Specification for Safety Circuits

Global Common

SD-011

ISSUED November 6, 2009
REVISED

Table of Contents

List of Figures

Foreword

This *Specification for Safety Circuits* (SD-011) is issued by Nexteer Automotive. This specification was developed as a "how to" document in support of the Nexteer Automotive *Design-In Health and Safety Specification* (SD-012), and is to be used for Nexteer as a specification for manufacturing equipment design. The specification's intent is to provide our plants with safe, well-designed, and reliable safety circuits for industrial machinery and equipment. The specification was developed based on international standards, and company specifications to:

- enhance safety.
- simplify and clarify those standards and specifications in order for equipment builders to comply at minimum cost.
- improve equipment reliability and maintainability.
- support lean manufacturing equipment.
- support design-in safety practices.

This shall be accomplished by using a risk assessment to identify equipment and process hazards. The "Hierarchy of Health and Safety Controls" found in Nexteer Automotives *Design-In Health and Safety Specification* shall be followed to eliminate exposure to these hazards. The ultimate goal is to support the operator.

The example circuits in the specification are based on currently available technology consistent with the international standard ISO 13849-1 (EN 954-1). The specification is not intended to inhibit new technology. As an example, some of the circuits in the specification are based on the use of redundant-input safety relays that could be replaced by other technology such as a safety-PLC. Consequently, we expect and encourage all industrial equipment builders to notify us of any specification situation which, in their opinion, inhibits the application of new technology. This approach allows new technology proposals to be evaluated as to their merit and compliance to the principles of this specification.

The drawings in the specification are intended to show safety circuit category requirements. These drawings are not intended to represent Nexteer Automotive drafting standards nor are they intended to show basic machine control design practices such as proper wire sizes, circuit protection, and fluid power sizing.

The specification was based solely on the equipment, operations, processes and facilities of Nexteer Automotive. While we believe that the specification provides a sound basis for the application of safety circuits on industrial machinery and equipment, it is only intended for use within Nexteer operations. It should not be relied on for use at operations other than Nexteer, and Nexteer specifically disclaims any liability should the specification be used outside its intended purpose.

1 Scope and Purpose

1.1 Scope

1.1.1 The specification addresses the use of control systems as applied to equipment safeguarding, (examples include safety gate circuits, light curtains, and two-hand control). Determining the required category of safety circuit is defined as a result of conducting a risk assessment for the equipment. The *Design-In Health and Safety Specification* details the Nexteer Automotive risk assessment process, including who conducts this risk assessment. The results of the risk assessment can include one or more different categories for the safety related part of the control system (reference Chapter 2 of this specification): Category B, 1, 2, 3, or 4.

1.1.2 Emergency stop devices and circuits (e-stop) fall into the scope and purpose of this specification. E-stop circuits perform an auxiliary stop function typically provided in addition to the machine's safeguarding systems.

1.1.3 Fluid power (pneumatic and hydraulic) portions of a control circuit are subjected to the same design criteria as the electrical portion to satisfy the requirements of the risk assessment and therefore fall into the scope and purpose of this specification. Merely removing control voltage from the machine control motion valves does not ensure that a safe fluid power condition exists. The design must also take into account the failure modes of the fluid power components when designing the safeguarding system. Therefore, additional safety circuitry might be required to meet the category requirements of the risk assessment.

1.1.4 This specification is intended to document and illustrate the basic principles of well designed safety circuits. It should not be considered as the sole source of safety circuit information. Additional information on safety circuits is available from device suppliers, seminars, ISO, IEC, and ANSI standards.

1.2 Purpose

1.2.1 This specification applies to the purchase of new equipment and control system rebuilds. It should not be implied that any existing equipment be required to be retrofitted in order to comply with this specification, however, this specification does apply to safeguarding modifications driven by a risk assessment conducted on existing equipment.

1.2.2 The use of safeguarding safety circuits does not replace well-established machine lockout procedures currently in place.

1.2.3 Each application is unique, and in all cases good engineering practices should be used. For safety device applications and safety circuits not explicitly covered in this specification the principles established in this specification should be followed.

1.2.4 The use of the word "shall" indicates requirements and the use of the word "should" indicates recommendations. The use of the word "may" indicates permission or allowance and the use of the word "can" indicates a possibility.

1.2.5 The user has the responsibility to ensure that all local, state and national laws, rules, codes and regulations relating to the use of this specification in any particular application are satisfied.

2 Safety Circuits – Circuit Categories:

ISO 13489-1 details the five categories of the Safety Related Part of the Control System (SRP/CS): Category B, and 1 through 4. Category B is the basic category. In Categories 1, 2, 3, and 4, progressively improved safety performance is achieved through component selection and the structure of the SRP/CS. Nexteer Automotive's minimum requirements for the SRP/CS as derived from ISO 13489-1 are as follows:

2.0 Category B requirements:

Standard control practices and components may be used.

1. Single channel circuitry is required.
2. SRP/CS inputs (sensing devices) may include standard devices, such as proximity switches and limit switches.
3. The safety circuit may be programmable, such as logic within a PLC. Hardwired relays are not required.
4. The final switching device may include standard control components, such as a PLC output.

2.1 Category 1 requirements:

As a minimum:

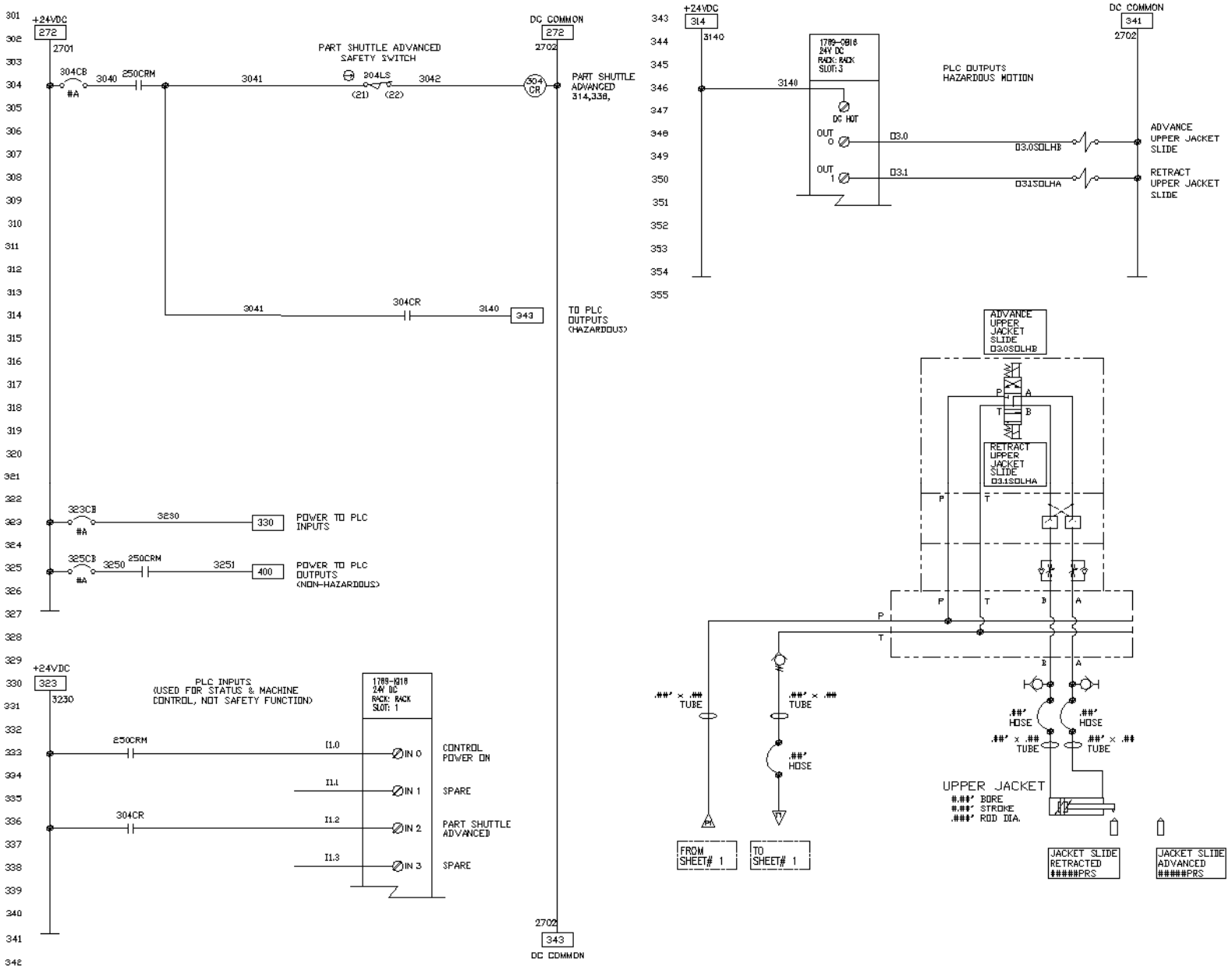
1. Single channel circuitry is required.
2. The SRP/CS input devices shall meet a one of the following three requirements. They shall:
   a. have positive-opening contacts, or
   b. be Type 2 ESPE rated, or
   c. be a minimum Category 1 technology.

   Exception: Two-hand control SRP/CS input device requirements are noted elsewhere in this document.
3. The safety circuit shall be hardwired. All logic functions of the SRP/CS shall be accomplished through industrial control relays.
4. Final switching devices shall be hardware-components such as industrial control relays, motor starter contactors, pneumatic and hydraulic motion valves, or electronic components such as servos when applied to a minimum Category 1.

Figure 2.1.a

Category 1 sample circuit:

Part Shuttle Guard and Hydraulic Motions



2.2 Category 2 requirements:

As a minimum:

1. Single channel circuitry is required.
2. The SRP/CS input devices shall meet one of the following three requirements. They shall:
   a. have positive-opening contacts, or
   b. be a Type 4 ESPE rated device, or
   c. be a minimum Category 2 technology.

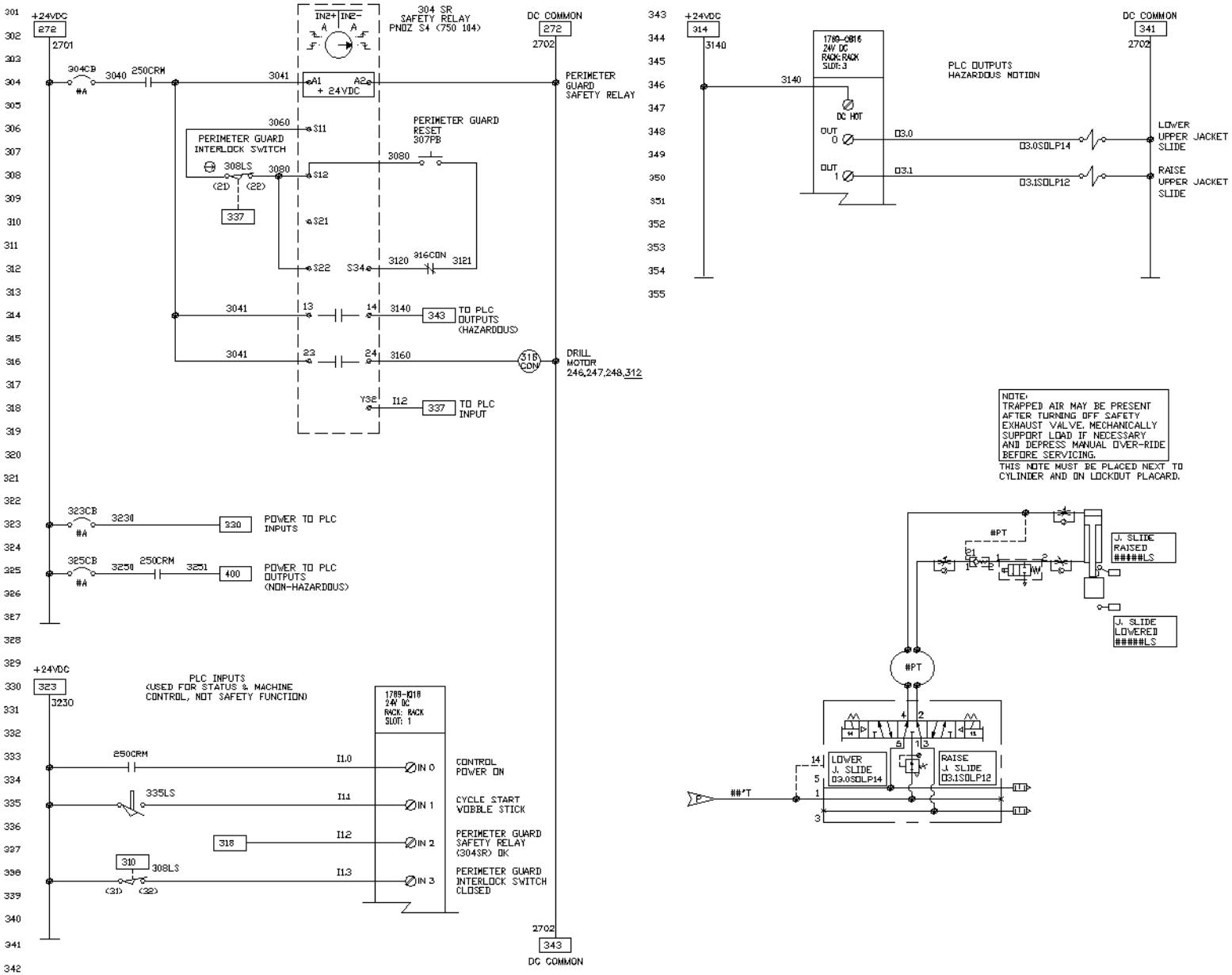
   Exception: Two-hand control SRP/CS input device requirements are noted elsewhere in this document.
3. The safety circuit shall be hardwired. All logic functions of the SRP/CS shall be accomplished through safety relays compliant to published component manufacturer's literature as a minimum Category 2.

   Clarification: Safety devices such as certain light curtains which include the safety relay functions do not in themselves require an additional safety relay.
4. Final switching devices shall be hardware-components such as:
   a. safety-rated safety relay contacts.
   b. an industrial control relay (or motor starter contactor).
   c. an electronic component such as a servo when applied at a minimum Category 2.
   d. the pneumatic and hydraulic motion valves.
5. A feedback contact from the final switching device(s) shall be wired into the feedback terminals of the safety relay.

   Clarification: Pneumatic and hydraulic motion valves do not require feedback into the safety relay.

Figure 2.2.a

Category 2 sample circuit:



Guard Door and Pneumatic Motions

2.3 Category 3 requirements:

As a minimum:

1. Redundancy in the SRP/SC is required.
2. The SRP/CS input devices shall meet one of the following four requirements. They shall be:
   a. a single device with two positive-opening contacts, or
   b. two devices with one positive-opening contact each, or
   c. a Type 4 ESPE rated device, or
   d. a minimum Category 3 technology.

   Exception: Two-hand control SRP/CS input device requirements are noted elsewhere in this document.
3. The safety circuit shall be hardwired. All logic functions of the SRP/CS shall be accomplished through safety relays compliant to published component manufacturer's literature as a Category 3. Safety relay circuits shall include input wiring short-circuit-detection.

   Clarification: Safety devices such as certain light curtains which include the safety relay functions do not in themselves require an additional safety relay.
4. Final switching devices shall be hardware-components such as:
   a. safety-rated safety relay contacts.
   b. redundant industrial control relays (or motor starter contactors) with mechanically-linked contacts.
   c. a fluid power blocking valve applied in conjunction with the pneumatic or hydraulic motion valves.
   d. a single hardware-component such as a servo or safety-rated fluid power blocking valve when rated and applied at a minimum Category 3.
5. A feedback contact from each final switching device shall be wired into the feedback terminals of the safety relay.

   Clarification: A fluid power blocking valve requires feedback into the safety relay; pneumatic and hydraulic motion valves do not require feedback into the safety relay.

