Specification for Safety Circuits

SD-011

ISSUED	November 6, 2009
REVISED	September 27, 2022

© 2022 Nexteer Automotive
All rights reserved.

Table of Contents

1. Scope and Purpose 4
2. Safety Circuits – Performance Levels and Circuit Categories 5
3. Application Requirements 21

Annex

A. SD-010, Standard Equipment Specification 60
B. References 63
C. Glossary 65

Forward

This Specification for Safety Circuits (SD-011) is issued by Nexteer Automotive (Nexteer). The specification was developed as a "how to" document in support of the Nexteer 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 in conjunction with other 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.

The above items shall be accomplished by using a machine risk assessment to identify equipment and process hazards. The "Hierarchy of Health and Safety Controls" found in Nexteer's Design-In Health and Safety Specification shall be followed to eliminate exposure to these hazards. The 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. 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, Nexteer expects and encourages all industrial equipment builders to notify Nexteer 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 requirements. These drawings are not intended to represent Nexteer drafting standards, nor are they intended to show basic machine control design practices such as proper wire sizes, circuit protection, and fluid power component sizing.

The specification was based solely on the equipment, operations, processes, and facilities of Nexteer. While Nexteer believes 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's operations. This specification 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 requirements of the safety circuit is defined as a result of conducting a machine risk assessment for the equipment. The Design-In Health and Safety Specification details the Nexteer machine risk assessment process, including who conducts this assessment. The results of this assessment can include one or more performance levels and circuit structure categories for the safety related part of the control system.

1.1.2 Emergency stop devices and circuits fall into the scope and purpose of this specification.

1.1.3 Fluid power (pneumatic and hydraulic) control circuits are subjected to the same design criteria as the electrical to satisfy the requirements of the machine risk assessment and therefore fall into the scope and purpose of this specification. Merely removing electrical power from the machine motion valves does not ensure that a safe fluid power condition exists for all performance levels. The safeguarding system design must also consider the failure modes of the fluid power components. Therefore, additional safety circuitry might be required to meet the performance level requirements of the machine risk assessment.

1.1.4 This specification is intended to document and illustrate the basic principles of safety circuits and well-tried safety principles. 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, control system rebuilds, and safeguarding modifications made to existing equipment in compliance with SD-012 Section 1.4. It should not be implied that any existing equipment be required to be retrofitted to comply with this specification.

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.

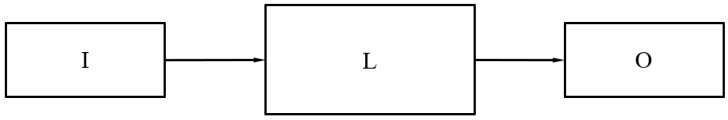
1.2.4 Use of the word “shall” denotes mandatory requirements. Use of the word “should” denotes a recommendation or good practice. Use of the word “may” denotes permission or allowance. Use of the word “can” denotes a possibility or a capability (a statement of fact).

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 application are satisfied.

2. Safety Circuits – Performance Levels and Circuit Categories

ISO 13849-1 details the characteristics for the Safety Related Part of the Control System (SRP/CS) performance level and circuit structure category. For ease and consistency, the following naming conventions are used thought this document.

- The term "**safety circuit"** is used in place of SRP/CS.
- The acronym "**PL"** is used in place of performance level.
- The term "**category"** has been used as a simple replacement for circuit structure category.
- A typical safety circuit consists of the **input** device(s), **logic** device(s), and **output** device(s) as shown in the simplified safety-rated block diagram Figure 2.0
- The term "**safety module**" has been used as a simple replacement for all safety logic devices such as safety relays, configurable safety modules, and Safety PLCs.



Key

I	input devices such as sensors or switches
L	logic device(s)
O	output devices such as relays, contactors, or valves

Figure 2.0 Simplified safety-circuit block diagram

An increased reliability is characterized by an increased PL for the safety circuit or devices, from the lowest PL a to the highest PL e, to achieve the required risk reduction. To support PL, progressively improved safety performance is achieved through component selection and the structure of the safety circuit from Category B, 1, 2, 3, through 4.

Nexteer's interpretations and minimum requirements for safety circuit applications, as derived from ISO 13849-1, are as follows.

2.1 PL a and PL b Requirements

Note: Nexteer does not require an engineered controls solution as the safeguarding solution for machine risk assessments applications that require PL a or PL b. Only Awareness Devices, Warnings, Training, PPE, or similar, are required. Therefore, engineered controls solution as the safeguarding solution will seldom be applicable for applications that require PL a or PL b.

Engineered controls safeguarding solutions identified by the machine risk assessment to require PL a or PL b shall comply to the following as a minimum.

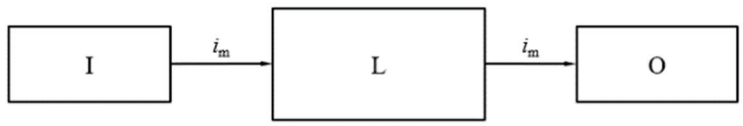
							INITIAL ASSESSMENT		
User	Task	Task-Hazard	MH	S	E	A	Risk Level	Required Performance Level (PL_r)	Solution
Operator	Load / Unload Parts and Initiate Cycle	Advance / Retract motion of Press	PNEUMATIC	S1	E1	A3	LOW-INFORM	PL b	Safeguarding
Operator	Load / Unload Parts and Initiate Cycle	Advance / Retract motion of Fixture Slide	PNEUMATIC	S1	E1	A1	NEGLIGIBLE	PL b	Safeguarding

2.1.1 Single channel circuitry is allowed, with minimum Category B circuit structure. Standard machine control practices and components may be used.

2.1.2 **Input** devices (sensing devices) may include standard devices, such as proximity switches and limit switches.

2.1.3 **Logic** may be programmable, such as within a standard PLC.

2.1.4 **Outputs** may include standard control components such as PLC outputs, motion valves, or serial-communicated commands.



Key

i_m	interconnecting means
I	input
L	logic
O	output

Figure 2.1 PL b safety circuit block diagram

2.2 PL c Requirements

Note: Only two types of Nexteer applications will typically indicate PL c safeguard solutions for engineered controls solutions identified on the machine risk assessment: Emergency Stop, and high exposure to only slight injury hazards.

Engineered controls safeguarding solutions identified by the machine risk assessment to require PL c shall comply to the following as a minimum.

							INITIAL ASSESSMENT		
User	Task	Task-Hazard	MH	S	E	A	Risk Level	Required Performance Level (PL_r)	Solution
Operator	Load / Unload Parts and Initiate Cycle	Advance / Retract motion of Part Clamp	PNEUMATIC	S2	E1	A2	MEDIUM	PL c	Safeguarding
Operator	Load / Unload Parts and Initiate Cycle	Advance / Retract motion of Part Locator	PNEUMATIC	S1	E2	A3	LOW	PL c	Safeguarding

2.2.1 Single channel circuitry as a minimum is required, with minimum Category 2 circuit structure.

2.2.2 **Input** devices shall meet one of the following requirements. At a minimum they shall:

1. Have positive-opening contacts, or
2. Be a Type 4 ESPE rated device, or
3. Be a minimum PL c rated technology, or
4. Be a minimum Category 2 rated technology.

   Exception: Emergency Stop pushbutton device requirements are noted elsewhere in this document.

2.2.3 **Logic** shall be accomplished through safety modules, compliant to published component manufacturer's literature. Safety modules shall be rated and applied at a minimum PL c or Category 2.

2.2.4 **Outputs** shall be hardware-components that meet one of the following requirements. They shall be:

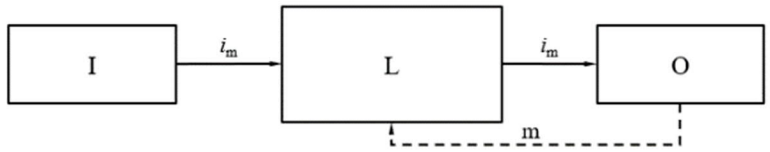
1. Safety-rated contacts from the safety module, or
2. An industrial control relay (or motor starter contactor), or
3. An electronic component such as a servo when rated and applied at a minimum PL c or Category 2, or
4. Fluid power (pneumatic and hydraulic) motion valves.

   Clarification: Removal of electrical power to the fluid power motion valves is accomplished through the removal of power to an output module or circuitry directly controlling the motion valve solenoid(s).

2.2.5 A feedback contact from relays or contactors as the output device(s) shall be wired into the feedback terminals of the safety module.

Clarification: Fluid power motion valves do not require feedback into the safety module.

Clarification: Device literature for electronic components, such as a servo, will indicate whether feedback into the safety module is required for device compliance at PL c or Category 2.

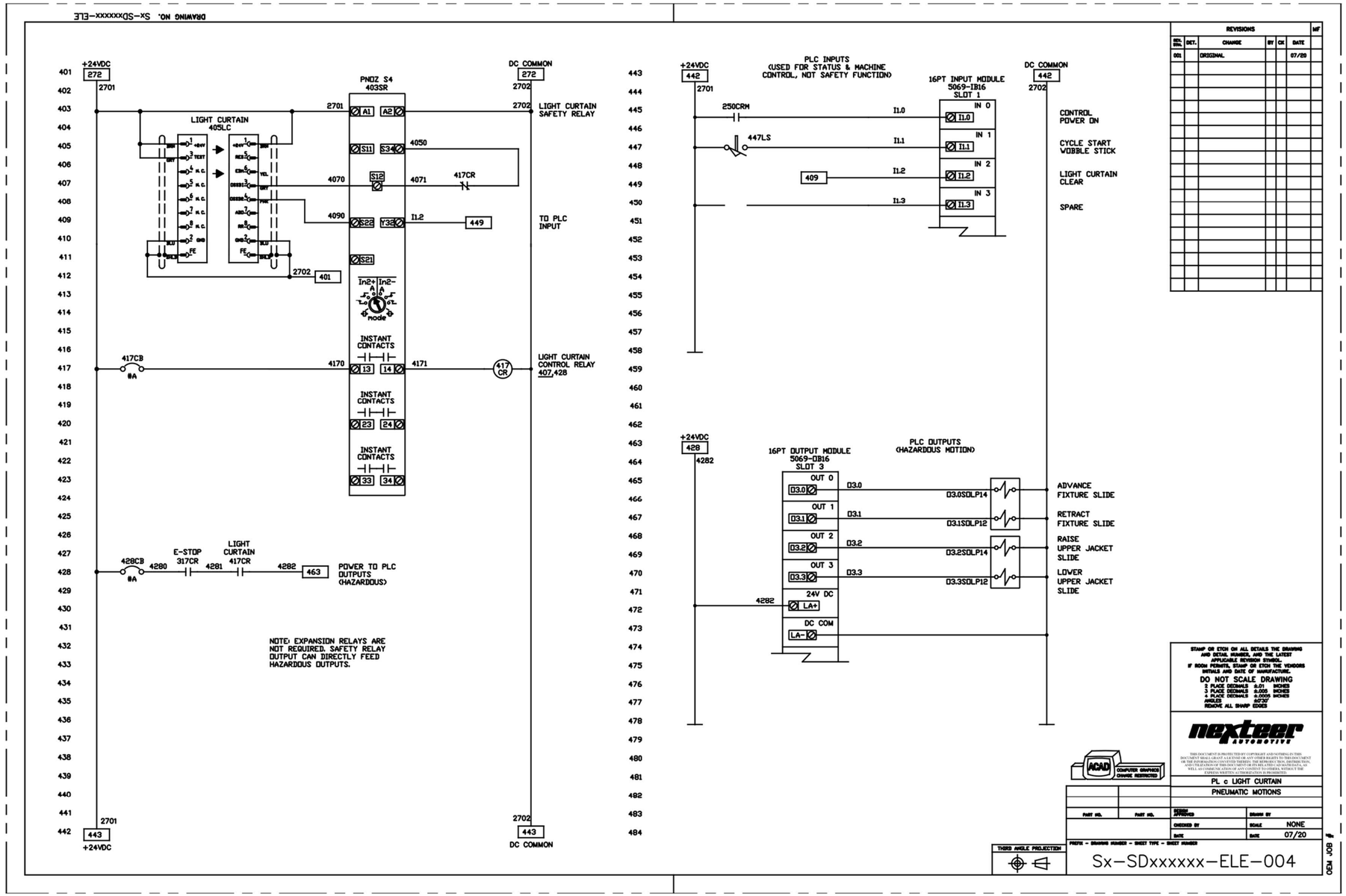


Key

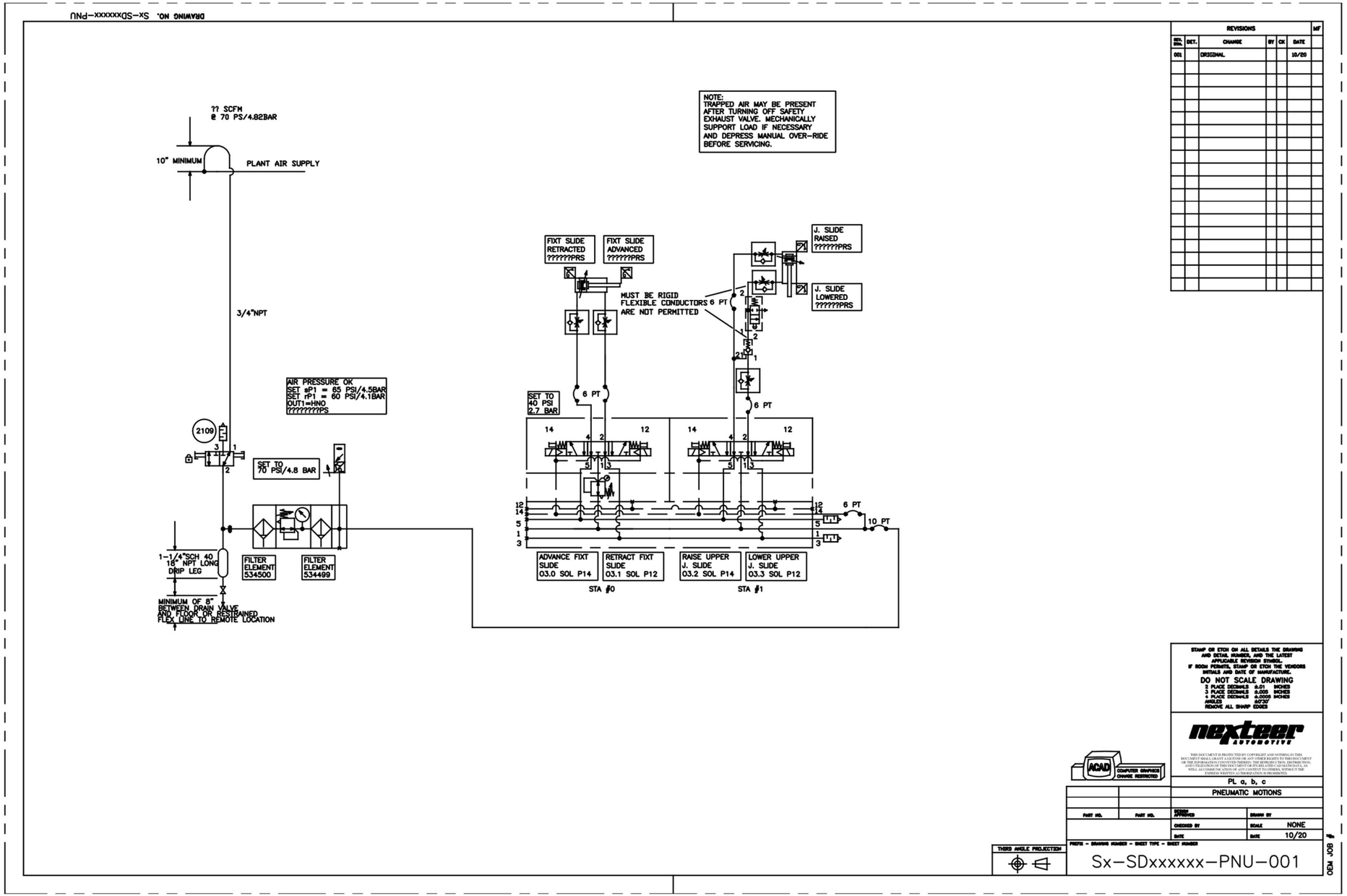
i_m	interconnecting means
I	input
L	logic
m	monitoring / feedback
O	output

Dashed lines represent reasonably practicable fault detection

Figure 2.2 PL c safety circuit block diagram



Example PL c Safety Circuits: Light Curtain w/ Pneumatic Sheet 1 of 2



Example PL c Safety Circuits: Light Curtain w/ Pneumatic Sheet 2 of 2

2.3 PL d Requirements

Note: For Nexteer applications, nearly all engineered controls solutions identified on the machine risk assessment will require PL d safeguard solutions.

When engineered controls safeguarding solutions identified by the machine risk assessment to require PL d, they shall comply to the following as a minimum.

							INITIAL ASSESSMENT		
User	Task	Task-Hazard	MH	S	E	A	Risk Level	Required Performance Level (PL,)	Solution
Operator	Load / Unload Parts and Initiate Cycle	Advance / Retract motion of Fixture Slide	ELECTRIC	S3	E2	A2	HIGH	PL d	Safeguarding
Operator	Load / Unload Parts and Initiate Cycle	Lower / Raise motion of Jacket Slide	PNEUMATIC	S2	E2	A3	HIGH	PL d	Safeguarding

2.3.1 Redundancy in the safety circuit is required, with minimum Category 3 circuit structure.

Clarification: Single channel technology is allowed when device literature indicates a minimum PL d rating at single channel implementation.

2.3.2 **Input** devices shall meet one of the following requirements. At a minimum they shall be:

1. A single device with two positive-opening contacts, or
2. Two devices (per safeguard) with one positive-opening contact each, or
3. A Type 4 ESPE rated device, or
4. A minimum PL d rated technology, or
5. A minimum Category 3 rated technology.

Clarification: More than five input devices connected in series is allowed only if the device's literature clearly indicates compliance to PL d or higher rating when connected in series.

Exception: Two-hand control pushbutton device requirements are noted elsewhere in this document.

2.3.3 **Logic** functions of the safety circuit shall be accomplished through safety modules, compliant to published component manufacturer's literature. Safety modules shall be rated and applied at a minimum PL d.

2.3.4 **Outputs** shall be hardware-components that meet one of the following requirements. They shall be:

1. Safety-rated contacts from the safety module, or
2. Redundant industrial control relays (or motor starter contactors) with mechanically-linked contacts, or
3. An electronic component such as a servo when rated and applied at a minimum PL d, or
4. Fluid power motion valves, plus fluid power blocking valve when required as detailed in Section 3.20 and Section 3.21.

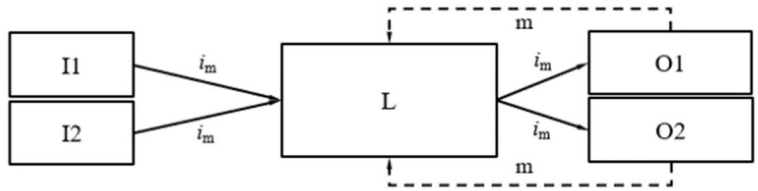
Clarification: Removal of electrical power to the fluid power motion valves is accomplished through the removal of power to an output module or circuitry directly controlling the motion valve and blocking valve solenoid(s).

2.3.5 A feedback contact from each output device shall be wired into the feedback terminals of the safety module.

Clarification: Fluid power motion valves do not require feedback into the safety module; for fluid power blocking valve feedback requirements refer to Section 3.20 and 3.21; for rod lock and rail brake motion valve feedback requirements refer to Section 3.22.

Clarification: The feedback contact from industrial control relays or motor starter contactors applied as output devices are required to be mechanically-linked contacts since mechanically-linked contacts are practicable. The feedback contacts from other devices applied as output devices are not required to be mechanically-linked.

Clarification: Device literature for electronic components, such as a servo, will indicate whether feedback into the safety module is required for device compliance at PL d.



