

DELPHI

Application Guideline for Muting Two-Hand Control Devices in a Control Reliable Circuit



DA-2103

Revision 1.0

October, 2003

Index

1 Abstract

2 Goals

Common References, Safety Circuits, and Performance Levels

3 Specifications

3.1 Control Reliable

3.2 Two-Hand Control

3.3 Muting

Components and Applications

4 Two-Hand Control Safety Components

5 Point-of-Operation Guarding

6 Two-Hand Safe Distance Calculations

Machine example

7 Machine Overview

8 Risk Assessment Sample

Hardwired Safety Circuit Design

9 Two-Hand Control Circuit Design

10 Muting Circuit Design

Other Considerations

11 Failure Mode Considerations

12 Logic Design Considerations

Annexes

A Bibliography

B Machine Schematics

1. Abstract

Muting of a hardwired safety circuit is allowed, using an equivalent safety level hardwired circuit. Muting a Control Reliable hardwired safety circuit must use a Control Reliable hardwired mute circuit. Product literature commonly shows muting in a Control Reliable fashion. Their examples however reflect straight-forward applications such as a dual-sensor Control Reliable safety circuit from a robot machine base which mutes a light curtain when the robot is a safe distance away.

This document looks more pointedly at a Control Reliable two-hand control application where it is safe to mute based on multiple machine positions, even muting while motion is occurring. The hazards have been eliminated for the retract motions such that the operator can let go of the two-hand devices, turning attention to other production tasks. Muting is allowed, and required, to keep the machine in-cycle yet must be designed to the same safety circuit performance level as the initial Control Reliable two-hand control. This document looks at specification, component, and circuit design considerations; summing these all up with the finalized design.

Within particular design criteria a safety circuit can be Control Reliable independent of a PLC being interconnected to the circuit.

2. Goals

It is Delphi's goal to have safe machines while minimizing cost, doing this by consistently applying the appropriate safety circuit to the application. This document has goals for the circuit design and additional goals for the overall document and process.

Goals for the circuit include:

- ✓ Meet appropriate safety specifications
- ✓ Ease to design
- ✓ Ease to adapt to different applications
- ✓ Ease to communicate / teach / and enforce
- ✓ Ease to maintain / troubleshoot

Goals for the document include:

- ✓ Document intent of safety specifications
- ✓ Encourage consistent control design consideration
- ✓ Document failure mode considerations
- ✓ Document other design options which should not be used

**Common references,
safety circuits, and
performance levels**

3. Specifications

It is the readers' responsibility to obtain, fully read and understand all the standards / specifications which apply to the application.

Delphi's *Design-In Health and Safety Specification* contains risk assessment and risk reduction sections¹ which detail the process to obtain the safety circuit performance level. For an operator loading to the point-of-operation (frequency is more than once per hour) where injury would be categorized as serious (OSHA recordable) whether avoidance is likely or unlikely; the associated circuit performance required is Control Reliable.

Note that, keeping all other criteria the same, but lowering the injury to a slight severity (non-OSHA recordable) lowers the required circuit performance to Single Channel², which allows PLC two-hand control and therefore PLC based muting³. This document does not address this lower circuit performance example.

3.1 Control Reliable

Several national and international standards give definition to Control Reliable. Delphi's *Design-In Health and*

Safety Specification establishes the rules for Control Reliable safety circuitry⁴ within Delphi. Control Reliable circuits are required to be hardware based, include checked redundancy to and including the final switching device(s), and take into account common modes of failure.

Electrical Control Reliable safety circuits require the use of dual-channel safety relays, two inputs with short circuit detection, and outputs relays with positive-guided contacts⁵. Contacts from any of these positive-guided relays are used in series to protect against a single failure, and "opposite state" contacts are used in circuitry which monitors the function of the safety circuits⁶. Positive-guided relays are sometimes added to a Control Reliable circuit to help monitor devices which do not have "positive-guided" indication that they are functioning properly⁷.

Safety interlock switches for Control Reliable applications require positive opening contacts (either two contacts on one switch or two switches with one contact each). Multiple switches, such as from a series of guards, can be run into one safety relay, but for a mute application one of the a typical device failure modes prohibits the practice of multiple sensors in series for the muting relay. Look for further details in the *Muting* subsection of this chapter.

Control Reliable safety circuits include checked redundancy in the fluid power

¹ DA-2006 section 3.3, 3.4, 3.5

² DA-2006 Table 4

³ DA-2001 item 6.3.2

⁴ DA-2006 item 3.5.5.4

⁵ DA-2001 item 4.1.2

⁶ DA-2001 section 5.4

⁷ DA-2001 item 5.4.5.2

controls⁸. This typically requires one or a combination of the following:

1. dual blocking valves with functional monitoring
2. dual motion valves where failure of one device is detected and does not lead to a hazard
3. use of safety-rated self-checked components
4. quick stopping / or position holding devices

3.2 Two-Hand Control

Two-hand control performance specifications can be found in many documents.

ANSI defines a two-hand control devices as “an actuating control that requires the concurrent use of the operator’s hands to initiate or control machine motion during the hazardous portion of the machine cycle.”⁹ Two-hand controls are required to be located far enough from the nearest hazard such that the operator cannot reach the hazard before it ceases¹⁰. Two-hand devices are also to be designed and installed to protect against accidental operation¹¹. This often means ring guards or other protective shields. Common practice in industry is to make all forms of operator safeguarding difficult to defeat.

For ergonomics and part handling reasons many machines within Delphi use a one-hand cycle initiation method; a whisker switch in combination with other guarding (e.g. sliding Plexiglas door). The use of dual whisker

switches for two-hand control however is discouraged; most pointedly because of the above ANSI requirements. Second, dual whisker switch combinations are too easily defeated by physically hooking a string or wire between both switches thus making it a one-hand control system.

Concurrency on actuation of the two-hand devices has historically been limited to 0.5 seconds, although some standards have state no limit or leave the limit to be specified by the machine supplier. The latest NFPA-79 does state a time limit of 0.5 seconds¹².

Delphi’s specification reiterate the above requirements for two-hand control.

3.3 Muting

Muting is the automatic temporary bypass of any safety related function¹³. The concept of muting circuits performing to the same safety level (as the safety function being muted) has been industry expectation for many years. “A simple cam-operated limit switch wired in parallel with the device’s output is inadequate as its failure can remain undetected¹⁴.”

