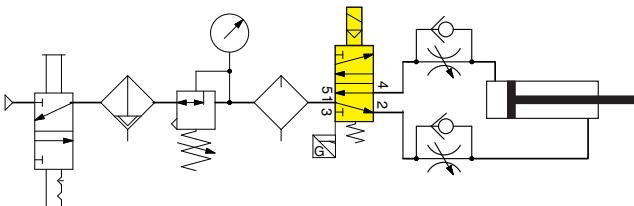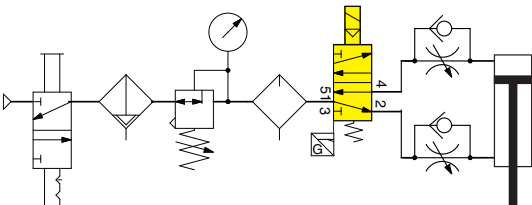
Pneumatic Safe Return Example 1 – Category 1

5/2 single-solenoid spring return control valve with no feedback.

Safety Function	The cylinder returns to its home position when de-energized
Residual Risk	Return motion creating a hazard If using inlet check – trapped pressure during lockout (LOTO)
Faults to Consider	A single channel circuit can fail dangerously Loss of supply pressure
Diagnostics	None
ANSI B11.26 Reference	11.3.3.3.1.1
ISO 13849-1 Reference	Safe direction
VDMA 24584 Reference	6.15 Safe Direction (SDI)
Solution Valve Series	Various

 ROSS CONTROLS®

Pneumatic Safe Return Example 2 – Category 2

5/2 single channel solenoid-operated spring return control valve with feedback - must be monitored by the safety controller.

Safety Function	The cylinder returns to its home position when de-energized
Residual Risk	Return motion creating a hazard If using inlet check – trapped pressure during lockout (LOTO)
Faults to Consider	A single channel circuit can fail dangerously, but can be detected Loss of supply pressure
Diagnostics	Feedback sensing
ANSI B11.26 Reference	11.3.3.3.2.1
ISO 13849-1 Reference	Safe direction
VDMA 24584 Reference	6.15 Safe Direction (SDI)
Solution Valve Series	NA

Pneumatic Safe Return Example 3 – Category 4

5/2 dual channel solenoid-operated spring return control valve with feedback - must be monitored by the safety controller. Monitoring may be internal or external depending on valve series selected.

Safety Function	The cylinder returns to its home position when de-energized
Residual Risk	Return motion creating a hazard If using inlet check – trapped pressure during lockout (LOTO)
Faults to Consider	Loss of supply pressure
Diagnostics	Feedback sensing
ANSI B11.26 Reference	11.3.3.3.3.1
ISO 13849-1 Reference	Safe direction
VDMA 24584 Reference	6.15 Safe Direction (SDI)
Solution Valve Series	A) RSe, Y7776, CM26

 ROSS CONTROLS®
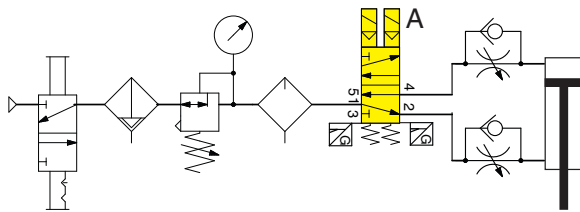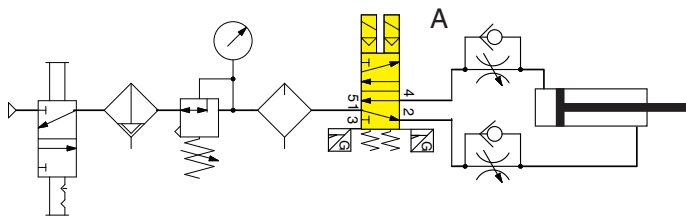
Safe Control and Stop

There is only one available valve choice that can perform perform the combined functions of safe control and stop at Cat 2, 3, or 4 without the use of multiple valves. Otherwise, it would require a safe exhaust valve, an open-center control valve, and multiple monitorable PO checks to achieve this function. Sometimes, a mechanical holding device may be required as well.

Safe Control and Stop Selection Flow Chart with ROSS Valve Series
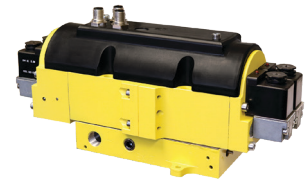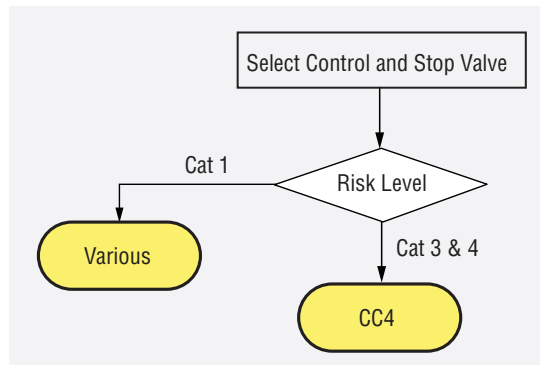
Pneumatic Safe Control and Stop Example 1 – Category 1

4/3 (or 5/3) single channel double solenoid-operated closed-center valve.

Safety Function	The cylinder stops when de-energized
Residual Risk	Trapped pressure during lockout (LOTO)
Faults to Consider	Failure of control valve could allow motion Motion due to leakage (i.e., seals, hose, fittings)
Diagnostics	None
ANSI B11.26 Reference	11.3.3.3.1.4
ISO 13849-1 Reference	NA
VDMA 24584 Reference	6.3 Safe Stop 2 (SS2) 6.4 Safe Stopping & Closing (SSC) 6.5 Safe Operating Stop (SOS)
Solution Valve Series	A) Various
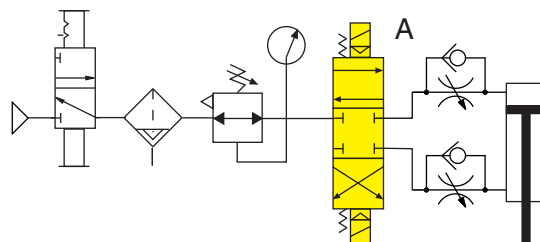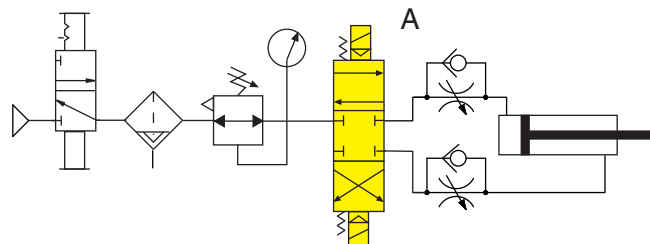
Pneumatic Safe Control and Stop Example 2 – Category 2

4/3 (or 5/3) single channel double solenoid-operated closed-center valve with feedback - must be monitored by the safety controller.

| Safety Function	The cylinder stops when de-energized
Residual Risk	Trapped pressure during lockout (LOTO)
Faults to Consider	Failure of control valve could allow motion, but can be detected Motion due to leakage (i.e., seals, hose, fittings)
Diagnostics	Feedback sensing
ANSI B11.26 Reference	NA
ISO 13849-1 Reference	NA
VDMA 24584 Reference	6.3 Safe Stop 2 (SS2) 6.4 Safe Stopping & Closing (SSC) 6.5 Safe Operating Stop (SOS)
Solution Valve Series	NA

                    ROSS CONTROLS®

Pneumatic Safe Control and Stop Example 3 – Category 4

4/3 dual channel double solenoid-operated closed-center valve with feedback - must be monitored by the safety controller.

| Safety Function	The cylinder stops when de-energized
Residual Risk	Trapped pressure during lockout (LOTO)
Faults to Consider	Motion due to leakage (i.e., seals, hose, fittings)
Diagnostics	Feedback sensing
ANSI B11.26 Reference	11.3.3.3.4.4.1
ISO 13849-1 Reference	NA
VDMA 24584 Reference	6.3 Safe Stop 2 (SS2) 6.4 Safe Stopping & Closing (SSC) 6.5 Safe Operating Stop (SOS)
Solution Valve Series	A) CC4

Safe Load Holding

The technique of safe load holding is quite complex and often misapplied. Category 1 directional valves with closed center positions are used commonly for holding loads. Pilot-operated check valves are also used for load holding in conjunction with directional valves. PO checks are typically not monitored and, also, are only good for applications up to PL c. These devices are also considered to be single-channel devices. Monitoring can bring these devices up to Category 2.

PO check valves have been a time-tested solution, and are typically directly piloted by the directional control valve. If the control valve were to malfunction, then the PO check valves would not operate correctly. A way to remediate control valve failure is to use an upstream exhaust valve that will remove pressure from the directional control valve – make sure that the directional valve is either a 4/2 or 5/2 single solenoid type or a 4/3 or 5/3 double solenoid open-center type. Even if the control valve were to malfunction, there would be no air pressure to create unwanted motion, and the pilot signals to the PO check valve(s) would be removed allowing them to function. The Category 1 and 2 examples below do not show an exhaust valve in the circuit because single channel failures are an acceptable risk at lower performance levels. The exhaust valve has been added to the Category 3 example.

One of the most overlooked aspects of load holding is how to manage trapped pressure. If trapped pressure is not relieved prior to maintenance, an adequate mechanical blocking/holding system must be in place to prevent any motion due to trapped pressure and/or gravity. Not including a way to manage trapped pressure in the design phase forces maintenance workers to take unnecessary risks, such as cracking open fittings in order to relieve trapped pressure. The solution is to design in an automatically- or remotely-operated method to safely relieve the pressure and allow the actuators to safely move to the safest possible position. Depending on the application, this could be as simple as adding a manually-operated valve to allow the trapped pressure to be relieved slowly, or it could be a system that automatically bleeds trapped pressure when the lockout valve is shut off.

Safe Load Holding Valve Selection Flow Chart with ROSS Valve Series

ROSS CONTROLS®
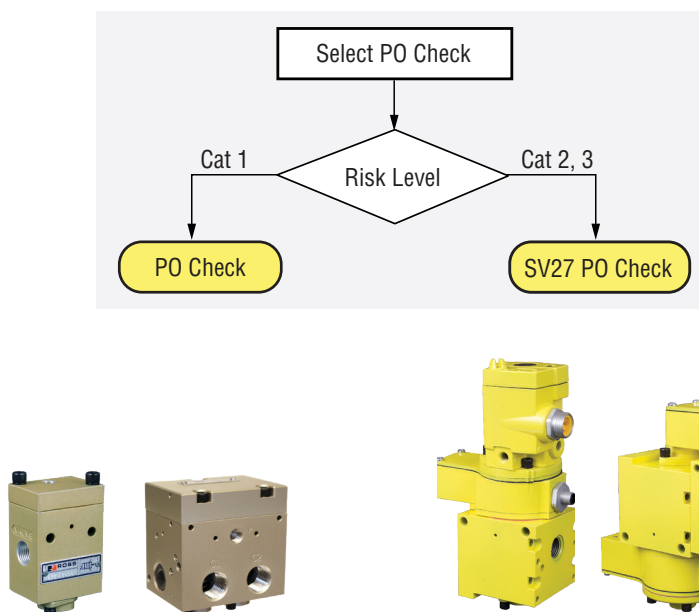
Pneumatic Safe Load Holding Example 1 – Category 1

Single channel pilot-operated check valve with no feedback.

Safety Function	The cylinder stops when de-energized
Residual Risk	Trapped pressure during lockout (LOTO)
Faults to Consider	Failure of control valve could allow motion Motion due to leakage (i.e., seals, hose, fittings)
Diagnostics	None
ANSI B11.26 Reference	11.3.3.4.1.1
ISO 13849-1 Reference	NA
VDMA 24584 Reference	6.3 Safe Stop 2 (SS2) 6.4 Safe Stopping & Closing (SSC) 6.5 Safe Operating Stop (SOS)
Solution Valve Series	A) PO check Cat 1
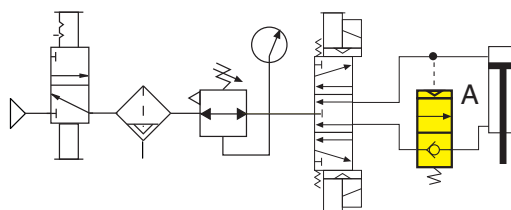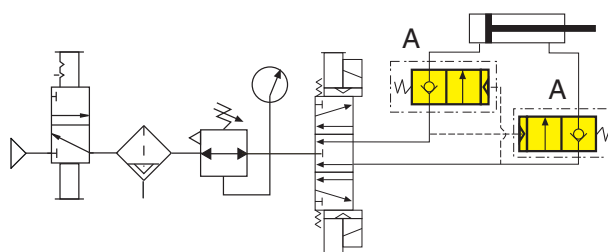
Note: Horizontal applications may need PO check valves on both the rod and cap ends of the cylinder to prevent movement.

Pneumatic Safe Load Holding Example 2 – Category 2

Single channel pilot-operated check valve with feedback - must be monitored by the safety controller.

Safety Function	The cylinder stops when de-energized
Residual Risk	Trapped pressure during lockout (LOTO)
Faults to Consider	Failure of control valve could allow motion, but can be detected Motion due to leakage (i.e., seals, hose, fittings)
Diagnostics	Feedback sensing
ANSI B11.26 Reference	NA
ISO 13849-1 Reference	NA
VDMA 24584 Reference	6.3 Safe Stop 2 (SS2) 6.4 Safe Stopping & Closing (SSC) 6.5 Safe Operating Stop (SOS)
Solution Valve Series	A) SV27 PO check
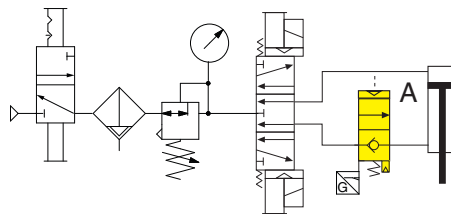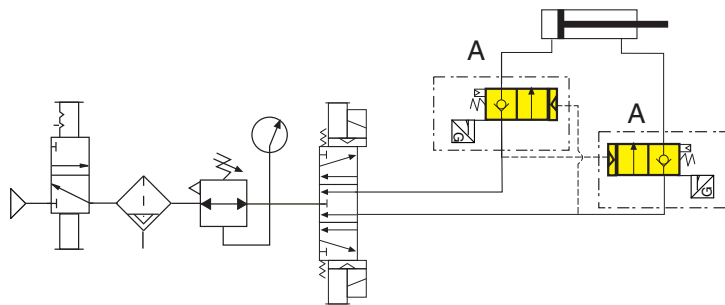
Note: Horizontal applications may need monitored PO check valves on both the rod and cap ends of the cylinder to prevent movement.

     ROSS CONTROLS®

Pneumatic Safe Load Holding Example 3 – Category 3

Redundant pilot-operated check valves with feedback - must be monitored by the safety controller. Addition of the safe exhaust valve ensures a failure of the control valve does not override the PO check function. Open-center directional valves are recommended because closed-center valves can hinder operation of the pilot-operated check(s).

Safety Function	The cylinder stops when de-energized
Residual Risk	Trapped pressure during lockout (LOTO)
Faults to Consider	Motion due to leakage (i.e., seals, hose, fittings)
Diagnostics	Feedback sensing
ANSI B11.26 Reference	11.3.3.4.3.1
ISO 13849-1 Reference	NA
VDMA 24584 Reference	6.3 Safe Stop 2 (SS2) 6.4 Safe Stopping & Closing (SSC) 6.5 Safe Operating Stop (SOS)
Solution Valve Series	A) M35, RSe, MCSE, DM2®, DM1 B) SV27 PO check
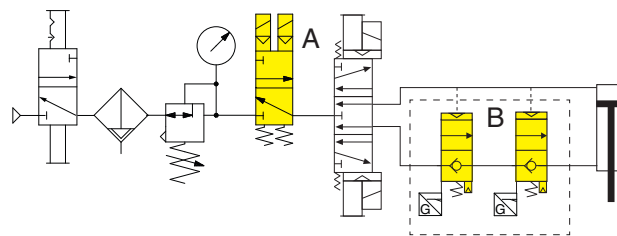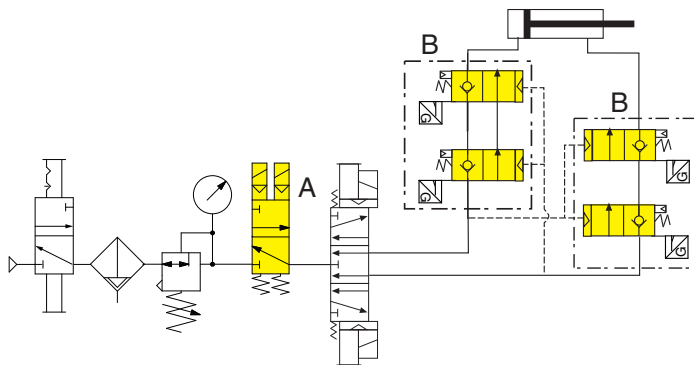
Note: Horizontal applications may need redundant monitored PO check valves on both the rod and cap ends of the cylinder to prevent movement.

Safe Pressure Select

Safe Pressure Select is used when a pneumatic actuator needs to be moved to accomplish a job task but "normal line pressure" would cause a potentially hazardous injury to a person that is interacting with the actuator at that time. One example would be a load station that uses pneumatic clamps to hold a part in place for a welding, crimping, or machining operation. A presence sensing device could be used to detect the presence of the operator and signal the valve to switch to a safe limited pressure (force below 150N).

High and low pressure calculations can be done using the ROSS pressure force calculator. The pressure force calculator can be found at www.rosscontrols.com, see Support and Downloads, Technical Tools page.

Safe Pressure Select Valve Selection Flow Chart with ROSS Valve Series
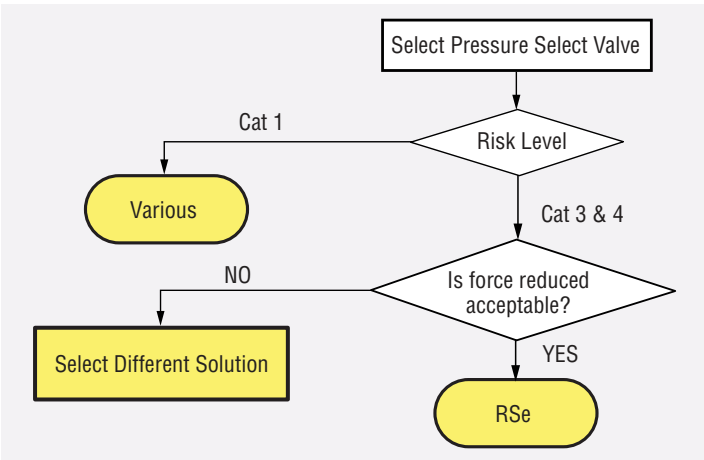
Safe Pressure Select Example 1 – Category 1

5/2 single solenoid-operated spring return control valve with no feedback.

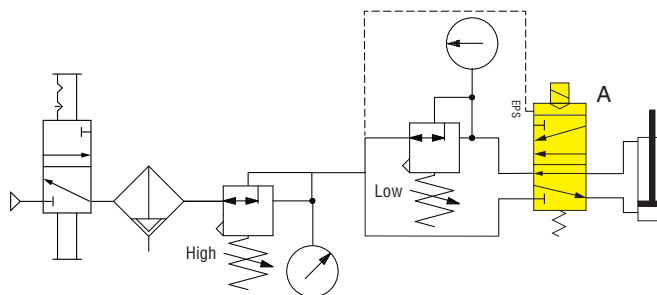| Safety Function	Reduced pressure and force at the point of operation
Residual Risk	NA
Faults to Consider	Loss of supply pressure Failure of pressure select valve could supply incorrect pressure Failure of control valve could cause cylinder motion to be in the wrong direction
Diagnostics	None
ANSI B11.26 Reference	NA
ISO 13849-1 Reference	Safety-related parameter such as speed, temperature or pressure
VDMA 24584 Reference	6.13 Safe Limited Pressure (SLP)
Solution Valve Series	Various

Note: The use of Safe Pressure Select solutions requires the force to be reduced to below the safe limited force of 150N. Calculations must be done to determine if Safe Pressure Select is a safe option.

 ROSS CONTROLS®

Safe Pressure Select Example 2 – Category 2

5/2 single channel solenoid-operated spring return control valve with feedback - must be monitored by the safety control system.