Figure 2.3.a

Category 3 sample circuit:

Light Curtain and Hydraulic Motions

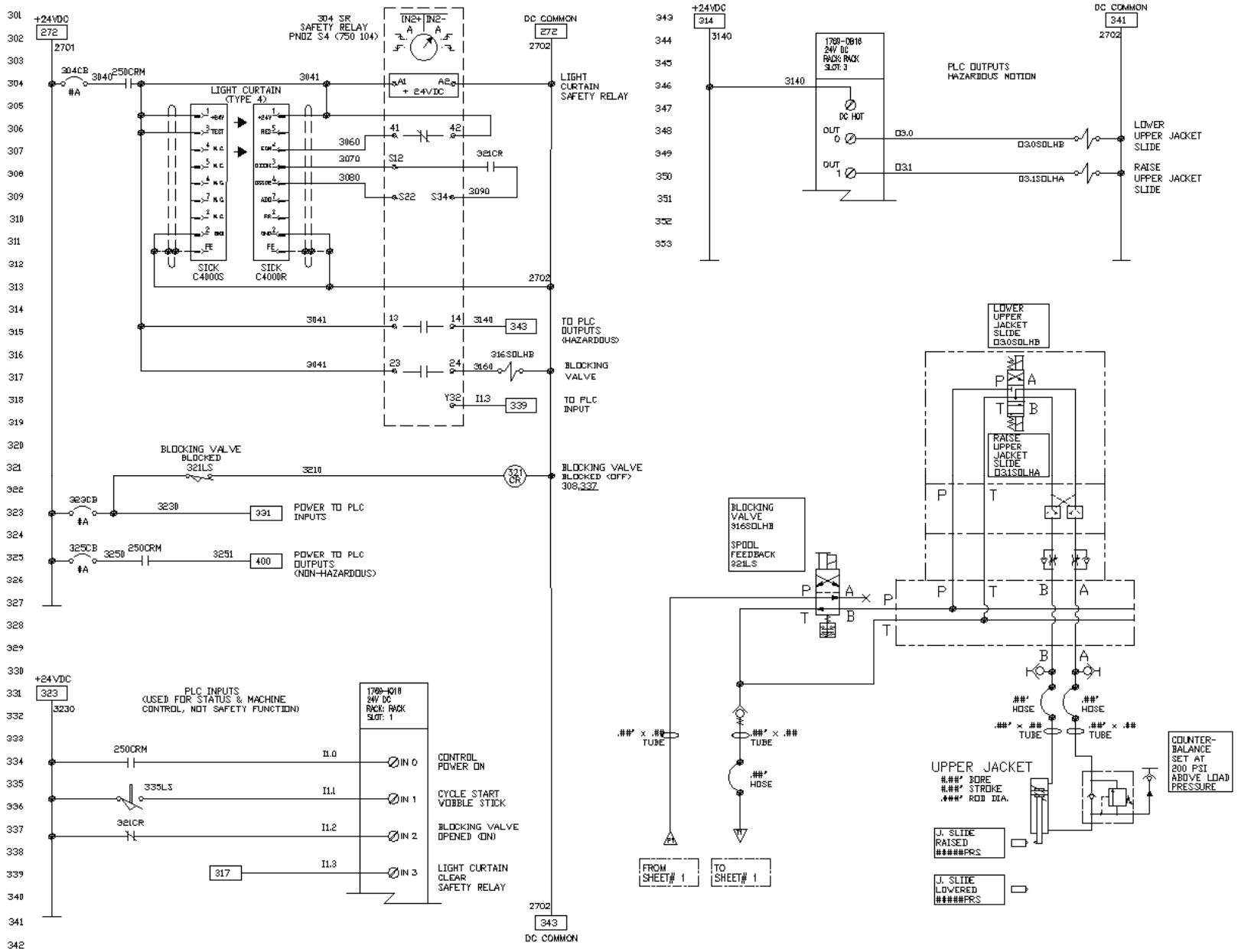


Figure 2.3.b

Category 3 sample circuit:

Locked Guard Door and Pneumatic Motions *(blocking valve not required per [3.14.3](#))*

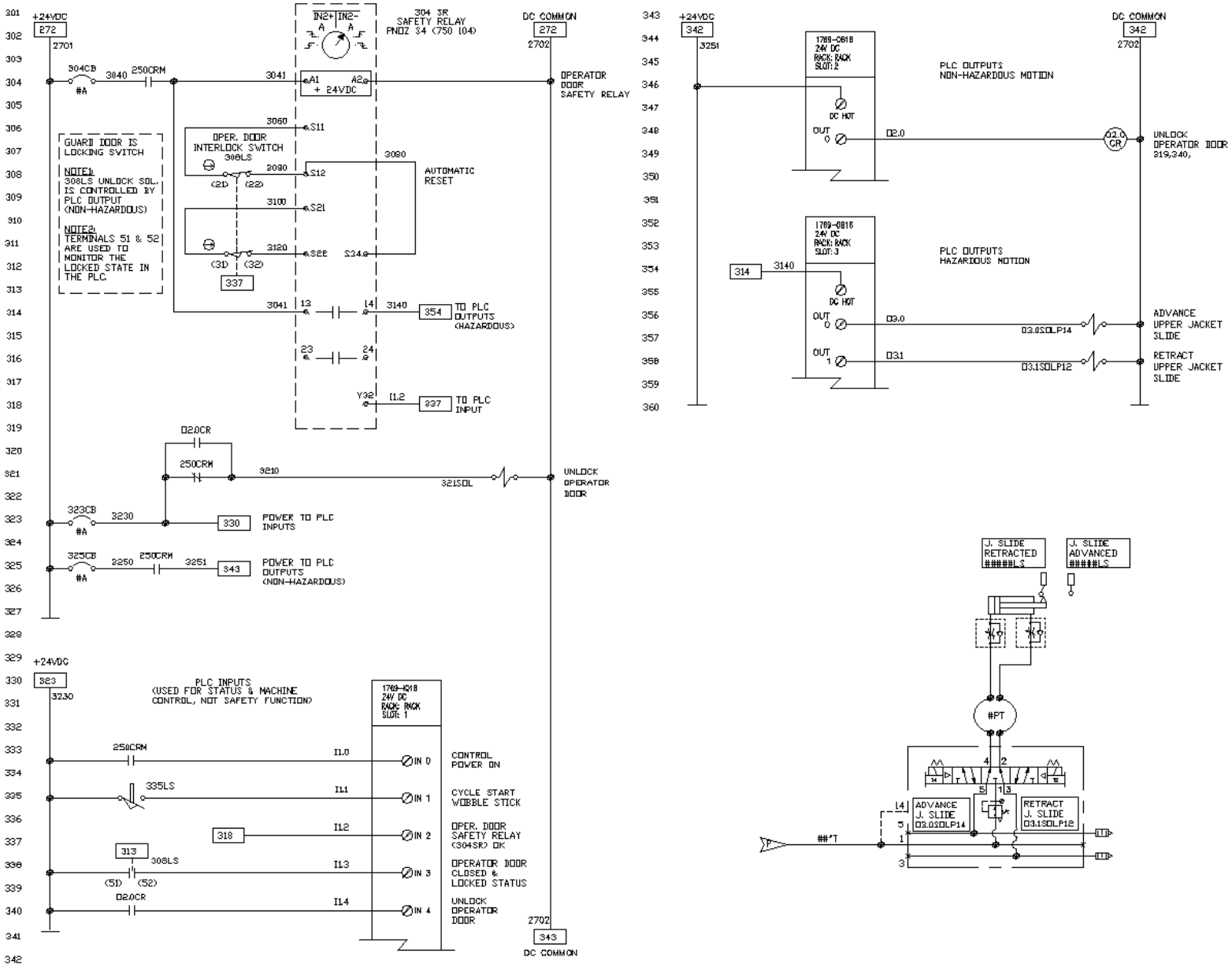
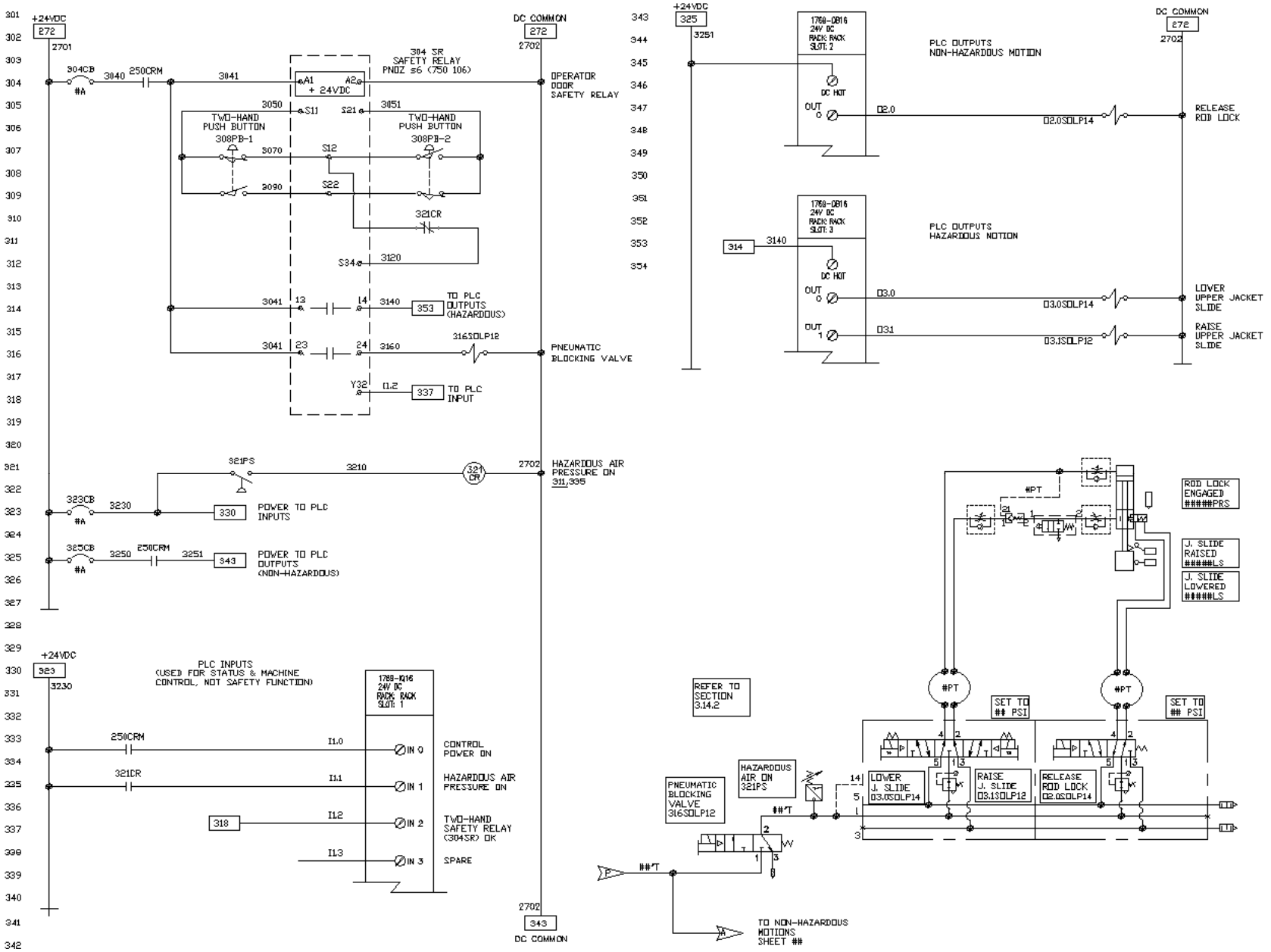


Figure 2.3.c

Category 3 sample circuit:

Two-Hand Cycle and Pneumatic Motions *(and blocking valve)*



2.4 Category 4 requirements:

As a minimum:

1. Redundancy in the SRP/SC is required.
2. The SRP/CS input devices shall meet one of the following three requirements:
   a. two devices with one positive-opening contact each, or
   b. be a Type 4 ESPE rated device, or
   c. be a minimum Category 4 technology (that is to say one input device is allowed if the device's literature clearly indicates it is Category 4 when connected in a Category 4 system).

   Exception: Two-hand control SRP/CS input device requirements are noted elsewhere in this document.
3. The safety circuit shall be hardwired. All logic functions of the SRP/CS shall be accomplished through safety relays compliant to published component manufacturer's literature at Category 4. Safety relay circuits shall include input wiring short-circuit-detection.
4. Final switching devices shall be hardware-components such as:
   a. safety-rated safety relay contacts.
   b. redundant industrial control relays (or motor starter contactors) with mechanically-linked contacts.
   c. redundant fluid power blocking valves.
   d. a single hardware-component such as a servo or safety-rated fluid power blocking valve when rated and applied at Category 4.
5. Feedback from each final switching device (including fluid power blocking valves) shall be through a mechanically-linked contact wired into the feedback terminals of the safety relay.

Figure 2.4.a

Category 4 sample circuit:

Light Curtain and Hydraulic Motions

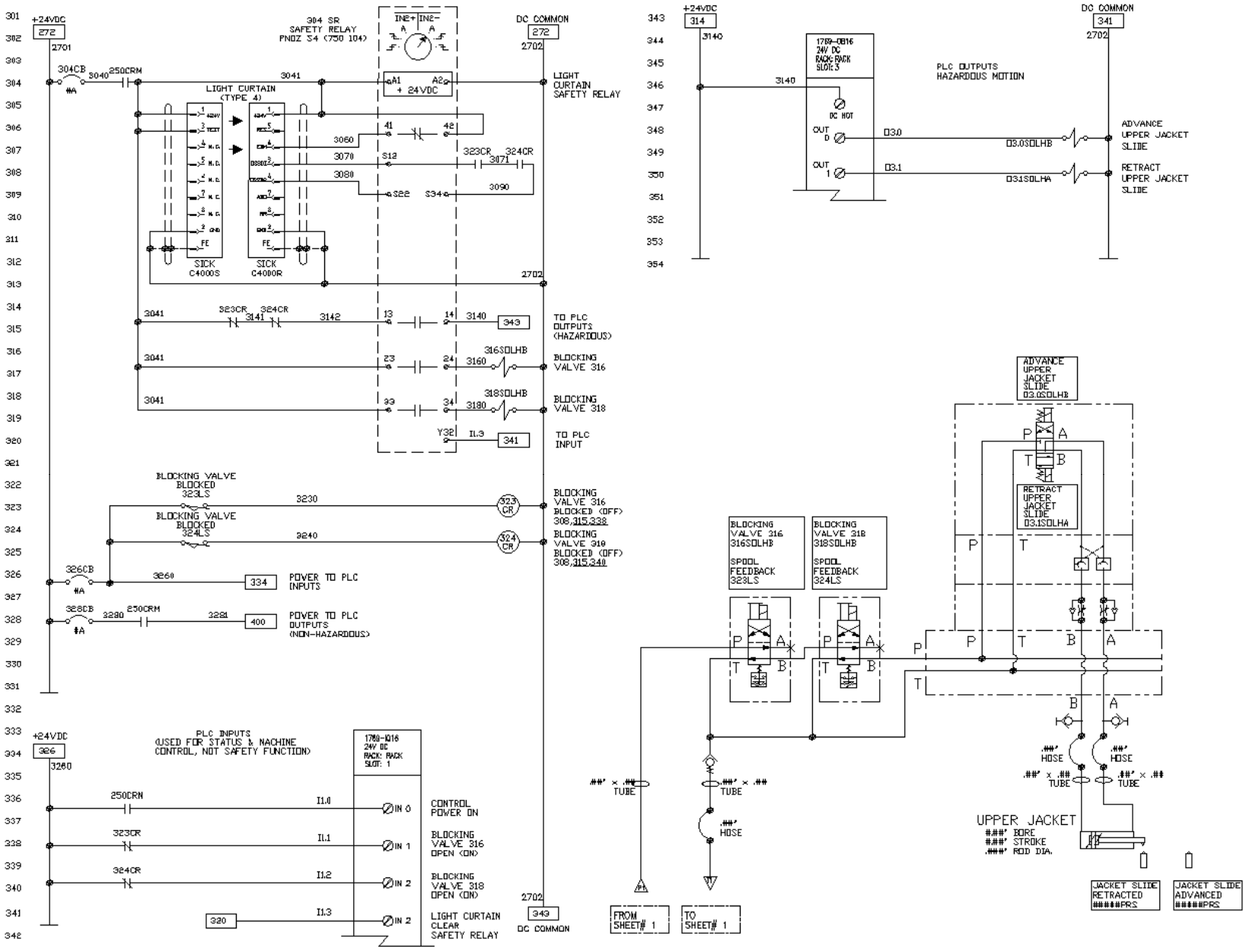
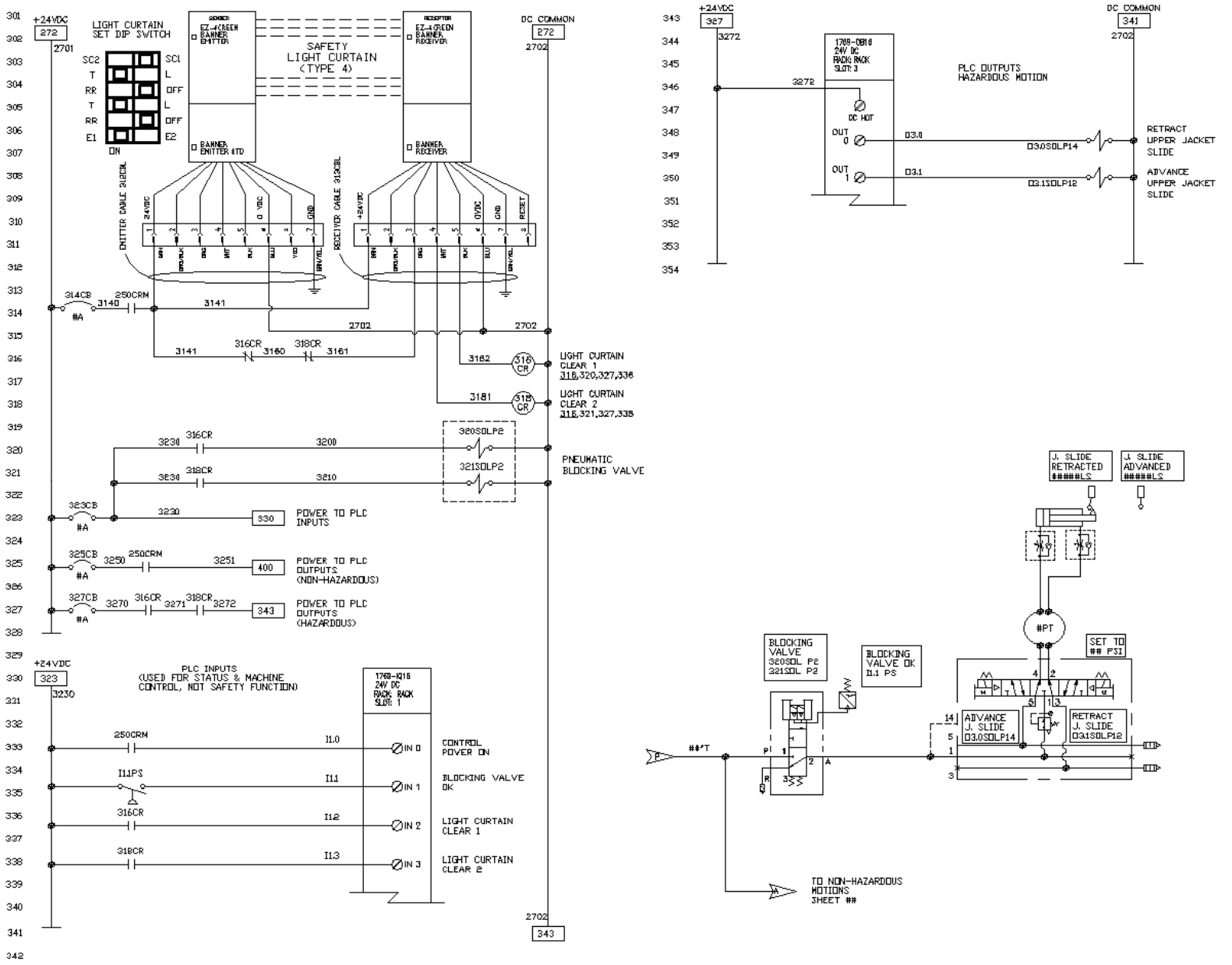


Figure 2.4.b

Category 4 sample circuit:

Light Curtain and Pneumatic Motions



This page intentional left blank

3 Application Requirements

Requirements organized by category (Category B, 1, 2, 3, and 4) are detailed in Chapter 2 above. The application requirements listed in the following chapter apply to all safety circuit categories unless explicitly noted otherwise.

3.1 Machine logic (as a consequence of interrupting a safety device)

3.1.1 The safety circuit(s) shall not disable the control circuit cycle-overtime timer unless interrupting the safety device also aborts the machine cycle.

3.1.2 Independent of the safety requirements for the safety circuits, the machine sequence logic should also give consideration to the following:

- Hazards arising from short or long term cylinder movement due to leakage, or from uncontrolled movement due to re-pressurization of cylinders that have been depleted of air, or equipment damage that can result from such an interruption
- Equipment damage that can result from allowing non-hazardous motions to continue
- Part quality if a process is stopped and/or started in mid-cycle

These considerations can in-turn affect the logical response to the drop-out of the safety circuit, but will never lower the category of a safety circuit.

Note: Machine logic requirements for safety circuit diagnostics are not covered within this specification.

3.2 Safety relay input circuits

3.2.1 Connecting several safety devices in series as inputs to the same safety relay shall follow the safety relay manufacturer's literature.

3.2.2 If four or more safety input devices are used, they shall be individually annunciated.

3.2.3 Diagnostics on safety input devices shall be done via independent contacts (such as a separate non-safety-rated contact from the safety gate interlock to a PLC), not with contacts used in the safety relay string.

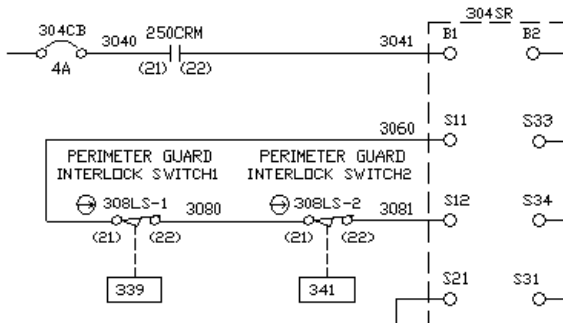


Figure 3.2.3 – Separate safety device contact for individual device annunciation

3.2.4 When a reset device is required for the safety circuit, the reset function shall be implemented such that the hazardous motions cannot be reinitiated by a reset device being tied-down.

Note: Anti-tie-down is typically a function of the reset input or feedback input on a safety relay.

3.3 Combined safety input circuits

Safety input circuits, combined in series, shall meet the most stringent circuit requirements as determined by the risk assessment.

Example: A risk assessment can document a light curtain application required to be Category 3 and a side-access door application to be Category 2. If, to minimize components, the light curtain and door interlock switch are connected in series as inputs to the same safety relay then the door interlock circuitry also has to meet all Category 3 requirements.

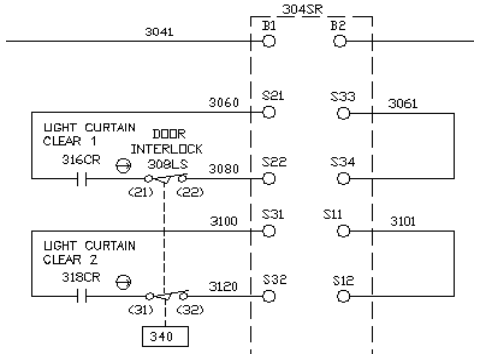


Figure 3.3 – Combined light curtain and door interlock switch

3.4 Safety relay output contacts

3.4.1 Safety relay output contacts shall be applied per the manufacture's documented contact ratings. *Note: Most safety relays have limited contact amperage ratings compared to the contacts on industrial control relays.*

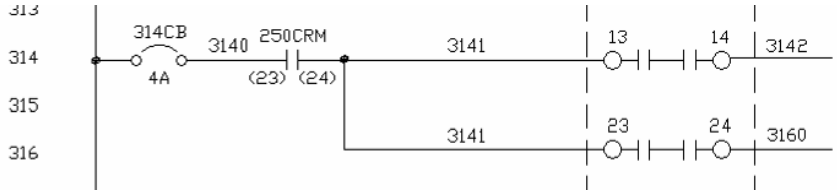


Figure 3.4.1 – Overcurrent protection for safety relay contacts

3.4.2 For category 3 circuits and category 4 circuits, when additional safety-rated contacts are required, two expansion relay/contactors shall be used.

a. Each expansion relay/contactor shall be powered through a separate safety relay output.

b. Two contacts, one from each expansion relay/contactor shall be used in series for each power-feed or hazardous device interconnection.

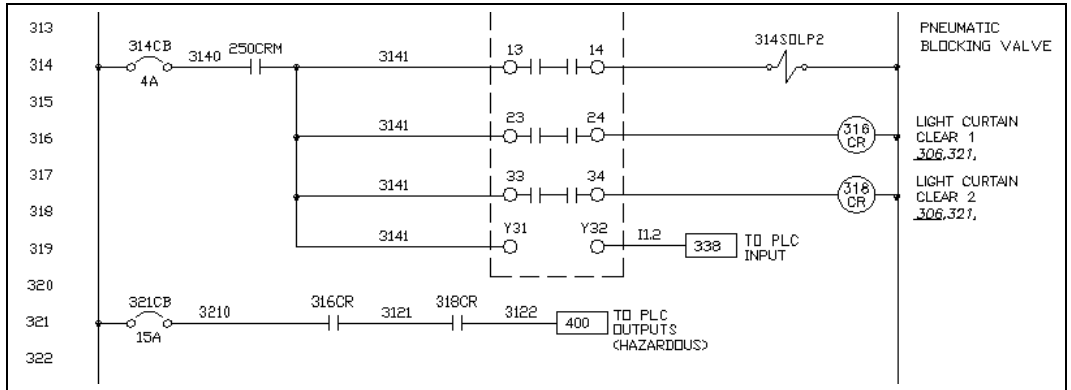


Figure 3.4.2 – Redundant expansion contacts

3.5 Final switching device feedback requirements

A final switching device is the electro-mechanical control device (such as a contactor, relay, or fluid power blocking valve) that removes power to the hazard. Regardless as to how many devices are in series after the output of a safety relay, the final switching device is the last device in the string. (Example: For a circuit in which a safety relay removes power to an expansion timer which removes power to a contactor that removes power to a motor, the final switching device is the contactor and not the expansion timer). Since many machines have multiple types of hazards (electrical, hydraulic, pneumatic, and other) many control systems will include multiple final switching devices. The feedback contact from each final switching device checks that this power removal device has properly shut-off when de-energized.

3.5.1 For Category B and Category 1 there are no feedback requirements.

3.5.2 For Category 2 or higher circuits a feedback contact from the final switching device(s) shall be wired into the feedback terminals of the safety relay.

3.5.3 Additionally, for Category 3 the feedback contact from industrial control relays or motor starter contactors applied as final switching devices shall be mechanically-linked contacts, since this is practicable. The feedback contact from all other devices applied as final switching devices is not required to be mechanically-linked.

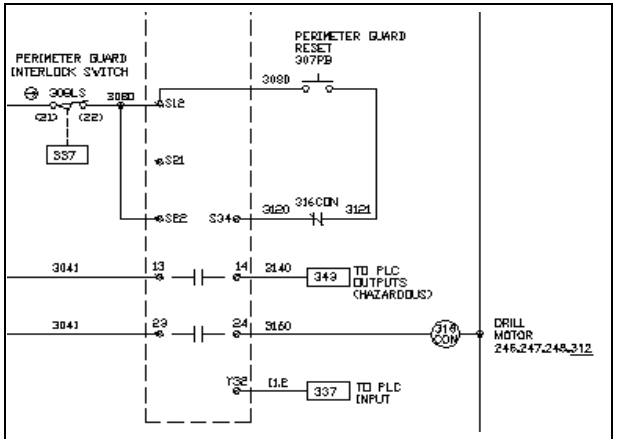


Figure 3.5.2 – Final switching device feedback contact

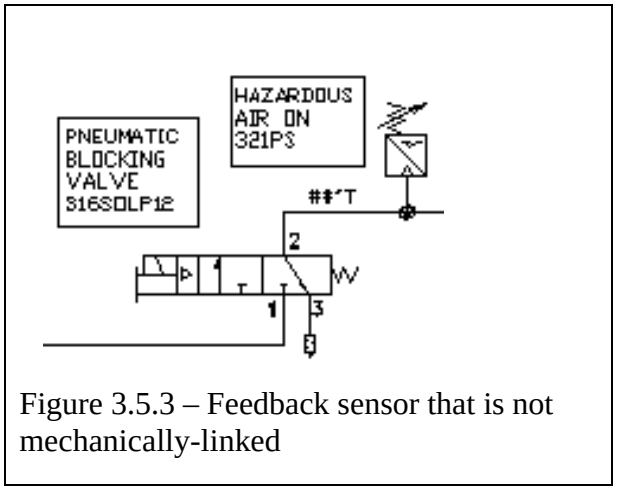


Figure 3.5.3 – Feedback sensor that is not mechanically-linked

3.5.4 Additionally, for Category 4 feedback from all final switching devices shall be provided through mechanically-linked contacts.

Exception: Feedback signals from final switching devices that do not have mechanically-linked contacts shall be designed per all of the following three requirements.

Note: This meets the reliability level of mechanically-linked feedback contacts.

a. A contact from each feedback sensor (or final switching device) shall control an industrial control relay with mechanically-linked contacts (feedback relay) (*see relays 323CR and 324CR in figure 3.5.4.a*).

b. A contact (typically normally-opened) from each feedback relay shall be connected to the safety relay feedback terminals (*see 323CR and 324CR contacts in figure 3.5.4.b*).

c. A second contact from each feedback relay (typically normally-closed, but required to be opposite-state to the feedback contact above) shall be connected in the power-feed line to the machine's hazardous devices (*see 323CR and 324CR contacts in figure 3.5.4.c*).

3.5.5 Final switching devices that meet the requirements of Category 4 safety sub-systems are not required to provide a feedback signal. *(Example: A Category 4 fluid power blocking valve does not require a feedback signal into the safety circuit.)*

Figure 3.5.4 – Category 4 Feedback: Three requirements for non-mechanically-linked final switching devices as follows:

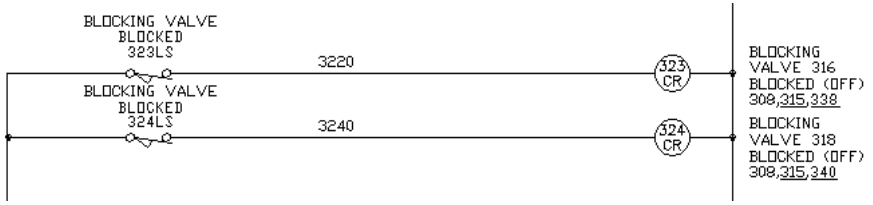


Figure 3.5.4.a - Feedback sensors controlling mechanically-linked relays

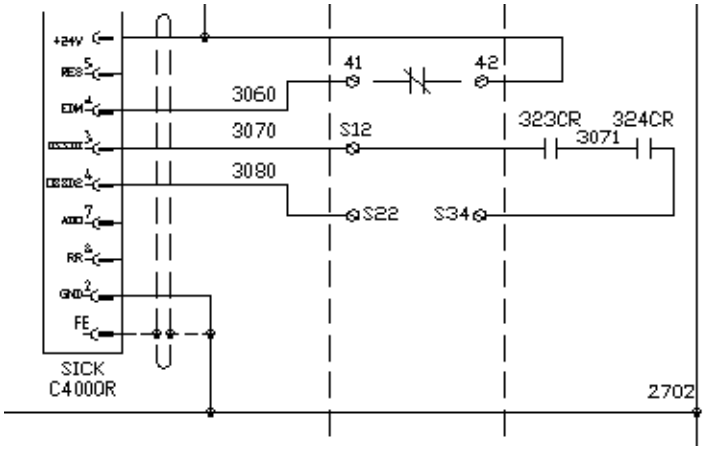


Figure 3.5.4.b - Feedback contacts into feedback terminals

Figure 3.5.4.c - Opposite-state feedback contacts in power-feed to hazardous devices

3.6 Emergency stop applications

3.6.1 Emergency stop devices and circuits (E-stop) perform an auxiliary stop function typically provided in addition to the machine's safeguarding, unless otherwise documented on the equipment's risk assessment.