Control Reliable muting circuits have to be hardware based, designed, constructed and applied such that any single component failure does not prevent the stopping of the equipment, and generate a stop when a fault occurs. Control systems incorporating software and firmware (PLCs) are allowed to either further limit the muting

⁸ DA-2001, section 8

⁹ ANSI B11.19-2003 item 3.73

¹⁰ *ibid* item 6.2

¹¹ ANSI B11.19-1990 item 4.2.4.2.1

¹² NFPA-79, 2002 item 9.2.5.6(2)

¹³ DA-2001 item 3.8

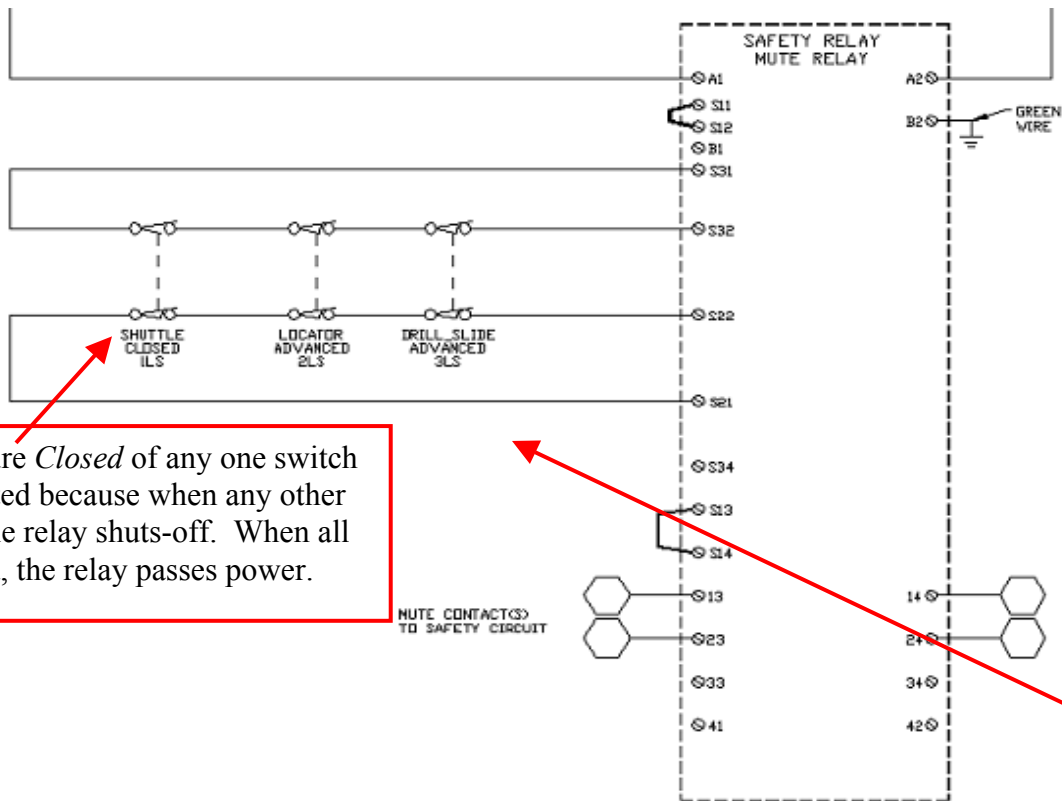
¹⁴ ANSI B11.19-1990 item 4.2.3.3.7

function of the hardwired circuit¹⁵, or provide protection against any single failure (shutdown to a safe state) equivalent to that of a hardwired control system¹⁶ (safety PLC implications).

On machines which could have the safeguarding muted after the completion of multiple motions, one might include a completely hardwired muting circuit as drawn below. **Note that the circuit depicted below is not an approved Control Reliable mute safety circuit.**

A method to design-out the failure modes detailed below would be to include multiple safety relays (in this case: one safety relay for **each** of the three motion limit switches). This can be complex depending on the machine, and does not address applications which need to mute while some cylinders are in motion.

Again, this document addresses these concerns through use of a PLC, while maintaining the safety circuit reliability independent of the PLC.



Note that a failure *Closed* of any one switch will go undetected because when any other switch opens, the relay shuts-off. When all are again closed, the relay passes power.

On a *Mute* application, which is different than multiple guards run into one guard safety relay, the failure of one limit switch is **guaranteed** to be ignored by the functioning of any other limit switch every cycle.

¹⁵ DA-2001 item 5.5.6
¹⁶ NFPA-79, 2002 item 9.4.3

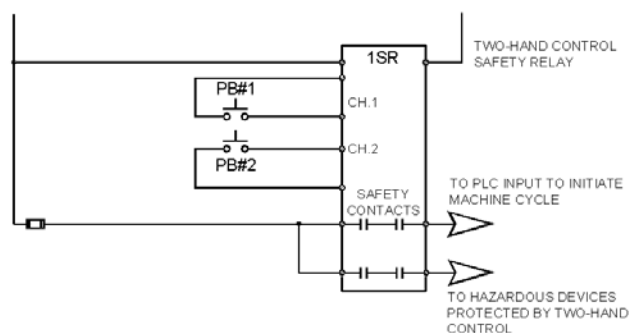
Components and applications

4. Two-Hand Control Components

Electrical, two-hand control, safety components consists of the safety relay and the input devices.

European standards on safety relays give classification to two-hand control safety relays. EN574 describes devices by type (type I, II, IIIA, IIIB, and IIIC) and risk assessment results as the basis for selecting devices¹⁷. None of these types exactly match Delphi requirements, although type IIIB can meet our requirements, and IIIC devices always meet them.

Delphi requires a hardwired, dual-channel, two-hand control safety relay with 500ms concurrency between single contacts off of two buttons¹⁸ for both Single Channel w/Monitoring and Control Reliable circuits.



¹⁷ EN 574

¹⁸ DA-2001 item 6.3.2

All of the basic criteria for safety relay selection, such as output contact current rating, monitor inputs, etc., have to be considered for two-hand control safety relay selection as well. Input simultaneity on two-hand control safety relays is set at 500ms maximum.