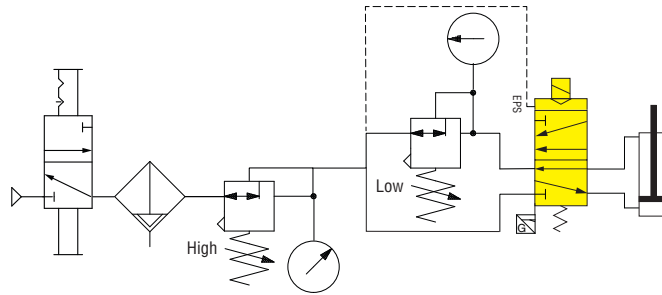| Safety Function	Reduced pressure and force at the point of operation
Residual Risk	NA
Faults to Consider	Loss of supply pressure Failure of pressure select valve could supply incorrect pressure, but can be detected Failure of control valve could cause cylinder motion to be in the wrong direction
Diagnostics	Feedback sensing
ANSI B11.26 Reference	NA
ISO 13849-1 Reference	Safety-related parameter such as speed, temperature or pressure
VDMA 24584 Reference	6.13 Safe Limited Pressure (SLP)
Solution Valve Series	NA

Note: The use of Safe Pressure Select solutions requires the force to be reduced to below the safe limited force of 150N. Calculations must be done to determine if Safe Pressure Select is a safe option.

Safe Pressure Select Example 3 – Category 4

5/2 dual channel solenoid-operated spring return control valve with feedback - must be monitored by the safety controller.

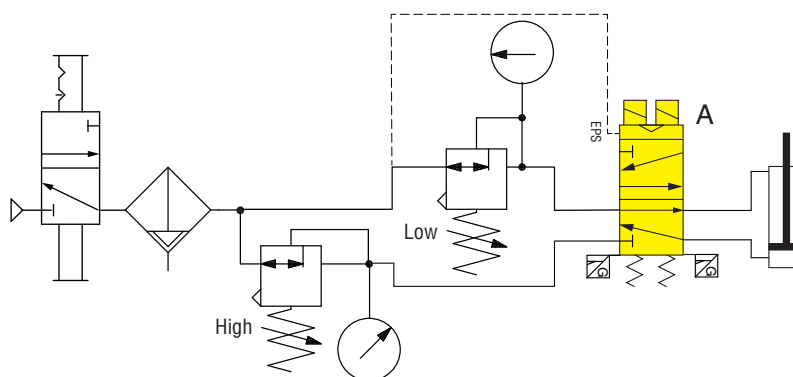| Safety Function	Reduced pressure and force at the point of operation
Residual Risk	NA
Faults to Consider	Loss of supply pressure Failure of control valve could cause cylinder motion to be in the wrong direction
Diagnostics	Feedback sensing
ANSI B11.26 Reference	NA
ISO 13849-1 Reference	Safety-related parameter such as speed, temperature or pressure
VDMA 24584 Reference	6.13 Safe Limited Pressure (SLP)
Solution Valve Series	A) RSe

Note: The use of Safe Pressure Select solutions requires the force to be reduced to below the safe limited force of 150N. Calculations must be done to determine if Safe Pressure Select is a safe option.

ROSS CONTROLS®

Safe Return Dual Pressure

Safe Return Dual Pressure valves are used to return a cylinder or other actuator to its home position when the valve is switched off or when there is a fault within the valve. Typically, two different pressures are supplied to the Safe Return Dual Pressure valve. The Safe Return Dual Pressure valve will cause the cylinder to extend at one pressure and return at the other pressure. If gravity is a hazard with loss of supply a check valve may need to be added to the supply of the Safe Return Dual Pressure valve. If a check valve is added to the supply line, trapped pressure can occur during lockout. High and low pressure calculations can be done using the ROSS pressure force calculator.

Safe Return Dual Pressure Valve Selection Flow Chart with ROSS Valve Series
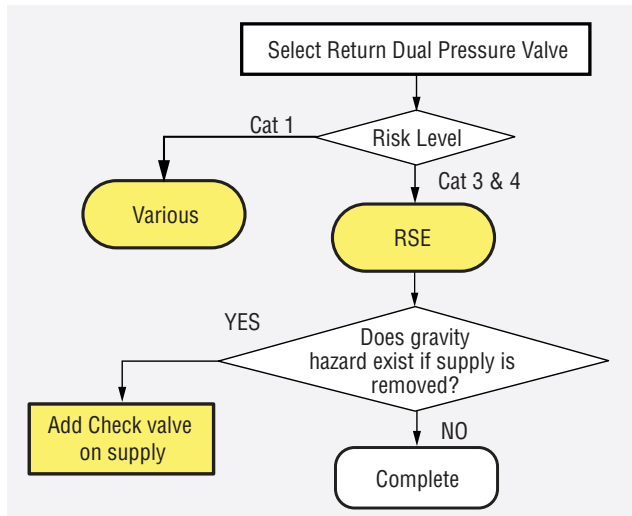
Safe Return Dual Pressure Example 1 – Category 1

5/2 single solenoid-operated spring return control valve with no feedback.

| Safety Function	The cylinder returns to its home position when de-energized
Residual Risk	Return motion creating a hazard If using inlet check – trapped pressure during lockout (LOTO) Return at high force if returning at high pressure (depending on which port low pressure is supplied on)
Faults to Consider	A single channel circuit can fail dangerously Loss of supply pressure
Diagnostics	None
ANSI B11.26 Reference	11.3.3.3.1.1
ISO 13849-1 Reference	Safe direction Safety-related parameter such as speed, temperature or pressure
VDMA 24584 Reference	6.15 Safe Direction (SDI)
Solution Valve Series	A) Various

Note: The use of Safe Return Dual Pressure solutions requires the force to be reduced to below the safe limited force of 150N. Calculations must be done to determine if Safe Dual Pressure is a safe option.

Safe Return Dual Pressure Example 2 – Category 2

5/2 single solenoid-operated spring return control valve with feedback - must be monitored by the safety controller.

Safety Function	The cylinder returns to its home position when de-energized
Residual Risk	Return motion creating a hazard If using inlet check – trapped pressure during lockout (LOTO) Return at high force if returning at high pressure (depending on which port low pressure is supplied on)
Faults to Consider	A single channel circuit can fail dangerously, but can be detected Loss of supply pressure
Diagnostics	Sensing feedback
ANSI B11.26 Reference	11.3.3.3.2.1
ISO 13849-1 Reference	Safe direction Safety-related parameter such as speed, temperature or pressure
VDMA 24584 Reference	6.15 Safe Direction (SDI)
Solution Valve Series	NA

Note: The use of Safe Return Dual Pressure solutions requires the force to be reduced to below the safe limited force of 150N. Calculations must be done to determine if Safe Dual Pressure is a safe option.

 ROSS CONTROLS®

Dual Safe Return Dual Pressure Example 3 – Category 4

5/2 dual channel solenoid-oprated spring return control valve with feedback - must be monitored by the safety controller.

Safety Function	The cylinder returns to its home position when de-energized
Residual Risk	Return motion creating a hazard If using inlet check – trapped pressure during lockout (LOTO) Return at high force if returning at high pressure (depending on which port low pressure is supplied on)
Faults to Consider	A single channel circuit can fail dangerously Loss of supply pressure
Diagnostics	Feedback sensing
ANSI B11.26 Reference	11.3.3.3.3.1
ISO 13849-1 Reference	Safe direction Safety-related parameter such as speed, temperature or pressure
VDMA 24584 Reference	6.15 Safe Direction (SDI)
Solution Valve Series	A) RSe

Note: The use of Safe Return Dual Pressure solutions requires the force to be reduced to below the safe limited force of 150N. Calculations must be done to determine if Safe Dual Pressure is a safe option.

9	HYDRAULIC SAFETY VALVE SELECTION

When choosing specific valves to address primary and residual risk, the choice will be dependent on a number of factors including desired safety function, flow rate, pipe size, voltage, and pressure range.

The flowchart below guides users through the selection process to determine the type of valve that is needed for a machine or hazard. Available hydraulic valve types are Safe Block and Bleed as well as Safe Block and Stop.
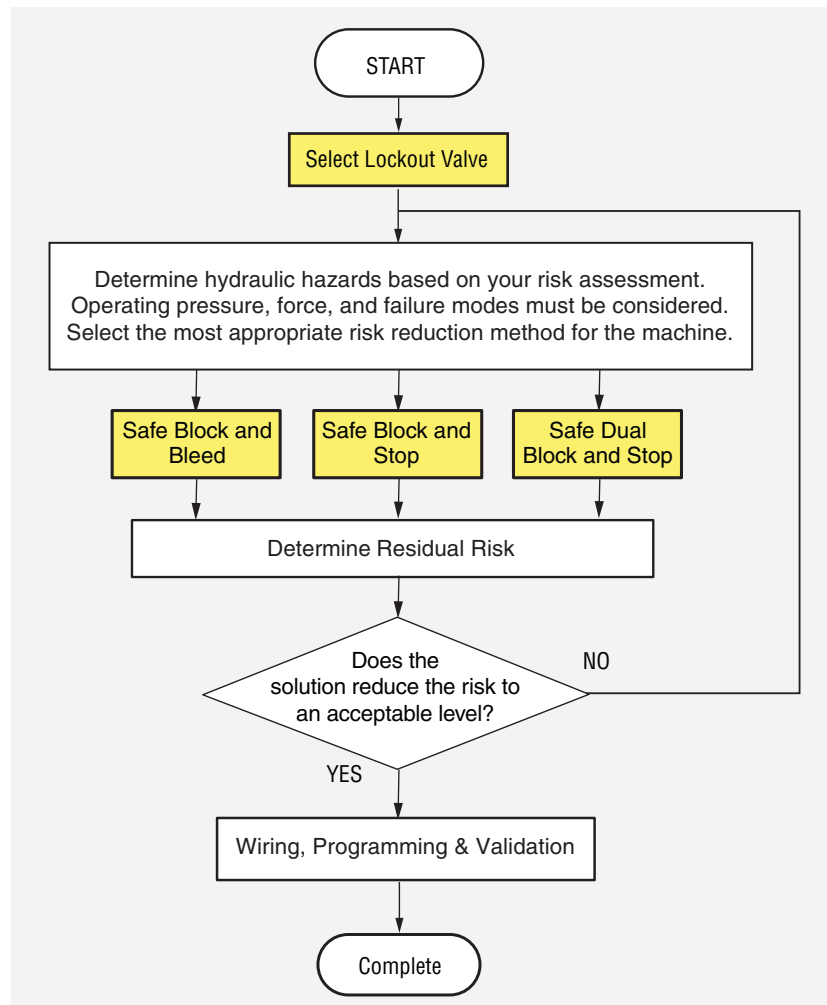
Lockout/Energy Isolation

The first step is to choose a lockout valve for energy isolation. All hydraulically operated machines are required to have a method for locking out the hydraulic energy. A single lockout valve may be used to isolate the entire machine or multiple valves may be needed for multiple zone isolation.

One of the common pitfalls of hydraulic lockout is that is that quite often the hydraulic system is considered to be safe by just isolating the electrical supply to the pump. However, there may be accumulators that store energy and/or other valves that block flow in the system causing trapped pressure. Locking out the electrical and using a valve to lockout the hydraulic supply along with a procedure to eliminate trapped pressure and unintended motion should provide a safe lockout condition.

ROSS CONTROLS®

Safe Block and Bleed

When machine access is required for production-related tasks it may be necessary to block the supply of hydraulic energy and also to bleed residual energy from downstream, especially from accumulators, in order to prevent further movement. The devices used to block and bleed hydraulic energy must meet the required Performance Level as determined by the risk assessment. Actuators could move as a result of releasing residual energy from the system. Therefore, an additional load-holding device may be needed to ensure no movement as a result of blocking & bleeding.

Hydraulic Safe Block and Bleed Valve Selection Flow Chart with ROSS Valve Series
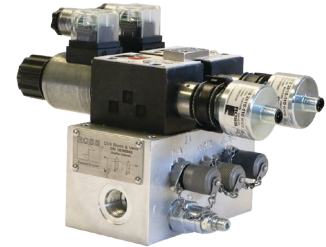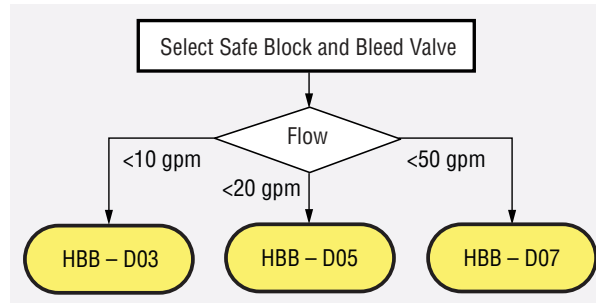
Safe Block & Bleed Example 1 – Category 4

Redundant dual channel solenoid-operated Block and Bleed valve with feedback - must be monitored by the safety controller.

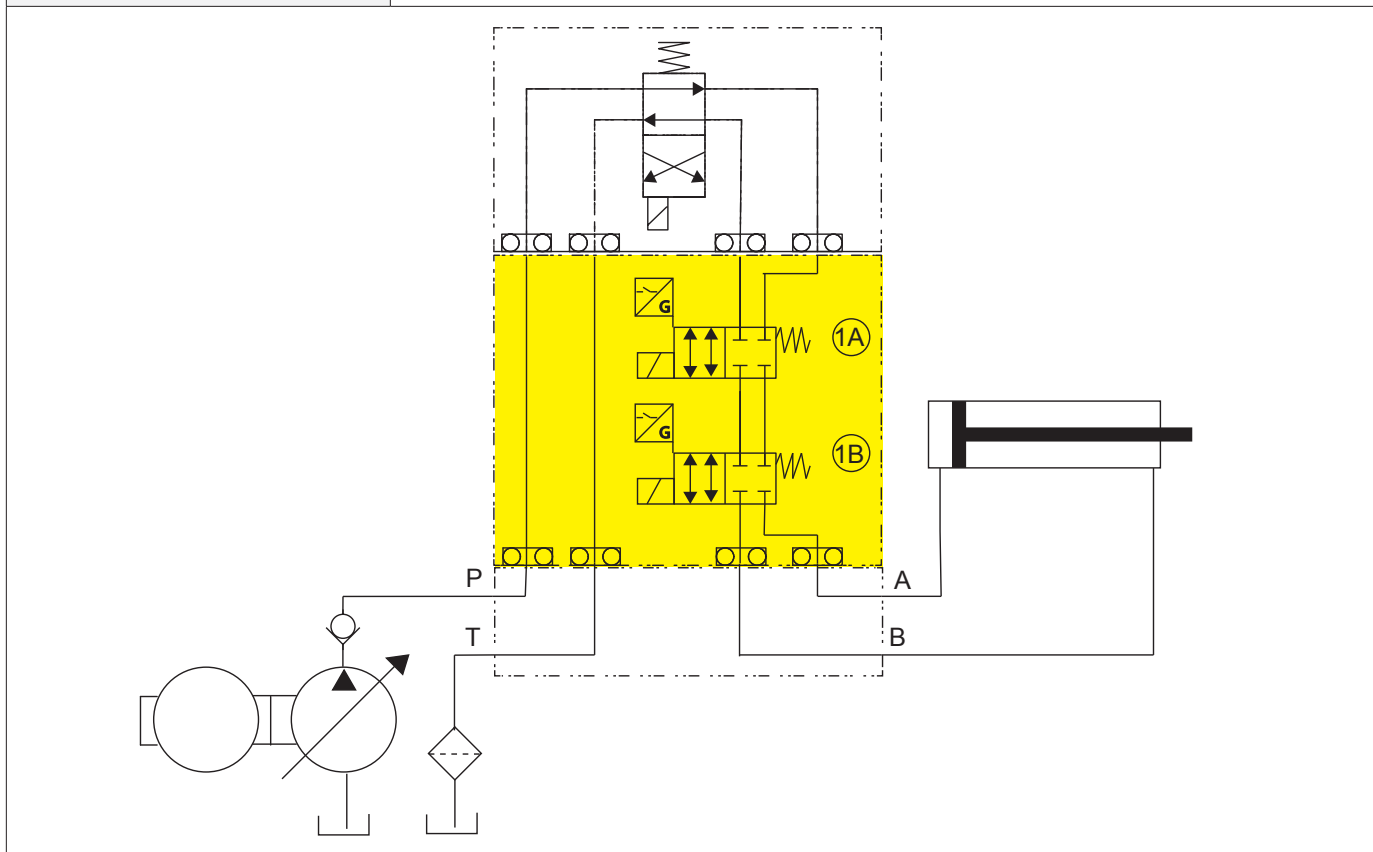| Safety Function	System supply is blocked and downstream pressure is relieved (bled) to tank
Residual Risk	Trapped pressure during lockout (LOTO) Motion due to relieved pressure
Faults to Consider	There are no pressure trapping components in the circuit below. However, in some applications there may be non-safety-rated downstream components that are expected to trap pressure in order to stop motion, and those could fail causing unexpected movement.
ANSI B11.26 Reference	11.4.3.1.4.1
ISO 13849-1 Reference	Safety related stop function initiated by a safeguard Start/restart function Prevention of unexpected startup Isolation and Energy dissipation Emergency Stop Function
VDMA 24584 Reference	6.1 Safe Torque Off (STO) 6.2 Safe Stop 1 (SS1) 6.17 Safe De-energization (SDE)
Solution Valve Series	HBB

Note: Block and Bleed valves are often used with an emergency stop to isolate supply pressure going to the valves that control machine actuators. Block and Bleed valves are also used on individual actuators to protect one area of a machine/system.

Safe Block and Stop

Block and Stop valves are used to block flow in order to prevent unwanted motion, and are typically integrated into individual actuator circuits to prevent movement of a particular component or components. The risk assessment should indicate the required block and stop needs and should indicate the required performance level and category of valves to complete the safety circuit. ROSS offers two series of Block & Stop valves – HDBH and HBH.

Hydraulic Safe Block and Stop Valve Selection Flow Chart with ROSS Valve Series
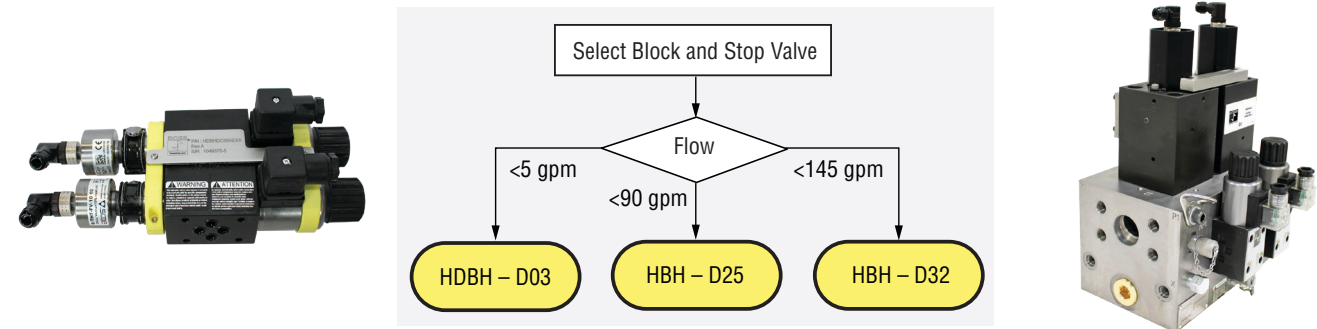
Safe Block & Stop Example 1 – Category 3

Redundant dual channel solenoid-operated Block and Stop valve with feedback – used to block one line - must be monitored by the safety controller.

