Introduction:

The following standards references are intended for informative purposes. They represent parts of the standard that reference one of three things:

1. General safety issues that support pneumatic safety requirements
2. General safety issues that support Ross product features and benefits
3. Specific pneumatic safety requirements

This is in no way a condensed version of the standards. Each standard contains much more information that is safety or pneumatic related but these are the main points that are needed to promote pneumatic safety and Ross safety products.

The crucial points to discuss specific valve requirements are in **bold**. I have inserted some brief notes that are in (***parenthesis, bold, and italics.)***

Table of Contents:

ISO 4414	Pneumatic Fluid Power	2
ANSI Z244 (CSA Z460)	Lockout and Alternative Measures	4
ANSI B11.0	General Safety Requirements and Risk Assessment	6
ANSI B11.1	Safety Requirements for Mechanical Power Presses	10
CSA Z142-10	Code for Power Press Operation	11
ANSI B11.19 (CSA Z432)	Performance Criteria for Safeguarding	13
ANSI B11.TR6	Safety Control Systems Design	15
PMMI/ANSI B155.1	Packaging Machinery Standard	23
ISO 14118 (EN 1037)	Safety of Machinery – Prevention of Unexpected Start Up	25
ISO 13849-1 & 2	Safety of Machinery – Safety Related Parts of Control Systems	27
EN 692	Machine Tool – Mechanical Presses – Safety	34
EN 422	Plastic & Rubber Machines – Blow Moulding Machines – Safety	36
ANSI B65-1:2011 &	Graphic Technology Safety Requirements	
ISO 12643-1:2009 Part 1	General Requirements	39
Part 5	Stand Alone Platen Press	42
ISO 13042:2009	Hollow Glass Machine Safety Requirements	
Part 1	Gob Feeder	43
Part 2	Handling Machines for Feeding	44
Part 3	IS Machines	45
Part 5	Presses	46
ISO 13851:2002	Safety of machinery -- Two-hand control devices	48

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

(This is being adopted by the NFPA as T2.25.1 R2 in its entirety in 2011. It is a Type B standard and applies to all machinery unless superseded by a Type C machine specific requirement.)

Scope: Deals with significant hazards associated with pneumatic fluid power systems and specifies principles to apply in order to avoid these hazards.

3.2 **Emergency Control**
Control function that brings a system to a safe condition

5.1.1 **Risk assessment** … 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.

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

5.2.2.4 Loss of pressure or pressure drop shall not expose persons to a hazard and should not damage the machinery.

5.2.7 Control or Energy Supply
Whatever the type of control or energy supply used (eh electrical, pneumatic) the following actions or occurrences (whether unexpected or intentional) shall not create a hazard:

a) Switching the supply on or off
b) Reducing the supply
c) Cutting off the supply
d) Restoring the supply

5.2.8 Positive Isolation from Energy Sources ***(Requires LOX)***
The system shall be designed to facilitate positive isolation from energy sources (see ISO 12100:2010, 6.3.5.4). In pneumatic systems, this can be done, for example, by

— Isolating the supply with a suitable shut off device, which should be lockable, and shall be accessible without causing a hazard

5.2.10 Unexpected start up
In order to prevent unexpected start-up, precautions shall be taken in accordance with ISO 14118.

5.2.11 Uncontrolled actuator movement
If rapid opening of the shut off valve can produce uncontrolled movement of the actuators, a soft-start/slow-start valve shall be incorporated.

5.4.3.8 Three position valves
Systems that use three position valves, particularly those with a closed center position, should be analyzed to determine if the leakage from the system and/or leakage through a valve can result in undesired effects, such as unexpected cylinder movement.

5.4.5.11 Failure of hose assemblies and plastic piping ***(Requires Hoze-Fuze)***
5.4.5.11.1 When failure of a hose assembly or plastic piping constitutes a whiplash hazard, it shall be restrained or shielded by suitable means. In addition**, an air fuse for compressed air should be mounted.**

5.4.6.8 Two hand controls
If two hand controls are provided, they shall be designed and applied in accordance with ISO 13849.

5.4.6.15 Emergency controls
The system shall incorporate an emergency stop in accordance with ISO 13850 or emergency control.

ANSI/ASSE Z244.1-2003 (R2008) & CSA Z460
Control of Hazardous Energy Lockout/Tagout and Alternative Methods

(This standard applies to all machines. It is what requires lockout and explains the requirements for alternative methods of lockout.)

1.2 Purpose
The purpose of this standard is to establish requirements and performance objectives for procedures, techniques, designs and methods that protect personnel where injury can occur as a result of the unexpected release of hazardous energy. Unexpected release of hazardous energy can include any unintended motion, energization, start-up or release of stored energy, deliberate or otherwise, from the perspective of the person(s) at risk.

Lockout/tagout is the primary method of hazardous energy control. When the tasks specified in 1.3 are routine, repetitive, and integral to the production process, or traditional lockout/tagout prohibits the completion of those tasks, alternative methods of control that are based on risk assessment (5.4.1) and that provide effective personal protection shall be used.

4.2 Energy isolating devices
Machines, equipment and processes shall be designed, manufactured, supplied, and installed with energy isolating devices to enable compliance with the requirements in 5.3. Consideration shall be given to the intended use of the machine, equipment or process. Devices shall be capable of controlling or dissipating hazardous energy, or both. The devices should be an integral part of the machine, equipment or process.

4.2.3 Capability
Energy isolating devices shall be capable of either being locked or otherwise secured in an effective isolating position.

5.4 Alternative methods
When lockout/tagout is not used for tasks specified in 1.3 that are routine, repetitive, and integral to the production process (see 1.2), or traditional lockout/tagout prohibits the completion of those tasks, then an alternative method of control shall be used. Control options such as those specified in 5.4.3 through 5.4.6 shall be used following the hierarchy in 5.4.2 to ensure effective protection.

Selection of an alternative control method by the user shall be based on a risk assessment of the machine, equipment, or process as specified in 5.4.1. The risk assessment shall take into consideration that existing safeguards provided with the machine, equipment or process may need to be removed or modified to perform a given task.

5.4.1 Risk assessment
For purposes of this standard, risk assessment is intended to be a qualitative estimation and does not require quantitative probabilistic analysis and shall include the following elements:

a) identification of the tasks (including foreseeable misuse) and related hazards;
b) qualitative estimation of exposure and severity to determine the level of risk;
c) assessment and evaluation of the risk;
d) identification of potential control actions considered to reduce the risk of each hazard;
e) identification of control actions selected as the best protective alternative;
f) verification of the effectiveness of the selected alternative; and
g) documentation of the risk assessment process.

5.4.2 Hierarchy of alternative control implementation

A hierarchical process shall be employed in the selection of alternative control methodologies in the following order of preference:

a) **Eliminate the hazard through design;**
b) **Use engineered safeguards as specified in 5.4.3;**
c) **Use warning and alerting techniques as specified in 5.4.4;**
d) **Use administrative controls (such as safe work procedures, practices, and training) as**
e) **specified in 5.4.5 and 5.4.6, respectively; and**
f) **Use personal protective equipment as specified in 5.4.7.**

5.4.3.2 Control circuit integrity

When control circuits are used as part of the safeguarding system intended for use during setup, troubleshooting, or other tasks requiring energization or partial de-energization, the level of risk must be determined. The level of risk is determined by identifying the involved tasks, hazards, potential severity of injury and exposure. The greater the severity potential for injury, the more frequent the access, and the more direct the contact with the hazard, then the greater the risk. **The control system selected must be of sufficient integrity to provide protection for the established level of risk**.

NOTE – Typical methods in increasing order of integrity are:

a.) Negligible Risk Potential – Infrequent exposure and low injury severity.

A single channel circuit of industrial rated components that mechanically or electro-mechanically isolates the incoming power from the motor, solenoid or other actuating device that produces hazardous motion.

b.) Low Risk Potential – Frequent exposure and low injury severity

A dual channel circuit of industrial rated components that mechanically or electro-mechanically isolates the power and is inspected as part of normal operations to ensure integrity of the system.

c.) Medium Risk Potential – Any exposure to serious injury

A dual channel circuit (one of which is hardwired) of industrial rated components that is selfchecking or monitored through the use of a safety relay or safety (multiple channel) PLCs to ensure integrity and performance of the control circuits. These systems typically have redundant interlock switch safety contacts, redundant isolation through positively guided electro-mechanical relays, and are monitored or self-checking through use of a safety relay or safety PLC that is designed and installed to a high level of integrity through the selection of robust components.

NOTE – Single Channel general purpose PLCs do not satisfy this requirement

d.) High Risk Potential – Any exposure to a catastrophic injury

A control reliable dual channel hardwired circuit of industrially-rated components that satisfies the design features as specified in ANSI B11.19 (with redundant door interlock switches etc.), using a safety relay or safety PLC to ensure integrity and performance of the safeguarding system. This system shall be designed to ensure protection equivalent to a mechanical disconnect switch or master shut-off valve.

NOTE – Under all circumstances, the individual shall have exclusive personal control over the means to maintain the state of the control circuit in a protective mode. Examples include personnel safety keys or other locking devices.

ANSI B11.0-2010
Safety of Machinery – General Requirements and Risk Assessment

(This is an "A level" standard that can apply to a broad range of machines. It requires a risk assessment, the use of the control hierarchy, and the control integrity of the safety system mitigates the risk level to an acceptable level.)

3.11 Control reliability: The capability of the (machine) control system, the safeguarding, other control components, and related interfacing to achieve a safe state in the event of a failure within their safety-related functions.

3.12 Control System: Sensors, manual input and mode selection elements, interlocking and decision making circuitry and output elements to the machine actuators, operating devices, and mechanisms.

3.47 Monitoring: The checking of system components to detect the failure of a component, subassembly, or module that affects machinery safety, including the safety-related functions.

3.61 Reasonably foreseeable misuse: The use of a machine in a way not intended by the supplier or user, but which may result from readily predictable human behavior.

Informative Note: For example, a risk assessment should address the following human factors (not intended as an all-inclusive list).

- Inappropriate actions as a result of mistakes, errors, and poor judgment, excluding deliberate abuse of the machine;
- Inappropriate actions or reactions taken in response to unusual circumstances such as equipment malfunction;
- The tendency to take the ―path of least resistance‖ in carrying out a task; and
- Misreading, misinterpreting or forgetting information.

3.67 Residual risk: The risk remaining after risk reduction measures (protective measures) are taken.

3.81 safety-related function: That portion of the control system or safeguarding device that eliminates exposure to a hazardous situation or reduces risk to an acceptable level.

Informative Note 1: The control system portion (part) of the safety-related function is frequently abbreviated as ―SRP/CS‖ (safety related parts of the control system).

Informative Note 2: For additional information, see ANSI B11.TR6, IEC 61508, IEC 62061, and ISO 13849.

6 The risk assessment process

6.1 General
Suppliers and users are required to perform a risk assessment (see clause 5).

6.1.2 Goal
The goal of risk assessment is to reduce risks to an acceptable level(s). The risk assessment process shall continue until acceptable risk is achieved (see 6.7).

