DELPHI

Specification for the Application of Safety Circuits

DA-2001

Revision 3.0

February 2007

DELPHI COMMITTEE ON THE
SPECIFICATION for the APPLICATION of SAFETY CIRCUITS

Michael Appold	- Delphi Steering, Saginaw, MI
Chris Bacon	- Delphi Steering, Saginaw, MI
Tony E Keller	- Delphi Electronics & Safety, Kokomo, IN
Wayne Coon	- Delphi Thermal Systems, Dayton, OH
Thomas J. Kiihr Jr.	- Delphi Thermal Systems, Troy, MI
John Klimowicz	- Delphi Powertrain Systems, Flint, MI
Dirk Malencia	- Delphi Electrical/Electronic Architecture, Warren, OH
Larry Morel	- Delphi Steering, Saginaw, MI
Eric Watson	- Delphi Powertrain Systems, Juarez, Mexico

Forward questions and /or comments to Delphi Controls Engineering COE members.

Table of Contents

Foreword

This *Specification for the Application of Safety Circuits* is issued by Delphi Corporation. The specification's intent is to provide Delphi plants with safe, well-designed, reliable and productive safety circuits for industrial machinery and equipment.

The specification was developed by the Delphi Controls Engineering COE with assistance from Delphi subject matter experts. The mission of the committee was to develop a specification based on national / international standards, and Delphi corporate / divisional / plant specifications to:

- enhance safety.
- simplify and clarify those standards and specifications in order for machinery and equipment builders to comply at minimum cost.
- encourage the implementation of safety circuit technology across Delphi plants.
- improve equipment reliability and maintainability.
- reduce the size and complexity of common divisional and plant specifications.
- support lean manufacturing equipment.
- support design-in safety practices.

The example circuits in the specification are based on currently available technology consistent with United States consensus standards and the international standard ISO 13849-1 (EN 954-1). The specification is not intended to inhibit new technology. As an example, some of the example circuits in the specification are based on the use of redundant-input safety relays that could be replaced by other control-reliable technology. Consequently, Delphi expects and encourages all industrial equipment builders to notify the purchasing division of any situation which, in their opinion, inhibits the application of new technology. This approach allows new technology proposals to be evaluated as to their merit.

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

Controls Engineering Center of Expertise (COE)

This specification was developed as a "how to" document in support of the Delphi "*Design-In Health and Safety Specification*" and is to be used by Delphi Manufacturing Engineers as a specification for Manufacturing Equipment Design. The **Lean Vision** created for the development of the *Design-In Health and Safety Specification*, was used as guiding principal in the development of this document as well.

> Least complicated machine, process and safety system that protects all personnel from injury and illness.
>
> The intent is to use a common method and consistent implementation worldwide to prevent occupational injuries and illnesses while simplifying equipment. This shall be accomplished by using a risk assessment analysis to identify equipment and process hazards. The "Hierarchy of Health and Safety Controls" shall be followed to eliminate exposure to these hazards. The ultimate goal is to support the operator.

The Controls Engineering COE supports this *Specification for the Application of Safety Circuits* as a Lean Manufacturing initiative because it results in reduced costs, increased customer satisfaction and our being a stronger company; while at the same time ensuring a safe work environment for our people. We expect you to use it as you design safety circuits for machinery and equipment.

John Klimowicz Delphi Powertrain Systems	Date 3/22/07	Tony E. Keller Delphi Electronics & Safety	Date 3/22/07
Dirk Malencia Delphi Electrical/Electronic Architecturec	Date 3/22/07	Larry Morel Delphi Steering	Date 3/22/07
Tom Kiihr Delphi Thermal & Interior	Date 3/22/07		

1 Scope and purpose

1.1 Scope

1.1.1 The specification addresses the use of safety circuits as applied to equipment safeguarding, (e.g., safety gate circuits, light curtains, safety mats, and two-hand control). Determining the proper level of circuit performance to be applied to an equipment safeguard is defined as a result of conducting a risk assessment for the equipment/process. The Delphi *Design-In Health and Safety Specification* details the Delphi risk assessment process, including who conducts this risk assessment. The Delphi *Design-In Health and Safety Specification* also defines different levels of circuit performance requirements for safety circuits. For North American sites these levels are (reference section 5.1 of this specification):

- Simple
- Single Channel
- Single Channel with Monitoring
- Control Reliable safety circuits.

For international sites that follow ISO 13849-1 (EN 954-1), refer to definitions as outlined in Annex E. Note that the circuit performance columns in Annex E indicate that either implementation is acceptable globally.

Proper implementation methodology for each circuit performance level is described in this specification and will hereafter be referred to as "applying the appropriate safety circuit".

1.1.2 Emergency stop devices and circuits fall into the scope and purpose of this specification. Emergency stop devices and e-stop relays are typically provided in addition to the machine's safeguarding systems (e.g., electrical interlocked gate guards or two hand control systems implemented through use of safety relays).

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

1.2 Purpose

1.2.1 This specification provides manufacturing engineers, control engineers, synchronous workshops and equipment suppliers, with direction on the consistent implementation of safety devices and circuits at all Delphi plant sites. This specification is to be used in conjunction with, and as referenced by, the Delphi *Design-In Health and Safety Specification* as a "how to" methodology for proper design and implementation of safeguarding circuits for equipment.

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

1.2.3 The use of safety circuits as applied to safeguarding does not replace well-established machine lockout/tagout procedures currently in place. In addition, the use of safety circuits as applied to safeguarding does not replace well-established controls lockout solutions procedures. The term controls lockout solutions refers to a hazardous energy control system used on rare and specific equipment/processes. The intent of a controls lockout solution is to provide a Control Reliable safety system for personnel to enter a work cell or work on equipment when it is not practical to follow machine lockout/tagout procedures (e.g., robotics cell).

1.2.4 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. Some items covered are required by law and others are needed to have a common system approach.

1.2.5 The use of the word “shall” indicates requirements and the use of the word “should” indicates recommendations.

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

1.2.7 Figures in the main section of the document use ANSI symbols and the IEC version is in Annex F. When using the electronic version of this document, by clicking on the figure number you go directly to the IEC version and return by clicking on Return.

The ANSI symbol version of sample electrical/pneumatic circuits are in Annex C and the IEC version is in Annex G. Pneumatic and Hydraulic circuits use ISO symbols. The IEC version of the electrical circuits in Annex D are in Annex H.

2 Normative references

2.1 ANSI B11.1, *Mechanical Power Presses*

2.2 ANSI B11.19, *Safeguarding When Referenced by the Other B11 Machine Tool Safety Standards*

2.3 ANSI B11.20, *Manufacturing Systems/Cells*.

2.4 ANSI B11.TR4, *ANSI Technical Report for Machine Tools – Selection of Programmable Electronic Systems (PES/PLC) When Applied to Machine Tools.*

2.5 Federal Register 1910-147, 1910-211 (Subpart O of 1910)

2.6 OSHA 1910.212

2.7 NFPA 79, *Electrical Standards for Industrial Machinery*

2.8 DA-2004, Delphi Corporation *Electrical Specification for Industrial Machinery*

2.9 DA-2006, Delphi Corporation *Design-In Health and Safety Specification*

2.10 EN-954-1, *Safety Related Parts of Control Systems*

2.11 EN 999, *Safety of Machinery - The positioning of protective equipment in respect of approach speeds of parts of the human body***.**

2.12 EN 1760, *Safety of Machinery - Pressure sensitive protective devices,* Part 1 safety of machinery pressure sensitive safety devices mats and floor. Part 2 safety of machinery pressure sensitive safety devices edges and bars.

2.13 EN 1088, *Safety of machinery – interlocking devices associated with guards – principals for design and selection.*

2.14 IEC 60204-1, *Electrical Equipment of Industrial Machines – General Requirements*

2.15 IEC 60947-5-1, *Electromechanical control circuit devices.*

2.16 IEC 60947-5-3, *Particular requirements for proximity devices with fault prevention measures or defined behavior under fault conditions.*

2.17 IEC-60947-5-5, *Low-voltage switchgear and control gear* – Part 5: Control circuit devices and switching elements – Part 5: Electrical emergency stop device with mechanical latching function.

2.18 IEC 61496, *Safety of Machinery - Electro-sensitive Protective Equipment*

2.19 ISO 13849-1, *Safety of Machinery – Safety-related parts of control systems* – Part 1: General principles for design.

2.20 ISO 13856-1, *Safety of machinery – pressure sensitive protective devices,* Part 1 General principles for design and testing of pressure sensitive mats and pressure sensitive floors.

3 Definitions

3.1 **bypass:** To render ineffective any safety related function of the control system or safeguarding device (ANSI B11.19).

3.2 **category 0 stop:** Stopping by immediate removal of power (including fluid power) to the machine actuators (i.e., an uncontrolled stop) (NFPA 79, IEC 60204)

3.3 **category 1 stop:** A controlled stop with power to the machine actuators available to achieve the stop and then removal of power (including fluid power) when the stop is achieved (NFPA 79, IEC 60204)

3.4 **electrical interlock:** An arrangement that interconnects guard(s) or device(s) with the control system and/or all or part of the electrical energy distributed to the machine.

3.5 **emergency stop relay:** A relay that enables power to hazardous devices.

3.6 **failure to danger:** A failure which prevents or delays all output signal switching devices going to and/or remaining in the OFF-state in response to a condition which, in normal operation, would result in their so doing (IEC - 61496-1).

3.7 **interlocked barrier guard:** A barrier, or section of a barrier, interlocked with the [machine] control system to prevent inadvertent access to the hazard during normal [machine] operation.

3.8 **muting:** The automatic temporary bypassing of any safety related function(s) of the control system or safeguarding device. (ANSI B11.19)

3.9 **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. The guard is not typically interrupted each cycle of the machine. Typical perimeter guards include movable barrier devices such as electrical interlocked doors or gates, or presence-sensing devices such as light curtains and safety mats.

3.10 **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. The operator normally trips the point-of-operation guard during each cycle of the machine. Typical point-of-operation guards include movable barrier devices such as interlocked doors or gates, presence-sensing devices such as light curtains and safety mats, or two-hand control devices.

3.11 **positive-guided relay/contactor:** Relay designed to eliminate any springing of the contacts to ensure a true making and breaking of contacts, and in the case of a failure, to ensure that a minimum clearance of 0.5 mm between the open contacts is maintained. These relays are sometimes called guided-contact, captive-contact, direct-drive, force-guided-contact or forced-contact relays.

3.12 **positive-opening contacts:** The achievement of contact separation as a direct result of a specified movement of the switch actuator through non-resilient members (i.e., not dependent upon springs).

3.13 **presence-sensing device (PSD):** A device that creates a sensing field, area or plane to detect the presence of an individual.

3.14 **safety circuit performance:** Levels of safety circuit performance have been identified to accommodate the risk reduction categories as determined by the risk assessment per the Delphi *Design-In Health and Safety Specification*. Four levels have been identified for North American sites which are Simple, Single Channel, Single Channel with Monitoring and Control Reliable. For all other sites, refer to definitions as outlined in Annex E. The circuit performance column in Annex E indicate that either implementation is acceptable globally.

3.15 **safety device:** Device (other than a guard) that eliminates or reduces risk, alone or associated with a guard.

3.16 **safety gate:** See interlocked barrier guard.

3.17 **safety interlock switch:** Mechanical switch used to interlock a safety gate with the control system.

3.18 **safety rated device**: A device specifically designed and rated for use in safety circuits adhering to applicable national and international standards for machine safety.

3.19 **safety relay:** A Single Channel with Monitoring or dual channel relay designed for use in a safety circuit.

3.20 **two-hand control relay:** A safety relay specifically manufactured for two-hand control applications. This relay typically does not have an internal reset function. This relay requires simultaneous actuation of the two inputs within a fixed time of each other, typically 500 milliseconds.

3.21 **two-hand control, type 1:** The provision of two control devices and their concurrent actuation by both hands; continuous concurrent actuation during the hazardous condition; and machine operation shall cease upon the release of either one or both of the control devices when hazardous conditions are still present (IEC 60204).

3.22 **two-hand control, type 2:** A type 1 control requiring the release of both control devices before machine operation is allowed to be reinitiated. (IEC 60204)

3.23 **two-hand control, type 3:** A type 2 control requiring concurrent actuation of the control devices as follows: it shall be necessary to actuate the control devices within a certain time limit of each other, not exceeding 500 milliseconds; where this time limit is exceeded, both control devices shall be released before operation may be reinitiated. (IEC 60204)

Note: The requirements outlined in NFPA 79 for two-hand control are consistent with IEC 60204 type 3.

3.24 **Type 2 ESPE device**: Shall have a means of periodic performance test to reveal a failure to danger. For a Type 2 ESPE (Electro-Sensitive Protective Element) device, a single fault affecting normal operation shall be detected immediately, or as a result of the next performance test of the device, or on actuation of the sensing function of the device and shall result in the initiation of a lockout condition within the ESPE (IEC - 61496-1).

Note: This use of the term “lockout” is not to be confused with machine lockout/tagout. Here industry typically refers to the output state of the ESPE being forced off.

3.25 **Type 4 ESPE device**: Shall provide a means for continual monitoring of performance testing to reveal a failure to danger. For a Type 4 ESPE device, a single fault affecting normal operation shall be detected immediately within the response time and shall result in the initiation of a lockout condition within the ESPE (IEC - 61496-1).

Note: This use of the term "lockout" is not to be confused with machine lockout/tagout. Here industry typically refers to the output state of the ESPE being forced off.

4 Safety rated device requirements

Section 4 is for safety rated devices only, which are required for Single Channel with Monitoring safety circuit and Control Reliable safety circuit applications.

4.1 Safety relays

4.1.1 Single Channel with Monitoring safety relays shall have a Single Channel input for use with electrical interlock switches and emergency stop buttons. They shall have a self-monitoring function that will result in a safe mode if a power failure or safety critical internal fault occurs to the safety relay. These relays shall have a contactor monitoring capability and should have an auxiliary contact for indication purposes.

4.1.2 Dual Channel safety relays (e.g., Control Reliable) shall have two inputs with short circuit detection, output relays with positive-guided contacts, and internal crosschecking of all relays. These safety relays shall generate a stop signal even if only one input is opened or a short is detected across the inputs. These relays shall have a contactor monitoring capability and should have an auxiliary contact for indication purposes.

Note: When the input circuit's short circuit detection is provided by the input device (i.e., solid state outputs from selected light curtains), the safety relay does not require additional short circuit detection.

4.1.3 When a reset device is required for a Single Channel with Monitoring circuit or Control Reliable circuit, the reset function shall be implemented such that the hazardous motions cannot be reinitiated by a reset device being tied-down.

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

4.2 Safety interlock switches

4.2.1 These switches shall have positive-opening contacts. They shall not be easily defeated with ordinary hand tools or by tying down the actuators. For Single Channel with Monitoring safety circuit applications, the electrical interlock shall consist of a single switch with one contact that is normally closed when in a safe state. For Control Reliable safety circuit applications, the electrical interlock shall consist of a single switch with two contacts that are normally closed when in a safe state, or two switches with one normally closed contact each. These switches shall comply with EN1088, IEC60947-5-1, and IEC60947-5-3.

Note: Plugs with a minimum of four connection points can be considered a mechanical switch with two positive-opening contacts.

4.3 Pushbuttons

4.3.1 Safety rated emergency stop pushbuttons for Single Channel with Monitoring and Control Reliable safety circuit applications shall have normally closed (1 for Single Channel with Monitoring, 2 for Control Reliable) positive-opening contact(s). For Control Reliable applications, emergency stop pushbuttons with removable contact blocks shall have the two contacts on separate contact blocks. These shall be installed such that if one contact block is loose the other contact block still operates. The pushbutton shall be red mushroom, 40 mm minimum diameter, with detent, requiring manual reset after actuation. E-stop buttons shall comply with IEC 60947-5-5.

4.3.2 Two-hand control pushbuttons shall meet all of the requirements in ANSI B11.19 for two-hand control devices. When using electronic pushbuttons, they shall be designed for use in a safety circuit and shall be immune to RFI or other types of electrical interference.

4.4 Cable-operated emergency stop switches

4.4.1 Safety rated cable-operated emergency stop switches for Single Channel with Monitoring and Control Reliable safety circuit applications shall have normally closed (1 for Single Channel, 2 for Control Reliable) positive-opening contact(s) that are opened both when the cable is pulled or when the cable goes slack. The switch contacts shall latch in the open position until the switch is manually reset. Cable-operated E-stop switches shall comply with IEC 60947-5-5.

4.5 Safety mats

4.5.1 Safety mats shall be suitable for use in an industrial environment and shall meet all of the requirements in ANSI B11.19 for safety mat devices.

Note: ANSI requirements include mounting per the safe distance formula. Reference Annex B.

4.5.2 Safety mats shall be certified (designed and tested) to EN 1760-1 and EN 954-1.

4.5.3 All safety mats shall be provided with a means for fixed permanent location.

4.5.4 Safety mats shall be conductive type, fiber-optic type, or tactile-sensitive type.

4.5.5 For conductive mats, a 4-wire normally open configuration shall be used.

4.6 Light curtains

4.6.1 Light curtains shall be certified in compliance with IEC-61496-1 part 1 and IEC-61496-2 part 2 (light curtains certified to the obsolete British standard BS 6491 parts I and II are acceptable for reuse)**.** For Control Reliable applications, use a type 4 ESPE. For Single Channel with Monitoring applications, type 2 or type 4 ESPE are acceptable.

4.6.2 Light curtain applications shall meet all of the requirements in ANSI B11.19 for presence-sensing devices

Note: ANSI requirements include mounting per the safe distance formula. Reference Annex B.

4.6.3 Light curtains shall include operational status indicators integral to either the sender or the receiver, or both.

Note: Including this indication at the sender / receiver unit facilitates periodic operator testing as recommended by the manufacturer, Annex A of this specification, or other operations' requirements.

5 Safety Circuits and Safety Device Application

5.1 Circuit performance. Four levels of safety circuit performance have been identified to accommodate the risk reduction categories as determined by the risk assessment per the Delphi *Design-In Health and Safety Specification*. These circuit performances include Simple, Single Channel, Single Channel with Monitoring, and Control Reliable.

5.1.1 **"Simple" safety circuit:** Simple safety circuits are designed and constructed using accepted single channel circuitry and may be programmable. Reference pages C1 and C2 in Annex C.

5.1.2 **"Single Channel" safety circuit:** Single Channel safety circuits are hardware based and are used in compliance with the manufacturers' recommended proven circuit designs (e.g., a single channel electro-mechanical positive-break device and electromechanical positive-guided relay which signals a stop in a de-energized state). Reference pages C3 and C4 in Annex C.

5.1.3 **"Single Channel with Monitoring" safety circuit**: Single Channel with Monitoring safety circuits include the requirements for Single Channel, are safety rated, and checked (preferably automatically) at suitable intervals. Reference pages C5 and C6 in Annex C.

a. The check of the safety function(s) shall be performed:
   1) At the machine start up
   2) Periodically during operation
b. The check shall either:
   1) Allow operation if no faults have been detected, or
   2) Generate a stop signal if a fault is detected. A warning shall be provided if a hazard remains after cessation of motion
c. The check itself shall not cause a hazardous situation
d. Following the detection of a fault, a safe state shall be maintained until the fault is cleared.

5.1.4 **"Control Reliable" safety circuit:** Control Reliable safety circuits are designed, constructed and applied such that any single component failure does not prevent the stopping action of the equipment and/or process. These circuits are hardware based and include automatic monitoring at the system level. Reference pages C7 - C10 in Annex C.

a. The monitoring shall generate a stop signal if a fault is detected. A warning shall be provided if a hazard remains after cessation of motion.
b. Following the detection of a fault, a safe state shall be maintained until the fault is cleared.
c. Common mode failures shall be taken into account when the probability of such a failure occurring is significant.
d. The single fault should be detected at the time of failure. If not practicable, the failure shall be detected at the next demand upon the safety function.

5.2 General requirements for all safety circuits

5.2.1 A safety circuit shall be used to remove power (including fluid power) from hazardous devices for all or a selected part of the machine protected by the safety device(s). A safety circuit shall be implemented using the safety circuit performance corresponding to the risk reduction category as determined by the risk assessment (i.e., the appropriate safety circuit). Figure 5.2.1 illustrates a Single Channel with Monitoring circuit. Reference Annex C for example circuits.

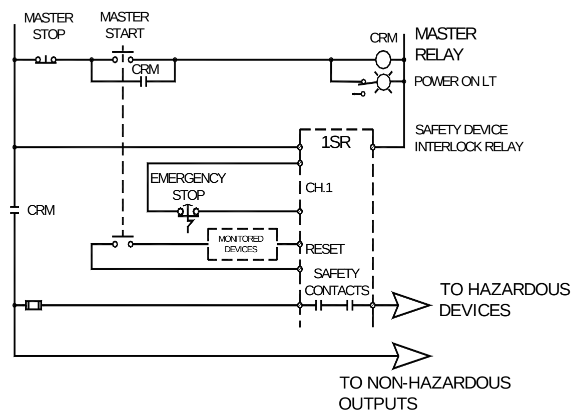


Figure 5.2.1 – Example Safety Circuit

5.2.2 Equipment utilizing safety circuits shall be capable of achieving a safe stop at any point in the cycle by removal of power (including fluid power) from all hazardous devices.

5.2.3 A common approach is to combine the master relay and emergency stop relay (figure 5.2.3). Combining the emergency stop relay and/or safety device circuitry into as few as one relay is also permitted. Combined safety circuits shall meet the most stringent circuit performance requirements as determined by the risk assessment.

Note: With the most common approach being to combine the master and e-stop *relays, illustrations throughout the remainder of this specification will assume that they are combined. The master relay in figure 5.2.1 is optional.*

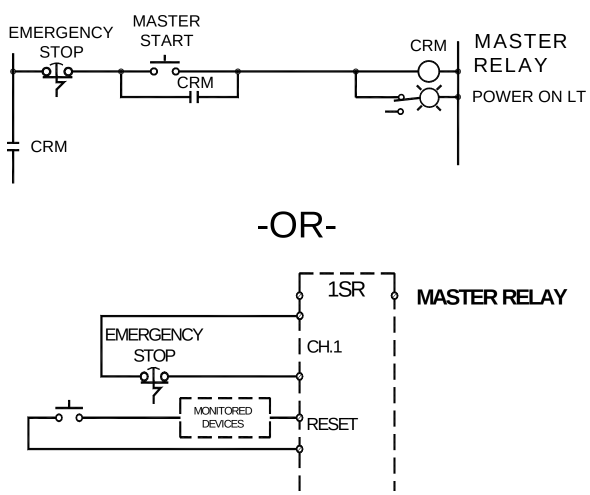


Figure 5.2.3 – Master Relay as a Safety Relay

5.3 Input circuits

5.3.1 Connecting several safety devices in series as inputs to the same safety relay is permitted within the design constraints of the safety relay. Reference figure 5.3.1.

Note: Diagnostics on safety devices shall be done via independent contacts and not with those used in the safety relay string (e.g., a separate contact on the e-stop button or safety device to a PLC).

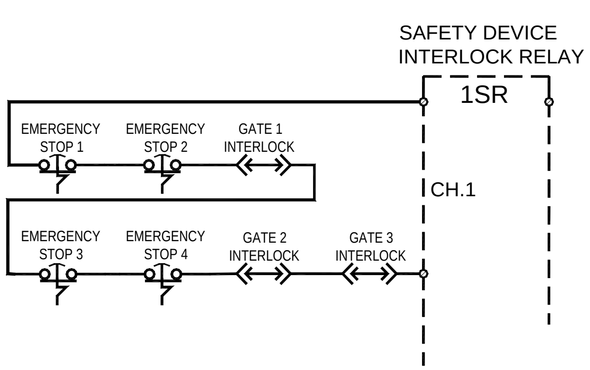


Figure 5.3.1 – Multiple Safety Devices

5.3.2 Some input devices (such as magnetic interlocking switches) require short circuit protection. The manufacturer's recommendation for proper type and size shall be followed.

5.4 Safety Relay Output Circuits

5.4.1 All safety relay output contacts should be protected with a short circuit protective device as specified by the safety relay manufacturer to minimize contact welding. Reference figure 5.4.1.

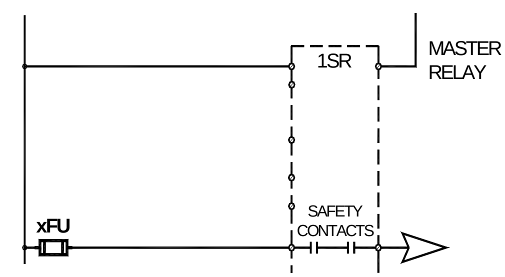


Figure 5.4.1 – Safety Contact Protection

5.4.2 When additional electrical safety circuit contacts are required, such as for current capability or circuit isolation, a positive-guided relay(s) or contactor(s) shall be driven by an output(s) from the primary safety relay. For a Single Channel with Monitoring circuit one relay/contactor shall be used (figure 5.4.2) and for a Control Reliable circuit two relays/contactors shall be used, each powered through a separate safety relay output. To accomplish monitoring requirements, a normally closed contact from each positive-guided output relay shall be used in the safety relay reset or monitoring circuit (reference IEC 60947-5-5).

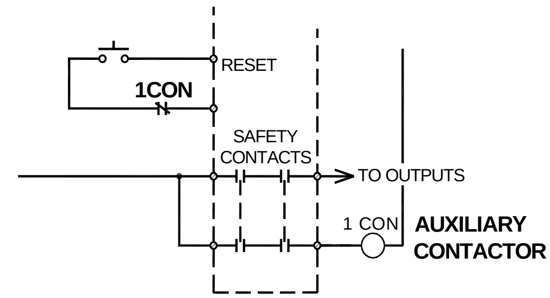


Figure 5.4.2 – Additional Safety Circuit Contacts

5.4.3 For Control Reliable circuits, two contacts, one from each positive guided relay/contactor shall be used in series for each power-feed or hazardous device interconnection from this safety relay output circuitry.

5.4.4 To accomplish the monitoring requirements, a normally closed contact from each positive-guided output relay/contactor shall be used in the safety relay reset or monitoring circuit. Reference figure 5.4.4.

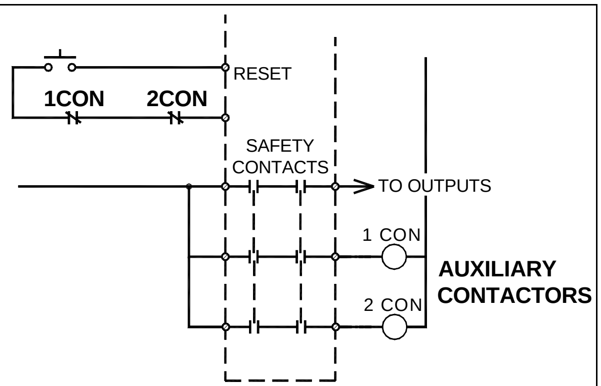


Figure 5.4.4 – Multiple Safety Circuit Contacts

5.4.5 For Single Channel with Monitoring and Control Reliable circuits, output devices that do not have a positive-guided normally closed contact are required to be monitored. The entire monitoring circuit shall be designed to be as fail-to-safe as a directly connected positive-guided normally closed contact.

5.4.5.1 For Single Channel with Monitoring circuits, monitoring shall be accomplished as follows:

- A contact from the device (or sensor in fluid power applications) to be monitored shall drive a positive-guided relay.
- A contact from this positive-guided relay shall be connected in the safety relay reset or monitoring circuit.
- A second contact from this positive-guided relay (opposite state from the above contact) shall be connected in the power-feed line to the machine's hazardous devices.

Refer to annex D, sheet D2.

5.4.5.2 For Control Reliable circuits, monitoring of output devices that do not have a normally closed positive-guided contact shall be accomplished by connecting a contact from each of the devices to be monitored (or sensor in fluid power applications) as separate inputs to a dual channel safety relay. The output of this monitoring relay shall be connected to the safety relay reset or monitoring circuit. An alternate method of monitoring these output devices would be through the use of two (redundant) single channel circuits described in 5.4.5.1 above. Reference figure 5.4.5.2a and b.

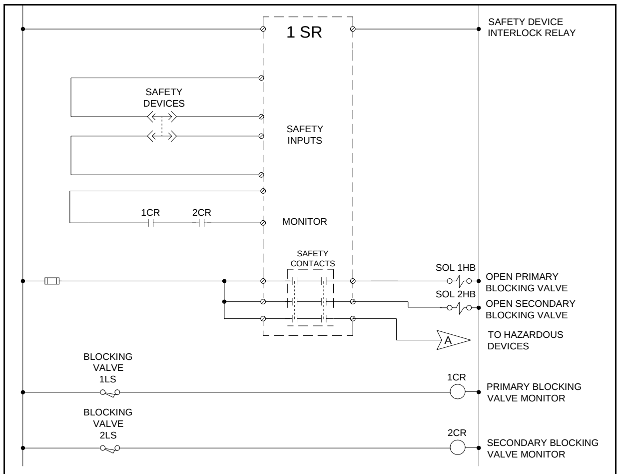


Figure 5.4.5.2a – Monitoring through redundant positive-guided relays

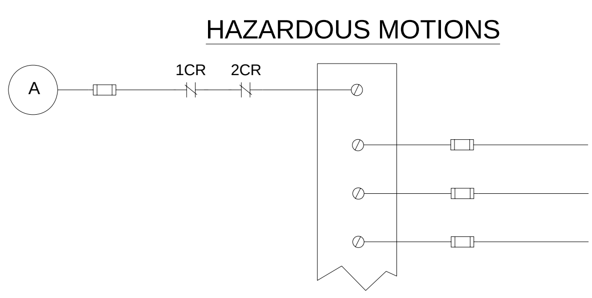


Figure 5.4.5.2b – Required additional fail-to-safe contacts

5.4.6 Any relays used in the output safety circuit shall have transient suppression consistent with the manufacturer's recommendations.

5.4.7 For fluid power output device requirements refer to section 8 of this specification.

5.5 Mute / Bypass safety circuits

5.5.1 A muting circuit used in a safety circuit is, in itself, a safety circuit. The performance of the muting circuit is to be consistent with the safety circuit being muted.

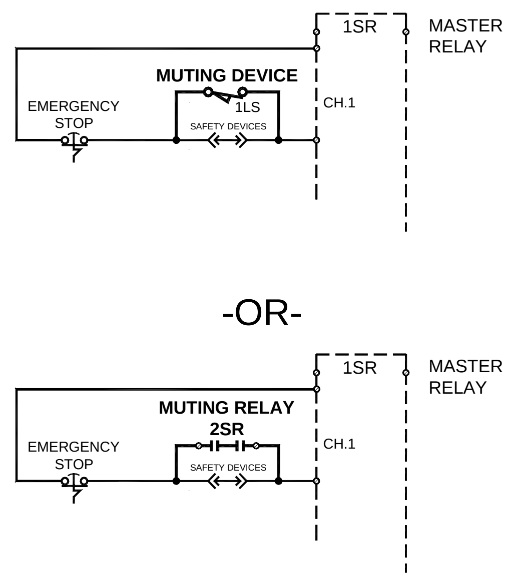


Figure 5.5.1 – Muting a Safety Device

5.5.2 Muting in a safety circuit is permitted during the automatic non-hazardous portion of the machine cycle (e.g., when a powered safety gate is closed, tooling is closed or the robot is in a safe position).

5.5.3 Bypassing a safety circuit is permitted for authorized purposes when alternative safeguards are used. Reference annex I drawing I1.

5.5.3.1 Auto mode shall be inhibited when a safeguard is bypassed.

5.5.3.2 Bypassing a safeguard shall be indicated.

5.5.4 Output contacts from emergency stop relays shall not be muted or bypassed. Emergency stop pushbuttons and cables shall not be muted or bypassed.

5.5.5 For a Single Channel with Monitoring circuit one safety muting device shall be used. Reference figures 5.5.5a and b. For a Control Reliable circuit muting shall consist of one safety muting device with two contacts that are normally closed when in a safe state, or two switches connected as inputs to a muting safety relay. Reference figure 5.5.5b and c.

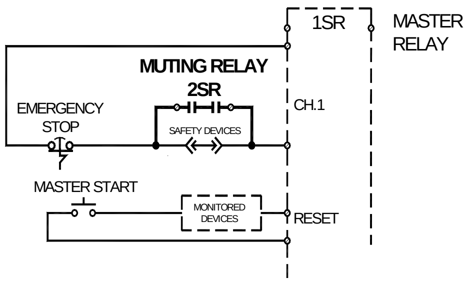


Figure 5.5.5a – Muting a Safety Device with a Safety Relay

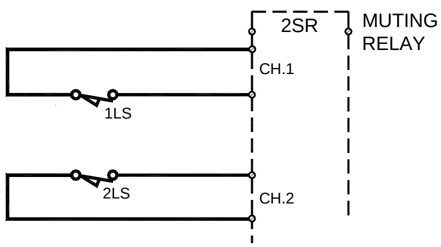


Figure 5.5.5b – Muting Relay

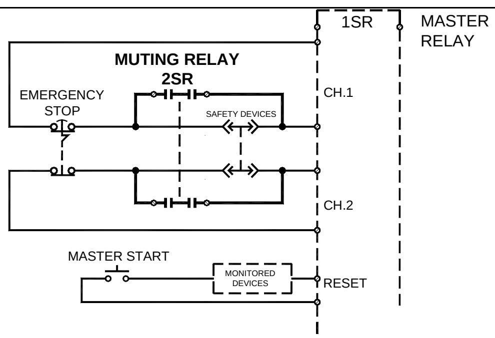


Figure 5.5.5c – Muting a Safety Device in a Control Reliable Circuit

5.5.6 In addition to the hardwired muting circuitry, the PLC is allowed to further control the muting function. Reference figures 5.5.6a thru f. To implement this PLC muting function, two PLC outputs shall be used. Reference figure 5.5.6b. The two PLC outputs shall be controlled by separate inverse rungs of logic; (i.e., "Mute" and "Not Mute"). Reference figure 5.5.6c. For Single Channel with Monitoring and Control Reliable, the two muting PLC outputs shall be connected to a safety relay. Reference figure 5.5.6d thru f.