Safety Function	One line coming from the directional control valve to the actuator is blocked to stop the cylinder from moving
Residual Risk	Trapped pressure during lockout (LOTO) Pressure intensification
Faults to Consider	Motion due to leakage (i.e., seals, hose, fittings)
ANSI B11.26 Reference	11.4.3.3.4.1
ISO 13849-1 Reference	NA
VDMA 24584 Reference	6.1 Safe Torque Off (STO) 6.2 Safe Stop 1 (SS1)
Solution Valve Series	HBH
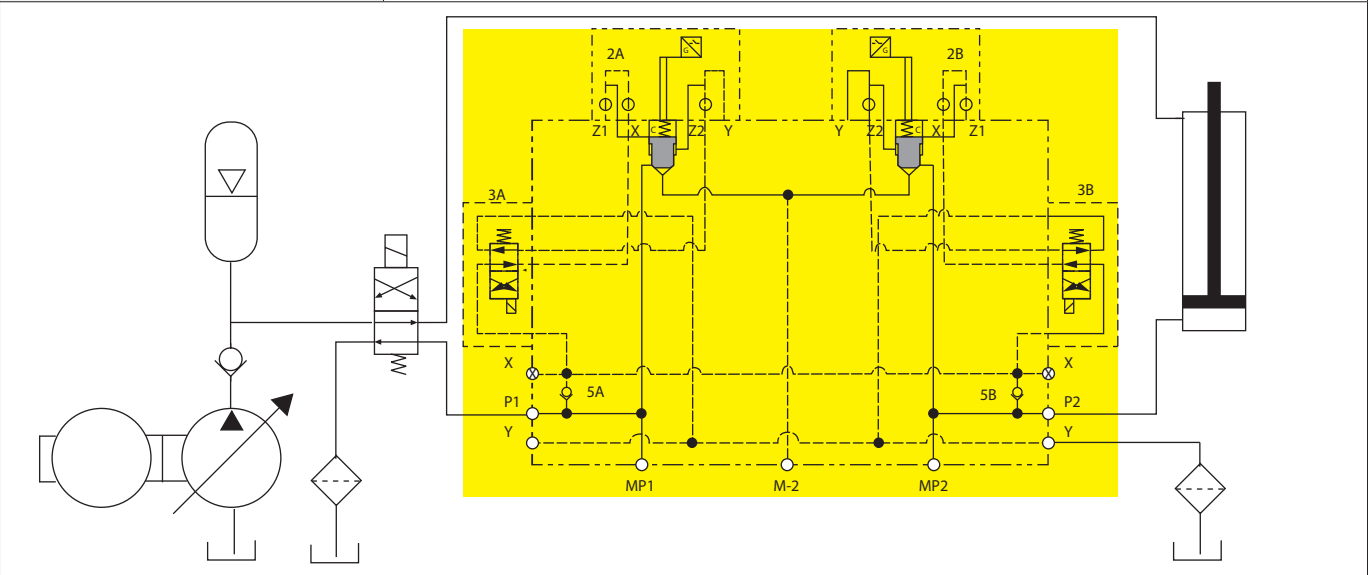
Note: Block and Stop valves are often used with an emergency stop to isolate supply pressure going to the valves that control machine actuators. Block and Stop valves are also are also used on individual actuators to protect one area of a machine/system.

 ROSS CONTROLS®

Dual Safe Block and Stop Example 2 – Category 4

Redundant dual channel solenoid-operated Block and Stop valve with feedback – used to block both cylinder lines - must be monitored by the safety controller.

Safety Function	Both lines from the directional control valve to the actuator are blocked to stop the cylinder from moving
Residual Risk	Trapped pressure during lockout (LOTO) Pressure intensification
Faults to Consider	Motion due to leakage (i.e., seals, hose, fittings)
ANSI B11.26 Reference	11.3.3.3.4.4.1
ISO 13849-1 Reference	NA
VDMA 24584 Reference	6.1 Safe Torque Off (STO) 6.2 Safe Stop 1 (SS1)
Solution Valve Series	HDBH

Note: Dual Block and Stop valves are often used with an emergency stop to isolate supply pressure going to the valves that control machine actuators. Dual Block and Stop valves are also typically used on individual actuators to protect one area of a machine/system.

Hydraulic Safety Valve Selection Summary:

Safety valve selection depends upon:

- Safety function required
- Flow rate
- Control system integration
- Residual risk mitigation

Ultimately, residual risk may not be acceptable, and lockout will be the only suitable solution. Integrating controls, programming, verification, and validation are important next steps in completing a machine safety system.

- For electrical power, mechanical power, and fluid power design
- Design verification calculations to ensure that the Performance Level achieved (PLa) exceeds or meets the Performance Level required (PLr)

Before diving into the design process it is important to discuss control integrity of the safety system. ANSI standards and OSHA have used the term control reliable for many years to define safety system requirements to be used in hazardous applications and for alternative methods of lockout. International standards ISO 13849-1, -2 and IEC 62061, as well as the Machinery Directive, have used terms like Performance Level (PL) and Safety Integrity Level (SIL) to describe similar concepts and requirements.

Control Reliability

Control reliability is defined in ANSI standards as "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." In practice this means that there is not only redundancy in the safety function but monitoring is included to ensure that the safety function occurs and that redundancy is maintained.

> ### *Control Reliability per ANSI B11.19*
>
> *"The goal of control reliability is to create a safety 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 command from occurring. The failure or the resulting fault must be detected at or before the next demand on the safety system (e.g., at the beginning or end of a cycle, or when an engineering controls–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.*
>
> *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 discernible component, module, device or system has failed and that the hazardous motion (or situation) is stopped or prevented from starting or restarting."*

Control Integrity

A common example of the pitfalls of fluid power with regard to Control Integrity is the application of a two-hand, anti-tie-down control device used in conjunction with a standard pneumatic valve to control a simple cylinder press. In practice, the use of this type of setup is widespread, but the failure to consider and address the possible faults and failures of the directional valve is also widespread.

Consider the following. The safety control circuit was designed to safely control a hand-loaded, cylinder press that incorporates a pneumatic cylinder, which, along with the tooling on the end of the cylinder, creates a pinch point hazard. A Category 4 control circuit was specified based upon a risk assessment. Subsequently, a two-hand anti-tie-down control device that provides a safety relay output was selected to control a standard single-solenoid, spring return, 4-way pneumatic valve that causes the cylinder to extend and retract. As a risk reduction method, the 2-hand control is expected to protect the operator from getting one of their hands caught in the pinch point. With this type of circuit, the assumption is that the 2-hand control can only signal the valve to extend the cylinder when the operator uses both hands to successfully start the machine, and the cylinder will only extend as long as the operator keeps both hands on the buttons. Removing one or both hands would instantly signal the valve to retract the cylinder. The other big assumption here is that retracting the cylinder is safe, in itself, and does not generate other hazards.

Remember that, in this example, the required level of control was deemed to be Category 4. This is the highest level of control reliability and it requires redundancy and monitoring to ensure that a single failure does not cause a loss of the safety function. As a chain is only as strong as its weakest link, so is the category of control for a safety control system. Looking back at the control circuit, you will see that the pneumatic valve that was chosen is only a Category B or 1 component because it is a single channel device with no capability for being monitored. Assuming that the 2-hand device and any associated electrical components, such as safety relays, are rated to Category 4, the valve is still a weak link and brings the whole circuit down to Category B or 1. ISO 12100 is a good reference for this situation in that it states, "When more than one safety-rated device contributes toward a safety function, the selection of those devices shall be consistent when considering their reliability and their performance." What does this mean, practically?

Looking at how an operator might interact with the cylinder press in the example, the situation arises where the operator has successfully started the press using both hands and then realizes that the work piece is not in the proper position. The normal reaction is to remove one or both hands from the 2-hand device buttons and to reach in and adjust the work piece. Then, the

ROSS CONTROLS®

operator would attempt to run the press again using both hands. The operator has been trained to believe in the 2-hand device and to trust that it will do its job – every time. Unfortunately, what the operator does not understand, and many controls engineers do not either, is that the single channel pneumatic valve that actually drives the cylinder to extend and retract could stick in the on position even though the operator took both hands off the 2-hand device. This type of failure comes without warning and there is no backup device in the circuit to detect the failure and prevent the cylinder from extending in spite of the failure within the valve. Also, there are a number of causes for a valve to stick – broken return spring, oil, water, and dirt that create varnish, and other contaminants that affect seals, or even objects in the air line that could block movement of the valve elements. Another valve (think redundancy) would have to be incorporated to provide that "back-up" to perform the safety function in the event of the first failure. This is most easily incorporated in the form of a redundant, monitored valve that still performs its safety function in spite of a single failure within the valve. The valve could be of a type that monitors itself or is monitored by the safety control system. A Category 4 valve, in essence, would eliminate the "weak link" in the safety control circuit as all components would be rated to Category 4. In either event, the fault would have to be registered to warn of possible further failures. This puts the operators, maintenance, and, hopefully, engineering on notice that something is up with the valve. This example of how a valve can be overlooked as a weak link can be applied to almost any fluid power system, both pneumatic and hydraulic.

Applications for control-reliable valves exist anytime reliability is an issue for either hydraulic or pneumatic systems. Typical applications for control-reliable Category 3 or 4 valves include: E-stop, two-hand-anti-tie-down, light curtains, safety gates, pneumatic locking devices for safety gates, hydraulic brakes, air brakes, air and hydraulic clutches, rod locks, or any other application where the integrity of the circuit is dependent upon valve operation.

A broad area of applications where control-reliable valves are used is in alternative measures to lockout/tagout (LOTO) for production-related tasks. Currently, non-lockout type valves used to isolate energy for production tasks in the United States must be control-reliable to meet OSHA law.

https://www.osha.gov/laws-regs/standardinterpretations/2004-10-20

> "a circuit that meets the control reliability and control-component-failure-protection requirements of the American National Standards for machine tools (ANSI B11.19-1990) would provide alternative safeguarding measures with respect to the minor servicing exception contained in 1910.147(a)(2)(ii)."

Safety System Performance According to ISO 13849-1

ISO 13849-1defines the principles and requirements of safety circuit design and device selection. Part of the device selection process is to obtain detailed specification and functional safety data for possible components that are being considered for use in each safety function to ensure that when the components are integrated into the system, the system will meet or exceed the required Performance Level (PLr). In order to design a suitable circuit for a safety function, a category (structure) should be selected, as a target, and components should be chosen to meet or exceed that target (e.g., Category 3). The reliability data for each component should be evaluated and used to calculate an overall system $MTTF_D$. Next, a method of monitoring should be chosen and a system Diagnostic Coverage must be calculated and has to be sufficient to help achieve the required Performance Level. Measures taken against Common Cause Failures must also be scored with a minimum cumulative score of 65 points. Once all this is done, the resultant Category, $MTTF_D$, DC, and CCF information can be used to verify that the proposed system achieves the required Performance Level (PLa = PLr). If the achieved Performance Level of the proposed system does not meet or exceed the required Performance Level, a different combination of components with different Categories, $MTTF_D$, DC, and/or CCF will have to be evaluated alternatively. This quite often requires a different selection of components, and can be an iterative process that is necessary to develop a system to reduce risk effectively. Examples of how to go through this process of calculations are shown below.

ISO 13849 Benefits

ISO13849 includes a systematic approach to safety system design and provides quantitative and qualitative analysis factors for reliability and diagnostics. Under this standard, users are required to design safety systems through consideration and implementation of Functional Safety Management (FSM) principles.
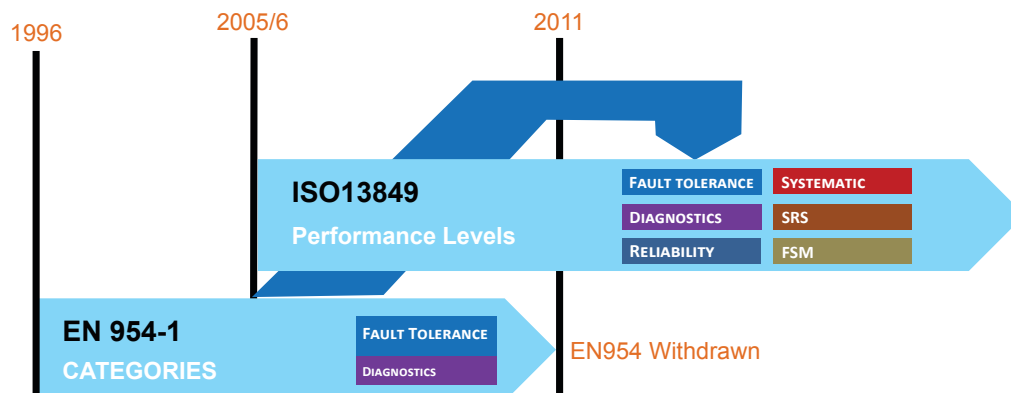
Performance Levels According to ISO 13849-1

ISO 13849-1 defines and uses Performance Levels to specify the risk level of a hazard and the required attributes of the Safety Related Parts of the Control System (SRP-CS). The four key attributes of Performance Levels are shown below.
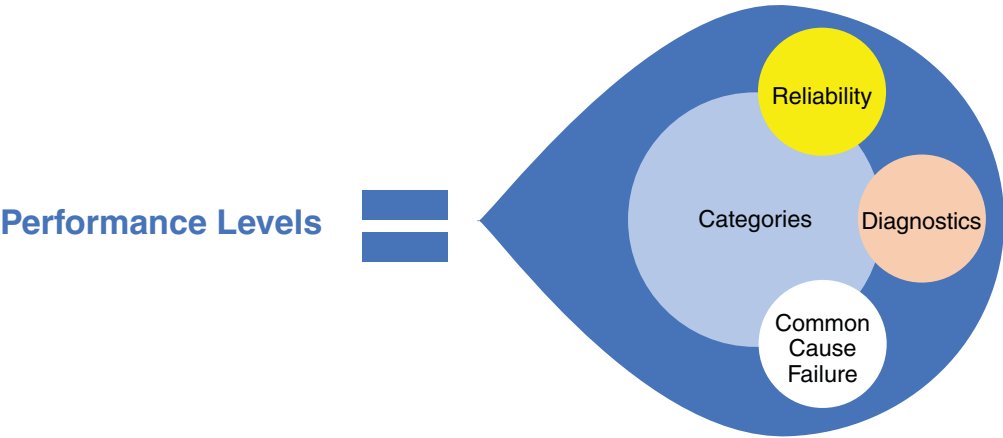
In the course of performing a risk assessment, machinery risk must be evaluated to determine the minimum required performance level (PLr) that any proposed safety function must meet in order to effectively reduce the identified risk to an acceptable level. Once the required performance level is determined, an evaluation of the combination of categories, reliability, diagnostics, and a common cause failure analysis is necessary for the system designer to determine a proposed safety function's achieved performance level (PLa). If the proposed safety function's achieved performance level (PLa) meets or exceeds the required performance level (PLr), the designer can say with confidence that the risk will be sufficiently reduced. Once the system is built, its function must be verified and validated.

A performance level can be obtained using a variety of different levels of Category, $MTTF_D$, and DC. Looking at Figure 5, in the event that your resultant PL bridges two Performance Levels, you must further verify the results by using Table K. Table K shows the specific $MTTF_D$ values that equate to the performance level achieved. This allows the designer to make informed decisions to create a more reliable and, therefore, safer system.

Figure 5 shows the relationship between PL and the Category, $MTTF_D$, and DC values for each safety function.

   ROSS CONTROLS®
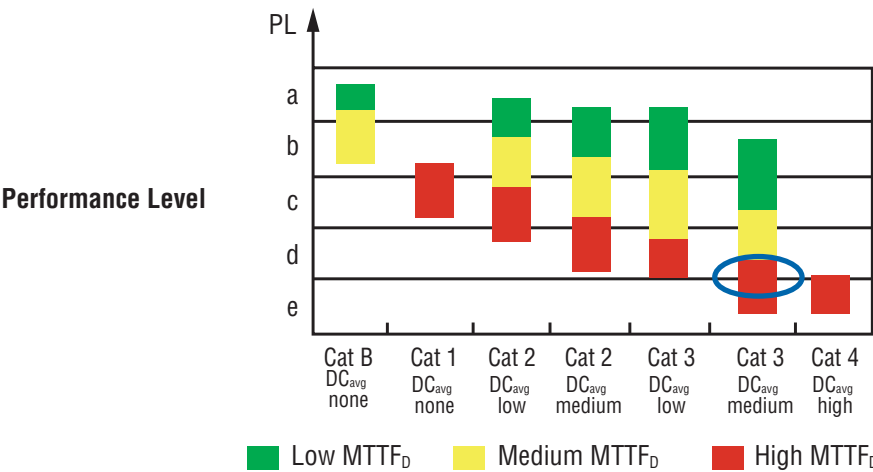
Table K.1

MTTF$_D$ for each channel years	Average probability of a dangerous failure per hour, PFH$_D$ (1/h) and corresponding performance level													
	Cat. B	PL	Cat. 1	PL	Cat. 2	PL	Cat. 2	PL	Cat. 3	PL	Cat. 3	PL	Cat. 4	PL
	DC$_{avg}$ = none		DC$_{avg}$ = none		DC$_{avg}$ = low		DC$_{avg}$ = medium		DC$_{avg}$ = low		DC$_{avg}$ = medium		DC$_{avg}$ = high	
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
110													$2{,}23 \times 10^{-8}$	e
120													$2{,}03 \times 10^{-8}$	e
130													$1{,}87 \times 10^{-8}$	e
150													$1{,}61 \times 10^{-8}$	e
160													$1{,}50 \times 10^{-8}$	e
180													$1{,}33 \times 10^{-8}$	e

NOTE 1 If for Category 2 the demand rate is less than or equal to 1/25 of the test rate (see 6.1.8), then the PFH$_D$ values stated in the Table K.1 for Category 2 multiplied by a factor of 1.1 can be used as a worst-case estimate.

NOTE 2 The calculating of the PFH$_D$-values was based on following DC$_{avg}$:
— DC$_{avg}$ = low, calculated with 60 %;
— DC$_{avg}$ = medium, calculated with 90 %;
— DC$_{avg}$ = high, calculated with 99 %;

Categories According to ISO 13849-1

The most significant attribute of a Performance Level is the structure of the circuit or Category. Table 10 in ISO 13849-1 defines the type of components and principles that are used to design a safety circuit.

Table 10						
Category	Summary of Requirements	System behavior	Principle used to achieve safety	MTTF$_D$ of each channel	DC avg	CCF
B (see 6.2.3)	SRP/CS and/or their protective equipment, as well as their components, shall be designed, constructed, selected, assembled and combined in accordance with relevant standards so that they can withstand the expected influence. Basic safety principles shall be used.	The occurrence of a fault can lead to the loss of the safety function.	Mainly characterized by selection of components	Low to medium	None	Not relevant
1 (see 6.2.4)	Requirements of B shall apply. Well-tried components and well-tried safety principles shall be used.	The occurrence of a fault can lead to the loss of the safety function but the probability of occurrence is lower than for category B.	Mainly characterized by selection of components	High	None	Not relevant
2 (see 6.2.5)	Requirements of B and the use of well-tried safety principles shall apply. Safety function shall be checked at suitable intervals by the machine control system (see 4.5.4).	The occurrence of a fault can lead to the loss of the safety function between the checks. The loss of safety function is detected by the check.	Mainly characterized by structure	Low to high	Low to medium	See Annex F
3 (see 6.2.6)	Requirements of B and the use of well-tried safety principles shall apply. Safety-related parts shall be designed, so that — a single fault in any of these parts does not lead to the loss of the safety function, and — whenever reasonably practicable, the single fault is detected.	When a single fault occurs, the safety function is always performed. Some, but not all, faults will be detected. Accumulation of undetected faults can lead to the loss of the safety function.	Mainly characterized by structure	Low to high	Low to medium	See Annex F
4 (see 6.2.7)	Requirements of B and the use of well-tried safety principles shall apply. Safety-related parts shall be designed, so that — a single fault in any of these parts does not lead to a loss of the safety function, and — the single fault is detected at or before the next demand upon the safety function, but that if this detection is not possible, an accumulation of undetected faults shall not lead to the loss of the safety function.	When a single fault occurs the safety function is always performed. Detection of accumulated faults reduces the probability of the loss of the safety function (high DC). The faults will be detected in time to prevent the loss of the safety function.	Mainly characterized by structure	High	High including accumulation of faults	See Annex F
NOTE For full requirements, see Clause 6.						

Categories of control are used to define different circuit structures of safety control systems and are defined by the relationships between input, logic, and output portions of the circuit. In general, the structure of a circuit is classified based on whether or not the circuit is of a single channel or dual channel design, whether or not diagnostics are implemented, and how well the diagnostics work to detect failures in the circuit.

Another important concept that goes along with circuit structure is fault tolerance. A redundant valve system provides fault tolerance, whereas a non-redundant valve has no fault tolerance. For instance, if a single valve is used to shut off flow and that valve fails open, there was no fault tolerance. Adding redundancy can provide fault tolerance, but must be implemented properly. For example, in a safe exhaust valve there is a combination of two safety functions – blocking supply and exhausting downstream pressure. The blocking function should be redundant in series. If one device sticks open, the other one can still shut off flow. This is an example of single fault tolerance. For the exhaust function, this redundancy should be in parallel. In parallel, the second device can still open to exhaust if the first device fails closed. This provides a fault tolerance of 1 for the exhaust function. For a safe exhaust valve whose function is to block supply and exhaust downstream pressure, this is a well-tried concept. Furthermore, fault-tolerance combined with excellent diagnostics can create a true fail-to-safe system.

ROSS CONTROLS®

Categories B, 1, and 2 have single-channel structure with differing levels of reliability. Category 2 is further differentiated from B and 1 due to the addition of diagnostics to the circuit. This single channel structure allows that a single fault within the system can lead to a dangerous failure. This fault could occur within the input, logic, or output device. At Category 2 this dangerous fault must be detected and indicated by the diagnostics. The function blocks below represent Categories B, 1, and 2.