6.2 Prepare for and set scope (limits) of the assessment
Suppliers and users either jointly or separately shall adequately prepare for, set limits on, document the parameters of the assessment, and establish the level(s) of acceptable risk.

6.3 Identify tasks and hazards
The reasonably foreseeable tasks and associated hazards shall be identified for the applicable phases of the lifecycle of the machine. …

Identifying hazards shall take into account the different tasks, operating modes and intervention procedures, in particular when the machine does not perform the intended function (i.e., it malfunctions) due to a variety of reasons, such as:

- variation of a property or of a dimension of the processed material or of the product;
- failure of one (or more) of its component parts or services;
- external disturbances (e.g., shocks, vibration, electromagnetic interference);
- interruption of its power source.

6.4 Assess initial risk

6.4.2.1 Assess severity
Severity of harm addresses the degree of injury or illness that could occur. When estimating severity, the highest credible level of severity of harm shall be selected.

6.4.2.2 Assess probability
Occurrence probability is estimated taking into account the frequency, duration and extent of exposure, speed of occurrence, human errors, training and awareness, and the characteristics of the hazard. When estimating probability, the highest credible level of probability shall be selected.

6.4.3 Derive risk level
For each hazard or task/hazard pair, an initial risk level shall be derived using the risk scoring system. Once the initial risk is estimated, the risk level can be compared to acceptability levels. If the risk is not acceptable, the next step is to reduce the risk.

6.5 **Reduce risk**

6.5.1 **Use the hazard control hierarchy**
Risks can be reduced by reducing the potential severity of harm presented by the hazard, improving the possibility of avoiding the harm, and/or reducing the need for access to the hazard zone. In selecting the most appropriate risk reduction measures, apply the following principles in the order (6.5.1.1 through 6.5.1.6) as they appear below.

6.5.1.1 Eliminate by design
6.5.1.2 Substitution
6.5.1.3 Guards and safeguarding
6.5.1.4 Awareness devices
6.5.1.5 Procedures and training
6.5.1.6 PPE

6.6 Assess residual risk

6.7 Achieve acceptable risk
Risk reduction is complete when risk reduction measures are applied and acceptable risk has been achieved for the identified hazards.

6.8 Verify/Validate risk reduction measures

6.9 Document the process

7 Risk reduction methods

7.1 Access to machinery
Machinery shall be designed, constructed and used to allow access to the machine in order to enable all tasks to be carried out with acceptable risk. Where personnel are required to enter the machine, one or more means of protection shall be provided.

7.2 Control systems
The design of control systems which could include electronic, electromechanical, hydraulic or pneumatic components, shall comply with the principles and methods presented in 7.2.1 through 7.2.8. These principles and methods shall be applied singly or in combination as appropriate to the circumstances.

7.2.1 General
The design measures of the control system shall be chosen so that its safety-related performance provides a sufficient amount of risk reduction.

7.2.2 Zones
A machine or an assembly of machines may be divided into several control zones

7.2.9 Safety-related parts of control system

7.2.9.1 General
The design and performance of the safety-related parts of the control system (SRP/CS) shall be commensurate with the risk (see clause 6). The SRP/CS shall be appropriate for their intended use. The integrity of the safety components and/or systems shall be determined by the appropriate product, system, and/or application safety standard/technical report.

> Informative Note1: SRP/CS can be electrical, electronic, hydraulic, and/or pneumatic or any combination thereof (see ISO 13849). The SRP/CS may be composed of sensors, logic solvers and actuators. Examples of system standards/technical reports include: ANSI B11.TR4, ANSI B11.TR6, ANSI B11.19, NFPA 79, ISO 13849-1, ISO 13849-2, ISO 13849-100, ISO 13850, IEC 62061, IEC 60204-1, and IEC 61508.
>
> Informative Note 2: Different levels of risk reduction and performance are shown below in ANSI B11.TR6 Table 4. This table applies only to hardware and not software.

7.2.9.2 Stop functions
When pneumatic or hydraulic elements are incorporated into a safety stopping function, the circuit design and component selection shall be appropriate for the required level of safety performance. Devices that produce a hazard shall have power removed during a stop function, provided a greater hazard is not created in the process. Devices that are related to non-hazardous machine functions such as annunciators and awareness warning or visual devices do not need power interrupted.

7.7 Control of hazardous energy (lockout / tagout)

The machinery and/or machinery system shall be provided with adequate means to control hazardous energy in accordance with ANSI / ASSE Z244.1. Information to conform to NFPA 70E shall be provided. See also, 8.3.

7.9 Safeguarding
7.9.1 General
The guards, safeguarding devices, awareness devices, and safeguarding measures on machinery shall conform to the applicable ANSI B11 machine-specific (C-level) standard and/or ANSI B11.19.

7.9.2.6 Stopping time
When the performance of safeguarding relies on machine stopping time, the supplier shall provide information concerning the stopping time of the machine. See also, ANSI B11.19 and any of the relevant ANSI B11 machine-specific safety standards listed in 7.15.

7.11 Hydraulic and pneumatic (including vacuum) systems
All elements of the machinery, and especially pipes and hoses, shall be protected against abrasion, contamination, ultraviolet radiation, and mechanical or other damage.
Hydraulic systems shall conform to the applicable sections of NFPA/T2.24.1 R1-2000(R2005).
Pneumatic systems shall conform to the applicable sections of NFPA/T2.25.1 R2-2005.

7.11.1 **Safety shut-off and exhaust valve *(Requires LOX)***
An energy isolating device shall be provided to shut off and release pressure from the various systems and shall:

- **be located outside of the hazardous area(s);**
- **be capable of being locked in the OFF (closed)position only;**
- **be easy to operate (e.g., a simple pull/push action for pneumatics);**
- **have a properly sized exhaust port equal to or greater than its supply port;**
- **have a pressure indicator (i.e., a gauge), that is visible to the operator to indicate that the line is relieved of pressure (see also, 7.7 and 7.11.2).**

Sintered metal or paper mufflers shall not be used on energy isolation devices.

7.11.3 Air valve mufflers
Air valve mufflers for safety systems and air dumps shall have sufficient capacity so as not to restrict the exhausting of the system and shall not be prone to contamination over time. Paper or bronze sintered elements shall not be used.

6.4.4.1 Clutch/brake valve

The clutch/brake operating valve(s) for a part revolution clutch press shall be designed and constructed to prevent a significant increase in the normal stopping time due to any single failure within the operating valve mechanism and to inhibit further operation if such failure does occur.

6.4.4.2 Clutch/brake air–valve exhaust systems

Exhaust systems used with clutch/brake air valves
shall be designed to prevent a significant increase in the normal stopping time of the press.

6.4.6 Direct drive brake system

The brake system for direct drive presses shall be designed and constructed to prevent a significant increase in the normal stopping time due to any single failure within the operating valve mechanism and to inhibit further operation if such failure does occur.

6.4.6.1 Brake air–valve exhaust

When used, an exhaust valve shall be designed to prevent a significant increase in the normal stopping time of the press.

6.8 Pressure vessels

All pressure vessels with an inside diameter greater than 152 mm (6 in) and used in conjunction with presses shall conform to Section VIII of the ASME Boiler and Pressure Vessel Code, and be equipped with a safety vent valve in the event of over or under pressurization.

C.4 Maximum Stop Time Test

The purpose of performing a maximum stop time test is to establish the distance for the location of the safeguarding from the point-of-operation. This test should be performed during the downward motion (mid-stroke) of the slide. Factors to consider when conducting this test include but are not limited to:

- Mode of operation;
- Speed of the slide on variable speed machines;
- Weight of the upper die;
- Counterbalance pressure;
- Clutch or brake performance;
- Control valve response;
- Servo system tuning.

Press safety valve — a pneumatic or hydraulic valve with dual body and solenoids and with a self-contained monitoring system that inhibits further operation of the valve in the event of a failure.

Safety shut-off and exhaust valve — a means of shutting off and exhausting air from a system during maintenance.
Note: *This device can also be locked in the OFF position.*

7.1.4.11.3 Pneumatic presses
Interlocks or monitoring circuits shall be provided to prevent or stop slide/ram/platen motion if
(a) power to a safeguarding device fails; or
(b) the valves that control the hazardous motion fail.

7.2.1 Brake requirements
Note: *See Annex D.*

7.2.1.1 Spring-set/air release (dynamic brake type)
Spring-set/air release brakes shall
(a) be connected to a properly sized pneumatic line and a press safety valve;
(b) be designed so that the brake is self-engaging and requires power or force from an external force for disengaging; and
(c) have a brake capacity sufficient to stop the motion of the slide/ram/platen and capable of holding the slide/ram/platen and its attachments at any point in its travel.

If the stopping action of the press depends on spring action, the spring(s) shall be of the compression type, operating on a rod or guided within a hole or tube, and designed to prevent interleaving of the spring coils in the event of breakage (see Figures 1 and 2).

7.2.3.1 Press safety valve
Press safety valves shall be installed on all presses with spring-set/air release brakes, be constructed to meet the requirements of CSA C22.2 No. 139, and meet the requirements of Clause 8. In the event of a malfunction of the actuating valve, there should not be an increase in the stopping time of the press, and further operation of the press should be prevented. If individual press safety valves for clutch and brakes are used, a cyclic check of pressure in both systems of the press safety valve shall be carried out. The solenoids of the press safety valve shall be independently controlled.

7.2.3.3 Safety shut-off and exhaust valve
A means shall be provided to shut off and release pressure from the various systems during times of maintenance. This device shall
(a) be capable of being locked in the OFF position;
(b) be easy to operate (e.g., through a simple pull/push action);
(c) have an exhaust port equal to or greater than its supply line; and
(d) have a pressure indicator installed nearby (i.e., a gauge) that is visible to the operator to indicate that the line is bled.

7.2.3.4 Mufflers
Mufflers shall have capacity sufficient to not restrict the exhausting of the system throughout their life.

7.3.3.2 Multiple-cylinder systems
Where there is a risk of injury due to unintended gravity falls and press tonnage is developed by the use of two or more cylinders, at least two of the cylinders shall be independently controlled by a cyclically monitored valve capable of independently holding the slide/ram/platen/die combination in the event of a mechanical or hydraulic/pneumatic failure of a cylinder. If the cylinders are not capable of independently holding the slide/ram/platen/die, at least one of the following shall be provided:
(a) a monitored mechanical restraint device(s); or
(b) a monitored hydraulic restraint device(s).

The restraint devices shall operate automatically and shall be effective throughout all portions of the stroke/cycle during all times that operators have access to the tools, pinch points, or danger zone. Each restraint device shall be individually capable of holding the slide/ram/platen and all of its attachments.

8 Safety-related control system performance (hardware/software)

8.1 General

8.1.1

Safety-related control systems (electric, hydraulic, pneumatic, and software) shall meet, at a minimum, the requirements specified in Clause 8.1.2.

Alternatively, Standards other than this Standard that include performance requirements providing an equivalent level of risk reduction, e.g., control reliable circuitry, may be used.

8.1.2

Safety-related control systems and their parts shall be designed, constructed, and applied in such a manner that

(a) a single fault in any part does not lead to loss of the safety function;
(b) a single fault is detected at the time of failure. If such detection is not practicable, the fault shall be detected at the next demand upon the safety function;
(c) when a single fault occurs, the safety function is always performed and a safe state is maintained until the fault is corrected; and
(d) all reasonably foreseeable faults are detected.