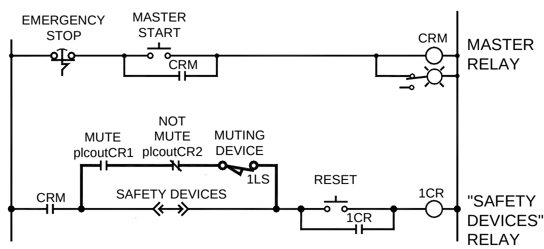


Figure 5.5.6a – Additional PLC Muting – Single Channel

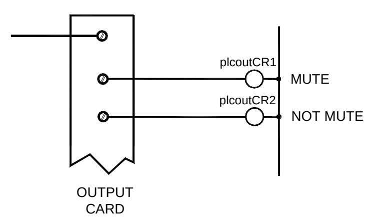


Figure 5.5.6b – PLC Mute Relays

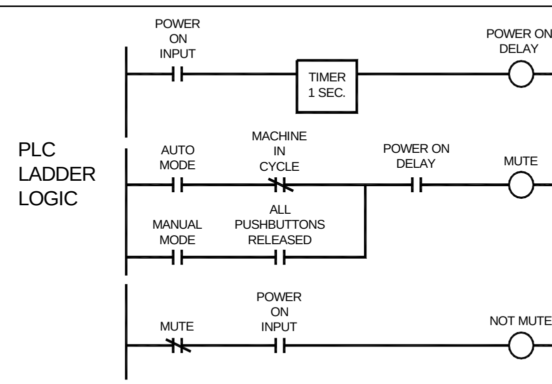


Figure 5.5.6c – PLC Mute Programming

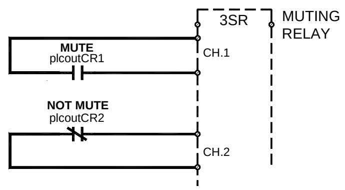


Figure 5.5.6d – PLC-Relays Muting

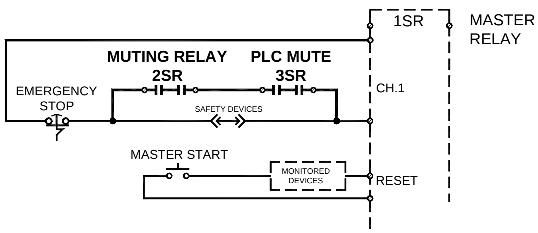


Figure 5.5.6e – Additional PLC Muting – Single Channel With Monitoring

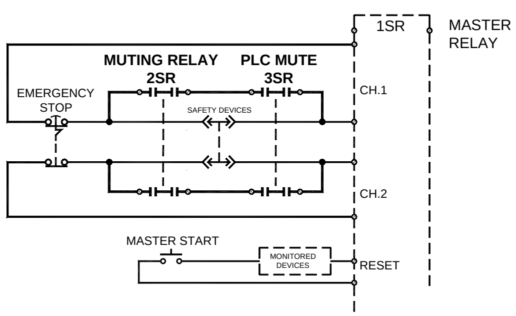


Figure 5.5.6f – Additional PLC Muting – Control Reliable

Safety Relay Application Note: Because of variable input response times on safety relays, additional debounce logic may be needed for PLC outputs such as the "Mute" and "Not Mute". Safety relays may lock-up on quick on-off-on transitions of their inputs where the relay senses one input transition but not the other.

5.6 Manual Operation

5.6.1 If the process requires manual operations with a safety device bypassed (e.g., safety gate open) type 3 two-hand control shall be used and implemented consistent with the circuit performance of the device being bypassed. For Single Channel circuit applications, two-hand control may be programmable. For Single Channel with Monitoring and Control Reliable applications, two-hand control shall be implemented using a dual channel two-hand control safety relay. The bypassing circuit(s) shall be implemented consistent with the muting circuits above. Reference page I1 of Annex I.

5.6.2 If the safeguarding method for automatic cycle is type 3 two-hand control, implemented using a dual channel two-hand control safety relay, special consideration should be given to provide individual manual motion control (as determined by the risk assessment). One of the following methods may by used:

- With the machine in manual mode, select from the operator interface which manual function is to operate. Logic for that motion should be enabled, but hardwired power is still removed as a result of the safety circuit. The motion can then be initiated by applying hardwired power via the two-hand control safety circuit. Or**,**
- With the machine in manual mode, initiate the manual motion by holding a button on the operator interface. Logic for that motion should be enabled and, as long as the motion button is held, logic driving a *Manual Output* relay should be powered. This relay output is connected into one input of the automatic cycle two-hand control safety relay, in parallel with one of the cycle pushbuttons (reference figure 5.6.2). Simultaneous to the manual motion initiation, the hardwired safety circuit can pass power using the other two-hand control safety circuit pushbutton as the "common".

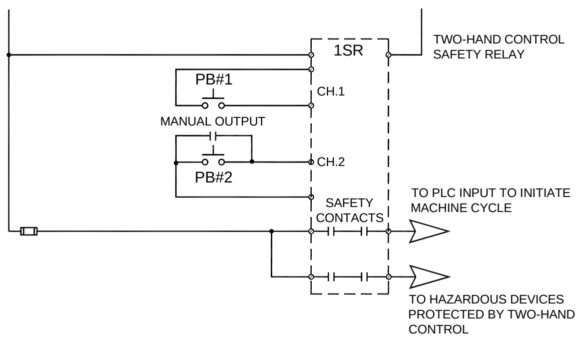


Figure 5.6.2 – Manual Enable for Two Hand Control - Control Reliable

5.7 Emergency stop circuits

5.7.1 The emergency stop circuit shall, as a minimum, be Single Channel when all other hazards have been addressed and documented by the risk assessment. The E-stop relay shall not energize by resetting the device that caused the stoppage or by reapplication of power. Energizing the relay shall only occur by activation of a reset pushbutton. The safety circuit could be the master relay on machines that only have a master relay (figure 5.6.1) or an emergency stop relay for machines that have both a master relay and an emergency stop relay. In the latter case the master relay can be a standard control relay.

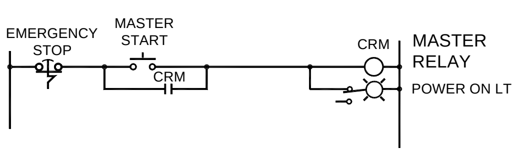


Figure 5.7.1 – Single Channel E-Stop

5.7.2 Combining the emergency stop relay and/or safety device circuitry into as few as one relay is also permitted. Combined safety circuits shall meet the most stringent circuit performance requirements as determined by the risk assessment.

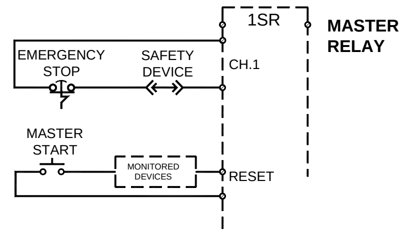


Figure 5.7.2 – E-Stop as part of a Safety Circuit

5.7.3 In Simple, Single Channel and Single Channel with Monitoring applications, the E-stop pushbutton may have one normally closed contact connected to the safety circuit. For Control Reliable applications, the E-stop pushbutton shall have two normally closed contacts (figure 5.6.3) connected to a safety relay.

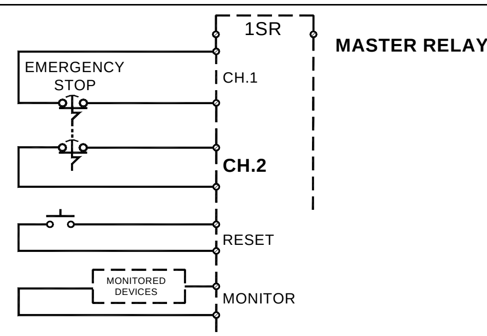


Figure 5.7.3 – Dual/Redundant Contacts

5.7.4 For cable-operated emergency stop switches, single or multiple normally closed contacts shall be connected to the appropriate safety circuit consistent with the requirements of section 5.6.3 of this specification.

5.8 Safety gate switch circuits

5.8.1 Safety interlock switch(es) shall be connected to an appropriate safety circuit.

5.8.2 Safety interlock switch contact requirements shall be the same as in section 5.6.3 of this specification.

5.8.3 Safety interlock switch(es) shall be located and mounted to minimize tampering. Tamper-resistant mounting hardware (typically provided by the manufacturer) shall be used.

5.8.4 Safety interlocks switch(es) shall be installed to ensure that the positive-opening contacts are forced open by operation of the guard.

5.8.5 When using a non-coded magnetic switch, the switch shall be mounted such that it cannot be accessed when the guard door is open. Coded magnetic switches shall be used where the switch is exposed and could be overridden with a magnetic device. Coded magnetic safety switches require the use of a controller.

5.9 Safety mat circuits

5.9.1 Safety mats shall meet the requirements of the circuit performance level for which they are specified.

5.9.2 Safety mats must be installed in accordance with the safe distance formula. Reference Annex B.

5.9.3 The safety mat shall cover the entire distance from the machine hazard to the minimum safety distance (e.g., D_s from safe distance formula).

5.9.4 Where a sensing area is made up of more than one mat the entire mat area shall have no dead zone.

5.9.5 It is permitted to connect several safety mats in series to the same safety relay. The manufacturer's recommendation for size and number of mats shall be followed.

5.9.6 The mat shall be permanently affixed to the floor. Manufacturer supplied edge trim should be used to avoid creating a tripping hazard with the mat.

5.9.7 Each safety mat shall be connected to a mat controller designed for the specific mat type.

5.9.8 Safety mat circuits shall initiate a stop signal by application of a load.

Note: This requirement means a safety mat shall not be used to initiate a stop signal when a load is removed from the mat. A mis-applied safety mat can easily be defeated by placing an object such as a toolbox on the safety mat.

5.9.8.1 All controllers shall initiate a stop signal if a malfunction is detected in the safety mat or mat wiring. Conductive and Tactile mat controllers shall have the ability to detect open and shorted wires. Fiber Optic mat controllers shall have the ability to detect broken fibers.

5.9.8.2 Safety mat controller's normally open safety output contact(s) shall be connected to a safety circuit. This safety circuit shall either be a safety relay or direct connection to positive-guided relay(s) with contact monitoring feedback**.**

- When the mat controller has an embedded safety relay, outputs can be driven directly from the safety contacts.
- For Single Channel with Monitoring, the output safety circuit may be a Single Channel safety relay or a single positive-guided relay.
- For Control Reliable circuits, the output safety circuit may be a dual channel safety relay or two positive-guided relays with dual monitoring.

5.10 Safety light curtain circuits

5.10.1 Light curtains shall not be used on full revolution power presses. Light curtains shall not be used as the sole protection means on applications where a physical barrier is needed to provide protection from flying debris, spray, splashing liquids, welding arc, etc.

5.10.2 The light curtain shall be mounted in accordance with the safe distance formula. Reference Annex B.

5.10.3 The light curtain application should be tested per Annex A.

5.10.4 The light curtain's normally open safety output contact(s) shall be connected to a safety circuit. Reference figure 5.9.4.

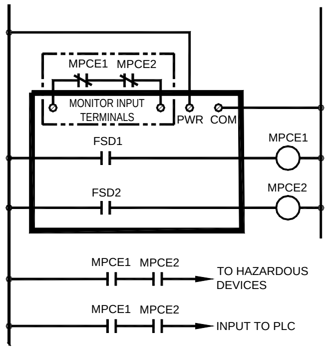


Figure 5.10.4 – Light Curtain w/ Relays

5.10.4.1 For Single Channel with Monitoring the output safety circuit shall be a single channel safety relay or a single positive-guided relay with monitoring.

5.10.4.2 For Control Reliable circuits the output safety circuit shall be a dual channel safety relay or two positive-guided relays with dual monitoring.

5.10.4.3 When the light curtain has an embedded safety relay, outputs can be driven directly from the safety contacts.

6 Point-of-operation guarding requirements

6.1 Point-of-operation guarding is 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. The operator normally trips the point-of-operation guard during each cycle of the machine. Typical point-of-operation guards include movable barrier devices such as interlocked doors or gates, presence-sensing devices such as light curtains and safety mats, or two-hand control devices.

6.2 Installation

6.2.1 Movable barrier devices and presence-sensing devices shall be installed as detailed in the Delphi *Design-In Health and Safety Specification* and the device specific sections 4 and 5 of this specification.

6.2.2 The two-hand control devices shall be permanently located and arranged so that actuation by means other than the two hands of the operator is prevented. The two-hand control devices shall meet all the requirements of *Two-hand operating lever, trip and control devices* sections of ANSI B11.19.

Note: Whisker switches for two-hand control are not recommended.

6.3 Interlocking circuits

6.3.1 The interlocking of the point-of-operation guard and the machine's control system shall be implemented using the appropriate safety circuit. Reset of the safety circuit should not require a pushbutton.

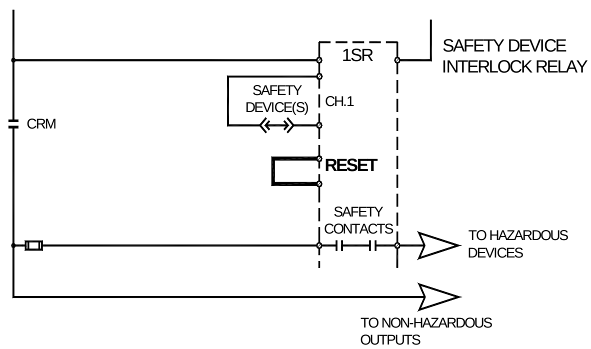


Figure 6.3.1 – Automatic Reset

6.3.2 Two-hand control shall be type 3, requiring simultaneous actuation of the two devices within 500 milliseconds of each other (figure 6.3.2). For Single Channel circuit applications two-hand control may be programmable. For Single Channel with Monitoring and Control Reliable applications, two-hand control shall be implemented using a dual channel two-hand control safety relay.

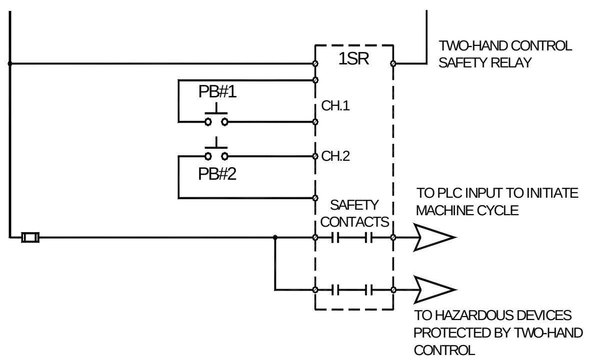


Figure 6.3.2 – Two Hand Control - Control Reliable

6.3.3 When the machine cycle is interrupted during the hazardous portion of the cycle, by interrupting the point-of-operation guard electrical interlock or release of either two-hand control device, the appropriate safety circuit shall remove power (including fluid power) from hazardous devices.

6.4 Machine Logic

6.4.1 The point-of-operation safety circuit(s) shall not disable the control circuit cycle-overtime timer unless interrupting the point-of operation guard aborts the machine cycle.

6.4.2 Independent of the safety requirements for point-of-operation guard safety circuits, the machine sequence logic should also give consideration to the following:

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

These process specific considerations may in-turn affect the control circuit response to the drop out of the point-of-operation guard safety circuit, but shall never lower the performance of the appropriate safety circuit.

7 Perimeter guarding requirements

7.1 A perimeter guard is a device used to stop and/or prevent the starting of a machine when a person enters an area where hazards exist. The guard is not typically interrupted each cycle of the machine. Typical perimeter guards include movable barrier devices such as electrical interlocked doors or gates, or presence-sensing devices such as light curtains and safety mats.

7.2 Installation

7.2.1 Movable barrier devices and presence-sensing devices shall be installed as detailed in the Delphi Design-In Health and Safety Specification and the device specific sections 4 and 5 of this specification.

7.2.2 In a perimeter guard application it may be possible for a person to pass completely through the guard(s), placing their body between that guard(s) and the hazard.

7.2.3 When it is possible for a person to completely pass through the perimeter guard, the following additional requirements shall apply:

7.2.3.1 The perimeter guard safety circuit shall remove power (including fluid power) from hazardous devices on an under voltage condition (or power off) and shall not be reset by the return of line voltage.

7.2.3.2 The perimeter guard safety circuit shall not be reset by the physical closure of the perimeter guard.

7.2.3.3 A perimeter guard safety circuit reset device shall be provided (figure 7.2.3.3) and be positioned so that the reset device cannot be reached from within the protected area.

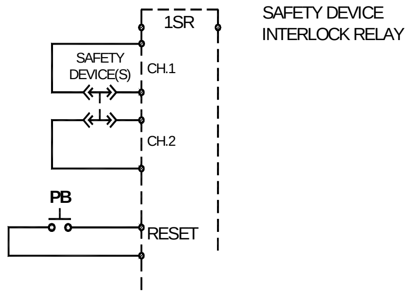


Figure 7.2.3.3 – Manual Reset

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

Exception: Where the entire area protected by the perimeter guard is not visible from the reset location, multiple reset devices shall be installed. These reset locations shall be positioned to collectively allow viewing the entire area protected by the perimeter guard. The number of reset locations should be minimized. The reset devices shall be connected to an appropriate safety circuit(s), which is designed to force a certain reset sequence with specific timing (figure 7.2.3.4). The equipment manufacturer should consult with the purchasing division for application specifics.

7.2.3.5 Perimeter-guard safety circuit reset device(s) is permitted to be a control device that also performs a different function, such as the Master Start pushbutton, provided all the requirements of this item are met.

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

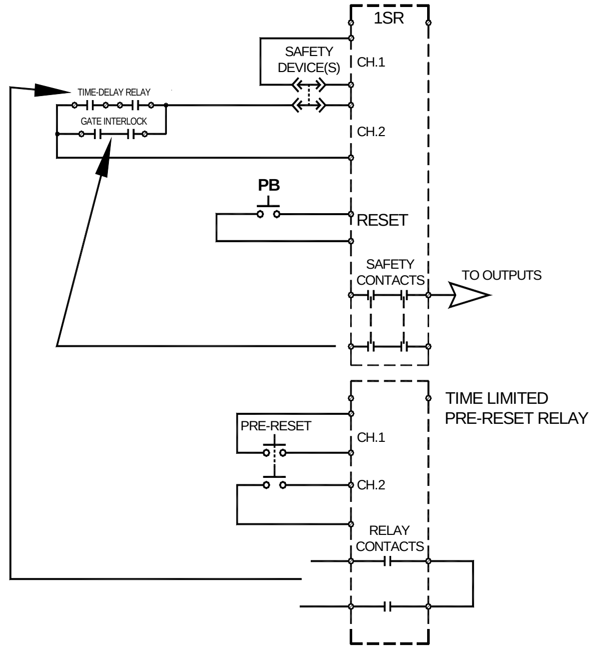


Figure 7.2.3.4 – Multiple Gate Resets

7.3 Interlocking circuits

7.3.1 When the electrical interlock device is interrupted, the perimeter guard safety circuit shall remove power (including fluid power) from hazardous devices.

7.4 Machine Logic

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

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

These process-specific considerations may in-turn affect the control circuit response to the interruption of the perimeter guard safety circuit, but shall never lower the performance of the appropriate safety circuit.

8 Fluid Power Circuits and Application

8.1 Fluid power circuit performance

Refer to section 5.1 of this document for performance level descriptions and requirements.

8.1.1 “Simple” safety circuit:

Refer to section 5.1.1. Reference page C2 of Annex C for pneumatic and D1 in Annex D for hydraulic examples. Reference figure 8.1.1.

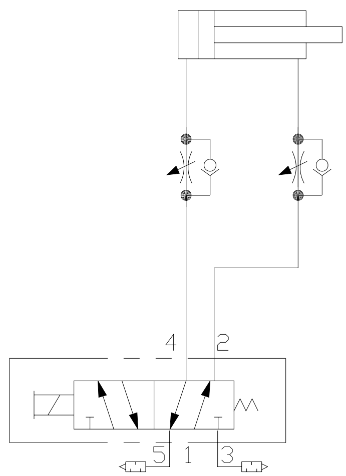


Figure 8.1.1 – Simple and Single Channel Pneumatic Circuit

8.1.2 “Single Channel” safety circuit:

Refer to section 5.1.2. Reference page C4 in Annex C for pneumatic and D1 in Annex D for hydraulic examples. Reference figures 8.1.1 and 8.1.2.

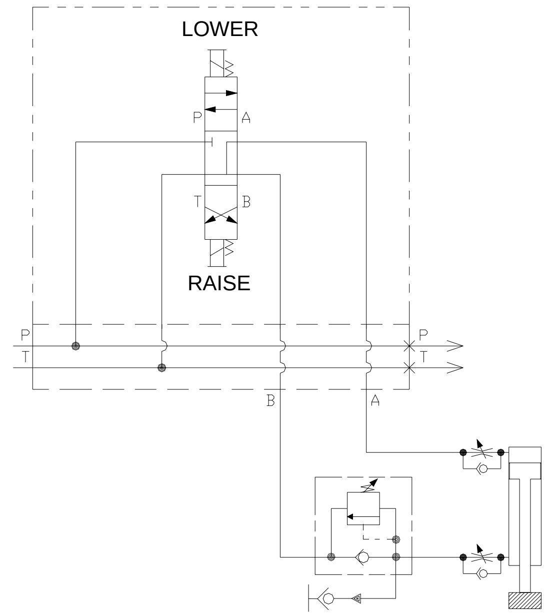


Figure 8.1.2 – Simple and Single Channel Hydraulic Circuit

8.1.3 “Single Channel with Monitoring” safety circuit:

Refer to section 5.1.3. Reference page C6 in Annex C for pneumatic and D3 in Annex D for a hydraulic example. Reference figures 8.1.3a and 8.1.3b.

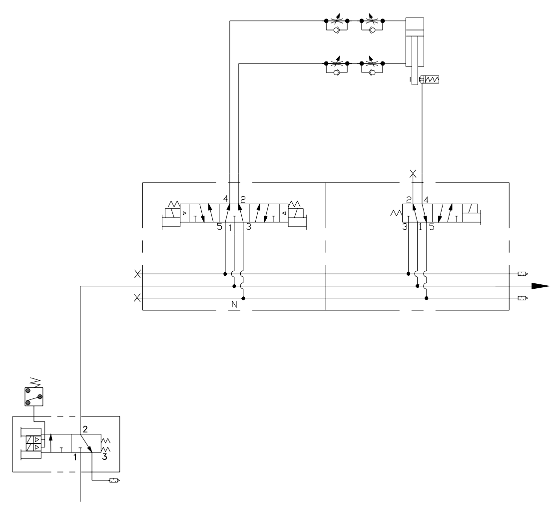


Figure 8.1.3a – Single Channel with Monitoring Pneumatic Circuit

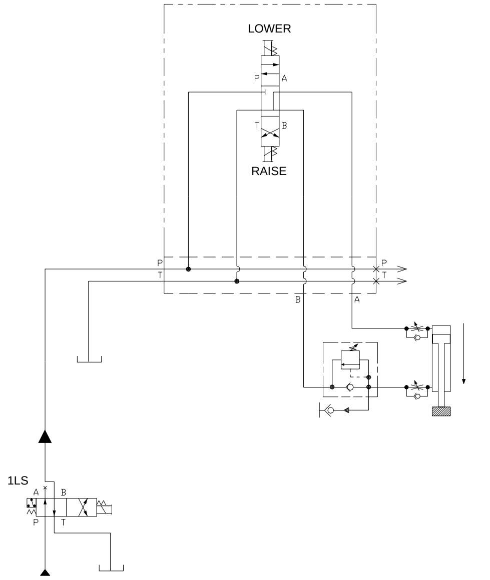


Figure 8.1.3b – Single Channel with Monitoring Hydraulic Circuit

8.1.4 "Control Reliable" safety circuit:

Refer to section 5.1.4.

Pneumatics: Reference sample drawings C9 for examples of hazards in one or both directions, as well as pneumatic brake or clutch/brake applications. Commercially available safety technology is preferred.

Hydraulics: Reference sample drawing D5 for flows less than 18 GPM and D7 for flows in excess of 18 GPM in Annex D.

Note: Redundant dual stage spool valves are available to handle flows in excess of 18 GPM, but for safety applications their use is discouraged for the following reasons:

- Only the pilot stage spool is monitored, not the main stage, which ultimately controls the motion. Therefore failure of the main stage would go undetected, as the properly functioning pilot stage would still indicate proper operation.
- Pressure switch monitoring of the main stage typically adds more controls complexity, plumbing and cost than the recommended cartridge valve circuit.

8.2 General requirements for all fluid power circuits.

8.2.1 From a safety and reliability perspective, safety circuit valves shall be selected based on the design characteristics that promote the least likelihood of failure under all operating conditions, and where possible be specifically designed for safety applications.

8.2.2 Spools with resilient seals should be avoided due to the higher probability of seal failure.

8.2.3 Springs – Consider the available return spring forces for the valve. The higher the spring force, the greater the valve's ability to overcome contamination and return to its de-energized position. A spring failure must also be considered and its impact on the ability of the spool to return to its normal de-energized position.

8.2.4 Dry Service – Pneumatic applications should be rated for dry service. This reduces the likelihood of valve spool sticking due to poor maintenance of the lubricators.

8.2.5 Directional control valves shall be mounted so that the valve spool(s) are in the horizontal plane. This is to prevent uncontrolled movement in the event of a spring failure. This includes the pilot sections of pilot operated valves.

8.2.6 Valve response and line pressurization/exhaust times shall be included in the time distance calculations for fluid power systems used in safety circuits. Refer to Safe Distance Calculation, Annex B.

8.2.7 Line volumes shall be kept to a minimum to facilitate better control and shorter stop distances/times. Line lengths between the valve and actuator should be 18 inches or less.

8.2.8 Cylinders may require the use of one or more quick stopping features shown in the reference circuits to minimize safe distance and increase operator safety. For pneumatic systems use rod brakes. This is due to the potential for movement in the event of a leak within the system. For hydraulic systems with heavy vertical loads, or motions with high inertia, counter balance or braking valves are required.

8.2.9 Proper filtration shall be used to minimize component failure due to contamination. Systems shall be evaluated to determine and eliminate sources of contamination ingression. Examples of methods used to minimize contamination are as follows:

- Filtration consistent with manufacturers recommendations. (This reduces contamination related to internal wear.)
- Air breathers
- Fill filters
- Rod wipers (and in extreme cases) rod boots

A Annex A Application and design verification of safety circuits

A.1 Design and construction verification

A.1.1 The engineer responsible for the design and specification of the safety circuits should perform the following:

A.1.1.1 Verify that the type and design of the chosen components are compatible with the operational and safety requirements of the application.

A.1.1.2 Verify that the design applies the components per the manufacturers' recommendations.

A.1.1.3 Verify that the manufacturers' recommendations for mounting and alignment of all components have been strictly followed.

A.1.1.4 Verify all electrical connections between the safety components and the safety circuits, per the approved prints.

A.1.2 The person designated to perform the construction verification should complete all of the following:

A.1.2.1 Verify that the minimum separation distance from the hazards to the light curtain, safety mat, two-hand, and/or single initiation device is not less than the distance calculated in Annex B.

A.1.2.2 Verify that access to the hazards is not possible from any direction that is not protected by a safety device or hard guarding.

A.1.2.3 In a point-of-operation application, verify that the point-of-operation guard is permanently installed in a location that prohibits a person from placing their body between that guard(s) and the hazard. This includes verifying that safety mats are not the sole guarding means in applications where someone can step off of the safety mat or reach over it and into the hazard/hazardous area.

A.1.2.4 In a perimeter-guard application, verify the following:

A.1.2.4.1 The reset is positioned outside the protected area.

A.1.2.4.2 The reset is positioned within view of the entire protected area.

A.1.2.4.3 Multiple resets have been installed when the entire area protected by the perimeter guard is not visible from the reset locations. These reset locations shall be positioned to collectively allow viewing the entire protected area.

A.2 Initial Operation verification

A.2.1 Verify the effectiveness of the safeguarding and associated control system with the power "on". Verify normal operation as follows:

A.2.1.1 With the machine in motion, verify that all associated hazardous motions are eliminated upon interruption of each and every safety circuit input device.

A.2.1.2 With the machine at rest, verify that the associated hazardous motions cannot be re-initiated with the following:

A.2.1.2.1 a safety circuit interrupted.

A.2.1.2.2 re-application of the input device (where a reset is required).

A.2.1.2.3 a reset button being tied-down.

A.2.1.3 Verify the machine stopping response time with an instrument such as that described in Annex B.

A.2.1.4 In light curtain applications perform the following:

A.2.1.4.1 Perform steps A.2.1.1 and A.2.1.2 with the manufacturer's recommended test piece.

A.2.1.4.2 With the machine at rest, and using the specified test piece, follow the light curtain manufacturer's recommended test procedure to verify that the light curtain is operational throughout the physical ranges of the transmitter and receiver.

A.2.1.4.3 Remove power to the light curtain and verify that the light curtain goes to a lockout state (all outputs immediately de-energize). Verify that the light curtain outputs do not re-energize until the light curtain's reset is performed.

***Note**: This use of the term "lockout" is not to be confused with machine lockout/tagout. Here industry typically refers to the output state of the ESPE being forced off.*

B Annex B Safety distance formulas

B.1 General formula

The following general safety distance formula should be used to calculate the minimum safe distance to mount the safety device from the hazardous motions. Note that adaptations of this formula for single-device initiation, safety mats and light curtains are listed separately. This is the formula suggested in ANSI B11.19.

$$D_S = K \, x \, (T_S + T_C + T_r + T_{bm})$$

B.1.1 D_S = Minimum safety distance between the device and the nearest point of operation hazard in inches.

B.1.2 K = Hand speed constant of 63 inches per second

B.1.3 T_S = Stopping time of the equipment at the final control element (seconds).

B.1.4 T_C = Response time of the control system (seconds).

B.1.5 Note: T_S and T_C are usually measured by a stop-time measurement device such as the Gemco model 1999 Semelex SE-3-E Safetimeter test set .

B.1.6 T_r = Response time of the safeguarding device (seconds). This response time is available from the manufacturer of the device.

B.1.7 T_{bm} = Additional time required in press applications for the brake monitoring to compensate for variations in normal stopping time. Refer to ANSI B11.1-2001 for information on press brake monitors.

B.2 Single-device initiation and safety mats

The following safety distance formula shall be used to calculate the minimum safe distance to mount the safety device from the hazardous motions. This formula applies to safety mat applications and the initiation device in single-device initiation applications where the initiation device is used as the safeguard. Consideration of an individual's stride, reach, and point-of-entry to the hazard should be used in determining the safe distance. This formula is suggested by ANSI B11.19, and European Standard EN 999.

$$D_S = K \, x \, (T_S + T_C + T_r + T_{bm}) + C$$

B.2.1 C = 66 for single-device initiation applications, and safety mat applications where the individual being protected might be approaching the safety mat in-stride. The typical operator reach is approximately 66 inches.

B.2.2 C = 48 safety mat applications where the individual being protected does not approach the safety mat in-stride, i.e., the individual's first step toward the hazard is also directly onto the safety mat.

B.3 Light curtains

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

$$D_s = K \times (T_s + T_c + T_r + T_{bm}) + D_{pf}$$

B.3.1 D_{pf} = Added distance due to the penetration factor as shown on chart 1. The minimum object sensitivity is stated by the light curtain manufacturer. When beam blank outs or floating-window features are used, these figures should be added to the object sensitivity figure before using chart 1.

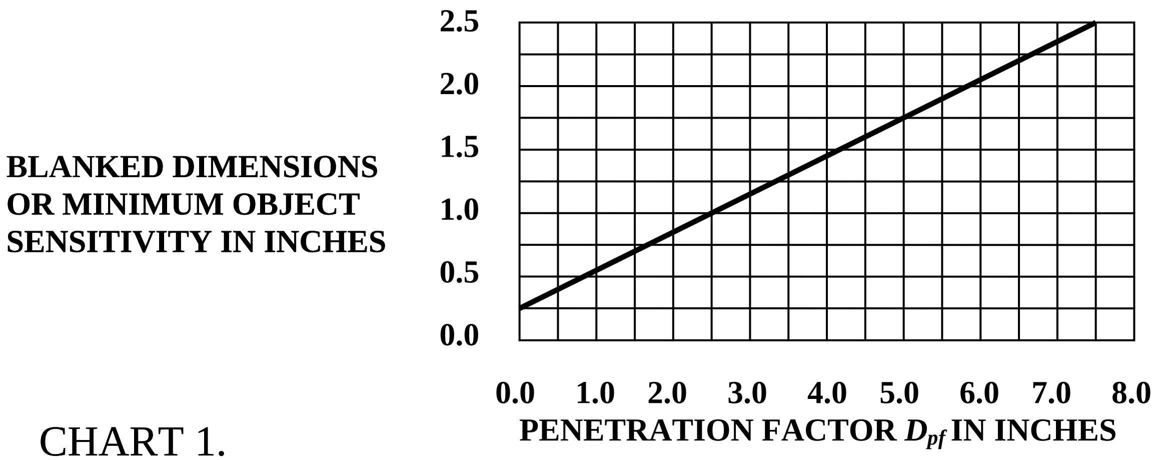
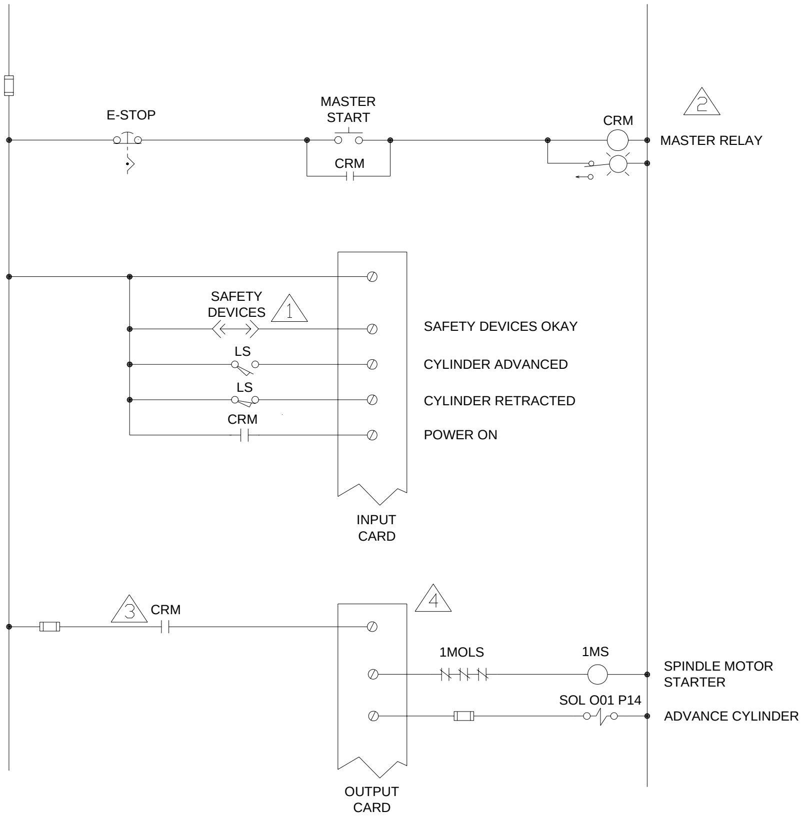


CHART 1.