Key

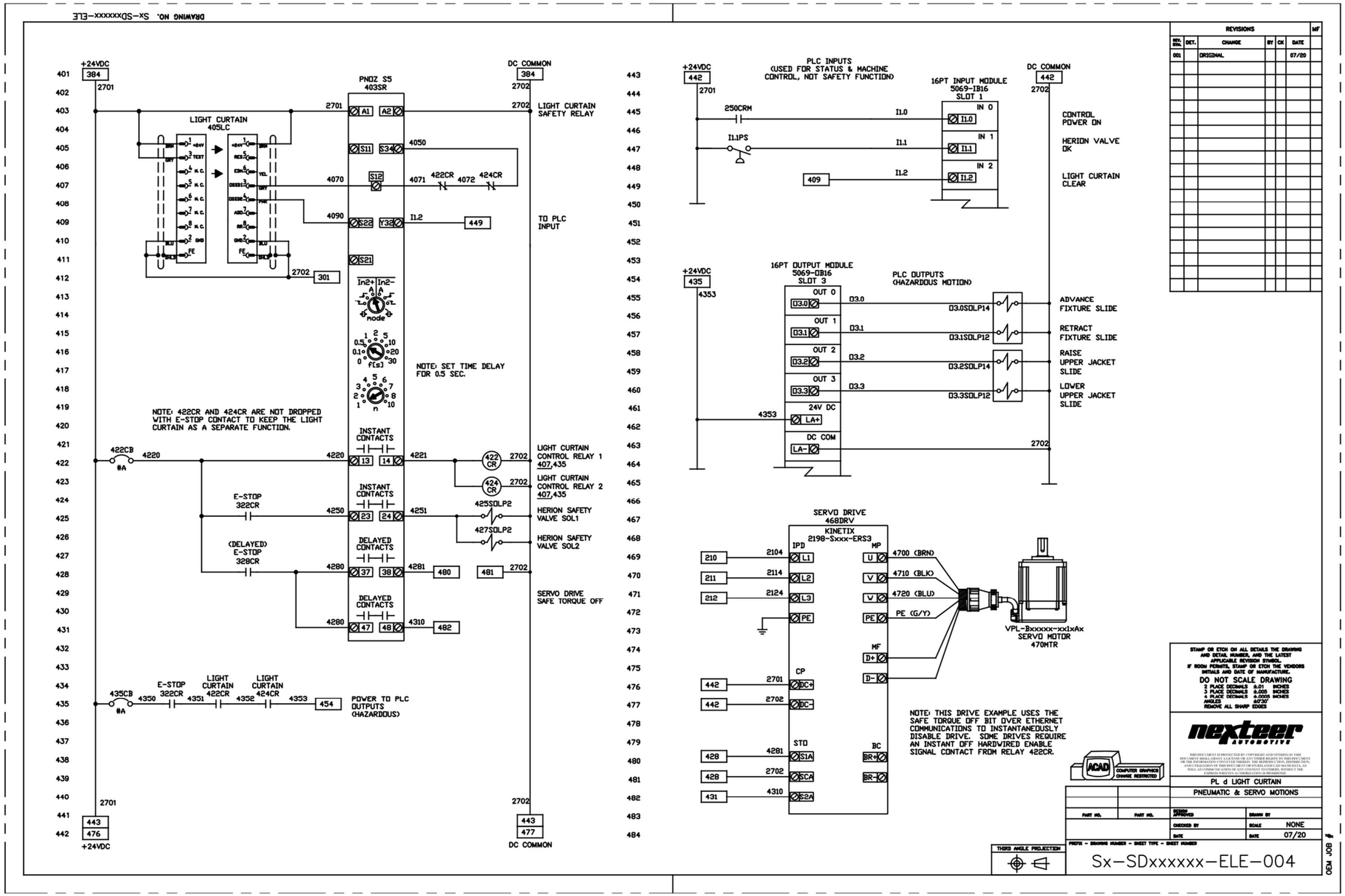
i_m	interconnecting means
I	input
L	logic
m	monitoring / feedback
O	output

Dashed lines represent reasonably practicable fault detection

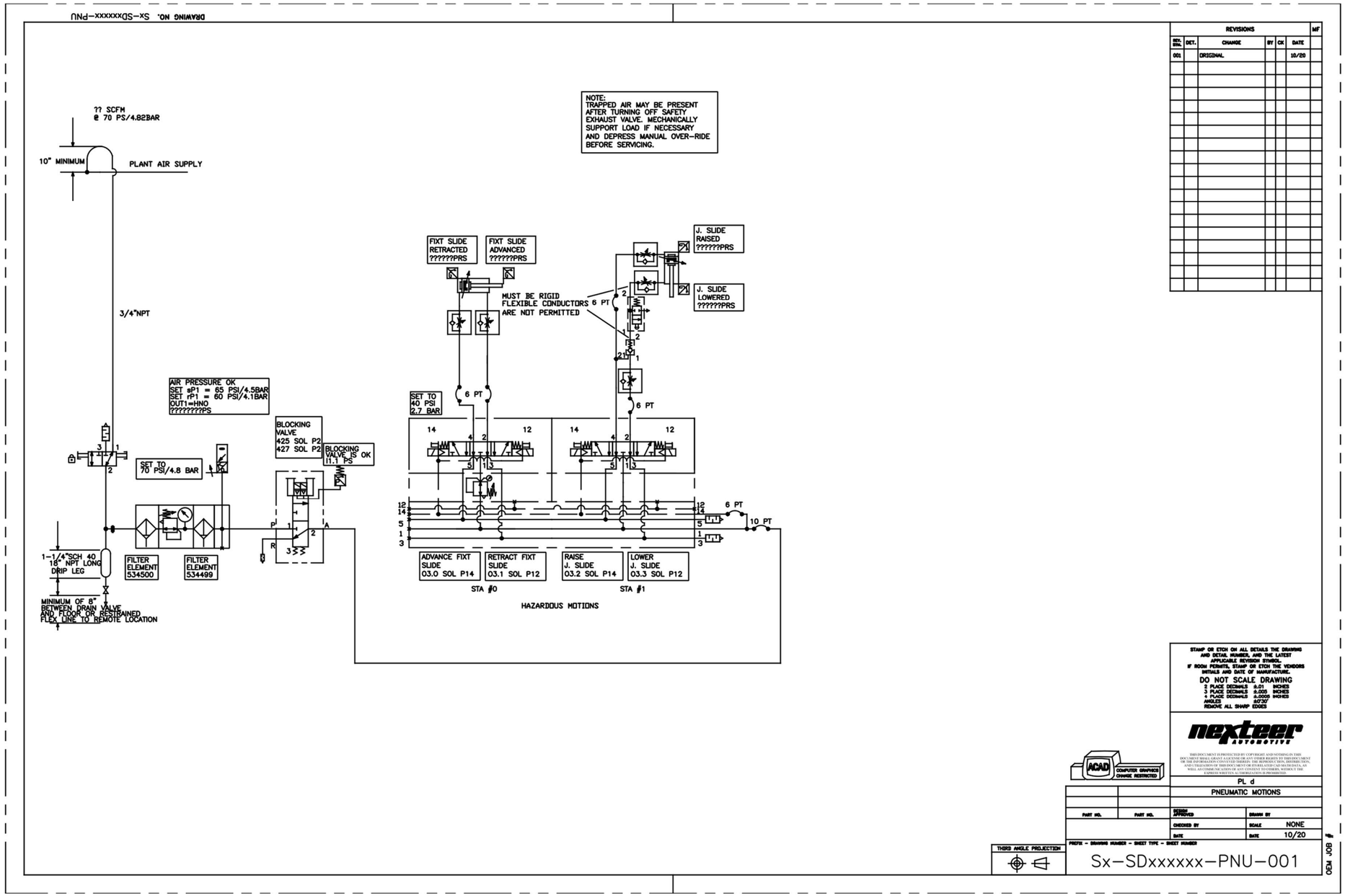
Figure 2.3 PL d safety circuit block diagram

2.3.6 When engineered controls safeguarding solutions identified by the machine risk assessment to require PL d, single channel circuitry is **only** allowed when **all** single channel devices are either rated a minimum of PL d, or all single channel devices are documented to have a $MTTF_D$ = high **and** a DC_{avg} ≥ medium.

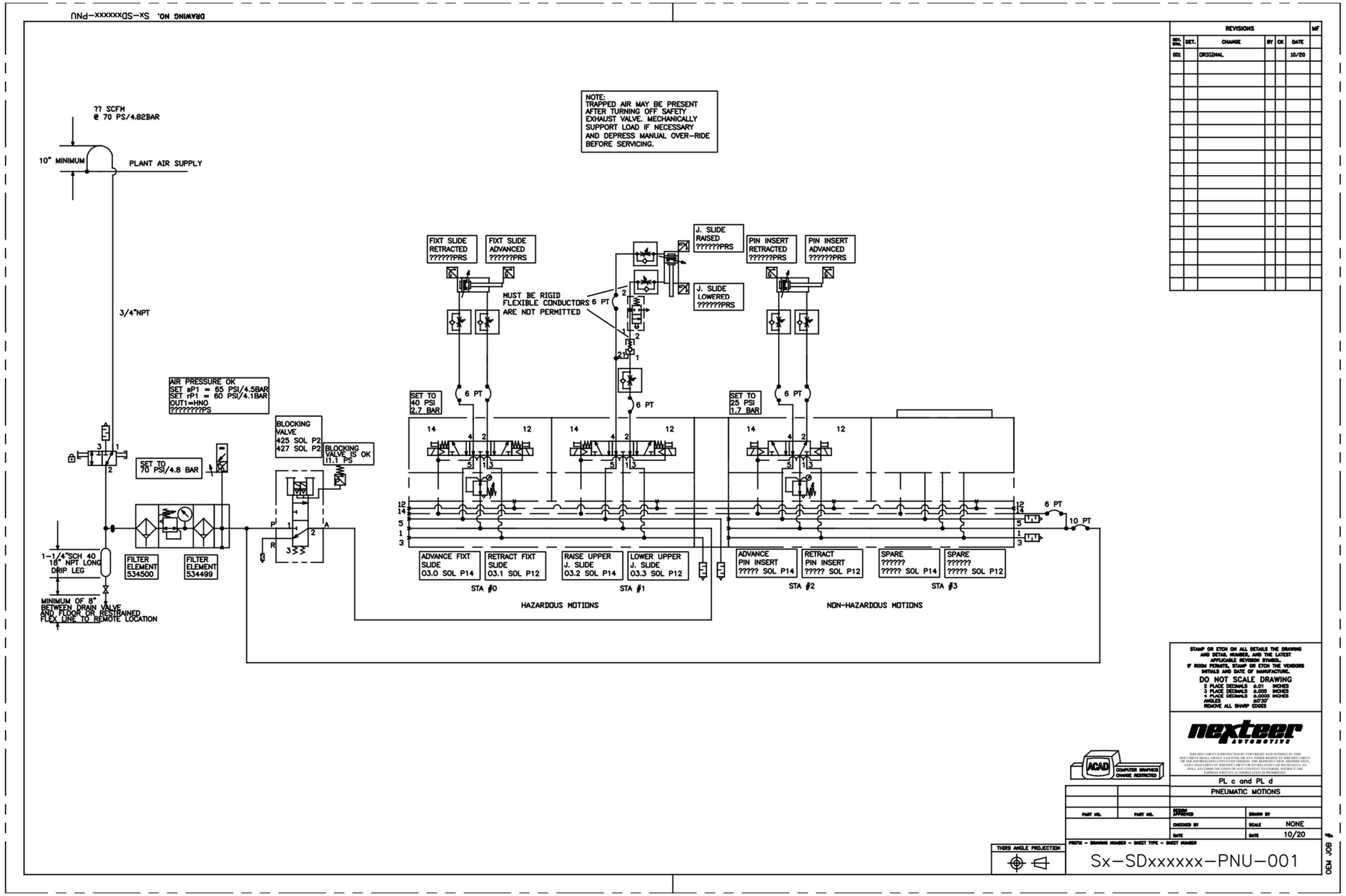
Clarification: Refer to PL d Category 2 - Required Improved Diagnostic Coverage section within Section 3 below.



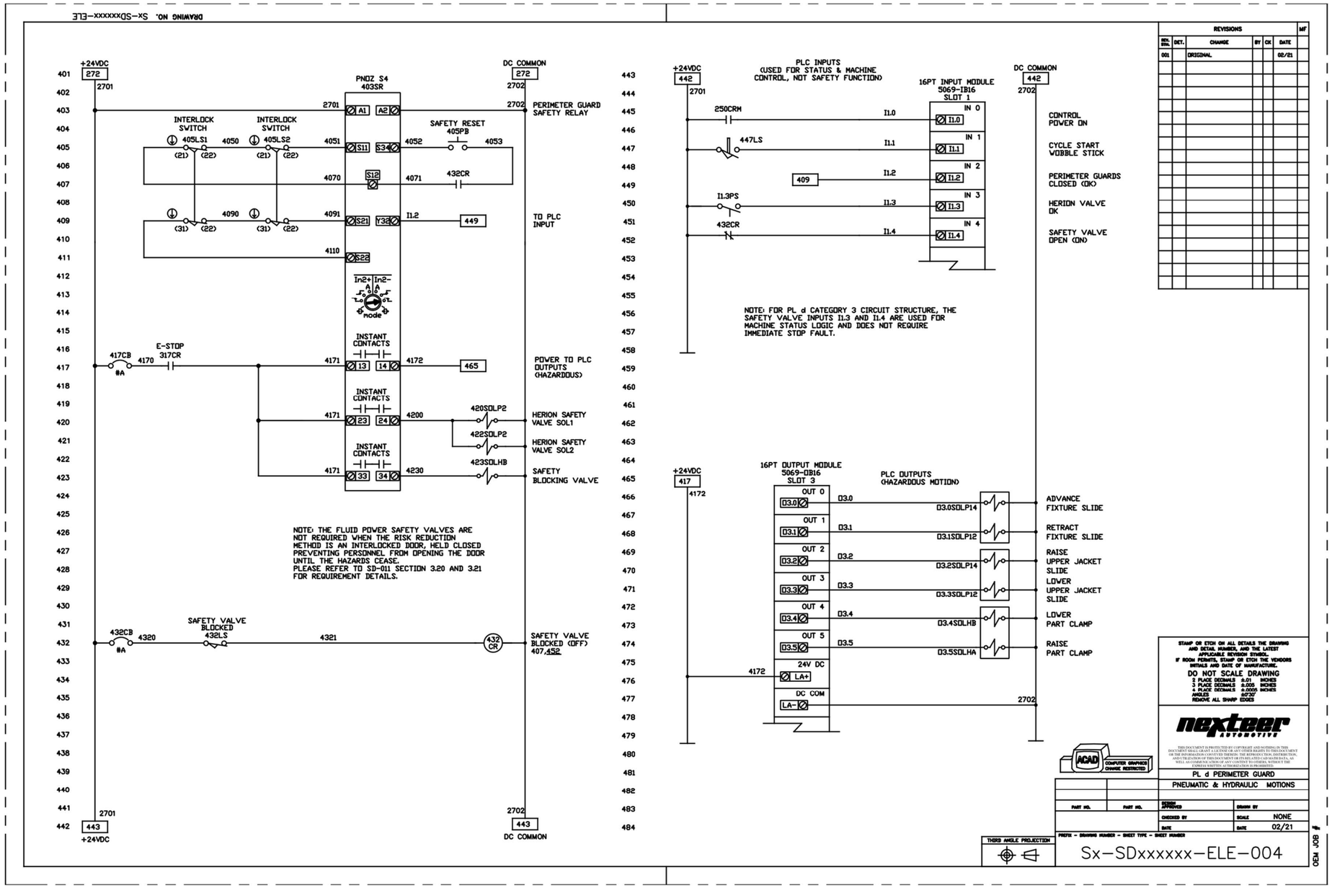
Example PL d Safety Circuits: Light Curtain w/ Pneumatic & Drive Sheet 1 of 3



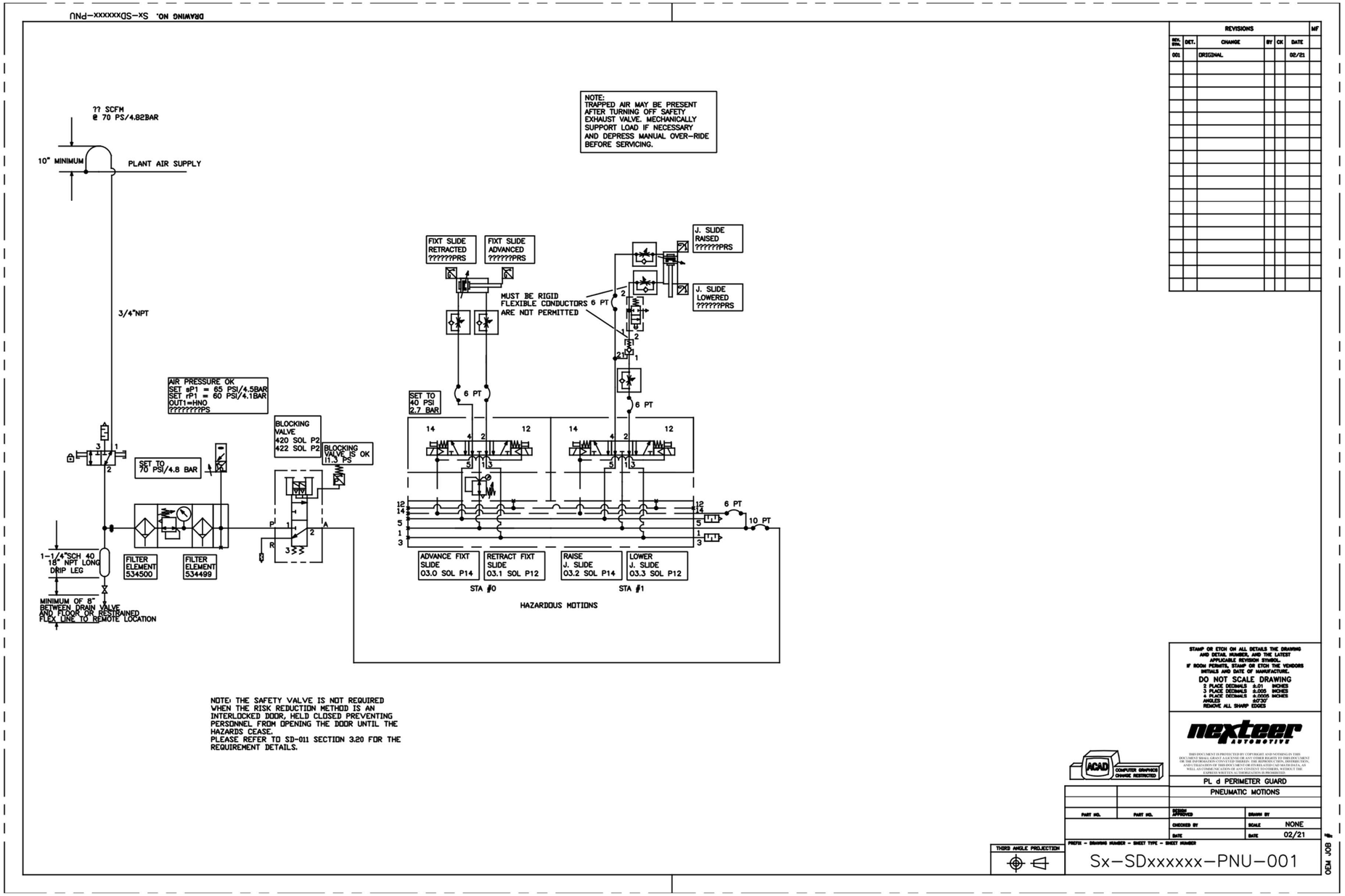
Example PL d Safety Circuits: Light Curtain w/ Pneumatic & Drive Sheet 2 of 3



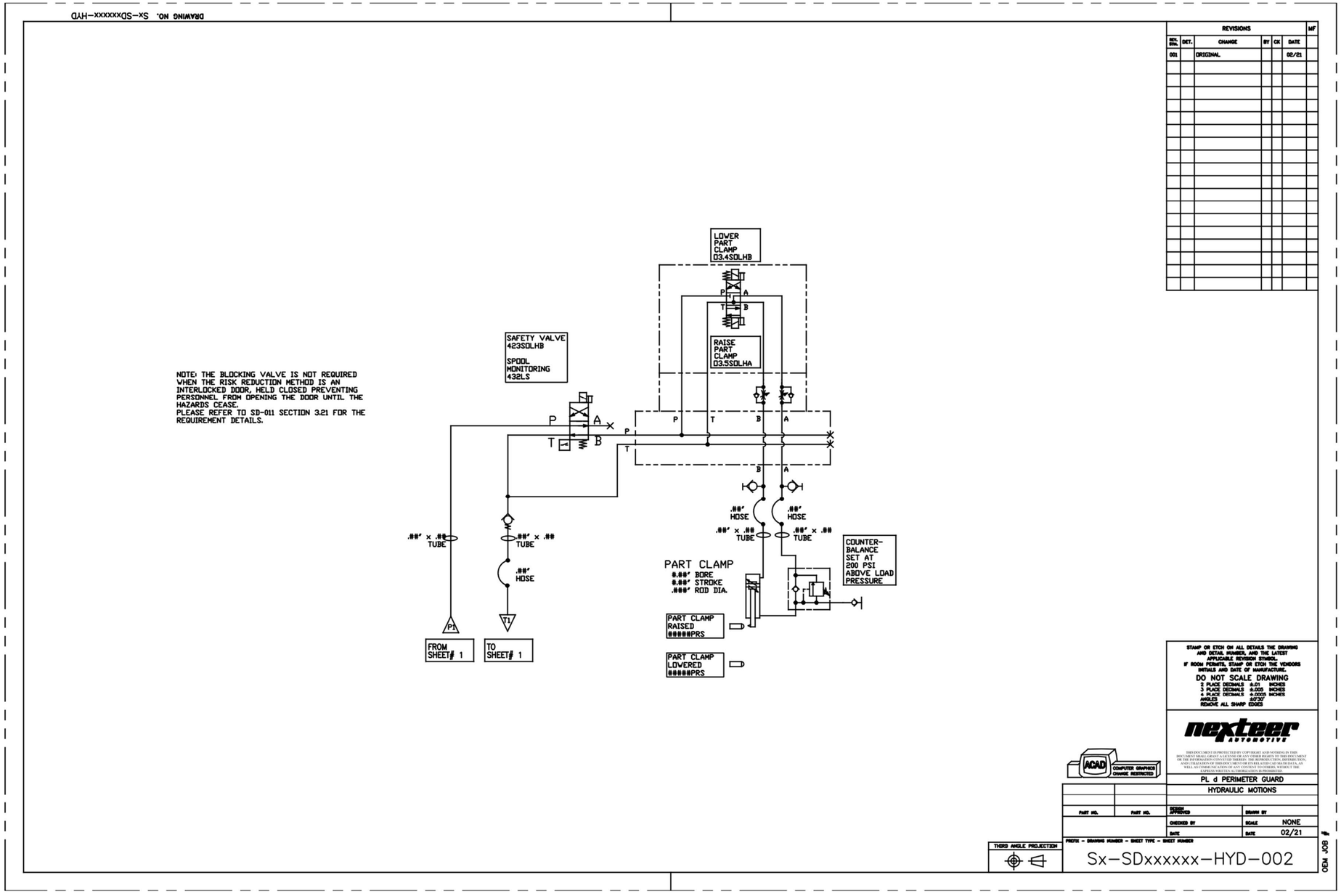
Example PL d Safety Circuits: Light Curtain w/ Pneumatic & Drive Sheet 3 of 3



Example PL d Safety Circuits: Perimeter Guard w/ Pneumatic and Hydraulic Sheet 1 of 3



Example PL d Safety Circuits: Perimeter Guard w/ Pneumatic and Hydraulic Sheet 2 of 3



Example PL d Safety Circuits: Perimeter Guard w/ Pneumatic and Hydraulic Sheet 3 of 3

2.4 PL e Requirements

Note: Nexteer prohibits engineered controls solutions as the safeguarding solution for applications that require PL e.