3.6.2 The E-stop function shall not be bypassed.

3.6.3 The E-stop circuit shall, as a minimum, be Category 1 when all other hazards have been addressed and documented by a risk assessment.

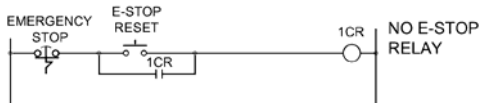


Figure 3.6.3 – Category 1 E-stop

3.6.4 E-Stop is often combined with the control Power On (Master Start) circuit, and/or combined with a machine's Category 2 perimeter guard door circuit.

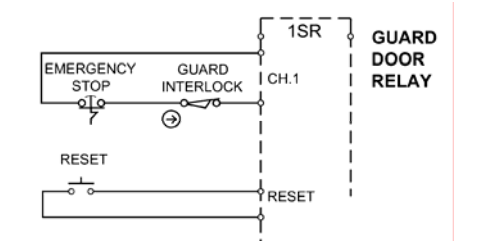


Figure 3.6.4 – E-stop combined into a Category 2 circuit

3.6.5 E-stop pushbuttons shall comply with IEC 60947-5-5. They shall be a red mushroom-head, the self-latching type requiring manual reset after actuation, and include background (such as the identification tag) colored YELLOW.

3.6.6 Safety-rated cable-operated E-stop switches shall comply with IEC 60947-5-5. They shall have a contact(s) that opens both when the cable is pulled or when cable tension is lost, and have contacts that latch in the open position until the switch is manually reset.

3.6.7 E-stop devices shall be readily accessible, located at each operator control station as a minimum.

3.6.8 E-stop devices shall be connected directly to a hardwired relay. The relay shall:

a. perform the required emergency stop function.

b. be reset (start) by a contact from the Master Start pushbutton, an E-stop reset pushbutton, or a PLC contact output with logic initiated by an HMI reset button.

c. not be reset by pulling-out or twist-release of an E-stop pushbutton.

d. not reset on application of power.

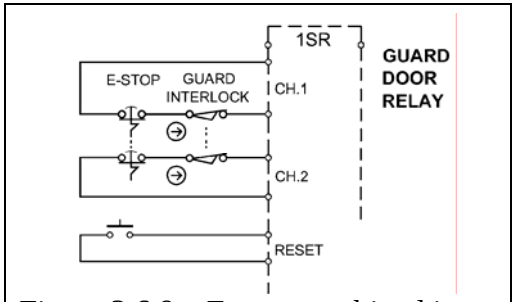


Figure 3.6.9 – E-stop combined into a Category 3 circuit

3.6.9 Combining E-stop with other safety device input circuitry is permitted and shall meet the most stringent category as determined by the risk assessment.

a. For Category 2: E-stop pushbuttons and cable-operated switches shall, at a minimum, have one normally closed contact connected to the safety relay input.

b. For Category 3 and 4: E-stop pushbuttons and cable-operated switches shall have two normally closed contacts connected to separate safety relay inputs.

3.7 Safety interlock switch applications

Safety interlock switch applications include all interlocked physical barriers such as interlocked guard doors, hinged guards, fencing, gates, hand-operated and machine-operated access doors, mechanical point-of-operation guarding, perimeter guarding, and interlocked mechanical components as documented on the risk assessment.

3.7.1 Safety interlock switches shall comply with EN 1088, IEC 60947-5-1, and IEC 60947-5-3.

Note: Solenoid-latching safety interlock switches compliant to EN 1088 are latched when de-energized.

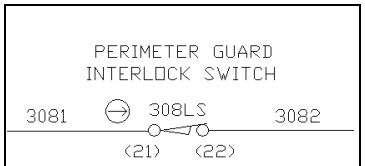


Figure 3.7.3 – Positive-opening contact symbol

3.7.2 Safety interlock switches on Category 2, Category 3, and Category 4 applications shall be connected into a safety relay.

3.7.3 Safety circuit input contacts used from safety interlock switches on Category 2, Category 3, and Category 4 applications shall be positive-opening.

3.7.4 A solenoid-position contact from solenoid-latching safety interlock switches shall be connected to the machine control system for diagnostics and process control.

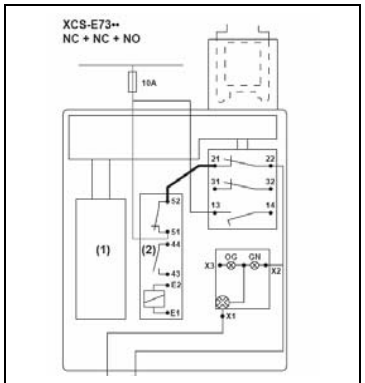


Figure 3.7.4 – Solenoid latching switch terminals

Note: Typically a factory-installed jumper from the solenoid-position contact to a safety contact exists, and may need to be removed since the solenoid-position contact is not to be connected to the safety circuit.

3.7.5 Power to unlatch a solenoid-latching safety interlock switch shall include a normally-closed contact from CRM in parallel with any application logical output.

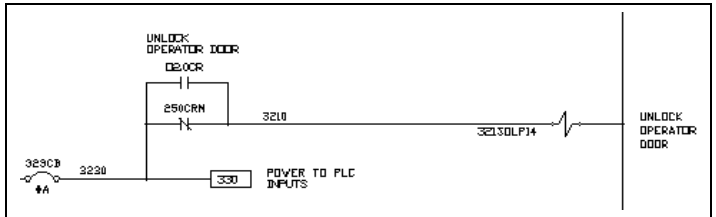


Figure 3.7.5 – Solenoid unlatch circuit

3.7.6 Safety interlock switches shall be located and mounted to minimize tampering. They shall not be easily defeated with ordinary hand tools or by tying down the actuators.

3.7.7 Solenoid-locking safety interlock switches require an unlock-override. The switches shall be located such that the unlock-override can be accessed.

3.7.8 When it is possible for a person to completely pass through an interlocked guard door, placing their body between that interlocked guard door and the hazard, the following reset requirements shall apply:

a. A safety interlock circuit reset device shall be provided. The safety interlock circuit shall not be reset by the physical closure of the safety interlock switch or by the return of line voltage (power-up).

b. The reset device shall be positioned such that it cannot be reached from within the protected area.

c. The reset device shall be positioned such that the entire area protected by the perimeter guard is visible.

Exception: Where the entire area protected by the perimeter guard is not visible from a single reset location, multiple reset devices shall be installed. The location of these reset devices shall be such to collectively allow viewing the entire area protected by the perimeter guard. The number of reset locations should be minimized. The reset devices shall be connected to an appropriate safety circuits which is designed to impose a certain reset sequence with specific timing.

d. Multiple, independent reset devices are permitted, provided the entire area protected by the perimeter guard is visible from each reset location.

e. Safety interlock circuit reset devices are permitted to be control devices that also perform a different function, such as the Master Start pushbutton, provided all the reset requirements above are met.

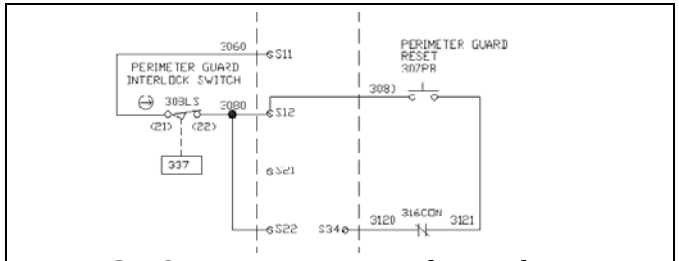


Figure 3.7.8.a – Perimeter guard reset device

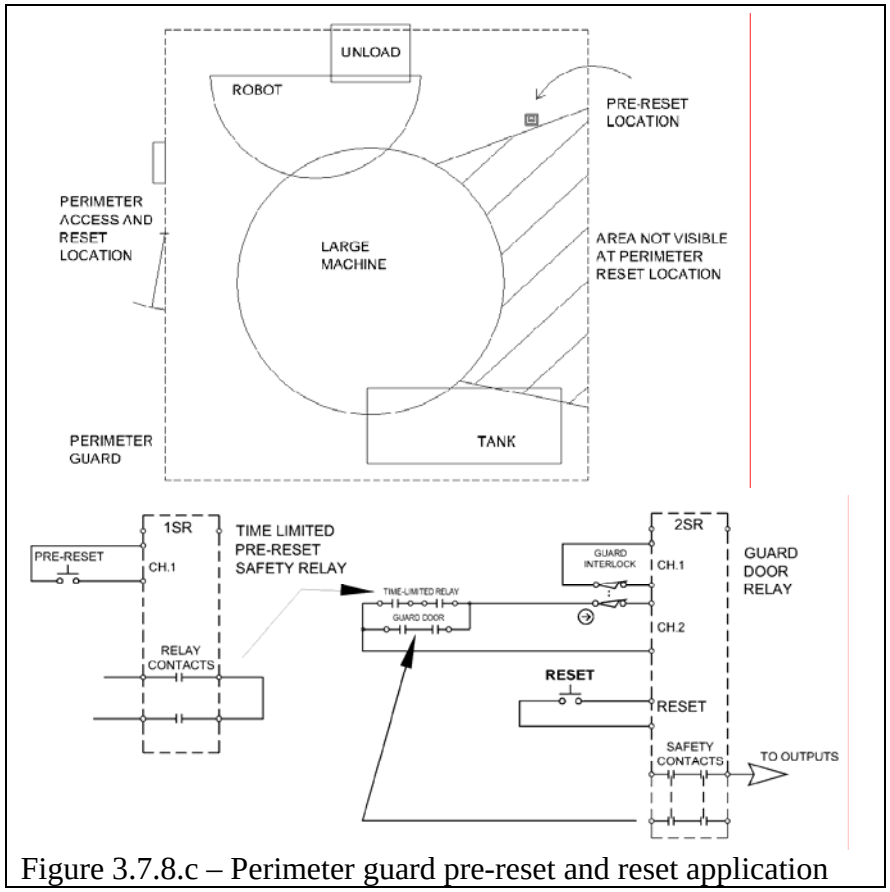


Figure 3.7.8.c – Perimeter guard pre-reset and reset application

3.8 Light curtain applications

3.8.1 Light curtains shall be certified in compliance with IEC 61496-1 and IEC 61496-2.

3.8.2 For Category 1 the light curtain shall (at a minimum):

a. be a Type 2 ESPE device.

b. remove power to the final switching device through a hardwired circuit.

3.8.3 For Category 2 the light curtain shall (at a minimum):

a. be a Type 4 ESPE device.

b. include an output to a single channel safety relay or a single industrial control relay with feedback to the light curtain external device monitoring terminals.

Note: Some light curtains have an embedded safety relay, or safety-rated relay output contacts, designed to the appropriate category such that the machine hazards may be driven directly from these relays. They also include appropriate external device monitoring terminals (feedback terminals).

3.8.4 For Category 3 and 4 the light curtain shall:

a. be a Type 4 ESPE device (at a minimum).

b. output to an appropriately rated safety relay or two mechanically-linked industrial control relays with feedback to the light curtain external device monitoring terminals.

Note 1: Some light curtains have an embedded safety relay, or safety-rated relay output contacts, designed to the appropriate category such that the machine hazards may be driven directly from these relays. They also include appropriate external device monitoring (feedback terminals).

Note 2: Light curtains that provide two solid-state output signals with short-circuit-detection may be wired directly into two 24vdc safety relay inputs.

3.8.5 Light curtains shall be mounted in accordance with the safe distance formula. Reference Annex B.

3.8.6 When it is possible for a person to completely pass through the light curtain, placing their body between the light curtain and the hazard, the reset requirements from the *Safety interlock switch applications* in Section 3.7.8 above shall apply.

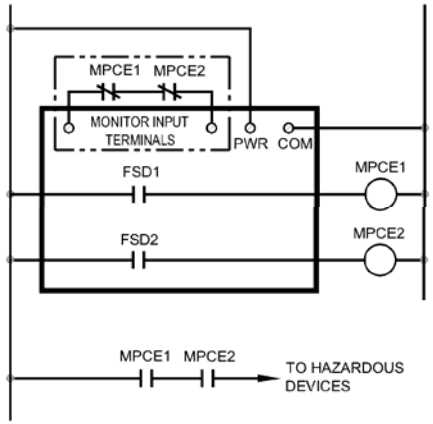


Figure 3.8.4.b – Light curtain control unit connected to mechanically-linked relays

3.9 Bypassed and muted safety circuits

3.9.1 Bypassing a safety circuit with another safety circuit is permitted as documented on the risk assessment. Bypassing shall be accomplished either by combining (in parallel) the outputs from the two safety circuits, or by combining (in parallel) two safeguarding devices as inputs into one safety circuit. Example bypass circuits include a live-man switch application or two-hand manual control.

3.9.2 Auto mode shall be inhibited when a safeguard is bypassed for any purpose other than normal machine cycle, such as set-up, calibration, tool change, and troubleshooting.

3.9.3 Safety inputs circuits, when combined in parallel, shall:

a. meet the most stringent input circuit requirements.

b. be selectable through mechanically-linked contacts from an industrial control relay, such that only one input circuit can be active.

Example: For a live-man switch (enabling device) application, provided to view limited machine motion while a point-of-operation guard door is open, the risk assessment documents the live-man switch application as Category 2 (allowing a single input) and the point-of-operation guard door application as Category 3 (requiring redundant inputs). Because of this Category 3 requirement the live-man switch will also require redundant inputs into the guard door safety relay.

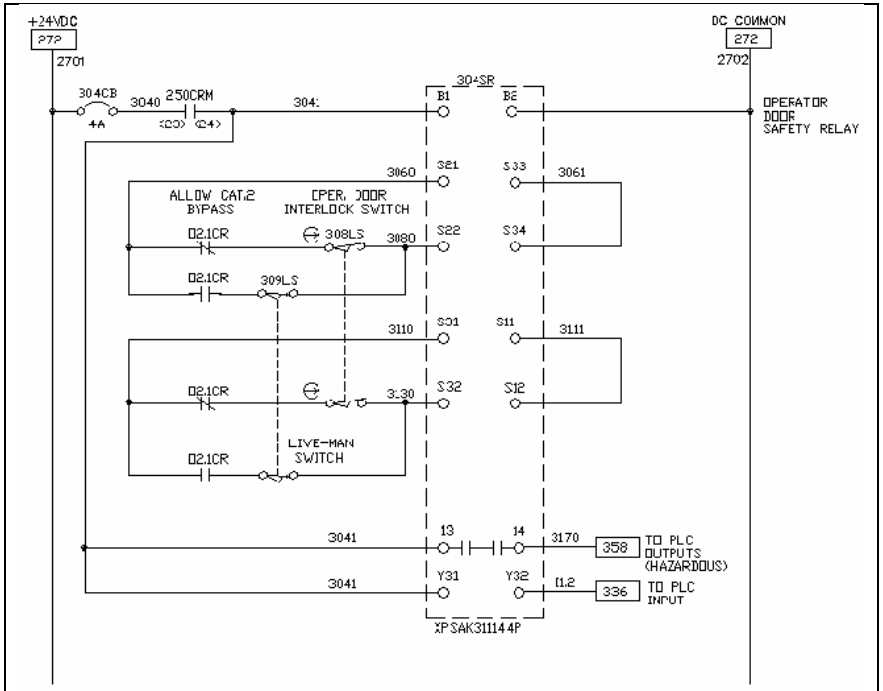


Figure 3.9.3 – Live-man switch bypassing guard door inputs

3.9.4 For additional Category 2, 3, and 4 parallel input example circuits refer to the two-hand manual control requirements in Section 3.13.

3.9.5 Muting a safety circuit with another safety circuit is permitted as documented on the risk assessment.

a. Muting shall be accomplished by combining (in parallel) the two safety circuit's outputs.

b. Muting shall meet the most stringent circuit requirements as determined by the risk assessment, including final switching device and feedback requirements.