C Annex C Sample electrical/pneumatic circuits

Simple Safety Circuit – Input Devices, sheet C1

SIMPLE SAFETY CIRCUIT
RISK ASSESSMENT R1 OR R2A
INPUT DEVICES



FUNCTION:
This drawing is an example that illustrates a Simple safety circuit which corresponds to the risk reduction category as determined by a risk assessment for a particular machine.

Risk assessment has determined that safeguard performance meets the requirements of R1 or R2A.

NOTES:
1) Safety devices (e.g. limit switch) are connected to inputs of the programmable device (e.g. PLC).
2) The master relay (CRM) performs a safety function at a Single Channel level.
3) No distinction is made for the category of outputs (i.e. between hazardous and non-hazardous).
4) The programmable device controls the state of the outputs based on the state of the inputs (including the safety devices).

Refer to the Specification document for detailed requirements. This drawing is not a drafting example.

REVISIONS

REV. SYM.	DET.	CHANGE				

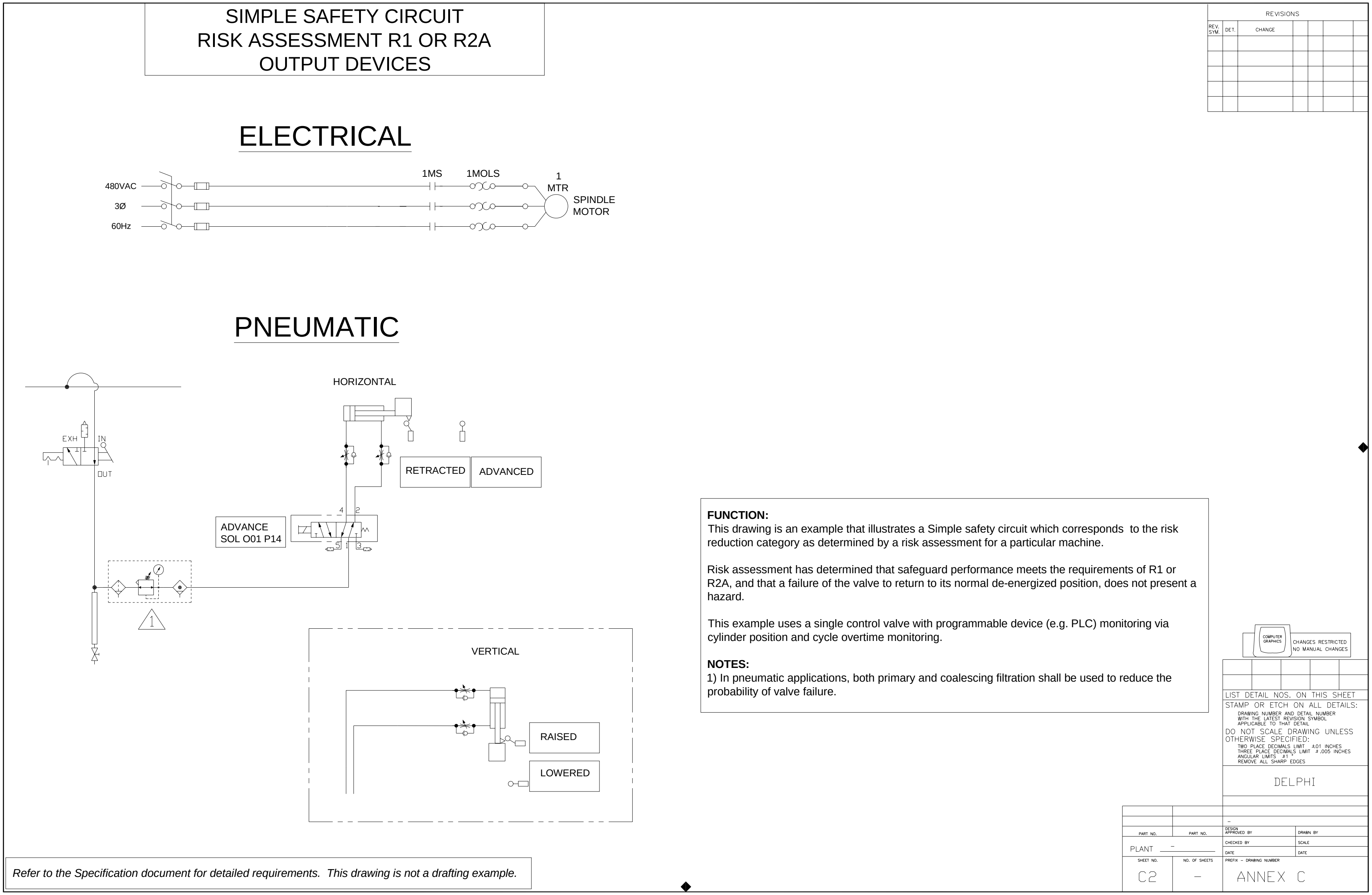
CHANGES RESTRICTED NO MANUAL CHANGES

LIST DETAIL NOS. ON THIS SHEET
STAMP OR ETCH ON ALL DETAILS: DRAWING NUMBER AND DETAIL NUMBER WITH THE LATEST REVISION SYMBOL APPLICABLE TO THAT DETAIL
DO NOT SCALE DRAWING UNLESS OTHERWISE SPECIFIED: TWO PLACE DECIMALS LIMIT ±.01 INCHES THREE PLACE DECIMALS LIMIT ±.005 INCHES ANGULAR LIMITS ±1 REMOVE ALL SHARP EDGES

DELPHI

PART NO. | PART NO. | DESIGN APPROVED BY | DRAWN BY
PLANT – | CHECKED BY | SCALE
DATE | DATE
SHEET NO. C1 | NO. OF SHEETS – | PREFIX – DRAWING NUMBER ANNEX C

Simple Safety Circuit – Output Devices, sheet C2



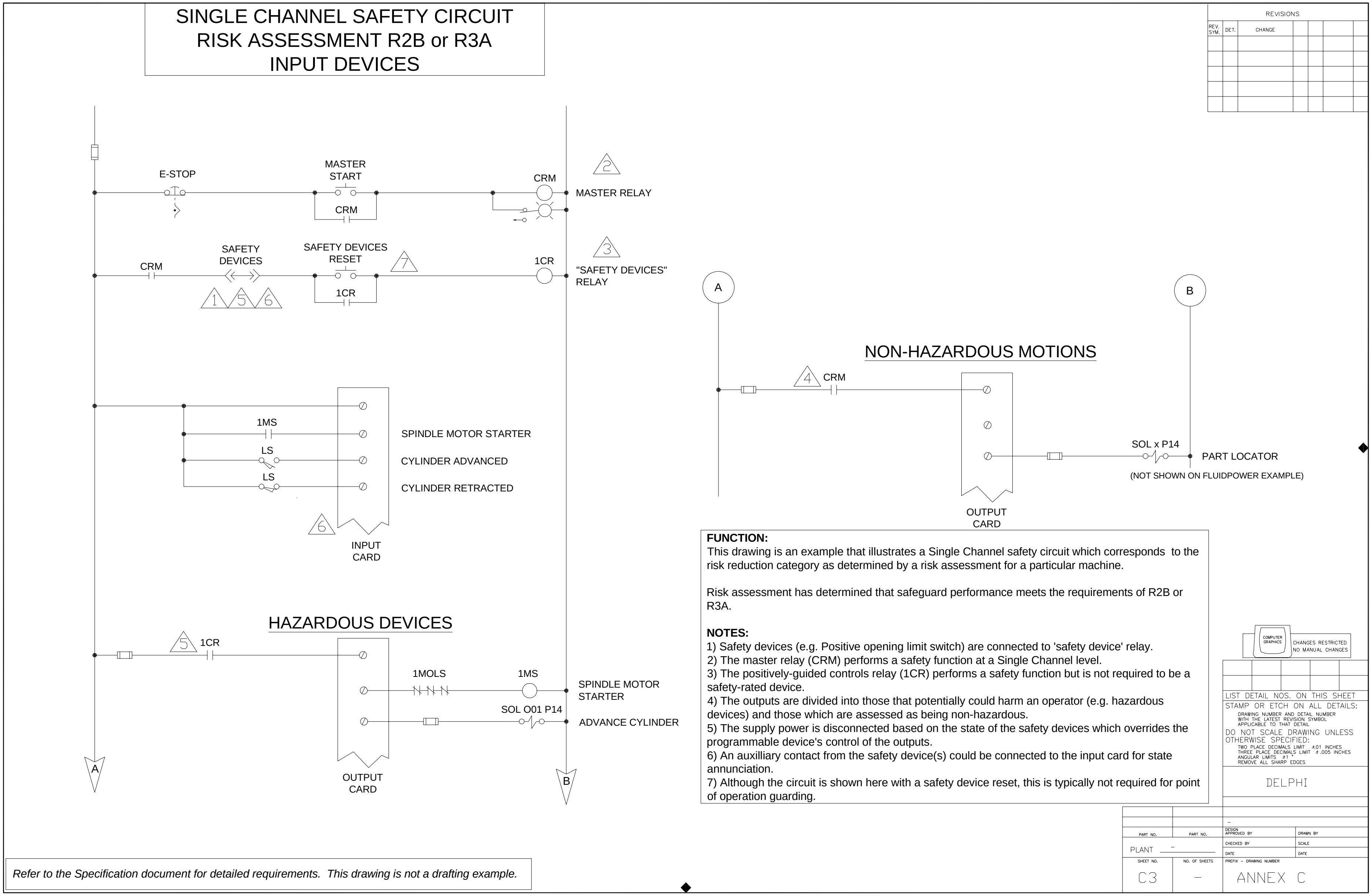
FUNCTION:
This drawing is an example that illustrates a Simple safety circuit which corresponds to the risk reduction category as determined by a risk assessment for a particular machine.

Risk assessment has determined that safeguard performance meets the requirements of R1 or R2A, and that a failure of the valve to return to its normal de-energized position, does not present a hazard.

This example uses a single control valve with programmable device (e.g. PLC) monitoring via cylinder position and cycle overtime monitoring.

NOTES:
1) In pneumatic applications, both primary and coalescing filtration shall be used to reduce the probability of valve failure.

Single Channel Safety Circuit – Input Devices, sheet C3



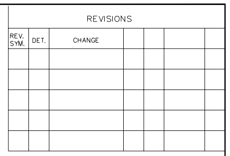
FUNCTION:
This drawing is an example that illustrates a Single Channel safety circuit which corresponds to the risk reduction category as determined by a risk assessment for a particular machine.

Risk assessment has determined that safeguard performance meets the requirements of R2B or R3A.

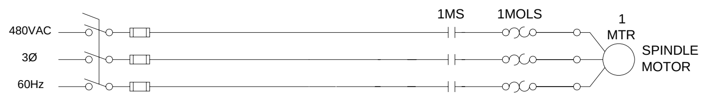
NOTES:
1) Safety devices (e.g. Positive opening limit switch) are connected to 'safety device' relay.
2) The master relay (CRM) performs a safety function at a Single Channel level.
3) The positively-guided controls relay (1CR) performs a safety function but is not required to be a safety-rated device.
4) The outputs are divided into those that potentially could harm an operator (e.g. hazardous devices) and those which are assessed as being non-hazardous.
5) The supply power is disconnected based on the state of the safety devices which overrides the programmable device's control of the outputs.
6) An auxilliary contact from the safety device(s) could be connected to the input card for state annunciation.
7) Although the circuit is shown here with a safety device reset, this is typically not required for point of operation guarding.

Single Channel Safety Circuit – Output Devices, sheet C4

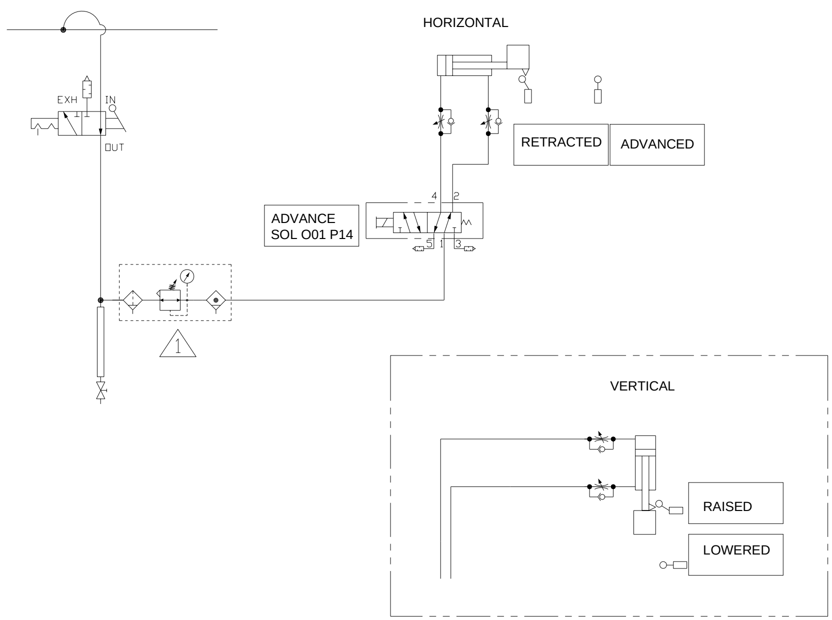
SINGLE CHANNEL SAFETY CIRCUIT
RISK ASSESSMENT R2B or R3A
OUTPUT DEVICES



ELECTRICAL



PNEUMATIC

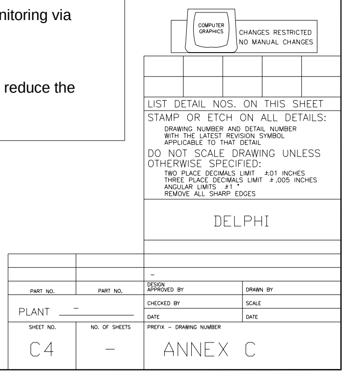


FUNCTION:
This drawing is an example that illustrates a Single Channel safety circuit which corresponds to the risk reduction category as determined by a risk assessment for a particular machine.

Risk assessment has determined that safeguard performance meets the requirements of R2B or R3A.

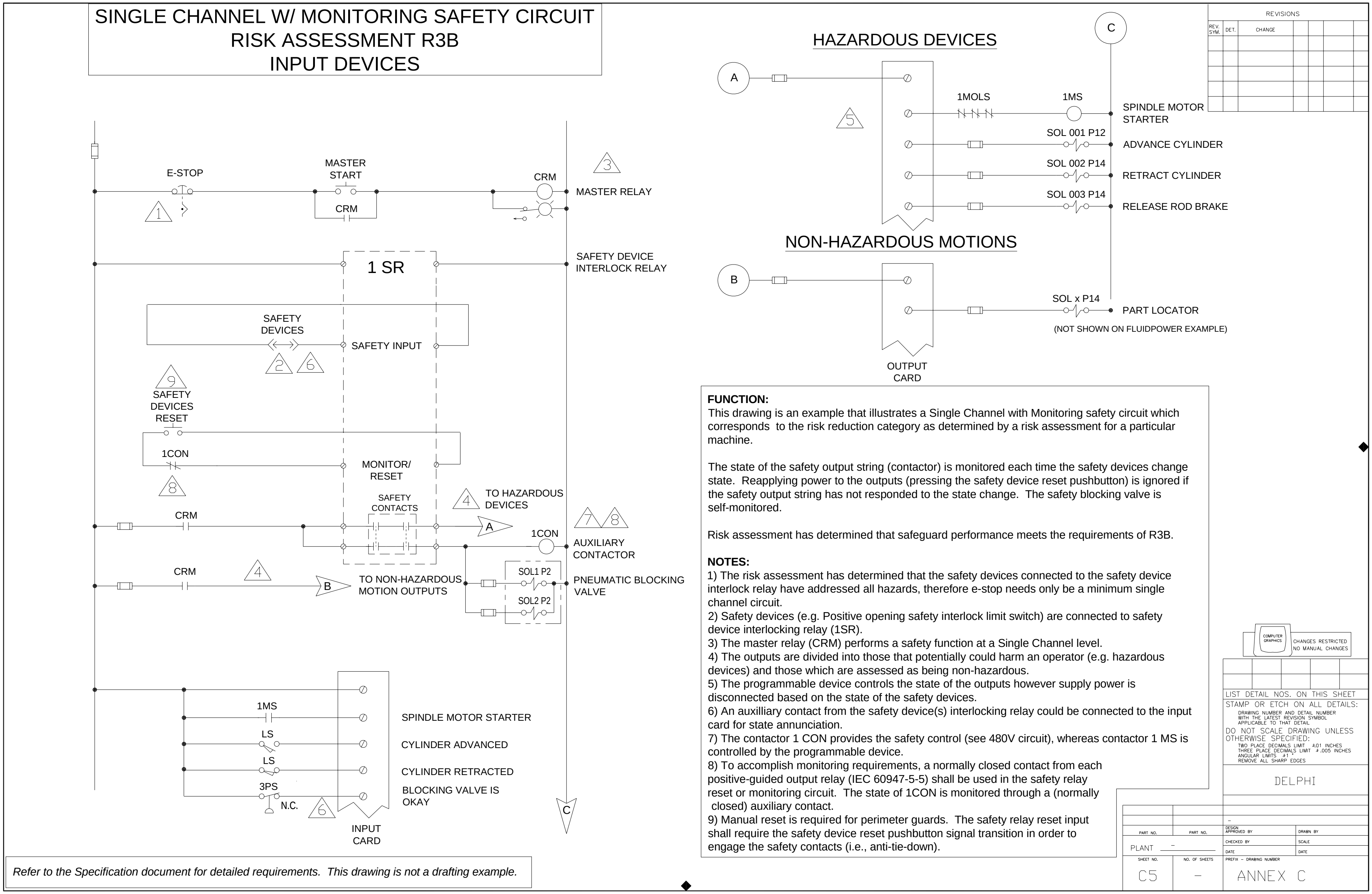
This example uses a single control valve with programmable device (e.g. PLC) monitoring via cylinder position and cycle overtime monitoring.

NOTES:
1) In pneumatic applications, both primary and coalescing filtration shall be used to reduce the probability of valve failure.



Refer to the Specification document for detailed requirements. This drawing is not a drafting example.

Single Channel with Monitoring Safety Circuit – Input Devices, sheet C5



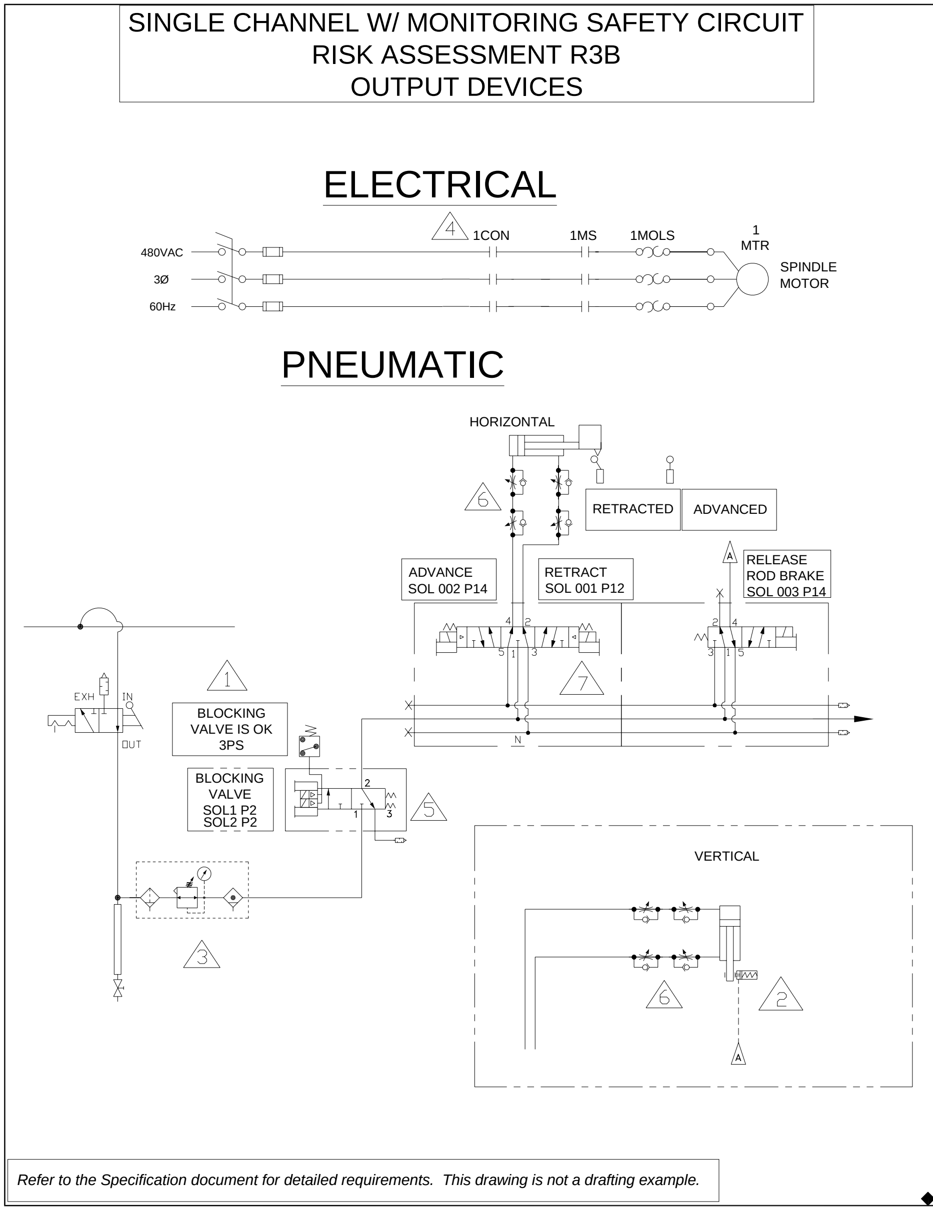
FUNCTION:
This drawing is an example that illustrates a Single Channel with Monitoring safety circuit which corresponds to the risk reduction category as determined by a risk assessment for a particular machine.

The state of the safety output string (contactor) is monitored each time the safety devices change state. Reapplying power to the outputs (pressing the safety device reset pushbutton) is ignored if the safety output string has not responded to the state change. The safety blocking valve is self-monitored.

Risk assessment has determined that safeguard performance meets the requirements of R3B.

NOTES:
1) The risk assessment has determined that the safety devices connected to the safety device interlock relay have addressed all hazards, therefore e-stop needs only be a minimum single channel circuit.
2) Safety devices (e.g. Positive opening safety interlock limit switch) are connected to safety device interlocking relay (1SR).
3) The master relay (CRM) performs a safety function at a Single Channel level.
4) The outputs are divided into those that potentially could harm an operator (e.g. hazardous devices) and those which are assessed as being non-hazardous.
5) The programmable device controls the state of the outputs however supply power is disconnected based on the state of the safety devices.
6) An auxilliary contact from the safety device(s) interlocking relay could be connected to the input card for state annunciation.
7) The contactor 1 CON provides the safety control (see 480V circuit), whereas contactor 1 MS is controlled by the programmable device.
8) To accomplish monitoring requirements, a normally closed contact from each positive-guided output relay (IEC 60947-5-5) shall be used in the safety relay reset or monitoring circuit. The state of 1CON is monitored through a (normally closed) auxiliary contact.
9) Manual reset is required for perimeter guards. The safety relay reset input shall require the safety device reset pushbutton signal transition in order to engage the safety contacts (i.e., anti-tie-down).

Single Channel with Monitoring Safety Circuit – Output Devices, sheet C6



FUNCTION:
This drawing is an example that illustrates a Single Channel with Monitoring safety circuit which corresponds to the risk reduction category as determined by a risk assessment for a particular machine.

Risk assessment has determined that safeguard performance meets the requirements of R3B.

This example uses a control reliable blocking valve with software diagnostics via a pressure switch.

NOTES:
1) A contact from 3PS shall be connected to a PLC input for valve diagnostics.
2) The pneumatic circuit may require additional controls to provide for safe operation. For example, on a vertical cylinder, a rod brake (preferred), counter-balance valve, or P.O. check shall be required, where the lowering of the actuator is a hazard. Where flexible lines are required due to actuator motion, these valves shall be installed directly at the cylinder port. Flexible lines between the cylinder port and the P.O. check/counter balance valve are not permitted.
3) In pneumatic applications, both primary and coalescing filtration shall be used to reduce the probability of valve failure.
4) The contactor (1CON) provides primary ("spindle") motor power while the programmable device performs secondary control (1MS).
5) Herion's XSz series is preferred. Valve is redundant and self-monitored.
6) When using open centered valves, install flow controls meter-in to prevent a run-away condition during the transition from center position to offset. A combination series meter-in/meter-out flow control may be required to provide pneumatic actuator braking.
7) The actuators directional control valve is not considered part of the safety circuit. Directional control valve spool configuration and additional controls are application-specific. Multiple directional control valves may be connected downstream of the safety blocking valve. These directional control valves may be PLC powered.

REV. SYM.	DET.	CHANGE			

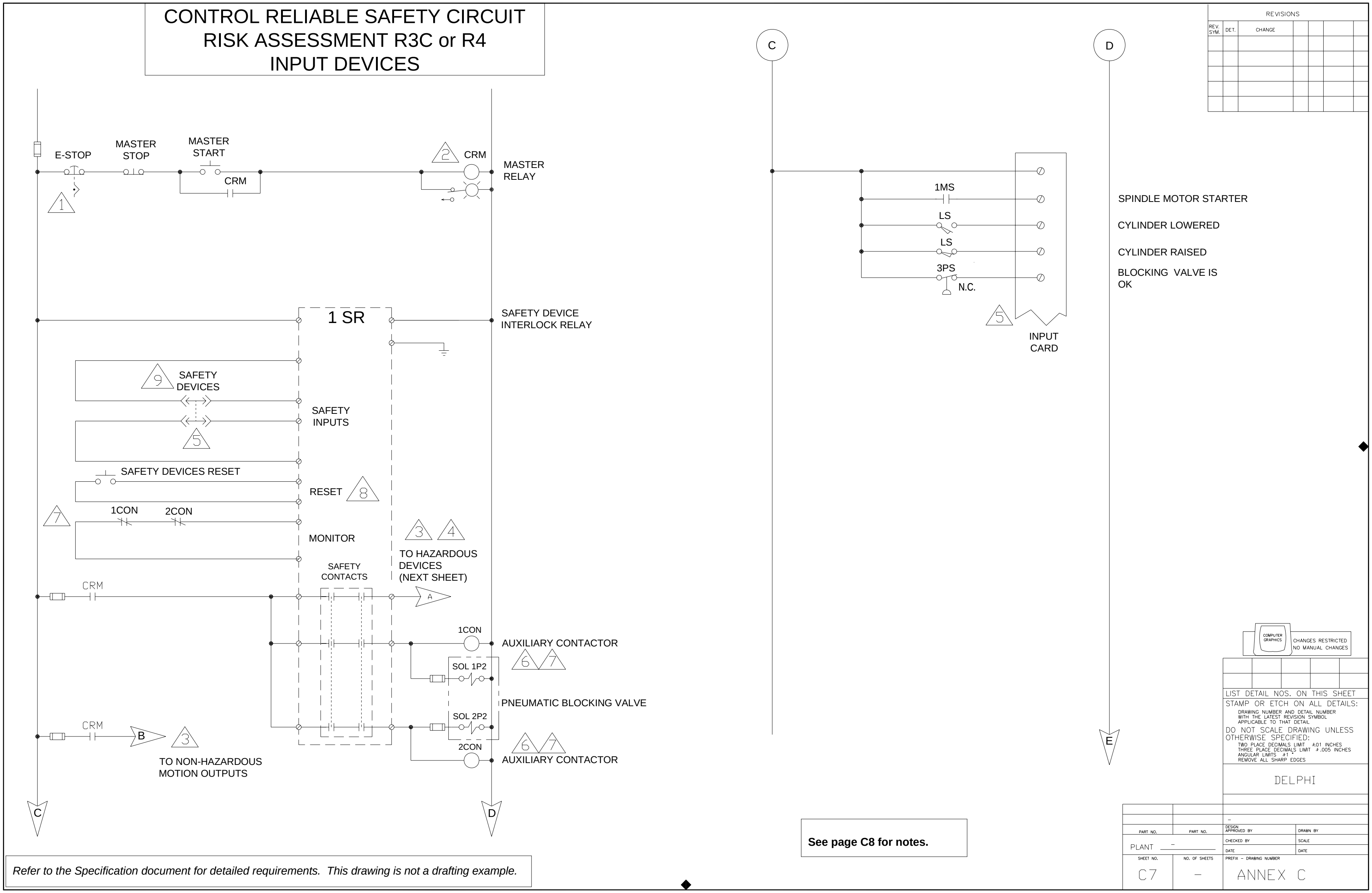
CHANGES RESTRICTED NO MANUAL CHANGES

LIST DETAIL NOS. ON THIS SHEET
STAMP OR ETCH ON ALL DETAILS: DRAWING NUMBER AND DETAIL NUMBER WITH THE LATEST REVISION SYMBOL APPLICABLE TO THAT DETAIL
DO NOT SCALE DRAWING UNLESS OTHERWISE SPECIFIED: TWO PLACE DECIMALS LIMIT ±.01 INCHES THREE PLACE DECIMALS LIMIT ±.005 INCHES ANGULAR LIMITS ±1° REMOVE ALL SHARP EDGES

DELPHI

PLANT –
SHEET NO. C6 | NO. OF SHEETS – | ANNEX C

Control Reliable Safety Circuit – Input Devices, sheet C7

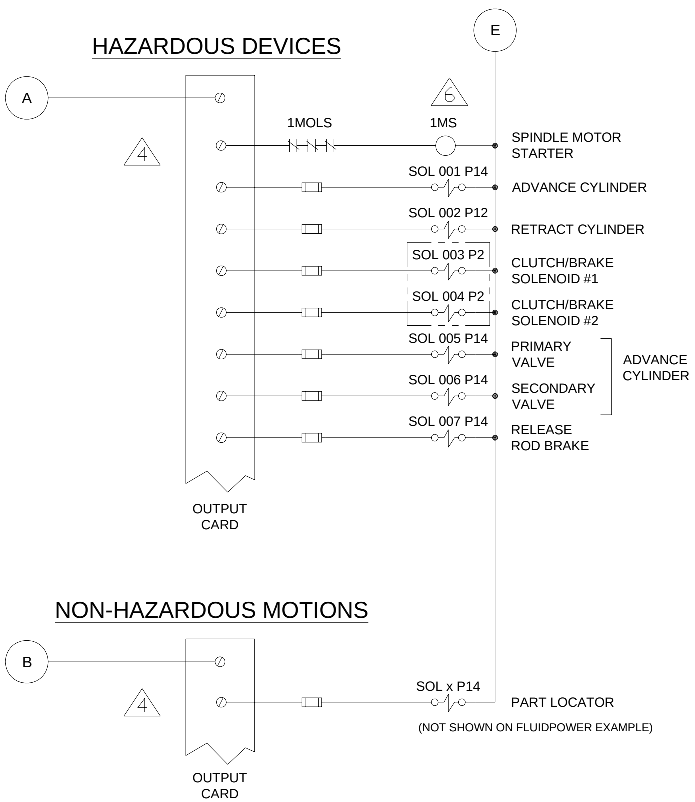


See page C8 for notes.

Refer to the Specification document for detailed requirements. This drawing is not a drafting example.

Control Reliable Safety Circuit – Input Devices, sheet C8

CONTROL RELIABLE SAFETY CIRCUIT
RISK ASSESSMENT R3C or R4
INPUT DEVICES



FUNCTION:
This drawing is an example that illustrates a Control Reliable safety circuit which corresponds to the risk reduction category as determined by a risk assessment for a particular machine.

Risk assessment has determined that safeguard performance meets the requirements of R3C or R4.

The state of the safety output string (contactors) are monitored by the safety device interlock relay. Redundancy is required for safety devices, the auxiliary contactors, and the blocking valves.

NOTES:

1) The risk assessment has determined that the safety devices connected to the safety device interlock relay have addressed all hazards, therefore e-stop needs only be a minimum Single Channel circuit.
2) The master relay (CRM) performs a safety function at a Single Channel level.
3) The outputs are divided into those that potentially could harm an operator (e.g. hazardous devices) and those which are assessed as being non-hazardous.
4) The programmable device controls the state of the outputs however supply power is disconnected based on the state of the safety devices.
5) An auxilliary output from the safety device(s) could be connected to the input card for state annunciation.
6) The contactors (1CON & 2CON) provide primary ("spindle") motor power (see 480v circuit) while the programmable device performs secondary control (1MS).
7) The state of the contactors (1CON & 2CON) are monitored through (normally closed) auxiliary contacts.
8) Manual reset is required for perimeter guards. The safety relay reset input shall require the safety device reset pushbutton signal transition in order to engage the safety contacts (i.e., anti-tie-down).
9) Safety devices (e.g. safety interlock switch such as a perimeter guard) are connected to 'safety device interlocking' relay.