Notes:

(1) *The requirements specified in this Clause are considered equivalent to the following, provided that the requirements specified in Clause 8.1.1 are met as well:*
(a) performance Level "d" with structure category 3, as described in ISO 13849-1; and
(b) a safety integrity level (SIL) of 2 with a hardware fault tolerance of 1, as described in IEC 62061.

(2) *Single fault detection does not mean that all faults will be detected. Accumulation of undetected faults can lead to unintended output and a hazardous situation.*

ANSI B11.19-2010 & CSA Z432
Performance Criteria for Safeguarding

(This standard deals with the specifics of safeguarding and what is required in safeguarding system design in terms of safety considerations and distance calculations.)

1 Scope

This standard provides performance requirements for the design, construction, installation, operation and maintenance of the safeguarding listed below when applied to machines.
a) Guards (see clause 7);
b) Safeguarding devices (see clause 8);
c) Awareness devices (see clause 9);
d) Safeguarding methods (see clause 10).

This standard also provides performance requirements for complementary equipment and measures (see clause 12), safe work procedures (see clause 11), and safety functions (see clause 6).

6.1 Performance of the safety-related function(s)
This subclause shall apply when referenced by other parts of this standard.

When a component, module, device or system failure occurs, such that it or a subsequent failure of another component, module, device or system would lead to the inability of the safety-related function(s) to respond to a normal stop command or an immediate stop command, the safety-related function shall:

• prevent initiation of hazardous machine motion (or situation) until the failure is corrected or until the control system is manually reset; or
• initiate an immediate stop command and prevent re-initiation of hazardous machine motion (or situation) until the failure is corrected or until the control system is manually reset; or
• prevent re-initiation of hazardous machine motion (or situation) at the next normal stop command until the failure is corrected or until the control system is manually reset
In the presence of a failure, the user shall be responsible to ensure that repetitive manual reset of the system or device is not used for production operation.

6.2.1.1 The protective stop circuit shall control the safeguarded hazard by causing an immediate stop command of hazardous machine motion(s) or situation(s).

When protective stop circuits are combined with a circuit of a lower safety performance level, the performance of the protective stop circuits shall not be reduced.

6.3 Safety distance
When required by this standard, the guard or safeguarding device shall be located at a distance from its associated hazard such that individuals cannot reach the hazard before cessation of hazardous motion (or situation).

6.4 Stopping performance monitor
When the stopping time of the machine can increase to a value where the calculated safety distance used in locating the safeguarding is no longer met, a stopping performance monitor shall be provided in accordance with 12.4 of this standard.

(Sluggish valve can effect stopping time unless supply air is exhausted in a control reliable way)

8.4.1.3 Two-hand operating levers shall be designed and constructed to require concurrent operation of both operating levers to initiate the machine cycle. If more than one pair of levers is to be provided, each pair shall be interlocked such that the concurrent operation of all levers is required to cycle the machine.
The two-hand trip and control devices shall be designed and constructed to require synchronous use of both hands (within 500 milliseconds) to initiate the machine cycle.

12.9 Emergency Stop

12.9.1.1 General
a) The device shall be actuated by a single human action and initiate an immediate stop command.
The emergency stop command shall:
• override all other functions and operations in all modes for hazardous motion;
• remove power to the machine actuators, which causes a hazardous situation(s), as quickly as possible without creating other hazards;

Annex D – Safety Distance

The factor is the total time that it takes for the hazardous motion to stop, or for the hazardous portion of the machine cycle to be completed. A power press may present a hazard during the closing portion of its cycle or a machining center may present a hazard during a tool change or while the tool is approaching the workpiece (trapping zone), but not present a hazard during the balance of the machine cycle. *T*
includes portions of time that vary by machine type and by the safeguarding device applied. The following affect the total stopping time: *T*

a) Type of actuator;
   I) Full revolution clutch, or machines that cannot be stopped during a machine cycle. See note 1.
   II) Part revolution friction clutch, or machines that can be stopped at any point in the machine cycle or anywhere during the hazardous portion of the machine cycle. See note 2.
   III) Braking mechanism. See note 3.
   IV) Stopping capability of the motors and drive. See note 4.
b) **Reaction time of valves. See note 5.**
c) Reaction time of the machine control system. See note 6.
d) Reaction time of the safeguarding device, including its interface. See note 7.
e) Additional time required by the use of braking performance monitor. See note 8.

Note 5: The stopping time, , of machines actuated or controlled by pneumatic or hydraulic valves must include the reaction time of the valve measured from the time that the valve is de-energized until motion is stopped. Stopping time for systems using valves may be affected by high or low supply pressures, exhaust restrictions, sluggish spools or poppets or performance of the pilot sections. *Ts*

(The note above is not a note I added to this document, it is the exact wording of the standard.)

ANSI B11.TR6-2010
Safety Control Systems for Machine Tools

(This standard deals with the specific circuit design required to get a control reliable system. It provides circuit examples and design concerns for different components in a safety system. This includes components such as light curtains, interlocks, and includes pneumatic valves. It provides text and a flowchart for considerations in pneumatic safety component design and selection.

Section 4.9 deals with general pneumatic concerns and the differences between what is available from single channel non-monitored valves up to control reliable dual safety valves.

Section 6 deals with specific valve types and provides a circuit example with detailed features and concerns. The valve types include:

- ***Exhaust valve***
- ***Directional control valve***
- ***PO Checks***
- ***Rod locks and brakes***
- ***Flow controls***
- ***Air logic circuits***

I've only attached two examples of the exhaust valves for Category 2 and category 4.)

Guide for using this document

Process steps needed to use this document:

- Conduct a risk assessment
- Determine the risk reduction required (e.g., Category, performance level, control reliability, SIL, etc.)
- Define the safety function (what needs to happen)
- Implement the safety function by selecting component(s) and designing the control circuit

Steps in the application of this document:

- Determine failure modes to be managed
- Select the safeguarding device and/or complementary equipment,
- Using the Table of Contents Clause 5 (Input devices (safeguarding devices complementary equipment)) subclause listings, choose the appropriate input device implementation
- Using the Table of Contents Clause 6 (Power controls and actuators) subclause listings, choose the appropriate output device implementation
- Evaluate the effectiveness of that system for the desired results

1 Scope

This Technical Report provides guidance in understanding and implementing safety-related control functions (functional safety) as they relate to electrical, electronic, mechanical, pneumatic, hydraulic components and systems for machines covered by the B11 series of safety standards.

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

4.7 **response time**

Diminished performance of the safety function due to response time change should be considered: Spring weakening or breaking; Valves leaking; Over-current or mechanical binding causing relays to stick; Clogged exhaust path; Contaminants in the fluid; Unintended or unauthorized adjustments to device response time.

4.9 Fluid Power (Pneumatics & Hydraulics)

4.9.1 General Considerations

Fluid power portions of a safety circuit must be subjected to the same design criteria as the electrical portion to satisfy the requirements of the risk assessment. The designer must recognize that merely removing control voltage from the machine control valve does not ensure that a safe fluid power condition exists. The designer must also take into account the failure modes of the fluid power components when designing the safeguarding system. Therefore, additional safety circuitry may be required to meet the necessary requirements of the risk assessment.

4.9.2 Basic Methodology for Safety Interfacing

There are five basic methods for reducing the hazards associated with fluid power control circuits:

- — Blocking of the fluid power energy source;
- — Removal of electrical power from the safety valve(s), conversion source (pump) and/or motion control valves. Removal of electrical power may not result in a safe state as it may not remove fluid power from the actuating device (e.g., detented valves or valves that have failed or stuck in position);
    - Caution: Consider wind down time of the pump when calculating stopping time/distance formulas.
- — Exhausting or removal of stored energy;
- — Selective trapping of fluid to maintain actuator position and prevent unintended hazardous movement caused by other energy sources such as gravity, springs, etc.;

4.9.7 Fluid Power Valve Crossover Considerations

The crossover condition‘s influence on the circuit shall be understood for fluid power valves being used in safety applications. These conditions may not be disclosed or may only be partially disclosed in catalog information.

Valve functions and schematics will typically depict 2 or 3 position valves indicating their normal operating positions. During operation, elements transit from an at rest condition to one (or two) energized positions. This provides an infinite number of crossover positions as the valve elements shift. The designer must take into consideration the effect on the load during the crossover condition.

There are two types of crossover conditions:

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

4.9.8 Single Channel Fluid Power Device A device whose failure to operate properly may result in the loss of the safety-related function.

4.9.9 Single Channel Fluid Power Device with Monitoring

- — A device whose failure to operate properly may result in the loss of the safety-related function;
- — The device is monitored, either internally or externally; to provide indication of its operating status;

— A fluid power system with single channel control and monitoring, which can be internal or external to the device (see Annex V).

4.9.10 Dual channel fluid power

— The use of redundant individual fluid power devices, where either can perform the safety-related function;
— The failure of one of the devices reduces the control to a single channel.

4.9.11 Dual Channel fluid power with Monitoring

— The use of redundant individual fluid power devices or assemblies, where either device can perform the safety-related function;
— The failure of one of the devices reduces the control to a single channel;
— The devices are monitored either internally or externally to provide indication of its operating status;
— The system designer must use the monitored status to prevent restarting of the fluid power system and initiate corrective action on the failed device.

4.9.12 Dual Channel Cross Monitoring

— Valve Redundant valve components contained within one assembly with cross flow paths between elements and monitoring that result in a Category 4 fluid power safety device;
— The monitoring can be internal or external to the device but must monitor for diminished performance (see Annex V).

4.9.13 Response Time Considerations

— Valve response, line pressurization and exhaust times shall be considered in the safety distance calculations for fluid power systems used in safety applications.

4.9.16 Diminished Performance Fault

A fault caused by the unacceptable increase in the shift time required for the valve. Standard fluid power valves can become sluggish increasing shift time. For applications which involve stopping time/distance (light curtains, interlocked doors or gates, etc.) an increase in shifting time will void the safety distance previously calculated and can render the guarding unsafe.

4.10.2 Safety Shut-Off and Exhaust Valve *(Requires LOX)*

An energy isolation device shall be provided to shut off and release pressure from the various systems during times of maintenance and shall:

— be located outside of the hazardous area(s);
— be capable of being locked in the OFF position only;
— be easy to operate (e.g., a simple pull/push action);
— have an exhaust port equal to or greater than its supply line;
— have a pressure indicator (e.g., a gauge, pop-up indicator or pressure tap), that is visible to the operator to indicate that the line is relieved of pressure.