Engineered controls safeguarding solutions identified by the machine risk assessment to require PL e shall comply to all the requirements of PL d and Category 3, plus the following as a minimum.

2.4.1 Redundancy in the safety circuit is required, with minimum Category 4 circuit structure.

2.4.2 **Input** devices shall meet one of the following requirements. At a minimum they shall be:

1. Two devices (per safeguard) with one positive-opening contact each, or
2. Be a Type 4 ESPE rated device, or
3. PL e technology, or
4. Category 4 technology.

Clarification: More than one input device connected in series is allowed only if the device's literature clearly indicates compliance to PL e or Category 4 rating when connected in series.

2.4.3 **Logic** functions of the safety circuit shall be accomplished through safety modules compliant to published component manufacturer's literature. Safety modules shall be rated and applied at PL e. Safety module input circuits shall include input wiring short-circuit-detection.

2.4.4 **Outputs** shall be hardware-components that meet one of the following requirements. They shall be:

1. Safety-rated contacts from the safety module, or
2. Redundant industrial control relays (or motor starter contactors) with mechanically-linked contacts each enabled through separate safety-rated contacts from the safety module, or
3. A single hardware-component such as a servo or safety-rated fluid power blocking valve when rated and applied at PL e, or
4. Redundant fluid power blocking valves.

2.4.5 A feedback contact from each output device (including fluid power blocking valves) shall be through a mechanically-linked contact wired into the feedback terminals of the safety module.

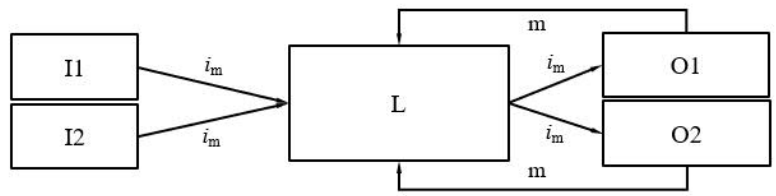
Clarification: Device literature for single hardware components, such as a servo or safety-rated fluid power blocking valve, will indicate whether feedback into the safety module is required for device compliance at PL e or Category 4.

Example: The pneumatic Herion safety valve currently listed in Nexteer's SD-007, Approved Components List, does not require a feedback signal into the safety circuit.

2.4.6 Feedback signals from output devices that do not have mechanically-linked contacts shall be designed per all three of the following requirements.

1. A contact from each feedback sensor (such as solenoid valve position sensor) shall control an industrial control relay with mechanically-linked contacts (feedback relay).
2. A contact (typically normally-opened) from each feedback relay shall be connected to the safety module feedback terminals.
3. 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.

   Note: Compliance to all the above three items provides diagnostic coverage consistent with that of mechanically-linked feedback contacts.



Key

i_m	interconnecting means
I	input
L	logic
m	monitoring / feedback
O	output

Solid lines for feedback represent diagnostic coverage higher than the architecture for PL d category 3.

Figure 2.4 PL e safety circuit block diagram

3. Application Requirements

Requirements organized by PL (including category) are detailed in Section 2 above. The requirements listed in this Application Requirements section apply to all safety circuit PLs and categories unless explicitly noted differently.

3.1 Safety Module Circuits - Logic

3.1.1 Safety modules shall be enabled when the machine disconnect is ON.

3.2 Safety Module Input Circuits

3.2.1 Connecting several safety devices in series as inputs to the same safety module shall follow the safety input device and safety module manufacturer's literature.

3.2.2 If two or more safety input devices are used in series as inputs into a single safety module, the state of each device (diagnostics typically indicating either Opened or Closed) shall be indicated as either messages or faults on the machine HMI.

3.2.3 Safety input device diagnostics (when required) shall be accomplished via independent contacts (such as a separate non-safety-rated contact from a safety gate interlock to a PLC input). PLC diagnostic inputs shall not connect to the safety module input circuitry.

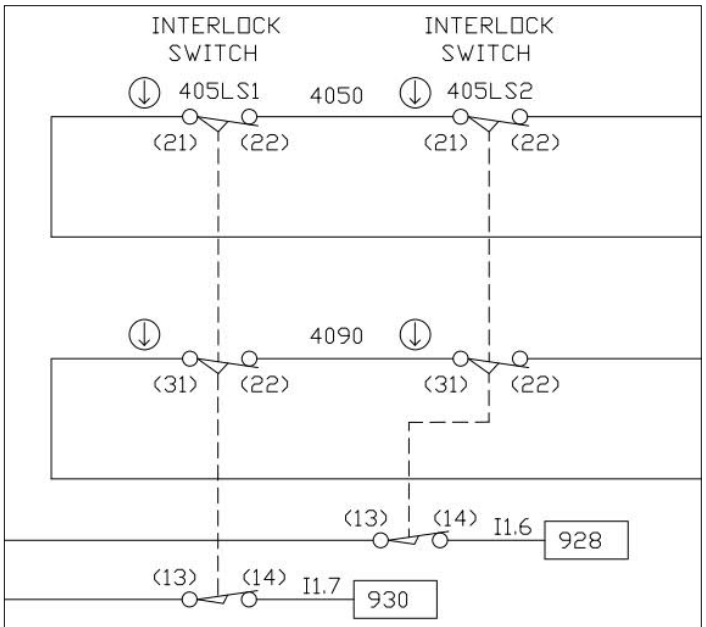


Figure 3.2.3 Independent Diagnostic Contacts

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. Anti-tie-down shall be accomplished by monitoring the reset device to have transitioned from *ON* to *OFF*.

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

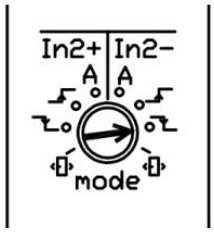


Figure 3.2.4 Reset set for Falling Edge transition

3.3 Combined Safety Input Circuits

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

Example: A machine risk assessment can identify a full-access door to require PL d for all system hazards, and small limited-access door to require PL c for only one motion. If, to minimize components and design, the two door switches are both connected in series as inputs to one safety module, then the entire door safety circuitry also must meet the one most stringent circuit requirements which in this example is PL d requirements.

3.4 Safety Module Outputs

3.4.1 Safety module outputs shall be applied per the manufacturer's documented ratings.

Note: Most safety modules have limited amperage ratings compared to the contacts available on industrial control relays.

3.4.2 When additional safety-rated outputs are required, or higher amperage rated contacts are required, expansion relays/contactors shall be used. The number of expansion relays included in the safety circuit shall be based upon category requirements from Section 2 above.

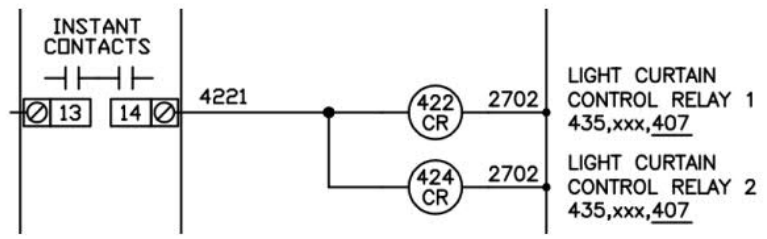


Figure 3.4.2.1 Redundant PL d Expansion Relays

1. For PL d, multiple expansion relays may be powered through one safety module output (within the amperage ratings of the safety module contact).
2. For Category 3 circuit structure, two contacts, one from each expansion relay/contactor, shall be used in series for each power-feed or hazardous device interconnection. Refer to Figure 3.4.2.2 below.

   Exceptions to item 2: Redundant contacts in series from each expansion relay are not required (a single contact from each relay is allowed) when each contact is used as separate inputs into an appropriately PL / Cat rated redundant safety input circuit such as fence inputs into a robot. Redundant contacts in series from each expansion relay are not required (a single contact from each relay is allowed) when each contact is used to provide redundant enable inputs into an appropriately PL / Cat rated safety device such as the Herion valve.

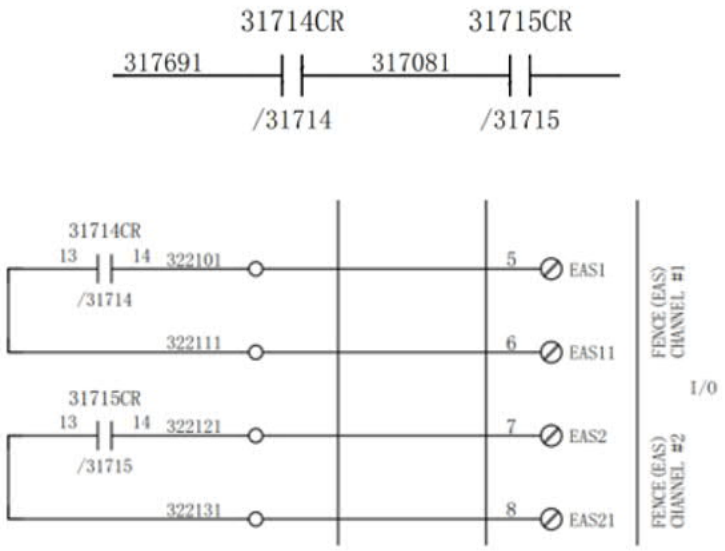


Figure 3.4.2.2 Use of Redundant PL d Expansion Contacts

- **In series as power-feed to hazardous motions (top)**
- **individual contacts to redundant safety input circuit (bottom)**

3.4.3 Safety module outputs shall not directly connect to standard PLC input modules or other potential diagnostic devices unless they are the only device connected to that safety output.

Clarification: Potential failure modes of standard PLC input modules and other diagnostic devices may compromise the safety circuit and therefore influence the safety function being performed.

3.5 Final Switching Device Feedback Clarification

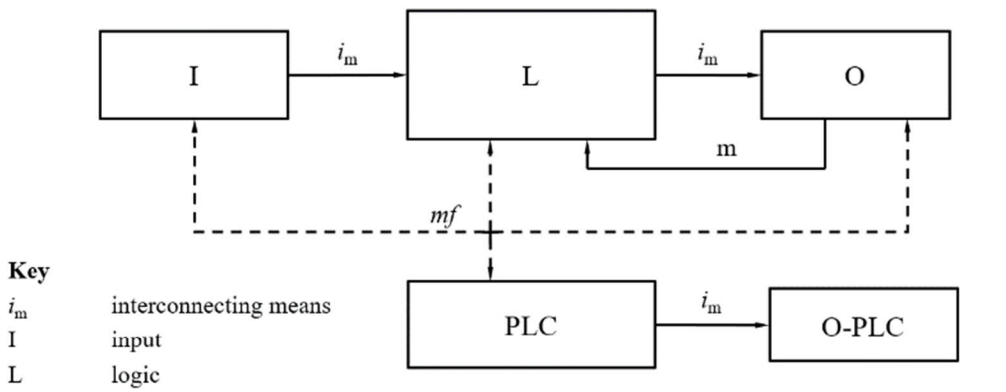
A final switching device is the electro-mechanical control device (such as a contactor, relay, motion valve, or fluid power blocking valve) that removes actual power to the hazard. The term **output** has been used in this document to include all output devices in series from the safety circuit logic device up to and including the final switching device. Since many machines have multiple types of hazards (electrical, hydraulic, pneumatic, and other) control systems might include multiple output devices.

For improved diagnostic coverage a feedback contact from each output is used to determine that the output has properly shut-off when de-energized. Nexteer specifications previously required only feedback from final switching devices.

3.6 PL d Category 2 - Required Improved Diagnostic Coverage

Clarification: Refer to Section 2 PL d requirements above. This specification's intent is that redundancy with Category 3 circuit structure is required for all custom-built machinery and the preferred solution for commodity available equipment.

3.6.1 For engineered controls safeguarding solutions identified by the machine risk assessment to require PL d, Category 2 single channel circuitry is **only** allowed when **all** single channel devices are either rated PL d, or all single channel devices are documented to have a $MTTF_D$ = high **and** a DC_{avg} ≥ medium.



Key

i_m	interconnecting means
I	input
L	logic
m	monitoring / feedback
mf	machine fault detection connections from safety devices
O	output
O-PLC	output of PLC based on machine diagnostics, including faults and machine motions
PLC	standard machine control (typically a PLC) including safety circuit diagnostics

Dashed lines represent machine fault detection

Solid lines for feedback represent diagnostic coverage higher than the architecture for PL d category 3

Figure 3.6.1 PL d Cat 2 safety circuit block diagram

3.6.2 Single channel outputs that are an industrial control relay (or motor starter contactors) shall provide mechanically-linked contacts and shall be documented to have a $MTTF_D$ = high.

3.6.3 The feedback contact from each output device (required by Section 2) shall be through mechanically-linked contacts.

3.6.4 Feedback from single-channel output devices that do not have mechanically-linked contacts shall be designed per all three of the following requirements.

1. A feedback contact from each device shall enable an industrial control relay with mechanically-linked contacts (feedback relay) (see relay 428CR in Figure 3.6.4 below).
2. A contact from each feedback relay shall be connected to the safety module feedback terminals (see 428CR contacts in Figure 3.6.4 below).
3. A second contact from each feedback relay (opposite-state to the feedback contact above) shall be connected in the power-feed line to the machine's hazardous devices (see 428CR contacts in Figure 3.6.4 below).

   Note: Compliance to all the above three items provides diagnostic coverage consistent with that of mechanically-linked feedback contacts.

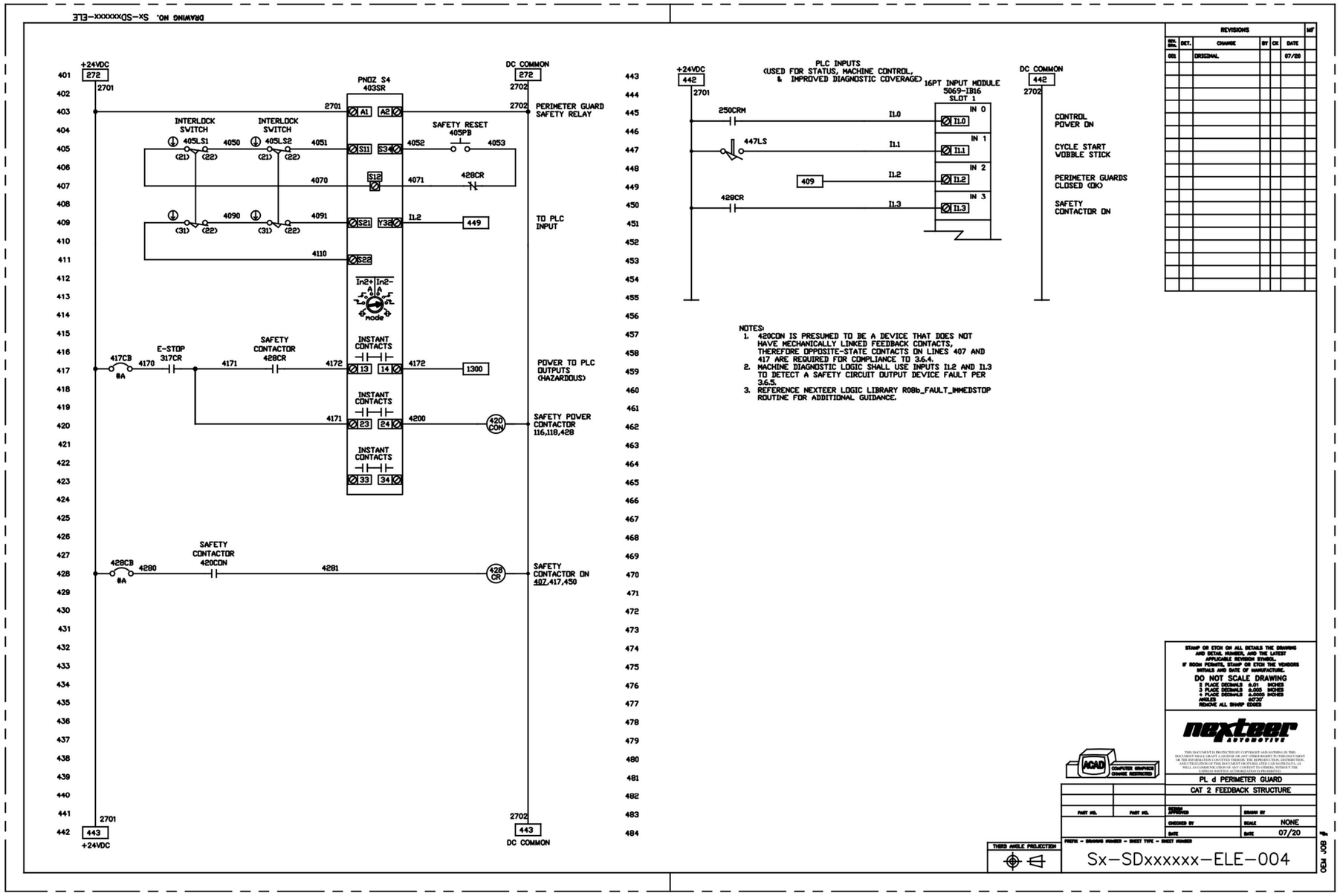


Figure 3.6.4 Example PL d Cat.2 Safety Circuits: Perimeter Guard w/ Monitoring non-Mechanically-Linked Contacts

3.6.5 For all output devices the machine diagnostics logic shall initiate an Immediate Stop fault when a safety circuit output device fault has been detected. The machine diagnostics logic shall compare PLC inputs from each output device (additional feedback contacts) against a PLC input of the safety module status. Refer to Figure 3.6.5 below.

Clarification: This machine logic and diagnostics may be integrated into the machine's non-safety-rated PLC.

Clarification: The above machine diagnostic logic and output device fault detection apply for output devices that require feedback signals into the safety module.

Clarification: Refer to Nexteer's SD-1032, Programmable logic Controller Application Specification, for machine logic details such as the definition of an Immediate Stop fault.

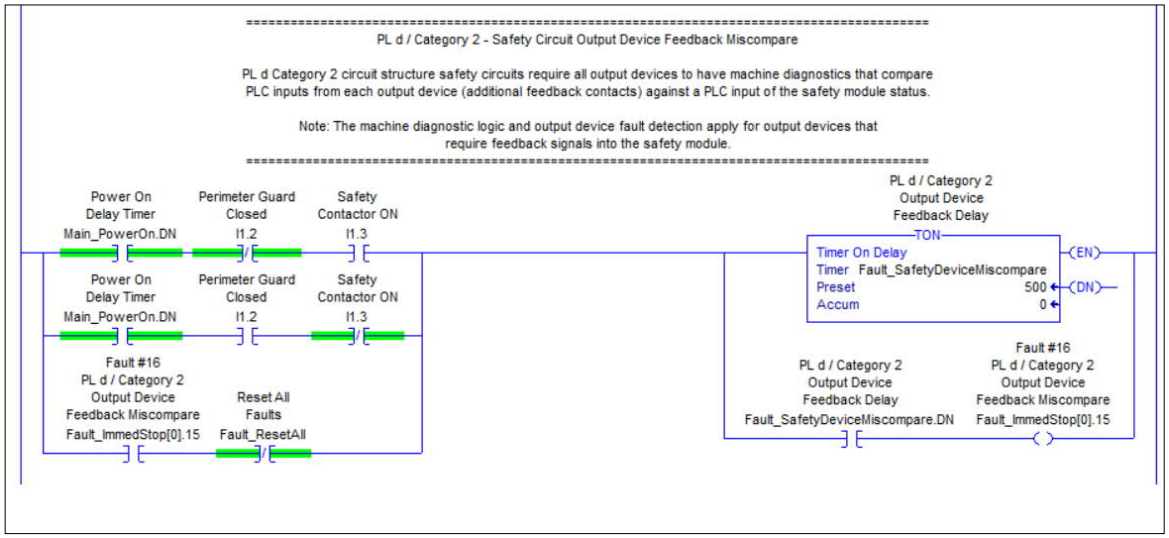


Figure 3.6.5 – Immediate Stop fault logic for Output Device Fault

3.7 Emergency Stop Applications

Clarification: Refer to Nexteer's SD-004, Electrical Specification for Industrial Machinery Addendum to IEC 60204-1, for additional Emergency stop application requirements. In case of conflict between SD-004 and SD-011, SD-004 Emergency stop requirements take precedence.

