LISTEN.
THINK.
SOLVE.℠

APPLICATION NOTE

INTERFACING AC DRIVES WITH SAFETY RELAYS

Purpose

This application note describes examples of how to interface AC Drives with safety relays. This document is intended to provide support for typical applications and only covers a sub task of a typical customer application involving safety technology. The examples shown do not claim to be complete and do not represent customer specific solutions.

Rockwell Automation reserves the right to make changes to this document without prior notice. When using examples in this document the user recognizes that Rockwell Automation cannot be made liable for any damage or claims. Because there are many application-specific variables, users MUST ensure that products are correctly used and the appropriate architecture is deployed.

IMPORTANT: A risk assessment should be performed to ensure that all task-hazard combinations have been identified and addressed. The risk assessment may require additional circuitry to reduce the risk to a tolerable level. Safety circuits must take into consideration safety distance calculations which are not part of the scope of this document. This application note is targeted for advanced users and assumes knowledge of drive and safety systems. Please contact Rockwell Automation Global Manufacturing solutions to find out more about our safety risk assessment services capabilities.

General Information

References

- NFPA79, Electrical Standards for Industrial Machinery, 2007 Edition
- EN954-1, Safety of Machinery - safety related parts of a control system - Part 1: General Principles for Design
- EN60204-1 : 2006 Safety of Machinery - Electrical Equipment of Machines - Part 1: General Requirements

Stop Categories

- Stop Category 0 - Coast. Immediate removal of power to the motor. With immediate removal of power to the motor, the motor will coast to stop. The time required to stop motion is dependent on the load inertia and speed as well as the friction in the mechanical power transmission equipment used in the system.
- Stop Category 1 - Controlled. Controlled Stop then removal of power to the motor. A ramp to stop will be used to control the mechanical power transmission to rest then power is removed from the motor. The time required to bring the mechanical system to rest is dependent upon load inertia and speed as well as the regenerative dissipation capacity of the drive.

Safety Categories per EN954-1

SUMMARY OF REQUIREMENTS:	SYSTEM BEHAVIOR:
Category B (see note 1) - Safety related parts of machine control systems and/or their protective equipment, as well as their components, shall be designed, constructed, selected, assembled and combined in accordance with relevant standards so that they can withstand the expected influence.	When a fault occurs it can lead to a loss of the safety function.
Category 1 - The requirements of B apply together with the use of well tried safety components and the safety principles.	As described for category B but with higher safety related reliability of the safety related function. (The higher the reliability, the less the likelihood of a fault.)
Category 2- The requirements of B and the use of well tried safety principles apply. The safety function(s) shall be checked at machine start-up and periodically by the machine control system. If a fault is detected a safe state shall be initiated or if this is not possible a warning shall be given.	The loss of safety function is detected by the check. The occurrence of a fault can lead to the loss of safety function between the checking intervals.
Category 3 (see notes 2 & 3) - The requirements of B and the use of well tried safety principles apply. The system shall be designed so that a single fault in any of its parts does not lead to the loss of safety function.	When the single fault occurs the safety function is always preformed. Some but not all faults will be detected. An accumulation of undetected faults can lead to the loss of safety function.
Category 4 (see notes 2 & 3) - The requirements of B and the use of well tried safety principles apply. The system shall be designed so that a single fault in any of its parts does not lead to the loss of safety function. The single fault is detected at or before the next demand on the safety function. If this detection is not possible then an accumulation of faults shall not lead to a loss of safety function.	When the faults occur the safety function is always preformed. The faults will be detected in time to prevent the loss of safety functions.

Note 1: Category B in itself has no special measures for safety but it forms the base for the other categories.

Note 2: Multiple faults caused by a common cause or as inevitable consequences of the first fault shall be counted as a single fault.

Note 3: The fault review may be limited to two faults in combination if it can be justified but complex circuits (e.g. microprocessor circuits) may require more faults in combination to be considered.