Category B and 1	Category 2

Categories 3 and 4 have dual channel structures with Category 4 requiring the highest level of reliability and diagnostics. A dual channel (redundant) structure provides the ability of a second channel to perform the safety function if a failure occurs within the other channel. The level of diagnostics determines which faults are detected and whether an accumulation of faults can lead to the loss of the safety function (Category 3) or if this accumulation is not allowed (Category 4). Accumulation of faults can happen when a fault is not detected (masked) until another fault occurs. Masking of faults is dangerous because the first fault can cause the system to run essentially as a single channel system. For example, having a number of guard interlocks wired in series could allow for a short in one interlock to go unnoticed until that specific interlocked door is opened.

Category 3	Category 4
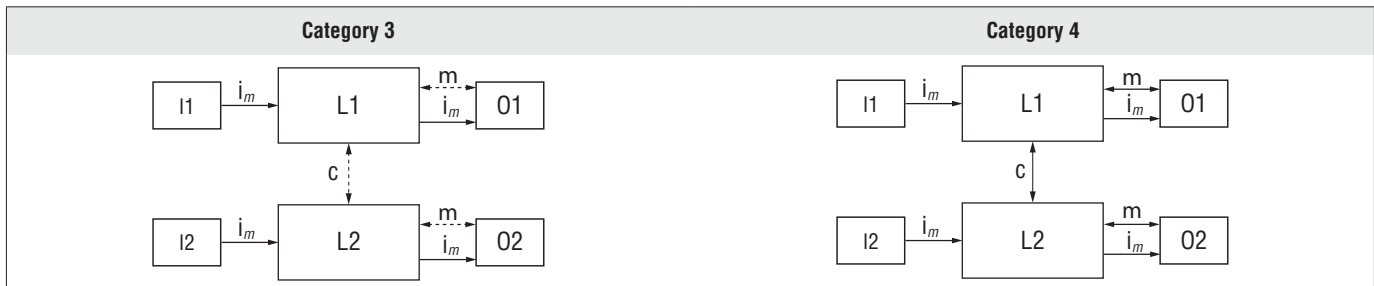
The required system category can be achieved easiest by using input, logic, and output devices that are rated at or above the required category which was derived from a risk assessment. However, the system is limited to the lowest category of the input, logic, or output devices. The following examples illustrate this concept.

Example 1

A Category 3 safety system can be constructed of Category 3 input, logic, and output devices.

Cat 3 + Cat 3 + Cat 3 = Cat 3
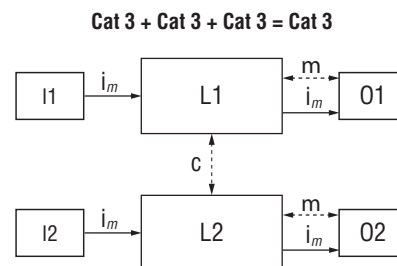
Example 2

A Category 3 safety system could use Category 4-rated logic and output devices along with a Category 3 input device such as a floor mat.

Cat 3 + Cat 4 + Cat 4 = Cat 3
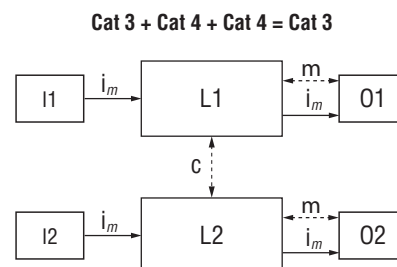
Example 3

Using a Category 2 input device such as a type 2 light curtain will limit the rating to Category 2 even though the other devices are rated higher. The input device does not allow the system to have dual channels throughout, and a single fault could lead to the loss of the safety function.

Cat 2 + Cat 3 + Cat 3 = Cat 2
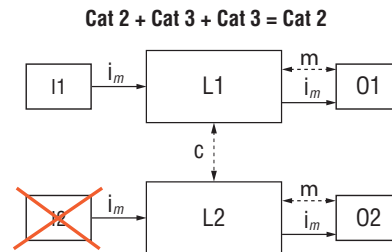
Example 4

A common occurrence is the use of a fluid power output device that is only Category 2 to try to meet Category 3 requirements. Again, the circuit Category rating is limited to the lowest-rated component.

Cat 3 + Cat 3 + Cat 2 = Cat 2
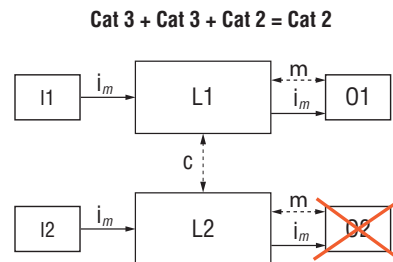
Example 5

Another common occurrence is the use of a fluid power device that is only Category 1 to try to meet Category 3 requirements.

Cat 3 + Cat 3 + Cat 1 = Cat 1
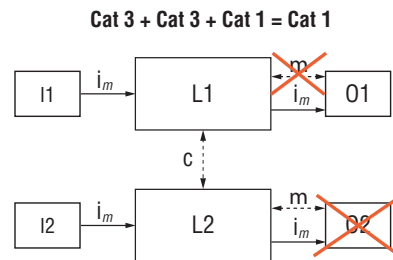
Additionally, the individual input, logic, or output portion of the circuit can be created using a combination of lower Category components to create a subsystem that is equal to the desired Category. Simple examples include using a Category 1 valve with the addition of a feedback sensor creating a Category 2 output or using two Category 2 valves to create a Category 3 or 4 output.

Care must be taken in creating these systems, particularly when creating Category 3 or 4 solutions which require a fail-to-safe design. The designer must understand the specific failure modes and design limitations of the specific products being used and how they can affect the overall system performance.

A simple Category 3 circuit may use two 3/2 normally closed exhaust valves with a pressure switch connected to the outlet of each valve for monitoring downstream pressure. Putting these two Category 2 valves in series does provide redundancy of the safety function but the malfunction of one valve can be masked. If valve two has failed dangerously in the energized position, valve one will still perform the correct valve operation, and both feedback switches will still indicate that the "redundant" system is functioning correctly. Of course, a masked fault is not detected, and the system is essentially running without redundancy.

Stuck valve
not detected
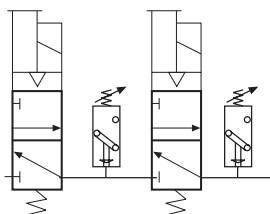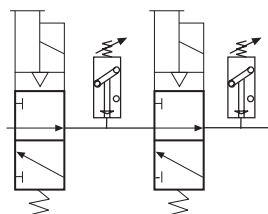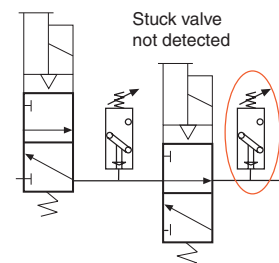
De-energized   Energized   De-energized with masked fault

ROSS CONTROLS®

Reliability According to ISO 13849-1

Reliability represents the life expectancy of a component based on component life cycle testing and the application in which it will be used. Component reliability is reported by manufacturers in a variety of ways. It might be in terms of B_{10}, B_{10D}, $MTTF_D$ or PFH_D depending on the testing standard that was followed. Reliability for electrical and solid-state components is usually represented in terms of $MTTF_D$ or PFH_D. Electro-mechanical devices like valves and contactors are usually expressed in terms, such as B_{10} or B_{10D}.

> B_{10} – The number of cycles at which point 10% of the tested product failed (Dangerous or Safe)

> B_{10D} – The number of cycles at which point 10% of the tested products failed to a dangerous state.

Reliability must be calculated for each safety function to prove that it is suitable for a particular application. The combined reliability of all components of the SRP/CS (input, logic, & output) is the MTTFd of the system.

> $MTTF_D$ – System $MTTF_D$ is the calculated estimate of life of the system in days before a dangerous failure would occur.

> PFH_D – System PFH_D is the calculated estimate of life of the system in hours before a dangerous failure would occur.

"Best-in-class" manufacturers publish reliability information for their products but sometimes default information must be used for products that do not have published data. This default information can be found in ISO 13849-1 Tables C1-C3.

Table C.1 in ISO 13849-1 lists $MTTF_D$ and B_{10D} values for basic and well-tried safety components. This can only be used if manufacturer's data is not available.

Table C.1 — International Standards dealing with $MTTF_D$ or B_{10D} for components

	Basic and well-tried safety principles according to ISO 13849-2:2012	Relevant standards	Typical values: $MTTF_D$ (years) B_{10D} (cycles)
Mechanical components	Tables A.1 and A.2	–	$MTTF_D = 150$
Hydraulic components with $n_{op} \geq 1\ 000\ 000$ cycles per year	Tables C.1 and C.2	ISO 4413	$MTTF_D = 150$
Hydraulic components with $1\ 000\ 000$ cycles per year $> n_{op} \geq 500\ 000$ cycles per year	Tables C.1 and C.2	ISO 4413	$MTTF_D = 300$
Hydraulic components with $500\ 000$ cycles per year $> n_{op} \geq 250\ 000$ cycles per year	Tables C.1 and C.2	ISO 4413	$MTTF_D = 600$
Hydraulic components with $250\ 000$ cycles per year $> n_{op}$	Tables C.1 and C.2	ISO 4413	$MTTF_D = 1\ 200$
Pneumatic components	Tables B.1 and B.2	ISO 4414	$B_{10D} = 20\ 000\ 000$
Relays and contactor relays with small load	Tables D.1 and D.2	EN 50205 IEC 61810 IEC 60947	$B_{10D} = 20\ 000\ 000$
Relays and contactor relays with nominal load	Tables D.1 and D.2	EN 50205 IEC 61810 IEC 60947	$B_{10D} = 400\ 000$
Proximity switches with small load	Tables D.1 and D.2	IEC 60947 ISO 14119	$B_{10D} = 20\ 000\ 000$
Proximity switches with nominal load	Tables D.1 and D.2	IEC 60947 ISO 14119	$B_{10D} = 400\ 000$
Contactors with small load	Tables D.1 and D.2	IEC 60947	$B_{10D} = 20\ 000\ 000$
Contactors with nominal load	Tables D.1 and D.2	IEC 60947	$B_{10D} = 1\ 300\ 000$ (see Note 1)
Position switches [a]	Tables D.1 and D.2	IEC 60947 ISO 14119	$B_{10D} = 20\ 000\ 000$
Position switches (with separate actuator, guard-locking) [a]	Tables D.1 and D.2	IEC 60947 ISO 14119	$B_{10D} = 20\ 000\ 000$
Emergency stop devices [a]	Tables D.1 and D.2	IEC 60947 ISO 13850	$B_{10D} = 100\ 000$

For the definition and use of B_{10D}, see C.4.
NOTE 1 B_{10D} is estimated as two times B_{10} (50 % dangerous failure) if no other information (e.g. product standard) is available.
NOTE 2 "Nominal load" or "small load" should take into account safety principles described in ISO 13849-2, like over-dimensioning of the rated current value. "Small load" means, for example, 20 %.
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 SRP/CS. 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 may be possible, that the machine builder can apply a fault exclusion according to ISO 13849-2, Table D.8, considering the specific application and environmental conditions of the device.
[a] If fault exclusion for direct opening action is possible.

Diagnostics According to ISO 13849-1

ISO 13849-1 uses Diagnostic Coverage (DC) to measure how well a safety system can detect dangerous faults in the system. DC is the ratio of detectable dangerous faults versus total dangerous faults for each component used in the safety function. This ratio is expressed as a percentage for each component in the safety circuit (Input, Logic, Output(s)) and then used to calculate the overall DC for the entire safety circuit.

Diagnostic coverage is only considered in Categories 2, 3, and 4.

$$DC = \frac{\sum \lambda_{DD}}{\sum \lambda_{Dtotal}} \quad (1)$$

where

$\sum \lambda_{DD}$ is the sum of all failure rates of detected dangerous failures;

$\sum \lambda_{Dtotal}$ is the sum of all failure rates of total dangerous failures.

Table 5 — Diagnostic coverage (DC)

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

NOTE 1 For SRP/CS consisting of several parts an average value DC avg for DC is used in Figure 5, Clause 6 and E.2.

NOTE 2 The choice of the DC ranges is based on the key values 60 %, 90 % and 99 % also established in other standards (e.g., IEC 61508) dealing with diagnostic coverage 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 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 borders of this table are assumed within an accuracy of 5 %.

Diagnostic coverage can be determined through an FMEA or single element fault testing of the device. This testing would include incremental position testing of the internal elements to simulate sticking at any point during shifting, as well as damaging wear components such as seals and springs. The goal of the testing is to bring to light any unsafe conditions, especially ones that are not detectable.

FMEA evaluation is needed for all specific potential safety components and associated applications. For example, the ROSS RSe valve can be used as a 5/2 safe return valve and was tested thoroughly to prevent/design out any undetected dangerous failures. Additional valve testing was done to validate its use as a pressure select or dual pressure spring return valve.

Direct monitoring of valve internals with a safety-rated switch should indicate whether or not the valve internals are in the normal, "safe" position, but cannot detect if there is seal damage. Seal damage can cause leakage and could cause the release of trapped pressure or the addition of supply pressure even though the valve internals are in the "safe" position. Depending on the valve safety function and the internal design of the valve, this could be a safe failure or a dangerous failure. The application will determine if this undetected failure is dangerous or not.

It is important to understand the consequences of all possible failures that a component may exhibit in order to determine whether or not they should be considered as safe failures or dangerous failures. Please note that these failures may have different consequences in different applications. For example, a leaky poppet may merely be a nuisance in a 3/2 exhaust valve, but would be a dangerous failure in a PO check valve used to hold a cylinder in position. A dangerous failure is a failure that can immediately lead to loss of the safety function. In a redundant system no first failure should result in the loss of the safety function. For a Category 2 valve, it is accepted that dangerous failures can occur but that the failures will be detected. Simply putting two Category 2 valves together may create a redundant device with high diagnostic coverage but there still may be a single failure that can cause the loss of the safety function. An example of this is two 3/2 block and bleed (or safe exhaust) valves in series that have a closed crossover position. If the downstream valve sticks in this crossover position it will block the addition of pressure but will not remove stored energy as the safety function requires. This does not meet the requirements of a Category 3 or 4 system due to a single failure, resulting in the loss of the safety function.

 ROSS CONTROLS®

Manufacturers publish diagnostic coverage information for their products but, as with reliability, sometimes default information must be used for products that do not have published data. Table E.1 of ISO13849-1 provides estimates of the typical diagnostic coverage for input, logic, and output devices. These estimates can be helpful to understand typical values of diagnostic coverage for common types of monitoring and can be used as a starting point for determining what type of monitoring might work best for your application. However, it is important to understand that these are generic estimates, and any proposed safety system must be properly analyzed for actual diagnostic coverage capabilities prior to implementation.

Table E.1 — Estimates for diagnostic coverage (DC)

Measure	DC
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	0 % to 99 %, depending on how often a signal change is done by the application
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	0 % to 99 %, depending on the application; this measure alone is not sufficient for the required performance level e!
Monitoring some characteristics of the sensor (response time, range of analogue signals, e.g. electrical resistance, capacitance)	60 %
Logic	
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 %
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)	90 % (depending on the testing technique)
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 demand it, 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 (8 bit)	90 %
Invariable memory: signature of double word (16 bit)	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: RAM monitoring with modified Hamming code or RAM self-test (e.g., "galpat" or "Abraham")	99 %
Processing unit: self-test by software	60 % to 90 %
Processing unit: coded processing	90 % to 99 %
Fault detection by the process	0 % to 99 %, depending on the application; this measure alone is not sufficient for the required performance level "e"!

NOTE 1 For additional estimations for DC, see, e.g. IEC 61508–2:2010, Tables A.2 to A.15.

NOTE 2 If medium or high DC is claimed for the logic, at least one measure for variable memory, invariable memory and processing unit with each DC at least 60 % has to be applied. There may also be measures that used other than those listed in this table.

NOTE 3 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 a FMEA should be the basis for the estimation of the DC.
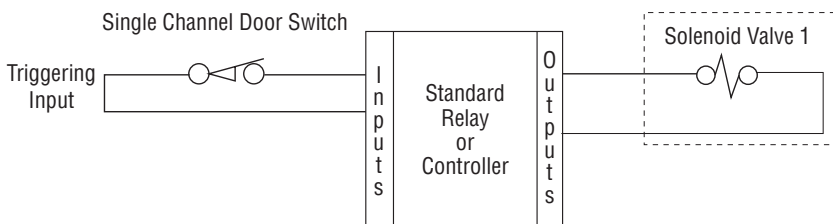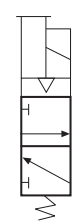
Table E.1 — *(continued)*

Measure	DC
Output device	
Monitoring of outputs by one channel without dynamic test	0 % to 99 % depending on how often a signal change is done by the application
Cross monitoring of outputs without dynamic test	0 % to 99 % depending on how often a signal change is done by the application
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 actuators by logic and test equipment	99 %
Indirect monitoring (e.g., monitoring by pressure switch, electrical position monitoring of actuators)	90 % to 99 %, depending on the application
Fault detection by the process	0 % to 99 %, depending on the application; this measure alone is not sufficient for the required performance level "e"!
NOTE 1 For additional estimations for DC, see, e.g. IEC 61508–2:2010, Tables A.2 to A.15.	
NOTE 2 If medium or high DC is claimed for the logic, at least one measure for variable memory, invariable memory and processing unit with each DC at least 60 % has to be applied. There may also be measures that used other than those listed in this table.	
NOTE 3 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 a FMEA should be the basis for the estimation of the DC.	

ROSS CONTROLS®

Diagnostics Examples

The following examples help identify the characteristics and concepts of the types of diagnostics that are common in fluid power safety solutions.
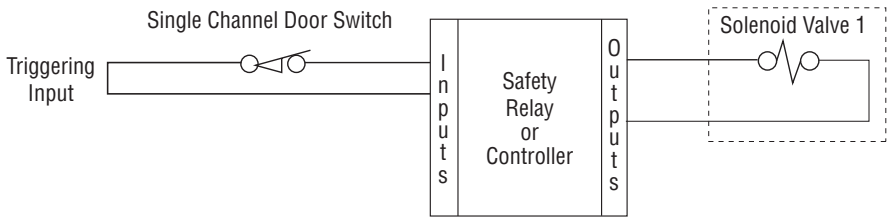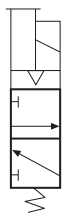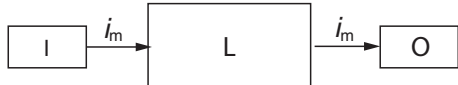
The example characteristics and considerations are intended to identify commonly overlooked issues or potentially dangerous failures. These are not specific to ROSS Control's valves or circuits and should be considered generic concerns for any manufacturers products or systems.