4.10.6 Air Valve Mufflers

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

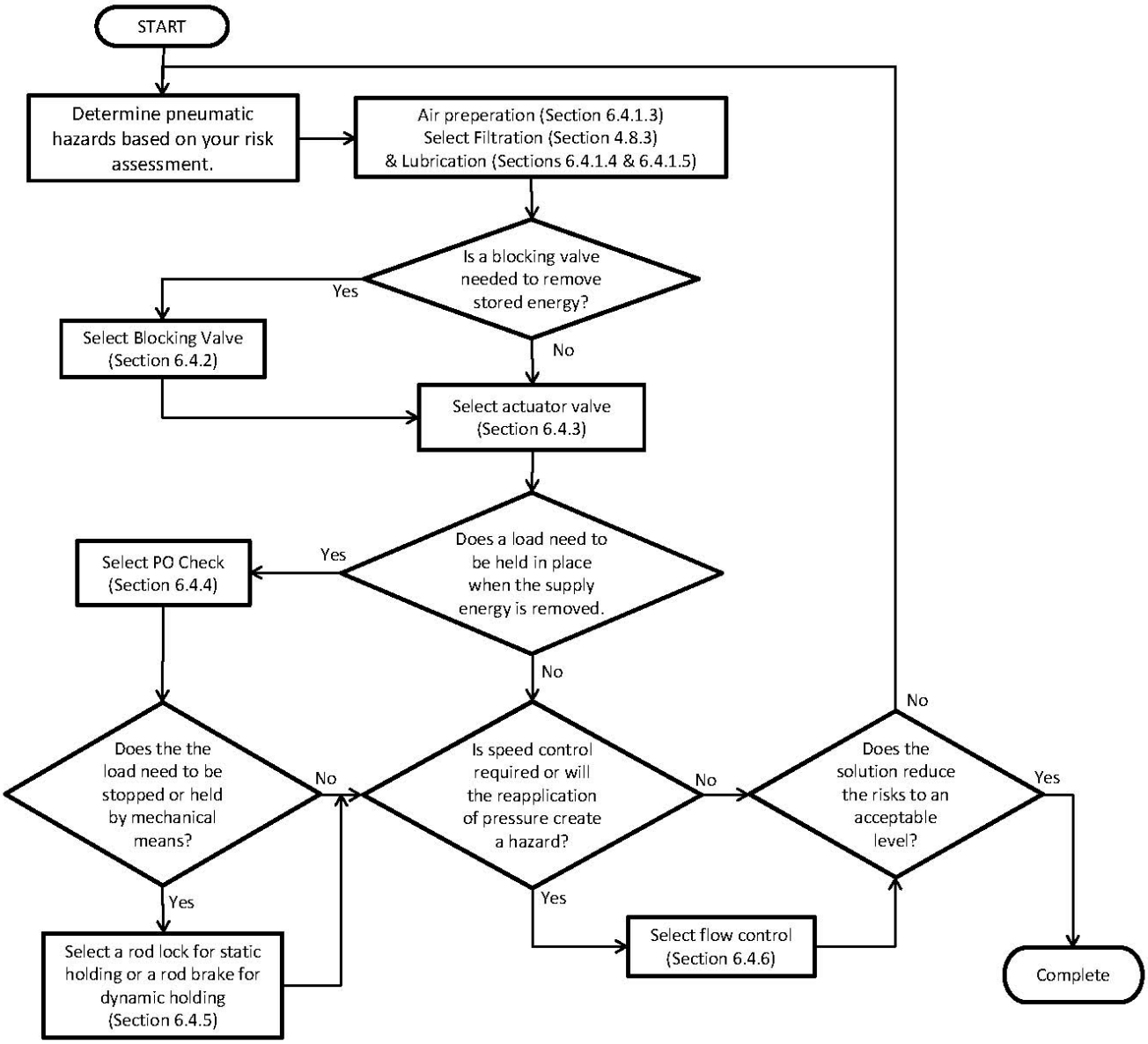
6.4 Pneumatic Systems

6.4.1 General Considerations

Pneumatic circuits use compressed gas (air) to store the energy necessary to perform work. This stored energy must be properly managed and conditioned to minimize or eliminate hazards associated with component failures and the release of stored energy.

To effectively mitigate these hazards the pneumatic design process should be broken up into the following steps:

- Determine the pneumatic hazards based on the risk assessment;
- Select the appropriate air preparation components based on the required contamination control (see 6.4.1.2), filtration level required (see 4.10.3), and lubrication only if it is required (see 4.10.5);
- If a blocking valve is required to remove stored energy select the appropriate valve based on the hazard level requirements (see 6.4.2);
- Select the actuator valve most appropriate for your applications (see 6.4.3);
- If a load needs to be held in place select a pilot operated check (see 6.4.4);
- If the load needs to be stopped or held by mechanical means select the appropriate lock, brake, or equivalent mechanical device (see 6.4.5);
- If speed control is required or the re-application of pressure can create a hazard select the appropriate flow control solution (see 6.4.6);
- Evaluate each remaining risk to determine whether or not it is tolerable.


START
Determine pneumatic hazards based on your risk assessment.
Air preperation (Section 6.4.1.3)
Select Filtration (Section 4.8.3)
& Lubrication (Sections 6.4.1.4 & 6.4.1.5)
Is a blocking valve needed to remove stored energy?
Yes
No
Select Blocking Valve (Section 6.4.2)
Select actuator valve (Section 6.4.3)
Does a load need to be held in place when the supply energy is removed.
Yes
Select PO Check (Section 6.4.4)
No
Does the the load need to be stopped or held by mechanical means?
No
Yes
Select a rod lock for static holding or a rod brake for dynamic holding (Section 6.4.5)
Is speed control required or will the reapplication of pressure create a hazard?
No
Yes
Select flow control (Section 6.4.6)
Does the solution reduce the risks to an acceptable level?
No
Yes
Complete

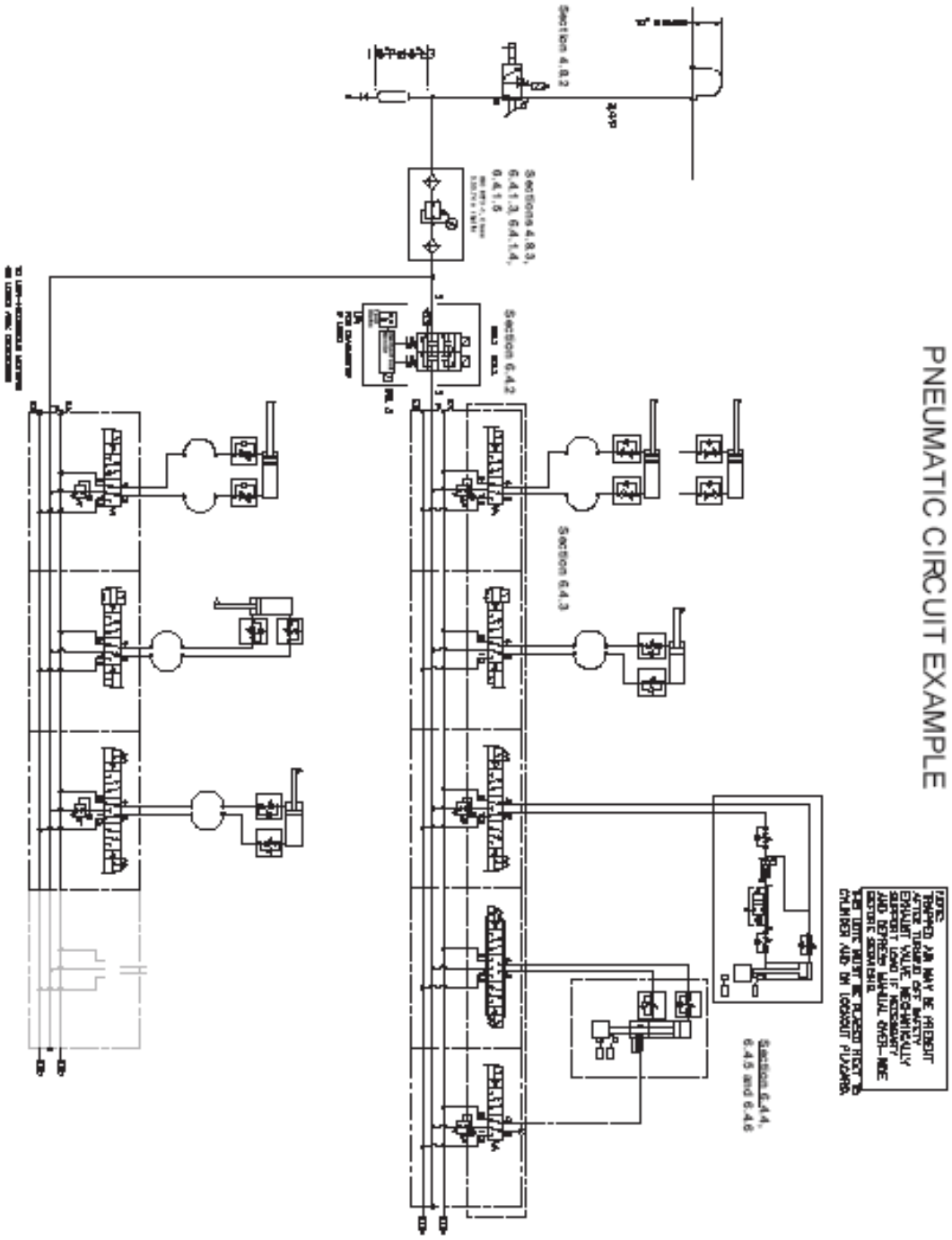
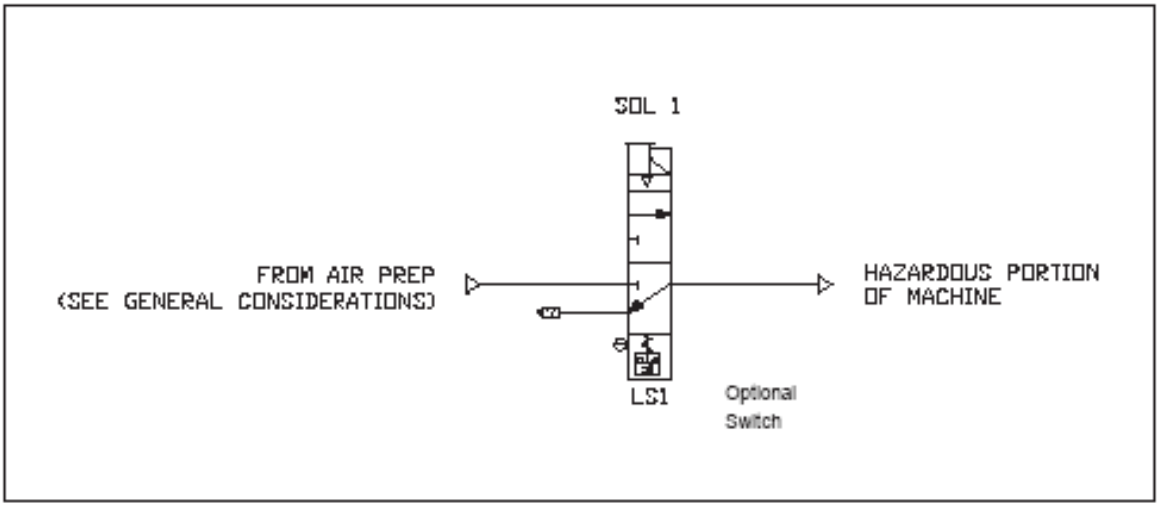

PNEUMATIC CIRCUIT EXAMPLE
Section 4.8.2
Sections 4.8.3, 6.4.1.3, 6.4.1.4, 6.4.1.5
Section 6.4.2
Section 6.4.3
Section 6.4.4, 6.4.5 and 6.4.6

Figure K

6.4.2.2 Low / Intermediate Risk Reduction (Category 2)

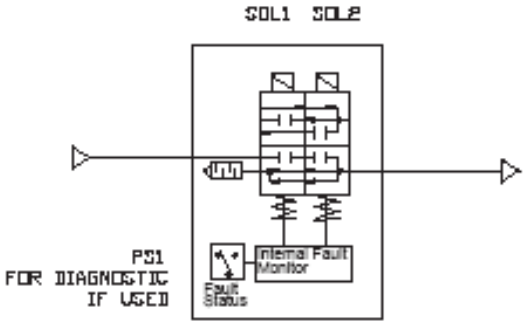
6.4.2.2.1 Single Monitored Directional Valve (Category 2)

A Category 2 circuit does not require a safety exhaust (blocking) valve to be used upstream of the motion or process control valve(s). A Category 2 circuit requires the addition of monitoring to the safety function as designed into what otherwise would be a Category 1 circuit. System monitoring is done through the use of methods using external or integral devices such as integrated safety switches used to detect valve function, actuator motion, or a downstream pressure switch monitoring the safety function (a minimum operating switch is not intended for this use due to pressure change set point). The following example represents a 3 way valve used on a single acting cylinder, a process control valve, or as an exhaust valve for one or more downstream actuator valves. Monitoring is not shown.