Many devices have been used as inputs to two-hand control safety relays, such as capacitive devices, low-force buttons, etc. When considering component selection it should be noted that some safety relays are rated for mechanical switches only, requiring an unspecified delay in the reaction time between the buttons N.O. and N.C. contacts. Others are now coming on the market designed for electronic devices. In addition, electronic pushbuttons for safety circuits have to be immune to RFI or other type of electrical interference.

Industry does market some devices that combine both the pushbuttons and safety relay; which can be used when compliant to the appropriate standards.

5. Point-of-Operation Guarding

Point-of-operation guarding, in this case a two-hand control system, is used to guard a person who performs an interactive task such as loading, unloading or inspecting in an area of a machine where a hazard exists. The two-hand control not only provides a guarding function while the machine is in-cycle, but also provides cycle initiation via a non-safety-rated means.

Compared to light curtains, application of two-hand control devices typically does not require additional fixed hard guarding. However, for process

containment, hard guards and an additional interlocked moveable guard such as a closing door which operates each cycle may be required.

Interruption of the two-hand control safety circuitry (release during the hazardous portion of the cycle) does not need to disable the PLC machine-in-cycle logic although frequently it will. When the machine-in-cycle logic is not inhibited the cycle overtime timer should also continue timing.

Release of the two-hand control safety circuitry during the hazardous portion of the cycle raises additional logic concerns. In some applications, an immediate stop may be required and the part classified as a reject. In other applications there may be good reason for the machine to continue its cycle when the two-hand devices are again actuated.

6. Two-Hand Safe Distance Calculations

Many safety standards refer to a safe distance formula for the proper placement of safeguards; this includes two-hand controls. Refer to Delphi's *Specification for the Application of Safety Circuits* Annex B, Safe Distance Formulas¹⁹. The placement of the two-hand pushbuttons shall be consistent with these calculations. In some applications *where* to mount the two-hand devices may relate to *when* to mute.

Machine Example

7. Machine Overview

Application: The machine is a manually loaded lean assembly station, which pushes bushings and washers into opposing sides of the rack & pinion steering gear housing. The term "press" is used throughout the machine prints, but this is not to say that the machine is a hydraulic or mechanical power press. Designing the mute circuit for this machine, because multiple motions would indicate when the machine was in a safe position to mute, and the need to mute while some of these motions were retracting, a PLC-determined hardwired Control Reliable circuit was proposed.

Description: As initially built, the machine sequence was as follows. (Refer to sheet 13 of the ACAD prints in Annex B)

The operator loads bushings into the bottom press mandrels, then a housing into the fixture. The operator then needs to press and maintain the two-hand control for the complete upper and lower press-to-depth and dwell. The top press then retracts.

The operator is allowed to release the two-hand control to load washers, then must reactivate and hold the two-hand control to reapply the top press and dwell. Both presses are then retracted, the cycle is complete, and the operator allowed to release the two-hand control.

¹⁹ DA-2001 Annex B

New machine sequence: The revision to the machine sequence, which drove the need for the mute circuit, was basically a production improvement to allow the operator to release the two-hand control after press-depth.

The operator's hands were freed during the first press dwell and top retract, to prepare to load the washers prior to the second half of the cycle.

The operator is also allowed to release the two-hand control after the washer press; now available to stage the next housing and bushings during the dwell, retract, and unclamp.

The mechanics of the machine have been modified with Plexiglas covers to protect the operator from retract motions.

Since this was an existing machine, the request to revise the machine's safety circuits meant the changes had to be designed to the same circuit performance level as the initial safety circuit. Since the existing two-hand was control reliable, the muting would have to be control reliable.

8. Risk Assessment Example

This machine was built prior to the formal Delphi documented risk assessment being put in place. The following is a sample risk assessment which could have been done in order to document the appropriate circuit performance level; both for the initial machine build, and then an updated risk assessment for the production floor changes.

| Application: | | Description: | | | | | | |
|---|-------------------------|--|----|----|----|----------|------------|--|
| Bushing and Washer Assembly Station for a Rack & Pinion Steering Gear Housing | | Sample Risk Assessment for use in the Delphi Controls COE whitepaper titled Muting Two-Hand Control Devices in a Control Reliable Circuit. Twice during a normal machine cycle, the operator releases the two-hand control to manually load components. The mechanics of the machine has been modified to eliminate hazards in the retract direction(s), yet single-solenoid valves could not be the risk reduction method as some motions need to stay advanced / energized for process dwells during the second part-load stage. | | | | | | |
| Compan | | | | | | | | |
| Delphi Saginaw Steering Systems, Plant 7 | | | | | | | | |
| User | Task | Hazard / Failure Mode | S | E | A | Category | Solution | Risk Reduction Methods |
| Operator | Manually loads bushings | Unexpected clamp motion | S1 | E2 | A1 | R2B | Engr Ctrls | Single-channel safety circuit: hardwired removal of power to the basic motion control |
| Operator | Manually loads bushings | Unexpected press(es) advancing | S1 | E2 | A1 | R2B | Engr Ctrls | |
| Operator | Manually loads housing | Unexpected clamp motion | S1 | E2 | A1 | R2B | Engr Ctrls | |
| Operator | Manually loads housing | Unexpected press(es) advancing | S2 | E2 | A1 | R3C | Engr Ctrls | Control-reliable two-hand control with dual blocking valves in hydraulic circuit |
| Operator | In cycle | Expected clamp motion | S1 | E2 | A1 | R2B | Engr Ctrls | |
| Operator | In cycle | Expected press(es) advancing | S2 | E2 | A1 | R3C | Engr Ctrls | |
| Operator | In cycle | Expected retracting | S2 | E2 | A1 | R3C | Engr Ctrls | Control-reliable two-hand control with dual blocking valves in hydraulic circuit |
| Operator | In cycle | Expected retracting | S2 | E2 | A1 | R3C | Engr Ctrls | Fixed mechanical guards over all retract motions (R3C did not apply to clamp but clamp's R2B is covered by suggested |
| Operator | Manually loads washer | Unexpected top press advancing | S2 | E2 | A1 | R3C | Engr Ctrls | |
| Operator | Manually loads washer | Unexpected bottom press or clamp retracting | S2 | E2 | A1 | R3C | Engr Ctrls | |
| Operator | Manually unload part | Unexpected clamp motion | S1 | E2 | A1 | R2B | Engr Ctrls | |
| Operator | Manually unload part | Unexpected press(es) advancing | S2 | E2 | A1 | R3C | Engr Ctrls | |
| Skilled Trades | Troubleshooting | exposure to all hazards outlined above | | | | | | Solutions for operator and job setter address exposure |
| Skilled Trades | Major Repair | numerous | | | | | Lockout | Remove all hazardous energy |
| Operator | Machine Cleaning | numerous | | | | | Lockout | Remove all hazardous energy |

Task/hazard combinations highlighted indicate the most stringent category for various motions, and therefore the safety circuit performance level for those motions.