Example: For an operator-loaded grinder, both an inner door and outer door provide for operator protection during loading and part-processing respectively. The risk assessment documented both door applications. When the outputs of these safety circuits are integrated in parallel, each circuit has to be implemented to the most stringent category of the two applications including that category's final switching device and feedback requirements.

3.9.6 Muting the point-of-operation guard during the machine load/unload is required for Category 3 pneumatic blocking valve applications. Refer to Annex C for the required muting circuit.

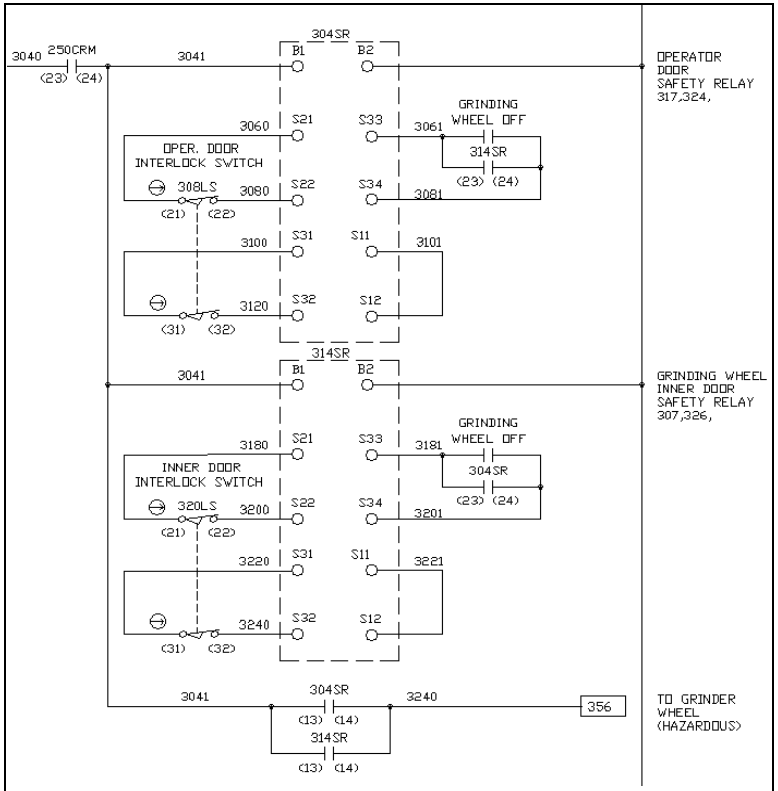


Figure 3.9.5 – Category 3 automatic inner door output, in parallel with a Category 3 outer operator door output

3.10 Two-hand control – general

The following are requirements for two-hand control, whether applied as machine cycle initiation or applied as manual control.

3.10.1 Two-hand control devices shall be design, constructed, and arranged to:

a. protect against unintended or inadvertent operation of the machine.

b. require the use of both hands for actuation (separation such that the operator cannot operate the two devices by the use of one hand and the elbow, or other portion, of the same arm).

c. be located at a distance from the nearest hazard such that the operator cannot reach the hazard before cessation of hazardous motion. Reference Annex B.

3.10.2 Limit switches shall not be used for two-hand control operators. *Note: Limit switches applied as two-hand control are too easily defeated.*

3.10.3 Two-hand control circuits shall be designed such that:

a. continuous concurrent actuation by both hands is required during the hazardous situation.

b. machine operation shall cease upon the release of either one or both of the control devices when hazardous situations are still present.

3.11 Two-hand control - machine cycle initiation

Note: Two-hand control implemented for machine cycle initiation, documented in the risk assessment as "frequent exposure", will require either a Category 1 or a Category 3 (or 4).

3.11.1 Category 1 two-hand cycle initiation shall:

a. be hardwired, as a minimum, per figure 3.11.1.

b. require the release of both control devices before machine operation can be reinitiated.

c. require the control devices be actuated within a time limit of each other, not exceeding 2.0 seconds. Where this time limit is exceeded, both control devices shall be released before machine operation can be initiated.

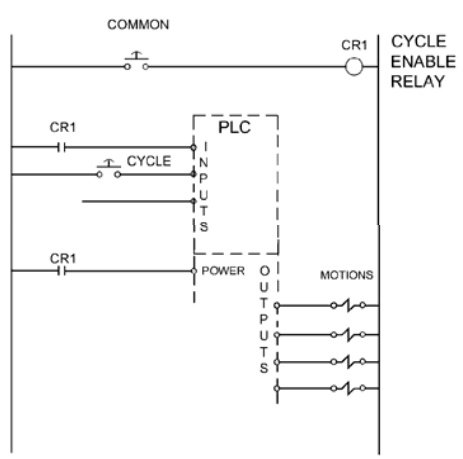


Figure 3.11.1 – Category 1 two-hand machine cycle initiation

3.11.2 Category 3 and Category 4 two-hand cycle initiation shall:

a. require the use of a two-hand control safety relay of the appropriate category.

b. require final switching device(s) and feedback circuits implemented to the appropriate category per Chapter 2.

Note: Anti-tie-down and control device input concurrency time of 0.5 seconds are included within Category 3 and Category 4 two-hand control safety relays.

3.11.3 For all categories, consecutive machine cycles shall not result even though both control devices are continuously actuated.

3.12 Two-hand control – Category B two-hand manual control

Note: Category B two-hand manual control circuits are typically implemented as a bypass on equipment that includes a Category 1 point-of-operation guard.

3.12.1 Category B two-hand manual control shall be implemented as a Category 1 two-hand control per the following conditions. It shall:

a. be hardwired, as a minimum, per figure 3.12.1.

b. include pushbuttons on the machine HMI as the second control device.

c. require the release of both control devices before the next manual motion command can be initiated.

d. require the control devices be actuated within a time limit of each other, not exceeding 2.0 seconds. Where this time limit is exceeded, both control devices shall be released before the next manual motion command can be initiated.

Note: Category 1 two-hand manual control applications do not exist / are not covered by this specification.

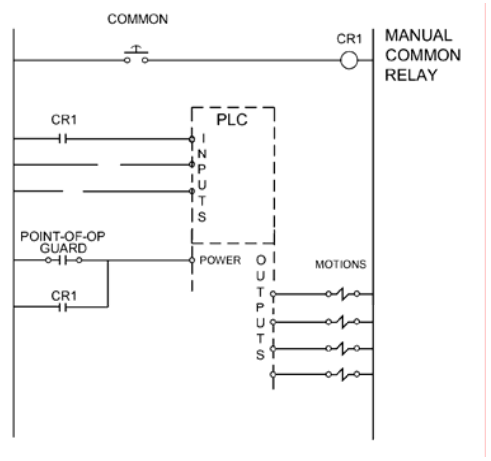


Figure 3.12.1 – Category B two-hand manual control

3.13 Two-hand control - Category 2 two-hand manual control

Note: Category 2 two-hand manual control circuits are typically implemented as a bypass on equipment that includes a Category 3 (or 4) point-of-operation guard, although they can also be used to bypass a Category 2 perimeter guard.

3.13.1 Category 2 two-hand manual control circuits shall be implemented as redundant, parallel inputs into the guard safety relay.

Note: If the guard is a light curtain, the light curtain will have to be implemented as redundant inputs into a safety relay (and not the industrial control relay option allowed in Section 3.8.4.b) such that the Category 2 two-hand manual control can be implemented.

Note: If the guard is a Category 2 perimeter guard, the guard will have to be implemented as redundant inputs into a safety relay such that the Category 2 two-hand manual control can be implemented.

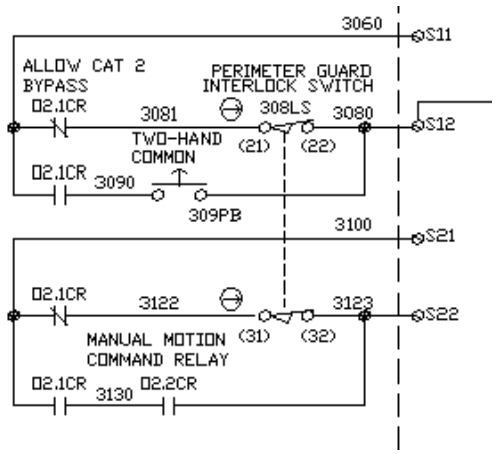


Figure 3.13.1 – Category 2 two-hand manual control bypass parallel inputs

3.13.2 The two-hand control inputs shall consist of one Two-Hand Common pushbutton and one PLC output relay labeled “Manual Motion Command”.

a. Both the Two-Hand Common pushbutton and the Manual Motion Command relay shall have contacts run to separate PLC inputs for machine logic and diagnostics.

b. The Manual Motion Command output logic shall be driven by the HMI through logic functionally equivalent to figure 3.13.2.b.

c. The PLC logic shall require the release of both control devices (the Two-Hand Common and HMI pushbutton) before the next manual motion command can be initiated.

d. The PLC logic shall require the two-hand control devices be actuated within a time limit of each other, not exceeding 2.0 seconds. Where this time limit is exceeded, both control devices shall be released before the next manual motion command can be initiated.

The following three rungs set up the output for
the MANUAL MOTION COMMAND RELAY,
which is the second input to the two-hand safety relay

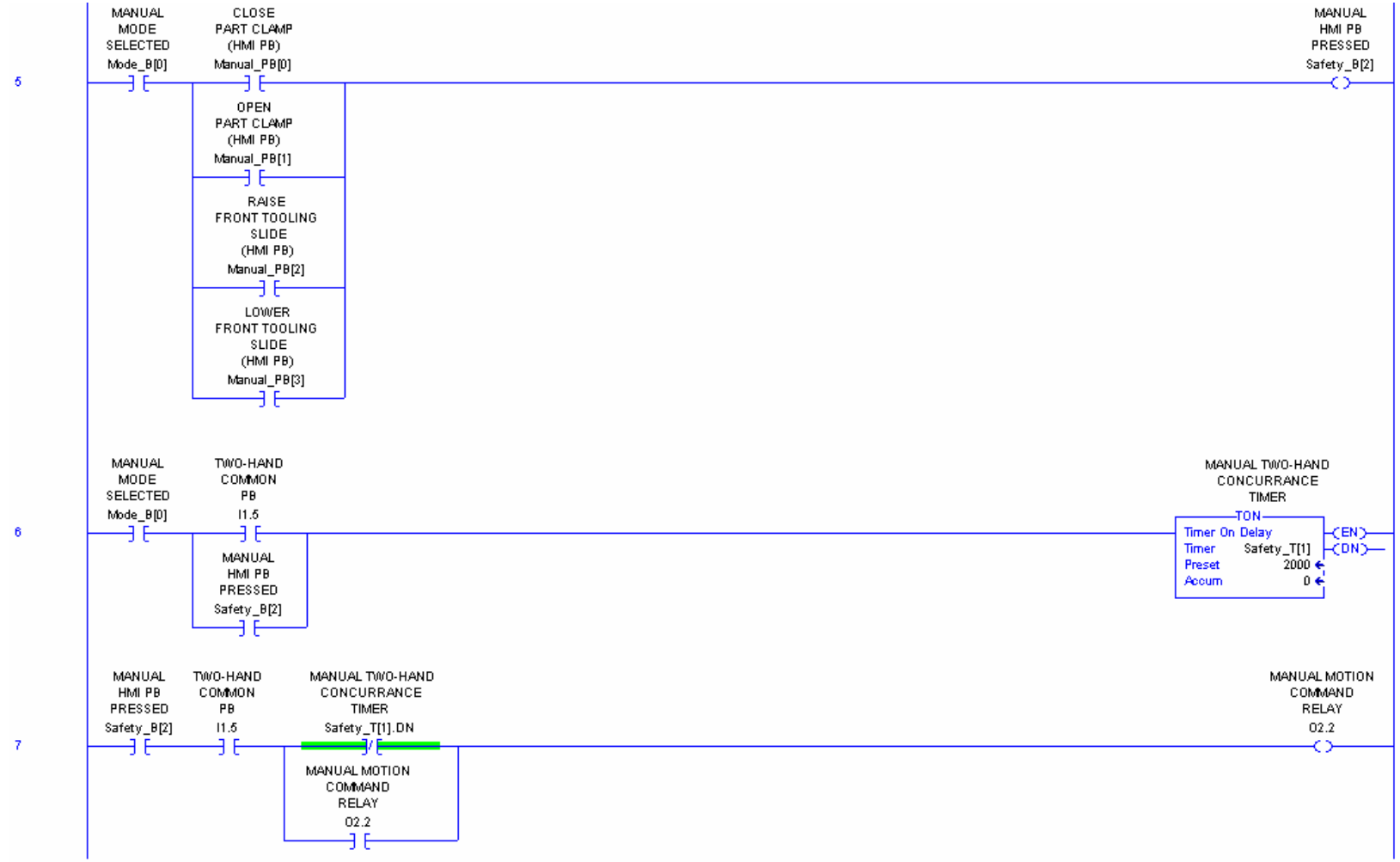


Figure 3.13.2.b –Category 2 Manual Motion Command Relay output logic

3.13.3 The redundant parallel inputs (two-hand control or guarding) shall be selectable through mechanically-linked contacts from an industrial control relay labeled “Allow Category 2 Bypass” such that only one input circuit can be active.

a. Normally-open contacts shall enable the two-hand control inputs; normally-closed contacts shall enable the guarding inputs.

b. The Allow Category 2 Bypass relay shall be driven by PLC output logic functionally equivalent to figure 3.13.3.b.

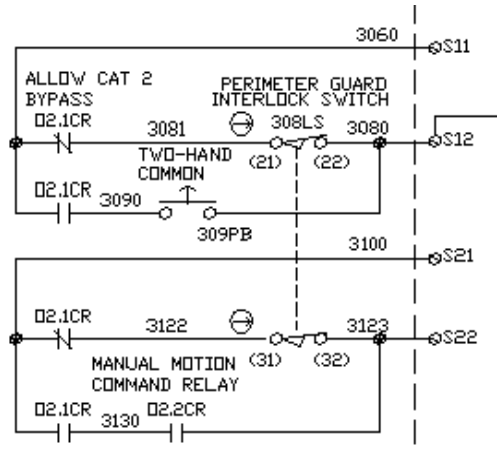


Figure 3.13.3 – Allow Category 2 Bypass relay

The following three rungs set up the output for the ALLOW CATEGORY 2 BYPASS relay

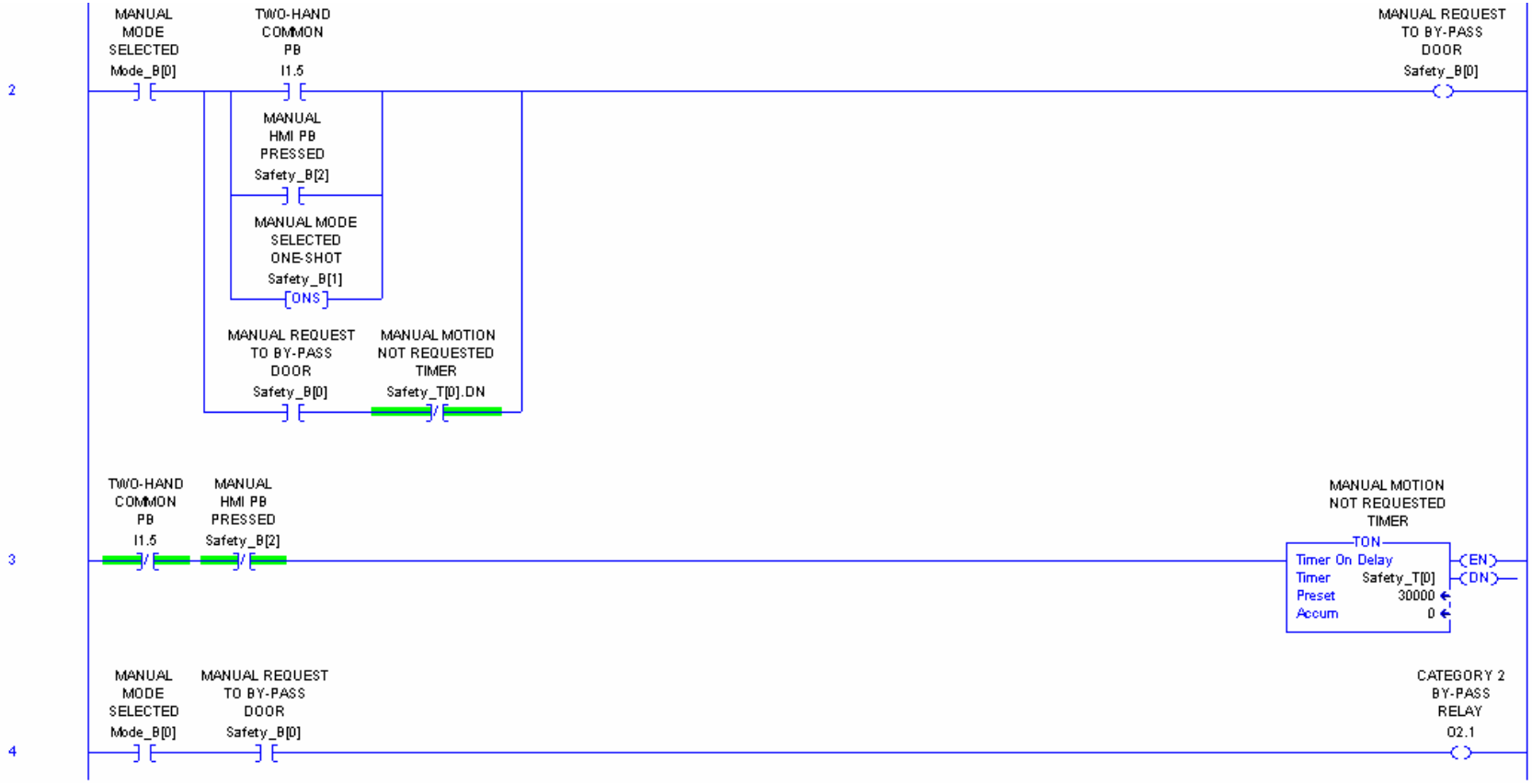


Figure 3.13.3.b –Category 2 Allow Category 2 Bypass relay output logic

3.13.4 For Category 2 two-hand manual control bypass of a Category 3 or Category 4 point-of-operation guard, the final switching device and feedback circuit requirements are determined by the risk assessment for the point-of-operation guard, as either Category 3 or Category 4 per Chapter 2.