Safety Function:	When the electrical signal is removed, the valve exhausts fluid power from the hazardous portion of the machine. A safety rated device indicates the position of the valve element in a de-energized state. A slow or sticking valve may affect response time of the safety system.
Faults to Consider:	Solenoid pilot section of valve stuck in actuated position. Pilot seal failure – can lead to unexpected valve element movement. Pilot section manual actuator seal failure – can lead to unexpected valve element movement. Leakage or improper sealing of components. Valve element not actuating or de-actuating properly due to fluid contamination or internal wear. Broken components (piston, poppet, spring) within a valve element. Failure of safety device LS1 to indicate valve element position.
Fault Exclusion:	None to consider.
Safety Principle	Well tried device designed to be mechanically biased to exhaust downstream fluid power. When the valve element is in the energized position the safety device contacts of LS1 must be directly driven open. To achieve Category 2 the dump valve must be periodically tested (see 4.5.1).

6.4.2.4.3 Safety Rated Valve – Automatic Valve Reset (Category 4)



Safety Function:	When the electrical signals are removed the valve exhausts fluid power from the hazardous portion of the machine. The internal dynamic monitoring shall ensure both independent valve elements function simultaneously. Non-synchronous movement of the independent elements while actuating or de-actuating shall result in a fault condition (diminished performance fault). While the valve is in the faulted state, the fluid power to the hazardous portion of the machine shall remain off. Provides feedback when a faulted condition exists. PS1 Fault status switch may also be connected to a PLC input for status indication. PS1 provides monitoring of the valve fault condition. Pilot and power spool failures and changes in dynamic response are detected by internal valve function.
Faults to Consider:	Failure of PS1 device to annunciate faults that automatically reset.
Fault Exclusion:	None to consider.
Safety Principle:	The reset is triggered by de-energization of the solenoid valves. The control circuit should prevent the normal reset and require an acknowledgement that a valve failure has occurred before the valve can be re-energized. Monitoring of PS1 device used to prevent repetitive automatic reset. Resetting the valve shall not cause the valve to shift and provide pressure downstream.

ANSI/PMMI B155.1-2011 – Approved March 2, 2011
Safety Requirements for Packaging Machinery and Packaging Related Converting Machinery

Section 5 – Requirements for design, construction, modification, installation

Suppliers, Users, Integrators, modifiers, and re-builders shall use a risk assessment and reduce the risk to an acceptable level.

Section 6 – Risk Assessment

Shall be hazard and task based and assess the severity of harm, achieve an acceptable risk, and be documented.

Identify Tasks associated with the intended use and reasonably foreseeable misuse.

Severity levels in the example include:

- Catastrophic – death or permanently disabling injury
- Critical – severe injury or illness with irreversible damage
- Marginal – injury that requires medical care
- Negligible – minor injury with no or minimal care

Section 7 – Specific risk reduction and safeguarding methods

7.2 Control Systems include electronic, electromechanical, hydraulic, and pneumatic components.

7.2.9.1 The design and performance of safety related parts of the control system (SRP/CS) shall be commensurate with the risk.

7.2.9.2 "**Stop Functions** – **When pneumatics or hydraulics are incorporated into a safety stopping function, the circuit design and component selection shall be commensurate with the required performance of the SRP/CS.**

Devices that produce a hazard shall have power removed during a stop function, provided a greater hazard is not created."

7.11 Packaging machinery shall minimize potential hazards from:

- Over pressure
- Pressure surges
- Pressure Loss
- Fluid Jet
- Stored energy
- Sudden hazardous movement of a hose resulting form leakage or component failure

7.11.1 Safety Shut Off and Exhaust Valve
An energy isolating device shall be provided to shut off and release pressure from the various systems and shall:

- Be capable of being locked in the off (closed) position only
- Be easy to operate (e.g. simple pull/push action for pneumatics)

- Have a properly sized exhaust port to exhaust pressure in an acceptableperiod of time as determined by the risk assessment
- Have a pressure indicator that is visible to the operator to indicate that the line is relieved of pressure

7.11.3Air valve mufflers

Air valve mufflers shall for safety syetms and sir dumps shall have sufficient capacity so as to not restrict the exhausting time of the system and shall not be prone to clogging over time.

EN 1037 1995 R:2008
Safety of Machinery – Prevention of Unexpected Start-up

0 – Introduction
Keeping a machine in a stopped condition while persons are present in danger zones is one of the most important conditions of the safe use of machinery and hence one of the major aims of the machine designer and machine user.

Machine automation has made the relationship between “operating” and “moving” on the one hand, “stopped” and “at rest” on the other hand more difficult to define. Automation has also increased the potential for unexpected start up, and there are a significant number of accidents where machines, stopped for diagnostic work or corrective actions, start up unexpectedly.

1 – Scope
This standard applies to unexpected start-up from all types of energy source, ie:
- — Power supply, e.g. electrical, hydraulic, pneumatic
- — Stored energy due to, e.g. gravity, compressed springs
- — External influences, e.g. wind

3.2 - Unexpected (unintended) start-up
Any start-up caused by:
- — a start command which is the result of a failure in or an external influence on, the control system
- — restoration of the power supply after an interruption

3.3 - Isolation and energy dissipation
A procedure which consists of all of the four following actions:
a. isolating the machine from all power supplies
b. if necessary, locking (or otherwise securing) all of the isolating units in the isolating positions
c. dissipating or restraining (containing) any stored energy which may give rise to a hazard
   NOTE: Energy may be stored in e.g.
   - — mechanical parts continuing to move through inertia
   - — mechanical parts liable to move by gravity
   - — capacitors, accumulators
   - — pressurized fluids
   - — springs

4.2 – Other means to prevent unexpected (unintended) start-up
If the use of isolation and energy dissipation is not appropriate (e.g. for frequent short intervantions in danger zones), the designer shall provide, according to the risk assessment (see prEN 1050), other measures (see clause 6) to prevent unexpected start-up.

5.1.1 Isolation devices shall:
- — ensure a reliable isolation (disconnection, separation);
- — have a reliable mechanical link between the manual control and the isolation element(s);
- — be equipped with clear and unambiguous identification of the state of the isolation device which corresponds to each position of its manual control (actuator)

5.4 Verification
5.4.1 The machine and the isolation and energy dissipation devices shall be designed, selected, and arranged so that reliable verification of the effectiveness of the isolation and energy dissipation can be carried out.

6.2.2 Design of the safety-related parts of the data storage and processing equipment

NOTE 2: … it is inadvisable to rely solely on such a single channel system where a significant hazard can occur due to malfunction of the control system

ISO 13849-1:2006
Safety of Machinery – Safety Related Parts of the Control Systems
Part 1: General Principles for design

1 Scope

This part of ISO 13849 provides safety requirements and guidance on the principles for the design and integration of safety-related parts of control systems (SRP/CS), including the design of software. For these parts of SRP/CS, it specifies characteristics that include the performance level required for carrying out safety functions. It applies to SRP/CS, regardless of the type of technology and energy used (electrical, hydraulic, pneumatic, mechanical, etc.), for all kinds of machinery.

3.1.5
dangerous failure
failure which has the potential to put the SRP/CS in a hazardous or fail-to-function state

NOTE 1 Whether or not the potential is realized can depend on the channel architecture of the system; in redundant systems a dangerous hardware failure is less likely to lead to the overall dangerous or fail-to-function state.

3.1.19
reasonably foreseeable misuse
use of a machine in a way not intended by the designer, but which may result from readily predictable human behavior

3.1.21
monitoring
safety function which ensures that a protective measure is initiated if the ability of a component or an element to perform its function is diminished or if the process conditions are changed in such a way that a decrease of the amount of risk reduction is generated

3.1.23
performance level
PL
discrete level used to specify the ability of safety-related parts of control systems to perform a safety function under foreseeable conditions

3.1.26
diagnostic coverage
DC
measure of the effectiveness of diagnostics, which may be determined as the ratio between the failure rate of detected dangerous failures and the failure rate of total dangerous failures

NOTE 1 Diagnostic coverage can exist for the whole or parts of a safety-related system. For example, diagnostic coverage could exist for sensors and/or logic system and/or final elements.

machine control system
system which responds to input signals from parts of machine elements, operators, external control equipment or any combination of these and generates output signals causing the machine to behave in the intended manner

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

4.2.1 General
The strategy for risk reduction at the machine is given in ISO 12100-1:2003, Clause 5, and further guidance is given in ISO 12100-2:2003, Clauses 4 (inherent design measures) and 5 (safeguarding and complementary protective measures). This strategy covers the whole life cycle of the machine.

The hazard analysis and risk reduction process for a machine requires that hazards are eliminated or reduced through a hierarchy of measures:

- hazard elimination or risk reduction by design (see ISO 12100-2:2003, Clause 4)
- risk reduction by safeguarding and possibly complimentary protective measures (see ISO 12100-2:2003, Clause 5)
- risk reduction by the provision of information for use about the residual risk (see ISO 12100-2:2003, Clause 6)

5.2.6 Response time

The following applies in addition to the requirements of Table 9.

The response time of the SRP/CS shall be determined when the risk assessment of the SRP/CS indicates that this is necessary (see also Clause 11).

NOTE The response time of the control system is part of the overall response time of the machine. The required overall response time of the machine can influence the design of the safety-related part, e.g. the need to provide a braking system.

6.2.1 General

Each SRP/CS shall comply with the requirements of the relevant category, see 6.2.3 to 6.2.7.

…

The designated architectures cannot be considered only as circuit diagrams but also as logical diagrams. For categories 3 and 4, this means that not all parts are necessarily physically redundant but that there are redundant means of assuring that a fault cannot lead to the loss of the safety function.