While ROSS valves are shown in the graphical representations the concerns listed may not apply to the specific valve image represented. For example, the category 2 direct monitoring example lists "Switch may not change state prior to valve allowing flow" but this specific valve has had this consideration designed out. However, this consideration is a distinct issue within the fluid power industry and is entirely dependent upon the specific manufacturer and valve design.
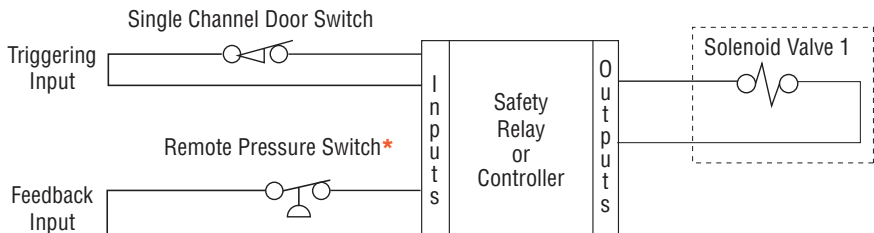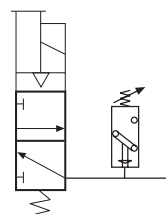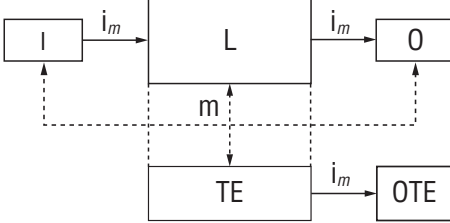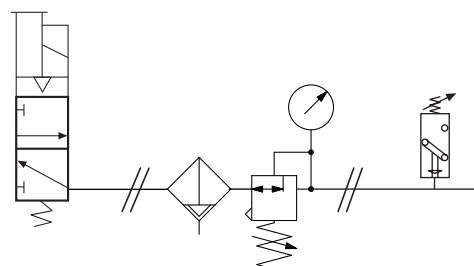
Category B – Example with No Monitoring

Circuit Description	Single channel input, logic & output using standard products with no feedback monitoring	Category B
Diagnostic Coverage	ISO 13849-1 Table E.1: No feedback monitoring	DC 0%
Circuit Schematic Example		Fluid Power Schematic Example

	Triggering Input	Logic	Output (No Feedback)	
	Cat B	+ Cat B	+ Cat B	= Cat B

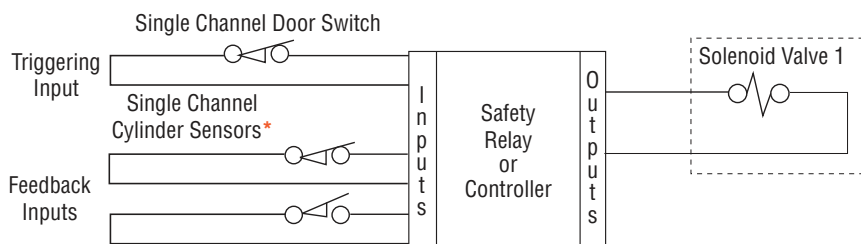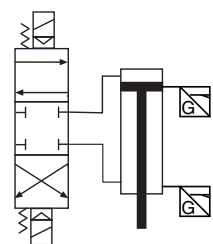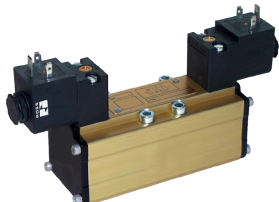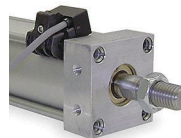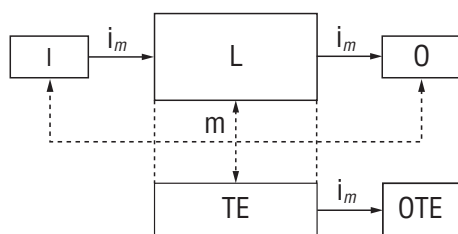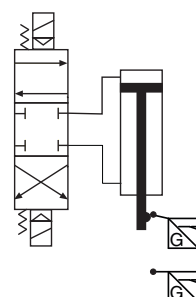| Characteristics	Single channel input device Single channel logic device Single channel output device No Feedback
Considerations	Can use a mix of standard and safety products Single fault can lead to a loss of safety function but would not be detected Faults in the valve are not detected Devices with Low or Medium range MTTF$_D$ are limited to Cat B
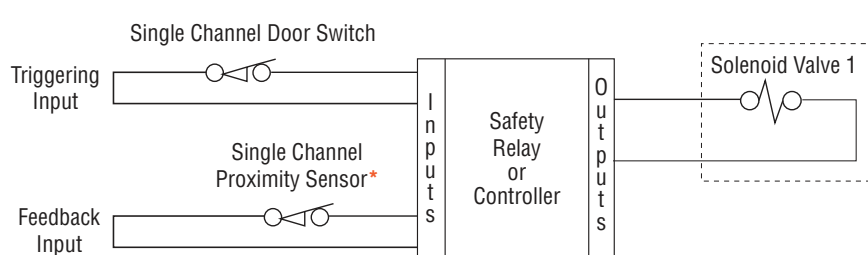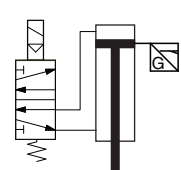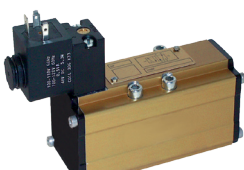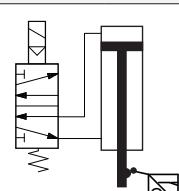
Category 1 – Example with No Monitoring

Circuit Description	Single channel input, logic & output using standard products with no feedback monitoring	Category 1
Diagnostic Coverage	ISO 13849-1 Table E.1: No feedback monitoring	DC 0%
Circuit Schematic Example		Fluid Power Schematic Example

Triggering Input   **Logic**   **Output**
(No Feedback)

Cat 1   +   Cat 1   +   Cat 1   =   Cat 1

Characteristics	Single channel input device Single channel logic device Single channel output device No Feedback
Considerations	Can use a mix of standard and safety products Single fault can lead to a loss of safety function but would not be detected Faults in the valve are not detected Devices with High range $MTTF_D$ can be used for Cat 1

     ROSS CONTROLS®

Category 2 – Example 1 with Indirect Monitoring

Circuit Description	Single channel input, logic & output using safety products with indirect feedback monitoring	Category 2
Diagnostic Coverage	ISO 13849-1 Table E.1: Indirect monitoring (e.g., monitoring by pressure switch, electrical position monitoring of actuators)	DC 90-99%*
Circuit Schematic Example		Fluid Power Schematic Example

Single Channel Door Switch

Triggering Input

Remote Pressure Switch*

Feedback Input

Inputs

Safety Relay or Controller

Outputs

Solenoid Valve 1

Triggering Input   **Logic**   **Output**   **Feedback Input**

Cat 2   +   Cat 2   +   (Cat 1   +   Feedback)   =   Cat 2

Cat 2

I — i_m → L — i_m → O

m

TE — i_m → OTE

Characteristics	Single channel safety input device Single channel safety logic device Single channel safety output device Feedback Sensing is external to the valve (indirect) *Selection of 90-99% will be application related and can be affected by switch location
Considerations	Single fault can lead to a loss of safety function but could be detected Indirect monitoring of a Cat 1 output device can result in a Cat 2 sub-system Placement of the pressure switch is critical due to the effect of downstream devices Pressure setting of switch should result in a safe condition (should not be minimum operating pressure)

Additional Considerations

Note: The location of the pressure switch should be placed so that it indicates that the system has achieved a safe condition - i.e., pressure released. In most systems it can be placed immediately after the safe exhaust valve. A system with long piping runs with T's, reducers, or intermediate components that may restrict exhaust flow such as filters and regulators should be evaluated to place the switch in the most appropriate location.
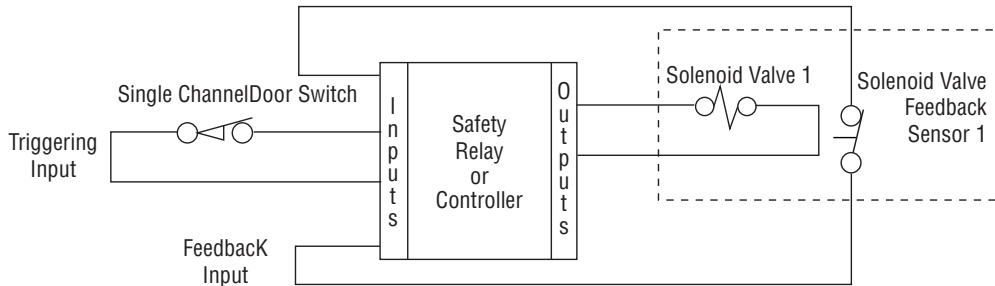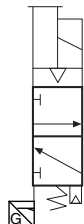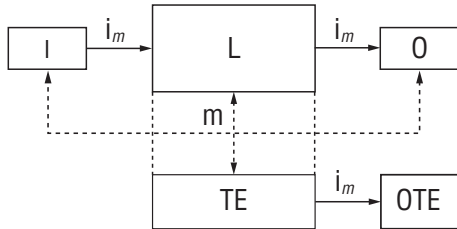
Category 2 – Example 2 with Indirect Monitoring

Circuit Description	Single channel input, logic & output using safety products with indirect feedback monitoring	Category 2
Diagnostic Coverage	ISO 13849-1 Table E.1: Indirect monitoring (e.g., monitoring by pressure switch, electrical position monitoring of actuators)	DC 90-99% *
Circuit Schematic Example		Fluid Power Schematic Example

Triggering Input   **Logic**   **Output**   **Feedback Input**

Cat 2   +   Cat 2   +   (Cat 1   +   Feedback)   =   Cat 2

Cat 2

Characteristics	Single channel safety input device Single channel safety logic device Single channel safety output device Feedback Sensing is external to the valve (indirect) and only detects the de-energized valve via the cylinder being fully retracted *Selection of 90-99% will be application related and can be affected by valve type and switch(es) locations
Considerations	Single fault can lead to a loss of safety function but could be detected Indirect monitoring of a Cat 1 output device can result in a Cat 2 sub-system Proximity or limit switch only indicates end of stroke (fully retracted) Loss of supply air could cause loss of safety function

Additional Considerations

Note: It should be noted that this example uses a 4-way single solenoid valve for a safe-return function and not as a safe exhaust. Therefore, the safe condition is when the cylinder is retracted, as indicated by the switch on the cylinder. Proper execution of the safety function in this case is fully dependent upon the availability of supply air to the valve.
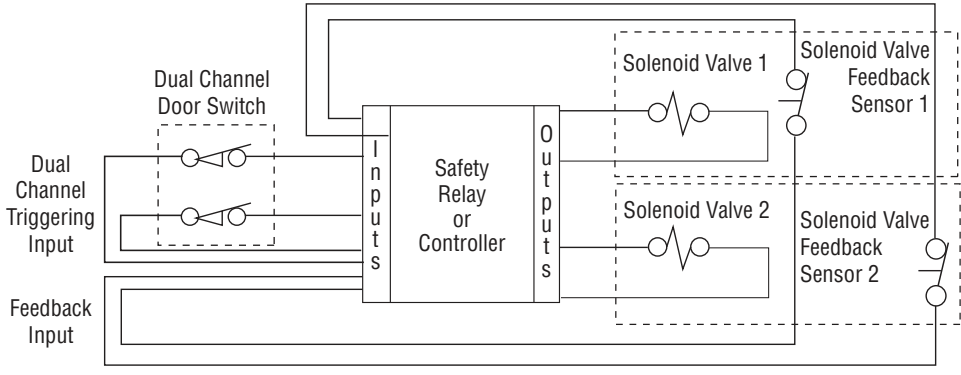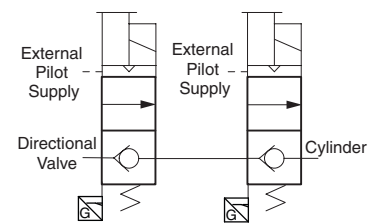
Note: Indirect monitoring of actuators can be done with sensors integrated into the actuators or added externally. Proximity sensors or limit switches are most commonly used to provide this feedback. This feedback monitoring can indicate that the machine cycle was performed correctly on the last cycle. It could also indicate that the safe position was not obtained within an expected time. An increase in cycle time could indicate a potentially hazardous situation such as a jammed part. The diagnostic coverage of the system is dependent upon detecting dangerous failures. The level of diagnostic coverage claimed depends on what hazards exist, what the feedback detects, and how this feedback is monitored within the logic.
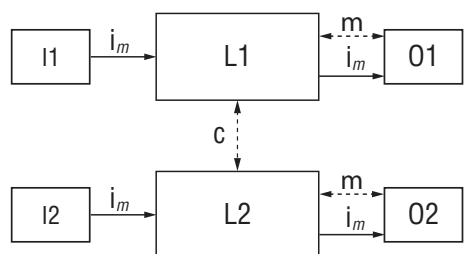
 ROSS CONTROLS®

Category 2 – Example 3 with Indirect Monitoring

Circuit Description	Single channel input, logic & output using safety products with indirect feedback monitoring	Category 2
Diagnostic Coverage	ISO 13849-1 Table E.1: Indirect monitoring (e.g., monitoring by pressure switch, electrical position monitoring of actuators)	DC 90-99%*
Circuit Schematic Example		Fluid Power Schematic Example

Triggering Input   Logic   Output   Feedback Input

Cat 2   +   Cat 2   +   (Cat 1   +   Feedback)   =   Cat 2
$$\text{Cat 2}$$

Characteristics	Single channel safety input device Single channel safety logic device Single channel safety output device Feedback Sensing is external to the valve and only indicates end of stroke positions (indirect) *Selection of 90-99% will be application related and can be affected by valve type and switch(es) locations
Considerations	Single fault can lead to a loss of safety function but could be detected Indirect monitoring of a Cat 1 output device can result in a Cat 2 sub-system Safety function is to stop immediately regardless of cylinder position which may be mid-stroke – feedback sensors will not indicate intermediate stop positions

Additional Considerations

Note: Indirect monitoring of actuators can be done with sensors integrated into the actuators or added externally. Proximity sensors or limit switches are most commonly used to provide this feedback. This feedback monitoring can indicate that the machine cycle was performed correctly on the last cycle. It could also indicate that the safe position was not obtained within an expected time. An increase in cycle time could indicate a potentially hazardous situation such as a jammed part. The diagnostic coverage of the system is dependent upon detecting dangerous failures. The level of diagnostic coverage claimed depends on what hazards exist, what the feedback detects, and how this feedback is monitored within the logic.

Category 2 – Example with Direct Monitoring

Circuit Description	Single channel input, logic & output using safety products with direct feedback monitoring	Category 2
Diagnostic Coverage	ISO 13849-1 Table E.1: Direct monitoring (e.g., electrical position monitoring of control valves, monitoring of electromechanical devices by mechanically linked contact elements)	DC 99%
Circuit Schematic Example		Fluid Power Schematic Example

Triggering Input	Logic	Output	Feedback Input

Cat 2   +   Cat 2   +   Cat 2   =   Cat 2

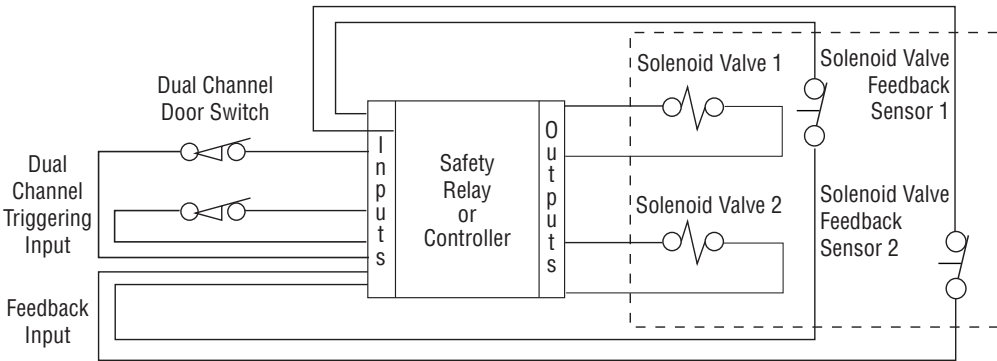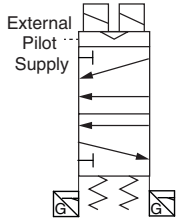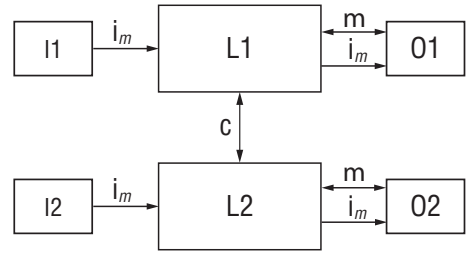| Characteristics	Single channel safety input device Single channel safety logic device Single channel safety output device Feedback Sensing is integral to the valve (direct)
Considerations	Single fault can lead to a loss of safety function but could be detected Depending on how the switch is integrated into the valve, the switch might not change state prior to valve allowing flow – sufficient overlap would prevent this

     ROSS CONTROLS®

Category 3 – Example with Direct Monitoring (Cylinder Holding)

Circuit Description	Dual channel input, logic & output using safety products with direct feedback monitoring - redundant solenoid PO Checks for cylinder holding	Category 3
Diagnostic Coverage	ISO 13849-1 Table E.1: • Redundant shut-off path with monitoring of the actuators by logic and test equipment • Direct monitoring (e.g., electrical position monitoring of control valves, monitoring of electromechanical devices by mechanically linked contact elements)	DC 90%
Circuit Schematic Example		Fluid Power Schematic Example

Triggering Input   **Logic**   **Output with Feedback**

Cat 3   +   **Cat 3**   +   **Cat 3**   =   **Cat 3**

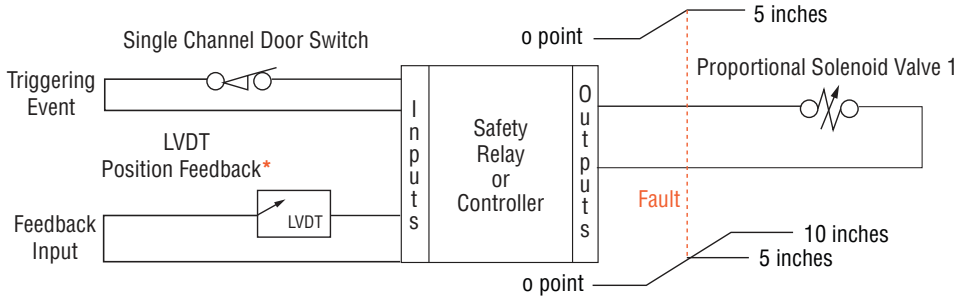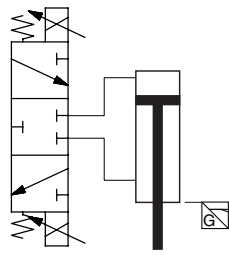| Characteristics	Dual channel safety input device Dual channel safety logic device Dual channel safety output device Feedback Sensing is integral to the valves (direct) Safe function is to trap pressure in the cylinder to prevent motion – leakage can allow motion
Considerations	Single fault does not lead to loss of safety function and can be detected, but an accumulation of faults can lead to loss of safety function Leakage will not be detected, and extra measures should be taken to avoid leaks, such as hard piping instead of hose, etc. Depending on how the switch is integrated into the valve, the switch might not change state prior to valve allowing flow – sufficient overlap would prevent this

Category 4 – Example with Direct Monitoring (Safe Exhaust)

Circuit Description	Dual channel input, logic & output using safety products with direct feedback monitoring - redundant solenoid exhaust valves for safe exhaust	Category 4
Diagnostic Coverage	ISO 13849-1 Table E.1: • Redundant shut-off path with monitoring of the actuators by logic and test equipment • Direct monitoring (e.g., electrical position monitoring of control valves, monitoring of electromechanical devices by mechanically linked contact elements)	DC 99%
Circuit Schematic Example		Fluid Power Schematic Example

Triggering Input	Logic	Output with Feedback	Output with Feedback	

Cat 4 + **Cat 4** + **(Cat 2 with Feedback** + **Cat 2 with Feedback)** = **Cat 4**

Cat 4

Characteristics	Dual channel safety input device Dual channel safety logic device Dual channel safety output device Feedback Sensing is integral to the valves (direct) Safety function is to exhaust downstream pressure Further operation is prevented ensuring that a buildup of faults does not lead to loss of the safety function
Considerations	Single fault does not lead to loss of safety function and can be detected – an accumulation of faults cannot lead to loss of safety function Leakage is not a consideration

 ROSS CONTROLS®

Category 4 – Example with Direct Monitoring

Circuit Description	Dual Channel input & Redundant shut-off path with dual element monitoring	Category 4
Diagnostic Coverage	Direct monitoring (e.g., electrical position monitoring of control valves, monitoring of electromechanical devices by mechanically linked contact elements)	DC 99%
Circuit Schematic Example		Fluid Power Schematic Example

Triggering Input   **Logic**   **Redundant Output with Feedback**

Cat 4   +   Cat 4   +   Cat 4   =   Cat 4

Characteristics	Dual channel safety input device Dual channel safety logic device Dual channel safety output device Dual element feedback sensing is integral to the valve (direct) Further operation is prevented ensuring that a buildup of faults does not lead to loss of the safety function
Considerations	Single fault does not lead to loss of safety function and can be detected – an accumulation of faults cannot lead to loss of safety function

Category 2 – Example with Monitor by Process

Circuit Description	Single channel input, logic & output using safety products with monitoring of the process	Category 2
Diagnostic Coverage	ISO 13849-1 Table E.1: Fault detection by the process	DC 0-99%*
Circuit Schematic Example		Fluid Power Schematic Example

Triggering Input **Logic** **Output** **Feedback Input**

Cat 2 + Cat 2 + (Cat 2 + Feedback) = Cat 2
Cat 2

Characteristics	Single channel safety input devices Single channel safety logic device Single channel proportional output devices *Feedback sensing is external to the valve and measures cylinder position throughout the stroke Selection of 0-99% will be application related
Considerations	Single fault can lead to a loss of safety function but could be detected Indirect monitoring of a Cat 1 output device can result in a Cat 2 sub-system The diagnostic coverage will be based on what is considered a dangerous failure and the test interval.

Additional Considerations

Note: Monitoring by process is done with sensors integrated or added externally to the actuators or other process equipment. Linear displacement sensors, flow sensors, volume sensors, load cells, and rotary encoders are just a few examples of sensors that provide linear feedback that can be used to monitor the machine condition during the manufacturing process. Multiple sensors can also be used to simulate linear feedback. The diagnostic coverage of the system is dependent upon detecting dangerous failures. The level of diagnostic coverage claimed depends on what hazards exist, what the feedback detects, the effects of incorrect or incomplete feedback, and how this feedback is monitored within the logic.