CHANGES RESTRICTED NO MANUAL CHANGES

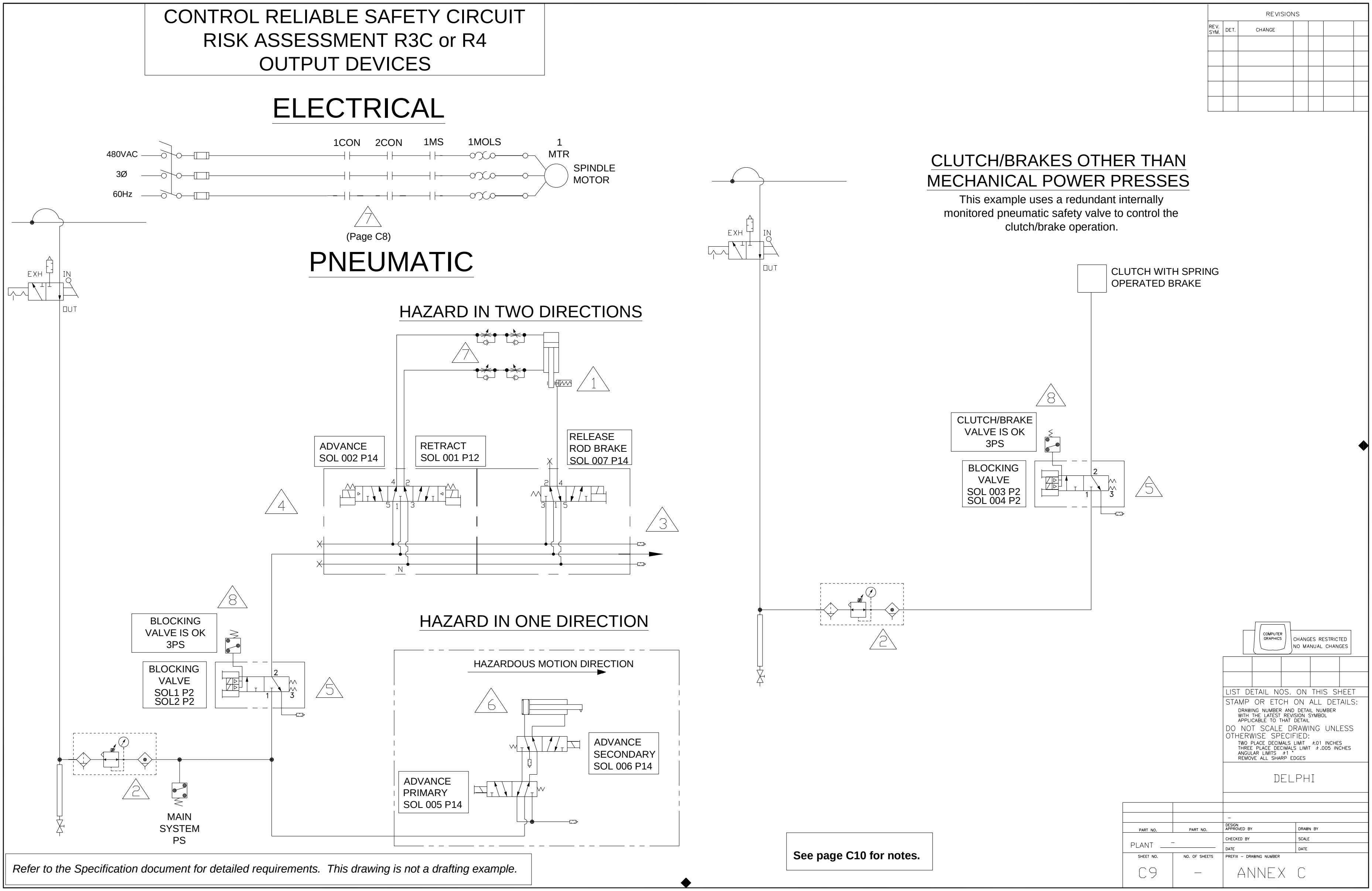
DELPHI

PLANT –

C8 – ANNEX C

Refer to the Specification document for detailed requirements. This drawing is not a drafting example.

Control Reliable Safety Circuit – Output Devices, sheet C9



Control Reliable Safety Circuit – Output Devices, sheet C10

CONTROL RELIABLE SAFETY CIRCUIT
RISK ASSESSMENT R3C or R4
OUTPUT DEVICES

REVISIONS						
REV. SYM.	DET.	CHANGE				

FUNCTION:
This drawing is an example that illustrates a Control Reliable safety circuit which corresponds to the risk reduction category as determined by a risk assessment for a particular machine.

Risk assessment has determined that safeguard performance meets the requirements of R3C or R4.

These examples show either a control reliable self monitored safety blocking valves with software diagnostics via a pressure switch, or redundant standard direction valves configured to fail in a safe condition.

NOTES:
1) For vertical applications a rod brake, counter balance valve, or pilot operated check shall be required to prevent dropping of loads that would be considered a hazard. Cylinder rod brakes are preferred.
2) Both primary and coalescing filtration shall be used to reduce the probability of valve failure.
3) The actuators directional control valve is not considered part of the safety circuit. Directional control valve spool configuration and additional controls are application-specific. Multiple directional control valves may be connected downstream of the safety blocking valve. These directional control valves may be PLC powered.
4) Consideration should be given to the use of a three-position directional control valve.
5) Herion's XSz series is preferred. Valve is redundant and self-monitored.
6) Assumes guarding provided to protect against hazardous motion in the retract position.
7) Meter-in flow controls are required for controlled restart after the cylinder has been exhausted.
8) A contact from 3PS shall be connected to a PLC input for valve diagnostics.

CAUTION!
Detented and spring offset valves that were de-energized with the actuator in mid-position, will either continue their motion, or retract to the home direction, when the safety circuit and corresponding blocking valves are reset. In the case of automatic reset, this would occur immediately upon releasing the safety device. For manual reset applications, this motion would occur only after depressing the reset button.

COMPUTER GRAPHICS
CHANGES RESTRICTED
NO MANUAL CHANGES

LIST DETAIL NOS. ON THIS SHEET

STAMP OR ETCH ON ALL DETAILS:
DRAWING NUMBER AND DETAIL NUMBER WITH THE LATEST REVISION SYMBOL APPLICABLE TO THAT DETAIL

DO NOT SCALE DRAWING UNLESS OTHERWISE SPECIFIED:
TWO PLACE DECIMALS LIMIT ±.01 INCHES
THREE PLACE DECIMALS LIMIT ±.005 INCHES
ANGULAR LIMITS ±1 °
REMOVE ALL SHARP EDGES

DELPHI

PART NO.	PART NO.	DESIGN APPROVED BY	DRAWN BY
PLANT –		CHECKED BY	SCALE
		DATE	DATE
SHEET NO. C10	NO. OF SHEETS –	PREFIX – DRAWING NUMBER ANNEX C	

See sheet C9 for circuits.

Refer to the Specification document for detailed requirements. This drawing is not a drafting example.

D Annex D Sample hydraulic circuits

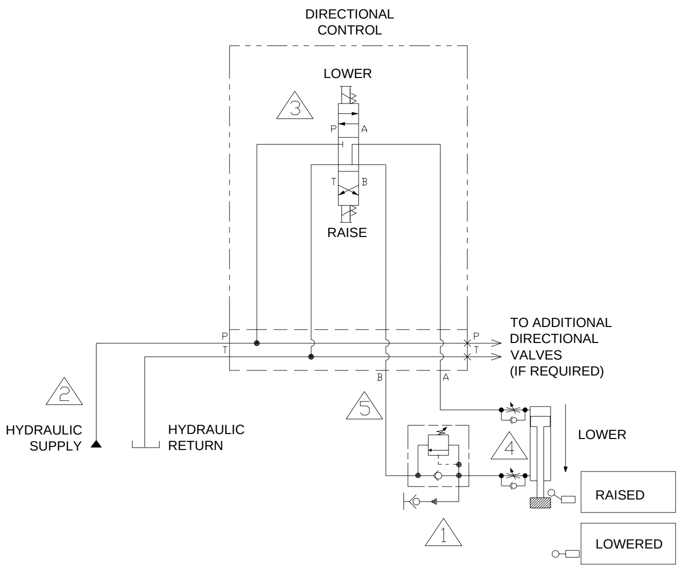
Simple and Single Channel Safety Circuit – Output Devices, sheet D1

SIMPLE & SINGLE CHANNEL SAFETY CIRCUIT
RISK ASSESSMENT R1, R2, OR R3A
OUTPUT DEVICES

REVISIONS

REV. SYM.	DET.	CHANGE				

HYDRAULIC



FUNCTION:
This drawing is an example that illustrates a Simple and Single Channel safety circuit for the hydraulic controls which corresponds to the risk reduction category as determined by a risk assessment for a particular machine. Refer to Annex C for simple and single channel electrical requirements.

Risk assessment has determined that safeguard performance meets the requirements of R1, R2A or R3A.

This example uses a single control valve with programmable device (e.g. PLC) monitoring via cylinder position and cycle overtime monitoring.

NOTES:
1) The hydraulic circuit may require additional controls to provide for safe operation. For example, on a vertical cylinder, a counter-balance valve or P.O. check will be required. These valves shall be mounted directly at the cylinder port. Flexible lines between the cylinder port and the Pilot Operated check/counter-balance valves are not permitted.
2) Filtration consistent with manufacturer's recommendations shall be used to reduce the probability of valve failure due to solid particle or oil contamination.
3) Valve may be relay or plc controlled.
4) To obtain optimal speed and motion control, mount the flow controls as close to the cylinders as possible, preferable using close hex nipples.
5) Line volumes shall be kept to a minimum (18" or less preferred, with 36" maximum), to optimize system stiffness. In no case shall the line volume exceed the cylinder volume. This requirement promotes an exchange of oil from the cylinder during each stroke, carrying away contamination that had entered through the rod seal.

COMPUTER GRAPHICS
CHANGES RESTRICTED
NO MANUAL CHANGES

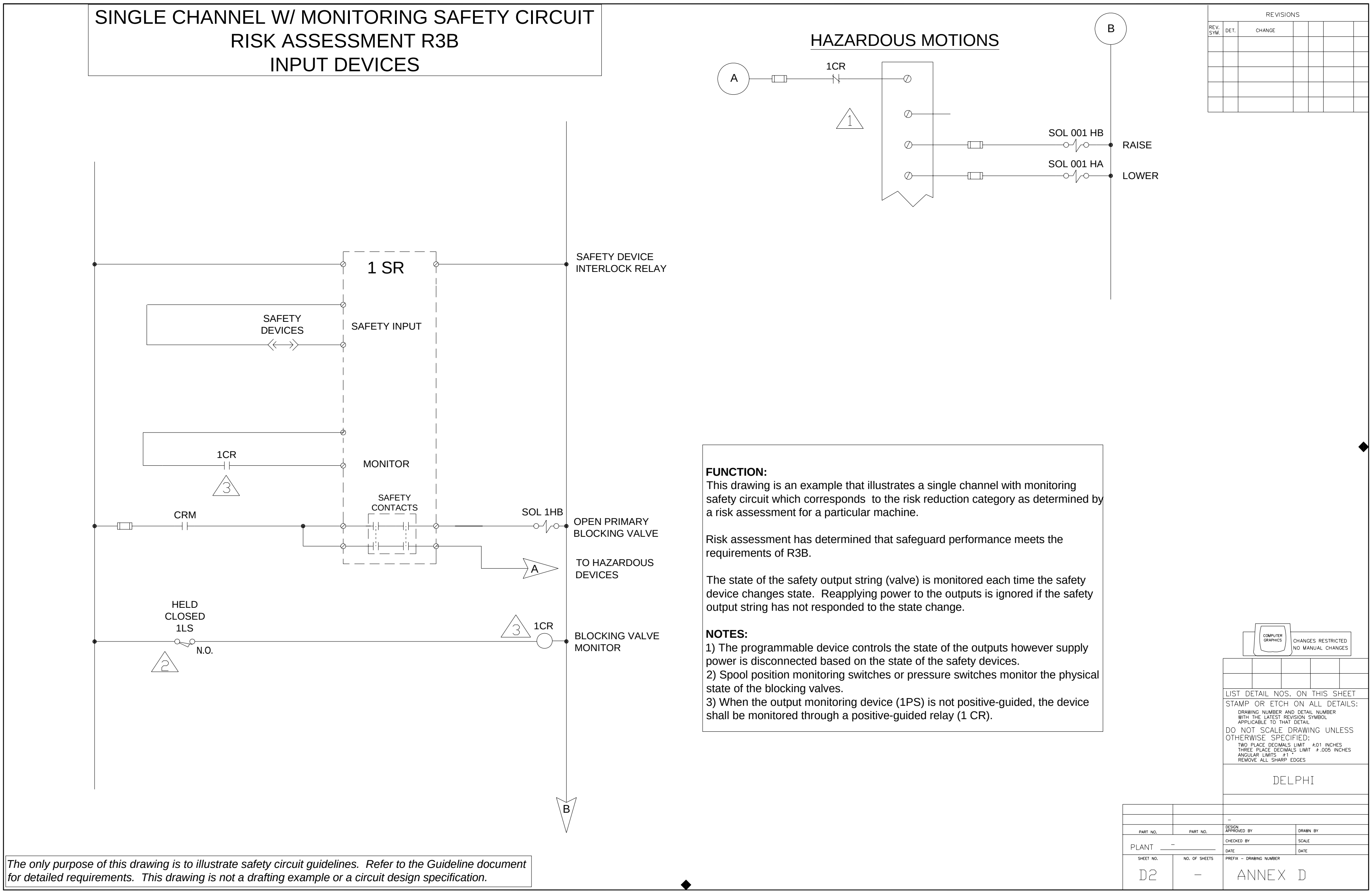
LIST DETAIL NOS. ON THIS SHEET
STAMP OR ETCH ON ALL DETAILS:
DRAWING NUMBER AND DETAIL NUMBER WITH THE LATEST REVISION SYMBOL APPLICABLE TO THAT DETAIL
DO NOT SCALE DRAWING UNLESS OTHERWISE SPECIFIED:
TWO PLACE DECIMALS LIMIT ±.01 INCHES
THREE PLACE DECIMALS LIMIT ±.005 INCHES
ANGULAR LIMITS ±1 °
REMOVE ALL SHARP EDGES

DELPHI

PART NO.	PART NO.	DESIGN APPROVED BY	DRAWN BY
PLANT –		CHECKED BY	SCALE
		DATE	DATE
SHEET NO. D1	NO. OF SHEETS –	PREFIX – DRAWING NUMBER ANNEX D	

Refer to the Specification document for detailed requirements. This drawing is not a drafting example.

Single Channel with Monitoring Safety Circuit – Input Devices, sheet D2

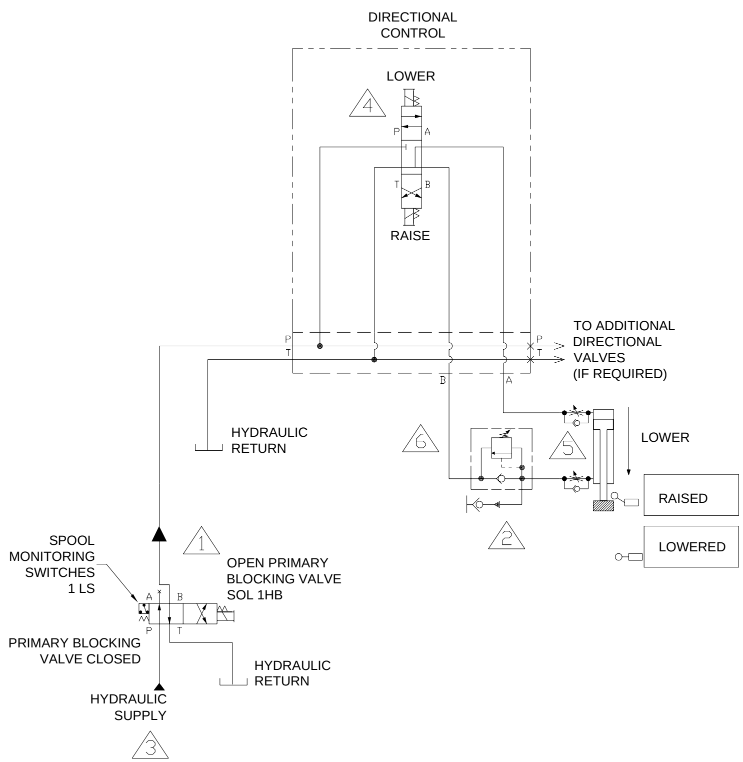


Single Channel with Monitoring Safety Circuit – Output Devices, sheet D3

SINGLE CHANNEL W/ MONITORING SAFETY CIRCUIT
RISK ASSESSMENT R3B
OUTPUT DEVICES

REVISIONS						
REV. SYM.	DET.	CHANGE				

HYDRAULIC



FUNCTION:
This drawing is an example that illustrates a Single Channel with Monitoring safety circuit which corresponds to the risk reduction category as determined by a risk assessment for a particular machine.

Risk assessment has determined that safeguard performance meets the requirements of R3B.

NOTES:
1) Solenoid 1HB shall be hardwire monitored for proper operation by position or pressure. Monitoring method must be checked to ensure proper sensor transition at suitable intervals, and shall inhibit further machine cycles until the problem is detected.
2) The hydraulic circuit may require additional controls to provide for safe operation. For example, on a vertical cylinder, a counter-balance valve or P.O. check will be required. These valves shall be mounted directly at the cylinder port. Flexible lines between the cylinder port and the Pilot Operated check/counter-balance valves are not permitted.
3) Filtration consistent with manufacturer's recommendations shall be used to reduce the probability of valve failure due to solid particle or oil contamination.
4) Valve may be relay or plc controlled, but the control power must come from a safety rated device.
5) To obtain optimal speed and motion control, mount the flow controls as close to the cylinders as possible, preferable using close hex nipples.
6) Line volumes shall be kept to a minimum (18" or less preferred, with 36" maximum), to optimize system stiffness. In no case shall the line volume exceed the cylinder volume. This requirement promotes an exchange of oil from the cylinder during each stroke, carrying away contamination that had entered through the rod seal.

COMPUTER GRAPHICS — CHANGES RESTRICTED NO MANUAL CHANGES

LIST DETAIL NOS. ON THIS SHEET
STAMP OR ETCH ON ALL DETAILS: DRAWING NUMBER AND DETAIL NUMBER WITH THE LATEST REVISION SYMBOL APPLICABLE TO THAT DETAIL
DO NOT SCALE DRAWING UNLESS OTHERWISE SPECIFIED: TWO PLACE DECIMALS LIMIT ±.01 INCHES; THREE PLACE DECIMALS LIMIT ±.005 INCHES; ANGULAR LIMITS ±1°; REMOVE ALL SHARP EDGES

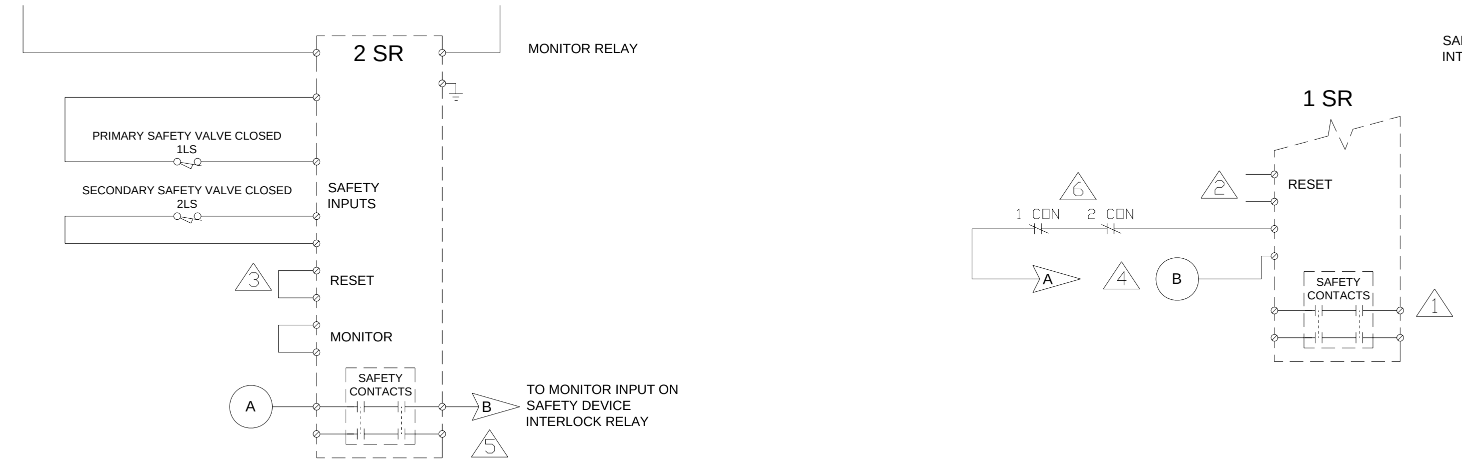
DELPHI

PART NO.	PART NO.	DESIGN APPROVED BY	DRAWN BY
PLANT –		CHECKED BY	SCALE
		DATE	DATE
SHEET NO.	NO. OF SHEETS	PREFIX – DRAWING NUMBER	
D3	–	ANNEX D	

Refer to the Specification document for detailed requirements. This drawing is not a drafting example.

Control Reliable Safety Circuit – Spool Blocking Valves, sheet D4

CONTROL RELIABLE SAFETY CIRCUIT
RISK ASSESSMENT R3C or R4
SPOOL BLOCKING VALVES

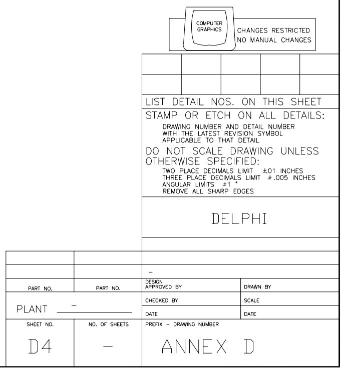


FUNCTION:
This drawing is an example that illustrates a Control Reliable safety circuit which corresponds to the risk reduction category as determined by a risk assessment for a particular machine.

Risk assessment has determined that safeguard performance meets the requirements of R3C or R4.

This circuit represents that portion of the electrical safety circuit required to control the redundant monitored spool valves used to remove hazardous energy, typically on low (<18 GPM) systems.

NOTES:
1) Safety relay 1SR removes power to the safety valves.
2) Refer to the specification for application specific reset requirements.
3) The valve monitor safety relay 2SR can be any safety relay capable of automatic reset, with no monitor input capability, and no input concurrency requirements.
4) The valve monitor safety relay 2SR monitors non positive-guided contacts from the safety valves. When the safety valves are de-energized (when power is removed by 1SR) 2SR will allow power to the reset string of 1SR.
5) Safety contacts of 2SR are wired to the monitor string of 1SR.
6) Monitor of output device auxiliary contacts.

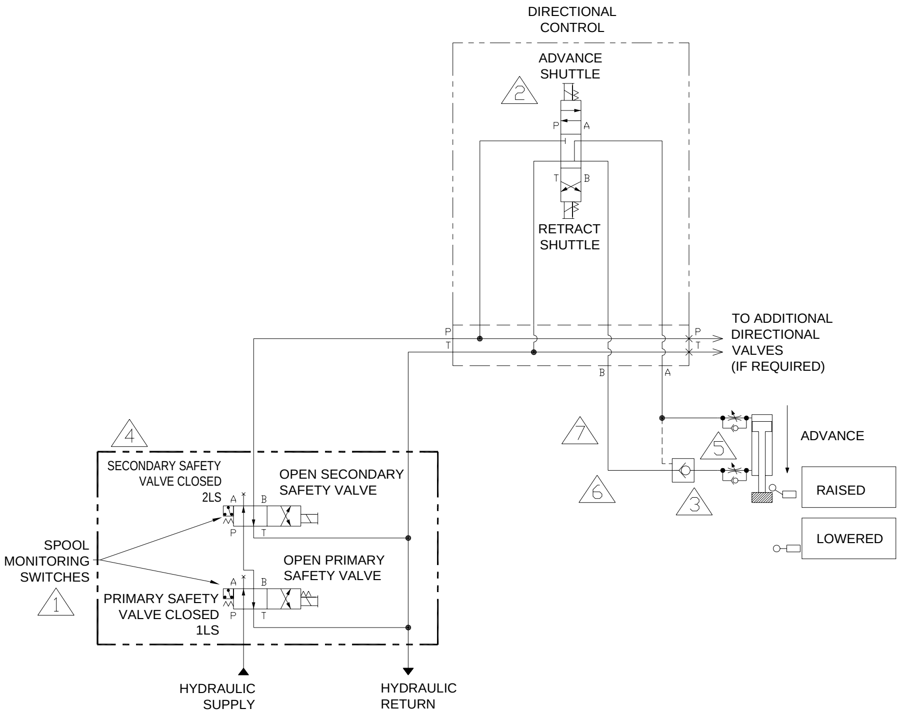


Refer to the Specification document for detailed requirements. This drawing is not a drafting example.

Control Reliable Safety Circuit – Spool Blocking Valves, sheet D5

CONTROL RELIABLE SAFETY CIRCUIT
RISK ASSESSMENT R3C or R4
SPOOL BLOCKING VALVES

HYDRAULIC



FUNCTION:
This drawing is an example that illustrates a Control Reliable safety circuit which corresponds to the risk reduction category as determined by a risk assessment for a particular machine.

Risk assessment has determined that safeguard performance meets the requirements of R3C or R4.

This circuit reflects redundant, monitored hydraulic spool style blocking valves used to remove hazardous energy, and can be used on systems with flows less than 18 GPM. The 18 gallon limitation is the maximum flow rate of a single stage DO5 series directional valve.

The motion valve may be relay or PLC controlled, but the control power must come from a safety rated device. The control power for the blocking valves must come from a safety rated device.

NOTES:
1) The safety circuit blocking valves are conventional spool style valves with an optional spool-monitoring switch indicating that the valves are in the de-engergized position.
2) PLC outputs may be used to control the directional valves provided that the output card receives its power from the electrical safety circuit. Directional control valve spool configuration and additional controls are application specific. Caution! Detented and spring offset valves that were de-energized with the actuator in mid-position, will either continue their motion, or retract to the home direction, when the safety circuit and corresponding blocking valves are reset. Normally this is not a concern due to the fact that the operator must be out of the safety device during the reset, but it is an item that must be considered during the risk assessment.
3) The hydraulic circuit may require additional controls to provide for safe operation. For example, on a vertical cylinder a counter-balance valve or P.O. check will be required. When flexible lines are used due to actuator motion, these valves shall be installed directly at the cylinder port. Flexible lines between the cylinder port and the P.O. check/counter balance valve are not permitted.
4) Blocking valves shall be mounted with their spools in a horizontal plane to prevent inadvertent shift due to spring breakage and gravity. This also prevents premature coil failure due to water build-up around the coil, or around the spring end cap.
5) To obtain optimal speed and motion control, mount the flow controls as close to the cylinders as possible, preferable using close hex nipples.
6) Line volumes shall be kept to a minimum (18" or less preferred, with 36" maximum), to optimize system stiffness. In no case shall the line volume exceed the cylinder volume. This requirement promotes an exchange of oil from the cylinder during each stroke, carrying away contamination that had entered through the rod seal.
7) Line diameters and components are to be sized to promote efficient operation. Excessive oversizing of components is not permitted as it adds initial and long-term operational costs.

Refer to the Specification document for detailed requirements. This drawing is not a drafting example.

REVISIONS

REV. SYM.	DET.	CHANGE				

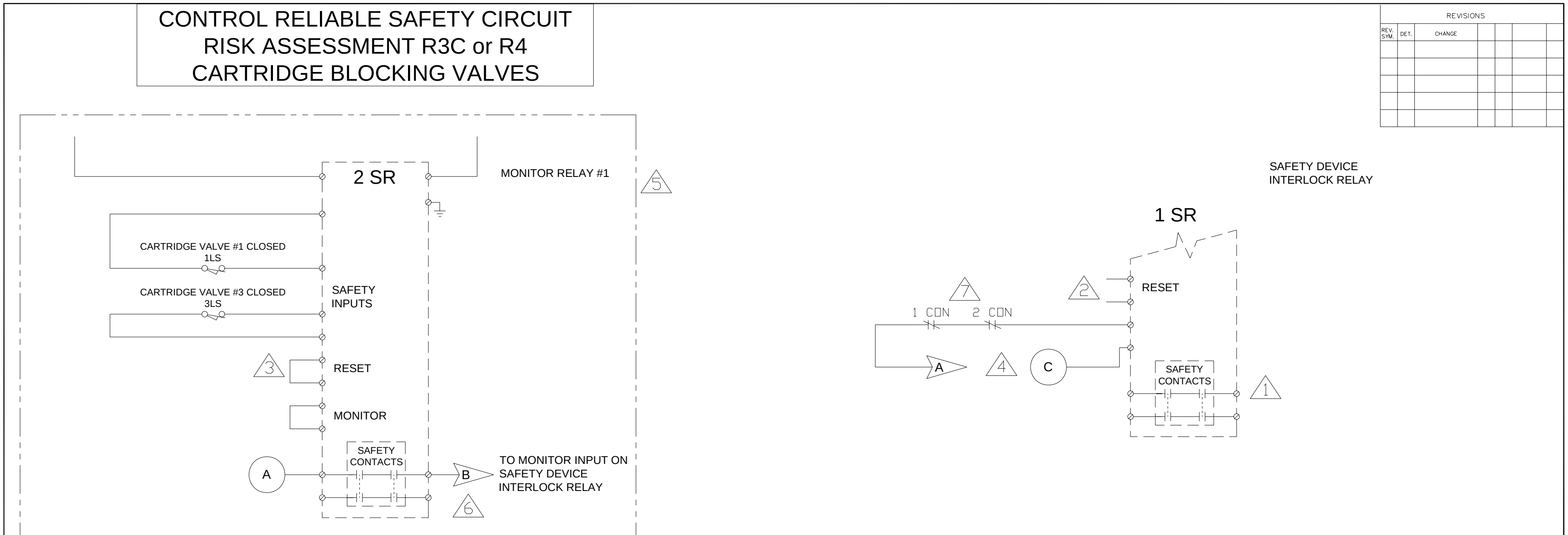
CHANGES RESTRICTED NO MANUAL CHANGES

LIST DETAIL NOS. ON THIS SHEET
STAMP OR ETCH ON ALL DETAILS: DRAWING NUMBER AND DETAIL NUMBER WITH THE LATEST REVISION SYMBOL APPLICABLE TO THAT DETAIL
DO NOT SCALE DRAWING UNLESS OTHERWISE SPECIFIED: TWO PLACE DECIMALS LIMIT ±.01 INCHES; THREE PLACE DECIMALS LIMIT ±.005 INCHES; ANGULAR LIMITS ±1°; REMOVE ALL SHARP EDGES

DELPHI

PART NO.	PART NO.	DESIGN APPROVED BY	DRAWN BY
PLANT –		CHECKED BY	SCALE
		DATE	DATE
SHEET NO.	NO. OF SHEETS	PREFIX – DRAWING NUMBER	
D5	–	ANNEX D	

Control Reliable Safety Circuit – Cartridge Blocking Valves, sheet D6

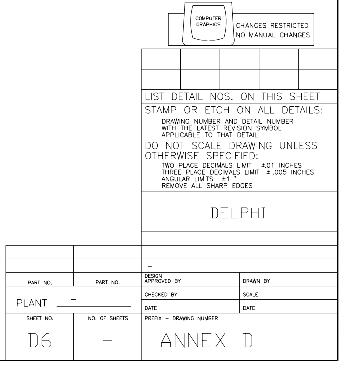


FUNCTION:
This drawing is an example that illustrates a Control Reliable safety circuit which corresponds to the risk reduction category as determined by a risk assessment for a particular machine.

Risk assessment has determined that safeguard performance meets the requirements of R3C or R4.

This circuit represents that portion of the electrical safety circuit required to control the redundant monitored cartridge valves used to remove hazardous energy, typically on high GPM systems.

NOTES:
1) Safety relay 1SR removes power to the pilot control safety valves (SOL1 & 2).
2) Refer to the specification for application specific reset requirements.
3) The valve monitor safety relay 2SR and 3SR can be any safety relay capable of automatic reset, with no monitor input capability, and no input concurrency requirements.
4) The valve monitor safety relay 2SR and 3SR do not work in conjunction with each other during normal advancing and retracting of the cylinder. When all solenoids are de-energized (when power is removed by 1SR) both 2SR and 3SR will allow power to the reset string of 1SR.
5) The circuits inside this box provides the monitoring function.
6) Safety contacts of 2SR and 3SR are wired in series to the monitor string of 1SR.
7) Monitor of output device auxiliary contacts.



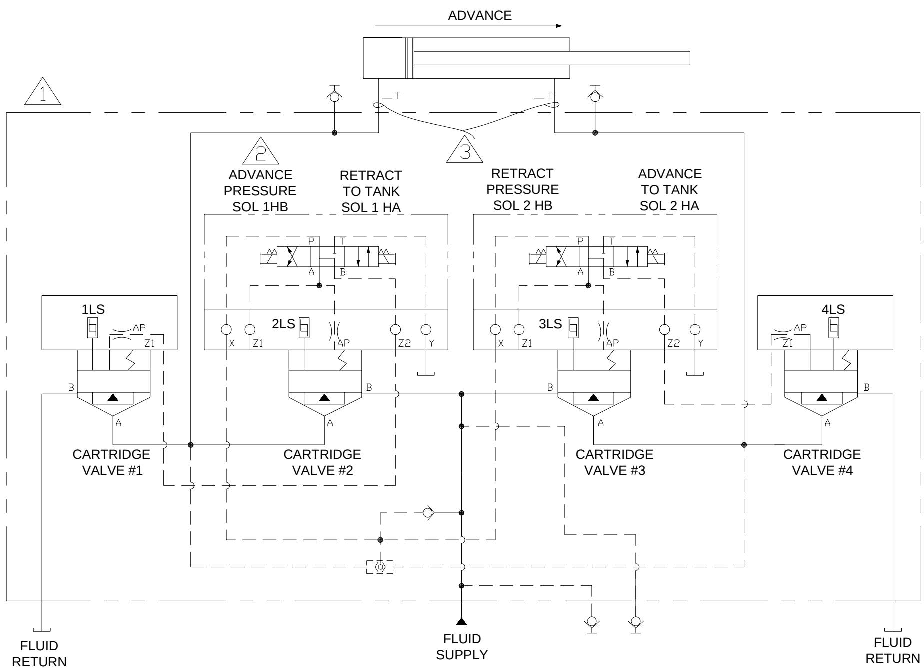
Refer to the Specification document for detailed requirements. This drawing is not a drafting example.

Control Reliable Safety Circuit – Cartridge Blocking Valves, sheet D7

CONTROL RELIABLE SAFETY CIRCUIT
RISK ASSESSMENT R4
CARTRIDGE BLOCKING VALVES

REVISIONS		
REV. SYM.	DET.	CHANGE

HYDRAULIC



SWITCH & SOLENOID CHART

SOL/SW	1HB	1HA	2HB	2HA	1LS	2LS	3LS	4LS
ADVANCE CYL.	X	0	0	X	X	0	X	0
RETRACT CYL.	0	X	X	0	0	X	0	X
ADVANCE REGEN.	X	0	X	0	X	0	0	X
STOP	0	0	0	0	X	X	X	X

1LS	CARTRIDGE VALVE #1 CLOSED
2LS	CARTRIDGE VALVE #2 CLOSED
3LS	CARTRIDGE VALVE #3 CLOSED
4LS	CARTRIDGE VALVE #4 CLOSED

Refer to the Specification document for detailed requirements. This drawing is not a drafting example.

FUNCTION:
This drawing is an example that illustrates a Control Reliable safety circuit which corresponds to the risk reduction category as determined by a risk assessment for a particular machine.

Risk assessment has determined that safeguard performance meets the requirements of R3C and R4.

This circuit reflects redundant, monitored hydraulic pilot control and piloted cartridge valves used to remove hazardous energy, and can be used on systems with flows higher than 18 GPM.