Component Descriptions

- Gate Interlock - The Trojan gate interlock uses direct opening contacts. When the gate is opened, the contacts in the interlock are forced open by non-resilient components (e.g., not by springs). A redundant (two) set of double break contacts are designed to ensure that at least one signal is sent to the safety relay, when the gate is opened.
- E-Stop - When the E-Stop button is pressed the safety function is activated (Drive goes to safe state). When a contactor is used it is opened by the E-Stop circuit. The E-stop button must utilize direct-opening contacts. The button must latch to an open state when the contacts open (i.e., you must not be able to tickle the contacts without latching the button). The button must be a red with a yellow background.
- Contactor - Provides electromechanical disconnection of the motor from the drive. Its normally-closed mechanically linked contacts are monitored by the safety relay to help ensure that the contactor has dropped out before the next resetting of the safety relay.
- Start / Stop Pushbuttons - The Start and Stop pushbuttons are used to turn the drive on and off. They are also symbolic of the non-safety related parts of the machine control system. These buttons can be replaced by a programmable control system.
- Generic Drive - Describes a drive that does not contain a Safe-off option
- The PowerFlex® Safe-off Option Board:
  - is designed to safely remove power from the gate firing circuits of the drives output power devices (IGBT's). This prevents then from switching in the pattern necessary to generate AC power to the motor.
  - Can be used in combination with other safety devices to meet the Stop and protection against restart requirements of EN954-1.

> **IMPORTANT:** The option is suitable for performing mechanical work on the drive system or affected area of a machine only. It does not provide electrical safety.

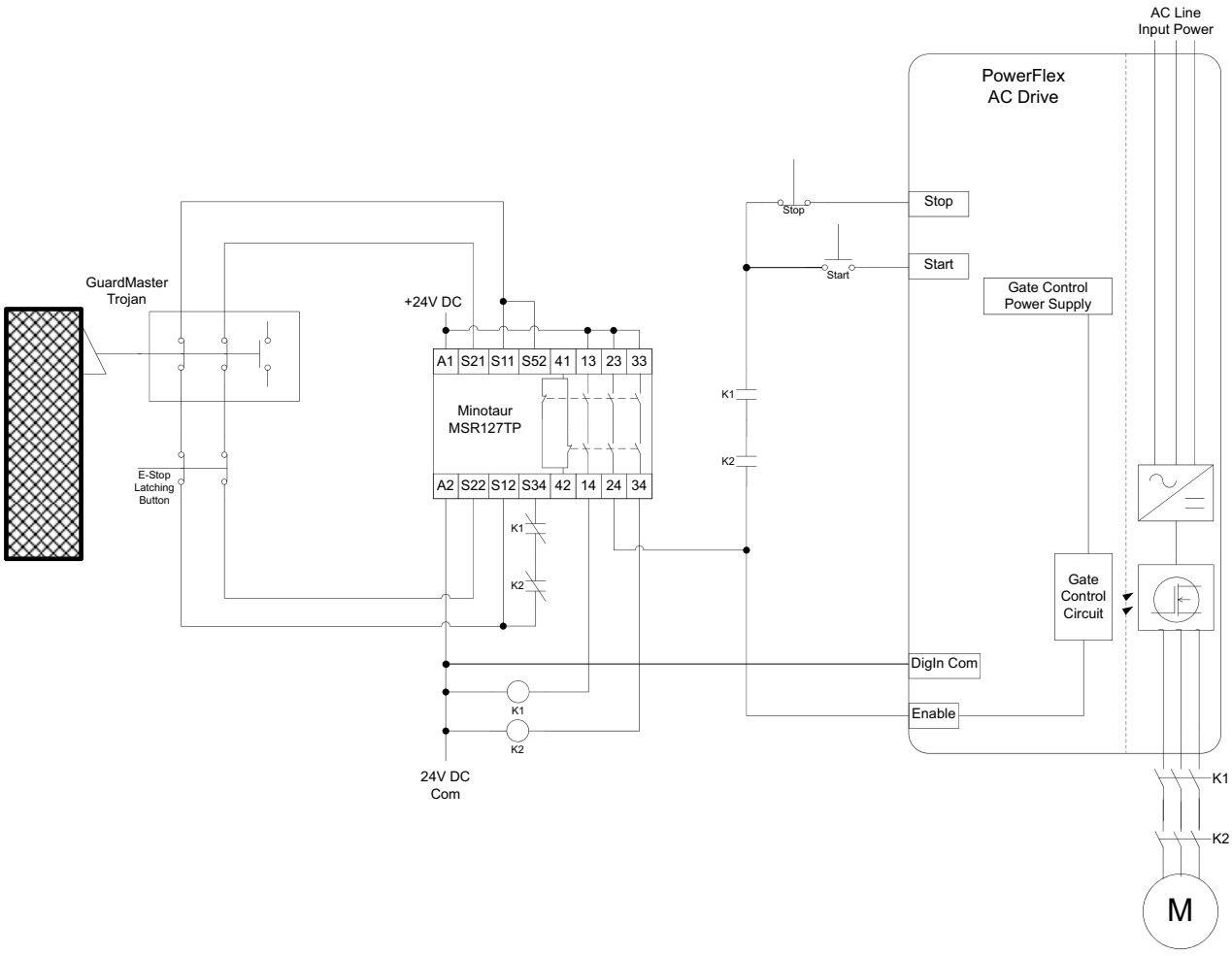
- Safety Relay Reset - The examples in this document use an automatic reset scheme for the safety relay. The use of a manual or automatic reset should be dictated by the application.