6.2.6 Category 3

For category 3, the same requirements as those according to 6.2.3 for category B shall apply. “Well-tried safety principles” according to 6.2.4 shall also be followed. In addition, the following applies.

SRP/CS of category 3 shall be designed so that a single fault in any of these parts does not lead to the loss of the safety function. Whenever reasonably practicable, the single fault shall be detected at or before the next demand upon the safety function.

The diagnostic coverage (DC_{avg}) of the total SRP/CS including fault-detection shall be low. The $MTTF_d$ of each of the redundant channels shall be low-to-high, depending on the PL_r. Measures against CCF shall be applied (see Annex F).

NOTE 1 The requirement of single-fault detection does not mean that all faults will be detected. Consequently, the accumulation of undetected faults can lead to an unintended output and a hazardous situation at the machine. Typical examples of practicable measures for fault detection are use of the feedback of mechanically guided relay contacts and monitoring of redundant electrical outputs.

NOTE 2 If necessary because of technology and application, type-C standard makers need to give further details on the detection of faults.

NOTE 3 Category 3 system behaviour allows that

- when the 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

6.2.7 Category 4

For category 4, the same requirements as those according to 6.2.3 for category B shall apply. “Well-tried safety principles” according to 6.2.4 shall also be followed. In addition, the following applies.

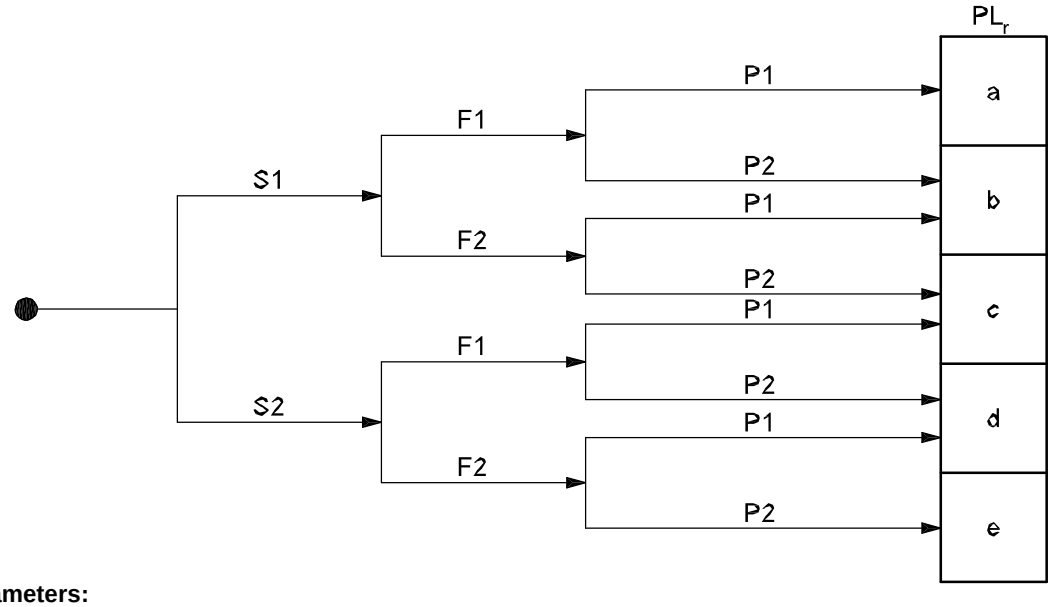
SRP/CS of category 4 shall be designed such that

- a single fault in any of these safety-related parts does not lead to a loss of the safety functions, and
- the single fault is detected at or before the next demand upon the safety functions, e.g. immediately, at switch on, or at end of a machine operating cycle

but if this detection is not possible, then an accumulation of undetected faults shall not lead to the loss of the safety function.

The diagnostic coverage (DC_{avg}) of the total SRP/CS shall be high, including the accumulation of faults. The $MTTF_d$ of each of the redundant channels shall be high. Measures against CCF shall be applied (see Annex F).

Annex A
Performance Level Risk Assessment:



Risk parameters:

S severity of injury
S1 slight (normally reversible injury)
S2 serious (normally irreversible injury or death)

F frequency and/or exposure to hazard
F1 seldom-to-less-often and/or exposure time is short
F2 frequent-to-continuous and/or exposure time is long

P possibility of avoiding hazard or limiting harm
P1 possible under specific conditions
P2 scarcely possible

Annex C

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

	Basic and well-tried safety principles according to ISO 13849-2:2003	Other relevant standards	Typical values: $MTTF_d$ (years) B_{10d} (cycles)
Mechanical components	Tables A.1 and A.2	—	$MTTF_d$ = 150
Hydraulic components	Tables C.1 and C.2	EN 982	$MTTF_d$ = 150
Pneumatic components	Tables B.1 and B.2	EN 983	B_{10d} = 20 000 000
Relays and contactor relays with small load (mechanical load)	Tables D.1 and D.2	EN 50205 IEC 61810 IEC 60947	B_{10d} = 20 000 000
Relays and contactor relays with maximum load	Tables D.1 and D.2	EN 50205 IEC 61810 IEC 60947	B_{10d} = 400 000
Proximity switches with small load (mechanical load)	Tables D.1 and D.2	IEC 60947 EN 1088	B_{10d} = 20 000 000
Proximity switches with maximum load	Tables D.1 and D.2	IEC 60947 EN 1088	B_{10d} = 400 000
Contactors with small load (mechanical 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} = 2 000 000
Position switches independent of load [a]	Tables D.1 and D.2	IEC 60947 EN 1088	B_{10d} = 20 000 000
Position switches (with separate actuator, guard-locking) independent of load [a]	Tables D.1 and D.2	IEC 60947 EN 1088	B_{10d} = 2 000 000
Emergency stop devices independent of the load [a]	Tables D.1 and D.2	IEC 60947 ISO 13850	B_{10d} = 100 000
Emergency stop devices with maximum operational demands [a]	Tables D.1 and D.2	IEC 60947 ISO 13850	B_{10d} = 6 050
Push buttons (e.g. enabling switches) independent of the load) [a]	Tables D.1 and D.2	IEC 60947	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).

NOTE 2 "Small load" means, for example, 20 % of the rated value (for more information, see EN 13849-2).

[a] If fault exclusion for direct opening action is possible.

Annex E

E.1 Examples of diagnostic coverage (DC)

See Table E.1

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 %

Table E.1 (continued)

Measure	DC
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 behaviour 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”!

Table E.1 (continued)

Measure	**Diagnostic coverage (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 no monitoring of the actuator	0 %
Redundant shut-off path with monitoring of one of the actuators either by logic or by test equipment	90 %
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”!
Direct monitoring (e.g. electrical position monitoring of control valves, monitoring of electromechanical devices by mechanically linked contact elements)	99 %
NOTE 1 For additional estimations for DC, see, e.g., IEC 61508-2:2000, 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.	

Annex F

Table F.1 — Scoring process and quantification of measures against CCF

No.	Measure against CCF	Score
1	**Separation/ Segregation**	
	Physical separation between signal paths: separation in wiring/piping, sufficient clearances and creep age distances on printed-circuit boards.	**15**
2	**Diversity**	
	Different technologies/design or physical principles are used, for example: first channel programmable electronic and second channel hardwired, kind of initiation, pressure and temperature, Measuring of distance and pressure, digital and analog. Components of different manufactures.	**20**
3	**Design/application/experience**	
3.1	Protection against over-voltage, over-pressure, over-current, etc.	**15**
3.2	Components used are well-tried.	**5**
4	**Assessment/analysis**	
	Are the results of a failure mode and effect analysis taken into account to avoid common-cause-failures in design.	**5**
5	**Competence/training**	
	Have designers/ maintainers been trained to understand the causes and consequences of common cause failures?	**5**
6	**Environmental**	
6.1	Prevention of contamination and electromagnetic compatibility (EMC) against CCF in accordance with appropriate standards. 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. Electric systems: Has the system been checked for electromagnetic immunity, e.g. as specified in relevant standards against CCF? For combined fluidic and electric systems, both aspects should be considered.	**25**
6.2	Other influences Have the requirements for immunity to all relevant environmental influences such as, temperature, shock, vibration, humidity (e.g. as specified in relevant standards) bee considered?	**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.

1.4 This standard also applies to ancillary devices which are an integral part of the press. For the safeguarding of integrated manufacturing systems using presses, see also ISO 11161

5.2.2.4 The clutch and its control system shall be designed so that, in the ev nt of failure of pneumatic, hydraulic or electrical supply, 'the clutch is disengaged and the brake is immediately applied.

5.2.4.10 Operating valves shall be so designed that it is not possible for both the inlet port and the exhaust ports to remain closed at the same time.

5.2.4.11 Exhaust ports and piping between clutch operating cylinders and valves shall be
.·of sufficient capacity to ensure prompt release of fluid from clutch operating cylinders. Precautions shall be taken to ensure th.at the exhaust ports of operating valves are of adequate size to prevent residual pressure in the cylinder. The valve shall be selected so that the pressure ratio between clutch and brake is such that the residual pressure in the cylinder will not become excessive in the event of a valve fault.

NOTE: Normally, a ratio of at least 3,5 to 1 between spring pressure in the brake and residual pressure in the cylinder is satisfactory.

5.4 The control and monitoring system

5.4.1 Control and monitoring functions

This subclause shall apply to all safety related components which directly or indirectly control or monitor the functioning of moving parts of the press or its tools. EN 60204-1 shall be followed for the design of electrical systems and EN 954-l for electrical, mechanical, pneumatic and hydraulic systems.

5.4.2.3 Where the provision is necessary for redundancy and monitoring of the clutch/brake control system, this shall conform to the following requirements:

a) the press shall be fitted with either at least two single valves or a double bodied solenoid operated valve which directly control the fluid to the operated clutch and brake, or the equivalent in the case of other forms of drive;

b) the valve solenoids shall be connected to the control circuit by separate wiring so that a single fault in the wiring cannot activate both solenoids;

c) it shall be established that a short circuit. between connections of the safety valve (e.g. solenoid to solenoid, or solenoid to self-monitoring assembly) will be detected automatically and will not lead to additional or unexpected motion of the slide;

d) where for the valve monitoring function there is a need for sensors detecting the valve state, these sensors shall be an integral part of the valves. The valve can have an inherent monitoring system in which valve failure is self-revealing;

e) the monitoring shall be dynamic with a frequency of at least once per cycle and shall ensure that, in the case of a failure within the valve(s), the clutch is disengaged and the brake applied

f) it shall only be possible to restore further operation of the press by a restricted means, e.g. by tool, key or electronic password.

5.4.9

Valves

Manual override devices incorporated into valves shall be designed to include a captive lid or cover which requires the use of a tool or key to open it. Electrical override devices shall be key operated and their operation shall only be possible with the slide in BDC position, motor off and flywheel stopped.

4.1 General hazards

- Crushing, shearing or impact due to the whiplash of flexible hoses under pressure in normal operation or in case of rupture or disconnection, see 5.1.4.
- Injury by impact of ejected fluids or hot plastic materials, see 5.1.5.1.
- Puncture by the blowing needles, see 5.2.1.
- Crushing, shearing or impact due to movements associated with hydraulic and pneumatic accumulators, see 5.1.4.
- Crushing, shearing or impact due to movements of power operated guards, see 5.1.5.1 and 5.3.1.
- Crushing, shearing or impact due to movements of parts of the machine by gravity, see 5.1.6 and 5.1.12.