Clarification: Refer to Nexteer's SD-007, Approved Components List, for additional Emergency stop device requirements. In case of conflict between SD-007 and SD-011, SD-007 device requirements take precedence.

Emergency stop (E-stop) devices and circuits provide a complementary protective measure that is typically not the primary risk reduction method (safeguard) for hazards on a machine.

3.7.1 The E-Stop circuit performance level shall meet the required PL level of each task-hazards primary safeguard as documented on the machine risk assessment and be implemented at a minimum PL c.

Clarification: If a task-hazard requires a PL d primary safeguard circuit performance, the E-Stop circuit shall be implemented PL d as well for that hazard.

Note: E-Stop circuits on robot applications require a minimum PL d.

3.7.2 E-stop pushbuttons shall comply with IEC 60947-5-5. E-stop pushbuttons 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.

3.7.3 Safety-rated cable-operated E-stop switches shall comply with IEC 60947-5-5. Cable-operated E-stop switches shall have contacts that opens when the cable is pulled and opens when cable tension is lost. These contacts shall latch in the opened position until the switch is manually reset.

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

Note: Refer to SD-004 and SD-012 for additional E-stop location details.

3.7.5 The Emergency Stop function "Span of Control" shall cover the whole machine unless stopping all machinery would result in additional hazards or it would unnecessarily affect production. If multiple E-Stop zones are necessary, they should be clearly defined and identifiable at each E-Stop device location.

Note: Refer to SD-012 for additional E-stop span of control details.

3.7.6 E-stop devices shall provide redundant inputs to the safety circuit.

3.7.7 A maximum of five E-stop devices may be wired in series to the safety module inputs for PL d circuit performance applications.

3.7.8 E-stop devices shall be connected directly to a dedicated E-Stop safety module. The safety module shall perform the required emergency stop function.

Clarification: This requirement prohibits both the connecting of E-Stop devices as inputs directly into the safety module of another safeguarding circuit such as perimeter guard, and it prohibits connecting other input devices such as perimeter guard devices as inputs into the dedicated E-Stop safety module.

3.7.9 The E-Stop safety module outputs may either feed an input into another safeguarding circuit (redundant inputs for PL d safeguarding) or, be applied in series with the other safeguarding outputs.

Note: SD-004 requires that all servo drive applications be implemented as Stop Category 1 which requires that the E-stop circuitry for the servo drive also be applied as a Stop Category 1.

3.7.10 The E-stop safety module reset function shall:

1. be reset (start) by a contact from an E-stop reset pushbutton, or a PLC output with the reset function initiated by an HMI reset button.
2. not be reset by pulling-out or twist-release of an E-stop pushbutton.
3. not reset on application of power.

3.7.11 The E-stop function shall not be bypassed.

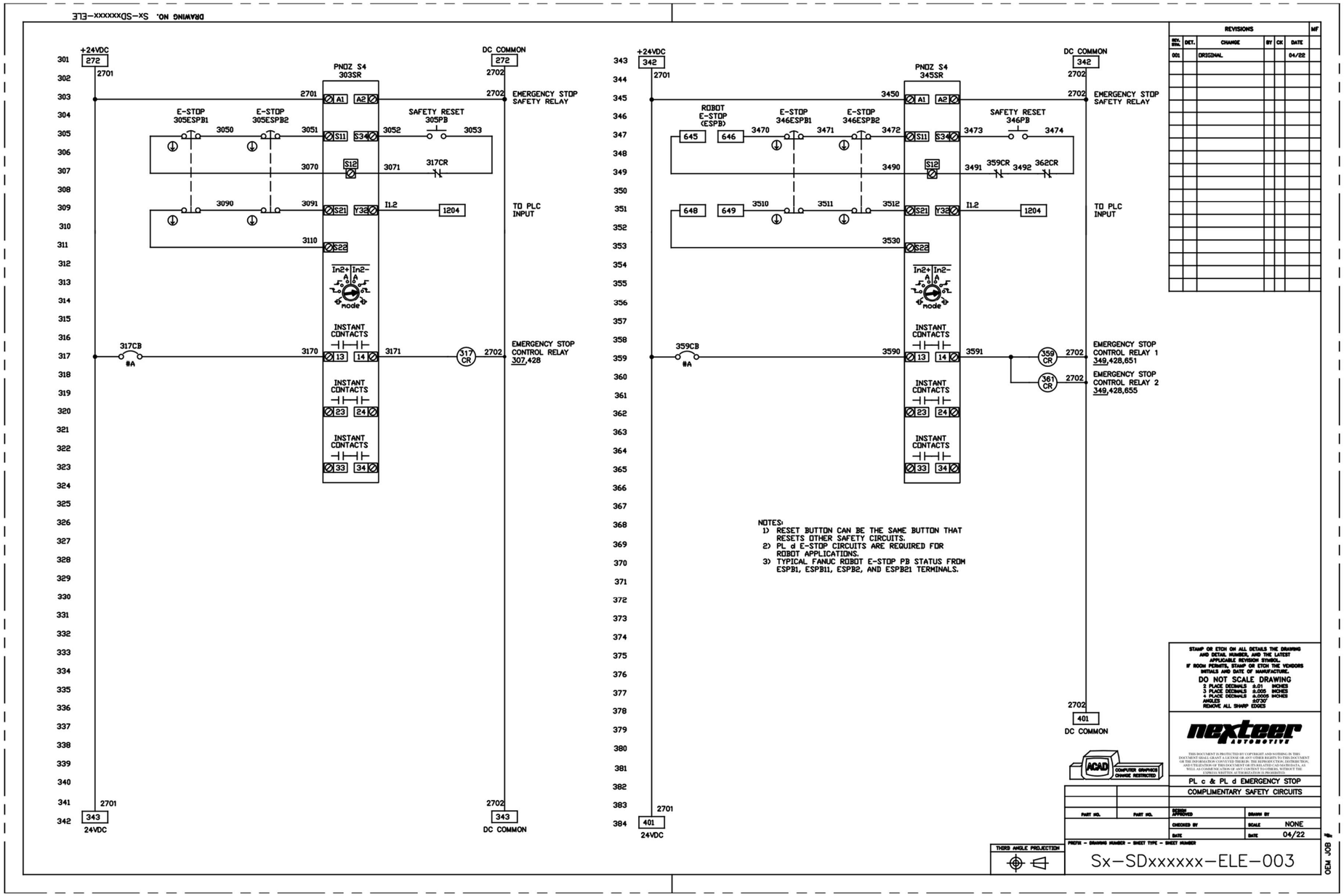


Figure 3.7 (a) Example PL c Safety Circuits: E-Stop

Figure 3.7 (b) Example PL d Safety Circuits: E-Stop

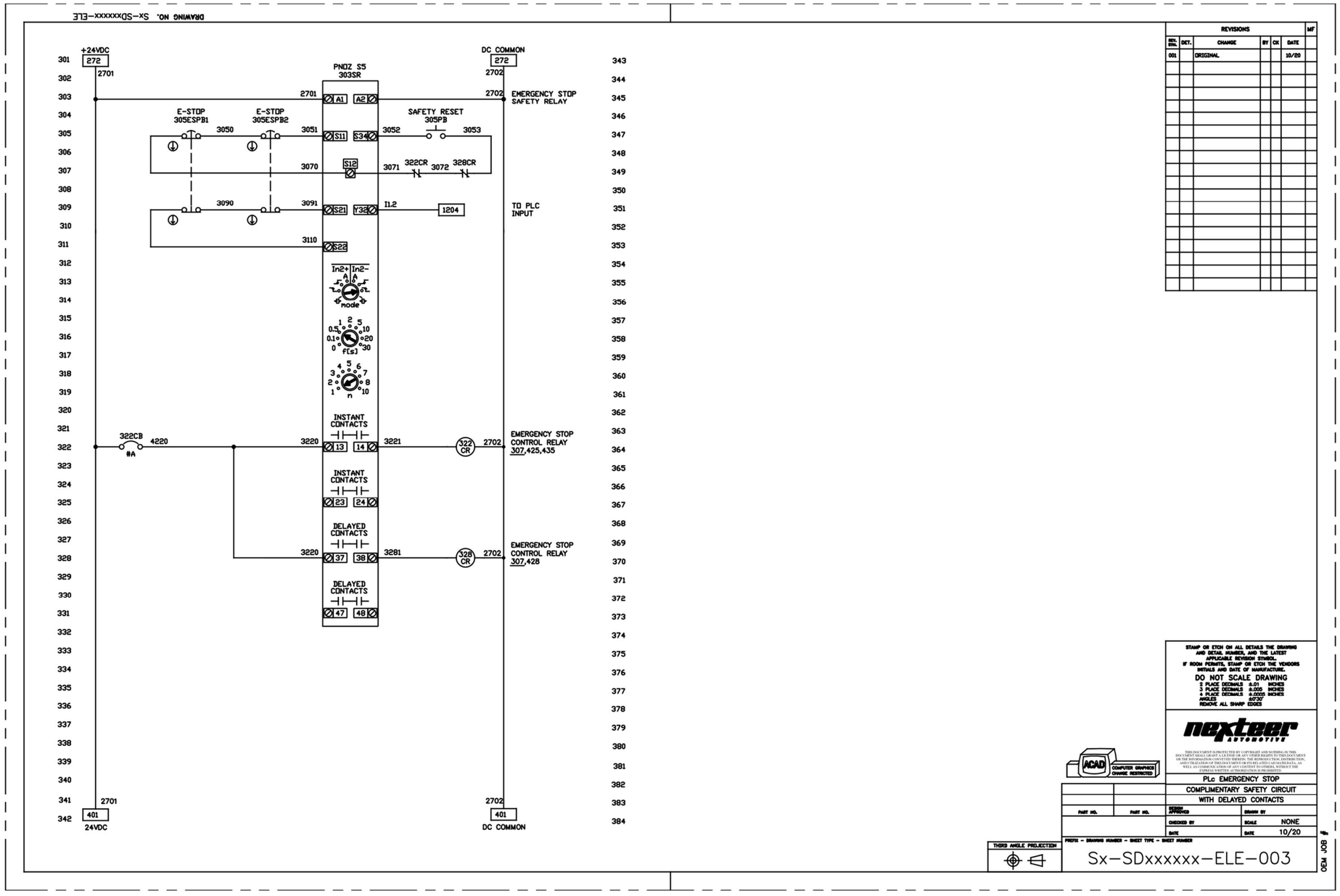


Figure 3.7 (c) Example PL c Safety Circuits: E-Stop with Category 1 stop delay

3.8 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 machine risk assessment.

3.8.1 Safety interlock switches shall comply with IEC 60947-5-1 for mechanical type switches, and IEC 60947-5-3 for non-contact type switches.

3.8.2 Safety interlock switches shall be connected into a safety module.

3.8.3 A maximum of five mechanical safety interlock switches may be wired in series to safety module inputs for PL d circuit performance applications.

3.8.4 Mechanical safety interlock switches shall not be wired in series to safety circuit inputs on PL e circuit performance applications.

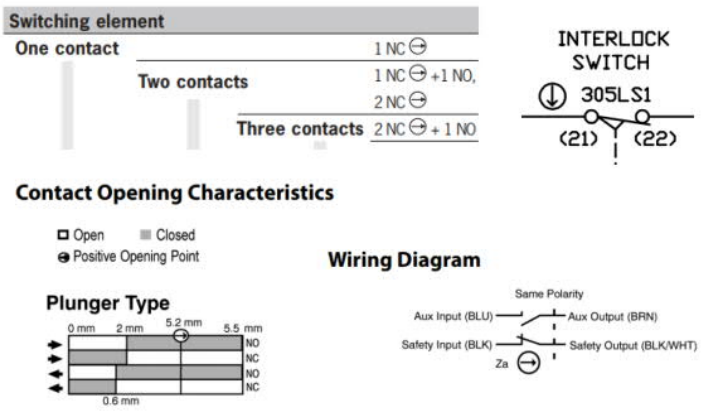


Figure 3.8.4 Indication of Positive-opening Examples

3.8.5 Safety circuit input contacts used from mechanical safety interlock switches shall be positive-opening and shall be safety output (OSSD) signals for non-contact type interlock switches.

3.8.6 Safety interlock switches shall be located and mounted to prevent damage and to minimize tampering. They shall be installed in accordance with the instructions provided by the device manufacturer. They shall not be easily defeated with readily available tools, objects, or by tying down the actuators.

3.8.7 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:

1. 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).
2. Safety interlock circuit reset devices are permitted to be reset devices that also perform other reset functions, such as the E-Stop Reset pushbutton, provided all the reset requirements of this section are met.
3. The reset device shall be positioned such that it cannot be reached from within the protected area.
4. The reset device shall be positioned such that the entire safeguarded area is visible, allowing the operator to view that no personnel are in the safeguarded area.

5. Exception to item 4 above: Where the entire safeguarded area 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 safeguarded area. The number of reset locations should be minimized. The reset devices shall be connected to an appropriate safety circuit which is designed to impose a certain reset sequence with specific timing. Refer to Figure 3.8.7.5 Example diagram.
6. Multiple, independent reset devices are permitted, provided the entire area protected by the perimeter guard is visible from each reset location.

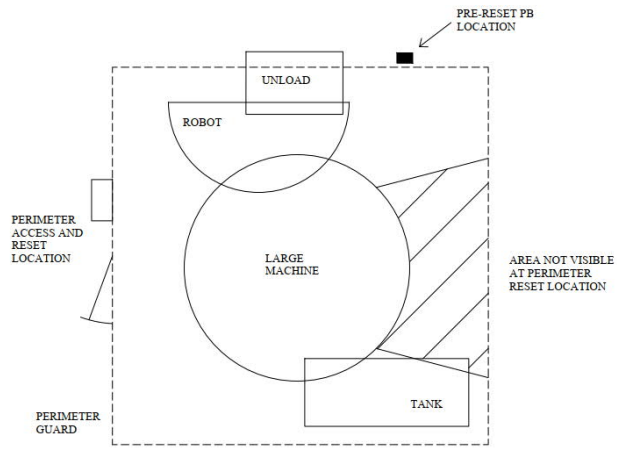


Figure 3.8.7 Item 5 Example - Entire Safeguarded Area Not Visible from Reset Location

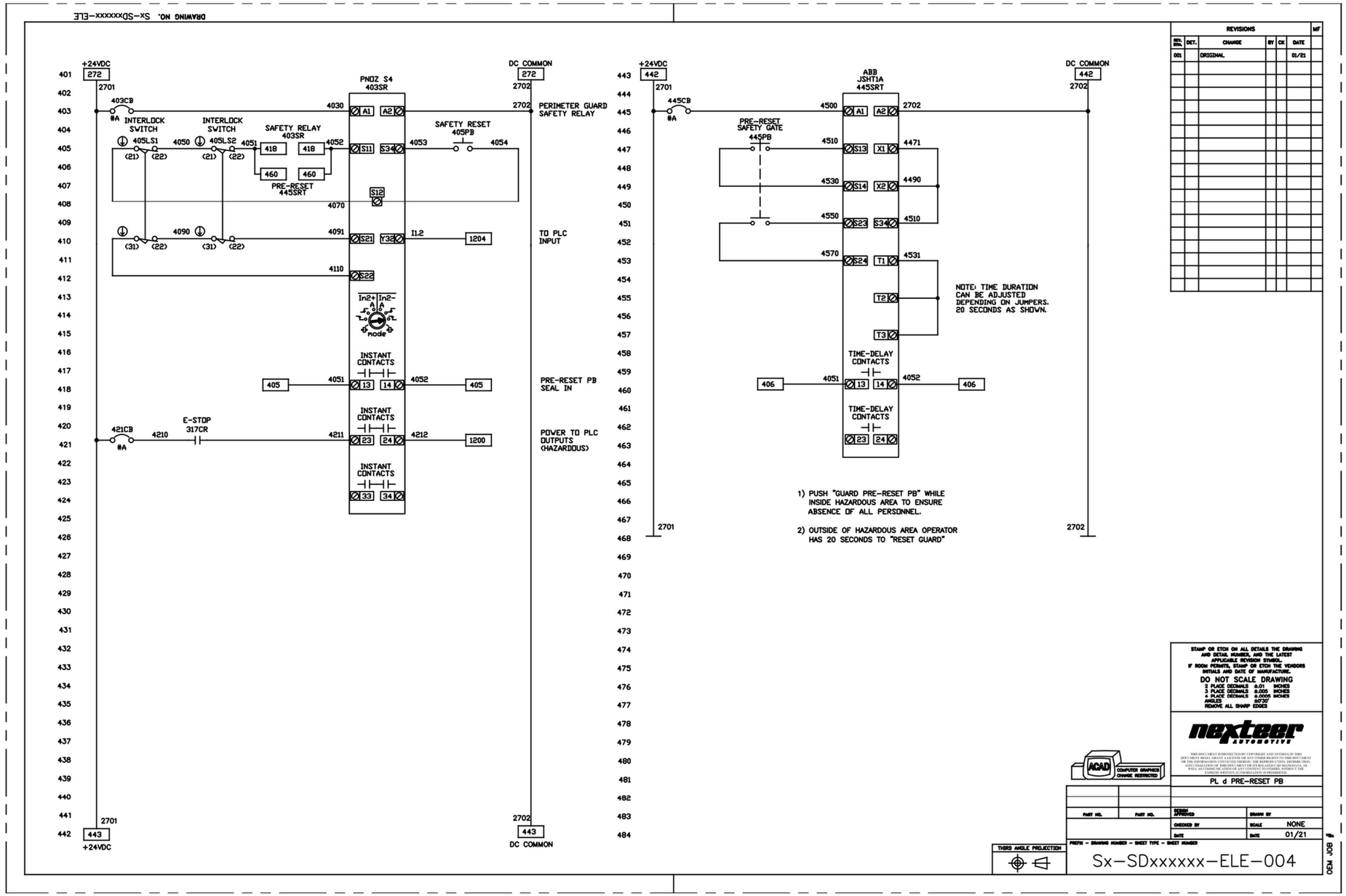


Figure 3.8.7.5 Example PL d Pre-Reset Circuit for Perimeter Guard Application

3.9 Guard Locking Safety Interlock Applications

Guard locking is applied on applications to keep a movable guard closed during machine functions preventing personnel from gaining access to hazards that will not stop in time or from interrupting the process.

Guard locking safety interlock applications include interlocked guard doors that are held-closed by the application of guard locking safety interlock switches as well as interlocked guard doors that are held-closed by other mechanical means such as a shot pin. This section details the requirements for both the guard locking safety interlock switches (referred to as locking interlock switches) and for the complete application (referred to as guard locking).

3.9.1 Guard locking applications shall comply with all the requirements of the Safety Interlock Switch Application section above.

3.9.2 The closed and locked position safety contacts (outputs) from guard locking safety interlock switches shall be connected into a safety module.

Note: If the locking mechanism can only engage when the guard is in the closed position, the closed and locked position sensing can be accomplished by the monitoring of the locked position only.

3.9.3 Locking interlock switches shall be "Power-ON to release" for risk reduction methods identified by the machine risk assessment that indicate guard locking for the safety of personnel.

Note: Typical Power-ON applications can include induction equipment that requires cooling the part prior to allowing access to a guarded area, high-momentum grinding wheels that have lengthy stop-times, or machining cells to prevent machine damage, broken tools, or flying parts if the system is interrupted during cycle.

3.9.4 Locking interlock switches are allowed to be "Power-OFF to release" for interlocked guard applications in which guard locking has not been included for the safety of personnel and used solely for the protection of a process.

Note: The locking mechanism will release during loss of power, often lengthening the stopping time of machine considerably. It can be possible to access hazards before they cease. This shall be considered during the risk assessment.

3.9.5 Guard locking applications shall prevent unlocking of the guard until all hazardous machine functions safeguarded by the guard have ceased for risk reduction methods identified by the machine risk assessment that indicate guard locking for the safety of personnel.

3.9.6 Unless otherwise identified by the machine risk assessment, the command to unlock the guard locking mechanism may be generated by the control system PLC.

Note: Solutions to prevent unlocking until hazards cease may include, but are not limited to safe-speed monitoring, zero speed switch, signal from safe stop control/drive control, or a safety timer.

Note: The command to unlock the guard locking mechanism for linear fluid power applications can be generated by the control system PLC.

3.9.7 Lock position sensing shall be connected to the machine control system for diagnostics and process control.

Clarification: Examples of lock position sensing can include a solenoid-position contact from solenoid-type locking interlock switch, or a proximity switch sensing a guard locking cylinder, electromagnetic lock sensing, or similar.

3.9.8 Power-ON to release locking interlock switches shall include an auxiliary release. The locking interlock switch shall be positioned such that the auxiliary release is accessible from outside the guarded area. Unlocking of the interlock switch by use of this auxiliary release shall generate a stop command.

Clarification: The required auxiliary release is intended to be used in exceptional cases where power is lost, being the locking interlock switch will remain locked. It is not an Escape Release located inside of a cell.