Related Publications

- DriveGuard® User Manual for the Safe-off Option

Example: Drive Without Safe-off, Coast Stop

OVERVIEW:
This example shows how to provide Stop and protection against restart (Category 3 per EN954-1) on a drive without a safe-off feature.
The contactors can also satisfy the NFPA79 Emergency Stop requirements.
Stop Type: Category 0, Coast
Safety Level: EN954-1, Category 3
Drive Type: Drive without Safe-off option
Other: Output contactor for NFPA79 & EN60204 Emergency Stop operation



Circuit Operation:

The gate will trigger the safety function. When triggered the safety relay outputs (Terminals 13 to 14, 23 to 24, and 33 to 34) open. This immediately removes +24vdc from the drive Enable, the drive Start/Stop inputs and both contactor coils K1 & K2. The result is the drive is disabled, a stop signal is asserted, the contactors open, and the motor will coast to stop. The N.O. auxiliary contact of K1 and K2 open to prevent a drive Start before the contactors close. The N.C. auxiliary contacts are monitored by the safety relay at terminals S52 & S34.

When the E-Stop is activated, the safety function is triggered and performs the same as the gate triggered function. Restoration of the E-Stop also recovers in the same manner as the gate restoration.

If the contactors N.C. auxiliary contacts are in an abnormal state, as monitored by the safety relay (S52 & S34) the safety relay will prevent operation at the next cycling of the "safety" circuit.

The safe-off jumper in the drive must be installed when the Safe-off Option is not present.

Other Considerations:

Drives with hardware enable feature:

-PowerFlex® 40 or 40P drives do not have programmable enable, this must be accomplished by removing hardware enable jumper and then programming one of the digital inputs as a stop.

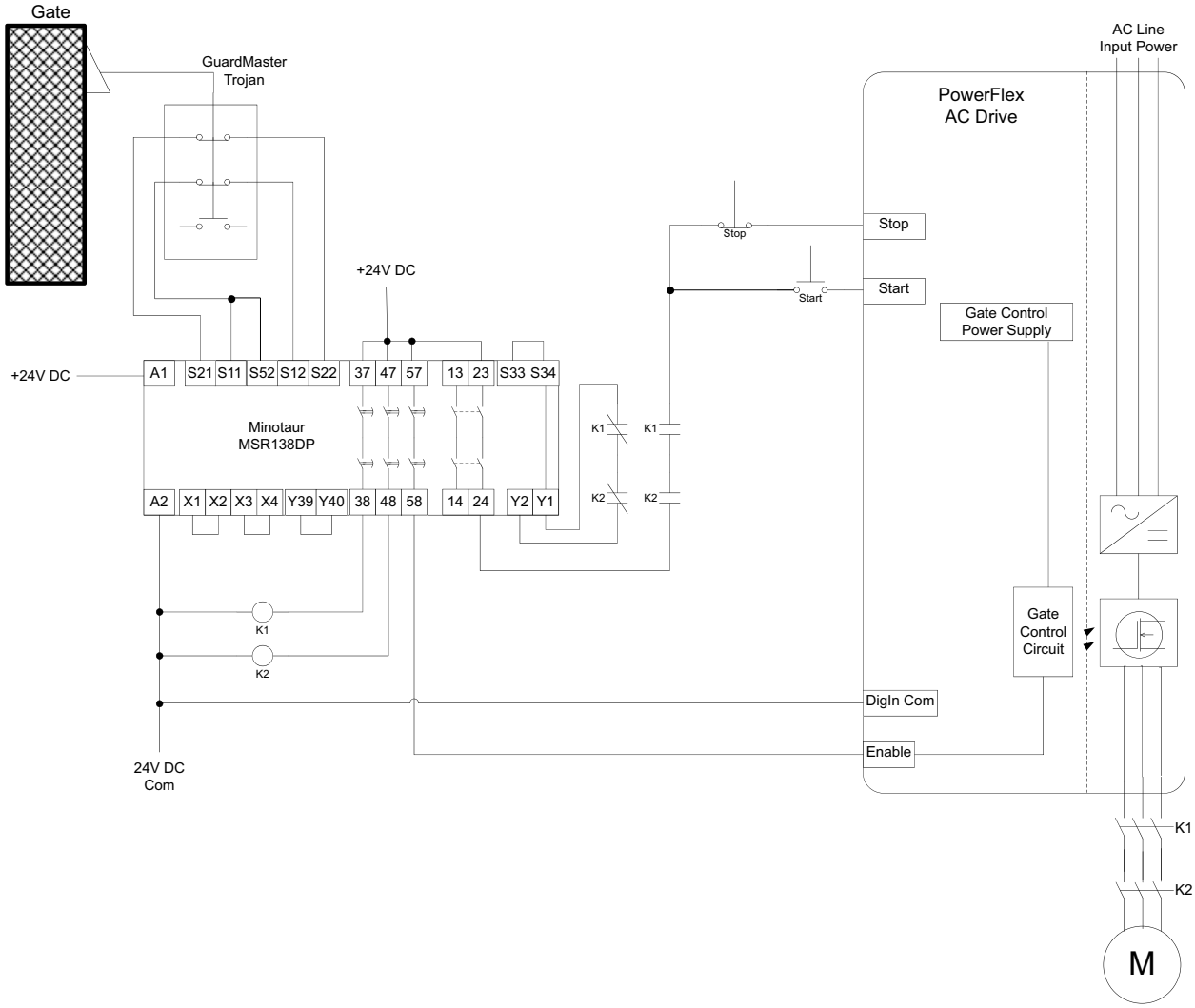
-PowerFlex® 70, 700, 700S or 700H drive hardware enable is not required but in general is recommended when the drive is interfaced with a safety relay.