NOTES:
1) The valves within the box are the safety circuit blocking valves and directional control valves. These blocking valves are conventional cartridge style valves with an optional solid state PNP spool-monitoring switch indicating the valve is closed.
2) PLC outputs may be used for directional control of the cartridge valves provided that the output card receives its power from the electrical safety circuit.
3) The hydraulic circuit may require additional controls to provide for safe operation. For example, on a vertical cylinder, a counter-balance valve or P.O. check will be required. These valves shall be mounted directly at the cylinder port. Flexible lines between the cylinder port and the Pilot Operated check/counter-balance valves are not permitted.

COMPUTER GRAPHICS — CHANGES RESTRICTED NO MANUAL CHANGES

LIST DETAIL NOS. ON THIS SHEET
STAMP OR ETCH ON ALL DETAILS:
DRAWING NUMBER AND DETAIL NUMBER WITH THE LATEST REVISION SYMBOL APPLICABLE TO THAT DETAIL
DO NOT SCALE DRAWING UNLESS OTHERWISE SPECIFIED:
TWO PLACE DECIMALS LIMIT ±.01 INCHES
THREE PLACE DECIMALS LIMIT ±.005 INCHES
ANGULAR LIMITS ±1°
REMOVE ALL SHARP EDGES

DELPHI

PART NO.	PART NO.	DESIGN APPROVED BY	DRAWN BY
PLANT –		CHECKED BY	SCALE
		DATE	DATE
SHEET NO.	NO. OF SHEETS	PREFIX – DRAWING NUMBER	
D7	–	ANNEX D	

E Annex E: Safety Circuit Performance Requirements

Delphi	ISO13849-1 (EN954-1)	Interpretation of Circuit Requirements
Simple (3.5.5.1)	Category B	Control as per basic specifications.
Single Channel (3.5.5.2)	Category 1	Use of well-tried and tested components and principles.
Single Channel w/ Monitoring (3.5.5.3)	Category 2	Safety function shall be tested/checked at suitable intervals (frequency determined according to application). Single fault may cause the loss of the safety function.
Control Reliable (3.5.5.4)	Category 3	A single fault must not cause the loss of the safety function. The fault should be detected whenever reasonably practicable. An accumulation of faults may cause the loss of the safety function.
	Category 4	A single fault must not cause the loss of the safety function. The fault shall be detected at or before the next demand of the safety function. An accumulation of faults must not cause the loss of the safety function.

Notes:

1. The above information is derived from Table 3, page 8, ANSI B11.TR4, 2004.
2. The ANSI B11 series of machine tool safety standards include a note within an explanatory annex stating that control reliability for machine tools is not directly comparable to the requirements of ISO 13849-1 and exceed a Category 2.
3. The Delphi task based risk assessment process is based on the robot risk assessment per ANSI/RIA R15.06. Further, ANSI/RIA R15.06 (clause 4.5) includes a note that states that the ISO 13849-1 Categories are different from the performance criteria within R15.06, and exceed Categories B, 1, 2, and 3. Control reliability for robots typically exceeds a Category 3, but is not necessarily intended to be a Category 4. Circuits that are “dual channel with monitoring” and safeguarding devices with dual safety outputs that are certified for Category 3 usage, such as safety mats and area scanners, are generally accepted for use in robot applications that require Control Reliable safety performance, as defined in that standard.

F Annex F IEC Figures

Figure 5.2.1 Example Safety Circuit

Return

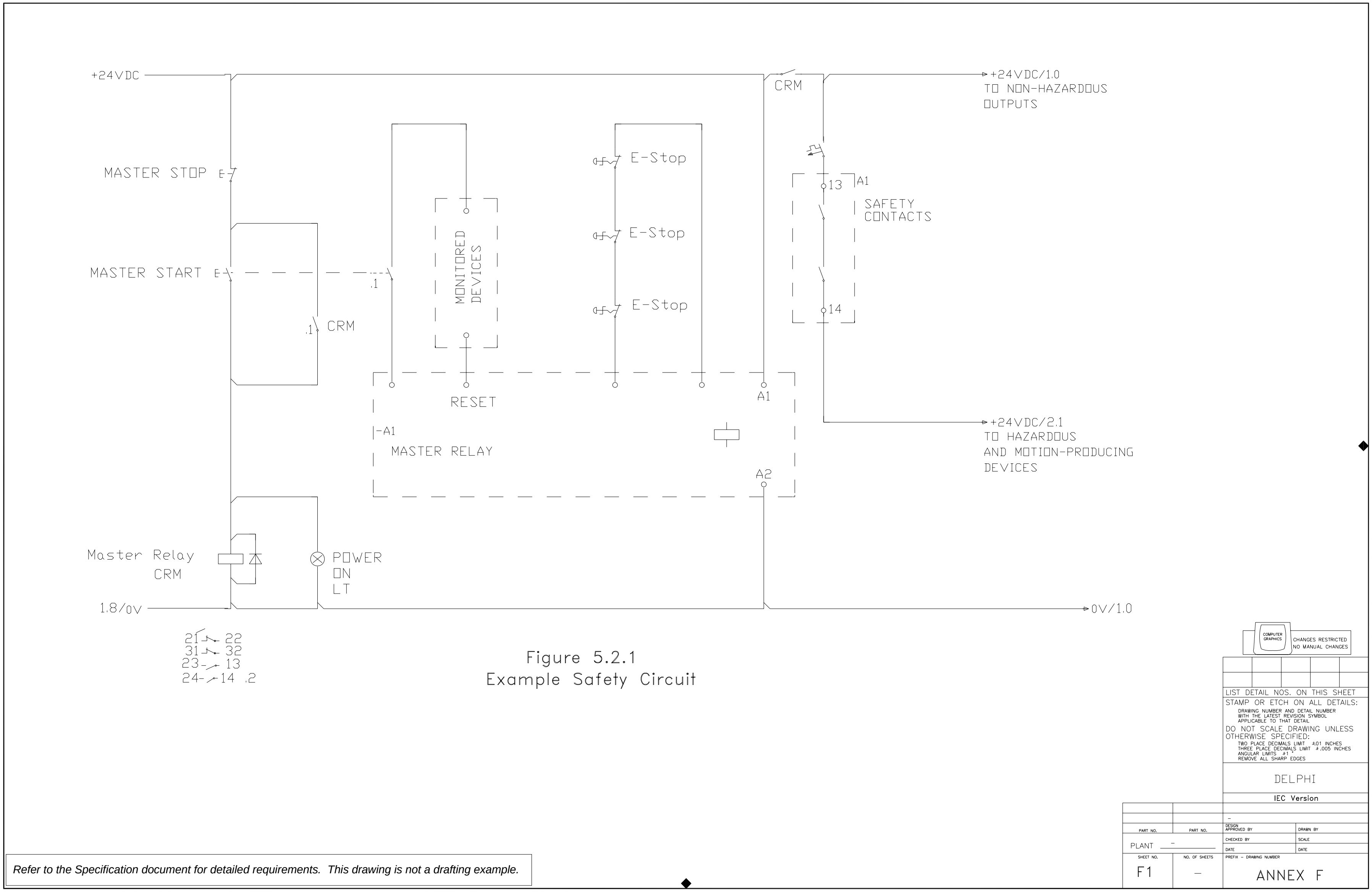


Figure 5.2.3 Master Relay as a Safety Relay

Return

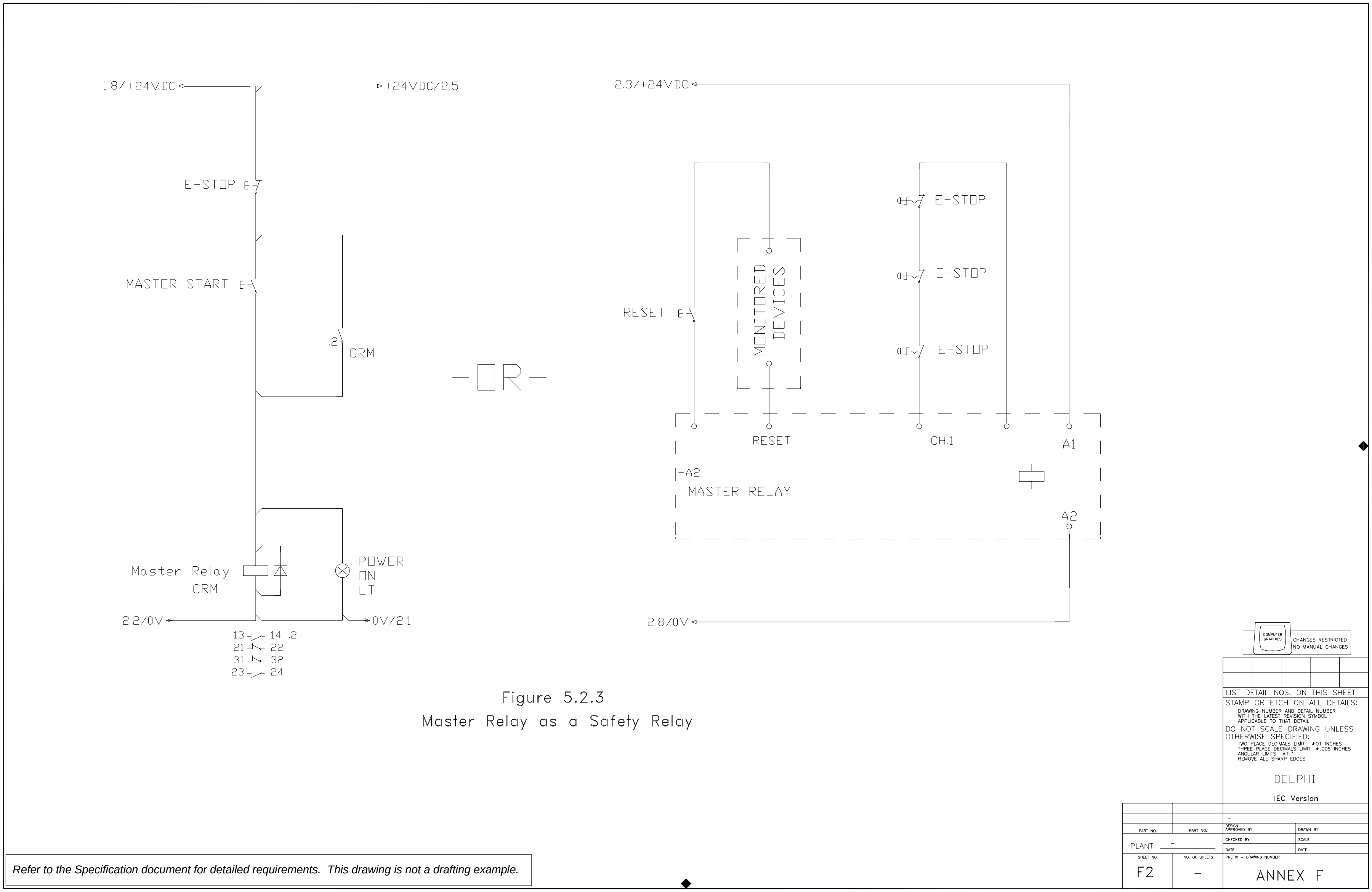


Figure 5.3.1 Multiple Safety Devices [Return]

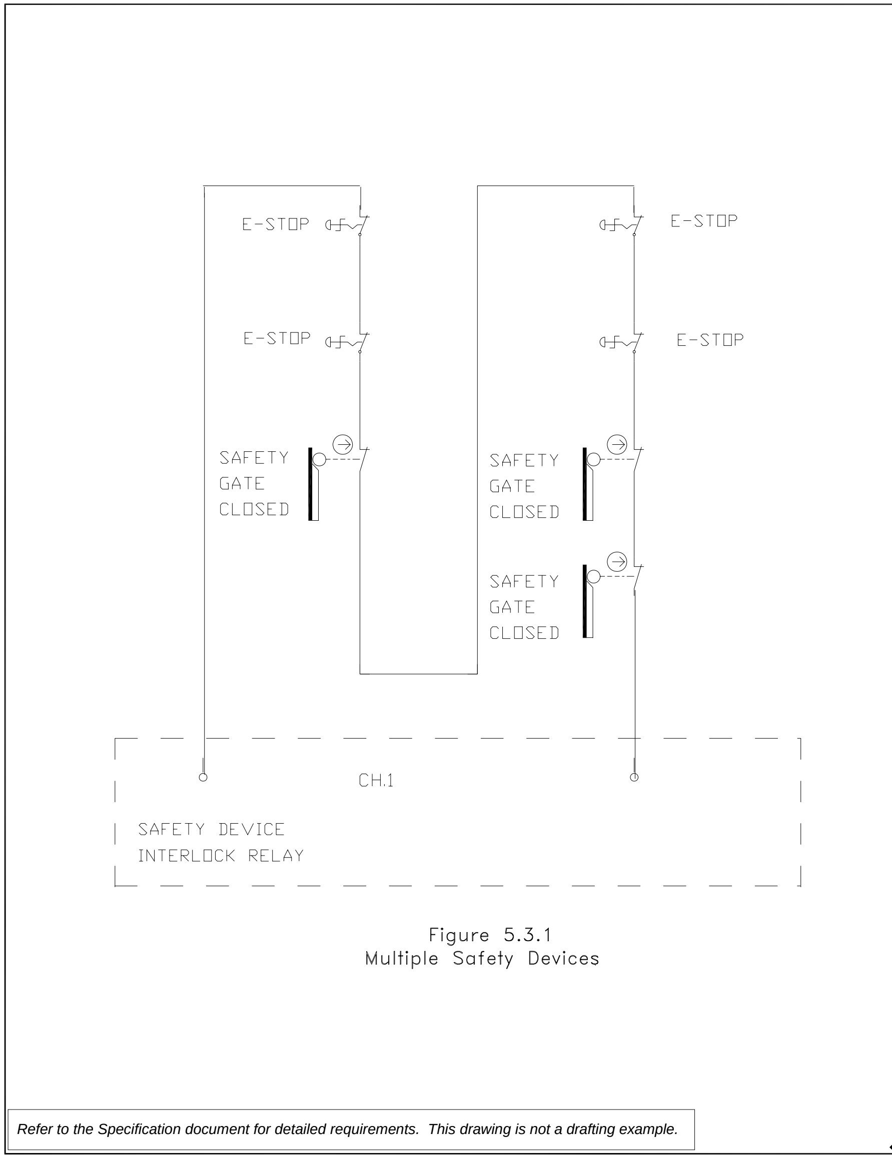


Figure 5.4.1 Safety Contact Protection [Return]

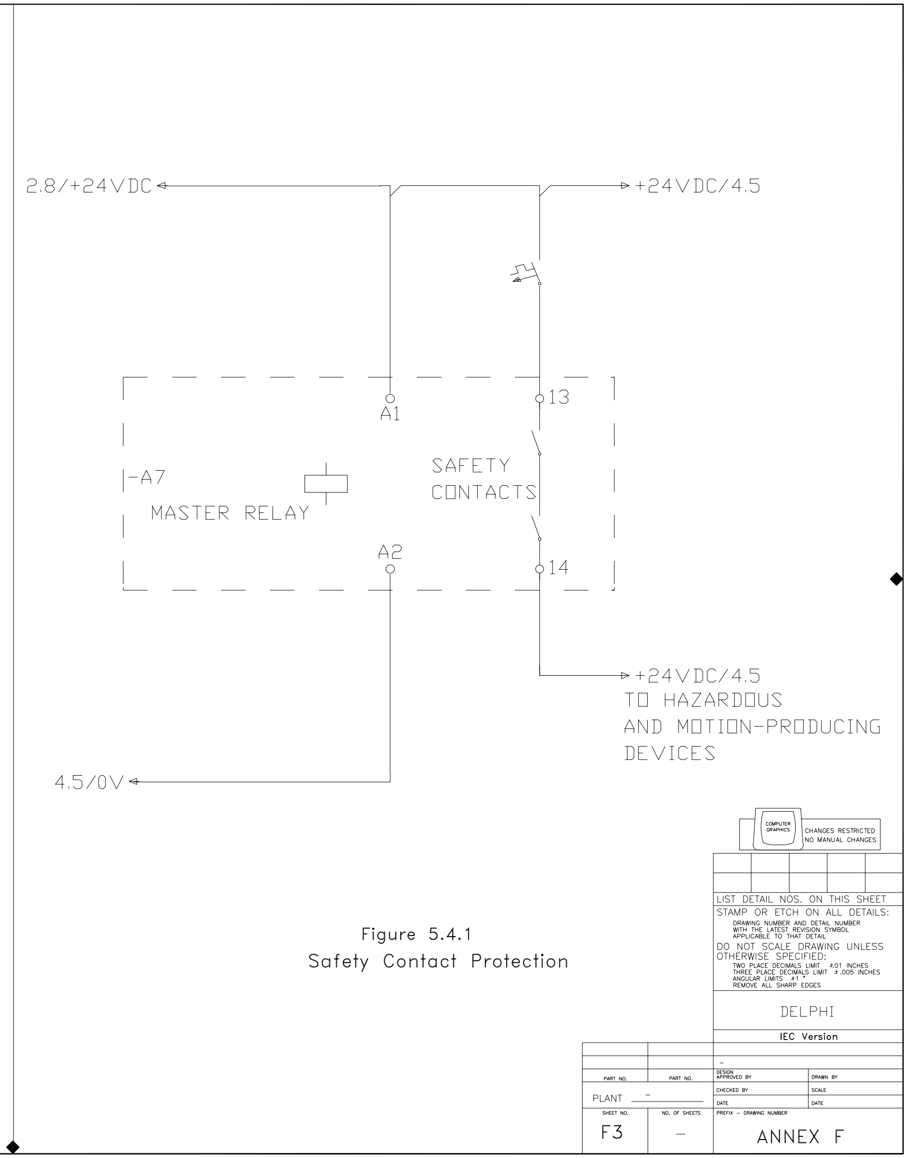


Figure 5.4.2 Additional Safety Circuit Contacts [Return]

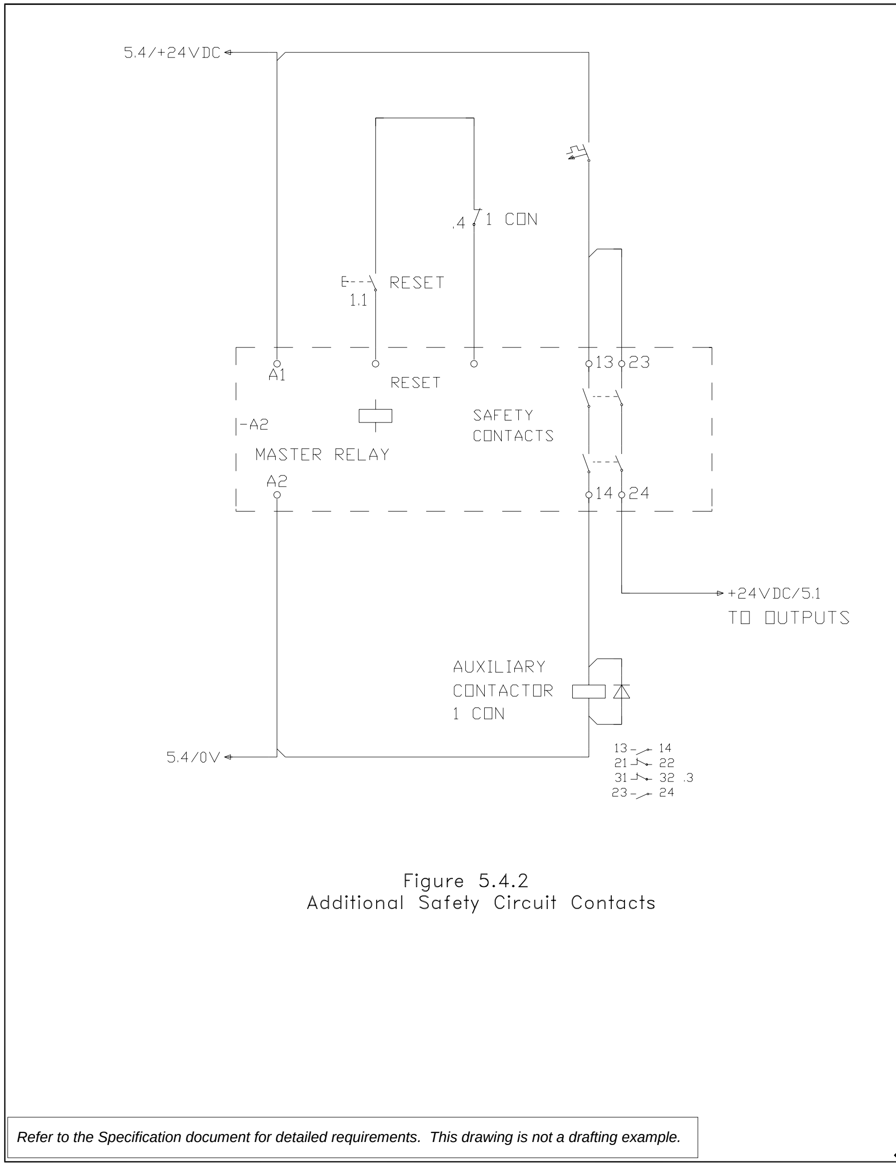


Figure 5.4.4 Multiple Safety Circuits Contacts [Return]

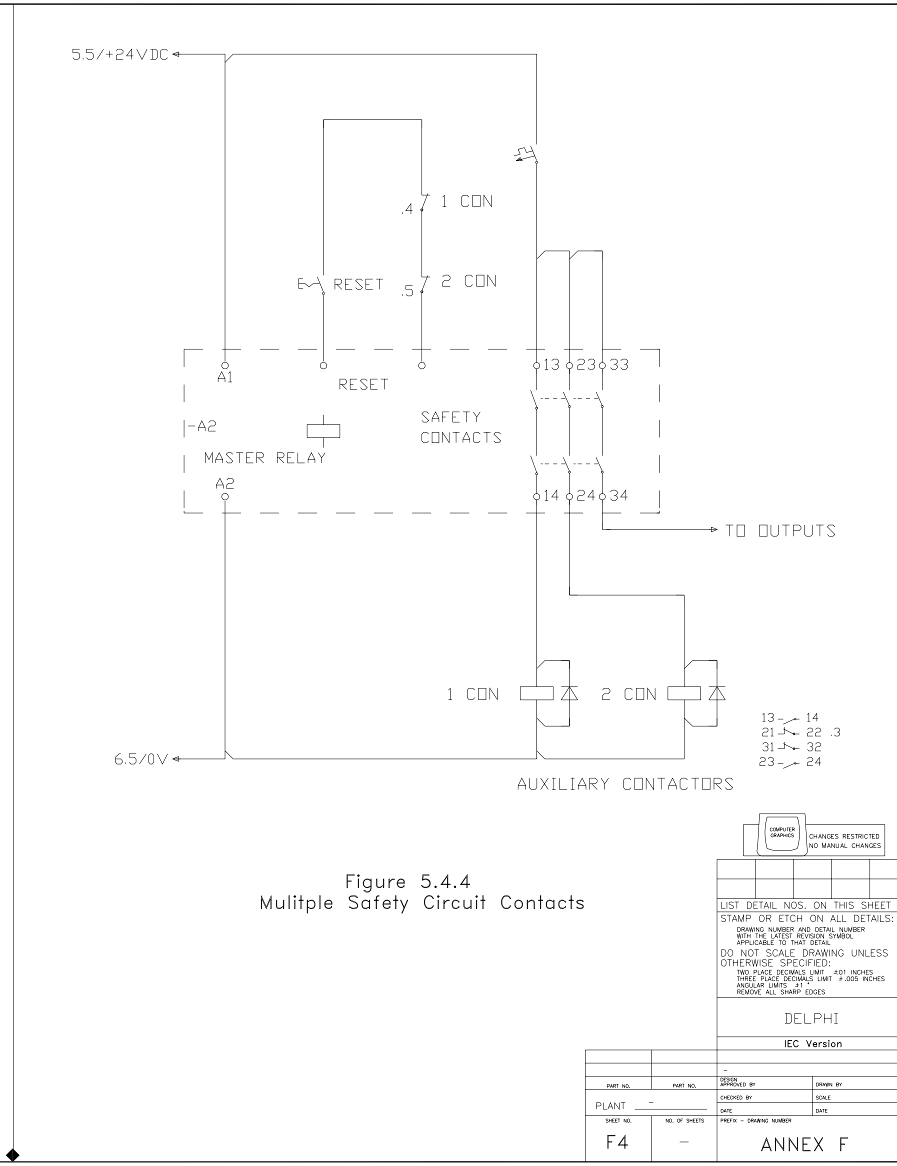
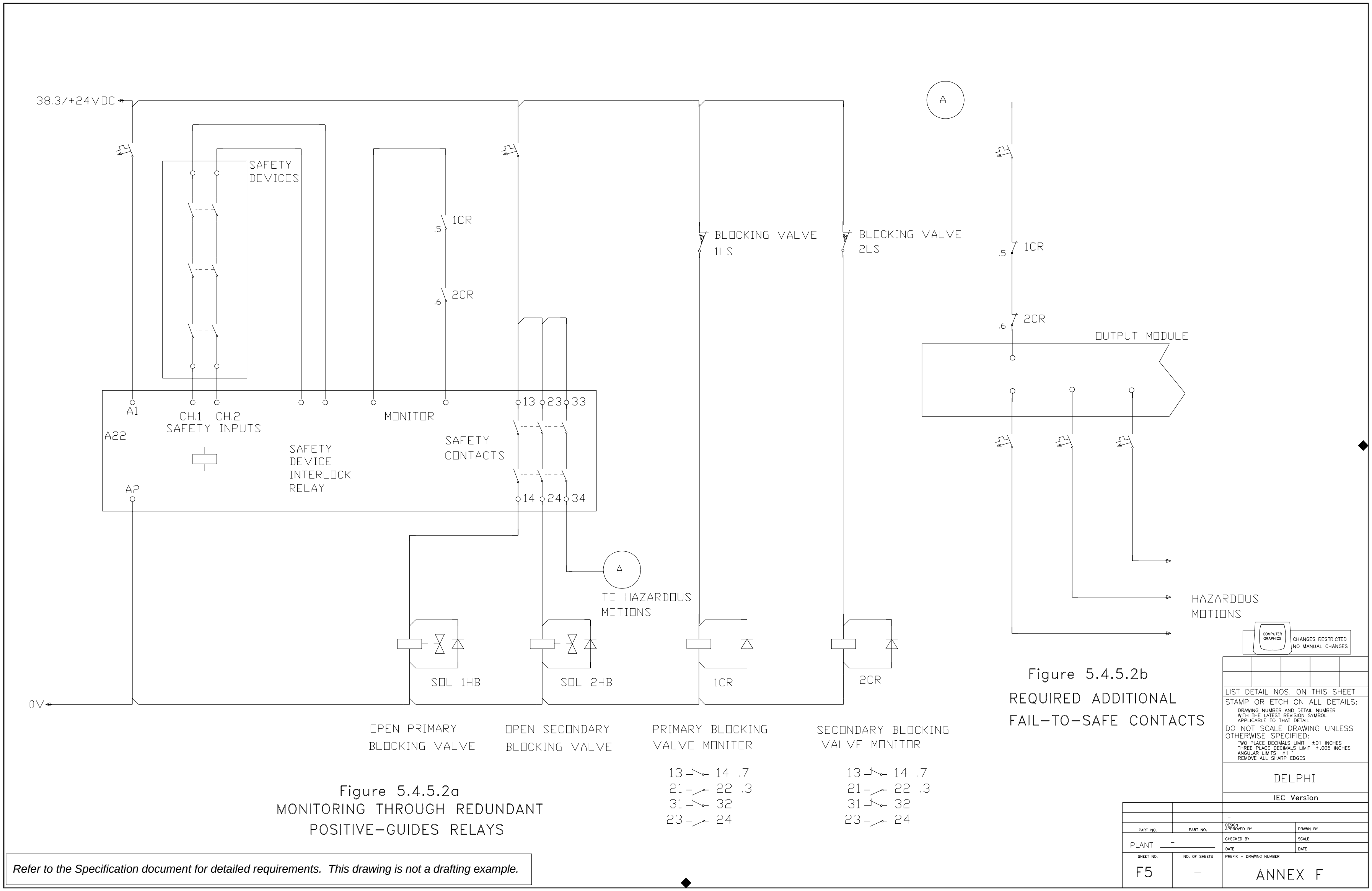


Figure 5.4.5.2a – Monitoring through redundant positive-guided relays Return

Figure 5.4.5.2b – Required additional fail-to-safe contacts Return



`

Figure 5.5.1 – Muting a Safety Device

Return

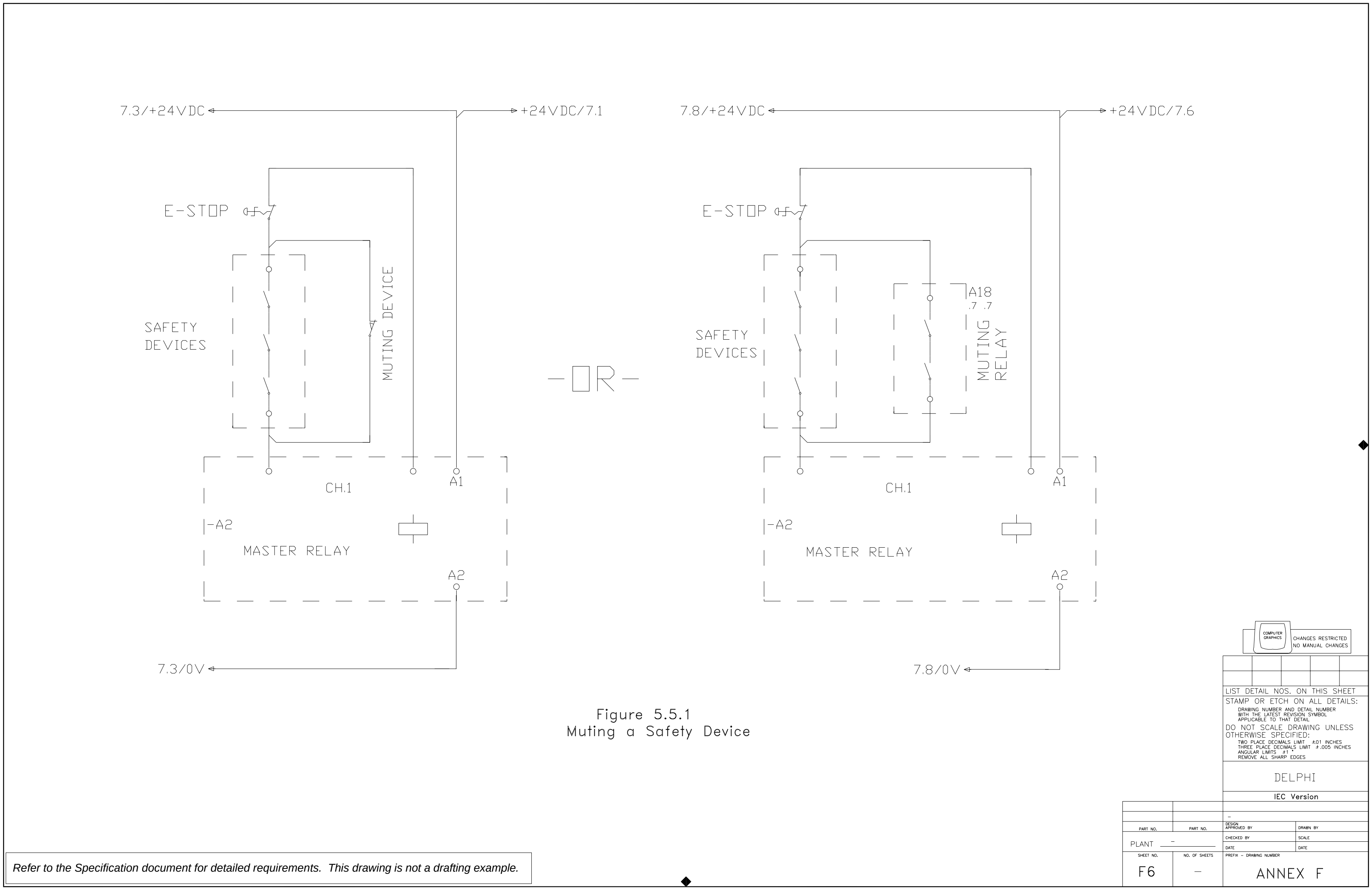


Figure 5.5.5a – Muting a Safety Device with a Safety Relay Return

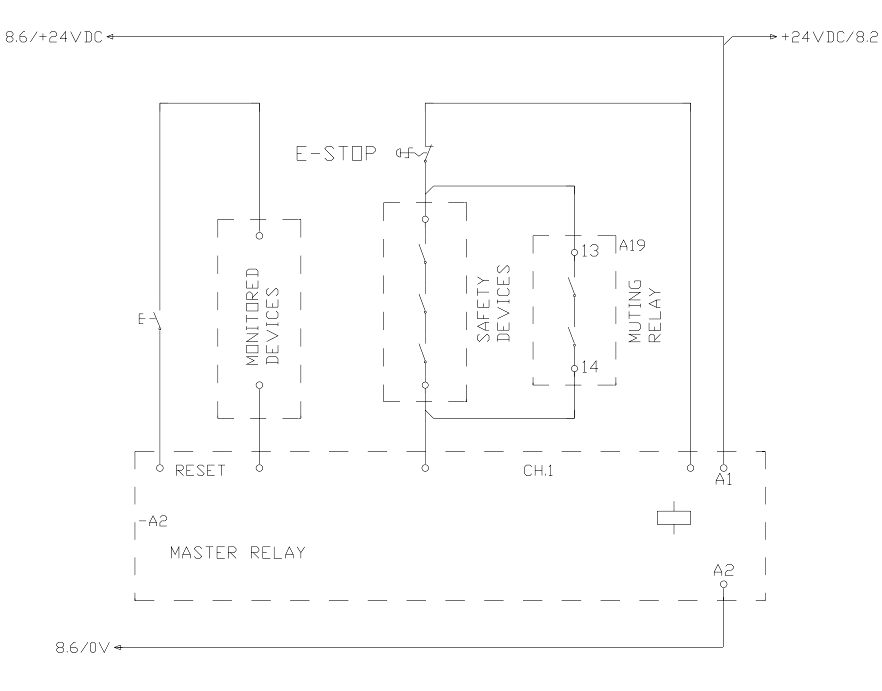


Figure 5.5.5a
Muting a Safety Device With a Safety Relay

Refer to the Specification document for detailed requirements. This drawing is not a drafting example.