Note: If a solenoid-locked door was implemented to eliminated the blocking valve(s) for a Category 4 point-of-operation guard, then the addition of a Category 2 two-hand manual control bypass includes the requirement of the blocking valve(s).

3.13.5 The Category 2 two-hand manual control bypass of a Category 2 perimeter guard will typically require the bypass of the Reset button, but shall never bypass the feedback from any final switching device.

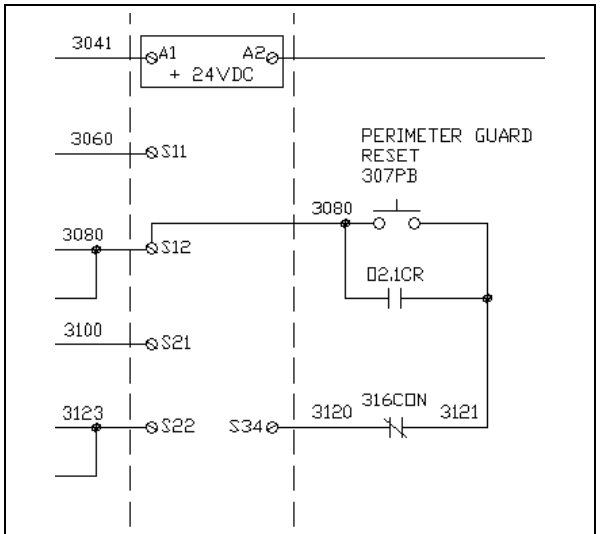


Figure 3.13.5 – Category 2 two-hand manual control bypass of reset button

This page intentional left blank

3.14 Pneumatic applications

3.14.1 Category B, Category 1, and Category 2 pneumatic safety circuit requirements are met by the removal of electrical power to the motion valves per the electrical requirements of the category.

3.14.2 Category 3 circuits require a blocking valve used in conjunction with the motion valves.

Note: A single Category 4 rated blocking valve may be used in place of a standard blocking valve and final switching device feedback circuits.

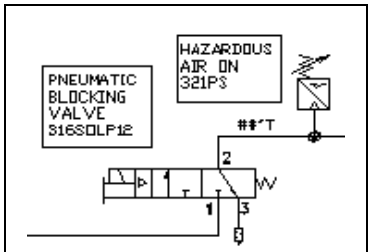


Figure 3.14.2 – Category 3 pneumatic blocking valve

3.14.3 For Category 3 circuits, the blocking valve is not required when both of the following conditions are met:

a. The risk reduction method is a solenoid-locked door, locked closed preventing personnel from opening the door until the hazards cease, and

b. the motion valves are not capable of initiating hazardous motion without being given an electrical command. The Festo VTSA series of valves listed in Nexteer Automotive's SD-007-GC meet this requirement.

3.14.4 Category 3 motions with hazards in only one direction do not require a blocking valve when the motion is controlled by a two single-solenoid valve circuit designed per figure 3.14.4.

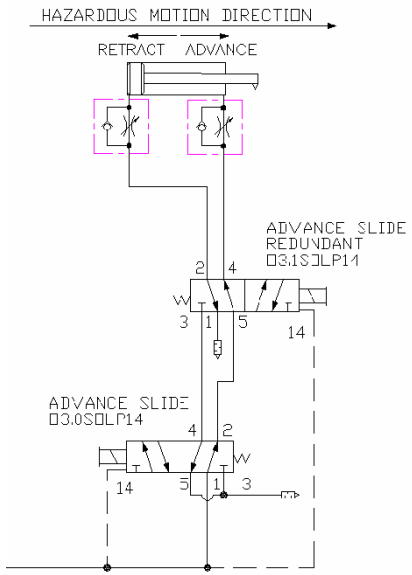


Figure 3.14.4 – Permitted circuit for Category 3 hazard in one direction

3.14.5 Category 4 circuits require the use of a blocking valve selected from the Safety Valve section of Nexteer Automotive's SD-007-GC.

3.14.6 For Category 4 circuits, the blocking valve is not required when all three of the following conditions are met:

a. The risk reduction method is a solenoid-locked door, locked closed preventing personnel from opening the door until the hazards cease, and

b. manual motions require the solenoid-locked door to be locked closed, and

c. the motion valves are not capable of initiating hazardous motion without being given an electrical command. The Festo VTSA series of valves listed in Nexteer Automotive's SD-007-GC meet this requirement.

(Category 3 and Category 4 blocking valve requirements continue on the next page)

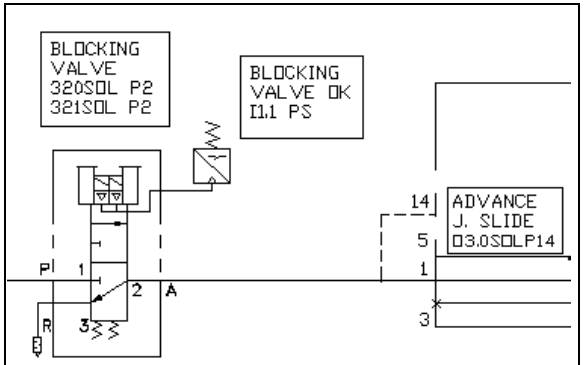


Figure 3.14.5 – Category 4 pneumatic blocking valve

3.14.7 For Category 3 and Category 4 circuits, blocking valves shall:

a. exhaust when in the electrically de-energized state.

b. include feedback circuitry meeting the feedback requirements in Section 3.5.

c. include diagnostic input to the PLC (if a status switch or diagnostic indication is provided with the blocking valve).

d. be mounted according to the manufacturer's recommendations and as close to the motion valves as possible to minimize stop time. Refer to Annex B. *Note: This includes minimizing line volumes.*

3.14.8 For Category 2, 3, and 4, system filtration shall be provided such that the air quality meets ISO 8573-1 class 5.5.5.7.4 as a minimum. *Note: Use of filters from the Air Preparation section of Nexteer Automotive's SD-007-GC is one method of meeting this ISO classification.*

3.14.9 Piston rods shall be equipped with rod wipers and scrapers wherever possible to minimize contamination ingression.

3.14.10 Exhaust mufflers shall be sized and plumbed such that they do not restrict the flow of the safety exhausting function.

3.14.11 Motion valves (or directional valves) shall be mounted:

a. such that the main spool and pilot spools are in the horizontal position to prevent the effects of gravity from influencing the valves operation and causing motion.

b. as close to the actuator(s) as practicable to minimize stop time. Refer to Annex B. *Note: Line lengths between the motion valves and actuator should be 18 inches or less.*

3.14.12 Motion valves shall be selected based on the motion desired when the electrical command signal is removed.

a. Single solenoid valves are allowed for control of actuators with strokes less than 3 inches when the desired action is a return to the home position. *An example is a conveyor stop that engages the pallet upon loss of the electrical command.*

b. Single solenoid valves are allowed for control of actuators with strokes longer than 3 inches when there is no hazard in the electrically de-energized position.

c. The use of double solenoid detented valves is discouraged. Double solenoid detented valves are allowed for control of actuators with strokes less than 3 inches when the desired action is to maintain the last commanded position such as some clamp applications. Hazards shall be eliminated such that personnel cannot enter the hazardous motion before it stops.

Note: Mechanical means of eliminating the pinch point can include - tooling design such that pinch points are inaccessible (within the tooling), or tooling design such that the part covers any pinch points, or the addition of a fixed guard located at the pinch point. A method of removing the stored energy can include the addition of a blocking valve.

d. Double solenoid three-position valves with an exhaust center spool configuration shall be used for control of actuators with strokes exceeding 3 inches and for stopping the actuator motion in mid-position by removal of the electrical command signals.

e. Double solenoid three-position valves with an exhaust center spool configuration are allowed for all other applications.

f. Blocked center valves shall not be used. *Note: Blocked center valves can create stored energy on both sides of the actuator creating potential for injury should one of the sides have a leak.*

3.15 Hydraulic applications

3.15.1 Category B, Category 1, and Category 2 hydraulic safety circuit requirements are met by the motion valves upon the removal of electrical power at the appropriate category.

3.15.2 Category 3 circuits require a blocking valve used in conjunction with the motion valves.

3.15.3 For Category 3 circuits, the blocking valve is not required when both of the following conditions are met:

a. The risk reduction method is a solenoid-locked door, locked closed preventing personnel from opening the door until the hazards cease, and

b. the motion valves are not capable of initiating hazardous motion without being given an electrical command. The hydraulic directional control valves listed in Nexteer Automotive's SD-007-GC meet this requirement.

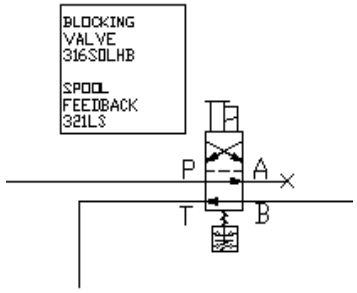


Figure 3.15.2 – Category 3 hydraulic blocking valve

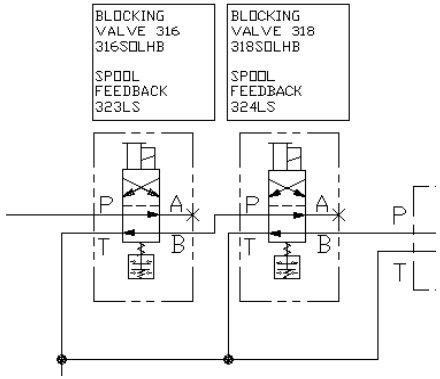


Figure 3.15.4 – Category 4 redundant hydraulic blocking valves

3.15.4 Category 4 circuits require redundant blocking valves, or a Category 4 blocking valve.

3.15.5 For Category 4 circuits, the blocking valve is not required when all three of the following conditions are met:

a. The risk reduction method is a solenoid-locked door, locked closed preventing personnel from opening the door until the hazards cease, and

b. manual motions require the solenoid-locked door to be locked closed, and

c. the motion valves are not capable of initiating hazardous motion without being given an electrical command. The hydraulic directional control valves listed in Nexteer Automotive's SD-007-GC meet this requirement.

3.15.6 For Category 3 and Category 4 circuits, blocking valves shall:

a. block the hazardous energy supply when in the electrically de-energized state.

b. include feedback circuitry meeting the feedback requirements in Section 3.5.

c. include diagnostic input to the PLC (if a status indicating switch or diagnostic indication is provided with the blocking valve).

d. be mounted according to the manufacturer's recommendations.

3.15.7 Hydraulic circuits requiring blocking valve flows greater than 20 GPM shall use a cartridge valve(s).

3.15.8 System filtration shall be provided to limit the in-service particulate contamination level to values appropriate for the safety circuit components. The contamination level shall be expressed in accordance with ISO-4406. Reference ISO-4406 Table VI, and Table VII partially re-printed herein (based on manufacturer's recommendations).

System Pressure: / **Valves:**	**< 14 MPa < 2000 PSI *< 140 bar***	**14 - 21 MPa 2000-3000 PSI *140 - 210 bar***	**> 21 MPa > 3000 PSI *> 207 bar***
Directional (solenoid)	20/18/15	19/17/14	18/16/13
Check	20/18/15	20/18/15	19/17/14
Cartridge	19/17/14	18/16/13	17/15/12
Screw-in	19/17/14	18/16/13	17/15/12
Proportional directional (throttle)	17/15/12	17/15/12	16/14/11*
Proportional cartridge	17/15/12	17/15/12	16/14/11*
Proportional screw-in	17/15/12	17/15/12	16/14/11*
Servo	16/14/11*	16/14/11*	15/13/10*
*Requires precise sampling practices to verify cleanliness levels.			

Figure 3.15.8 - Hydraulic Filtration - ISO-4406 Table VII.1 (partial)

3.15.9 Piston rods shall be equipped with rod wipers and scrapers wherever possible to minimize contamination ingression.

3.15.10 A check valve(s) shall be installed in the hydraulic tank line(s) to prevent fluid from draining to the tank creating an uncontrolled (motion) hazard. *Note: The check valve should not have more than 35 kPa (5 PSI) cracking pressure.*

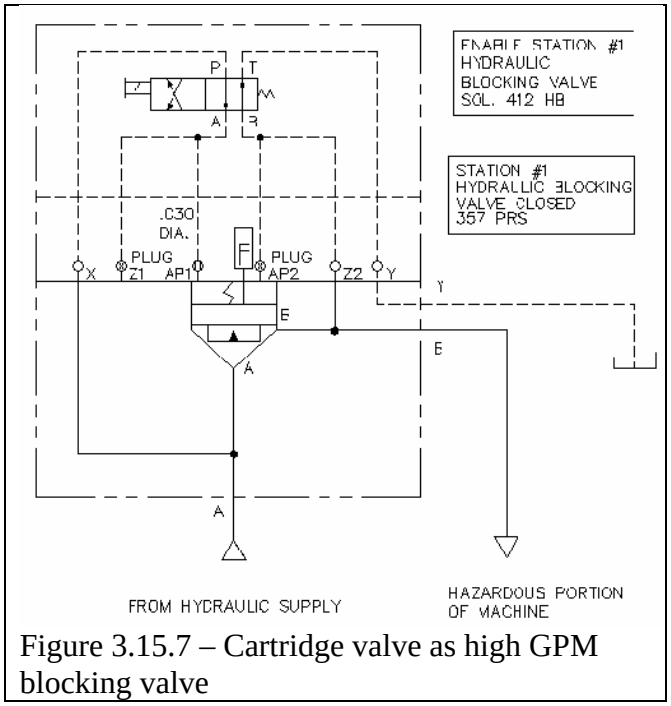


Figure 3.15.7 – Cartridge valve as high GPM blocking valve

3.15.11 Motion valves (or directional valves) shall be mounted so that the main spool and pilot spools are in the horizontal position to prevent the effects of gravity from influencing the valves operation and causing motion.