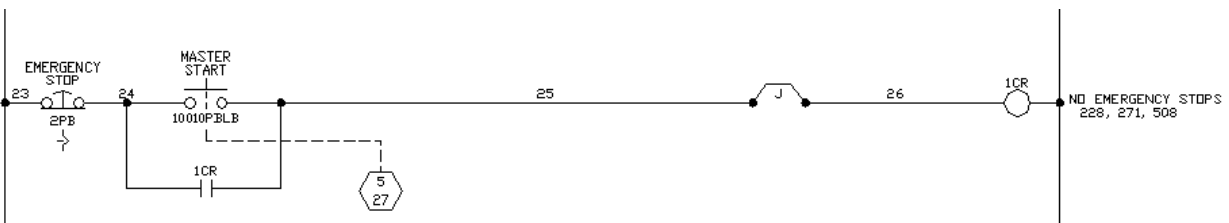
The update to the risk assessment reflecting the changes to the existing machine; the fixed guard risk reduction method replaces holding the two-hand control for the complete cycle.

Hardwired safety circuit design

9. Two-Hand Control Circuit Design

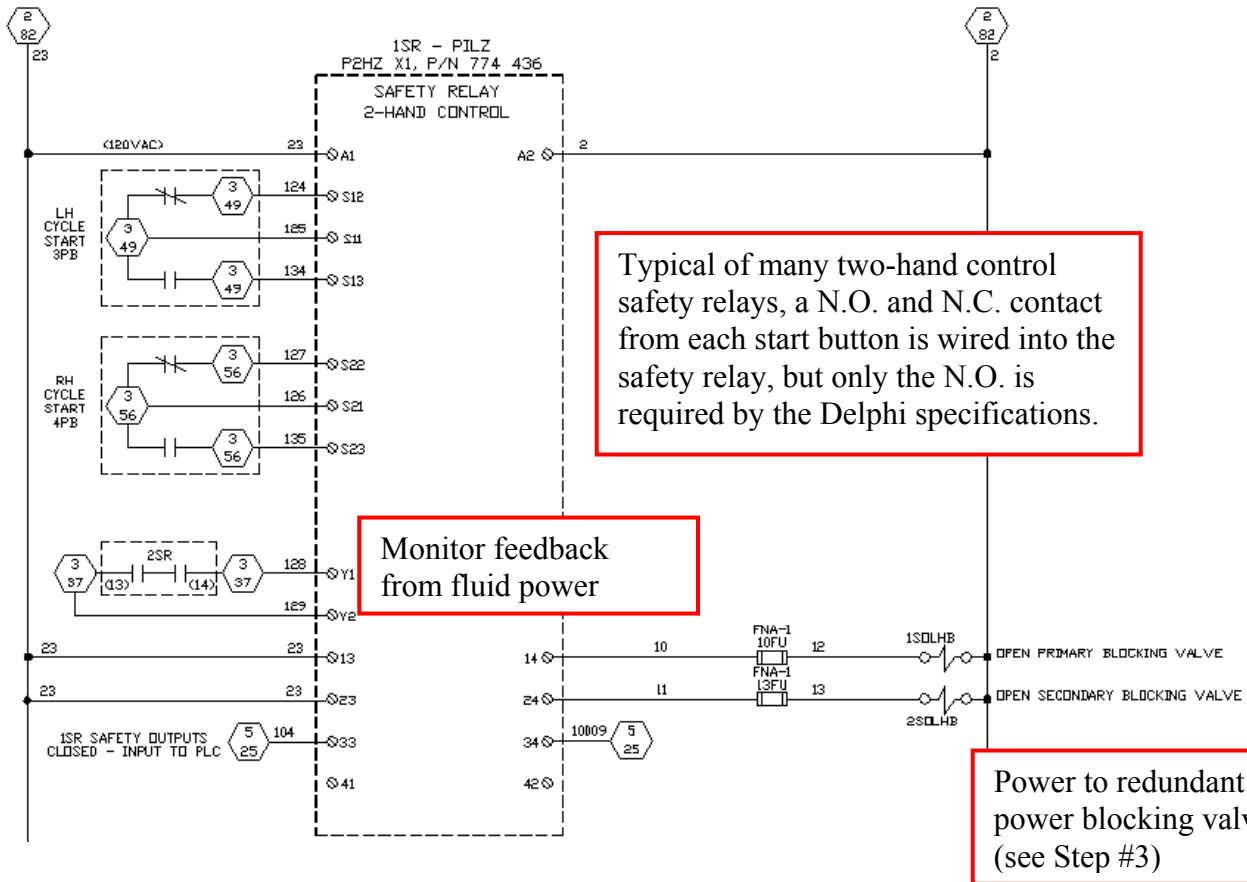
The hardwire control circuit design is for a Control Reliable implementation and has been broken down into individual circuit steps for clarity purposes. The first few steps, covered in this section, were from the initial machine design, not reflecting the changes required to implement the mute function. Also note that the complete machine control print has been included in this document as Annex B.