   ROSS CONTROLS®

Common Cause Failures According to ISO13849-1

Common Cause Failures (CCF) are failures of multiple components that can be generated simultaneously by a common event. For example, freezing of moisture in a redundant valve causing both valve elements to fail open is a common cause failure. The CCF for a safety system is determined by a cumulative scoring of the measures taken against common cause failures during design and implementation.

No.	Measure against CCF	Score	Fluid Power Considerations
1	**Separation / Segregation**		• Separating 24 vdc wiring from higher voltages • Separating signal paths • Pulse testing
	Physical separation between signal paths, for example: — separation in wiring/piping; — detection of short circuits and open circuits in cables by dynamic test; — separate shielding for the signal path of each channel; — sufficient clearances and creepage distances on printed-circuit boards.	15	
2	**Diversity**		
	Different technologies/design or physical principles are used, for example: — first channel electronic or programmable electronic and second channel electromechanical hardwired, — different initiation of safety function for each channel (e.g., position, pressure, temperature), and/or digital and analog measurement of variables (e.g., distance, pressure or temperature) and/or Components of different manufactures	20	• For example, use a mechanical pressure switch along with a pressure transducer for pressure feedback
3	**Design / Application / Experience**		• Fluids should be conditioned to keep the pressure and/or temperature within acceptable limits by use of regulators, relief valves, heat exchangers, etc.
3.1	Protection against over-voltage, over-pressure, over-current, over-temperature, etc.	15	
3.2	Components used are well-tried	5	
4	**Assessment / Analysis**		• Third-party certification of components is a good way to ensure that FMEA and incremental position failure testing is done
	For each part of safety related parts of control system a failure mode and effect analysis has been carried out and its results taken into account to avoid common-cause-failures in the design	5	
5	**Competence / Training**		• Safety system designers should be trained to understand the characteristics of different fluid power components and their failure modes in different applications
	Training of designers to understand the causes and consequences of common cause failures	5	
6	**Environmental**		
6.1	For electrical/electronic systems, prevention of contamination and electromagnetic disturbances (EMC) to protect against common cause failures in accordance with appropriate standards (e.g., IEC 61326–3-1). Fluidic systems: filtration of the pressure medium, prevention of dirt intake, drainage of compressed air, e.g., in compliance with the component manufacturers' requirements concerning purity of the pressure medium. NOTE: For combined fluidic and electric systems, both aspects should be considered.	25	• Pneumatic considerations include filtration and lubrication • Hydraulic considerations include filtration and oil temperature
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).	10	
	Total (max. achievable 100)		

Total score	Measures for avoiding CCF[a]
65 or better	Meets the requirements
Less than 65	Process failed => choose additional measures

a   Where technological measures are not relevant, points attached to this column can be considered in the comprehensive calculation.

11	DESIGN VERIFICATION

Safety Function Verification

Design verification uses Category, $MTTF_D$, DC, and CCF to verify that the proposed system achieves the required Performance Level.

Reliability information on each part of the safety function needs to be collected. For this example, the safety function example below will be used to show how to collect and convert manufacturer reliability data into information that can be used to calculate system reliability.

Triggering Input		Logic		Redundant Output with Feedback		
Cat 4	+	Cat 4	+	Cat 4	=	Cat 4
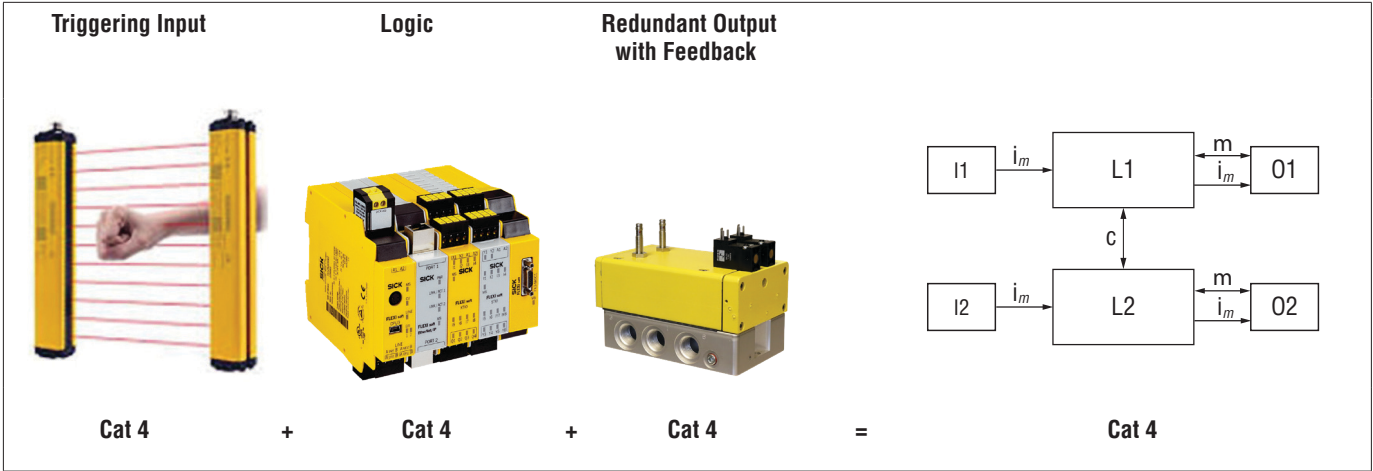
For this example:

- The Performance Level required (PL r) is Performance Level d (PL d)
- The machine has a cycle time of 2 parts per minute or 30 seconds
- The machine operates 360 working days per year at 16 working hours per day

Reliability Information Example for Input Devices

Input Device Reliability	
Type	Type 4 (IEC 61496-1)
Safety Integrity Level	SIL 3 (IEC 61508) SIL CL3 (IEC 62061)
Category	Category 4 (EN ISO 134849)
Performance Level	PL e (EN ISO 13849)
PFH$_D$ (mean probability of a dangerous failure per hour)	$15*10^{-9}$ (EN ISO 13849)

ROSS CONTROLS®

Reliability Information Example for Logic Devices
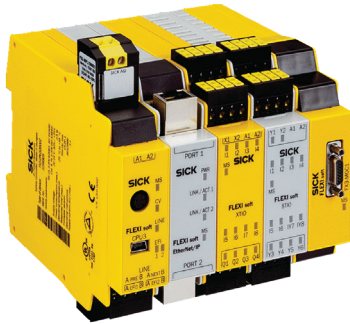
Logic Device Reliability	
Standards	EN 954-1, ISO 13849-1, IEC/EN 6024-1, IEC 60947-4-1, IEC 00947-5-1, ANSI B11.19, AS 4024, 1
Safety Classification	Cat. 4 per EN 954-1 (ISO 13849-1), SIL CL3 per EN IEC62061, PL e per ISO 13849-1
Functional Safety Data	$MTTF_D$ > 398 Years Suitable for performance levels PL e (according to ISO 13849-1:2006) and for use in SIL 3 systems (according to IEC 62061) depending on the architecture and application characteristics
Certifications	CE Marked for all applicable directives, cULus and DGUV

Reliability Information Example for Output Devices

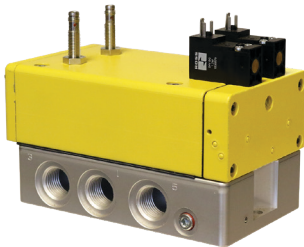| Output Device Reliability	
Safety Classification	Max. Category 4, PL e, SIL 3
B_{10D} Value	20 million cycles
Monitoring	Dynamic, cyclical, external with customer supplied equipment. Monitoring should check state of both valve position sensors with any and all changes in state of valve control signals.
Diagnostic Coverage (DC)	High, 99%
Certifications	CE Marked for all applicable directives, cULus and DGUV

Calculating Number of Operations (n$_{op}$)

The first step of calculating the $MTTF_D$ of a system is determining the Number of Operations (n_{op}) per year of the safety function.

This is done by collecting the following information:

- n_{op} = Number of operations per year
- d_{op} = Number of days per year of operation
- h_{op} = Number of hours per day of operation
- t_{cycle} = Time between cycles of the safety function

The number of operations formula is:

$$n_{op} = \frac{d_{op} \times h_{op} \times 3600 \text{ s/h}}{t_{cycle}}$$

The calculation would look something like this:

$$n_{op} = \frac{360 \frac{d}{y} \times 16 \frac{h}{d} \times 3600 \frac{s}{h}}{300 \frac{s}{cycle}} = 69120 \frac{cycles}{y}$$

Calculating MTTF$_D$

The second step of calculating the MTTF$_D$ of a safety system uses the calculated n_{op} and reliability of each component in the safety function to determine system reliability. Component reliability reporting varies from manufacturer to manufacturer and from device type to device type.

This is done by collecting the following information:

- MTTF$_D$ = Mean Time To Failure (dangerous)
- B$_{10D}$ = Number of cycles where 10% of the components fail to danger
- n_{op} = Number of operations per year

The Mean Time To Failure (dangerous) formula is:

$$MTTF_D = \frac{B_{10D}}{0,1 \times n_{op}}$$

Now, convert the individual product data into usable information to start the MTTF$_D$ calculation.

Input conversion from 15* 10^{-9} PFH$_D$ to MTTF$_D$

MTTF$_D$ = 1/(8760 hrs/year *PFH$_D$)

MTTF$_D$ = 1/(8760*0.000000015)

MTTF$_D$ = 7610 years for the light curtain

Logic information was given by the manufacturer in terms of MTTF$_D$ = 398 Years

Output conversion from 20 million B$_{10D}$ to MTTF$_D$

$$MTTF_D \text{ formula} = \frac{B_{10D}}{0.1* \; n_{op}}$$

$$MTTF_D \text{ calculation example} = \frac{20,000,000 \text{ cycles}}{0.1* \; 537,600}$$

MTTF$_D$ result = **372 years**

Determine the system's MTTF$_D$ by using the following formula.

$$\frac{1}{\text{System MTTF}_D} = \frac{1}{\text{Input MTTF}_D} + \frac{1}{\text{Logic MTTF}_D} + \frac{1}{\text{Output MTTF}_D}$$

$$\text{System MTTF}_D \text{ calculation example} = \frac{1}{7610} + \frac{1}{398} + \frac{1}{372}$$

MTTF$_D$ result = **188 years**

If the input, logic, and output devices are dual channel devices, or if the same input, logic and output devices are used on both channels, the calculation is complete. If channel 1 and channel 2 use different devices, an additional symmetrization calculation must be performed. See example below.

$$MTTF_D = \frac{2}{3}\left[MTTF_{DC1} + MTTF_{DC2} - \frac{1}{\frac{1}{MTTF_{DC1}} + \frac{1}{MTTF_{DC2}}} \right]$$

For the example, the result is HIGH reliability because the calculation resulted in an MTTF$_D$ of 188 years.

Denotation of MTTF$_D$	Level of MTTF$_D$
Low	3 years ≤ MTTF$_D$ < 10 years
Medium	10 years ≤ MTTF$_D$ < 30 years
High	30 years ≤ MTTF$_D$ < 100 years
MTTF$_D$ of the system = 188 years = HIGH	

ROSS CONTROLS®

Calculating Diagnostic Coverage (DC)

Diagnostic Coverage (DC) is a representation of what percentage of faults within the safety system can be detected. DC is calculated by understanding the monitoring potential of each device in the system. Calculating the DC of a system uses the following information (from above):

- Number of Operations per year (N_{op}) = 69120 cycles per year
- Input device $MTTF_D$ = 7610 years
- Logic device $MTTF_D$ = 398 years
- Output device $MTTF_D$ = 372 years

For the example 99% DC was selected for all components.

- The monitoring capability of the input device = 99%
- The monitoring capability of the logic device = 99%
- The monitoring capability of the output device = 99%

The formula for calculating Diagnostic Coverage (DC) is:

$$DC\ avg = \frac{\dfrac{DC_1}{MTTF_{D1}} + \dfrac{DC_2}{MTTF_{D2}} + \dfrac{DC_N}{MTTF_{DN}}}{\dfrac{1}{MTTF_{D1}} + \dfrac{1}{MTTF_{D2}} + \dfrac{1}{MTTF_{DN}}}$$

The $MTTF_D$ data that was calculated earlier is used along with the DC data from Table E.1 to determine the overall system DC.

$$DC\ avg = \frac{\dfrac{Input\ DC}{Input\ MTTF_D} + \dfrac{Logic\ DC}{Logic\ MTTF_D} + \dfrac{Output\ DC}{Output\ MTTF_D}}{\dfrac{1}{Input\ MTTF_D} + \dfrac{1}{Logic\ MTTF_D} + \dfrac{1}{Output\ MTTF_D}}$$

$$DC\ avg = \frac{\dfrac{99\%}{7610} + \dfrac{99\%}{398} + \dfrac{99\%}{372}}{\dfrac{1}{7610} + \dfrac{1}{398} + \dfrac{1}{372}}$$

DC avg = 99.0%

Since the overall system diagnostic coverage is 99%, the system has a DC range of High.

Determining Common Cause Failures Score

Common Cause Failures (CCF) can be avoided through the use of good engineering practices. The CCF scoring table can be found in table F.1 of ISO13849-1.

No.	Measure against CCF	Score
1	Separation / Segregation	15
2	Diversity	0
3	Design / Application / Experience	20
4	Assessment / Analysis	5
5	Competence / Training	5
6	Environmental	35
Total		80

ISO13849-1 requires the designer to achieve a CCF score of 65 or higher to prove that they have used good engineering and design practice to reduce the effect of systematic failures. The example here achieves a score of 80 because of the selected design and components.

Performance Level

The last step in the design verification process uses the calculated $MTTF_D$, calculated DC, and selected structure to determine if the Performance Level Achieved (PLa) meets or exceeds the Performance Level Required (PLr). In the example circuit, $MTTF_D$ is High, DC is 99%, and structure is Category 4. Therefore, the achieved performance level is e which exceeds the required Performance Level of d (from page 77).
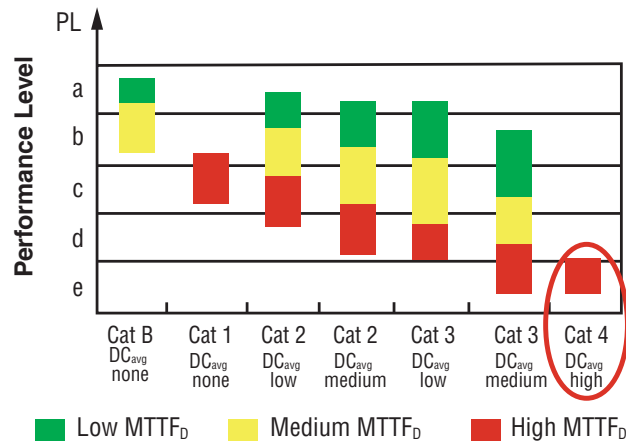
SISTEMA Software

The previous calculations can be cumbersome to perform and difficult to document. The DGUV in Germany publishes the SISTEMA "Safety Integrity Software Tool for the Evaluation of Machine Applications" which is free software that allows you to create devices and safety functions to verify the PL of the system. The user models the structure based on design architecture and populates the $MTTF_D$ or B_{10D} values, DC, and CCF data. Many manufacturers publish SISTEMA data libraries with all pertinent data for their products that can be loaded into the safety function. ROSS Controls' SISTEMA library can be found on the ROSS website.

This is an example of a SISTEMA report that shows the Performance Level that can be achieved using certain selected products. The SISTEMA software uses the product manufacturer's data through the use of imported libraries.

© 2021, All Rights Reserved. **ROSS** CONTROLS®

12	INSTALLATION AND VALIDATION

- Installation process & procedures according to manufacturer
- Validation that each safety function operates as intended
- Validation should include fault injection and functional testing

Safety products are shipped with operating instructions which include functional safety data (B_{10D}, DC, and CCF), installation information, initial test procedures, and technical specifications. All safety products must be installed according to the instructions and technical specifications to ensure proper operation. The example below is the test procedure for a ROSS M35 Series Safe Exhaust valve.

8.1. Test Procedure

1. *Only Solenoid A energized – Valve is faulted, supply is shut off, downstream air exhausts through port 3. Sensor A is off, sensor B is on.*

2. *Reset valve by de-energizing both solenoids – Valve is off, supply is shut off, and downstream air is exhausted through port 3. Sensors A & B are on.*

3. *Only Solenoid B energized – Valve is faulted, supply is shut off, downstream air exhausts through port 3. Sensor A is on, sensor B is off.*

4. *Reset valve by de-energizing both solenoids – Valve is off, supply is shut off, and downstream air is exhausted through port 3. Sensors A & B are on.*

5. *Solenoids A & B energized – Valve is on, air pressure is supplied downstream through port 2 and port 3 is shut off. Sensors A & B are off.*

6. *Solenoids A & B de-energized – Valve is off, supply is shut off, and downstream air is exhausted through port 3. Sensors A & B are on.*

Use the validation checklist to ensure that all plumbing, monitoring, and programming has been done correctly.

M35 Validation Test Procedure for Valve Operation and External Monitoring Logic

NOTE 1:	This validation test procedure should only be performed with an M35 valve that is known to be functioning properly. If basic valve function is in question please refer to Section 8 of the Product Operating Instructions for the Valve Test Procedure.
NOTE 2:	These procedures require fault simulation. It will be necessary to induce faults electrically by disabling a different solenoid or sensor at different times. This will be most easily done by disconnecting solenoid or sensor wires at the safety controller. **Also, be aware that this would only be possible with solenoid wiring option A.** See product data sheet.
NOTE 3:	Power for the sensor/LED board needs to be maintained throughout the entire procedure. Pins 1 and 3 must remain connected at all times during this validation test.
NOTE 4:	If FLT light is flashing and either or both solenoid lights are ON – it indicates the monitoring logic is not properly detecting this fault. The M35 unit should be powered down and monitoring logic reviewed and re-tested before putting into operation again.
NOTE 5:	If FLT light is flashing and both solenoid lights are OFF – it indicates the unit has an internal malfunction and should be replaced before continuing operation.
NOTE 6:	Port 2 should be connected to a small volume of approximately 20 cubic inches (~ 300 cubic centimeters) with a gauge or pressure sensor teed into the line.
NOTE 7:	Supply pressure will need to be supplied to inlet port 1. Insufficient supply flow and/or maximum soft-start settings (adjustment screw almost all the way in) could prevent detection of some induced faults during the validation test. Be sure not to restrict inlet flow with undersized piping/tubing. Also, begin testing with the soft start screw backed all the way out - counter-clockwise).
NOTE 8:	"-" Indicates no change from previous step.
NOTE 9:	Actuate Signal is the signal to switch on the solenoids either from a physical input switch or a software signal.

Step	Action	Sensor Power LED	Actuate Signal	Solenoid LEDs		Port Conditions	Outlet Pressure	Sensor Conditions		Safety System Fault	Valve Fault LED	Pass/Fail
			Sol A & Sol B	Sol A	Sol B		Port 2	Sensor A	Sensor B			(P/F)
1	Energize solenoids A & B	Green	ON	Green	Green	1 to 2 | 3	Pressure	OFF	OFF	No	OFF	
2	De-energize solenoids A & B	Green	OFF	OFF	OFF	1 | 2 to 3	None	ON	ON	-	-	
3	Disconnect solenoid signal wire from solenoid B	Green	OFF	OFF	OFF	1 | 2 to 3	None	ON	ON	No	OFF	
4	Attempt to energize solenoids A & B	Green	ON	-	-	-	-	-	-	Yes*	-	
5	Reconnect solenoid B	Green	-	-	-	-	-	-	-	-	-	
6	De-energize solenoids A & B	Green	OFF	-	-	-	-	-	-	-	-	
7	Reset the safety control system	Green	-	-	-	-	-	-	-	No	-	
8	Disconnect solenoid signal wire from solenoid A	Green	OFF	OFF	OFF	1 | 2 to 3	None	ON	ON	No	OFF	
9	Attempt to energize solenoids A & B	Green	ON	-	-	-	-	-	-	Yes*	-	
10	Reconnect solenoid A	Green	-	-	-	-	-	-	-	-	-	
11	De-energize solenoids A & B	Green	OFF	-	-	-	-	-	-	-	-	
12	Reset the safety control system	Green	-	-	-	-	-	-	-	No	-	
13	Energize solenoids A & B	Green	ON	Green	Green	1 to 2 | 3	Pressure	OFF	OFF	No	OFF	
14	Disconnect solenoid signal wire from solenoid A	Green	-	OFF	OFF	1 | 2 to 3	None	ON	ON	Yes*	-	
15	Reconnect solenoid A	Green	-	-	-	-	-	-	-	-	-	
16	De-energize solenoids A & B	Green	OFF	-	-	-	-	-	-	-	-	
17	Reset the safety control system	Green	-	-	-	-	-	-	-	No	-	
18	Energize solenoids A & B	Green	ON	Green	Green	1 to 2 | 3	Pressure	OFF	OFF	No	OFF	
19	Disconnect solenoid signal wire from solenoid B	Green	-	OFF	OFF	1 | 2 to 3	None	ON	ON	Yes*	-	
20	Reconnect solenoid B	Green	-	-	-	-	-	-	-	-	-	
21	De-energize solenoids A & B	Green	OFF	-	-	-	-	-	-	-	-	
22	Reset the safety control system	Green	-	-	-	-	-	-	-	No	-	

It is critical that every machine safety system be validated to ensure proper functionality. For example, there have been instances of where two "identical" machines were built, and one machine was validated, but the other was not because of time constraints and the assumption that the machines were "identical." Two years later someone noticed that the safety exhaust valve was not exhausting the air when it should have been. The root cause was that the way the valve was plumbed into the system the safety valve was bypassed. Validation would have caught this immediately.