3.15.12 Motion valves shall be selected based on the motion desired upon the loss of the electrical command signal.

a. Single solenoid valves are allowed for control of actuators with strokes less than 3 inches, when the desired action is a return to the home position. *An example is a conveyor stop that engages the pallet upon loss of the electrical command.*

b. Single solenoid valves are allowed for control of actuators with strokes longer than 3 inches when there is no hazard in the electrically de-energized position.

c. The use of double solenoid detented valves is discouraged. Double solenoid detented valves are allowed for control of actuators with strokes less than 3 inches when the desired action is to maintain the last commanded position such as some clamp applications. Hazards shall be eliminated such that personnel cannot enter the hazardous motion before it stops.

Note: Mechanical means of eliminating the pinch point can include - tooling design such that pinch points are inaccessible (within the tooling), or tooling design such that the part covers any pinch points, or the addition of a fixed guard located at the pinch point. A method of removing the stored energy can include the addition of a blocking valve.

d. Double solenoid three-position valves with exhaust (float) center spool configuration shall be used for control of actuators with strokes exceeding 3 inches and for stopping the actuator motion in mid-position by removal of energy.

e. Double solenoid, three-position valves with exhaust (float) center spool configuration are allowed for all other applications.

f. Blocked center valves shall not be used. *Note: Blocked center valves can cause motion due to the internal leakage from P to both A and B within the valve.*

This page intentional left blank

3.16 Control of suspended vertical loads (due to gravity)

On electrical applications, brakes may be required to stop or hold suspended vertical loads if mechanical devices such as shot pins or counter-balance weights have not been provided. Note: Suspended vertical loads shall be controlled by a mechanical device when the application is outside the design constraints of the brake.

On fluid power applications, control devices such as PO check valves, rod-locks (rod brakes), and counter-balance valves, may be required to stop or hold suspended vertical loads if mechanical devices such as shot pins or counter-balance weights have not been provided.

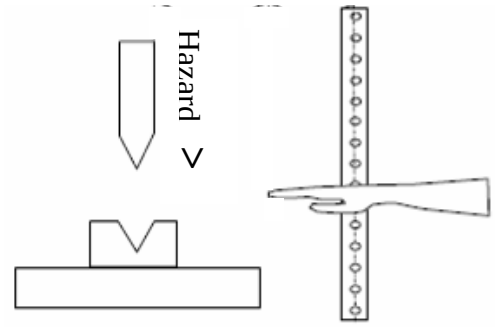


Figure 3.16 – Suspended vertical load

3.16.1 Fluid power circuits for suspended vertical loads shall include PO check valves.

a. Pneumatic and hydraulic PO checks shall be installed as close as practicable to the actuator's port that supports the suspended vertical load.

b. Pneumatic PO checks require a meter-out flow control to be installed between the PO check and the actuator.

c. Pneumatic PO checks shall be installed between the meter-in flow control and the actuator.

d. Pneumatic PO checks that do not automatically vent their downstream pressure on a loss of the incoming supply require additional provisions to manually exhaust stored energy. Warning tag(s) shall be documented on the drawings and be placed next to each PO check on the machine. PO check locations should be documented on the lockout placard.

e. Hydraulic PO checks shall not be used on single rod cylinders where intensification could exceed the rating of components. *Note: Failure of the check to open on single rod applications, or the sudden stopping of fast moving loads, can cause intensified pressures that exceed the working pressure ratings of the cylinder or PO check. An exception may be made where a safety relief is installed between the cylinder and the PO check. A better solution to this is a counter-balance valve which has an integrated relief valve.*

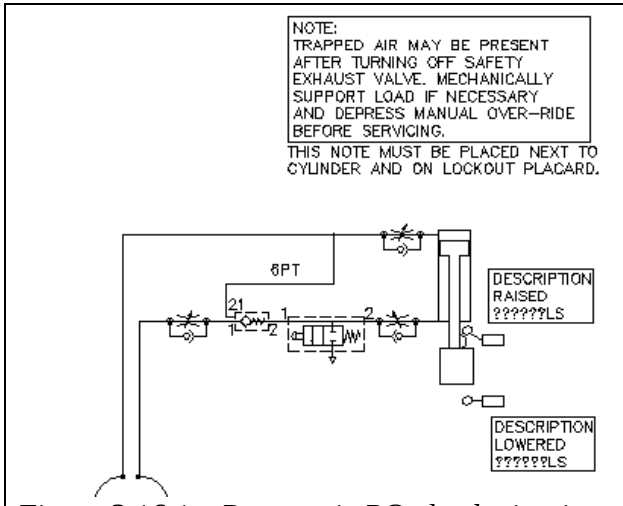


Figure 3.16.1 – Pneumatic PO check circuit

3.16.2 Fluid power circuits for suspended vertical loads greater than 35 pounds shall include an additional control device such as a rod lock or a hydraulic counter-balance valve. Alternatively, suspended vetical loads can be controlled by a mechanical device such as a shot-pin or counter-balance weight. *Note: Suspended vertical loads shall be controlled by a mechanical device when the application is outside the design constraints of the control device.*

3.16.3 Rod-locks shall:

a. be rated for dynamic stopping.

b. be applied per manufacturer's recommendations.

c. include a PO check valve in the actuator circuit for pneumatic applications, meeting the requirements of Section 3.16.1. *Note: This PO check provides control of the load during the transition period between the release of the rod-lock and energization of the motion control valve.*

3.16.4 Hydraulic counter-balance valves shall include:

a. an internal relief function set 300 PSI above that required to suspend the load.

b. a manual means of relieving the trapped pressure. *Note: Some counterbalance valves are provided with a manual override.*

3.16.5 Gon tippers are special vertical load applications that require velocity fuses. The gon tipper circuit shall include:

a. veleocity fuses installed as close as practicable the actuator's port that supports the suspended vertical load.

b. rigid conductors between the velocity fuse and the actuator port.

Note: These velocity fuses are one method of reducing the whipping hazard caused by a ruptured hose.

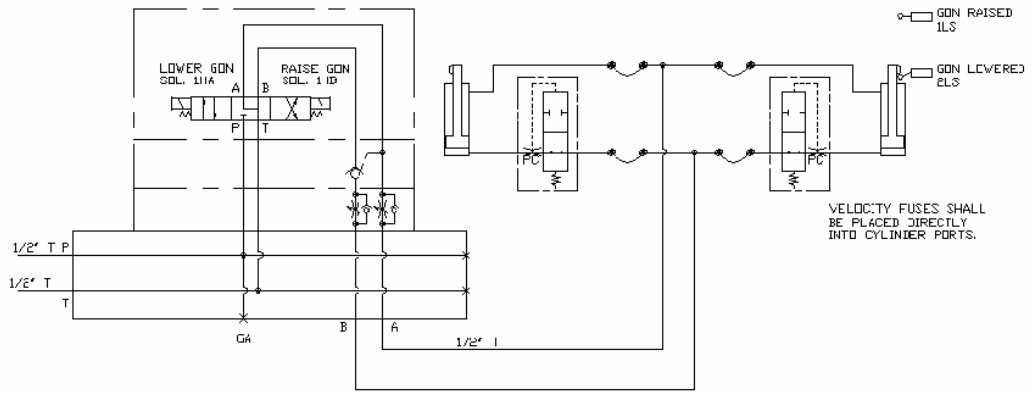


Figure 3.16.5 – Gon tipper velocity fuse circuit

A Annex A Glossary

A.1 **ANSI:** An acronym used as part of a standards publication number; in this case a document by the American National Standards Institute.

A.2 **anti-tie-down:** A term used typically in the requirements of two-hand control requiring the release of both control devices before machine operation can be initiated. The term is also used in the reset requirements on safety relays requiring the transition of the reset input before the relay will reset.

A.3 **blocking valve:** A valve that enables fluid power (such as pneumatic or hydraulic) to the motion valves for hazardous devices. In the electrically de-energized state this valve will exhaust, block, and/or dump fluid power based on the application and fluid power type. For ease and consistency the term *blocking valve* has been used throughout this document. This term is not to be confused with the term *safety valve* when used within this document, although a safety valve is a specific type of blocking valve.

A.4 **bypass (also bypass, bypassing):** To render ineffective any safety related function of the control system or safeguarding device. (ANSI B11.19:2003)

A.5 **category (or categories):** Classification of the safety-related parts of a control system in respect of their resistance to faults and their subsequent behavior in the fault condition, and which is achieved by the structural arrangement of the parts, fault detection and/or by their reliability. (ISO 13849-1:2006)

A.6 **control lockout solution:** The term refers to a Hazardous Energy Control system used on rare and specific equipment/processes to provide a reliable safety system for personnel to enter a work cell when it is not practical to lockout the complete equipment. Refer to SD-012, Nexteer Automotive *Design-In Health and Safety Specification*, for complete requirements.

A.7 **EN:** An acronym used as part of a standards publication number; in this case a European Normative standard.

A.8 **ESPE:** An acronym used in place of Electro-Sensitive Protective Equipment. An assembly of devices and/or components working together for protective tripping or presence-sensing purposes and comprising (as a minimum) a sensing device, controlling/monitoring devices and output signal switching devices. (IEC 61496-1:1997)

A.9 **enabling device:** A manually operated device which, when continuously activated, permits motion. See live man switch. (ANSI B11.19:2003)

A.10 **exposure:** One of three input factors to the risk assessment process, documenting frequency and/or exposure to a hazard for each task-hazard combination as either frequent or infrequent.

A.11 **external device monitoring:** A means by which an ESPE monitors the state of control devices which are external to the ESPE. See feedback. (IEC 61496-1:1997)

A.12 **feedback:** The 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. Alternative terms include *monitor* (*monitor:* ISO 13849-1:2006). For ease and consistency the term *feedback* has been used throughout this document.

A.13 **feedback contact:** The control signal from a final switching device indicating the performance of it switching function. Typical signals include mechanically-linked contacts, spool position sensors, or fluid power pressure sensors.

A.14 **feedback terminals:** The input terminals on safety relays, or external device monitoring terminals on ESPEs, for connection of the final switching device feedback contacts to accomplish the feedback function.

A.15 **final switching device:** The electro-mechanical control component of the machine's safety related control system that interrupts the circuit to the primary control element; that is to say removes power to the hazard. (IEC 61496-1:1997 adapted)

A.16 **IEC:** An acronym used as part of a standards publication number; in this case an International Electrotechnical Commission standard.

A.17 **ISO:** An acronym used as part of a standards publication number; in this case an International Organization of Standards document.

A.18 **interlocked guard door:** A barrier, or section of a barrier, interlocked with the control system to prevent inadvertent access to the hazard during normal machine operation. Alternative terms include hinged guards, fencing, gates, hand-operated and auto-operated access doors, mechanical point-of-operation guarding, perimeter guarding, and interlocked mechanical components.

A.19 **live-man switch:** An enabling device that requires the operator to hold the switch in the mid-position. Applying full pressure will remove the enable device signal(s) to the safety circuit. Release of the switch will also remove the enable device signal(s) to the safety circuit.

A.20 **mechanically-linked contacts:** Contacts on a control device such as a relay, that are constructed in such a way that normally closed contact element(s) and normally open contact element(s) cannot simultaneously be in the closed position. Alternative terms include force guided, positively driven, direct link, mechanically guided, and positive guided. (*force guided:* ANSI TR6:draft)

A.21 **monitoring:** See feedback.

A.22 **muting:** The temporary automatic suspension of a safety function(s) by the safety circuit. (ISO 13849-1:2006)

A.23 **NFPA:** An acronym used as part of a standards publication number; in this case a National Fire Protection Association standard.

A.24 **perimeter guard:** A device used to stop and/or prevent the starting of a machine when a person enters an area where a hazard exists. A perimeter guard encloses the perimeter of the machine or system. The guard is not typically interrupted each cycle of the machine. Typical perimeter guards are interlocked guard doors, although presence-sensing devices such as light curtains and safety mats can be implemented as perimeter guards.

A.25 **point-of-operation guard:** A guarding method used to protect a person who performs an interactive task such as loading, unloading, or inspecting in an area of a machine where a hazard exists, often a limited area of the machine. The operator normally trips the point-of-operation guard during each cycle of the machine. Typical point-of-operation guards include a presence-sensing devices such as a light curtain, or two-hand control devices, although interlocked guard doors or safety mats can be implemented as point-of-operation guards.

A.26 **positive opening contacts:** Use of rigid mechanical linkage between the limit switch actuator and contact element.

A.27 **readily accessible:** Capable of being reached quickly for operation, renewal, or inspections, without requiring those to whom ready access is requisite to climb over or remove obstacles or to resort to portable ladders, and so forth. (NFPA 79:2007)

A.28 **redundancy in the SRP/SC**: As applied to safety circuits, progressively improved safety performance is achieved through component selection and the structure of the safety related parts of the control system. The term *redundancy in the SRP/SC* is used to indicate such items as dual inputs to a safety relay, dual outputs from a safety relay, and dual output devices. All requirements for redundancy are detailed within the specification.

A.29 **risk assessment:** An overall process comprising risk analysis (combination of the specification of the limits of the machine, hazard identification, and risk estimation) and risk evaluation (judgment, on the basis of risk analysis, of whether risk reduction objectives have been achieved). (ISO 13849-1:2006, adapted) The Nexteer Automotive risk assessment process is detailed in Nexteer's *Design-In Health and Safety Specification*.

A.30 **SRP/CS:** An acronym used in place of Safety Related Part of the Control System. Part of a control system that responds to safety-related input signals and generates safety-related output signals. (ISO 13849-1:2006) For ease and consistency the term *safety circuit* has been used throughout this document.

A.31 **safety circuit:** See SRP/CS.

A.32 **safety valve:** A safety-rated device incorporating redundant internally monitored cross flow functional elements in a single body. The valve will typically inhibit further operation should an internal fault occur and will maintain the faulted condition until a reset action takes place. A status switch provides optional feedback and is not required for the valve's safety function. This term is not to be confused with the term *safety lockout and exhaust valve* which is used for machine lockout functions.

A.33 **safety gate:** See interlocked guard door.

A.34 **safety interlock switch:** A device used to connect a guard with the control system.

A.35 **safety mat:** *Note: Current Nexteer Automotive productions systems do not include the use of safety mats. Use of safety mats requires Nexteer control engineering approval.*

A.36 **safety-rated:** Specifically designed and category-rated for use in safety circuits adhering to applicable standards for machine safety.

A.37 **safety relay:** A category-rated relay or control module designed for use in a safety circuit. Control modules can include a configurable or programmable relay, a safety integrate module (SIM), or a safety-rated PLC. For ease and consistency the term *safety relay* has been used throughout this document.

A.38 **short-circuit-detection:** Detection of shorted inputs within the safety relay's dual input channels, typically accomplished by use of one 0vdc and one 24vdc input channel. Also accomplished by use of a safety relay requiring one channel to be energized and one de-energized in the safe-state. Some light curtains provide two 24vdc solid-state output signals with short-circuit detection designed into the light curtain control unit.

A.39 **single channel**: As applied to safety circuits, progressively improved safety performance is achieved through component selection and the structure of the safety related parts of the control system. The term *single channel* is used to indicate that only single devices in any part of the control system is required.

A.40 **suspended vertical loads**: Machine components that, due to gravity, could cause a pinch point or hazard should the tooling drop from the *raised* position to a *lowered* position. Weight reference for suspended vertical loads includes tooling, fixtures, fluid power cylinder rods, and other machine mechanics. Note that any weight reference within this specification includes only the vertical (or downward) component of the load. A motion that is a combination of both horizontal and vertical includes only some of the load weight measured in the vertical or downward direction (minus any frictional losses); the remainder of the load weight would act in the horizontal direction.

A.41 **two-hand control relay:** A safety relay specifically manufactured for two-hand control applications. This relay requires simultaneous actuation of the two inputs within a fixed time of each other, typically 500 milliseconds.

A.42 **Type 2 ESPE:** An ESPE specifically designed and rated for use in safety circuits adhering to applicable standards for machine safety, including at least one output switching device that goes to the *Off*-state when the sensing device is actuated, or when power is removed from the device. Particular requirements for a Type 2 ESPE can be found in IEC 61496-1.

A.43 **Type 4 ESPE:** An ESPE specifically designed and rated for use in safety circuits adhering to applicable standards for machine safety, including at least two output switching devices that go to the *Off*-state when the sensing device is actuated, or when power is removed from the device. Particular requirements for a Type 4 ESPE can be found in IEC 61496-1.