Step #1: E-stop circuit design



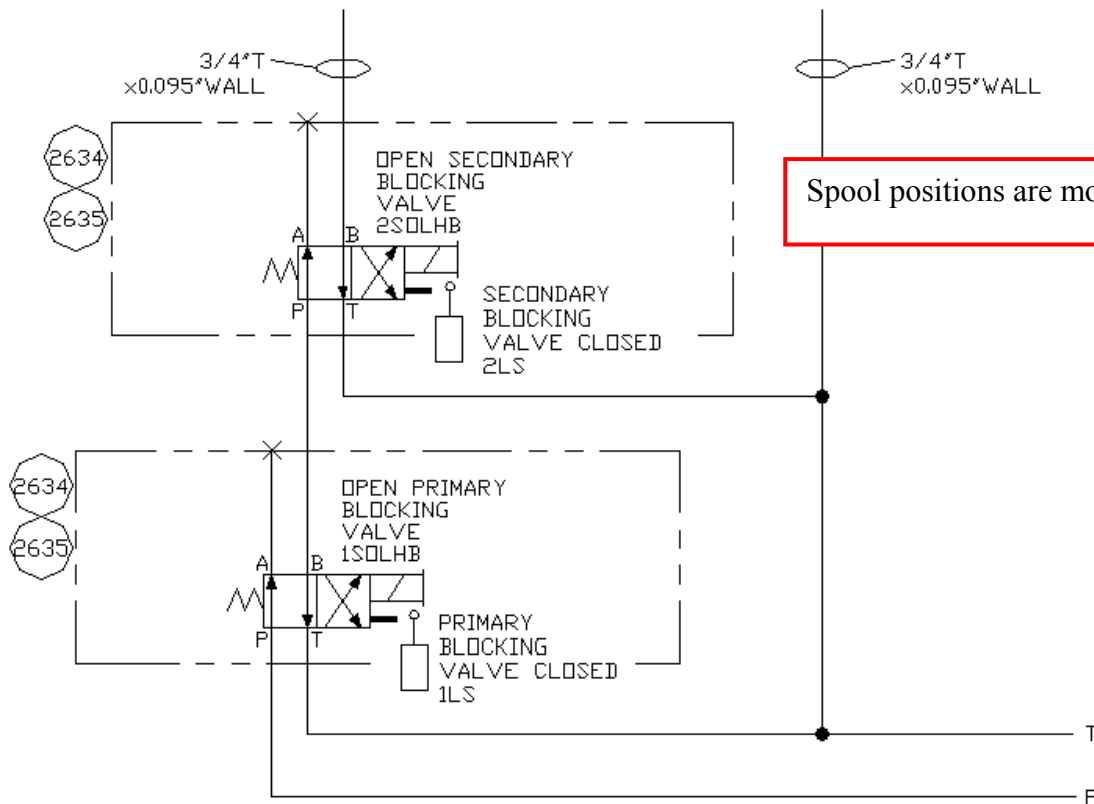
The risk assessment has determined that the two-hand control safety circuit addresses all hazards, therefore the e-stop circuit need only be a single channel circuit performance level.

Step #2: Two-hand control relay design



The two-hand control safety relay removes electrical power from redundant blocking valves.
An additional contact from 1SR is run to a PLC input to enable *Machine In Cycle*.

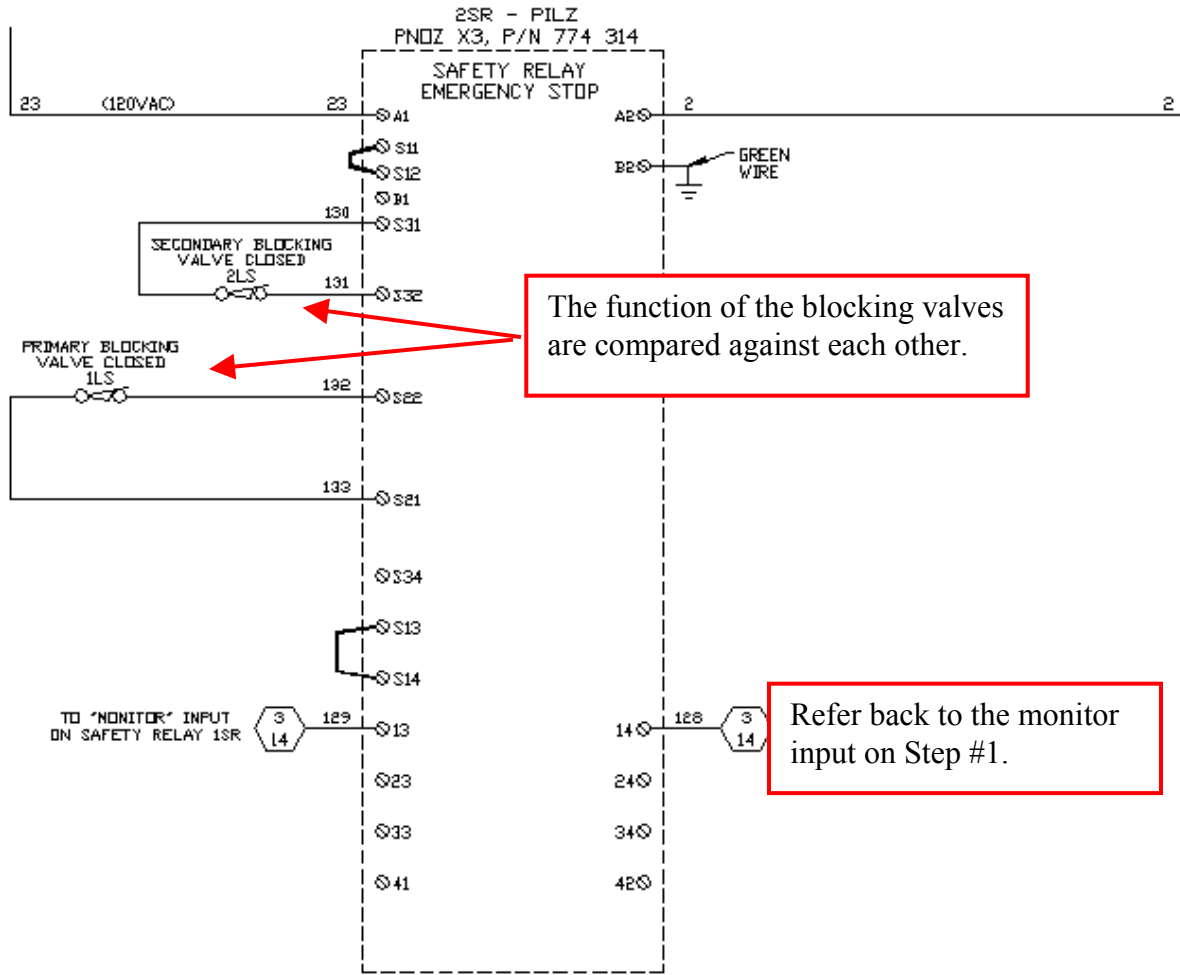
Step #3: Fluid power redundancy



Hydraulic fluid power to all motion valves was initially removed via redundant blocking valves, whenever the two-hand control was released.