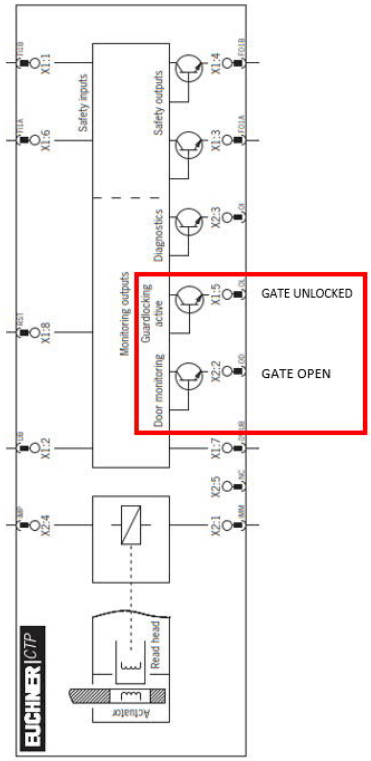


Figure 3.9.7 Lock Position Sensing / Indication

3.10 Safety Light Curtain Applications

3.10.1 Light curtains shall comply with both:

1. IEC 61496 as a Type 4 ESPE device, and
2. EN/ISO 13849 as a PL e device

3.10.2 Light curtains shall provide redundant safety inputs connected directly into a safety module.

3.10.3 Light curtains shall be located at a distance from the associated hazard(s) such that individuals cannot reach the hazard before cessation of hazardous motion (or situation). Refer to SD-012 Annex A for a method to calculate an estimated safe distance.

Note: Circuits that minimize the number of logic and output devices between the light curtain and the final switching device can also minimize the off-response time.

Note: For additional light curtain placement requirements particular to robot and operator Shared Workspace applications refer to the robot application section below.

3.10.4 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 3.8.6 above shall apply.

3.11 Safety Laser Scanner Applications

3.11.1 Laser scanners shall comply with both:

1. IEC 61496 as a Type 3 ESPE device, and
2. EN/ISO 13849 as a PL d device

3.11.2 Laser scanners applications shall meet the application requirements for light curtain applications above.

3.11.3 Laser scanners shall have a Class 1 laser classification.

3.12 Presence Sensing Device Initiation (PSDI) Applications

3.12.1 Light curtains used for PSDI shall:

1. meet all the requirements of the Light Curtain Applications section above.
2. cover only one opening of the machine.
3. not have Blanking implemented.
4. have a minimum object sensitivity no greater than 14 mm.

3.12.2 Cascading light curtains may be used in PSDI applications, but mirrors shall not be used.

3.12.3 Light curtain safety distance calculations or tested safety placement distance shall be documented on the hardware schematics.

3.12.4 PSDI shall not be implemented on full revolution mechanical power presses or in operations located in Brazil.

3.12.5 PSDI shall not be used on guard applications where an operator can pass completely through the light curtain and stand between the light curtain and the hazard.

3.12.6 Each machine incorporating PSDI shall have a caution sign that indicates PSDI is being used per figure 3.12.6. The sign shall use Black lettering on Yellow background. The sign shall be mounted in a position clearly visible to the operator.

Figure 3.12.6 PSDI Caution Sign

3.12.7 PSDI Cycle allows machine cycle through the PSDI Armed function. Selection of PSDI Cycle shall not enable PSDI Armed nor shall PSDI Cycle selection initiate any motion.

Note: Nexteer's equipment typically includes two modes, Auto and Manual. Per required Nexteer Library logic, for PSDI Cycle and PSDI Armed to be enabled Auto Mode shall be active.

3.12.8 PSDI Armed is the control function that makes a machine capable of going In Cycle, producing sequenced motions.

3.12.9 PSDI Armed shall be indicated with a white indicator pilot light. The light shall be mounted in a position clearly visible to the operator (such as near the caution sign required above). PSDI Armed may additionally be indicated on the operator HMI.

3.12.10 Operator initiation of PSDI Armed, cycle start initiation by use of a switch, is required after PSDI Cycle selection, and again after PSDI Armed is disabled.

3.12.11 PSDI Armed shall be disabled when not in PSDI Cycle, and when an E-stop occurs, and when a cycle overtime fault, light curtain field interrupted prior to end of cycle, or any other abnormal stop has occurred.

3.12.12 PSDI Armed shall also be disabled when the machine is not In Cycle for more than a preset time. The appropriate time setting will depend on the application.

3.12.13 Sensors shall be provided to detect that all parts are properly loaded before initiation of the machine cycle.

3.12.14 Initiation of the machine cycle shall occur only as the result of a specific sequence of events, such as part presence sensors released, followed by parts detected as loaded in position (anti-repeat) and the light curtain's field interrupted and cleared. Initiation of the machine cycle shall not occur based only on cycling of the light curtain one or more times.

3.13 Bypassed and Muted Safety Circuits

Clarification: Muting is an automatic bypass (such as during normal machine cycle) and therefore all Bypass requirements apply to Muting.

3.13.1 Bypassing a safety circuit with another safety circuit is permitted as identified by the machine risk assessment.

3.13.2 Bypassing shall be accomplished by combining (in parallel) the outputs from the two safety circuits.

3.13.3 Bypassing shall meet the most stringent requirements as determined by the machine risk assessment, including output device and feedback requirements.

3.13.4 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.

Example: Bypass circuits include a hand-held enable device application or two-hand manual control. The machine risk assessment identifies both a perimeter door application and an enable device to bypass the door safety circuit. The station can be energized when either the door is closed, or the enable device is actuated. These safety circuits are integrated in parallel; each circuit is required to be implemented to the most stringent PL /category for the machine hazards identified on the machine risk assessment.

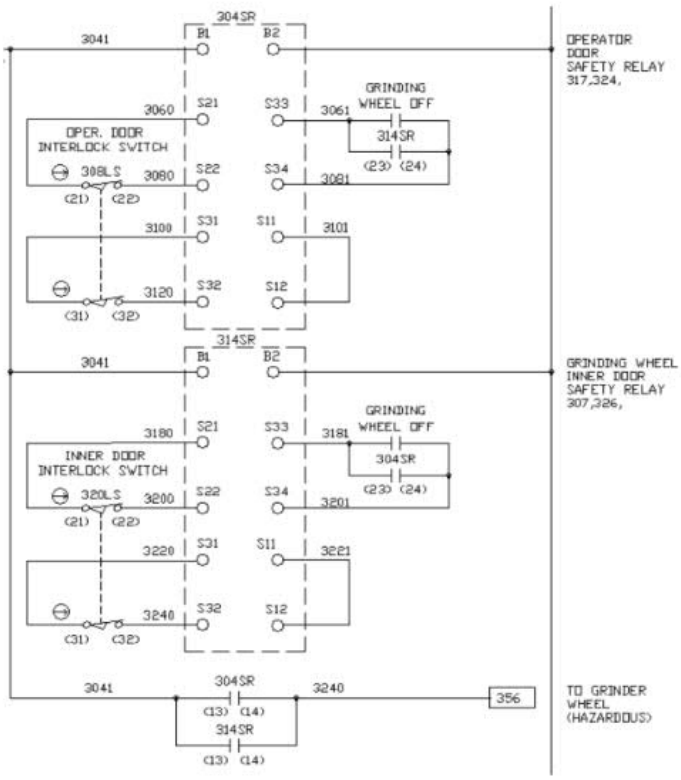


Figure 3.13 Bypass Safety Circuit (Two Safety Doors in Parallel)

Muting Example: An operator-loaded grinder, with both an inner door providing operator protection during loading, and an outer door providing operator protection when the inner door is open during part-processing. The machine risk assessment identifies both door applications; the grinding wheel spindle can be energized (maintain speed) when either door is closed. These safety circuits are integrated in parallel; each circuit is required to be implemented to the most stringent PL /category for the grinding wheel hazard identified on the machine risk assessment.

3.13.5 Bypass circuits should also consider the following:

- Bypass circuit contact ratings
- Safety module reset application details including feedback from output devices
- Feedback of collective output devices into multiple safety modules
- Bypassing of the final switching devices from two safety circuits might require additional final switching devices

3.14 Two-Hand Control – General

Note: Nexteer's equipment and processes included limited use of two-hand control. There are essentially two application types for two-hand control within Nexteer: one being machine cycle initiation where two-hand cycle initiation is the sole safeguarding solution, and the second being manual control where two-hand manual control bypasses another safeguarding solution.

3.14.1 The requirements within this section (Two-Hand Control – General) apply to all two-hand applications, whether applied as machine cycle initiation or applied as manual control.

3.14.2 Two-hand control devices (input devices) shall be designed, constructed, and arranged to:

1. Provide a normally-opened and a normally-closed contact from each device as input(s) to the safety module.
2. Protect against unintended or inadvertent operation of the machine.
3. 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).
4. Be located at a distance from the nearest hazard such that upon release of a two-hand control device the operator cannot reach the hazard before cessation of hazardous motion. Refer to SD-012 Annex A for a method to calculate an estimated safe distance.

   Note: Limit switches are not allowed as two-hand control operators because they cannot be protected against unintended or inadvertent operation.

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

1. Continuous concurrent actuation by both hands is required during the hazardous motion.
2. The hazardous motion(s) shall cease upon the release of either one or both of the control devices.

3.14.4 Two-hand control circuits shall require the use of a two-hand control safety module of the appropriate PL.

Note: Currently device manufacturers do not provide two-hand control safety modules that are rated PL c. Therefore, to meet the minimum Nexteer application requirements as described in Section 2 of this document, all two-hand control safety module applications require the use of minimum PL d safety modules.

3.15 Two-Hand Control – Machine Cycle Initiation

3.15.1 Two-hand cycle initiation circuits shall require:

1. The release of both control devices before machine operation can reinitiate (anti-tie-down).
2. The control devices be actuated within a time limit of each other, not exceeding 0.5 seconds (concurrency time). Where this time limit is exceeded, both control devices shall be released before machine operation can be initiated.

   Note: Anti-tie-down, and control device input concurrency time of 0.5 seconds, are both included within minimum PL d two-hand control safety modules.

   Note: Nexteer Brazil requires two-hand control machine cycle initiation to be implemented in addition to a light curtain that has been implemented as the risk reduction method. The light curtain is the risk reduction method. The two-hand control machine cycle initiation may be implemented in a standard PLC at a PL b safety rating.

3.15.2 Consecutive machine cycles shall not result from continuous actuation of both two-hand control devices.

3.16 Two-Hand Control – Manual Control

Note 1: PL b two-hand manual control circuits would typically be indicated on the machine risk assessment as a manual control bypass of a PL c point-of-operation guard.

Since bypassing a safety circuit requires the bypass safety circuit be equal or greater reliability than the safety circuit being bypassed, it follows that PL b two-hand manual control circuits are required to be implemented as a minimum PL c.

Also, since currently device manufacturers do not provide two-hand control safety modules that are rated PL c, and in order to meet the minimum Nexteer application requirements as described in Section 2 of this document, it also follows that PL b two-hand manual control safety module applications require the use of minimum PL d safety modules.

Note 2: PL d two-hand manual control circuits would typically be indicated on the machine risk assessment as a manual control bypass for a PL d guard (including PL d perimeter guards, and PL d point-of-operation guards), again basically requiring the use of minimum PL d safety modules.

3.16.1 Consequently, all safety modules for Two-hand manual control bypass of safeguarding are required to be a minimum PL d.

3.16.2 For Two-hand manual control bypass of a PL c safeguarding, the output device and feedback circuit shall be a minimum of PL c.

3.16.3 For Two-hand manual control bypass of a PL d safeguarding, the output device and feedback circuit shall be a minimum of PL d.

Note: If a guard locking door was implemented to eliminate the blocking valve(s) for a PL d point-of-operation guard, then the addition of two-hand manual control bypass reestablishes the requirement of the blocking valve(s).

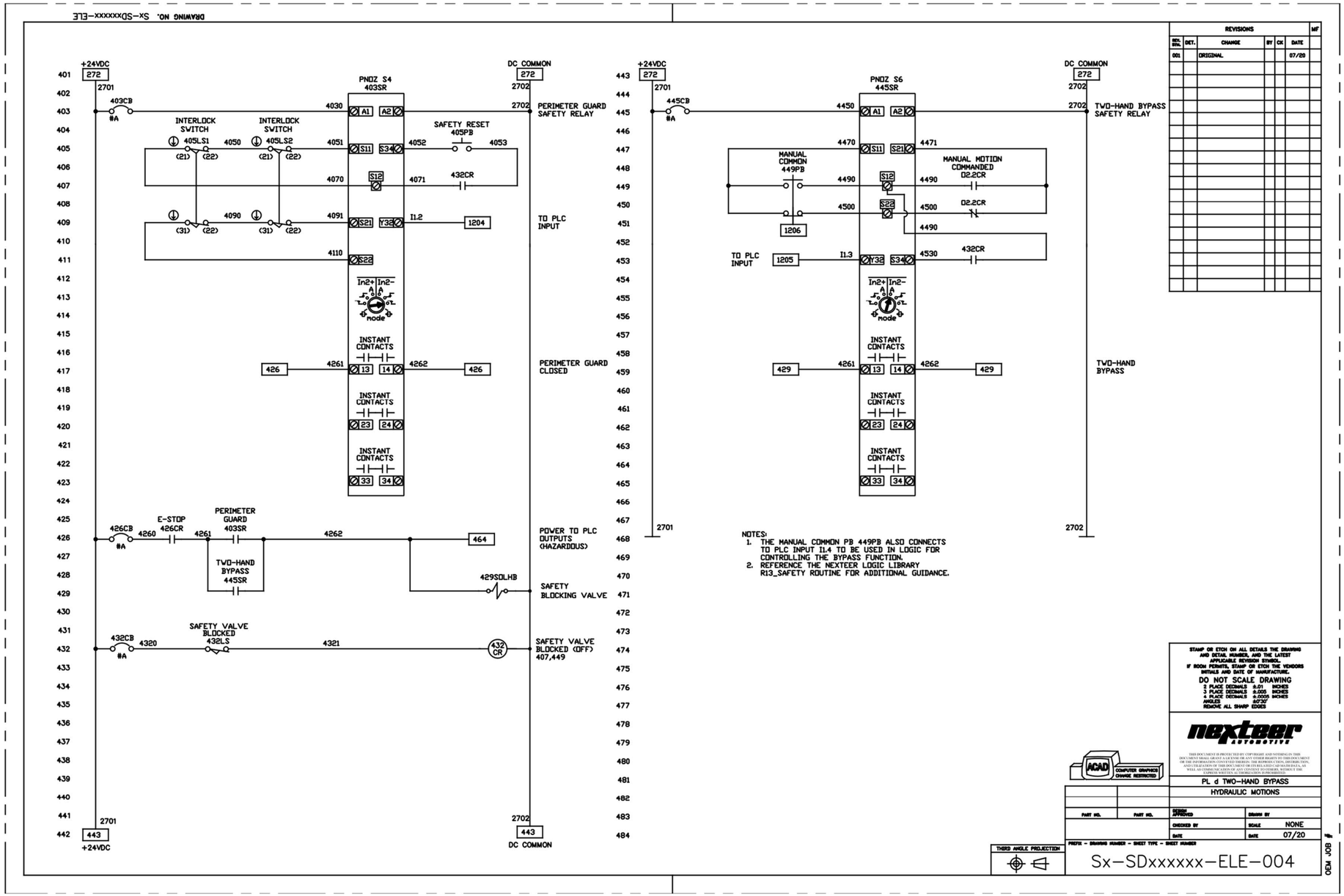


Figure 3.16.3 Example PL d Safety Circuit: Two-Hand Bypass of Perimeter Guard Sheet 1 of 2

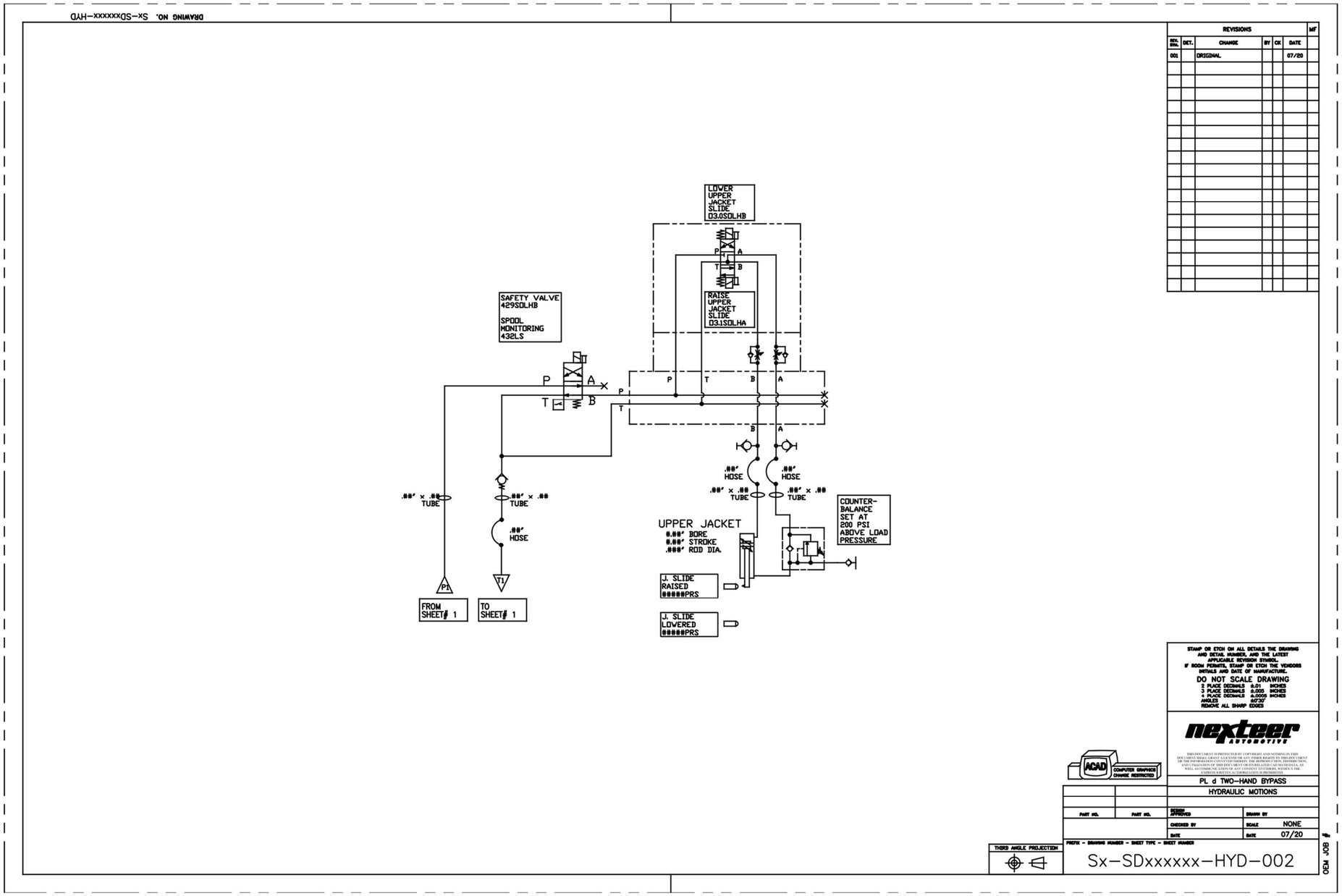


Figure 3.16.3 Example PL d Safety Circuit: Two-Hand Bypass of Perimeter Guard Sheet 2 of 2

3.17 Robot Applications

Nexteer specifications for robot applications are detailed in SD-012 and SD-1040 Fanuc Robot Specification. Safety circuit PL requirements for robot applications, and only safety-related requirements, are included within this specification. If there is conflict between this specification and either SD-012 or SD-1040, SD-012 or SD-1040 takes precedence.

Clarification: Topics covered in SD-012 include Shared Workspace Safeguarding and Lockable Manually Operated Perimeter Guard Door Interlock Switch Actuator.

3.17.1 The Emergency Stop circuit shall be implemented at a minimum PL d.

3.17.2 The interlocked guard door circuit shall be implemented at a minimum PL d.

Clarification: Robots typically use the term Protective Stop or Fence for interlocked guard door inputs.

3.17.3 A robot disable circuit shall be provided for all full body access robot cells.

1. The robot disable circuit shall be implemented at a minimum of PL d.
2. The robot disable circuit shall provide redundant inputs to the robot SVOFF inputs of each robot within the same safeguarded area. If the robot controller does not support SVOFF inputs, the redundant inputs shall connect to the robot Emergency Stop inputs.
3. Each robot disable switch shall be lockable, and lockable in the off position only.
4. Each robot disable switch shall be a two position, maintained switch.
5. Each robot disable switch shall be readily accessible where the operator can request to enter the cell, such as each operator control station or cell access point.

Note for item 1 and 2: For single robot applications, a lockable disconnect switch, directly feeding the robot SVOFF or Emergency Stop inputs, complies to these specification items.

Clarification for item 3: The robot disable switch shall be capable of being locked with a plant-approved personal lockout lock and not be a keyed-switch.

Clarification: The robot disable circuit is used when entering the safeguarded area to perform minor servicing activities other than teaching the robot.

Clarification: The robot disable circuit shall only require the use of a single robot disable switch to disable all robots in a designated safeguarded area.