B Annex B Safety distance formulas

B.1 General formula

The following general safety distance formula should be used to calculate the minimum safe distance to mount the safety device from the hazardous motions. Note that an adaptation of this formula for light curtains is listed separately. This is the formula suggested in ANSI B11.19 and EN 999.

$$D_S = K \times T$$

D_S = Minimum safety distance between the device and the nearest point of operation hazard (in inches).

K = Hand speed constant of 63 inches per second

T = The total time to stop hazardous motion which include various factors (in seconds).

The total time that it takes for hazardous motion to stop includes portions that vary by machine type and by the safeguarding device applied. The following affect the total stopping time:

Stop time of the equipment including stopping capability of motors, drives, and the reaction time of valves (referred to as T_S).

Response time of the machine control system (referred to as T_C).

Response time of the safeguarding device including its interface (referred to as T_r).

Note: $T_S + T_C + T_r$ can be measured by a stop-time measurement device such as the Gemco Series 1999 Semelex II Safetimeter test set .

B.3 Light curtains

The following safety distance formula shall be used to calculate the minimum safe distance to mount the light curtain from the hazardous motions. This is the formula suggested in ANSI B11.19 and EN 999.

$$D_S = K \times (T_S + T_C + T_r) + D_{pf}$$

D_{pf} = Added distance due to the penetration factor as shown on Chart 1 below. The distance a person's finger or hand must penetrate the light curtain sensing plane before detected by the light curtain. Light curtains with a narrower beam spacing will have a smaller D_{pf}, they will detect a person's finger.

The minimum object sensitivity, or the penetration factor D_{pf}, is stated by the light curtain manufacturer.

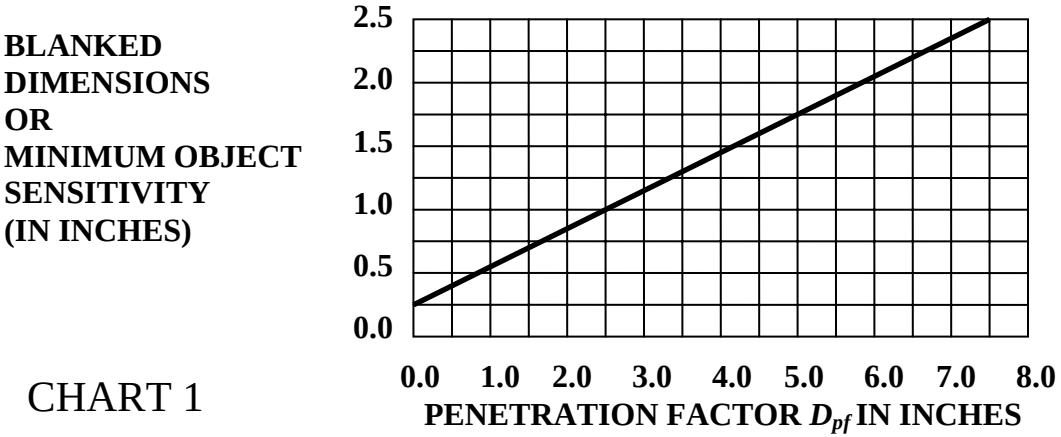
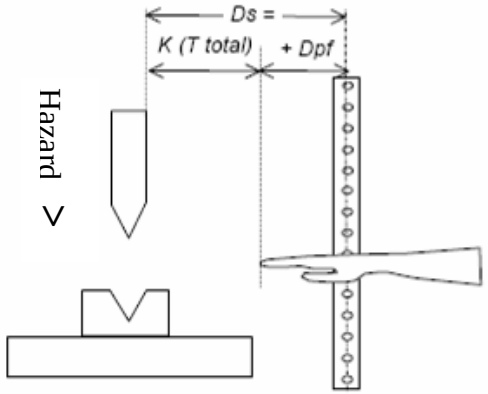
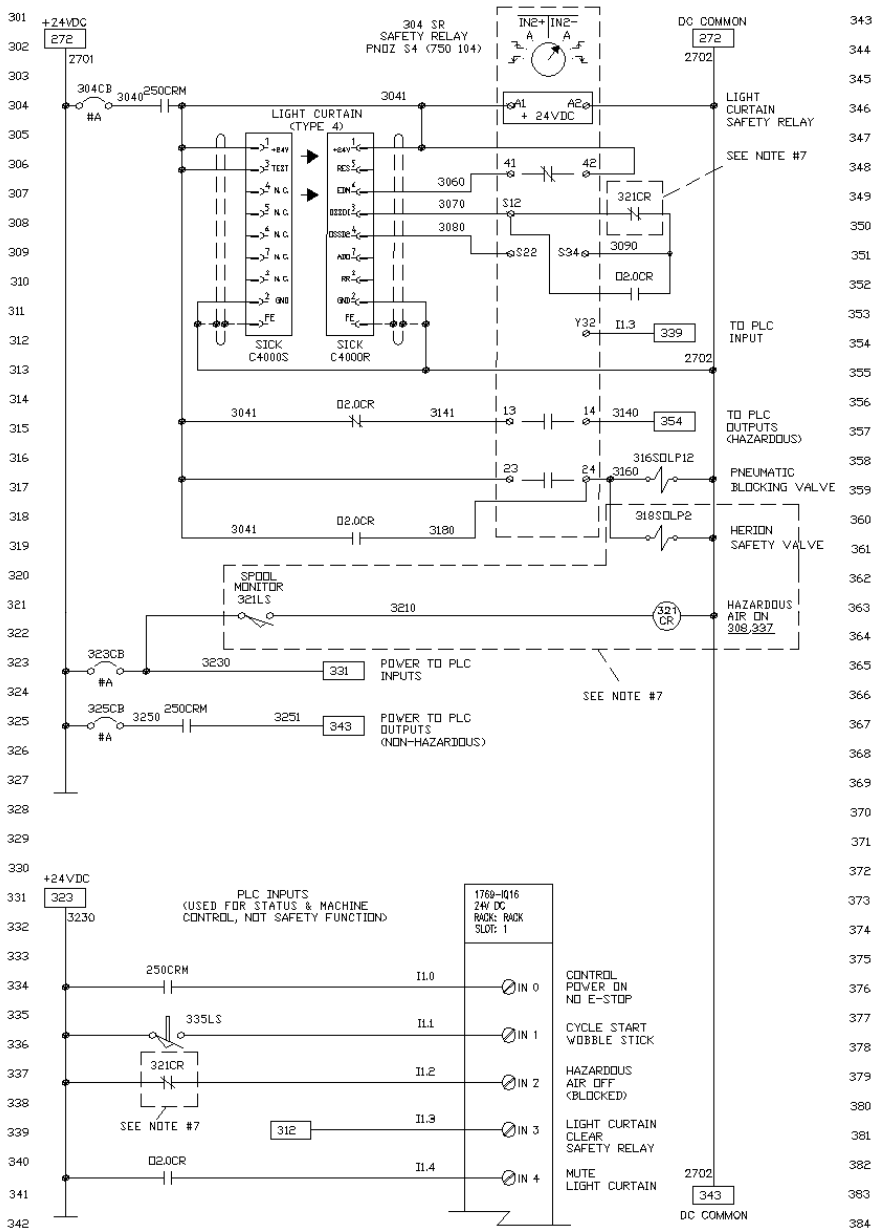
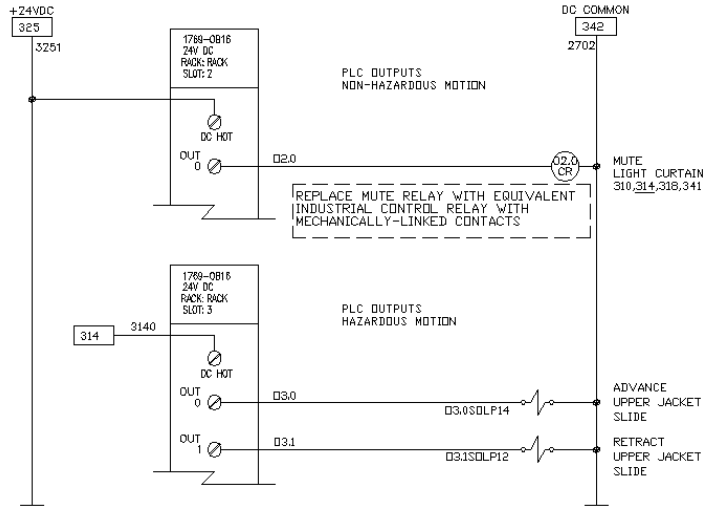


CHART 1



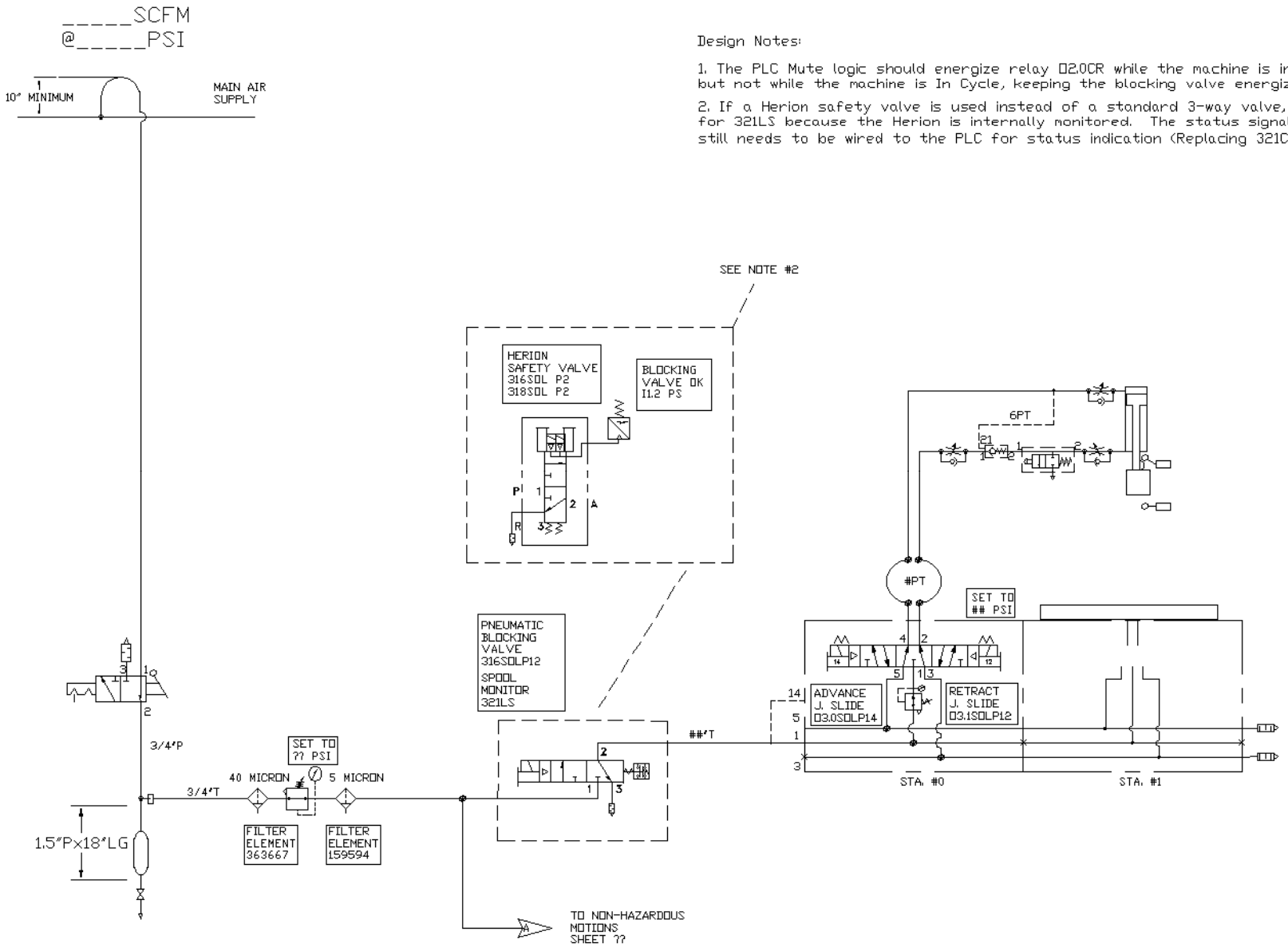
C Annex C Category 3 Light Curtain and Pneumatic Motions Muting Circuits





Design Notes:

1. The relay replacement note from line 349 shall be included on the final design prints.
2. The O2.0CR normally-closed contact on line 314 removes hazardous power upon relay or logic failure, failure to the ON-state.
3. The PLC logic shall include fault indication if the state of input I1.4 contradicts with the state of output O2.0.
4. The normally-open O2.0CR contact on line 341 is for machine diagnostics, does not have safety implications, and therefore can be either a normally-open or a normally-closed contact depending on availability.
5. The PLC Mute logic should energize relay O2.0CR while the machine is in Automatic mode but not while the machine is In Cycle.
6. If the light curtain is interrupted while In Cycle, the PLC Mute logic must NOT reenergize under this fault condition. Relay O2.0CR must stay de-energized to force the feedback 321CR to transition for light curtain reset.
7. If a Herion safety valve is used instead of a standard 3-way valve, there is no need for 321CR because the Herion is internally monitored. The status signal from the Herion still needs to be wired to the PLC for status indication (Replacing 321CR on Input I1.2).



Design Notes:

1. The PLC Mute logic should energize relay O2.0CR while the machine is in Automatic mode but not while the machine is In Cycle, keeping the blocking valve energized between cycles.

2. If a Herion safety valve is used instead of a standard 3-way valve, there is no need for 321LS because the Herion is internally monitored. The status signal from the Herion still needs to be wired to the PLC for status indication (Replacing 321CR with Input I1.2 PS).

D Annex D References

ANSI B11.19: Performance Criteria for Safeguarding: 2003

ANSI B11.TR6:200x: Technical Report for Machine Tools – Safety Control Systems for machine Tools: *draft*

EN 954-1: Safety of machinery – Safety-related parts of control systems – Part 1: General principles for design: 1996

EN 999: Safety of machinery – The positioning of protective equipment in respect of approach speeds of parts of the human body: 2008

EN 1088: Safety of machinery – Interlocking devices associated with guards – Principles for design and selection: 2008

IEC 60947-5-1: Low-voltage switchgear and controlgear – Part 5-1: Control circuit devices and switching elements – Electromechanical control circuit devices: Edition 2.2, 2000-03

IEC 60947-5-3: Low-voltage switchgear and controlgear – Part 5-3: Control circuit devices and switching elements – Requirements for proximity devices and defined behavior under fault conditions: 1999-03

IEC 60947-5-5: Low-voltage switchgear and controlgear – Part 5-5: Control circuit devices and switching elements – Electrical emergency stop device with mechanical latching function: Edition 1.1, 2005-04

IEC 61496-1: Safety of machinery – Electro-sensitive protective equipment – Part 1: General requirements and tests: 1997-08

IEC 61496-2: Safety of machinery – Electro-sensitive protective equipment – Part 2: Particular requirements for equipment using active opto-electronic protective devices: 1997-11

ISO 4406: Hydraulic fluid power – Fluids – Method for coding the level of contamination by solid particles: 1999

ISO 8573-1: Compressed air – Part 1: Contaminants and purity classes: 2001

ISO 13849-1: Safety of machinery – Safety-related parts of control systems – Part 1: General principles for design: Second edition 2006-11-01

NFPA 79: Electrical Standard for Industrial Machinery: 2007

SD-007 Nexteer Automotive Approved Components List, O6NO09

SD-012: Nexteer Automotive Design-In Health and Safety Specification, 06NO09

NOTE: To obtain a copy of Nexteer Automotive specifications visit our vendor document web-site nexteersuppliers.com. To obtain a copy of any other referenced specification they can be purchased, typically from the originating organization or at other industry specification web-sites.

3.17 RECORD OF REVISIONS

Revision #	Date	Section	Description
001	06NO09	All	Original Approval & Issue Date
002			
003			
004			
005			
006			
007			
008			
009			
010			
011			
012			
013			
014			
015			
016			
017			
018			
019			
020			
021			
022			
023			
024			
025			
026			
027			
028			
029			
030			