ROSS CONTROLS®

13	PERIODIC TESTING AND MAINTENANCE

- Maintenance according to manufacturer requirements
- Annual testing of each safety function

The safety system must be maintained the same way the machine is maintained. If the safety system is changed or partially disassembled, validation is highly recommended to prevent any mistakes from occurring during re-assembly. In fact, most companies make this part of the preventative maintenance process when they perform line shutdowns or upgrades.

It is not typical for a machine to remain unchanged throughout the life of the equipment. Any changes should be evaluated to determine if a risk assessment is necessary. ANSI B11.0 offers Table 1 as requirements for new and existing machinery. A new risk assessment is required when non-comparable components are replaced or when a change in use of the machine is made.

**Table 1 — Requirements for new and existing machinery**

Scenario and Description	Requirement
1. New Machinery / System (created utilizing new or used components)	Perform a risk assessment to confirm the risks are at an acceptable level. Comply with current applicable standard(s).
2. Repair / Rebuild / Refurbish Machinery (utilizing comparable components)	No risk assessment required. Comply with applicable standard(s) existing at time of manufacture or initial installation.
3. Rebuild / Refurbish Machinery (utilizing non comparable components, changing the use of the machinery)	Perform a risk assessment to confirm the risks are at an acceptable level. Comply with current applicable standard(s) on any new hazards.
4. Reconfigure / Relocate Machinery (existing machinery is relocated or layout is reconfigured)	Perform a risk assessment on any hazards created by the new layout or change in spatial configuration, and to confirm the risks associated with the reconfigured machinery are at an acceptable level.
	Comply with current applicable standard(s) on any new hazards associated with relocation. All other (pre-existing) hazards comply with applicable standard(s) existing at time of manufacture or initial installation.
5. Modify, Reconfigure, or Remanufacture Machinery (machinery or components are added to or removed from an existing machinery system, or are modified to introduce new features)	Perform a risk assessment to confirm the risks are at an acceptable level. Comply with current applicable standard(s).

CLOSING COMMENTS

Safety system development should follow a systematic approach that is repeatable. The risk assessment is the starting point that determines the required system performance that is to be implemented. It is critical to spend time developing a detailed mitigation plan/functional specification that will guide the design and selection process. No safety system is complete until it has been validated and tested against the risk assessment and mitigation plan.

ANNEX A

Safety Valve Selection Flowchart

ROSS CONTROLS®
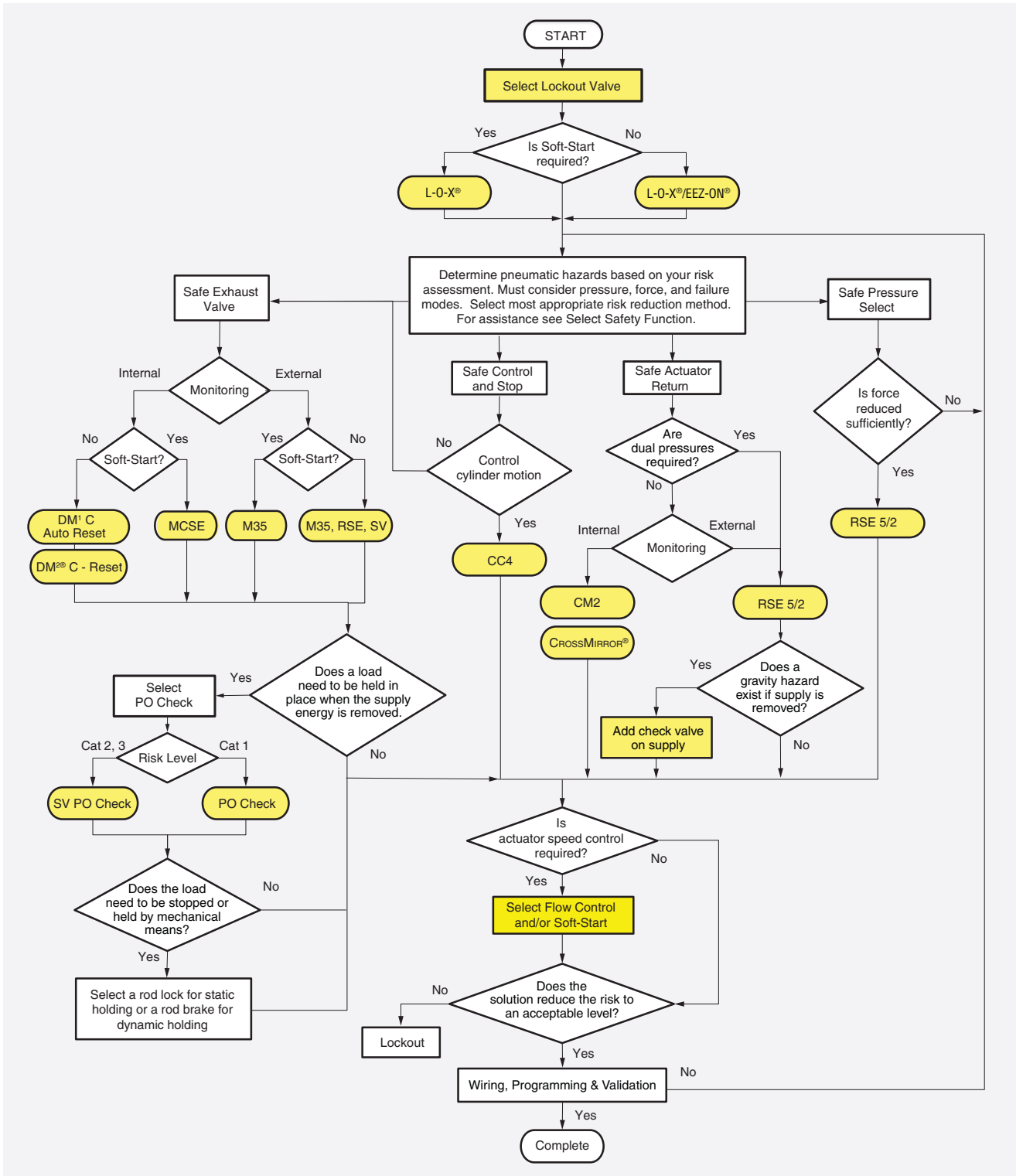
ANNEX B

Internal Versus External Monitoring

Mechanical power presses are inherently dangerous machines that have remained relatively unchanged in the past century. Their safety control systems including their pneumatic clutch/brake control systems have historically brought about new developments in machine safety with the introduction of dual valves, two hand control, and light curtain applications over the decades. During the post World War II boom the first steps were taken toward a control-reliable valve that could be used to safely control the supply of pneumatic energy to the clutch/brake of mechanical power presses.

Those first steps were to put two valves in series with no form of monitoring on the valves themselves. Without monitoring, valve faults could go undetected, and, since stopping time is critical in partial revolution presses, even just a sluggish valve could result in amputations or worse. The need to check that both sides of the redundant valve were, in fact, shifting every time became an important aspect of safety double valves.

Checking to see that both sides shifted was first done by arranging electromechanical limit switches on the bottom of the valves to follow the valve internals open and closed. The switches were hard-wired into the controls and "monitored" by the control system – this was the first dual valve with external monitoring. As with any guard interlock system of similar design, the switches could easily be bypassed to keep the press running if a switch stopped working or was out of alignment – unfortunately at the expense of safety. A German study from 2006 showed that 37% of protective measures on metalworking machines had been bypassed. Later forms of external monitoring included pressure-operated switches and electronic proximity switches but the same potential downside of bypassing the sensors existed.

In order to prevent the bypassing of the monitoring switches or sensors, internal monitoring was developed. This type of monitoring was accomplished using air pressure from the two independent sides of the valve operating on a monitoring spool. So long as the internals of the double valve shifted synchronously, the double valve would continue to work as needed to control the clutch/brake, letting the press operate. If the two sides were not in synch there would only be pressure from one side causing the monitoring device to trip into a latched position that would render the valve inoperative, but safe. The valve monitor would need to be reset to allow for further operation of the valve and the machine.

These internally-monitored double valves evolved over the years to incorporate a number of safety features within the valve itself, including:

- Fault detection
- Inhibit further operation until a reset occurs
- Anti-tie down of the reset (valve will not function if reset is engaged)
- Prevent operation if air is re-applied while power is on the solenoids

There is a trend in present-day safety valve manufacturing to provide double valves that are designed to be externally-monitored instead of internally-monitored. Manufacturers are adding pressure sensors or valve position sensors that can be monitored externally by a safety controller. Also, some valve manufacturers are using these sensors along with on-board electronic logic devices to create an electronic form of internal valve monitoring. This allows for internal monitoring but makes use of modern safety control technology within the device.

As computing technology has evolved, so have the electrical safety controllers used to control the dual safety valve. The controllers have become more powerful, smaller, and less costly utilizing redundant logic to monitor safe input devices and to redundantly shut off electrical outputs. Whereas, just 20 years ago programmable safety controllers were cost prohibitive except in the most complex machine safety systems, they are now common in all but the simplest machine guarding systems.

These advanced safety systems can be utilized to monitor safety double valves externally very effectively. The primary concern for bypassing safety circuits has been reduced by the use of valves with the sensors embedded in the valve with only an electrical connector interface taking the signals back to the safety controller and safety systems utilizing password protection and logging changes made to the safety control programs. This system, properly designed and installed, makes it possible for programmable control systems to externally monitor safety double valves very reliably in a way that is difficult to bypass.

The externally monitored valve will still block supply and exhaust downstream pressure in a faulted condition, but it is contingent on the monitoring system to:

- Detect the sensors indicating a fault
- Inhibit further operation until the valve fault has cleared and the system is reset
- Anti-tie down of the reset
- Prevent operation if air is re-applied while power is on the solenoids

Because the monitoring is so important with externally-monitored safety valves, ROSS has developed integration guides to assist with the logic and validation of the safety system with its externally monitored valves.

Basic Pneumatic Safety Circuit Elements


 ROSS CONTROLS®
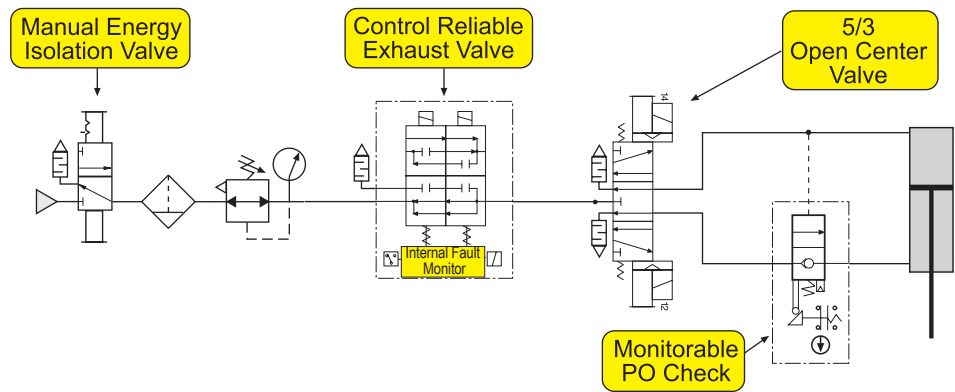
ANNEX C

Pneumatic Safety Systems and Cylinder Speed Control

Advancements in automation systems have led to tremendous increases in productivity for manufacturers. Machine controls utilizing sensing and verification of the product and position sensing of machine components allows for higher speeds of equipment and improvements in quality. Improvements in safety have also been achieved, greatly reducing the instances where operators are required to interact with the equipment during operation. However, automated machines are not autonomous. Material deviations or component malfunctions still require an operator to investigate and alleviate the situation. Because of this, operators and maintenance personnel must access potentially hazardous areas in the machine for functions such as clearing jams and other routine production related issues. These production related issues must of course be done in a safe manner; advancements in safety control systems are helping to make this possible.

Industry-accepted best practices for machine safety system design involve the completion of a risk assessment that looks at the tasks involved, foreseeable misuse, and component malfunction. The safety system should not cause damage or premature wearing of components. This damage could be caused by stop commands occurring at any point in the machine cycle or the reapplication of pneumatic energy causing rapid movement of components. Premature wear causes greater man-machine interaction due to it leading to a greater frequency of malfunctions and maintenance related activities.

Pneumatic safety, in the past, consisted of only a few primary components to stop and control motion. It was very common to use closed center valves in order to hold cylinders in place. This would trap pressure on both sides of the cylinder and generally leads to the desired effect. But this approach ignores three primary issues; slow or sticking valves, testing of the center position which is dependent on spring functions, and the effects of leakage when using spool valves. All three of these issues can result in potentially hazardous motion.

2/2 EEZ-ON® Valve

Slow valve response allows for motion to continue longer than anticipated. In normal operation a 5/3 closed-center valve may shift from one side to the other without the center position being used except during a safety event. An untested center position may result in a valve simply shifting as in normal operation. A closed-center valve traps pressure on both sides of the cylinder. Leakage on one side of the cylinder will result in movement. If the cylinder is mounted in a vertical orientation, a closed center valve will maintain pressure on the top side of the cylinder as well as on the bottom side. Leakage on the bottom side of the cylinder, especially in the event of a broken hose, will result in the cylinder being powered downward, not just moving due to gravity.

Leaks

Sluggish Valve
(varnished spool or
swollen seals)

Skips Center Position
(broken spring)
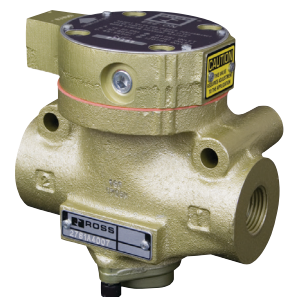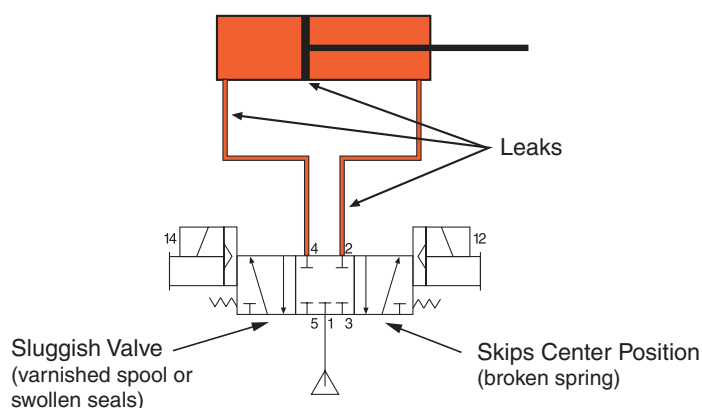
A sluggish valve might take longer to achieve the center position, thus, causing an increase in stopping time. Also, if the center position is only used for safety stops, it may not be tested regularly to make sure the valve will actually go to the center position when both solenoids are turned off. (What if a spring breaks in the valve?) Also, leaks in either cylinder line or in the cylinder piston seal can cause an unbalanced pressure condition in the cylinder allowing unexpected movement.

The issues of leakage and valve failures in closed-center valves led to the use of electrically operated safe exhaust valves used in conjunction with 5/3 open-center valves or 5/2 spring return valves. Safe exhaust valves are generally 3/2 normally-closed valves used to "dump" the air pressure from the downstream portion of the system. Because these safe exhaust valves are now being used as part of the safety system, they should also meet the same safety category requirements (or performance level) as the rest of the safety system. This configuration of safe exhaust valve and directional valve removes all pneumatic energy from the system so that even a malfunctioning valve would not result in continued motion due to pneumatic energy. Should there be concerns due to the speed and load requiring a more responsive and immobile stop, then pilot operated check valves would be used where required. With this arrangement the air supply is removed from both cylinder lines and the pilot operated check

valve(s) holds the cylinder in place by trapping pressure in the cylinder. With vertical cylinder arrangements where gravity is a factor it is usually only necessary to trap the pressure on the bottom end of the cylinder as opposed to trapping pressure on each end with horizontally oriented cylinders.

This use of a 3/2 control reliable electrically operated exhaust valve, 5/2 spring return or 5/3 open center cylinder valves, and pilot operated checks is the most effective safety circuit used in automated equipment. The end result is a safer machine that can be stopped at any point in its cycle, whether the cylinders are fully extended, fully retracted, or in a mid-position. There may be air trapped in one end and no air at the opposite end of the cylinder.

There are two primary reasons to stop the machine. The first is production related and the other is for maintenance purposes. Production related issues, including E-stop must utilize a risk assessment to ensure a safe state is reached and maintained to complete the required task. Maintenance issues will require lockout and steps must be taken to mechanically block the machine from moving and release any trapped pressure that had been selectively trapped for the purposes of affecting a safe stop.

The next step after the work is completed is to safely re-energize the machine. The re-application of air is an event that should not cause unexpected motion or cause what is otherwise avoidable damage to the machine. The old saw is, "When in doubt meter out." By using a flow control to reduce air flow out of a cylinder you can control the speed of the cylinder no matter how fast air is added to the opposite side. This is especially true to prevent meter-in slip-stick issues caused by a combination of friction, flow, volume, and load. This meter out assumption goes away with safety systems that remove the primary air supply and the air from all or parts of the cylinder. In this case there is no air left in the cylinder to meter out which can result in a run-away cylinder when air is re-applied or during the first cycle of the valve and cylinder.

Another possible solution for this is to meter into the cylinder. By using a flow control to limit the air flow into the cylinder you can control the motion. This is practical for most applications except where friction, flow, volume, and load create a slip-stick issue. Also, if a vertical load is enough to overcome the break-away friction of the cylinder seals, then a metering-in device on the top end may not have the speed limiting effect desired as the force of gravity alone will cause the cylinder to fall unless air is present in the bottom end of the cylinder and a meter out device is used.

An alternative to metering-in is to meter the entire system as a whole when air pressure is first applied after a safety event or even a normal shut-down. This is known as a soft start because the air pressure rises slowly until an adjustable preset point is reached before full line pressure is then supplied downstream to all components. Advantages are that the downstream components will move slowly into place and individual flow control components may not be required in all locations. There are devices available to soft start the whole system or just at the point-of-use. A soft start device coupled with meter-out flow controls at the actuators seems to be an ideal solution at first glance and can be in some cases.

PROBLEMS WITH SYSTEM-WIDE SOFT-START
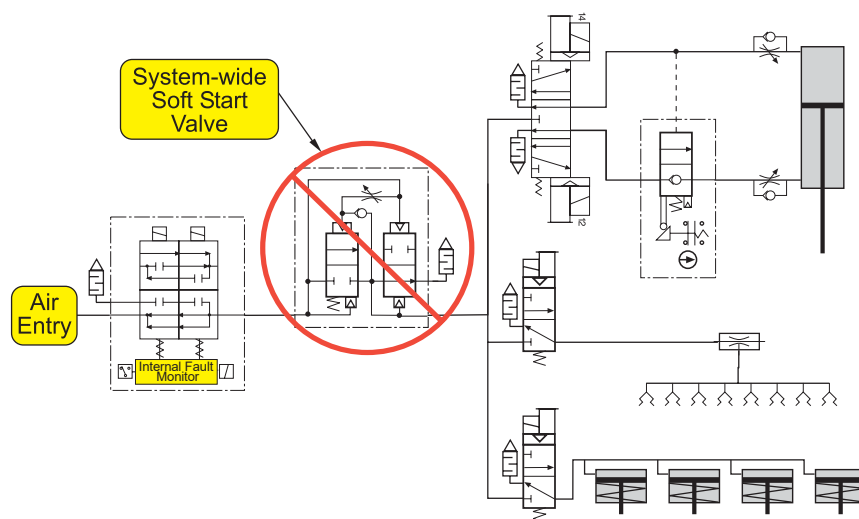
System-wide soft start can be problematic. In this example circuit with solenoid pilot valves downstream, the valves must remain switched off at least until minimum operating pressure is reached, otherwise they may not shift properly. This also means that the cylinders will not start softly, but will immediately see full pressure when the valves are switched on.