5 Safety requirements and/or protective measures

5.1.1 Basic requirements

Blow moulding machines shall comply with the safety requirements and/or protective measures of this clause. In addition, the machine shall be designed in accordance with the principles of EN ISO 12100 for relevant but not significant hazards which are not dealt with in this document.

The safety related parts of the control system shall be designed in accordance with EN ISO 13849-1:2006. The required performance level (PL_r) for each safety function is specified below. See also 7.1.2.

5.1.4 Fluid systems

Hydraulic and pneumatic systems shall be designed in accordance with respectively EN 982:1996 and EN 983:1996.

The flexible hoses for hydraulic fluids under a pressure of more than 50 bar and for pneumatic fluids of more than 10 bar shall be secured to the machine by additional fastenings (for example chains) limiting the whiplash. On machines equipped with guards, this requirement does not apply to flexible hoses situated inside the guards.

However, additional fastenings for flexible hoses for blowing fluids are also required inside the machine, except if the machine is safeguarded by interlocking guards with guard locking and the pressure in the pneumatic hoses is reduced to under 10 bar before the guard lock can be released. The PL_r for this safety function shall be c.

To avoid injury by ejected fluids accessible hoses and connections shall be covered by

guards.

For hydraulic or pneumatic accumulators the following shall apply.

— the operation of a protective device shall interrupt all power from accumulators for the blowing fluid or which are associated with dangerous movements.

— Actuation of the emergency stopping devices or disconnection of power to the machine shall isolate all power from accumulators for the blowing fluid or which are associated with dangerous movements. Where accumulators are integrated parts of the machine, unloading shall be initiated automatically.

— Visual indication of accumulator pressure shall be provided. Where hydraulic accumulators are integrated parts of the machine, the isolating valve or valves shall be position monitored. When the position monitoring system detects the valve or valves failing to isolate the accumulators, then:

— an optical or audible signal shall be given; and
— all accumulators connected with the failed valve or valves shall be automatically unloaded.

Machines with hydraulic or pneumatic supply from an external source shall be provided with a manual isolation valve lockable by key.

5.1.6 Movements caused by gravity

Machine parts which can have a dangerous movement under gravity shall be provided with an automatic blocking device which operates as soon as the corresponding movable guard is opened or ESPE is interrupted. The blocking shall remain active until a new start command is given. The required performance level for this safety function shall be PL_r c.

Table 1 — Required performance levels PLr

Dangerous movement or part	Automatic machines	Semi-automatic machines	Interlocking guards	ESPE	Other safeguards	PL_r	See also
Blowing mould closing (including drive mechanisms)	X		X	X*		d	
		X	X	X*		e	
Other movements of the blowing mould	X	X	X	X*		c	
Parison transfer; injection	X		X	X		b	5.2.2.1
		X	X	X		c	
Devices to take off or reject the parison	X	X	X			d	
Nozzle of injection unit	X	X	X			d	
Preform feeding device	X		X			d	
Cutting device	X	X	X	X		c	5.2.2.2

Table 1
(continued)

Dangerous movement or part	Automatic machines	Semi-automatic machines	Interlocking guards	ESPE	Other safeguards	PL_r	See also
Blowing needles, mandrels, stretch rods	X		X			b	
		X	X	X		c	
	X			X		c	
Withdrawal apparatus or transfer device for the blown parts	X		X	X		b	
		X	X	X		c	
Cooling mould closing (including drive mechanisms)	X	X	X			d	
Cooling mandrels	X	X	X			b	
Finishing equipment	X		X			b	
		X	X	X		c	
	X			X		c	
Preform handling device at the heating station	X	X	X		X	d	
Blowing (maximum pressure ≤ 15 bar)	X	X	X	X	X	b	5.1.4
Blowing (maximum pressure > 15 bar)	X	X	X	X	X	d	
* Light curtains only, see 2nd paragraph of this subclause							

ANSI 65-1:2011 (ISO 12643-1:2009 MOD)
Graphic Technology – Safety requirements for graphic technology equipment and systems
Part 1: General requirements

Content	B65 standard prior to 2011	Current B65 standard	Current ISO standard
General requirements for all equipment	Did not exist as a stand-alone document. Requirements were contained in each individual standard.	B65-1	ISO 12643-1
Requirements for printing press equipment and systems	B65.1	B65-2	ISO 12643-2
Requirements for binding and finishing equipment	B65.2	B65-3*	ISO 12643-3
Requirements for guillotine cutters	B65.3*	Requirements included in B65-3	Requirements included in ISO 12643-3
Requirements for three-knife trimmers, including rotary and single- and multiple-knife trimmers	B65.4*	Requirements included in B65-3	Requirements included in ISO 12643-3
Requirements for stand-alone platen presses	B65.5	B65-5	ISO 12643-5
* B65 standards containing specific requirements for guillotine cutters (B65.3) and three-knife trimmers (B65.4) have been withdrawn. The requirements for this equipment are now included in B65-3.			

3.14 drive
mechanism, divided into the following two general categories, which causes a machine or any of its elements to move:
— drives with no stored energy, which include, but are not limited to, direct-motor drives;
— drives having stored energy, which include, but are not limited to, motor-flywheel-clutch drives and hydraulic-pneumatic drives

3.26 infrequently used workplace
area in which an activity is carried out, such as observation, make-ready, jam clearing, minor servicing, crossing inserting hoppers or conveyer belts, etc., that is routine, repetitive, integral to (but not necessarily during) production, and is done only on an occasional basis

6.2.1.1 Type of guards
For the purpose of this standard, there are two types of guards, fixed and movable.

Guards that do not have to be opened frequently shall be interlocked or shall be fixed in such a way that their removal necessitates the use of a tool (see 3.61), such as a key or wrench, designed to operate a fastener.

The fixing systems of fixed guards that are designed for access by operators during operations (e.g. set-up, make-ready, routine cleaning, etc.) shall remain attached to the guards or to the machine when the guards are removed. Where possible, guards should be incapable of remaining in place without their fixings.

This requirement is not applicable to guards and enclosures removed by trained service personnel performing maintenance when the machine is not available for production.

All movable guards shall be interlocked in accordance with 6.5.

Guards that are designed to be opened, removed, and/or moved at least once per working shift (on average)

during normal operation, with or without the use of a tool, shall be interlocked.

6.5.4.2 Safety-position switches for interlocking guards

Safety-position switches shall be built in accordance with IEC 60947-5-1 and shall be installed in accordance with IEC 60204-1. **See S.1 for alternative references to NFPA 70 and NFPA 79, which are applicable in the U.S.**

For machines where routine and regular access to a hazardous area is not required, it is sufficient to provide only one safety-position switch for each interlocking guard.

NOTE A single switch is adequate because it is assumed that no safety-related malfunction will occur in switches built and installed to the specified requirements.

Control systems of safety-position switches shall satisfy PL_r d of ISO 13849-1 or SIL 2 of IEC 62061.

For manually fed devices where interlocking guards are used to safeguard routine and regular access (see 3.54) to hazard points, control systems for safety-position switches shall satisfy PL_r e of ISO 13849-1 or SIL 3 of IEC 62061.

6.6 Hold-to-run controls

If all hazard points are safeguarded by nip guards in accordance with 6.4, the requirements for hold-to-run controls and speed limitations do not apply.

Where hold-to-run controls are used for safeguarding a hazard, running the machine in the hold-to-run mode after opening the interlocking guard shall be possible only when guards protecting hazardous areas that are not visible from the operating position are closed.

When the hazardous area can be viewed from the operating position, machine motion with an interlocking guard open and hazardous points unprotected may be initiated by means of a hold-to-run device under only one of the following conditions:

a) with a displacement limited to a maximum of 25 mm or with a maximum operating (surface) speed of 1 m/min; or

b) with displacement limited to a maximum of 75 mm or with a maximum operating speed of 5 m/min where the measures defined in a) would reduce the ability of the machine to perform its function and where there would be no substantial increase in hazard.

Guard circuitry for the hold-to-run condition shall satisfy the requirements of PL_r d of ISO 13849-1 or SIL 2 of IEC 62061. Control circuitry (including selector switch relays and PLC circuits) that allows interlocked areas to be operated independently shall satisfy the requirements of PL_r b of ISO 13849-1 or SIL 1 of IEC 62061.

For hold-to-run devices designed as two-hand controls, the same limitations of displacement and speed shall apply.

10.5 Two-hand controls

10.5.1 General

Two-hand controls as safety devices are acceptable only if all hazardous movement stops when one manual control device is released. The hazardous movement shall come to a stop in a time period that, taking into consideration the hand-approach speed, ensures there is no hazard for the operator. The hand-approach speeds specified in ISO 13855 shall be taken as a basis (see 6.6 for hold-to-run devices designed as two- hand controls).

10.8 Braking devices and clutches

10.8.1 Switch-off of braking device

The braking device may be switched off only by either of the following:

a) use of a maintained-contact control, if the disengagement of the brake is interlocked with the hazardous machine movement; or

b) use of a momentary-contact control which, when released, re-engages the braking device.

Braking devices are switched off, for example, when powered machines operate in a non-powered mode.

10.8.2 Clutch or brake failure on single-stroke machines

On single-stroke operation machines, clutch or brake failures shall not cause any hazardous movement.

NOTE A single-stroke operation machine is one that completes a single cycle, then pauses before the next cycle is initiated. For example, trimmers, paper drills, and bundling machines are single-stroke operation machines. A guillotine cutter is the most common example of a single-stroke machine.

12.1.2 Performance levels

The performance level (PL) or safety integrity level (SIL) requirements of safety-related parts of control systems depend on the result of risk assessment (see Table 6).

In the hydraulic/pneumatic control system, the safety-related parts shall satisfy at least a required performance level PL_r c of ISO 13849-1. If there is a risk of head or torso injuries then the required performance level is PL_r d of ISO 13849-1.

In the electric/electronic control system, the safety-related parts shall meet the required safety levels of ISO 13849-1 (performance level PL_r) or IEC 62061 (safety integrity level SIL), based upon the potential extent of harm, as follows:

a) If a malfunction of the safety related control system can cause permanent injuries, or if there is a risk of head or torso injuries, PL_r d or SIL 2 is required.

b) If the hazards caused by a malfunction of the safety related control system are small (no permanent injuries), PL_r c or SIL 1 is required.

12.7 Additional requirements for hand-fed machines

12.7.2 Hydraulic/pneumatic control system

The safety-related parts of the hydraulic/pneumatic control system shall comply with the requirements of PL_r d of ISO 13849-1.

ANSI 65-5:2011 (ISO 12643-5:2010 MOD)
Graphic Technology – Safety requirements for graphic technology equipment and systems
Part 5: Stand-alone platen presses

5.7 Stopping distance
The stopping distance of the platen press shall not exceed 120 mm. This shall be measured between the top edges of the moveable fixed platens.

On manually-fed platen presses, if the stopping time or stopping distance specified by the manufacturer is exceeded, start up shall be prevented. The stopping distance shall be monitored at the end of each cycle.