The Drives I/O power supply may not have sufficient capacity to operate the safety relay and contactors. An external 24V DC power supply should be used for these devices.

Example: Drive Without Safe-off, Controlled Stop

OVERVIEW:
This example shows how to provide Controlled Stop and protection against restart (Category 3 per EN954-1) on a drive without a safe-off feature. The contactors can also satisfy the NFPA79 Emergency Stop requirements.

Stop Type: Category 1, Controlled
Safety Level: EN954-1, Category 3
Drive Type: Drive without Safe-off option
Other: Output contactor for NFPA79 & EN60204 Emergency Stop Operation



Circuit Operation:

The gate will trigger the safety function. When triggered the safety relay outputs (Terminals 13 to 14 and 23 to 24) open. This immediately removes +24vdc from the drive Start/Stop input. The result is the drive stop signal is asserted and a ramp to stop is issued.

Once the time delay in the safety relay expires, the safety relay time delay contacts (Terminals 37 to 38, 47 to 48, and 57 to 58) open. The +24vdc is then removed from the drive enable as well as both contactor coils K1 & K2. The N.O. auxiliary contact of K1 and K2 open to prevent a drive Start before the contactors close. The N.C. auxiliary contacts are monitored by the safety relay at terminals Y1 & Y2.

Note: The time delay of the safety relay must be greater than the deceleration ramp time of the drive otherwise a coast stop will occur when the timer expires.

When the gate is restored and satisfies the safety relay inputs, the safety relay is reset (terminals Y39 and Y40 are N.C.). The safety relay outputs are energized restoring +24vdc to the drive Enable input, the coils of the contactors and the Drive Start/Stop. A start command must be issued to the drive to restart.

Other Considerations:

The safe-off jumper in the drive must be installed when the Safe-off Option is not present.

Drives with hardware enable feature:

-PowerFlex® 40 or 40P drives do not have programmable enable, this must be accomplished by removing hardware enable jumper and then programming one of the digital inputs as a stop.