Additionally, when items such as venturi type vacuum generators are present they will act like a leak in the system which could prevent the soft start valve from switching to full flow. Also, supplying the suction cups and clamping cylinders from the safety exhaust valve can cause an additional hazard of possibly dropping material when a safety stop or e-stop is initiated. A solution is to use point-of-use soft start and move the supply for the vacuum generator and clamping cylinders upstream of the safety exhaust valve.

The overall effect of a soft start device is entirely dependent upon the actuator valves, the position of the cylinders when stopped, and auxiliary devices such as flow controls and pilot operated checks. The first consideration is determining where air is removed or trapped during normal operation of the safety system. The second consideration is to determine where air is removed or trapped during a component malfunction as required by the risk assessment.

When pneumatic energy is re-applied (assuming no electrical signals have already been re-applied, especially with the use of

ROSS CONTROLS®

direct solenoid valves) all actuators controlled by 5/2 spring return valves will move into their de-actuated position slowly and will also move at the proper speed when the valve is initially energized. The machine returns to its normal at rest condition in an orderly, safe fashion. If the spring return valve were to malfunction, the cylinder may move in the wrong direction when air is re-applied but would do so at a reduced speed.

However, in many continuous process machines, returning to an at-rest condition is not an option. Cylinders must stop in their location and remain there when pneumatic energy is re-applied. In these applications 5/3 open center valves with pilot operated checks are routinely used and system-wide soft start will have no affect whatsoever because the pressure will only build up slowly to the valve which, at rest, blocks flow further downstream. Because of this, the pneumatic supply to the actuator valves will be at full pressure (while the cylinder has no pressure on at least one end) when the valves are first actuated causing rapid initial motion; unless point-of-use soft start devices or meter-in flow controls are used.

The primary difference between a meter-in flow control and a point-of-use soft start is that the soft start allows full flow after a pre-set ramp-up pressure has been achieved. Also, we must not forget the problems with metering in; slip-stick cylinder motion can wreak havoc on machine processes. However, when utilizing point-of-use soft start devices, in conjunction with meter out flow controls, the re-application of pneumatic energy and cylinder speed is controlled while not inhibiting the normal, smooth cycling of the cylinder. The cylinder is controlled during every aspect of machine operation.

Another point to be made for not using system-wide soft start is that the design of these devices is to slowly bypass air downstream until a certain pressure is reached and then to open completely to allow full line pressure and flow through the valve. This bypass flow is usually limited, although adjustable, over the range of the limitation, and unfortunately pneumatic systems are generally plagued by leaks. Any system such as this that relies upon a build-up of pressure before fully opening will have an Achilles heel in that if the leaks downstream of the soft start valve are equal or greater than its bypass flow capability, the soft start valve will not open fully. Some machine processes such as blow-offs and vacuum generators constantly consume air, too. This consumption is virtually seen as a leak in a soft start system. In systems like this it is absolutely necessary to add in complexity for isolating the leaky areas of the system until after the soft start has completely opened for full flow or use point-of-use devices.

Even though applying a soft start device upstream of an entire machine circuit is often recommended, in many cases this is not the best solution. Whereas, utilizing point-of-use soft start in conjunction with flow controls limits the initial re-application of energy where needed and provides the most consistent solution for speed control for machines that must maintain position during a safety event and continue operation once the pneumatic energy is re-applied. This is especially true for safety systems that include the use of a control reliable safe exhaust valve along with a 5/3 open center directional valve to control cylinder operation.

POINT OF USE SOFT-START WITH CONTROL RELIABLE SAFE EXHAUST
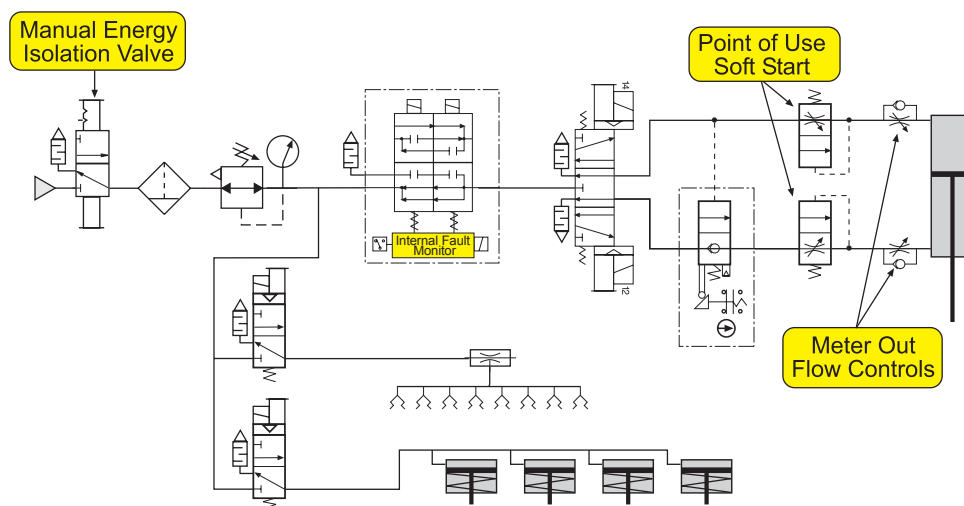
ANNEX D

Automatic Reset Versus Manual Reset – DM¹ & DM²®

ROSS offers both a DM¹ Series and a DM²® Series of safety valves. The primary difference is that, should a fault occur in the valve, the DM¹ safe exhaust valves can reset automatically, and the DM²® requires a dedicated reset signal in order to return to its ready-to-run state. But what does this difference really mean?

First, we should define what is considered a fault within the ROSS DM valve Series. Being a redundant valve with two sets of internal elements that must shift in synchronization in order to supply air downstream, a fault occurs when one of the internal elements moves out of synch with the second element by more than the designed discordance time. This results in the supply of air being blocked, the downstream pressure being bled to exhaust, and the element that is out of synch being unable to complete its return shifting function until the valve is de-energized and reset.

Auto reset means that, should a fault occur, the valve will return to a ready-to-run state once both main solenoid coils are de-energized and the internal elements return to the home state due to the internal valve dynamics. While this appears to be very convenient, the potential issue is that a fault could go unobserved by the operator or control system if the fault occurs during certain operations of the machine. Because of this, the ROSS DM¹ Series valves are available with an optional status indicator switch for additional diagnostics.

If using a DM²® Series valve, as opposed to a DM¹ Series valve, reset does not occur automatically when de-energizing the valve, but requires an actual dedicated reset procedure to un-latch after a fault. This means that when a fault occurs the valve will maintain a latched out condition until electrical power is removed from the main solenoids and a separate, dedicated reset signal is applied. This reset procedure requires air pressure to be present at the inlet of the valve. The inlet pressure is used by the reset solenoid valve to return all internal moving parts to the home position and puts the valve back into the ready-to-run state. The reset signal must be momentary because the DM²® has an anti-tie-down feature built into it to prevent inadvertent or intentional attempts to continuously override the latch-out feature. As long as the reset signal is present, valve operation cannot be initiated, and the valve will remain in the faulted state. This anti-tie-down feature prevents a person from holding the reset signal in place and, in essence, converting the valve into an automatic reset valve.

Another important feature is that if the DM valve, both Series DM¹ and Series DM²®, is energized and not faulted, removal of supply pressure will be sensed by the valve and it will fault accordingly. Main supply should never be able to be removed and re-applied without causing the valve to fault and go to the safe mode as long as the valve is energized. The resulting fault is the same if the main solenoids are energized prior to supplying air to the valve. This fault operation is very similar to how a safety monitoring relay works. When the supply power is lost the safety monitoring relay will go into its safe mode. You would then have to go through a startup procedure which would include a reset. No machine safety system should allow a machine to restart automatically.

These features allow the DM Series valves to meet the standard requirements for Energy Sources as well as Interruption of Energy Sources in ANSI B11.0. The ANSI B11.0 Safety of Machinery, General Requirements and Risk Assessment standard is quoted below but similar requirements are found within machine safety standards throughout the world.
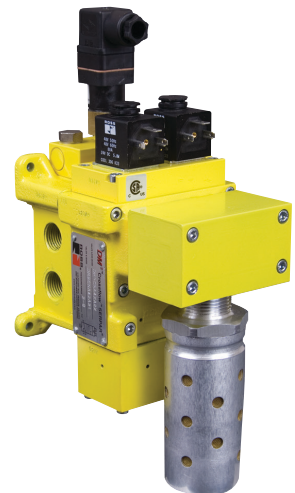
DM²® Series C Double Valve

7.3.4 Energy sources

Activating an internal or external energy source, including starting after a power interruption, shall not result in a hazardous condition.

7.3.5 Interruption of energy source

Machinery shall be designed to prevent hazardous conditions resulting from interruption or excessive fluctuation of the energy source (e.g., electrical, pneumatic, hydraulic). In the event of loss of energy, the following minimum requirements shall be met:

• the stopping function of the machine shall remain available;

• all devices whose permanent operation is required for safety shall operate in an effective way to maintain safety (e.g., locking, clamping devices, cooling or heating devices, braking); hazardous stored energy shall be safely controlled or dissipated by the operator and the control system.

ROSS CONTROLS®

DM¹ without indicator switch:

• Energization faults may be detected by an operator or controls system due to the machine operation not occurring properly, i.e., some part of the machine doesn't operate as expected. This situation can be observed by the operator and/or possibly by the controls system, indirectly. The operator may not know it was a valve fault, specifically, that caused the issue and normal operation could occur on the next machine cycle initiation.

• De-energization faults may not be detected by the operator or control system if the machine operation occurs normally and the fault clears prior to the next operation of the valve. In other words, the valve is being de-energized and we expect it to be going to the off position anyway, which outwardly results in the same condition – inlet shut off and outlet open to exhaust. Therefore, this fault could go undetected.

DM¹ with indicator switch:

• Same as above except that the indicator switch will change state during the fault condition and can be captured (recognized) by the control system so that the fault is annunciated and, therefore, can be acknowledged by the operator.

DM²® without indicator switch:

• Energization faults may be detected by an operator or controls system due to the machine operation not occurring properly, i.e., some part of the machine doesn't operate as expected. Also, the valve will latch in the faulted condition and will require a reset before proper operation can resume. The operator may not know, specifically, that it is the valve that faulted because there is no status indicator switch to signal a fault.

• De-energization faults may not be detected by the operator or control system if the machine operation occurs as normal. However, the valve will be latched in the faulted condition and will require a reset before proper operation can resume. The operator may not know, specifically, that it is the valve that faulted because there is no status indicator switch to signal a fault.

DM²® with indicator switch:

• Energization faults may be detected by an operator or controls system due to the machine operation not occurring properly, i.e., some part of the machine doesn't operate as expected. However, the valve will be latched in the faulted condition and will have to be reset before proper operation can resume. The status indicator switch will indicate that the valve is faulted and needs to be reset.

• De-energization faults may not be detected by the operator or control system if the machine operation occurs as normal. However, the valve will latch in the faulted condition and will have to be reset before proper operation can resume. The status indicator switch will indicate that the valve is faulted and needs to be reset.

ONLINE RESOURCES
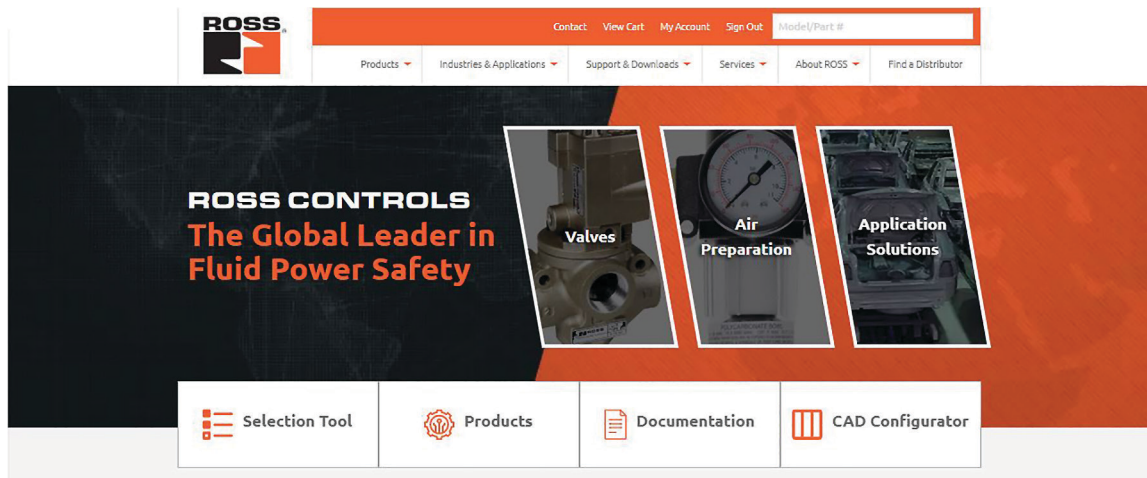
Safety Online Selection Tool

The ROSS Safety Tools will simplify your process of selecting the best product to fit your application, independent of your familiarity with Safety Valves and ROSS CONTROLS. To help your navigation, additional product feature explanations are available throughout the process. By simply selecting your criteria, product options are provided with a link for additional information such as data sheets, technical documentation and 3D models. These tools are available at ROSS' website and can be used from desktop and mobile devices.

Visit ROSS' website at www.rosscontrols.com to access the Hydraulic Safety Valve, Pneumatic Safety Valve or Press Controls Selection Tool.
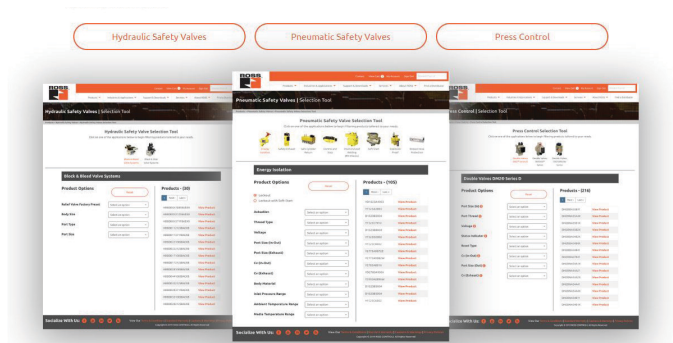
Safety Product Data for SISTEMA Library Users
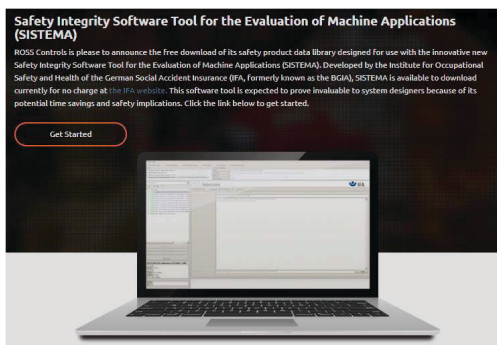
Safety product data library is designed for use with the innovative SISTEMA software tool (Safety Integrity Software Tool for the Evaluation of Machine Applications). Developed by the Institute for Occupational Safety and Health of the German Social Accident Insurance (IFA, formerly known as the BGIA), SISTEMA is available to download for no charge at the IFA web site. This software tool is expected to prove invaluable to system designers because of its potential time savings and safety implications. The free software tool and data library will help ensure compliance with the EN ISO 13849-1:2015 standard.

Most of the ROSS safety products have SISTEMA files that are located in the ROSS SISTEMA library, to help users in the design and verification process of complete safety solutions.

To download a copy of ROSS' Safety Product Data for the SISTEMA Library, visit www.rosscontrols.com.

2D Drawings & 3D CAD Models

To assist you with piping and connectivity designs, designers and engineers all over the world can preview and download product data in more than sixty (60) different CAD and graphic formats and validate their designs in their engineering design systems.

You can find drawings and models on individual product pages or from the Technical Tools Menu – both on www.rosscontrols.com.
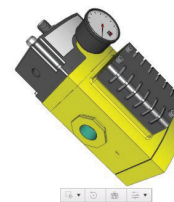
Intergration Guides
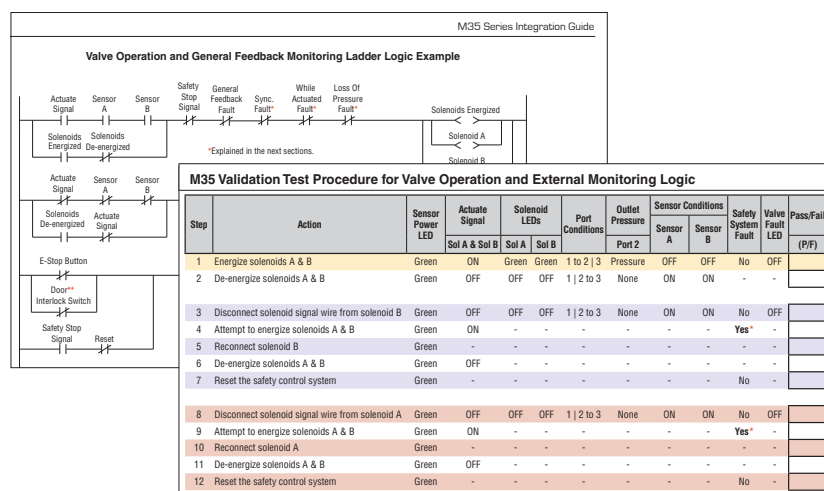
In addition to the Installation Instructions that are included with the product, Integration Guides for specific safety valves are available to provide important information necessary to integrate your new safety valve into your system.

Integration Guides include:
- Pneumatic Schematics
- Connector Pinouts
- Operation & Monitoring Requirements
- User Control Circuits
- Test Procedures

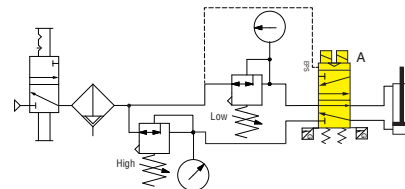Visit www.rosscontrols.com.

Training

ROSS offers a variety of fluid power related training topics to help you increase your base knowledge.
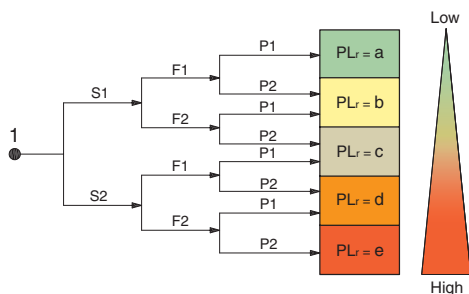
Available Training includes:
- Fluid Power Basics
- Fluid Power Safety
- Total Machine Safety
- Customer Specific

Consult ROSS.

Services

If you are looking for help beyond our available online resources and training for your team, ROSS offers several services to ensure your applications will achieve the performance and safety levels you need.

Services offered include:
- Lock-out/Energy Isolation Circuit Analysis
- Emergency Stop Circuit Analysis
- Category & Performance Level Estimation Analysis
- Fluid Power Application Reviews

Consult ROSS.

ROSS
a global family

			Tel	Website
AMERICAS	**USA**	**ROSS** CONTROLS	Tel: +1-248-764-1800	www.rosscontrols.com
		AUTOMATIC VALVE	Tel: +1-248-474-6700	www.automaticvalve.com
		ROSS DECCO	Tel: +1-248-764-1800	www.rossdecco.com
	Brazil	**ROSS** BRASIL	Tel: +55-11-4335-2200	www.rosscontrols.com.br
	Canada	**ROSS** CANADA	Tel: +1-416-251-7677	www.rosscanada.com
EUROPE	**France**	**ROSS** FRANCE SAS	Tel: +33-(0)1-49-45-65-65	www.rossfrance.com
	Germany	**ROSS** EUROPA	Tel: +49 (0)6103-7597-100	www.rosseuropa.com
		manufactIS	Tel: +49 (0)2013-16843-0	www.manufactis.net
	United Kingdom	**ROSS** PNEUMATROL (FKA ROSS UK Ltd. and pneumatrol Ltd.)	Tel: +44 (0)1254 872277	www.rossuk.co.uk www.pneumatrol.com
ASIA & PACIFIC	**China**	**ROSS** CONTROLS (CHINA) Ltd.	Tel: +86-21-6915-7961	www.rosscontrolschina.com
	India	**ROSS** CONTROLS INDIA Pvt. Ltd.	Tel: +91-44-2624-9040	www.rosscontrols.com
	Japan	**ROSS** ASIA K.K.	Tel: +81-42-778-7251	www.rossasia.co.jp

Connect with Us

To meet your requirements across the globe, ROSS distributors are located throughout the world. Through ROSS or its distributors, guidance is available for the selection of ROSS products, both for those using fluid power components for the first time and those designing complex systems.

For a current list of countries and local distributors, visit ROSS' at www.rosscontrols.com.