Figure 5.5.5b Muting Relay Return

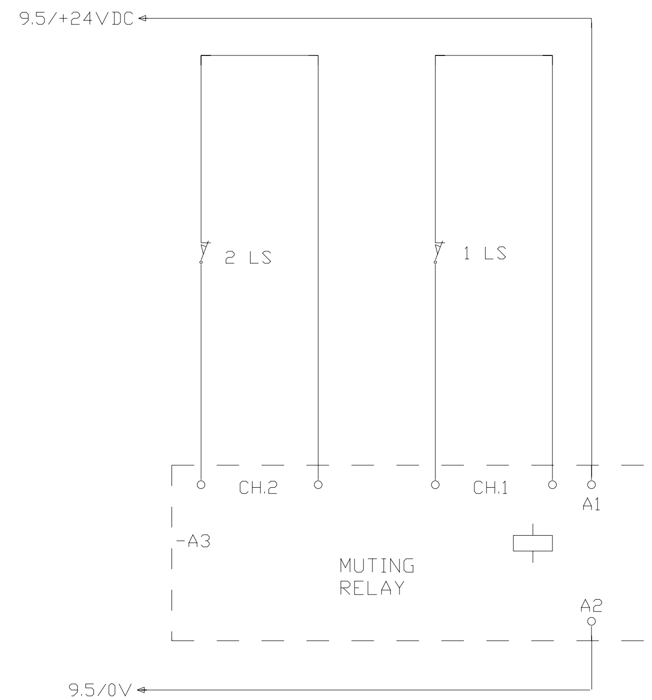


Figure 5.5.5b
Muting Relay

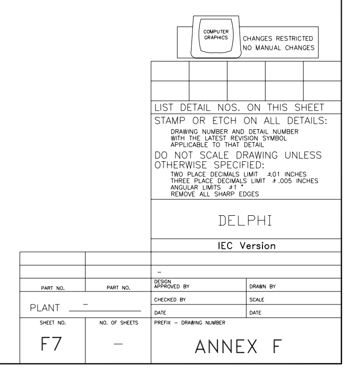


Figure 5.5.5c Muting a Safety Device in a Control Reliable Circuit

[Return]

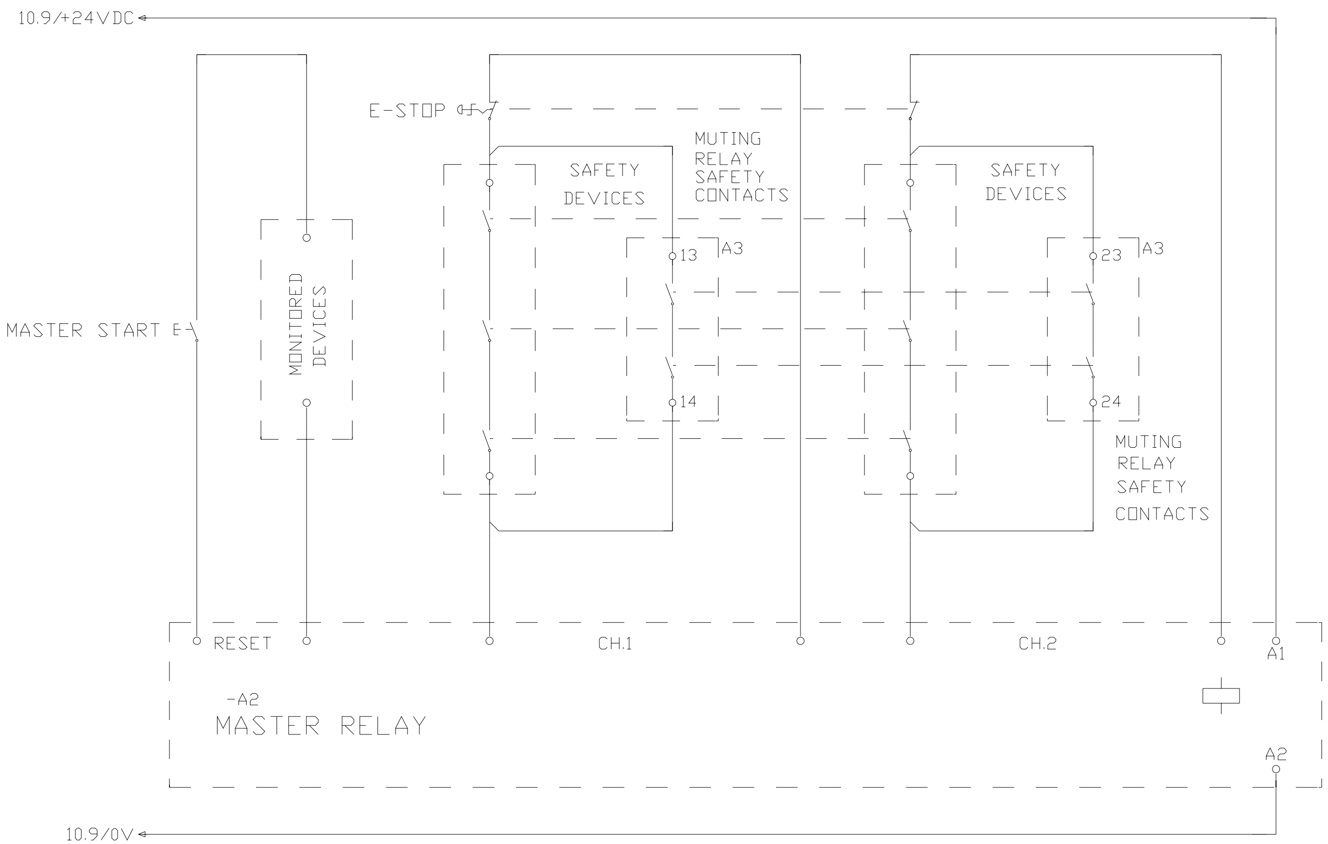


Figure 5.5.5c
Muting a Safety Device in a Control Reliable Circuit

Refer to the Specification document for detailed requirements. This drawing is not a drafting example.

CHANGES RESTRICTED
NO MANUAL CHANGES

LIST DETAIL NOS. ON THIS SHEET
STAMP OR ETCH ON ALL DETAILS:
DRAWING NUMBER AND DETAIL NUMBER WITH THE LATEST REVISION SYMBOL APPLICABLE TO THAT DETAIL
DO NOT SCALE DRAWING UNLESS OTHERWISE SPECIFIED:
TWO PLACE DECIMALS LIMIT ±.01 INCHES
THREE PLACE DECIMALS LIMIT ±.005 INCHES
ANGULAR LIMITS ±1°
REMOVE ALL SHARP EDGES

DELPHI
IEC Version

PART NO.	PART NO.	DESIGN APPROVED BY	DRAWN BY
PLANT –		CHECKED BY	SCALE
		DATE	DATE
SHEET NO.	NO. OF SHEETS	PREFIX – DRAWING NUMBER	
F8	–	ANNEX F	

Figure 5.5.6a Additional PLC Muting – single Channel Return

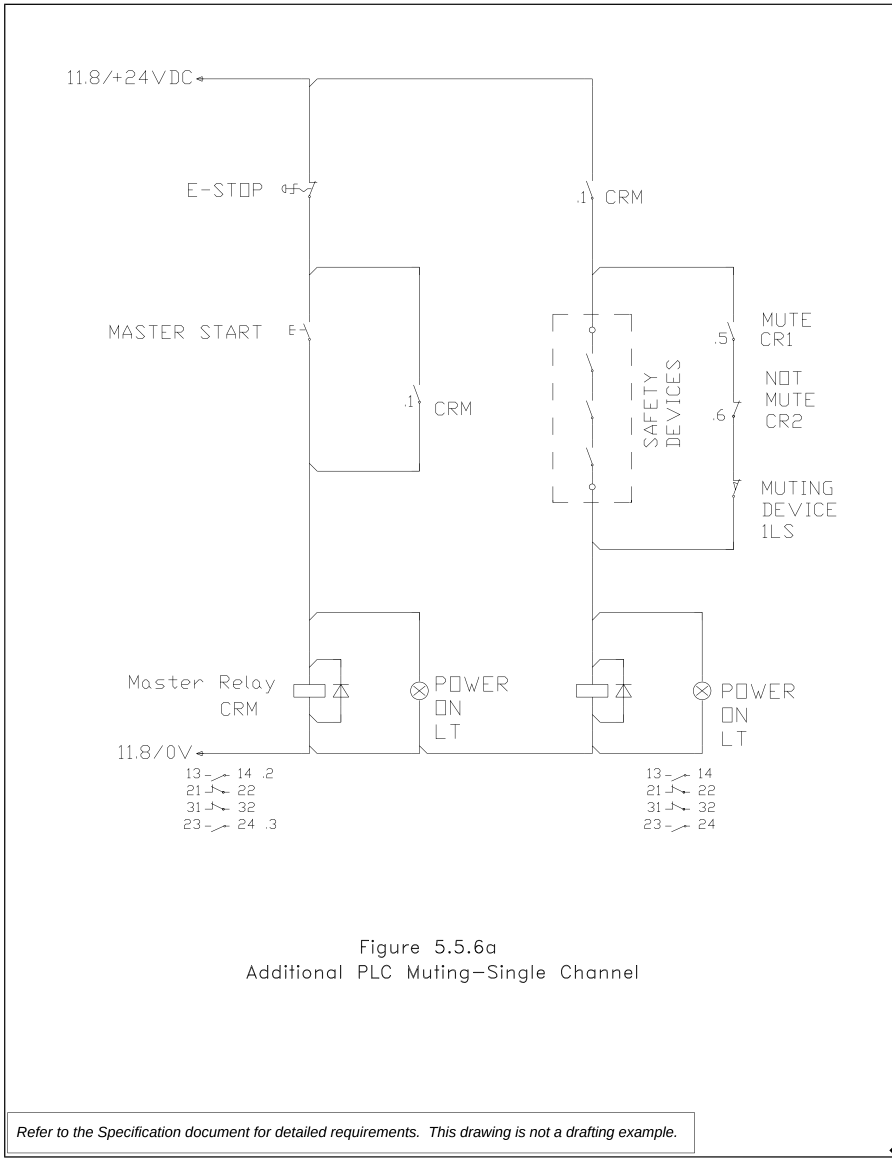


Figure 5.5.6b PLC Mute Relays Return

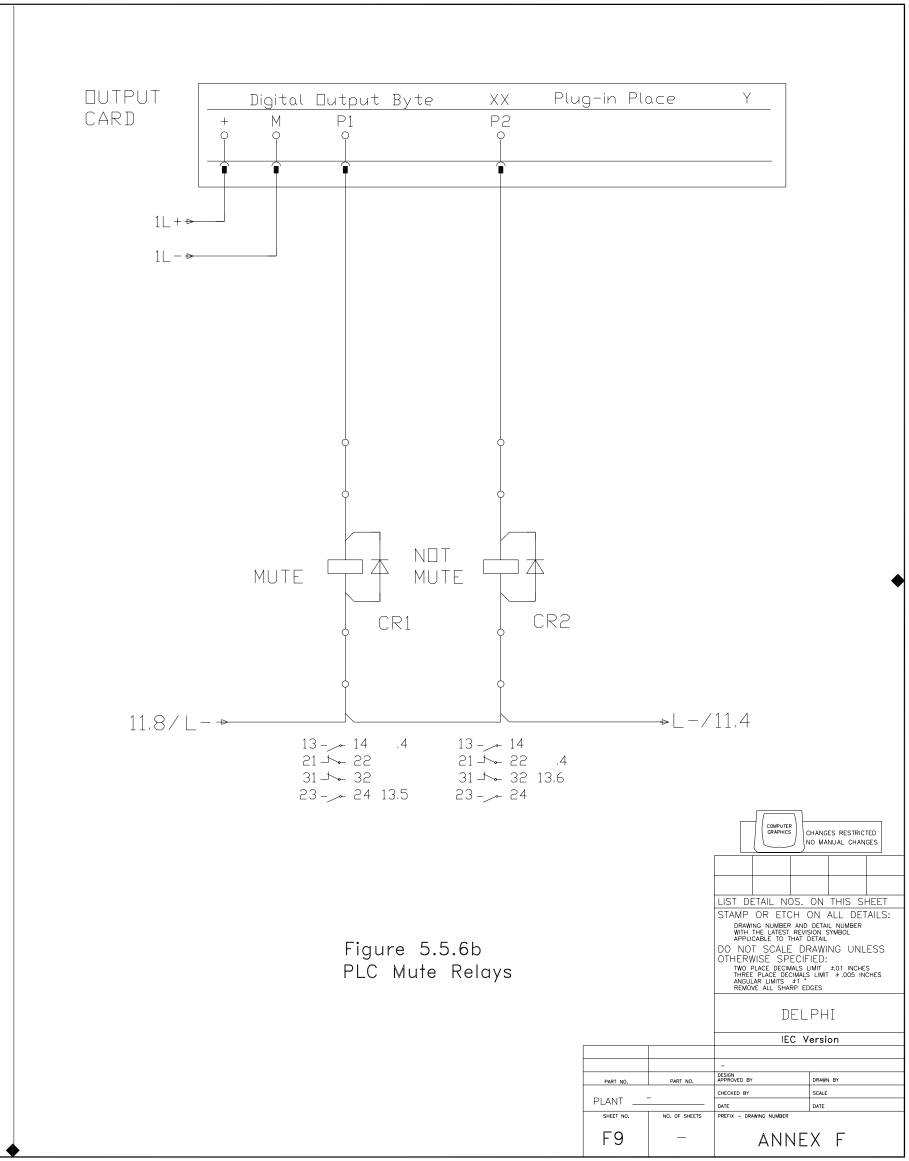


Figure 5.5.6d PLC-Relays Muting Return

Figure 5.5.6e Additional PLC Muting Single Channel with Monitoring Return

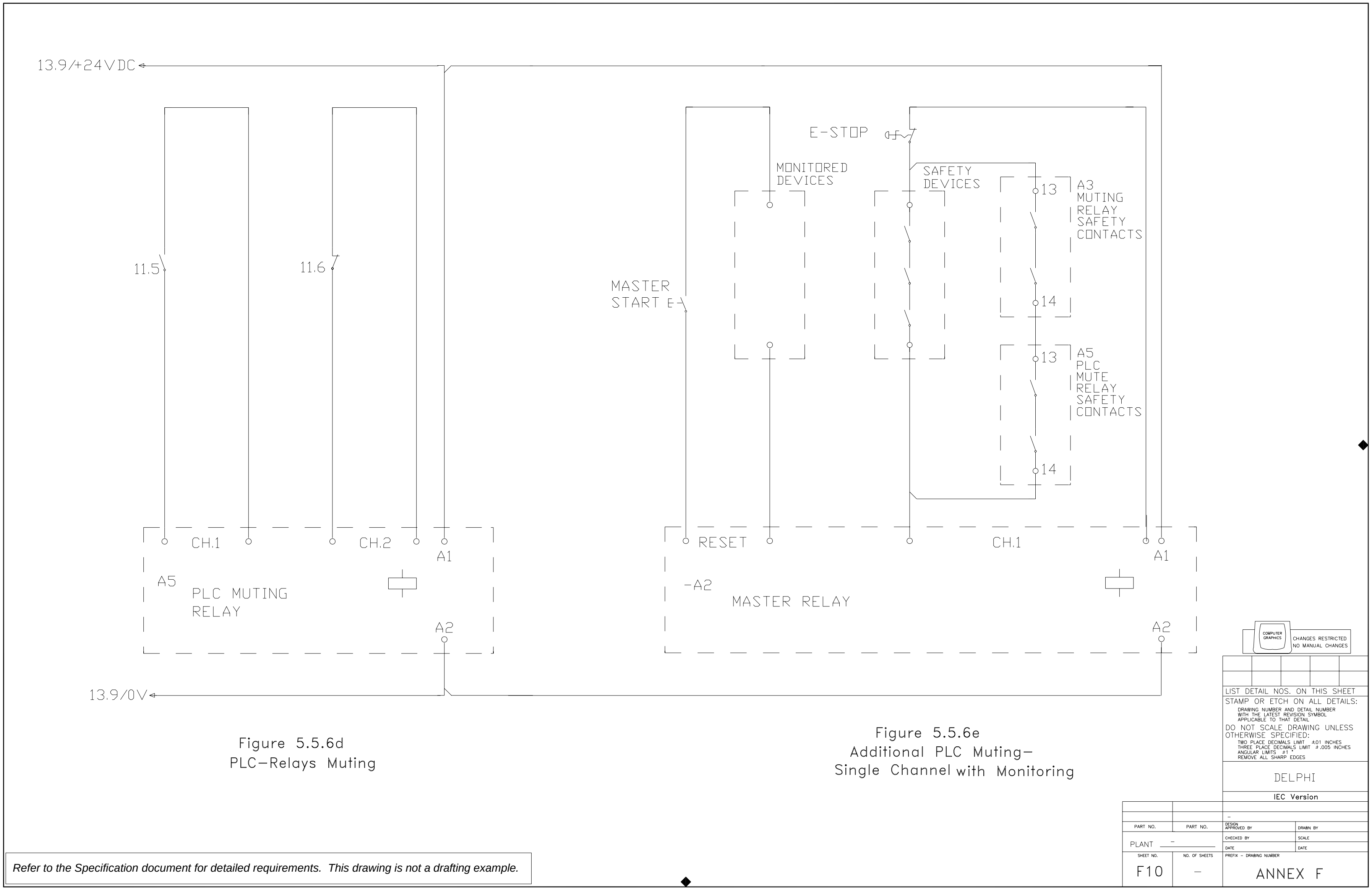


Figure 5.5.6f Additional PLC Muting – Control Reliable

[Return](#)

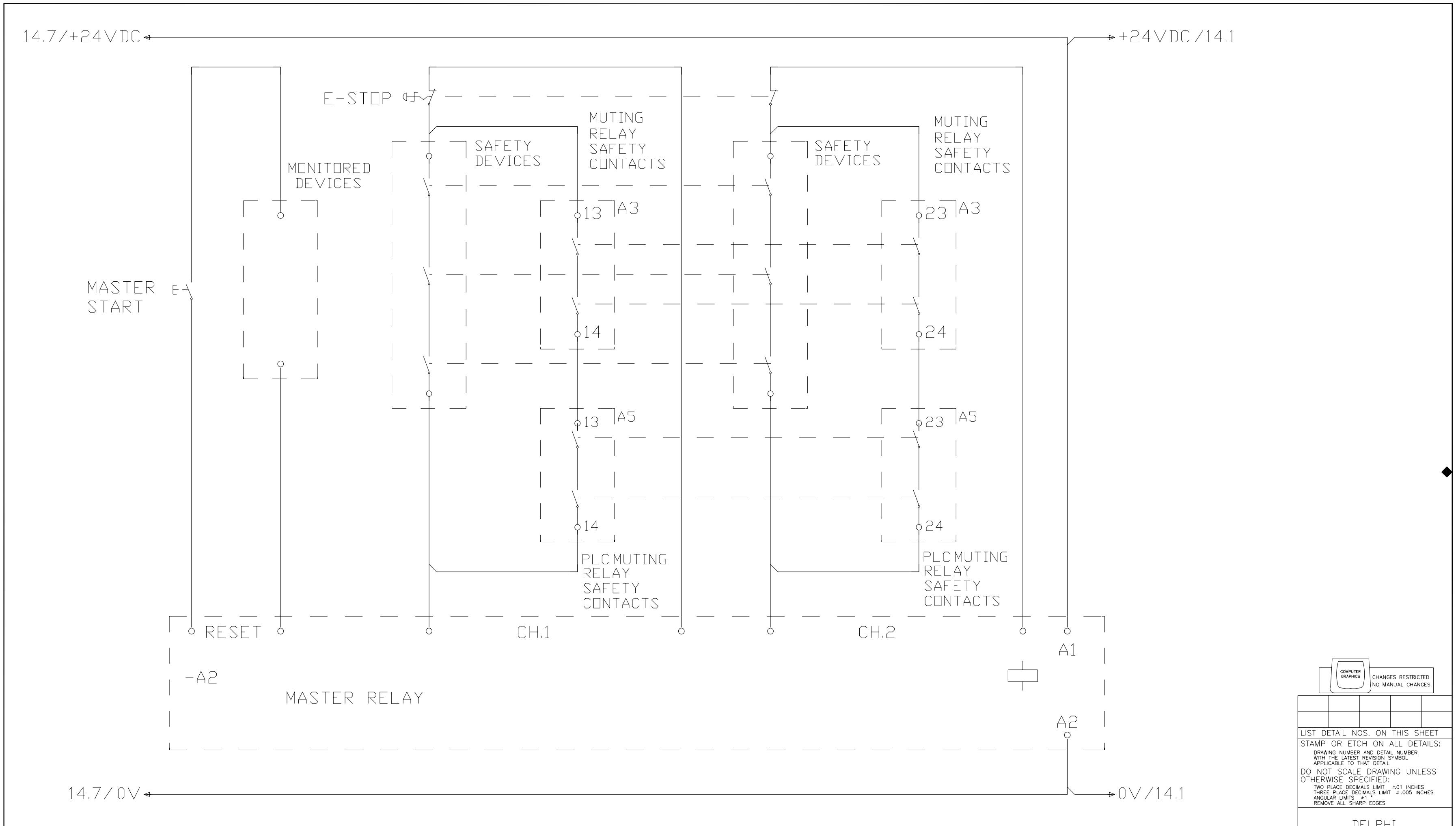


Figure 5.5.6f
Additional PLC Muting–Control Reliable

Refer to the Specification document for detailed requirements. This drawing is not a drafting example.

Figure 5.6.2 – Manual Enable for Two Hand Control - Control Reliable

[Return]

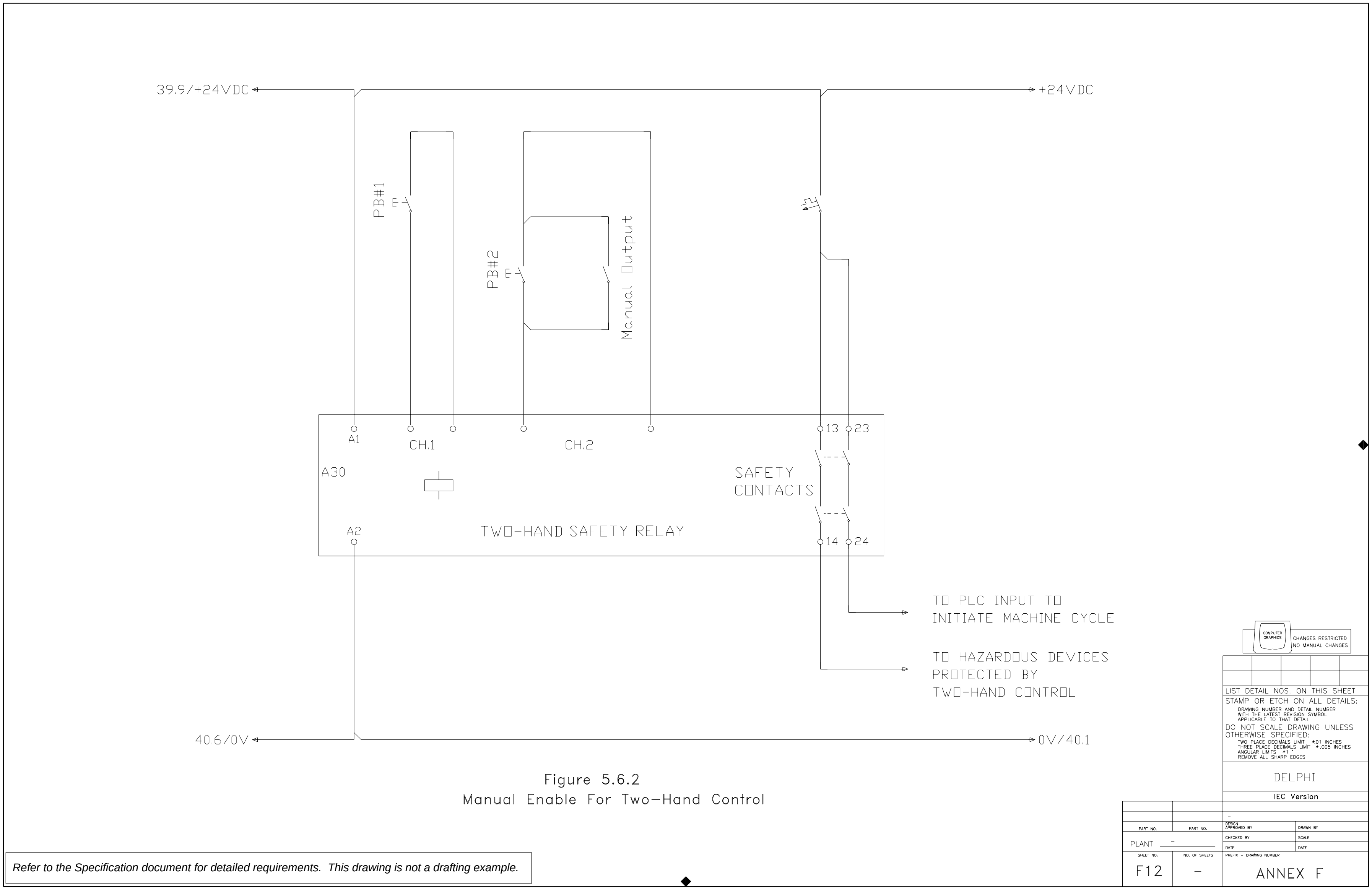


Figure 5.7.1 – Single Channel E-Stop

Return

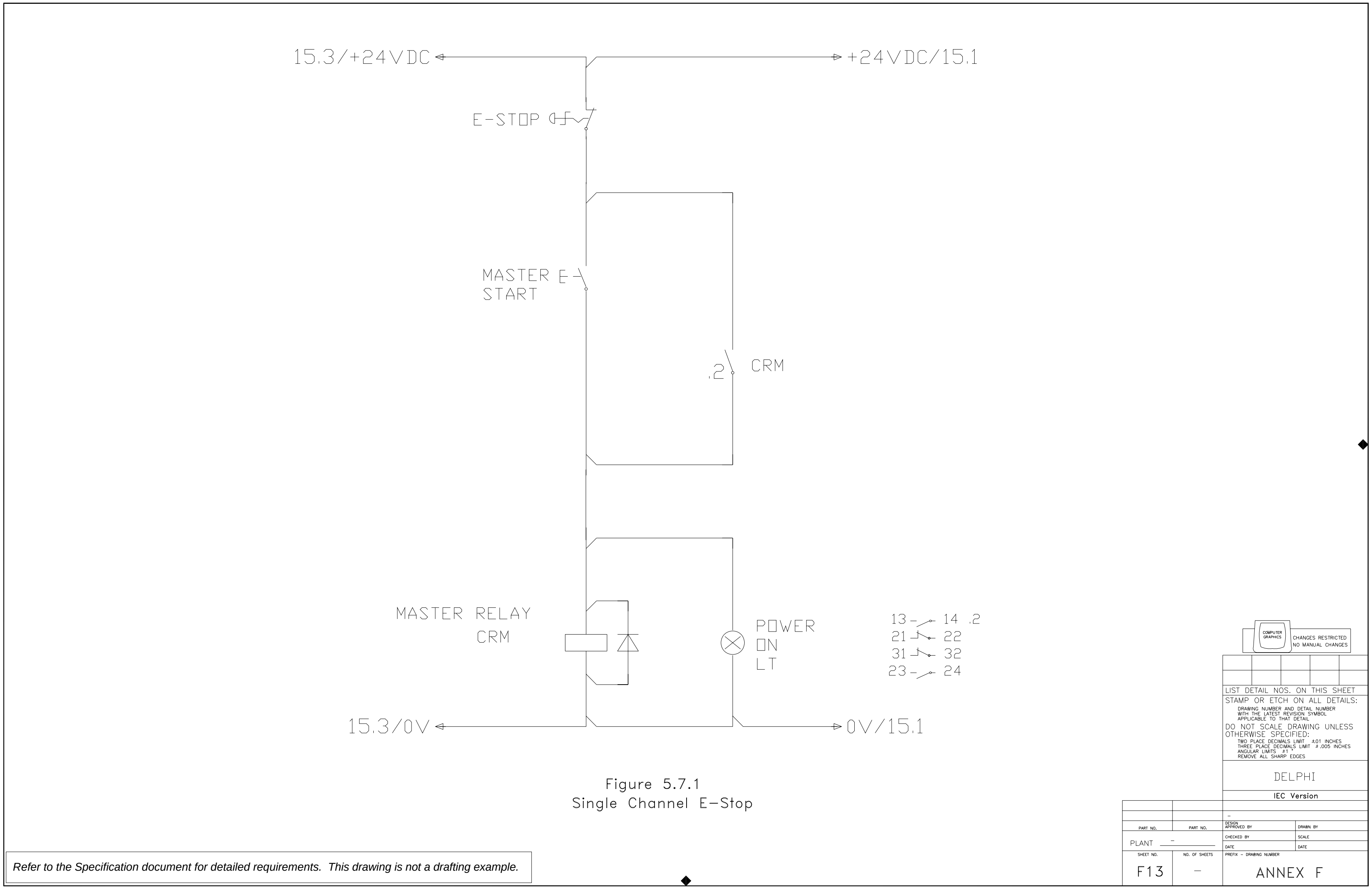


Figure 5.7.2 E-Stop as part of a Safety Circuit [Return]

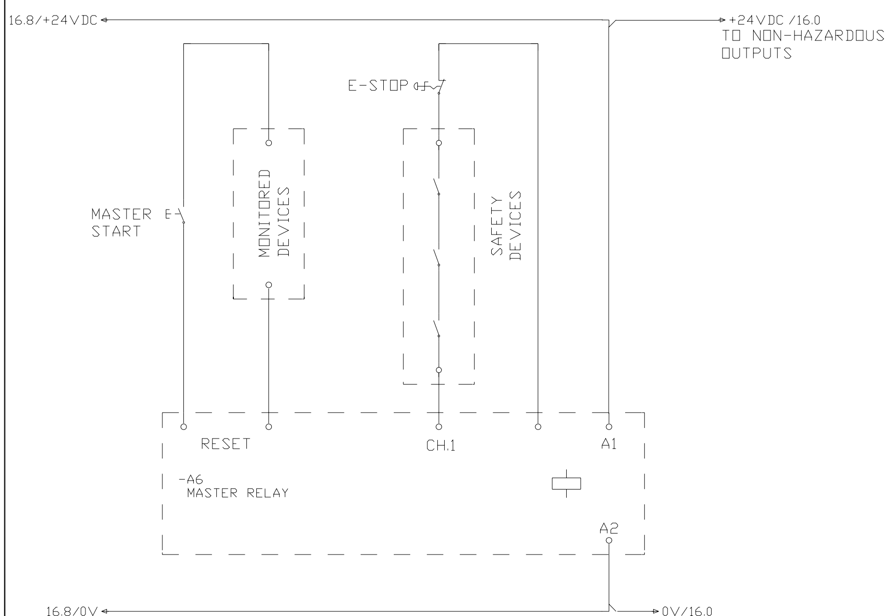


Figure 5.7.2
E–Stop as part of a Safety Circuit

Refer to the Specification document for detailed requirements. This drawing is not a drafting example.