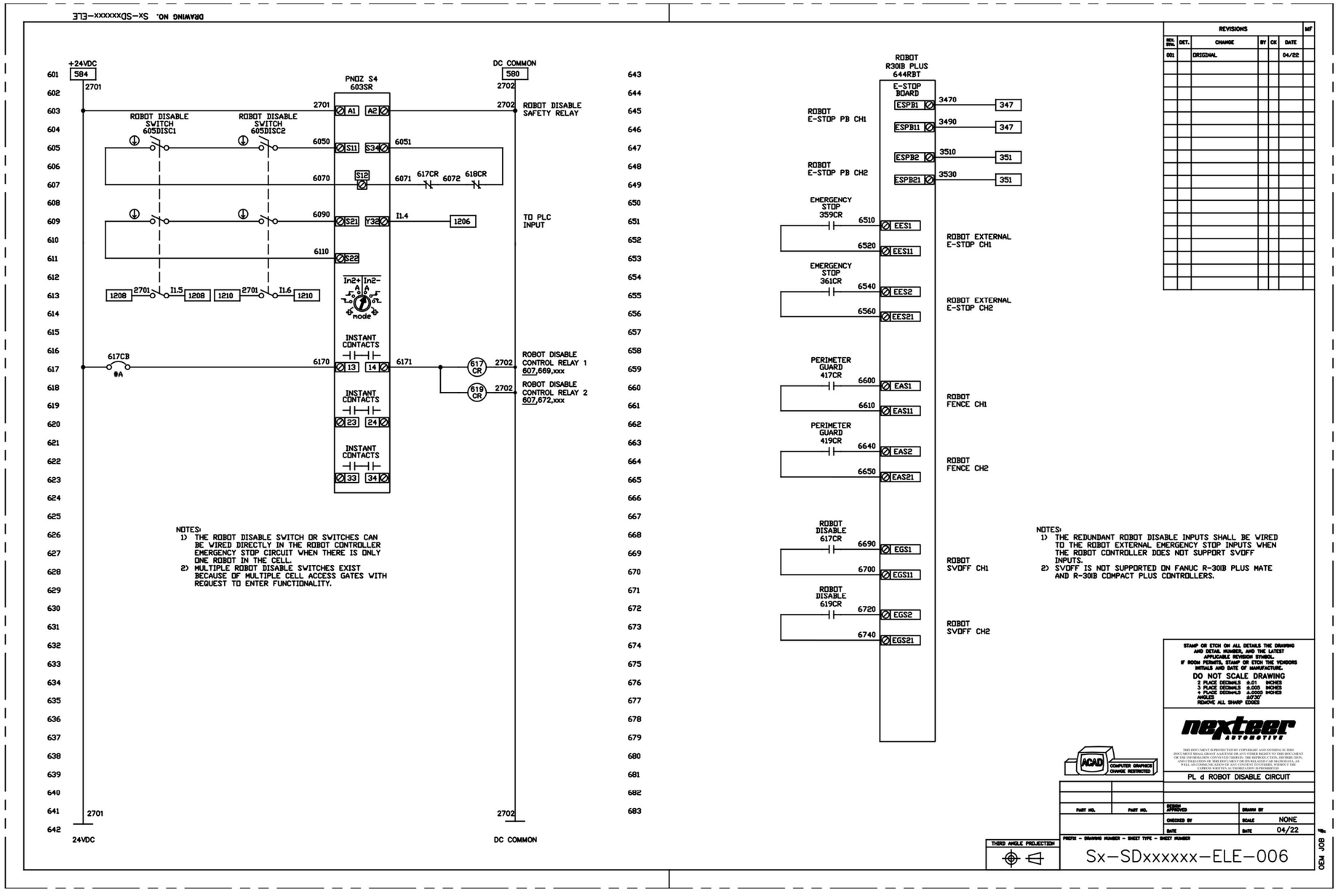


Figure 3.17.3 Example PL d Safety Circuit: Robot Disable

3.17.4 A hand-held enable device (3-position) shall be provided for each person required to be inside the safeguarded area when teaching a robot. The following requirements apply to enable devices that are integrated in addition to the robot teach pendant enable device provided with the robot.

1. Each enable circuit shall be implemented at a minimum of PL d.
2. Each enable device shall provide redundant inputs to an appropriately rated, configurable, safety module. This safety module in-turn provides inputs to the robot controller emergency stop safety inputs.
3. Each enable device shall have an integrated safety interlock for detecting when it is in the storage position. The enable device storage interlock switch shall be integrated into the robot safety circuit(s), bypassing the enable device.

   Clarification: Current Nexteer approved robots include a teach pendant with enable device for the primary operator teaching a robot.

   Clarification: The number of operators allowed in the cell is limited by the number of enable devices provided; however, fewer operators are allowed in the cell based on the teaching task.

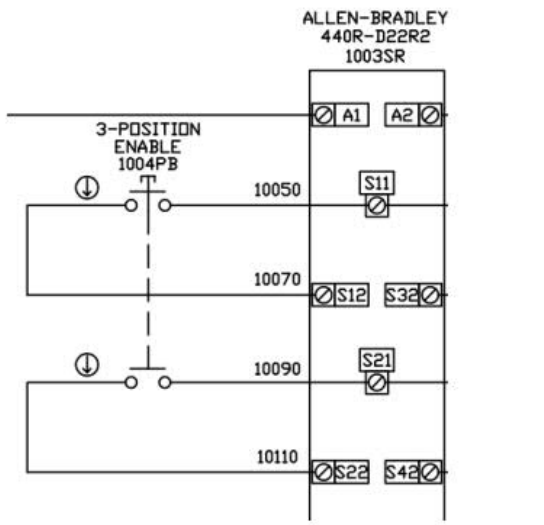


Figure 3.17.4 Enable Device Safety Inputs

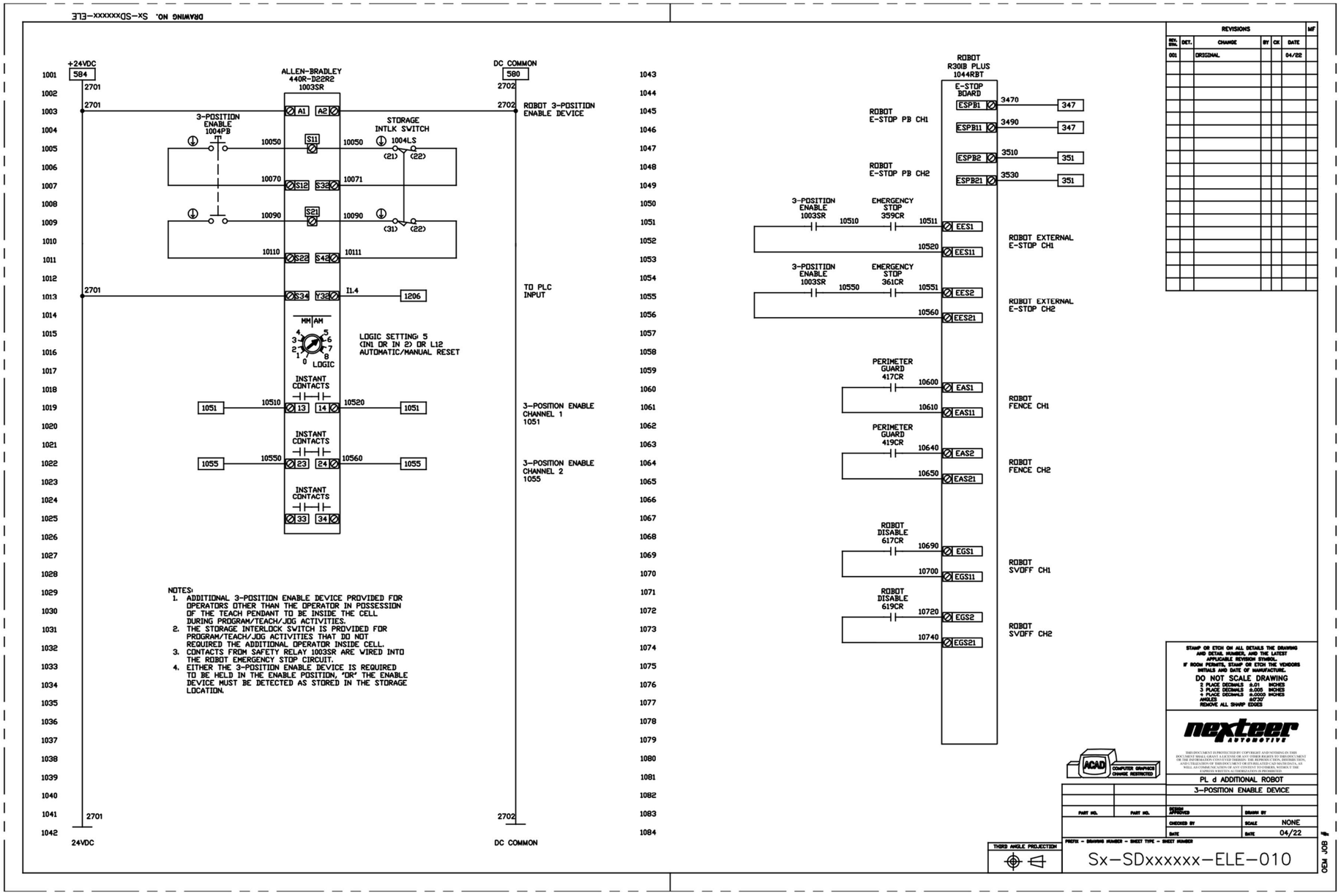


Figure 3.17.4 Example PL d Safety Circuit: Additional Robot 3-Position Enable Device

3.17.5 A teach mode selection circuit, when provided on robotic cells that have multiple robots within the same safeguarded area, shall comply to the following.

1. The teach mode selection circuit shall be implemented at a minimum of PL d.
2. PLC logic shall create a Robot Immediate Stop condition in the event T1 mode is selected and the robot is not concurrently selected by the teach mode selection switch.
3. The teach mode selection circuit shall provide redundant inputs to the Emergency Stop inputs for the robot selected to teach, to bypass the Run All contacts. The Run-All selection enables the Emergency Stop circuit of all robots.
4. The teach mode selection shall allow only one robot to be in teach mode at a time. Example: Run All, Teach Load Robot, and Teach Unload Robot.
5. The teach mode selection switch shall be a maintained selector switch with a position for each robot in the cell and a Run All position.
6. The teach mode selection switch shall be lockable.
7. The Run All position shall enable all robots to run in Automatic.
8. An indication of the teach mode selection shall be provided such as a message on the robot cell's HMI. Example: Run All, Teach Load Robot, and Teach Unload Robot.

Note: The determination for when to include teach mode selection is detailed in SD-1040.

Clarification for item 2: Robots are prohibited by SD-012 and SD-007 from having the ability to be taught in High Speed Teach mode (T2).

Clarification for item 6: The teach mode selection switch shall be capable of being locked with a plant-approved personal lockout lock and not be a keyed-switch.

Clarification: Teach mode selection is separate from the robot controller's local teach feature. Teach modes selection is integrated into the robot local teach feature such that the local teach feature cannot be used while teach mode selection is in Run All.

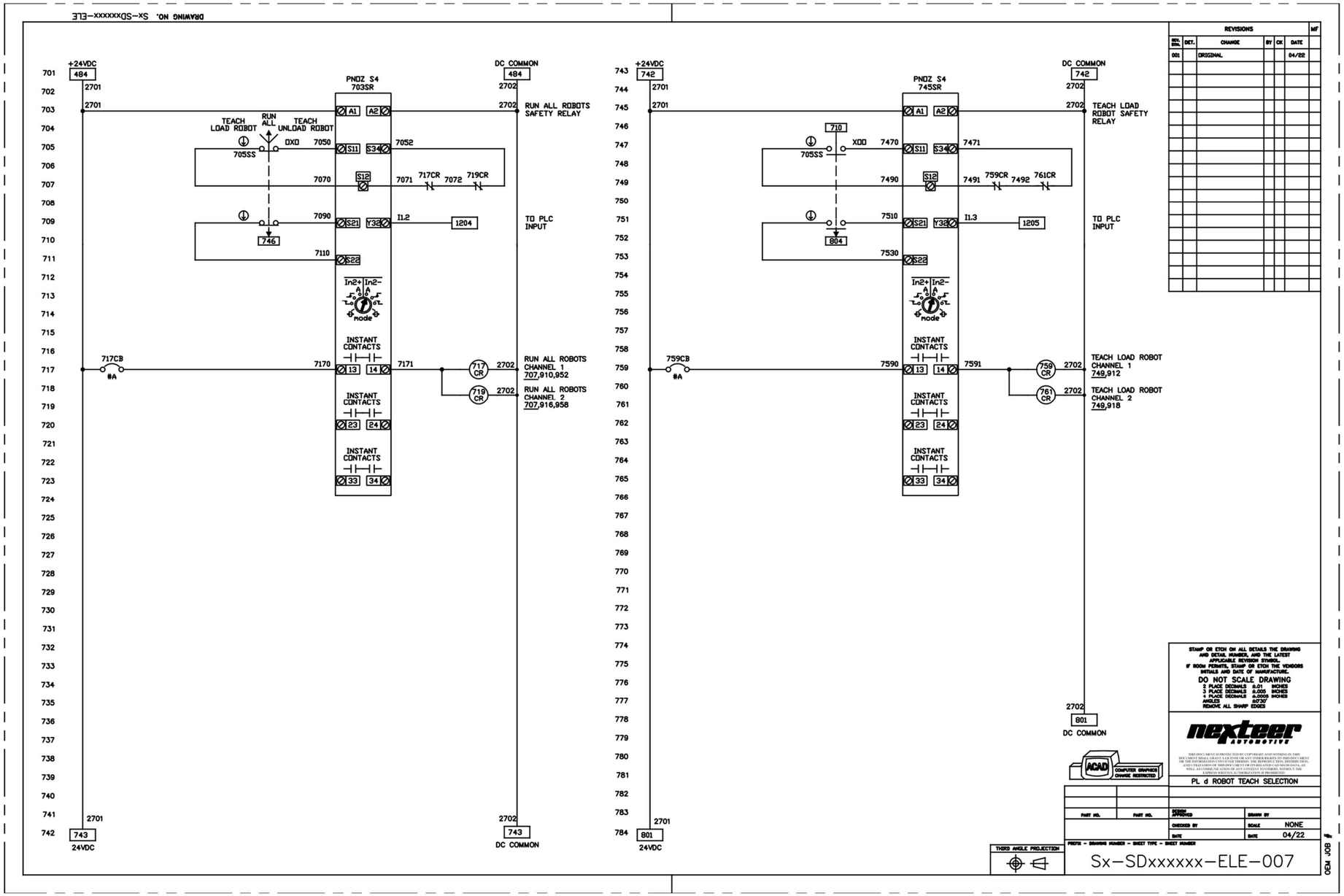


Figure 3.17.5 Example PL d Safety Circuit: Robot Teach Selection Sheet 1 of 3

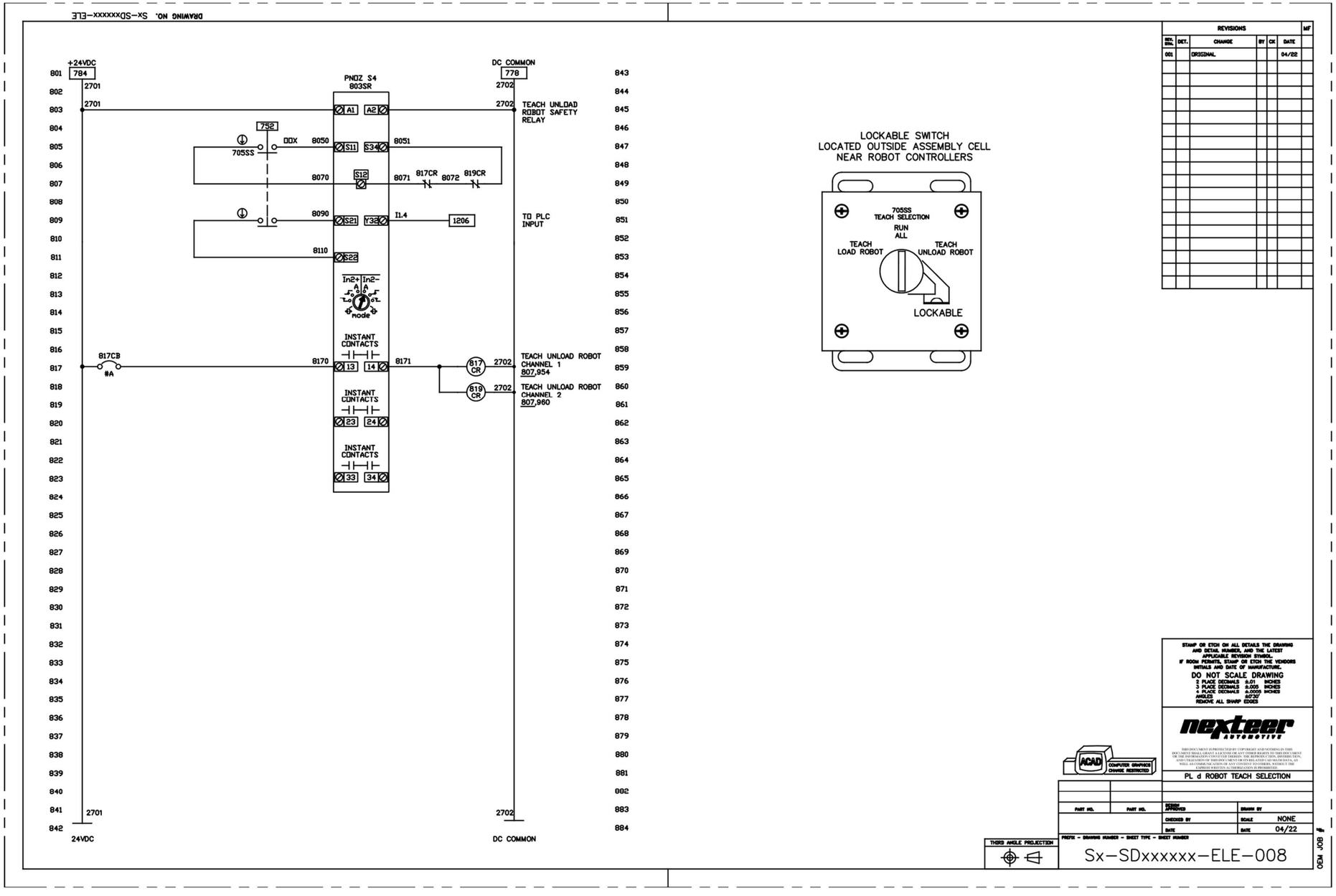


Figure 3.17.5 Example PL d Safety Circuit: Robot Teach Selection Sheet 2 of 3

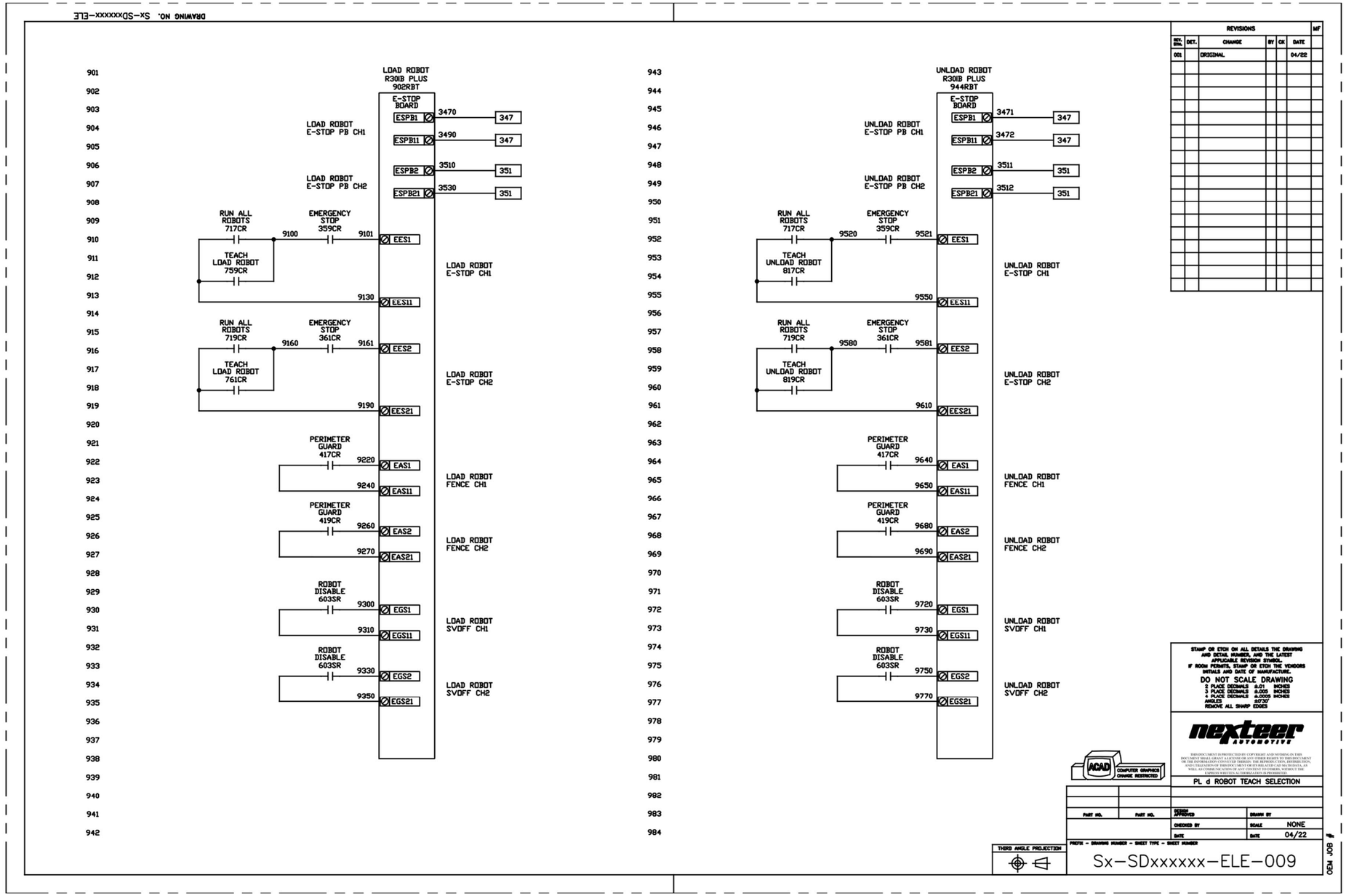


Figure 3.17.5 Example PL d Safety Circuit: Robot Teach Selection Sheet 3 of 3

3.17.6 The Fanuc EE interface connector circuits used for end-of-arm tooling (EOAT) motions are rated PL b. Hazardous EOAT motion circuits requiring PL c or PL d, shall use one of the following solutions:

1. Fanuc EE CRF8 Transit Board(s) (refer to Figure 3.17.6), or
2. Hazardous motion PLC controlled outputs

3.17.7 The positioning of a presence-sensing device used to detect operator entrance into the Shared Workspace from the operator side of a station is required to be located at a distance from the associated hazard(s) such that individuals cannot reach the hazard before cessation of hazardous motion.