5.8 Main drive braking and clutch/brake mechanism
All platen presses shall be equipped with either a fail-safe brake or a fail-safe clutch/brake mechanism which shall stop and prevent press motion when engaged. Hand-fed platen presses shall be equipped with a fail-safe clutch brake mechanism to disconnect the stored energy in the flywheel from the moving platen and bring the platen to a stop.

On presses with flywheels this mechanism shall be located on the fly wheel shaft.

When using a clutch/brake mechanism, electric power supply failure, or loss of pneumatic or hydraulic pressure, shall aactive the brake and disengage the clutch (i.e. fail-safe). The brake shall be of sufficient strength to maintain the platen in the position in which it stopped due to failure.

If a pneumatic system is used for the combined clutch and brake system (stopping closing movement of a platen) two pneumatic valves shall be provided. The pneumatic system shall meet PLr e of ISO 13849-1. The pneumatic system shall comply with the requirements of ISO 4414.

DIN EN 13042-1:2009
Machines and plants for the manufacture, treatment and processing of hollow glass – Safety requirements – Part 1: Gob feeder

5.10 Energy supply disconnecting devices
Lockable energy supply disconnecting devices shall be provided, e. g. a master switch in accordance with EN 60204-1:2006, 5.3, an isolation valve and provisions for dissipation of pressure in accordance with EN 982:1996, 5.1.6, and EN 983 as relevant.

5.11 Gob-loading interruption
The shear mechanism shall be interlocked for the purpose of interrupting automatically the delivery of glass to the forming machine, e. g. by insertion of a chute under the shear, should there be any irregularity in the operation of the cutting action of the shear. The related part of the control system shall present a performance level of at least c in accordance with EN ISO 13849-1:2008.

Manual controls (actuators) shall be provided to allow the delivery of glass to the forming machine to be interrupted. The related part of the control system shall present a performance level of at least c in accordance with EN ISO 13849-1:2008. The actuators shall be installed at the operator's station for the gob feeder, and provisions shall be made for the connection of these actuators to the associated glass-forming machine such that they per- form their intended function (see also 7.2.5).

5.14 Glass flow
In the case of an emergency stop (see 5.3) or switching off or a power failure at the gob feeder, it shall be ensured that the glass flow is stopped or is able to flow away from the hollow glass forming machine along suitable equip- ment (drainage chute, fall pipe etc.). Provisions shall be made for the connection of the necessary safety signals from the receiving glass-forming machine to the gob feeder (see 7.2.5).

5.15 Necessary movements in case of power failure
In case of power failure, necessary movements for the gob-loading interruption (see 5.11) and the flowing-off or the stop of the glass flow (see 5.14) shall be possible, e.g. by the use of an accumulator for compressed air.

DIN EN 13042-2:2009
Machines and plants for the manufacture, treatment and processing of hollow glass – Safety requirements – Part 2: Handling Machines for Feeding

5.3.1 Where access to the danger zone is required, movable interlocking guards according to EN ISO 13857:2008, Table 1, or trip devices, e.g. active opto-electronic protective devices in accordance with EN 61496-1:2004, type 4, and with CLC/TS 61496-2, or pressure mats, EN 1760-1:1997, Category 3, shall be provided. These shall cause a standstill of dangerous movements before the danger zone can be reached (see EN 999).

5.4 The closing movement of shears shall be able to be prevented by a mechanical restraint device (see 3.26.7 of EN ISO 12100-1:2003) or by the possibility to cut off the driving energy directly at the shear.

5.9.10 The control of the handling machine for feeding shall guarantee a shut-down according to EN 60204-1:2006, 9.2.2, Category 0 or 1, e. g., upon

- emergency switch-off;
- switch-off by safety equipment;
- deliberate automatic shut-down according to the operating concept(software).

This is achieved by:

5.9.10.1 control using contacts according to EN ISO 13849-1:2008, performance level c, whereby the other parts of the control system shall present a performance level d defined in accordance with EN ISO 13849-1:2008, or

5.9.10.2 an additional overriding control using for example contacts if an electronic control is used. The redundancy – electronic control/additional overriding control using contacts – shall present a performance level of at least d defined in accordance with EN ISO 13849-1:2008.

DIN EN 13042-3:2010
Machines and plants for the manufacture, treatment and processing of hollow glass – Safety requirements – Part 3: IS Machines

5.2.2 Prevention of an unexpected start-up

Each individual section shall be fitted on both sides with a device which maintains a stop command in accordance with EN 1037:1995, 6.3.2, until the device is reset manually (e. g. a latching-in stop control device). This switch shall prohibit a start of any movement of the respective section and the delivery of gobs into this section. All gob distributors shall also be fitted either with their own latching-in stop control device or a mechanical blocking device. The safety-related part of the control system shall be at least in accordance with EN ISO 13849-1:2008, performance level c (see also 7.2.4).

5.3 Emergency-stop equipment

The IS machine shall be equipped, as a minimum, at both sides of the machine and at the main control station with easily and quickly accessible emergency stopping devices. The emergency-stop equipment shall be in accor- dance with EN ISO 13850 and stop all moving parts of the IS machine, delivery of glass to the machine and the machine conveyor. The stop function shall be in accordance with stop category 0 or 1 (see EN ISO 13850:2008,
4.1.4, EN 60204-1:2006, 9.2.2 and 9.2.5.4.2) and the safety-related part of the control shall be at least in accor- dance with EN ISO 13849-1:2008, performance level c.

5.4 Prevention of unexpected movements of individual mechanisms

Measures against unexpected start-up and movements shall be present on the appropriate side of each manufacturing section which are capable of preventing unintentional or erroneously triggered movements of each of the individual mechanisms designated below (see also 7.2.4).

This applies on the blank mould side to:

— the invert/revert of the neck ring transfer mechanism;
— the closing of the blank mould;
— the setting down of the baffle;
— the movement of the funnel to the load position

and on the blow mould side to

— the closing of the blow mould;
— the setting down of the blow head;
— the movement of the take-out. Suitable measures are e.g.:
— valves, contactors to interrupt the energy for the respective drive. The safety-related part of the control system shall be at least EN ISO 13849-1:2008, performance level c;
— mechanical restraint devices such as bolts, latches.

DIN EN 13042-5:2009
Machines and plants for the manufacture, treatment and processing of hollow glass – Safety requirements – Part 5: Presses

5.9 Exclusion of unexpected start-up and stop of dangerous movements
To avoid an unexpected start-up and to stop dangerous movements of glass presses, the related parts of the control system shall comply with a minimum performance level c as defined in EN ISO 13849-1 and consist of:
– a control using contacts; stopping by immediate removal of power (EN 60204-1:2006, 9.2.2, category 0); or
– an electronically controlled stop where the power is removed using contacts, when the stop is achieved (EN 60204-1:2006, 9.2.2, category 1).

5.12 The control of the press shall be designed in such a way that no dangerous movement is initiated when the energy (electrical, hydraulic, pneumatic) is supplied or restored after an interruption.
It shall be possible to prevent the closing movement of plunger and ring by:

5.15.1 Switches on electrical controls or

5.15.2 Valves in hydraulic/pneumatic systems or

5.15.3 Locks able to resist the drive energy.

5.16 Hydraulic/pneumatic systems and components
Hydraulically and pneumatically driven glass presses shall use systems and components conforming to the requirements of EN 982 or EN 983 as appropriate.

NOTE According to 5.3.7.1 of EN 982:1996 full flow filters for oil should be installed in the supply line if servo or proportional valves are used.

5.17 Unexpected dangerous movements induced by gravity in hydraulic/pneumatic systems
In the event of leaks from the hydraulic or pneumatic systems, unexpected dangerous downwards movement of the rod or cylinder assemblies with or without mould parts and cages under the influence of a force of gravity exceeding 150 N shall be prevented by:

5.17.1 Weight balance or

5.17.2 Pressure springs or

5.17.3 Continuously working mechanical devices such as clamps at piston rods or

5.17.4 Seat valves (check valves, restraint valves) in hydraulic systems or valves with soft sealing in pneumatic systems, both in connection with leak-proof piston packing.

Solid pipework shall be used between cylinder and seat valve or pneumatic valve. Joints in pipework shall be welded or flanged or shall use peened ring fittings (flare fittings).

NOTE: The requirement of 5.17.4 – 2nd paragraph – excludes the use of hoses or cutting ring fittings (bite type fittings) glued ring (compression fittings) between cylinder and seat valve.

5.18 Stopping device (braking)
Glass presses shall be built or equipped so that dangerous movements can be stopped as quickly as possible e.g. by:

5.18.1 Spring-loaded brakes which are adequately dimensioned for the drive torque together with a control using contacts, or

5.18.2 Electronically controlled stop and removal of power using contacts when the stop is achieved (see 5.9.2) with an additional holding device such as a mechanical brake if an unexpected movement by gravity is possible, or

5.18.3 Valves which move to the stop position if the power from the control is removed e.g. by use of seat valves or slide (gate) valves with spring centring and positive overlap.

ISO 13851:2002
Safety of machinery -- Two-hand control devices

3.1 two-hand control device
a device which requires at least simultaneous actuation by the use of both hands in order to initiate and to maintain, whilst a hazardous condition exists, any operation of a machine thus affording a measure of protection only for the person who actuates it

3.5 synchronous actuation
a particular case of simultaneous actuation where the time lag between the start of one input signal and the start of the other is less than or equal to 0,5 s

4 Types of two-hand control device and their selection
Table 1 defines three types of two-hand control device. It sets out the functional characteristics and the minimum measures for the safety of each type of two-hand control device in this International Standard. All two-hand control devices shall comply with ISO/TR 12100 and with IEC 60204-1.

Table 1 — List of types of two-hand control device and minimum safety requirements

Requirements	Subclause	Type				
		I	II	III		
				A	B	C
Use of both hands (simultaneous actuation)	5.1	X	X	X	X	X
Relationship between input signals and output signal	5.2	X	X	X	X	X
Cessation of the output signal	5.3	X	X	X	X	X
Prevention of accidental operation	5.4	X	X	X	X	X
Prevention of defeat	5.5	X	X	X	X	X
Re-initiation of the output signal	5.6	a	X	X	X	X
Synchronous actuation	5.7			X	X	X
Use of category 1 (see ISO 13849-1)	6.2	X		X		
Use of category 3 (see ISO 13849-1)	6.3		X		X	
Use of category 4 (see ISO 13849-1)	6.4					X
a For the selection of type I, see 8.6.						

The selection and the design of the type (see Table 1) of two-hand control device will depend on
- the hazard(s) present;
- the risk assessment;
- experience in use of the technology;
- other factors, which shall be specified for each application [e.g. the prevention of accidental actuation and of defeat (see clause 8), as well as other conditions.

6 Requirements related to categories of control
6.1 Category selection
The behaviour of parts of a two-hand control device in the case of failure shall be in accordance with the selected category of ISO 13849-1 (see Table 2).

The category of control of two-hand control devices shall not be less than the category of control of the relevant safety related part of the machine control system (see ISO 13849-1).

Annex B describes the relationship between the types of two-hand control devices and the categories according to ISO 13849-1.