Figure 5.7.3 Dual/Redundant Contacts [Return]

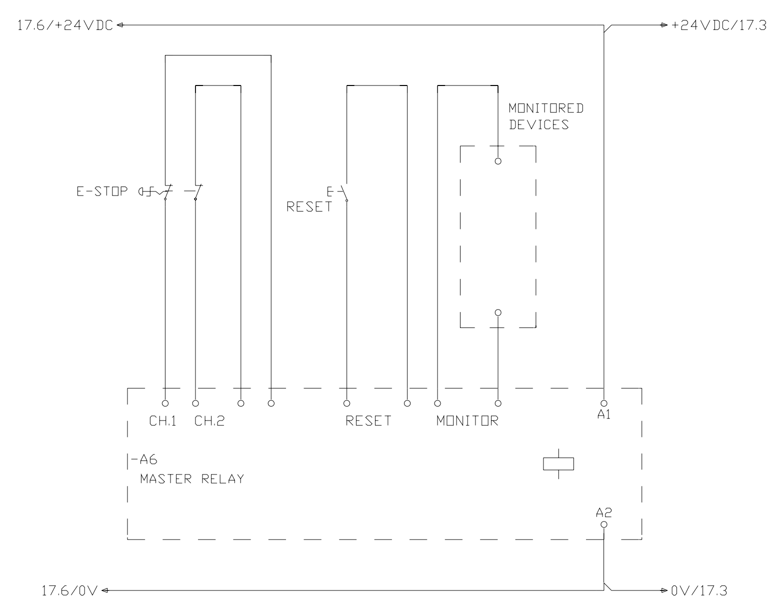


Figure 5.7.3
Dual/Redundant Contacts

CHANGES RESTRICTED
NO MANUAL CHANGES
LIST DETAIL NOS. ON THIS SHEET
STAMP OR ETCH ON ALL DETAILS:
DO NOT SCALE DRAWING UNLESS
OTHERWISE SPECIFIED:
DELPHI
IEC Version
PART NO. | PART NO. | APPROVED BY | DRAWN BY
PLANT –
SHEET NO. F14 | NO. OF SHEETS – | ANNEX F

Figure 5.10.4 – Light Curtain w/ Relays Return

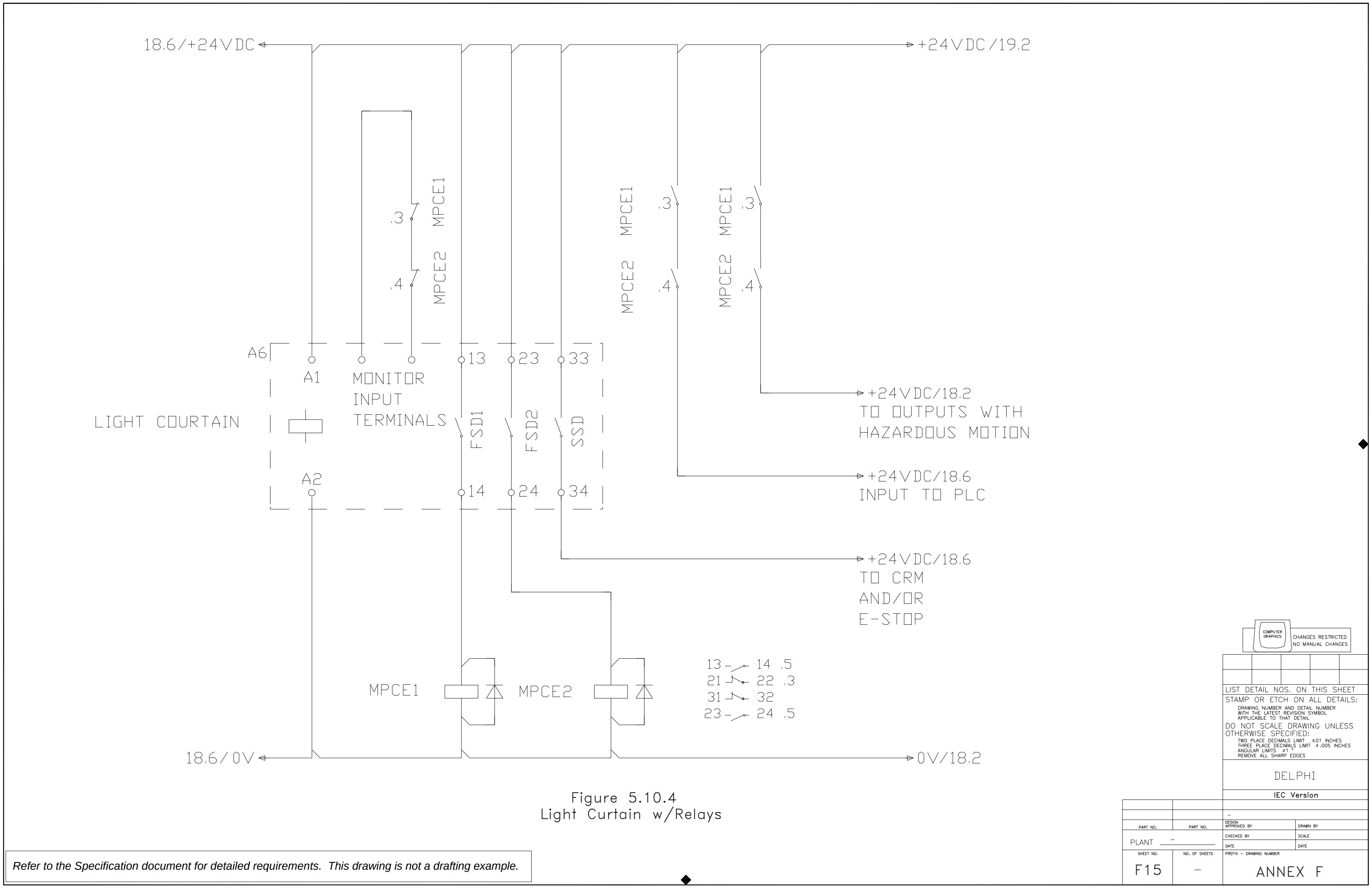
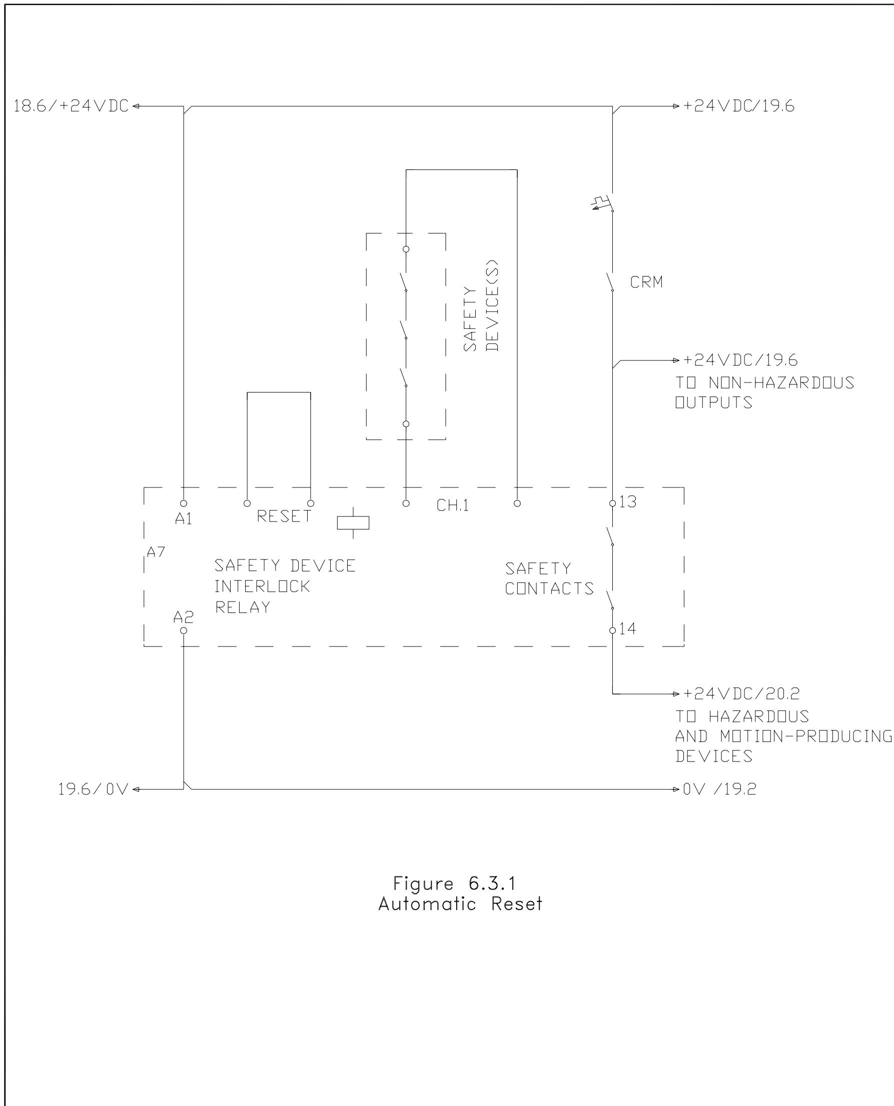


Figure 6.3.1 – Automatic Reset

[Return]



Refer to the Specification document for detailed requirements. This drawing is not a drafting example.

Figure 6.3.2 – Two Hand Control - Control Reliable

[Return]

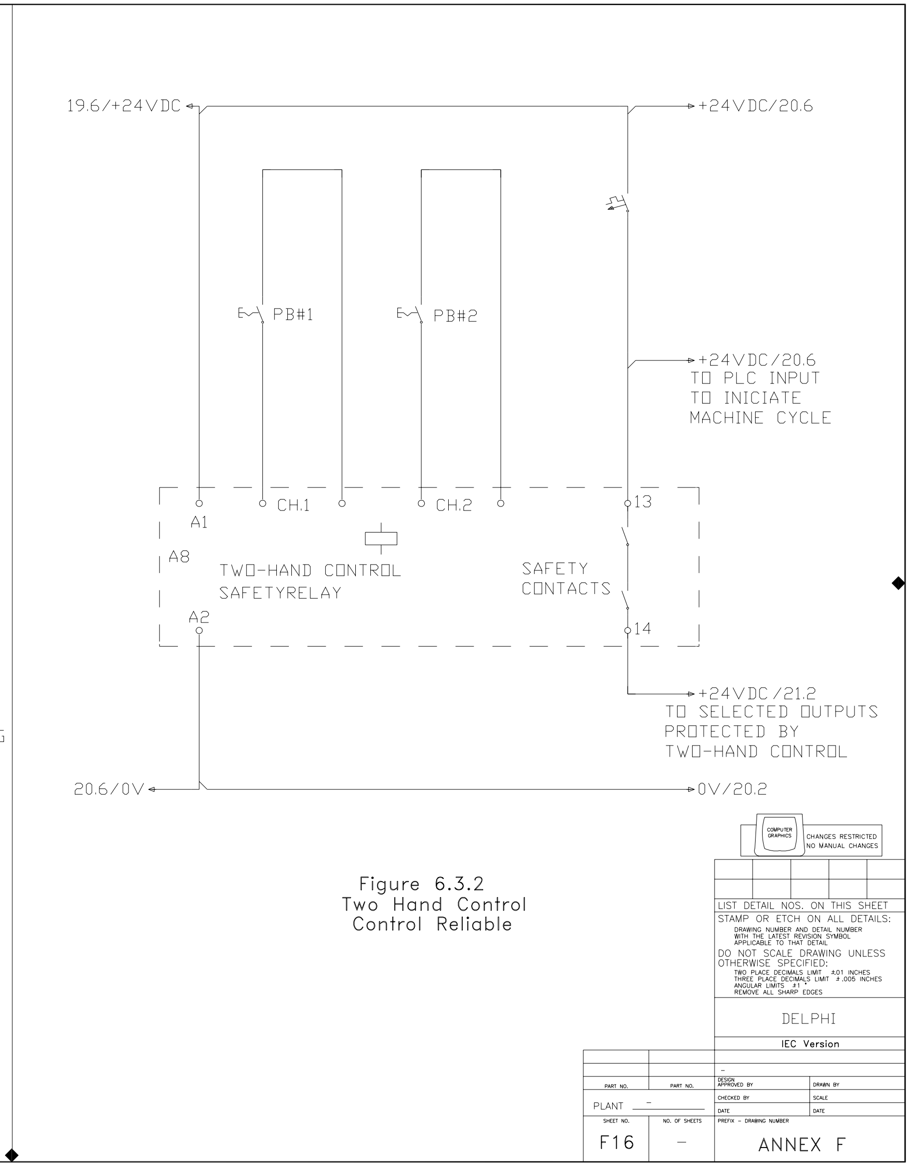
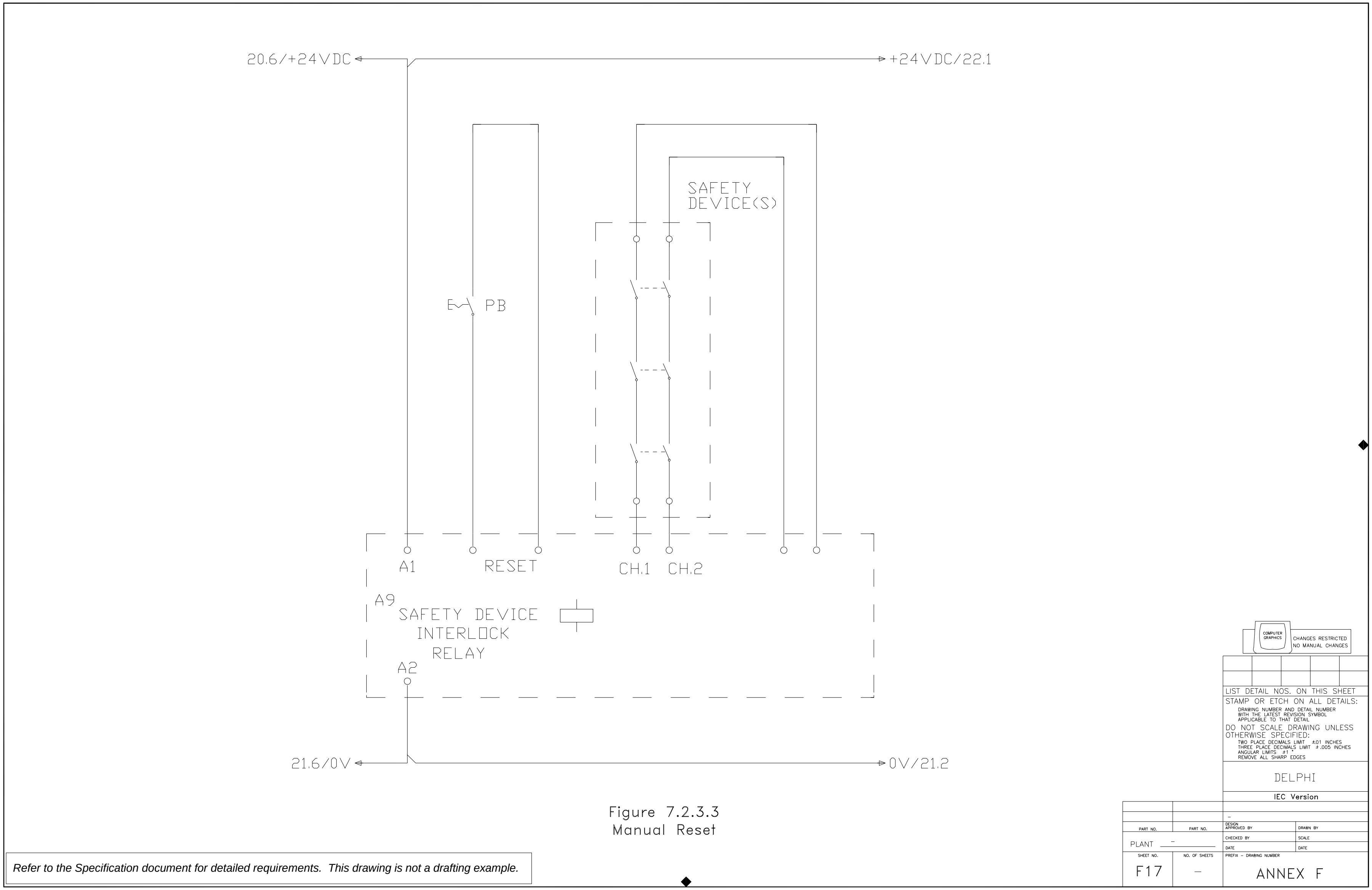


Figure 7.2.3.3 – Manual Reset

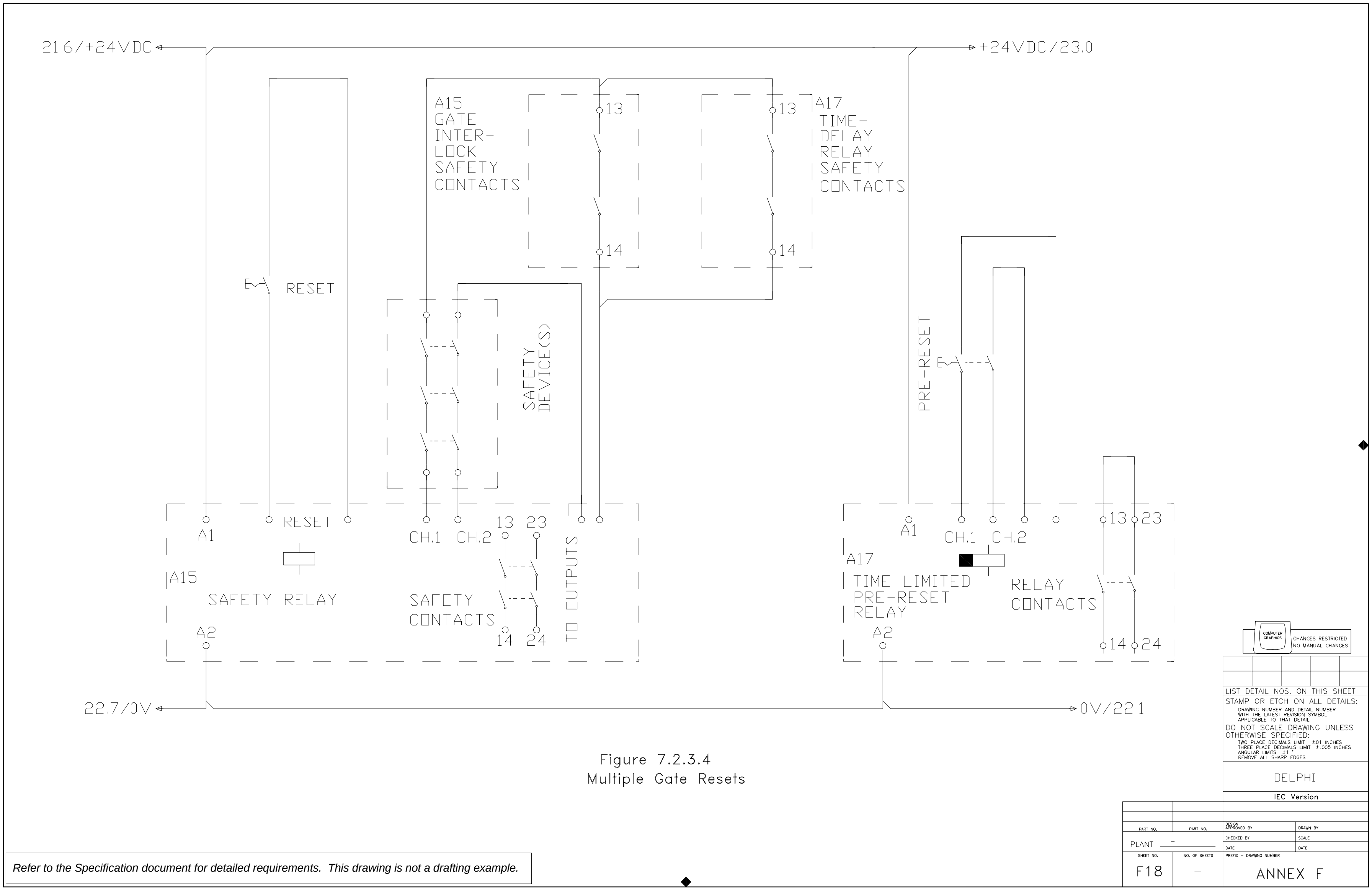
[Return]



Refer to the Specification document for detailed requirements. This drawing is not a drafting example.

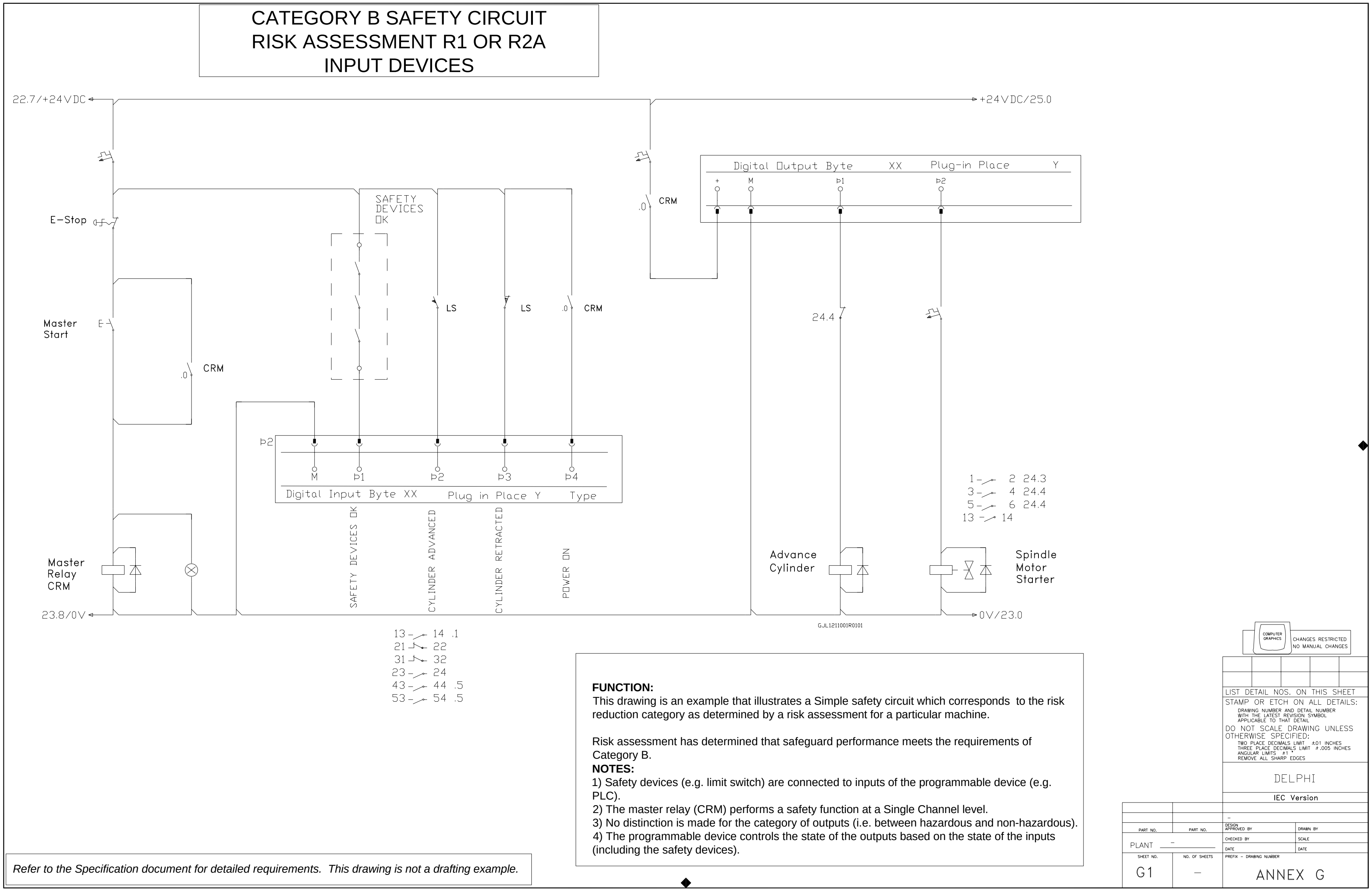
Figure 7.2.3.4 – Multiple Gate Resets

Return



G Annex G Sample IEC electrical/pneumatic circuits (Refer to Annex C)

Category B Safety Circuit – Input Devices, sheet G1



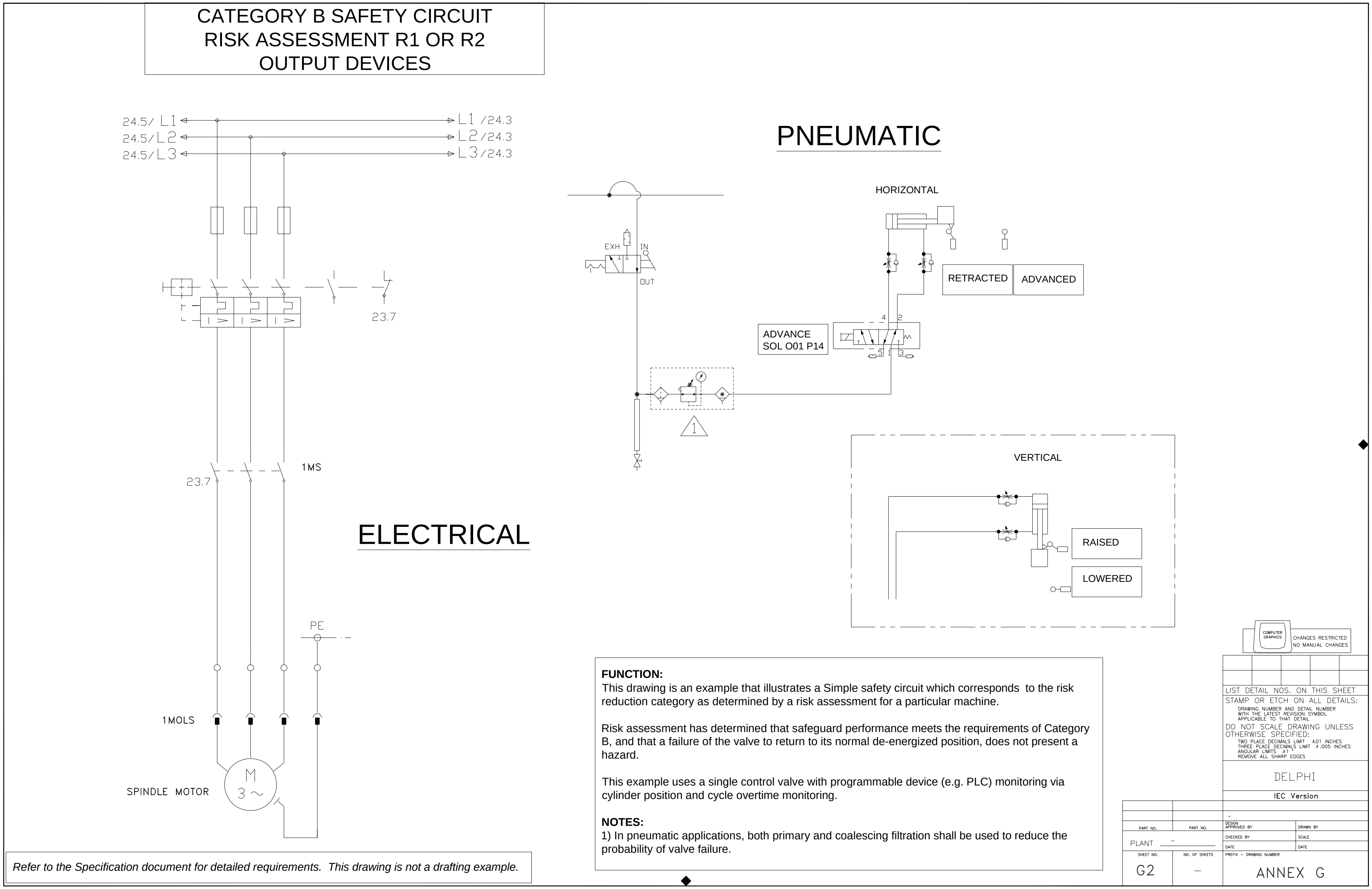
FUNCTION:
This drawing is an example that illustrates a Simple safety circuit which corresponds to the risk reduction category as determined by a risk assessment for a particular machine.

Risk assessment has determined that safeguard performance meets the requirements of Category B.

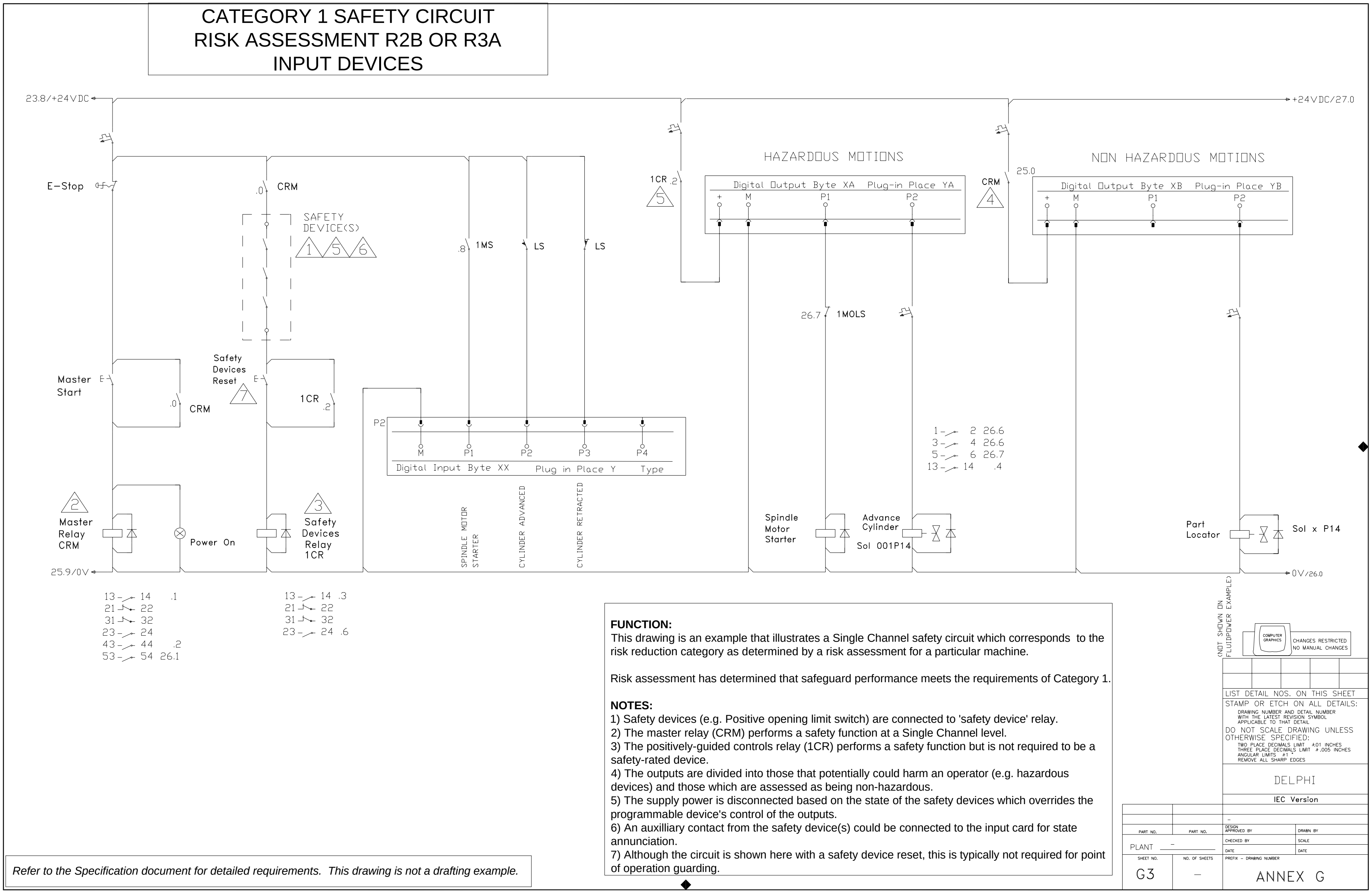
NOTES:
1) Safety devices (e.g. limit switch) are connected to inputs of the programmable device (e.g. PLC).
2) The master relay (CRM) performs a safety function at a Single Channel level.
3) No distinction is made for the category of outputs (i.e. between hazardous and non-hazardous).
4) The programmable device controls the state of the outputs based on the state of the inputs (including the safety devices).

Refer to the Specification document for detailed requirements. This drawing is not a drafting example.

Category B Safety Circuit – Output Devices, sheet G2



Category 1 Safety Circuit – Input Devices, sheet G3

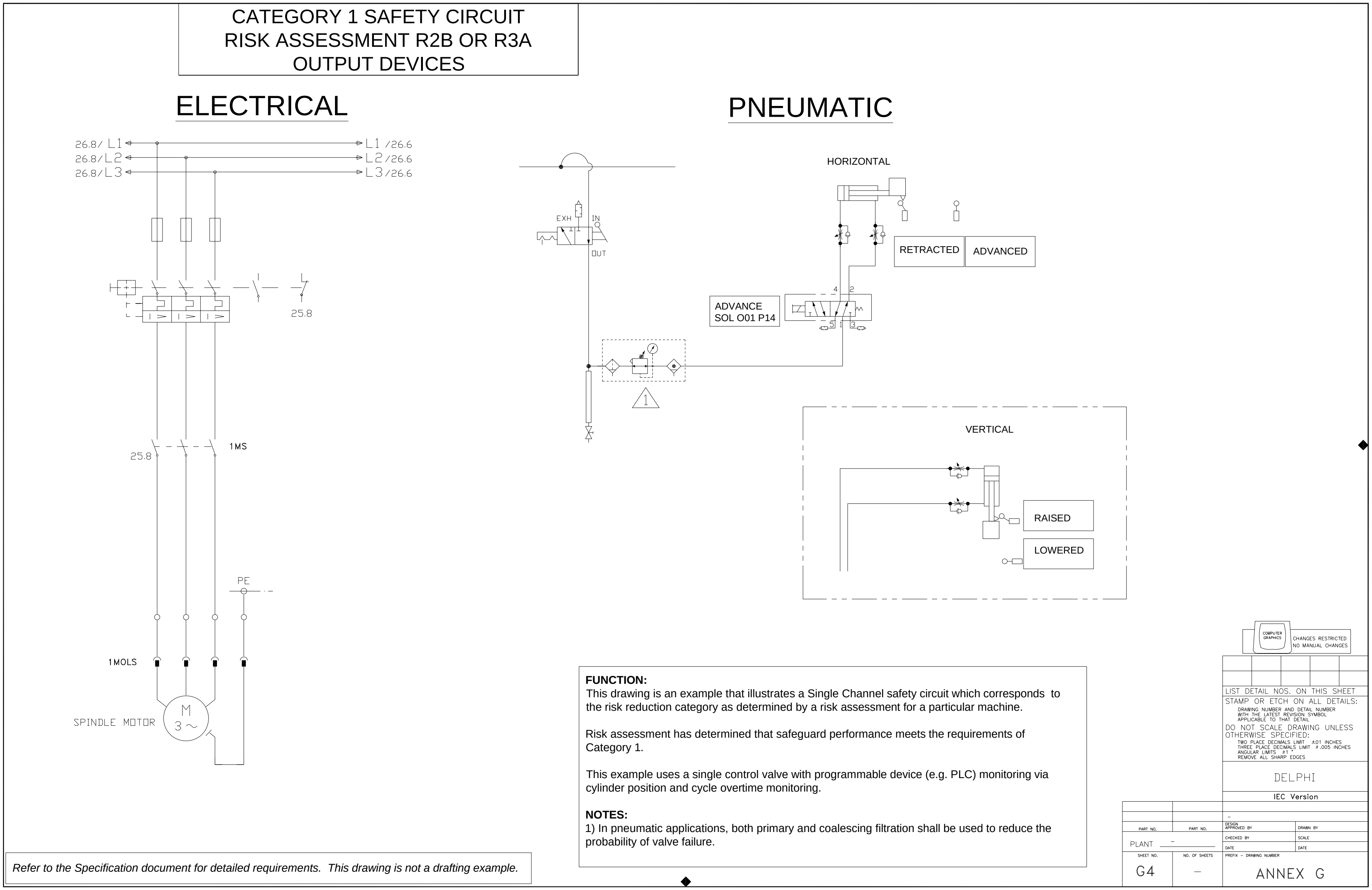


FUNCTION:
This drawing is an example that illustrates a Single Channel safety circuit which corresponds to the risk reduction category as determined by a risk assessment for a particular machine.

Risk assessment has determined that safeguard performance meets the requirements of Category 1.