Clarification: Since SD-012 requires robot restricted space using DCS (Dual Check Safety) to be configured to limit the robot motions to the normal operating space, the light curtain placement does not have to consider robot motion outside of the normal operating space.

3.17.8 The positioning of a presence-sensing device (such as a light curtain on the robot side of a station) used to detect robot presence within a Shared Workspace is required to be located at a distance from the point of operation such that the robot stops and does not create a severe hazard at the point of operation. Refer to SD-012 and SD-1040 for additional considerations and guidance.

Note: Appropriately configured DCS (Dual Check Safety) can eliminate the robot-side presence sensing device.

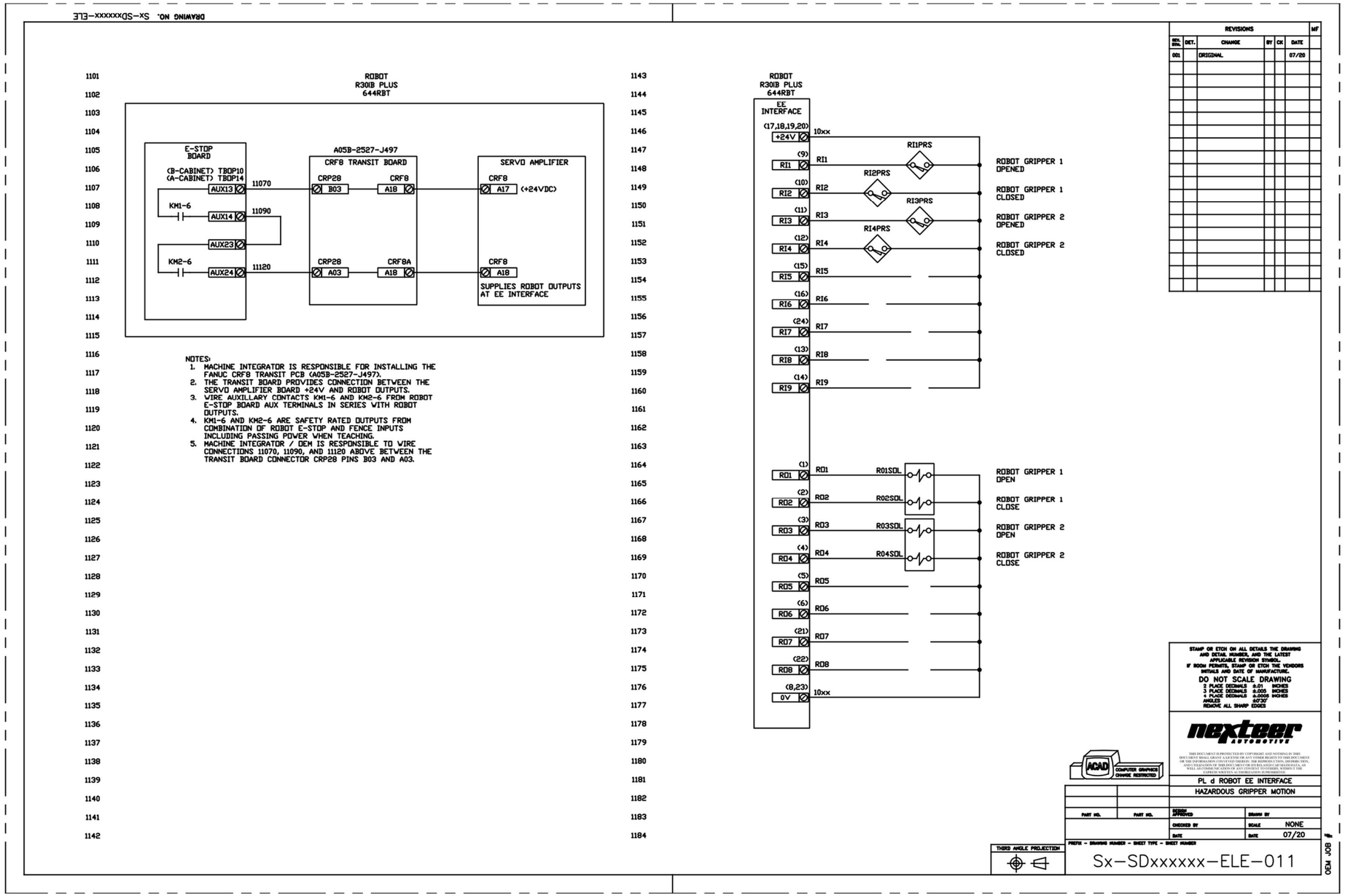


Figure 3.17.6 Example PL d Safety Circuit: End-of-Arm-Tooling EE Interface

3.18 Non-Safety Function Integration into a Safety Circuit

3.18.1 Non-safety parts of a controls system integrated into a safety circuit shall be integrated in such a method as to not lessen the PL rating of the safety circuit.

Example: PLC output-enabled contact that removes power to a pneumatic blocking valve in addition to (in series with) a light curtain safety module outputs and maintains the blocking valve in the OFF state until the next cycle initiation. The PLC output contact typically does not lessen the PL rating of the safety circuit, but instead only adds a non-safety function to the circuit.

3.18.2 Maintaining a pneumatic blocking valve in the OFF state during the machine load/unload is allowed for point-of-operation guard circuit applications. The logic should be designed to maintain the blocking valve OFF immediately after the safety circuit has shut OFF the blocking valve. The logic should allow the safety circuit to re-energize the blocking valve after initiation of the next cycle.

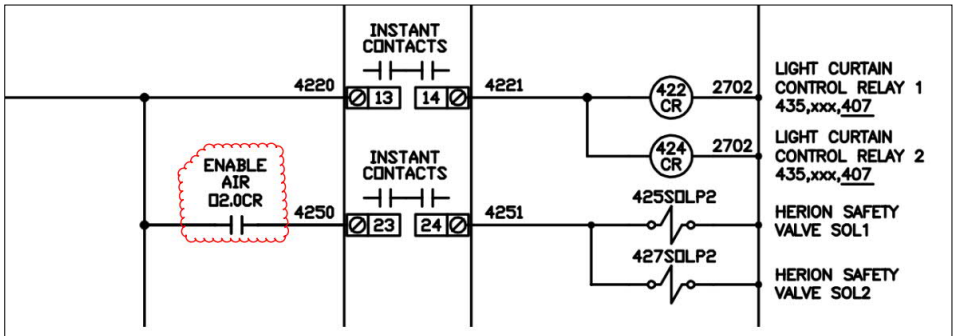


Figure 3.18.2 Non-Safety Function - Maintain Air Off

3.19 Machine Logic (as a consequence of interrupting a safety device)

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

3.19.2 Independent of the safety requirements for the safety circuits, the machine sequence logic should also consider the following:

- Hazards arising from short term 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

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

Note: Additional machine logic requirements for safety circuit device diagnostics are not covered within this document.

3.20 Pneumatic Applications

For pneumatic applications, this pneumatic section takes precedence over any other section of this document.

3.20.1 Piston rods shall be equipped with rod wipers and scrapers to minimize contamination ingression that could impact valve response or cause sticking, or a stuttering type of motion of an actuator.

3.20.2 Exhaust mufflers shall not use a sintered material and shall be sized and plumbed such that they do not restrict the flow rate of the exhaust.

3.20.3 Quick exhausts shall not be used as a means of decreasing stop distance relating to the safeguard placement due to:

1. Failure modes that would go undetected resulting in increased stop distances.
2. The complexity and cost of monitoring these failure modes.

3.20.4 PO (Pilot operated) checks shall only be used on vertical applications and shall only be installed in the lower cylinder line, never both cylinder lines. PO checks shall not be used on other actuator types, such as grippers, for the purpose of maintaining clamping force due to leakage that will eventually lead to a loss of control. Refer to section 3.22.1 for further PO check usage requirements.

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

1. such that the main spool and pilot spools are in the horizontal position. This prevents the effects of gravity from influencing the valves operation and potentially causing motion. Mounting on moving portions of the equipment is not permitted.
2. as close to the actuator(s) as practicable to minimize stop time. Refer to SD-014 for maximum allowable line lengths.

   Exception to item 1 above: Motion valves are permitted to be mounted on a robot shoulder, or in the base, when mounted in the horizontal position.

3.20.6 Motion valves shall be selected based on the motion desired when the electrical command signal is removed. The following are listed in the order of preference.

1. Double solenoid three-position valves with an exhaust center spool configuration shall be used for control of actuators with strokes exceeding 76 mm (3 inches) and for stopping the actuator motion in mid-position by removal of the electrical command signals. Open center valves used on vertical applications will require a PO check circuit in the lower cylinder line as shown in the Nexteer pneumatic templates. Short stroke cylinders, whose home position is normally lowered, may not require the PO check circuit, however, deviation requires Nexteer control engineering approval during the design review.
2. Single solenoid valves are allowed for control of actuators with strokes less than 76 mm (3 inches) when the desired action is a return to the home position on loss of the electrical command signal. Examples for using a single solenoid valve may include:
   - a conveyor stop that engages the pallet upon loss of the electrical command.
   - a robot gripper where the desired motion is to maintain gripping force. Maintaining gripper force may also be accomplished with a gripper with a return spring. The machine risk assessment shall identify hazards associated with removal of power (such as during E-Stop actuation) for single solenoid controlled, or spring return, robot grippers.
3. Double solenoid detented valves are allowed for control of actuators with strokes less than 76 mm (3 inches) when the desired action is to maintain the last commanded position.

   Example applications where detented valves may be acceptable are grippers, shot pins, and clamping applications. Hazards, controlled by detented valves and identified by the machine risk assessment to require PL d, shall be eliminated either by using a mechanical means of guarding such that personnel cannot reach the hazardous motion before the motion stops (moves full stroke), or by removal of energy (and only if removal of power does not create a potential hazard or create an undesired process condition).

Mechanical means of eliminating the pinch point can include:

- tooling design such that pinch points are inaccessible (within the tooling)
- tooling design such that the part covers any pinch points
- 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.

Double solenoid detented valves shall not be used for gripper applications where the operator is directly interacting with the grippers at a Frequent (E2) interval as documented on the machine risk assessment and the gap between the gripper tooling and the part are greater than 4 mm (1/6 inch).

4. Blocked center valves shall not be used. Blocked center valves can create stored energy on both sides of the actuator which could cause a movement creating a potential for injury should one of the sides have a leak. The spools could also leak internally which could also cause unintended motion.

3.20.7 For all pneumatic circuits, 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's SD-007 is one method of meeting this ISO classification.

3.20.8 In addition to the requirements listed above, PL a, PL b, and PL c pneumatic safety circuit requirements are each met by the removal of electrical power to the motion valves (listed above) and per the electrical requirements of Section 2 for PL a, or PL b, or PL c respectively.

3.20.9 In addition to the requirements listed above, PL d pneumatic safety circuits require the removal of electrical power to the motion valves per the electrical requirements of Section 2 for PL d, plus the requirements of the remainder of this pneumatic applications section.

3.20.10 Engineered controls safeguarding solutions identified by the machine risk assessment to require PL d require a blocking valve used in conjunction with the motion valves.

Note: A single safety rated blocking valve may be used in place of a standard blocking valve and output device feedback circuits.

3.20.11 The blocking valve is not required when all the following conditions are met:

1. The risk reduction method is guard locking preventing personnel from opening an interlocked guard until the hazards cease, or fixed guarding is used that requires the use of a tool to remove, and
2. Manual motions require the guard locking door to be locked closed or the fixed guarding to be in place and secured, and
3. The motion valves cannot initiate hazardous motion without being given an electrical command.

3.20.12 The blocking valve shall:

1. Exhaust when in the electrically de-energized state.
2. Include feedback circuitry meeting the feedback requirements in Section 3.5.
3. Include diagnostic input to the PLC.
4. Be mounted according to the manufacturer's recommendations and as close to the motion valves as possible to minimize stop time by reducing restrictions and minimizing line volumes. Refer to SD-012 Annex A for a method to calculate an estimated safe distance.

Clarification for item 2: A safety rated blocking valve does not require feedback circuits.

3.20.13 Nexteer prohibits engineered controls solutions as the safeguarding solution for applications that require PL e. For reference only, in addition to the requirements above, PL e circuits require the use of a blocking valve selected from the Safety Valve section of Nexteer's SD-007.

3.21 Hydraulic Applications

For hydraulic applications, this hydraulic section takes precedence over any other section of this document.

3.21.1 Piston rods shall be equipped with rod wipers and scrapers wherever possible to minimize contamination ingression that could impact valve response or cause sticking, or a stuttering type of motion of an actuator.

3.21.2 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 shall not have more than 35 kPa (5 PSI) cracking pressure.

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

1. Such that the main spool and pilot spools are in the horizontal position. This prevents the effects of gravity from influencing the valves operation and potentially causing motion. Mounting on moving portions of the equipment is not permitted.
2. As close to the actuator(s) as practicable to maximize the exchange of oil within the actuator during each cycle. Refer to SD-013 for exchange rate requirements.

3.21.4 Motion valves shall be selected based on the motion desired upon the loss of the electrical command signal. The following are listed in the order of preference.

1. Double solenoid three-position valves with exhaust (float) center spool configuration shall be used for control of actuators with strokes exceeding 76 mm (3 inches) and for stopping the actuator motion in mid-position by removal of electrical command signals. Exhaust (float) center valves used on vertical applications require a counterbalance valve in the lower cylinder line as shown in the Example PL d Safety Circuits hydraulic circuit within section 2.3.
2. Single solenoid valves are allowed for control of actuators with strokes less than 76 mm (3 inches), when the desired action is a return to the home position. Examples for using a single solenoid valve may include a shot pin that engages the tooling to maintain position upon loss of the electrical command.
3. Double solenoid detented valves are discouraged. Double solenoid detented valves are allowed for control of actuators with strokes less than 76 mm (3 inches) when the desired action is to maintain the last commanded position such as some clamp applications. Hazards controlled by detented valves and identified by the machine risk assessment to require PL d, shall be eliminated such that personnel cannot enter the hazardous motion before it stops.

   Mechanical means of eliminating the pinch point can include:

   - tooling design such that pinch points are inaccessible (within the tooling)
   - tooling design such that the part covers any pinch points
   - the addition of a fixed guard located at the pinch point
4. Blocked center valves shall not be used. Blocked center valves can cause motion due to the internal leakage from P to both A and B within the valve.

3.21.5 In addition to the requirements listed above, PL a and PL b hydraulic safety circuit requirements are met by the removal of electrical power to the motion valves (listed above) and per the electrical requirements of Section 2 for PL a and PL b.

3.21.6 In addition to the requirements above, PL c hydraulic safety circuit requirements are met by the removal of electrical power to the motion valves per the electrical requirements of Section 2 for PL c.

3.21.7 For PL c hydraulic safety circuits, system filtration shall be provided such that the oil quality meets ISO 4406 requirements based on the table below.

3.21.8 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).

Valves:	System Pressure		
	< 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.

3.21.9 In addition to the requirements above, PL d hydraulic safety circuits require the removal of electrical power to the motion valves per the electrical requirements of Section 2 for PL d, plus the requirements of the remainder of this hydraulic applications section.

3.21.10 Engineered controls safeguarding solutions identified by the machine risk assessment to require PL d require a blocking valve used in conjunction with the motion valves.

Note: A single safety rated blocking valve may be used in place of a standard blocking valve and output device feedback circuits.

3.21.11 The blocking valve is not required when all the following conditions are met:

1. The risk reduction method is guard locking preventing personnel from opening an interlocked guard until the hazards cease, or fixed guarding is used that requires the use of a tool to remove, and
2. Manual motions require the guard locking door to be locked closed or the fixed guarding to be in place and secured, and
3. The motion valves cannot initiate hazardous motion without being given an electrical command.

3.21.12 The blocking valve shall:

1. Block the hazardous energy supply when in the electrically de-energized state.
2. Include feedback circuitry meeting the feedback requirements in Section 3.5.
3. Include hardwired feedback (monitoring) into the safety circuit.
4. Be mounted according to the manufacturer's recommendations and as close to the motion valves as possible to minimize stop time by reducing restrictions and minimizing line volumes. Refer to SD-012 Annex A for a method to calculate an estimated safe distance.

Clarification for item 2: A safety rated blocking valve does not require feedback circuits.

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

3.22 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 counterbalance weights have not been provided. 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, PO check valves (pneumatics), counterbalance valves (hydraulics), rod locks, or rail brakes, may be required to stop or hold suspended vertical loads if mechanical devices such as shot pins or counterbalance weights have not been provided.

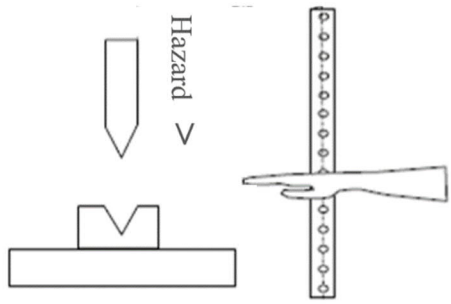


Figure 3.22 – Suspended vertical load

3.22.1 Fluid power circuits for suspended vertical loads shall include PO check valves or counterbalance valves that meet the following requirements:

1. Pneumatic PO checks and hydraulic counterbalance valves shall be installed as close to the actuator's lower port as possible. The conductors between the lower actuator port and the check or counterbalance shall be steel or hard piped.
2. Pneumatic PO checks require a meter-out flow control to be installed between the PO check and the actuator.
3. Pneumatic PO checks shall be installed between the meter-in flow control and the actuator.
4. Pneumatic PO checks that do not automatically vent their downstream pressure on a loss of the incoming supply require additional provisions, such as a manual override, 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 checks shall be documented on the lockout placard.
5. Hydraulic counterbalance valves shall include an internal relief function set 300 PSI above that required to suspend the load.
6. Hydraulic counterbalance valves shall include a manual means of relieving the trapped pressure.

   Note: Some counterbalance valves are provided with a manual override.
7. Hydraulic PO checks shall not be used on single rod cylinders where intensification could exceed the rating of the circuit 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 counterbalance valve which has an internal relief valve.

3.22.2 Fluid power circuits for suspended vertical loads greater than 16 kg (35 pounds) and the Machine Risk Assessment indicates Frequent exposure (E2), shall include one of the following secondary load holding devices:

1. Rod lock supporting an up-acting vertical cylinder.
2. Rail brake attached to the tooling.
3. Counterbalance weight.

Clarification: Suspended vertical loads where the Machine Risk Assessment indicates Infrequent exposure (E1) and a secondary load holding device is not provided, the task and related suspended load hazard should be documented by a Standard Work Instruction (SWI).

3.22.3 Rod locks and rail brakes shall:

1. Be rated for dynamic stopping.
2. Be applied per manufacturer's recommendations and sized appropriately.
3. Include a PO check valve in the actuator circuit for pneumatic applications, meeting the requirements of Section 3.22.1. 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.
4. Pneumatic systems shall include a quick exhaust valve mounted between the rod lock and the motion control valve. The quick exhaust valve shall be installed as close as possible to the rod lock.
5. Be monitored in both the feedback circuit of the safety module and the PLC by one of the following methods.
   - A motion valve spool position sensor.
   - Pressure switch installed between the motion valve and rod lock or rail brake.
   - Brake with internal position sensor.

   Exception: The rod lock or rail brake may be monitored by the PLC only, if the brake is used for process control and is not safety related.

3.22.4 Shot pins may be used for infrequent exposure (E1) applications and shall:

1. Directly engage the tooling.
2. Be sized appropriately.
3. Include a PO check valve in the actuator circuit for pneumatic applications, meeting the requirements of Section 3.22.1. This PO check provides control of the load during the transition period between the release of the shot-pin and energization of the motion control valve. The actuator shall be in the raised position prior to release of the shot-pin.
4. Be monitored by advanced and retracted shot-pin position sensors that directly monitor the shot-pin position. The use of integral sensors that monitor cylinder piston position are not permitted.

   Clarification: The shot pin position shall be monitored by the PLC at a minimum. Applications where the shot pin is the primary safeguarding means the shot pin engaged position shall be monitored with a safety rated device integrated into the safety circuit meeting the required PL rating as documented on the machine risk assessment.

3.22.5 Gon tippers are vertical load applications that require the following:

1. Velocity fuses installed as close as possible to the actuator's port that supports the suspended vertical load.
2. Rigid conductors between the velocity fuse and the actuator port.

   Note: Velocity fuses are required to prevent a hose whipping hazard and rapid lowering of the gon caused by a ruptured hose.