Pneumatic fluid power to the clamp has not been removed by any safety circuit or blocking valve. The risk assessment would have indicated that the motion required a Single Channel safety circuit, which is covered by the basic motion control circuit.

Step #4: Fluid power monitoring



The final switching devices, in this case the redundant hydraulic blocking valves, are monitored. When 1SR kills power to the blocking valves, both inputs to 2SR must close, indicating that both blocking valves have functioned, in order for 2SR's output to pass power to the *Monitor* input of 1SR. This allows 1SR to reset the next time the two-hand inputs are pressed.

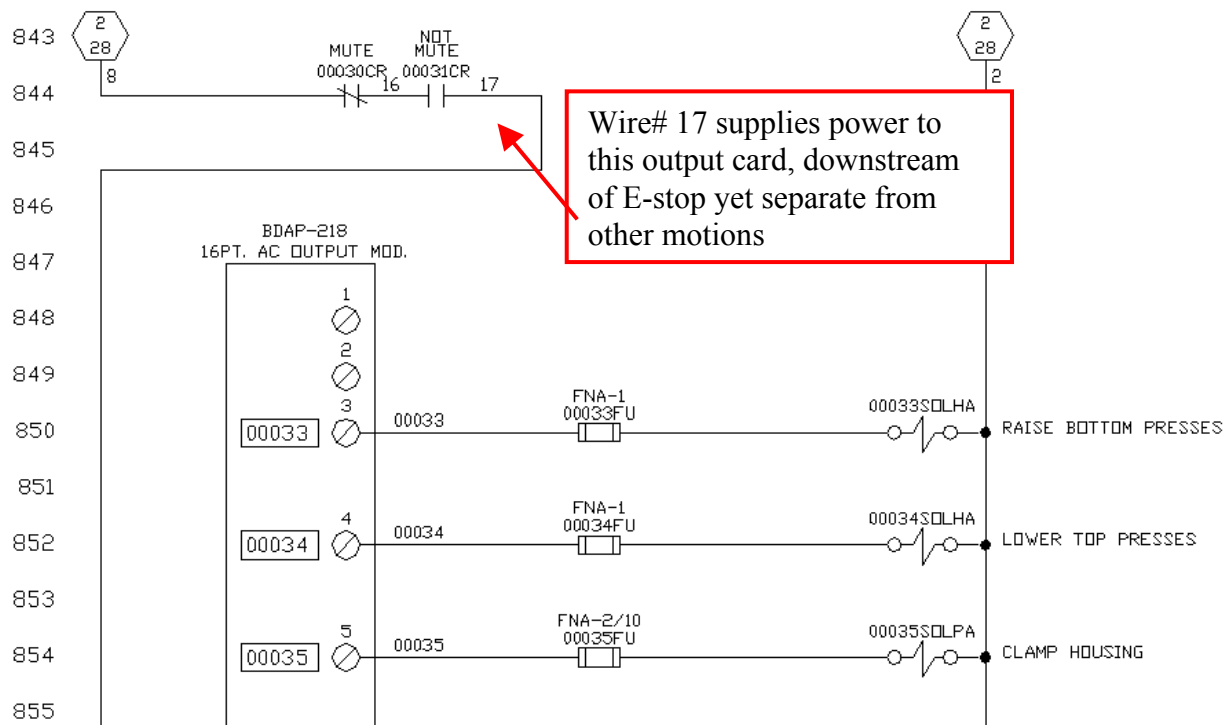
10. Muting Circuit Design

The revisions to the machine's control circuits, accomplishing Control Reliable muting yet driven by PLC logic, are described as follows:

Step #5: Separation of outputs

A critical component to designing the mute system as a hardwired safety circuit independent of the PLC is that the machine has motions which can be separated into those which are allowed to occur while muted, and those which are not. There needs to be multiple motions in each category. It is critical that these motions are on separate output cards, not just receiving power from a separate wire#. More detail is provided in the *Failure Mode Considerations* section of this document.

As it worked out for this machine, a new output card was added and three outputs moved to that card.

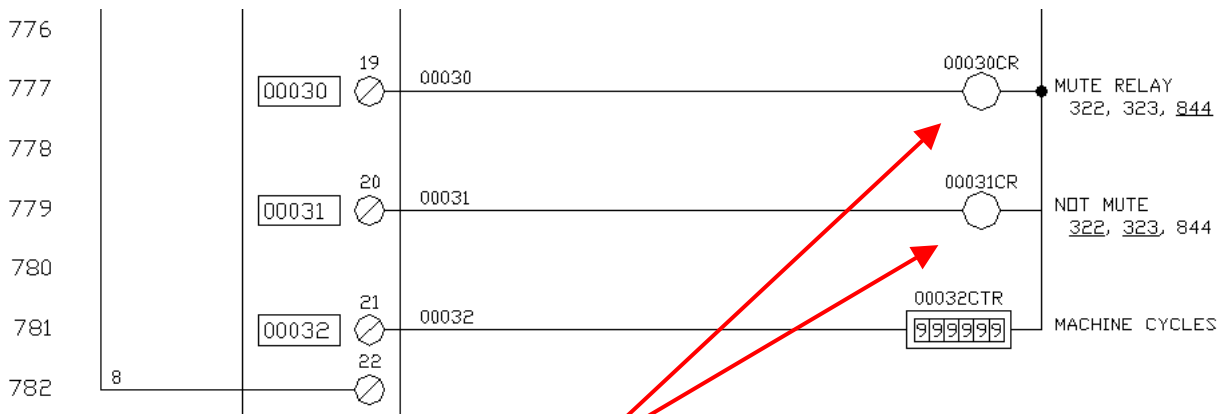


Wire# 17 supplies power to this output card, downstream of E-stop yet separate from other motions

These outputs were separated from the non-hazardous / retract motions.

Raise Bottom Presses and Lower Top Presses are the hazards protected by two-hand control. The initial design did not include the clamp in the two-hand circuit.