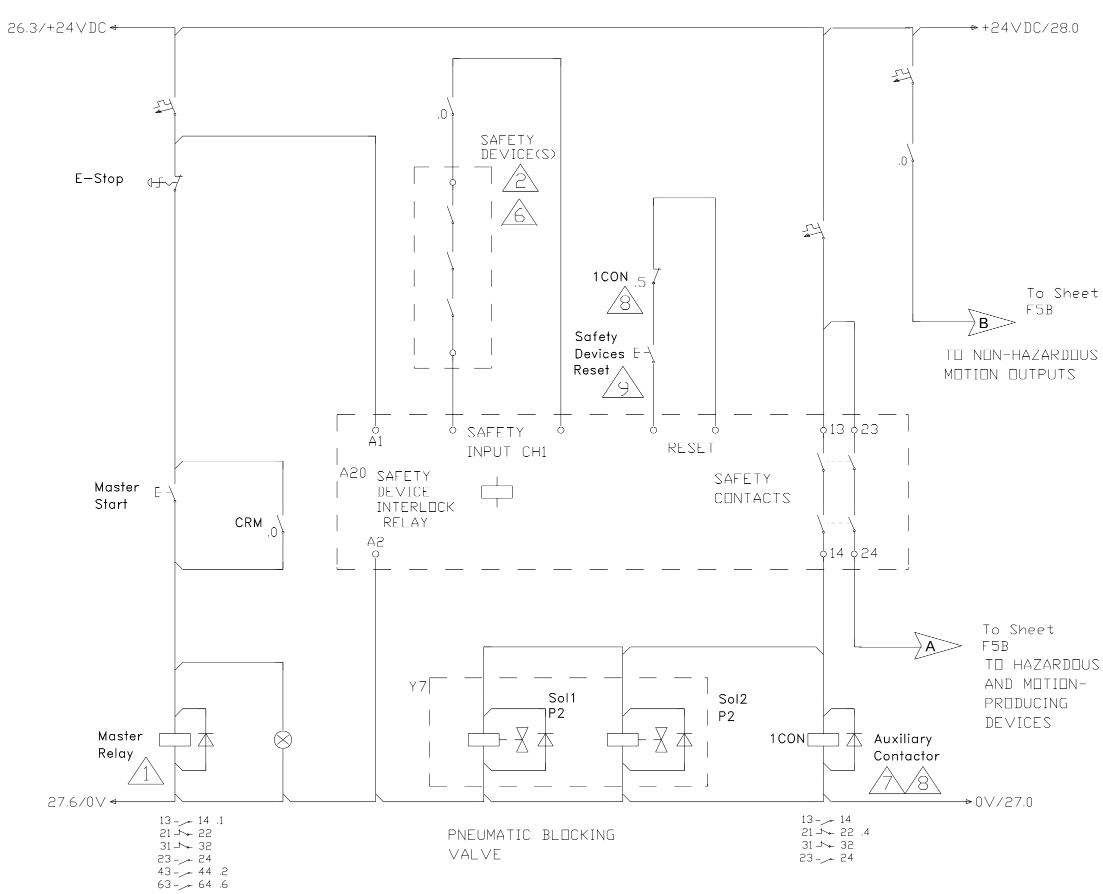
NOTES:
1) Safety devices (e.g. Positive opening limit switch) are connected to 'safety device' relay.
2) The master relay (CRM) performs a safety function at a Single Channel level.
3) The positively-guided controls relay (1CR) performs a safety function but is not required to be a safety-rated device.
4) The outputs are divided into those that potentially could harm an operator (e.g. hazardous devices) and those which are assessed as being non-hazardous.
5) The supply power is disconnected based on the state of the safety devices which overrides the programmable device's control of the outputs.
6) An auxilliary contact from the safety device(s) could be connected to the input card for state annunciation.
7) Although the circuit is shown here with a safety device reset, this is typically not required for point of operation guarding.

Category 1 Safety Circuit – Output Devices, sheet G4



Category 2 Safety Circuit – Input Devices, sheet G5A

CATEGORY 2 SAFETY CIRCUIT
RISK ASSESSMENT R3B
INPUT DEVICES

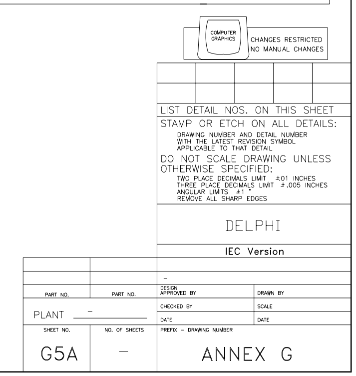


FUNCTION:
This drawing is an example that illustrates a Single Channel with Monitoring safety circuit which corresponds to the risk reduction category as determined by a risk assessment for a particular machine.

The state of the safety output string (contactor) is monitored each time the safety devices change state. Reapplying power to the outputs (pressing the safety device reset pushbutton) is ignored if the safety output string has not responded to the state change. The safety blocking valve is self-monitored.

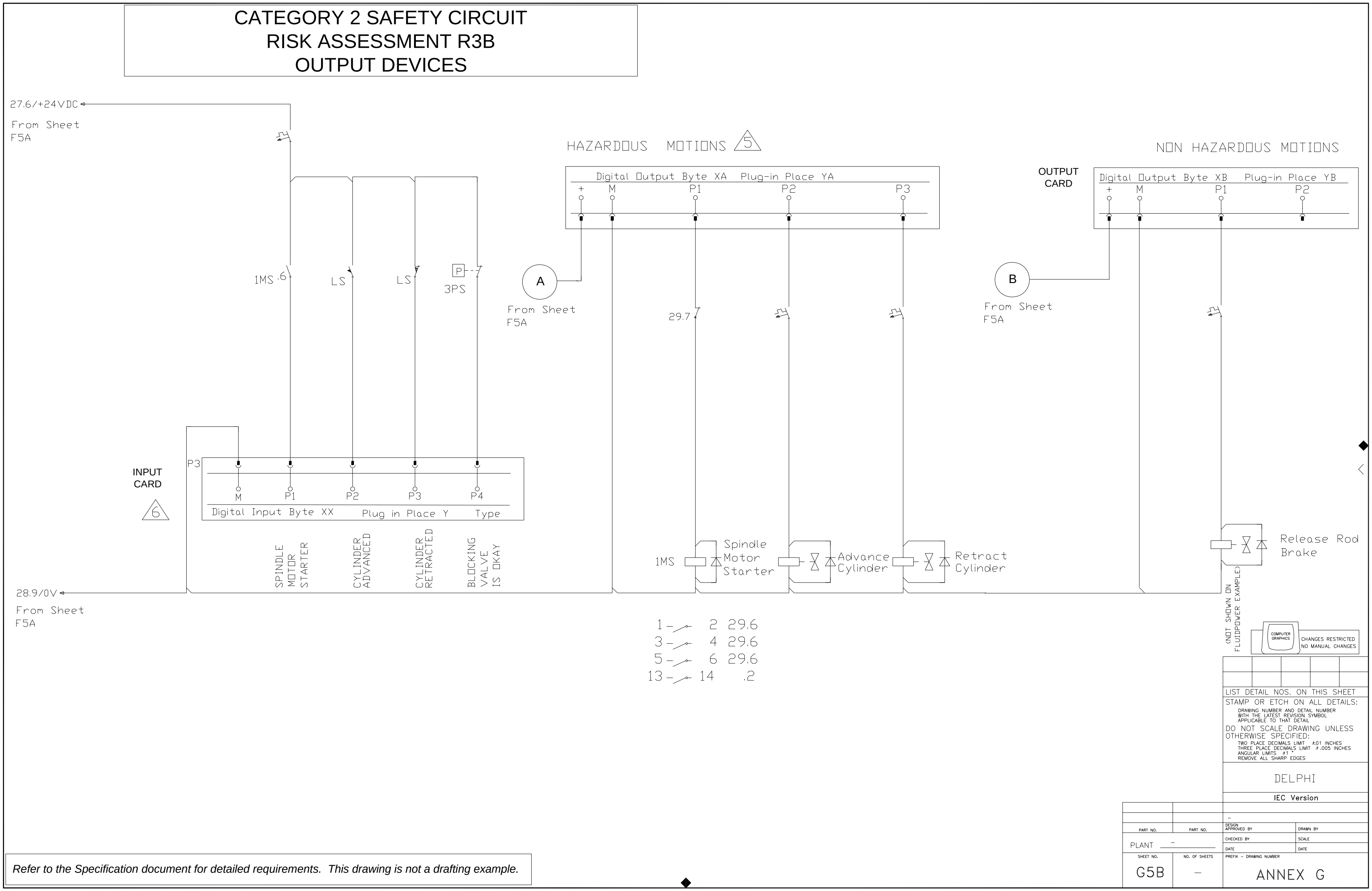
Risk assessment has determined that safeguard performance meets the requirements of Category 2.

NOTES:
1) The risk assessment has determined that the safety devices connected to the safety device interlock relay have addressed all hazards, therefore e-stop needs only be a minimum single channel circuit.
2) Safety devices (e.g. Positive opening safety interlock limit switch) are connected to safety device interlocking relay (1SR).
3) The master relay (CRM) performs a safety function at a Single Channel level.
4) The outputs are divided into those that potentially could harm an operator (e.g. hazardous devices) and those which are assessed as being non-hazardous.
5) The programmable device controls the state of the outputs however supply power is disconnected based on the state of the safety devices.
6) An auxilliary contact from the safety device(s) interlocking relay could be connected to the input card for state annunciation.
7) The contactor 1 CON provides the safety control (see 480V circuit), whereas contactor 1 MS is controlled by the programmable device.
8) To accomplish monitoring requirements, a normally closed contact from each positive-guided output relay (IEC 60947-5-5) shall be used in the safety relay reset or monitoring circuit. The state of 1CON is monitored through a (normally closed) auxiliary contact.
9) Manual reset is required for perimeter guards. The safety relay reset input shall require the safety device reset pushbutton signal transition in order to engage the safety contacts (i.e., anti-tie-down).

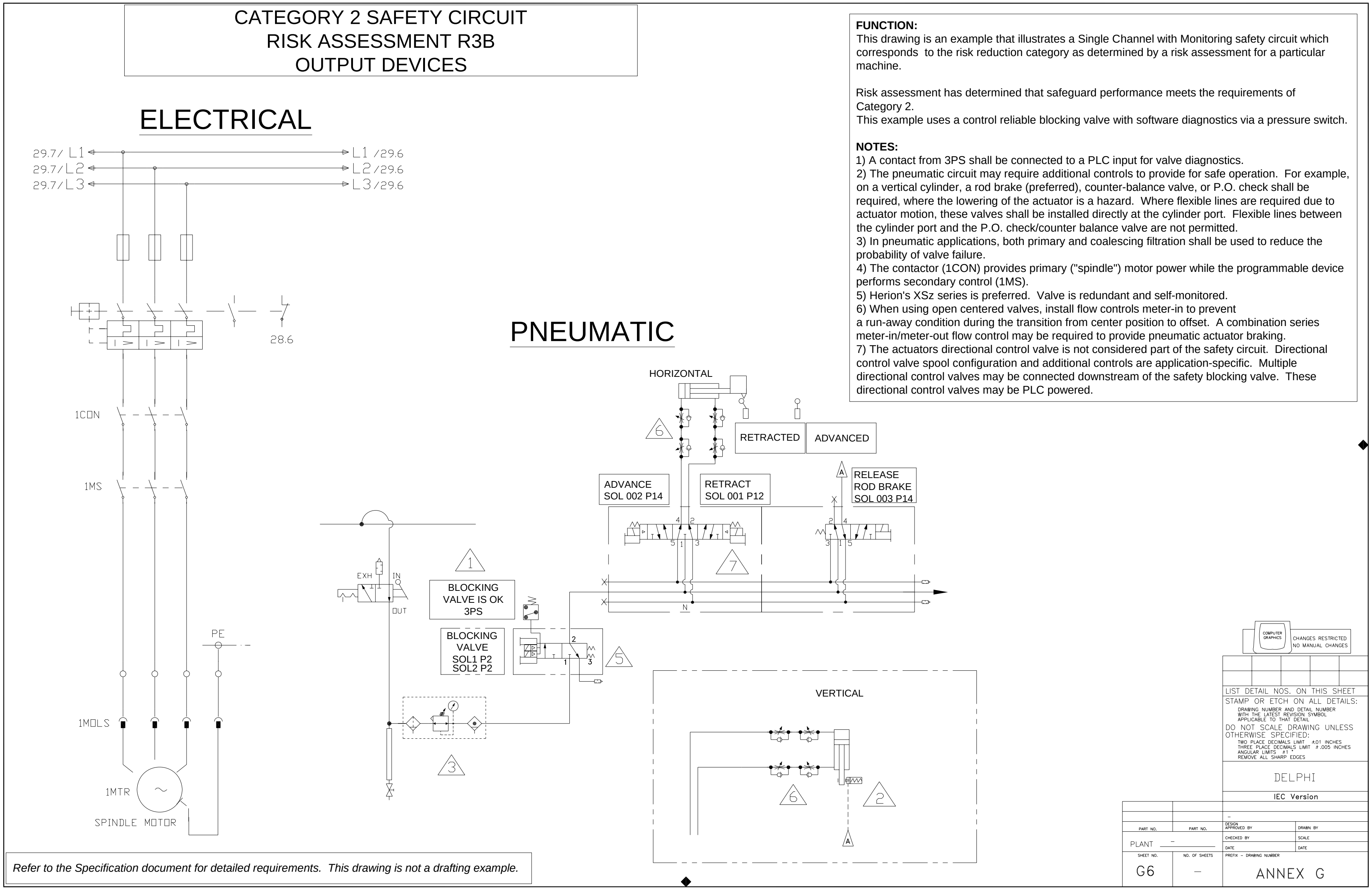


Refer to the Specification document for detailed requirements. This drawing is not a drafting example.

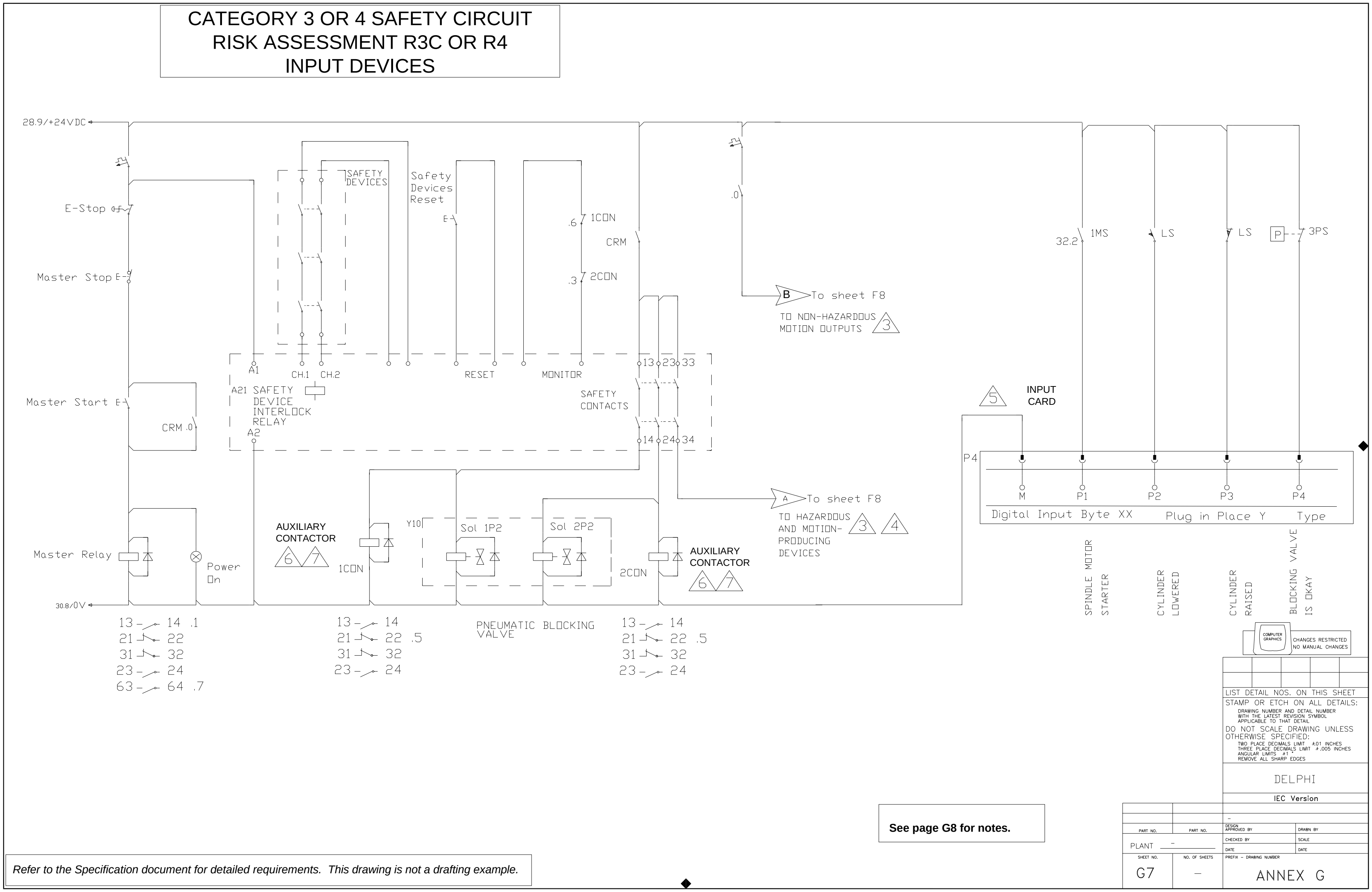
Category 2 Safety Circuit – Output Devices, sheet G5B



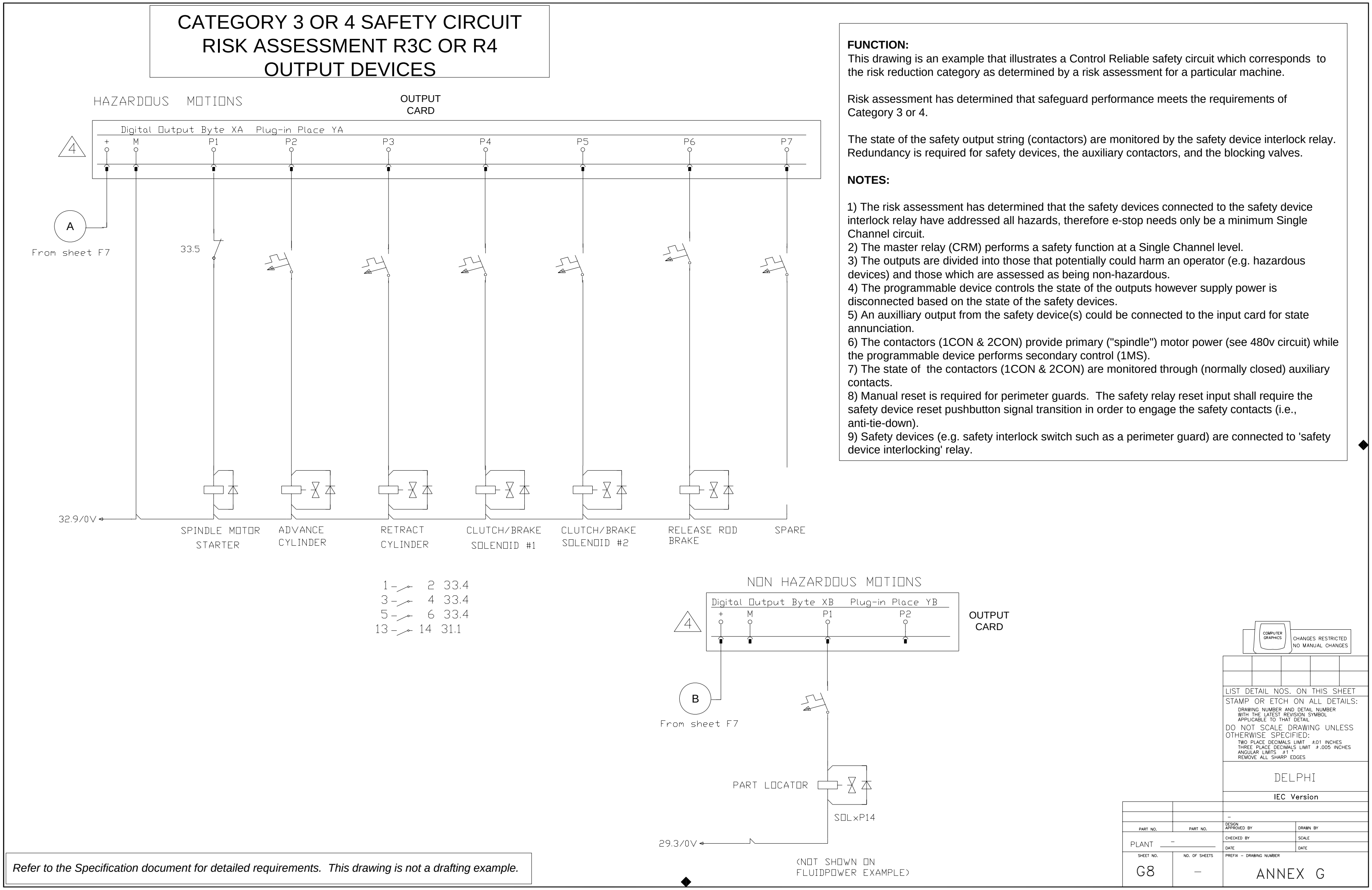
Category 2 Safety Circuit – Output Devices, sheet G6



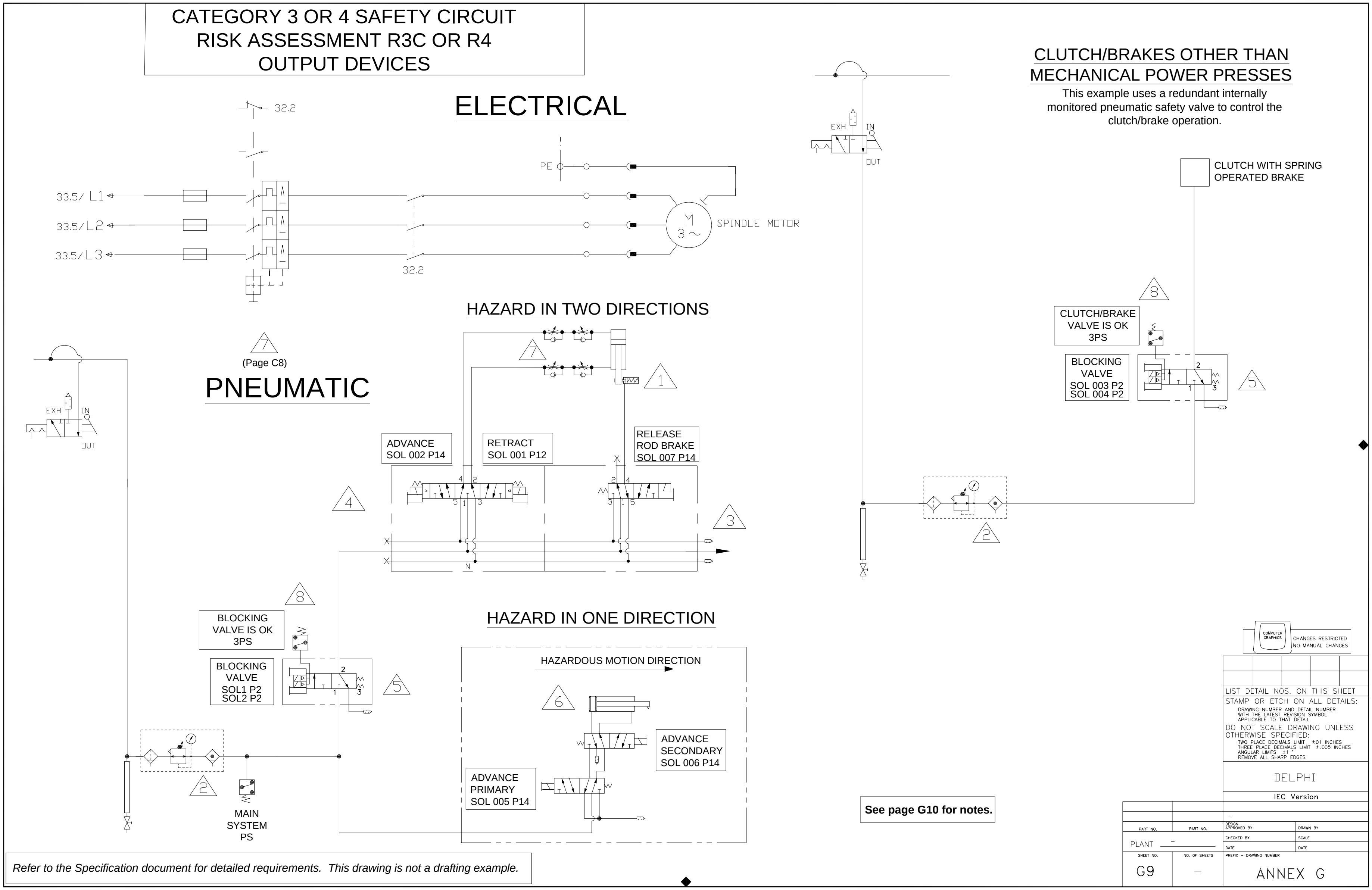
Category 3 or 4 Safety Circuit – Input Devices, sheet G7



Category 3 or 4 Safety Circuit – Output Devices, sheet G8



Category 3 or 4 Safety Circuit – Output Devices, sheet G9



Category 3 or 4 Safety Circuit – Output Devices, sheet G10

CATEGORY 3 OR 4 SAFETY CIRCUIT
RISK ASSESSMENT R3C OR R4
INPUT DEVICES

FUNCTION:
This drawing is an example that illustrates a Control Reliable safety circuit which corresponds to the risk reduction category as determined by a risk assessment for a particular machine.

Risk assessment has determined that safeguard performance meets the requirements of Category 3 or 4.

These examples show either a control reliable self monitored safety blocking valves with software diagnostics via a pressure switch, or redundant standard direction valves configured to fail in a safe condition.

NOTES:
1) For vertical applications a rod brake, counter balance valve, or pilot operated check shall be required to prevent dropping of loads that would be considered a hazard. Cylinder rod brakes are preferred.
2) Both primary and coalescing filtration shall be used to reduce the probability of valve failure.
3) The actuators directional control valve is not considered part of the safety circuit. Directional control valve spool configuration and additional controls are application-specific. Multiple directional control valves may be connected downstream of the safety blocking valve. These directional control valves may be PLC powered.
4) Consideration should be given to the use of a three-position directional control valve.
5) Herion's XSz series is preferred. Valve is redundant and self-monitored.
6) Assumes guarding provided to protect against hazardous motion in the retract position.
7) Meter-in flow controls are required for controlled restart after the cylinder has been exhausted.
8) A contact from 3PS shall be connected to a PLC input for valve diagnostics.

CAUTION!
Detented and spring offset valves that were de-energized with the actuator in mid-position, will either continue their motion, or retract to the home direction, when the safety circuit and corresponding blocking valves are reset. In the case of automatic reset, this would occur immediately upon releasing the safety device. For manual reset applications, this motion would occur only after depressing the reset button.

COMPUTER GRAPHICS — CHANGES RESTRICTED NO MANUAL CHANGES

LIST DETAIL NOS. ON THIS SHEET

STAMP OR ETCH ON ALL DETAILS:
DRAWING NUMBER AND DETAIL NUMBER WITH THE LATEST REVISION SYMBOL APPLICABLE TO THAT DETAIL

DO NOT SCALE DRAWING UNLESS OTHERWISE SPECIFIED:
TWO PLACE DECIMALS LIMIT ±.01 INCHES
THREE PLACE DECIMALS LIMIT ±.005 INCHES
ANGULAR LIMITS ±1 °
REMOVE ALL SHARP EDGES

DELPHI

IEC Version

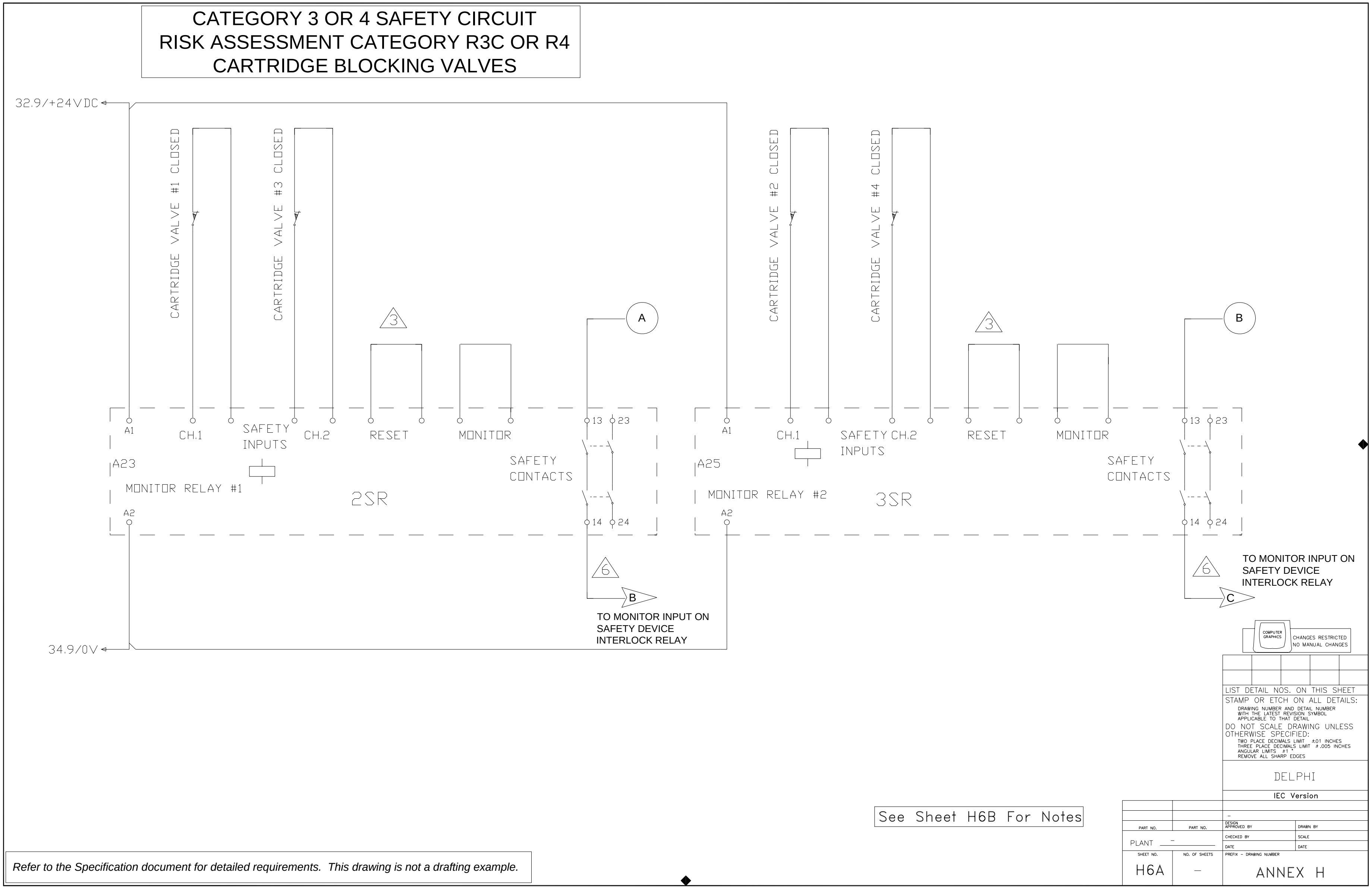
PART NO.	PART NO.	DESIGN APPROVED BY	DRAWN BY
PLANT –		CHECKED BY	SCALE
		DATE	DATE
SHEET NO. G10	NO. OF SHEETS –	PREFIX – DRAWING NUMBER ANNEX G	

See sheet G9 for circuits.

Refer to the Specification document for detailed requirements. This drawing is not a drafting example.

H Annex H Sample IEC electrical/hydraulic circuits (Refer to Annex D)

Category 3 or 4 Safety Circuit – Cartridge Blocking Valves, sheet H6A



Category 3 or 4 Safety Circuit – Cartridge Blocking Valves, sheet H6B

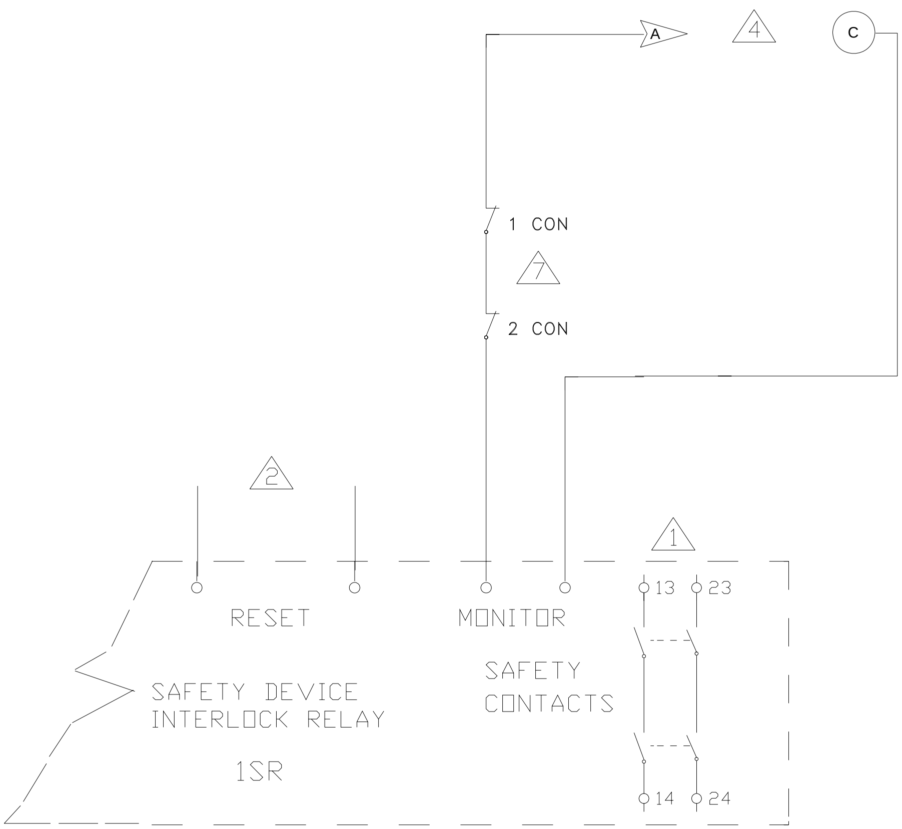
CATEGORY 3 OR 4 SAFETY CIRCUIT
RISK ASSESSMENT R3C OR R4
CARTRIDGE BLOCKING VALVES

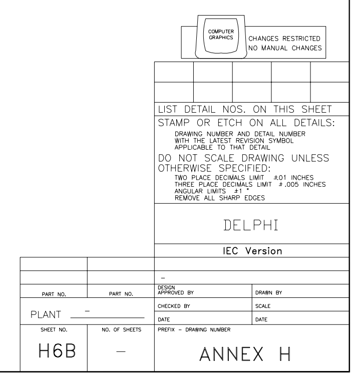
FUNCTION:
This drawing is an example that illustrates a Control Reliable safety circuit which corresponds to the risk reduction category as determined by a risk assessment for a particular machine.

Risk assessment has determined that safeguard performance meets the requirements of Category 3 or 4.

This circuit represents that portion of the electrical safety circuit required to control the redundant monitored cartridge valves used to remove hazardous energy, typically on high GPM systems.

NOTES:
1) Safety relay 1SR removes power to the pilot control safety valves (SOL1 & 2).
2) Refer to the specification for application specific reset requirements.
3) The valve monitor safety relay 2SR and 3SR can be any safety relay capable of automatic reset, with no monitor input capability, and no input concurrency requirements.
4) The valve monitor safety relay 2SR and 3SR do not work in conjunction with each other during normal advancing and retracting of the cylinder. When all solenoids are de-energized (when power is removed by 1SR) both 2SR and 3SR will allow power to the reset string of 1SR.
5) The circuits inside this box provides the monitoring function.
6) Safety contacts of 2SR and 3SR are wired in series to the monitor string of 1SR.
7) Monitor of output device auxiliary contacts.





Refer to the Specification document for detailed requirements. This drawing is not a drafting example.

I Annex I Other Example Circuits

Two-hand Bypass Circuit, sheet I1