3.23 Electrical Drives

3.23.1 The interconnection of safety circuits to and from electrical drives (such as servo or variable-frequency) shall be implement per device literature to meet or exceed the performance level indicated from the risk reduction method identified by the machine risk assessment.

Note: Most drive literature includes use of STO (safe torque off) connections for safety circuits.

3.23.2 Electrical drive safety interconnection circuits should consider the following:

- STO (or equivalent) should only be applied after the axis has been stopped (typically by removal of a hardwired or logic Enable) and the brake has engaged (typically a time-delay)

Note 1: SD-004 details Nexteer stop category requirements.

Note 2: The quickest stop time typically includes the immediate removal of an Enable signal and a delayed removal of STO signals (a Stop Category 1). Refer to example PL d safety circuit in section 2.3.

3.23.3 Electrical drive interconnection circuits should also consider the following:

- CRM or Master Power connections
- E-Stop connections
- Stop time based on either immediate removal of power (Stop Category 0) or a controlled stop with delayed removal of power (Stop Category 1)

Note 1: SD-004 details Nexteer stop category requirements.

Note 2: The quickest stop time typically includes the immediate removal of an Enable signal and a delayed removal of STO signals. Refer to example PL d safety circuit in section 2.3.

3.23.4 Electrical drive safety circuits implemented Stop Category 1 for the risk reduction method shall also be implemented Stop Category 1 for Emergency stop and Master stop.

A. SD-010, Standard Equipment Specification

A.1 General

Specification SD-010 defines Nexteer requirements for the quotation and purchase of supplier standard machine(s) including lathes, machining centers, CNC hobbs, and grinders.

SD-010 includes the safety-related requirement that the machinery being purchased must comply with SD-011. As such, SD-011 in its entirety applies to SD-010 machinery.

This annex provides clarifications, exceptions, and deviations from the main body of SD-011 for SD-010 machinery. This annex shall be used **in-conjunction with** the main body of SD-011.

A.2 Section 2.2 – PL c Requirements

The PL c requirements listed within section 2.2 can be modified as follows:

- Single channel circuitry is required. Category 2 circuit structure is recommended however, Category 1 circuit structure is allowed where the supplier provides documentation demonstrating a $MTTF_D$ = high for the circuitry.
- Input devices are allowed to be Type 2 ESPE rated devices. Type 4 ESPE rated devices are preferred.
- Input devices are allowed to be Category 1 rated technology where the supplier provides documentation demonstrating a $MTTF_D$ = high for the circuitry. Category 2 rated technology is preferred.
- Safety modules are allowed to be Category 1 rated (including an industrial control relay) where the supplier provides documentation demonstrating a $MTTF_D$ = high for the circuitry. Category 2 rated safety modules are preferred.
- Electronic components such as a servo are allowed to be applied at Category 1 where the supplier provides documentation demonstrating a $MTTF_D$ = high. It is preferred that electronic components such as a servo are rated and applied at PL c or Category 2.

A.3 Section 2.3 – PL d Requirements

Note: Section 3.6 details the requirements for compliance to PL d without using Category 3 circuit structure.

A.4 Section 3.1 – Safety module power

It is recommended, but not required, that safety modules be enabled when the machine disconnect is ON.

A.5 Section 3.2 – Safety module inputs

The safety input diagnostic requirements of 3.2.2 are recommended.

A.6 Section 3.7.1 – E-Stop circuit performance level

E-Stop circuit performance level shall be implemented at a minimum PL c. It is recommended, but not required, that the E-Stop circuit performance level meet the PL level for each task-hazard primary safeguard as documented on the machine risk assessment. E-Stop circuits on robot applications require a minimum PL d.

A.7 Section 3.7.6 – E-Stop inputs

E-stop devices shall provide, as a minimum, a single contact input to the safety circuit.

A.8 Section 3.7.7 – E-Stop devices in series

It is recommended that a maximum of five E-Stop devices are wired in series to safety module inputs for PL d circuit performance applications.

Note: ISO 14119 provides guidance on fault masking and how many E-Stop devices to allow in series based on the number of frequently used devices.

A.9 Section 3.7.8 – E-Stop safety modules

It is preferred that E-stop devices be connected directly to a dedicated E-Stop safety module. The E-Stop devices are allowed to be connected to a safety module that performs multiple functions (such as combined E-stop and Door Closed safety functions) however the E-Stop function shall not have a means of being bypassed.

A.10 Section 3.8.3 – Safety interlock switches in series

It is recommended that a maximum of five mechanical safety interlock switches be wired in series to safety module inputs for PL d circuit performance applications.

Note: ISO 14119 provides guidance on fault masking and how many switches to allow in series based on the number of frequently used guards.

A.11 Section 3.8.6 – Safety interlock switch location

It is recommended that safety interlock switches be located and mounted to prevent damage and to minimize tampering. They should be installed in accordance with the instructions provided by the device manufacturer. They should not be easily defeated with readily available tools, objects, or by tying down the actuators.

Note: ISO 14119 provides many details pertaining to device selection and mounting.

A.12 Section 3.9.2 – Guard locking safety interlock switch closed and locked position sensing

Closed and locked position safety contacts (outputs) shall be connected into a safety module for risk reduction methods identified by the machine risk assessment that indicate guard locking for the safety of personnel. Locked position safety contacts (outputs) should be connected into a safety module when guard locking is indicated for process protection only, while the closed position contacts remain a shall.

A.13 Section 3.9.7 – Guard locking safety interlock switch lock position sensing

Lock position sensing should be connected to the machine control system for diagnostics and process control.

A.14 Section 3.10.1 – Light curtains

For PL c applications light curtains are allowed to be a Type 2 ESPE device; Type 4 ESPE devices are preferred.

A.15 Section 3.10.2 – Light curtains

Risk reduction methods identified by the machine risk assessment to require PL c, the light curtain shall include (at a minimum):

1. an output as a single channel input to a safety module, or
2. an output to a single industrial control relay with feedback to the light curtain external device monitoring terminals.

Note: Some light curtains have an embedded safety module, or safety-rated relay output contacts, designed to the appropriate PL or category such that the machine hazards may be driven directly from the embedded relay contacts.

Risk reduction methods identified by the machine risk assessment to require PL d, the light curtain shall include (at a minimum):

3. an output as a single channel input to a safety module (when minimum rated PL d), or
4. dual output to an appropriately rated safety module, or
5. two outputs to two industrial control relays with mechanically-linked contacts including feedback to the light curtain external device monitoring terminals. Refer to Figure A.13 below.

Note: Some light curtains have an embedded safety module, or safety-rated relay output contacts, designed to the appropriate PL such that the machine hazards may be driven directly from the embedded relay contacts. The light curtain embedded safety module also includes appropriate external device monitoring (feedback terminals).

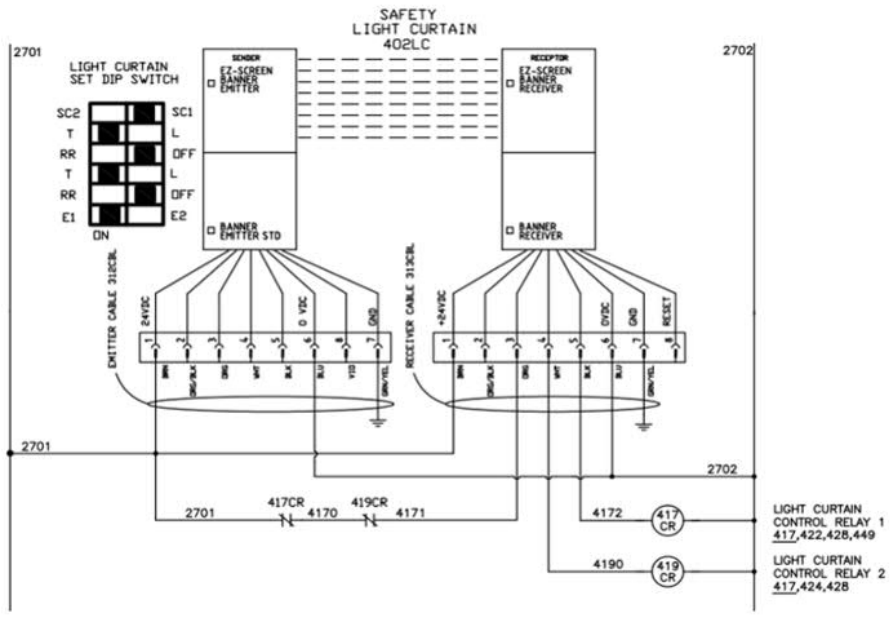


Figure A.15 Light Curtain at PL d Feeding Industrial Relays

A.16 Section 3.13 through 16 – Bypassed and muted safety circuits, and Two-hand control

These sections detail the principle that bypassing any safeguard circuit requires a safety circuit of equal or greater performance level. Most typical, for commodity CNC machines, these requirements and the result of the machine risk assessment will identify that bypassing a guard door safety circuit with CNC-controlled two-hand jog to be implemented PL d. (The result of the machine risk assessment will typically identify the guard door safety circuits on the CNC to require PL d.)

Use of Fanuc CNC Dual-Check safety function, or Siemens SINUMARIK Safety Integrated systems, is strongly recommended.

A.17 Section 3.23.3 – Electrical drives Stop Category 1

It is strongly recommended that electrical drive safety circuits implemented Stop Category 1 for the risk reduction method also be implemented Stop Category 1 for Emergency stop and Master stop.

B. References

ANSI B11.19: Performance Criteria for Safeguarding: 2010 and 2019

ANSI B11.TR6:2010: Technical Report for Machine Tools – Safety Control Systems for machine Tools: 2010

ANSI RIA 15.06: Industrial Robots and Robot Systems - Safety Requirements: 2012

IEC 60947-5-1: Low-voltage switchgear and controlgear – Part 5-1: Control circuit devices and switching elements – Electromechanical control circuit devices: Edition 3-2014

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: Edition 2.0-2013

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 1.2-2016

IEC 61496-1: Safety of machinery – Electro-sensitive protective equipment – Part 1: General requirements and tests: Edition 2.0b-2012

IEC 61496-2: Safety of machinery – Electro-sensitive protective equipment – Part 2: Particular requirements for equipment using active opto-electronic protective devices: Edition 3.0b-2013

IEC 62061: Safety of machinery - Functional safety of safety-related electrical, electronic and programmable electronic control systems: 2005 and 2015

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: 2001and 2010

ISO 10218-1: Robots and Robotic Devices - Safety Requirements for Industrial Robots – Part 1: Robots: 2011

ISO 10218-2: Robots and Robotic Devices - Safety Requirements for Industrial Robots – Part 2: Robot Systems and Integration: 2011

ISO 13849-1: Safety of machinery – Safety-related parts of control systems – Part 1: General principles for design: Third edition 2015-12-15

ISO 13849-2: Safety of machinery – Safety-related parts of control systems – Part 2: Validation: Second edition 2012-10-15

ISO 13855: Safety of machinery – The positioning of protective equipment in respect of approach speeds of parts of the human body: 2015

ISO 14119: Safety of machinery - Interlocking devices associated with guards - Principles for design and selection: 2013

NFPA 79: Electrical Standard for Industrial Machinery: 2018

SD-000: Nexteer Automotive Machinery and Equipment Specification

SD-004: Nexteer Automotive Electrical Specifications for Industrial Machinery - Addendum to IEC 60204-1

SD-007: Nexteer Automotive Approved Components List

SD-010: Nexteer Automotive Standard Equipment Specification

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

SD-013: Nexteer Automotive Hydraulic Fluid Power – General rules and safety requirements for systems and their components – Addendum to ISO 4413

SD-014: Nexteer Automotive Pneumatic Fluid Power – General rules and safety requirements for systems and their components – Addendum to ISO 4414

SD-1032: Nexteer Automotive Programmable Logic Controller Application Specification

SD-1040: Nexteer Automotive Fanuc Robot Specification

Note: To obtain a copy of Nexteer specifications, visit our vendor document website www.nexteerdataexchange.com under Vendor Documents. To obtain a copy of any other referenced specification, they can be purchased typically from the originating organization or at other industry specification websites.

C. Glossary

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

C.2 **AOPD:** An acronym used in place of Active Optoelectronic Protective Device (Example: light barrier) by select ISO standards. For ease and consistency, the acronym ESPE has been used throughout this document.

C.3 **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 modules requiring the transition of the reset input before the relay will reset.

C.4 **B_{10D}:** Number of cycles until 10% of the components fail dangerously (for pneumatic and electromechanical components). (ISO 13849-1:2015)

C.5 **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.

C.6 **bypass (also bypass, bypassing):** To render ineffective one or more safety-related function of the control system or safeguarding device. (ANSI B11.19:2010)

C.7 **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 13849-1:2015) The term category has been used in this document as a simple replacement for circuit structure category.

C.8 **diagnostic coverage, average (DC_{AVG}):** Diagnostic coverage is the 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. Diagnostic coverage can exist for the whole or parts of a safety-related system, for example inputs, logic, and/or outputs. DC_{AVG} is the average diagnostic coverage for the whole safety-related part of the controls system. (ISO 13849-1:2015 adapted)

C.9 **EN:** An acronym used as part of a standards publication number; in this case a European Normative standard.

C.10 **enabling device:** A manually operated control device which, when continuously activated and used in conjunction with a separate actuating control, will allow the machine to function. See live man switch. (ANSI B11.19:2010)

C.11 **emergency access:** A means to release the guard locking to make it possible to reach **into** the danger area in a machine quickly in an emergency. Emergency access is not a safety function. (ISO 14119:2013 adapted) Also called Emergency release.

C.12 **escape release**: A means to release manually, without aids, the guard locking from inside the safeguarded area to leave the area. Escape release is not a safety function. (ISO 14119:2013 adapted)

C.13 **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 and/or a safety-related data interface. (IEC 61496-1:2012)

C.14 **exposure:** One of three input factors to the machine risk assessment process, documenting frequency and/or exposure to a hazard for each task-hazard combination as either frequent or infrequent.

C.15 **external device monitoring:** A means by which an ESPE monitors the state of control devices which are external to the ESPE. See feedback. (IEC 61496-1:2012)

C.16 **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 13849-1:2015). For ease and consistency, the term feedback has been used throughout this document.

C.17 **feedback contact:** The control signal from an output device indicating the performance of its switching function. Typical signals include mechanically-linked contacts, spool position sensors, or fluid power pressure sensors.

C.18 **feedback terminals:** The input terminals on safety modules, or external device monitoring terminals on ESPEs, for connection of the output device feedback contacts to accomplish the feedback function.

C.19 **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, it removes power to the hazard. (IEC 61496-1:2012 adapted) The term *output* has been used in this document to include all output devices in series from the safety circuit logic device up to and including the final switching device.

C.20 **guard locking:** The complete application of the device intended to lock a guard in the closed position and linked to the control system, the associated controls system, and the interlocked guard door. (ISO 14119:2013 adapted).

C.21 **IEC:** An acronym used as part of a standards publication number; in this case an International Electrotechnical Commission standard.

C.22 **ISO:** An acronym used as part of a standards publication number; in this case an International Organization of Standards document.

C.23 **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.

C.24 **intrusion distance (C):** distance that a part of the body (usually a hand) can move past the safeguard towards the hazard zone prior to actuation of the safeguard.

C.25 **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.

C.26 **locking interlock switch:** A device used to connect a guard with the control system and intended to lock the guard in the closed position.

C.27 **machine 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 13849-1:2015, adapted) The Nexteer machine risk assessment process is detailed in Nexteer's Design-In Health and Safety Specification.

C.28 **mean time to dangerous failure ($MTTF_D$):** Expectation of the time to dangerous failure. (IEC 62061:2005, 3.2.34, modified) A portion of the overall reliability of components.

C.29 **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, direct opening action, direct mechanical action, mechanically guided, and positive guided. (force guided: ANSI TR6: draft)

C.30 **monitoring:** See feedback.

C.31 **muting:** The temporary automatic suspension of a safety function(s) by the safety circuit. (ISO 13849-1:2015)

C.32 **NFPA:** An acronym used as part of a standards publication number; in this case a National Fire Protection Association standard.

C.33 **output device fault:** A faulted condition where the state of a safety circuit output device did not deenergize when the safety logic has commanded a deenergized state.

C.34 **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.

C.35 **PL:** An acronym used in place of performance level. Performance level is used to specify the ability of safety-related parts of control systems to perform a safety function under foreseeable conditions. (ISO 13849-1:2015). For ease and consistency, the acronym PL is used throughout this document.

C.36 **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 device 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.

C.37 **positive opening contacts:** Use of rigid mechanical linkage between the limit switch actuator and contact element. Alternative terms include direct opening action and direct mechanical action.

C.38 **power-OFF to release:** Upon switching OFF the power to the guard locking release device the release device opens (typically by a spring). The guard locking device is also typically moved to the "locked" position upon application of power. This type of locking interlock switch typically does not accomplish safety function and might be used for common process-control (non-safety) applications at Nexteer.

C.39 **power-ON to release:** Upon switching ON of the power to the guard locking release device the release device opens. The guard locking device is also typically moved to the "locked" position (typically by a spring) on the removal of the power. This type of locking interlock switch accomplishes a safety function and is occasional used on Nexteer applications.

C.40 **presence-sensing device initiation (PSDI):** Operating mode of initiating a single cycle (indirectly) by a presence-sensing device. When the presence-sensing device senses that work motions of the operator (related to feeding or removing parts) are completed and all parts of the operator's body are withdrawn from the sensing field of the device, the cycle may be initiated. (ANSI B11.19:2010, adapted)

C.41 **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 79:2018)

C.42 **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 module, dual outputs from a safety module, and dual output devices. All requirements for redundancy are detailed within the specification.

C.43 **risk assessment:** See machine risk assessment.

C.44 **robot (industrial robot):** Automatically controlled, reprogrammable multipurpose manipulator, programmable in three or more axes, which can be either fixed in place or mobile for use in industrial automation applications. The industrial robot includes: the manipulator, including actuators, the controller, teach pendant, any communication interface (hardware and software), and any integrated additional axes. The following devices are also considered industrial robots for the purpose of this standard: hand-guided robots, the manipulating portions of mobile robots, collaborating robots. (ISO 10218-1:2011 and ANSI RIA 15.06-2012 harmonized, adapted)

C.45 **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 13849-1:2015) For ease and consistency the term safety circuit has been used throughout this document.

C.46 **safety circuit:** See SRP/CS.

C.47 **input, safety circuit:** A typical safety circuit consists of the input device(s), logic device(s), and output device(s) as shown in the simplified safety-rated block diagram below. Safety circuit inputs can vary depending on the required circuit performance level to include sensors, proximity switches, safety interlock switches, two-hand enable devices, ESPEs, or other. For ease and consistency Nexteer uses the term input throughout this specifically unless a specific input device is detailed.

C.48 **logic, safety circuit:** A typical safety circuit consists of the input device(s), logic device(s), and output device(s) as shown in the simplified safety-rated block diagram above. Safety circuit logic can vary depending on the required circuit performance level to include industrial control relays, safety modules, safety PLCs, can be part of the input device, or other. For ease and consistency Nexteer uses the term logic throughout this specifically unless a specific logic device is detailed.

C.49 **output, safety circuit:** A typical safety circuit consists of the input device(s), logic device(s), and output device(s) as shown in the simplified safety-rated block diagram above. Safety circuit outputs can vary depending on the required circuit performance level to include industrial control relays, electrical power contactors, fluid power motion valves, fluid power blocking valves, safety valves, can be part of the logic device, or other. For ease and consistency Nexteer uses the term output throughout this specifically unless a specific output device is detailed.

C.50 **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. The reset can be manual or automatic. The required status switch provides diagnostics that 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.

C.51 **safety gate:** See interlocked guard door.

C.52 **safety interlock switch:** A device used to connect a guard with the control system.

C.53 **safety mat:** Note: Current Nexteer production systems do not include the use of safety mats. Use of safety mats requires Nexteer control engineering approval.

C.54 **safety-rated:** Specifically designed and category-rated for use in safety circuits adhering to applicable standards for machine safety.

C.55 **safety module:** 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 module has been used throughout this document.

C.56 **shared workspace:** As applied to a robot application, the space or work area the robot reaches during normal automatic operation. It is also the space or work area that, at a different time, individuals can access as part of the normal production operation (SD-012).

C.57 **short-circuit-detection:** Detection of shorted inputs within the safety module's dual input channels, typically accomplished by use of one 0vdc and one 24vdc input channel. Also accomplished by use of a safety module 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.

C.58 **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.

C.59 **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. The weight of suspended vertical loads includes tooling, fixtures, fluid power cylinder rods, and other machine components.

C.60 **teach mode selection:** A robot cell control function, added to a cell that has multiple robots within the same guarded area, provided to ensure a type of lockout for all but one robot in teach. Teach mode selection is not the local teach feature typically provided within the robot manufacturer's robot controller.

C.61 **two-hand control relay:** A safety module 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.

C.62 **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. Requirements for a Type 2 ESPE can be found in IEC 61496-1.

C.63 **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. Type 4 ESPE requirements can be found in IEC 61496-1.

RECORD OF REVISIONS

Revision No	Date	Section	Description
001	06NO09	ALL	Original Approval and Issue Date
002	18DE13	3.9	Added PSDI applications section, renumbered all subsequent sections.
003	27SE22	ALL	Rewrite to align with SD-012 update and use of PL (per ISO 13849).
004			
005			
006			
007			
008			
009			
010			
011			
012			
013			
014			
015			
016			
017			
018			
019			
020			