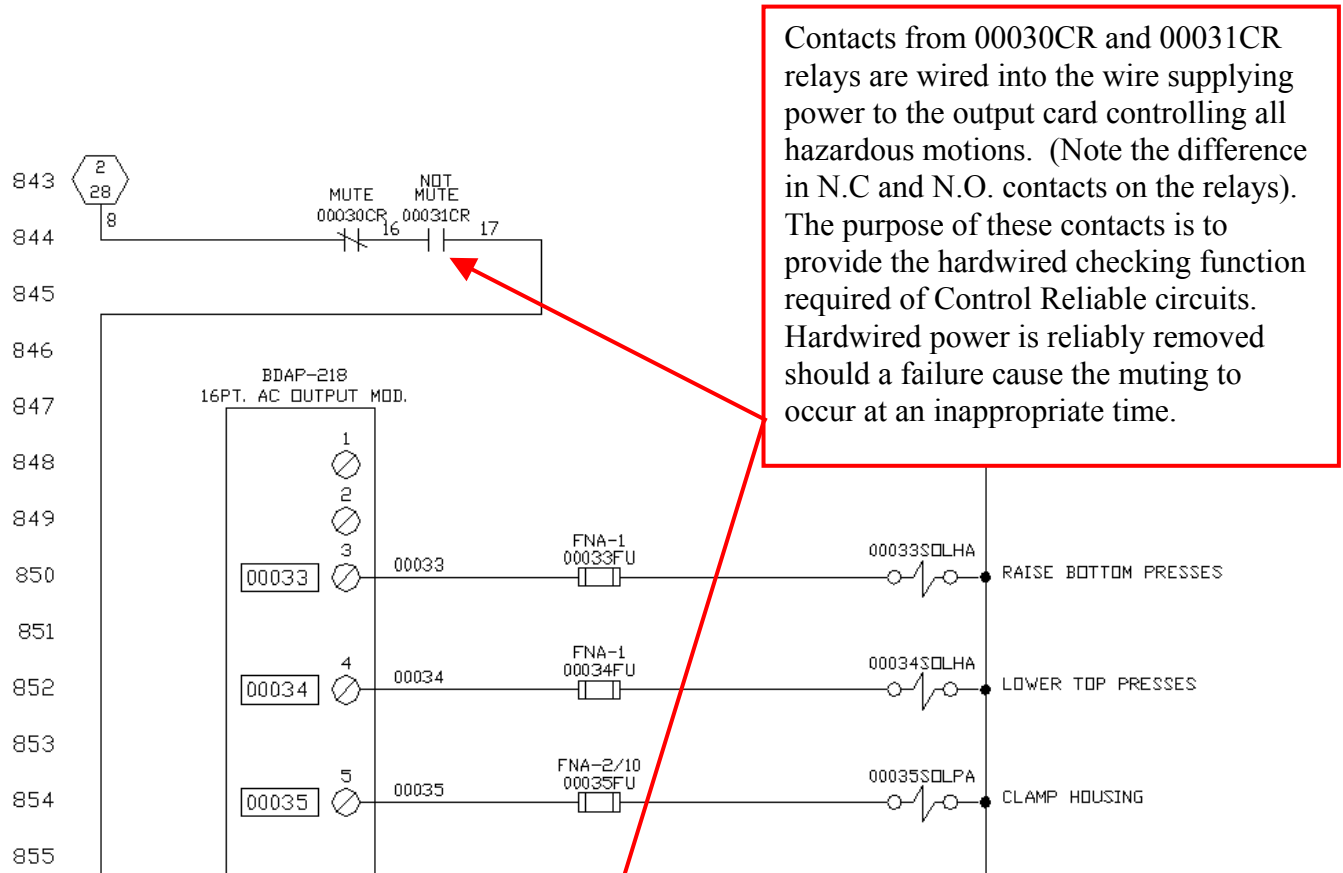
Step #6: PLC driven mute relays



00030CR and 00031CR are direct-drive relays with positively guided contacts. They can be controlled by any PLC output card that does not control hazardous motions. 00030CR is identified as the *Mute Relay* which energizes to provide power to the safety blocking valves when it is safe to release the two-hand control. 00031CR is the NOT state of the 00030CR

Note that the 00030CR / 00031CR cannot be replaced with two outputs driving a safety relay. There are two issues: One- current safety relays do not offer safety contacts which pass power when the relay is off (the contact required in *Step#8* of this document), and, Two- there are logic synchronization issues as noted in section 12.

Step #8: Hardwired safety contacts (checking function)



Contacts from 00030CR and 00031CR relays are wired into the wire supplying power to the output card controlling all hazardous motions. (Note the difference in N.C and N.O. contacts on the relays). The purpose of these contacts is to provide the hardwired checking function required of Control Reliable circuits. Hardwired power is reliably removed should a failure cause the muting to occur at an inappropriate time.

A safety relay cannot be used in place of 00030CR / 00031CR (combined) because the opposite-state contacts required here are not available from a safety relay.

Other Considerations

11. Failure Mode Considerations

Control Reliable circuit applications are by definition to be implemented in hardware, and not controlled by a PLC²⁰. The mute circuit implemented on this machine requires interface with a PLC for determination of *when* it is safe to mute the circuit, yet keeps the safety portion of the circuit as hardware component based. Failures of a single component, such as the PLC, have been addressed per the following failure mode considerations.

Failure mode considerations for the Control Reliable two-hand control and blocking valve circuits are not documented herein.

Normal mode of operation: In normal operation of the machine, 00030CR relay will turn on and mute the two-hand safety relay after the press-to-depth. The mute shuts off upon the next cycle request (two-hand control PLC input), but is turned back on after the washer press. This functionality is controlled by the PLC enabling of 00030CR (and disabling 00031CR) positive guided relay(s).

Failure Modes:

1. If 00030CR hardware should fail in an **"Always On"** state (electronic output failure, coil seizure, contact weld, etc.), the hardwired circuit would remove power to the output card controlling hazardous motion through the N.C. 00030CR contact in the incoming power feed wire (refer to *Steps #5 & #8* of section 10 above). This keeps the machine from sequencing. Particularly, one failure has not caused an improper

mute, yet hardware disables the hazardous motions.

2. If 00030CR hardware should fail in an **"Always Off"** state, the hydraulic blocking valves will be de-energized (go to a blocking state) when the operator releases the two-hand control (refer to *Step #7* of section 10 above). Note that for this mode of failure the machine may actually completely cycle if the operator continues to hold the two-hand control.
3. If there is a program error or other PLC error that allows 00030CR to **"Turn On"** at the wrong time in the cycle (e.g., too early), power will be removed from the hazardous motions output card through the N.C. 00030CR contact in the incoming power feed wire (refer to *Step #5 & #8* of section 10 above). This will hardware disable motion until the failure is corrected. This contact is critical to why this system is considered a hardware safety circuit (not PLC based).
4. If there is a program error that allows 00030CR to **"Turn Off"** at the wrong time in the cycle, the hydraulic blocking valves will be de-energized (go to a blocking state) when the operator releases the two-hand control (refer to *Step #7* of section 10 above).
5. Field wiring, output card electronic failures (all outputs electronically **"Turn On"**), and other failures which would cause 00030CR and 00031CR to function "as the same relay" are addressed by 00031CR being *Not Mute*, the logical opposite of 00030CR.
6. All failure modes of 00031CR are addressed by 00030CR considerations (opposites mode) mentioned in item 1 through 4 above.

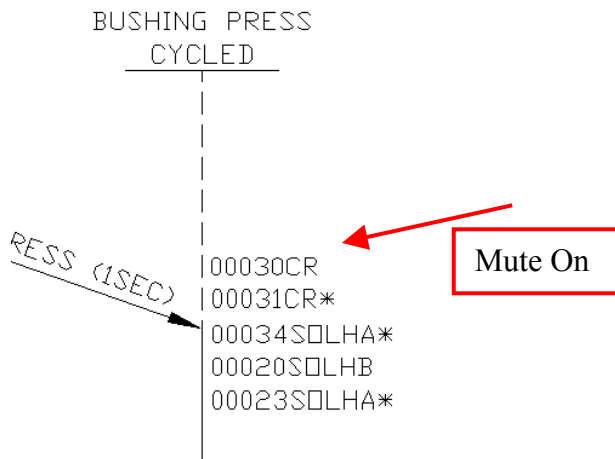
²⁰ DA-2001 item 5.1.4

12. Logic Design Considerations

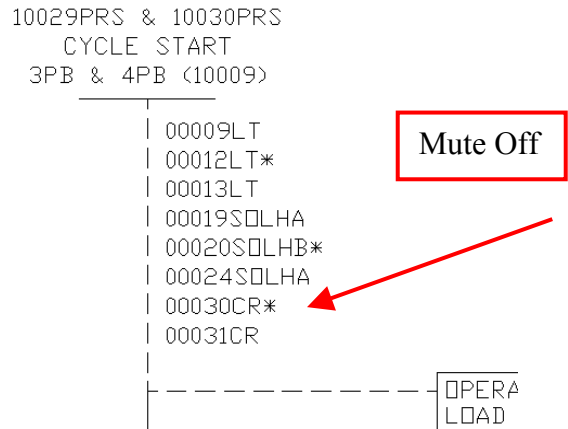
As with all point-of-operation guard applications, the machine sequence logic needs to consider such things as part quality issues if the two-hand is released early and then reapplied. Should the sequence be allowed to continue? These sort of logic issues are independent of the Mute function.

This machine's logic had to be revised to match the new machine sequence; adding the *Mute On* and *Mute Off* points as noted in the line sequence diagram.

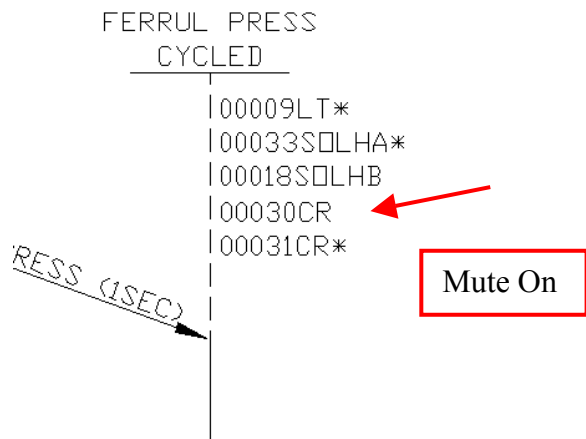
The mute was activated after press to-depth:



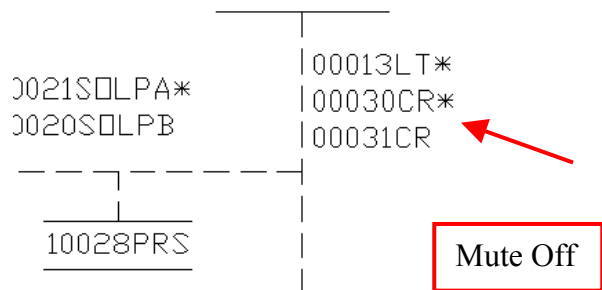
but turned off at the start the second half of the cycle:



The mute was also activated after the washer-press:



and left on until the cycle completed.



12. Logic Design Considerations (continued)

One final logic-related issue should be considered. As pointed out (in *Step #6* from section 10 of this document), there are logic constraints on designs which had used a PLC-driven safety relay for the mute function. Due to reaction times (both *On* and *Off*) for safety relay input channels, PLC de-bounce timers are frequently required when switching between *Mute On* and *Mute Off* modes. To avoid nuisance safety relay lock-ups, logic and timers would be used to keep the machine in either *Mute On* or *Mute Off* mode for a minimum amount of time (typically 0.5 seconds). This de-bounce particular **does not** need to be considered for the positive-guided relay version of mute presented in this document.

The mute logic is very basic; mute while in-cycle and at the appropriate sequences. A printout of the machine logic is not embedded in this document.

Annex A. Bibliography

DA-2006, *Design-In Health and Safety Specification*, Delphi Automotive Systems, Version 1.0, December 20, 2001

DA-2001, *Specification for the Application of Safety Circuits*, Delphi Corporation, Revision 2.1, March 2003

ANSI B11.19-2003, *Performance Criteria for Safeguarding*, American National Standards Institute, Inc.

ANSI B11.19-1990, *Safeguarding When Referenced by the Other B11 Machine Tool Safety Standards – Performance Criteria for the Design, Construction, Care, and Operation*, American National Standards Institute, Inc.

NFPA 79, *Electrical Standard for Industrial Machinery 2002 Edition*, National Fire Protection Agency

EN 574, *Safety of Machinery – Two-Hand Control Devices – Functional Aspects – Principles for Design*, European Committee for Standardization