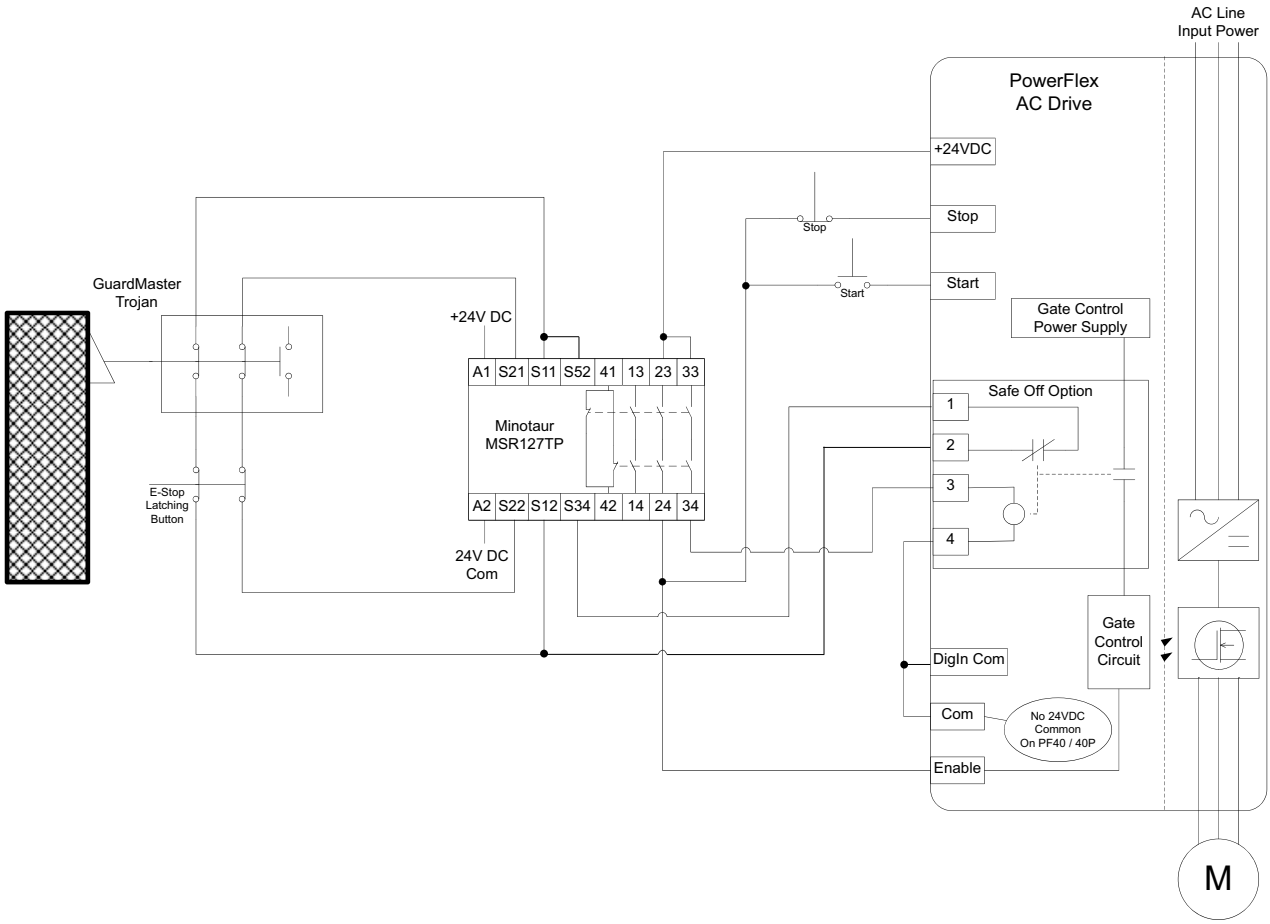
-PowerFlex® 70, 700, 700S or 700H drive hardware enable is not required but in general is recommended when the drive is interfaced with a safety relay.

The Drives I/O power supply may not have sufficient capacity to operate the safety relay and contactors. An external 24V DC power supply should be used for these devices.

Example: Safety Drive, Coast Stop

OVERVIEW:
This example shows how to provide Stop and protection against restart (Category 3 per EN954-1) on a drive with a safe-off feature.

Stop Type: Category 0, Coast
Safety Level: EN954-1, Category 3
Drive Type: Drive with Safe-off Option
Other: NFPA79 & EN60204 Emergency Stop Operation



The gate will trigger the safety function. When triggered the safety relay outputs (Terminals 13 to 14, 23 to 24, and 33 to 34) open. This immediately removes +24vdc from the drives enable and Start/Stop inputs, and the Safe-off Option relay. The result is the drive is disabled, a stop signal is asserted, the Safe-Off Option goes to a safe state (off), and the motor will coast to stop. The Safe-off Option N.C. auxiliary contacts are monitored by the safety relay at terminals S52 & S34.

When the gate is restored and satisfies the safety relay inputs, the safety relay is reset. The safety relay outputs are energized restoring +24vdc to the drive Enable input and Drive Not Stop, and the Safe-off Option relay. A start command must be issued to the drive to restart.

If the Safe-off monitor contact is in an abnormal state, as monitored by the safety relay (S52 & S34) the safety relay will prevent operation at the next cycling of the "safety" circuit.

When the E-Stop is activated, the safety function is triggered and performs the same as the gate triggered function. Restoration of the E-Stop also recovers in the same manner as the gate restoration.

Other Considerations:

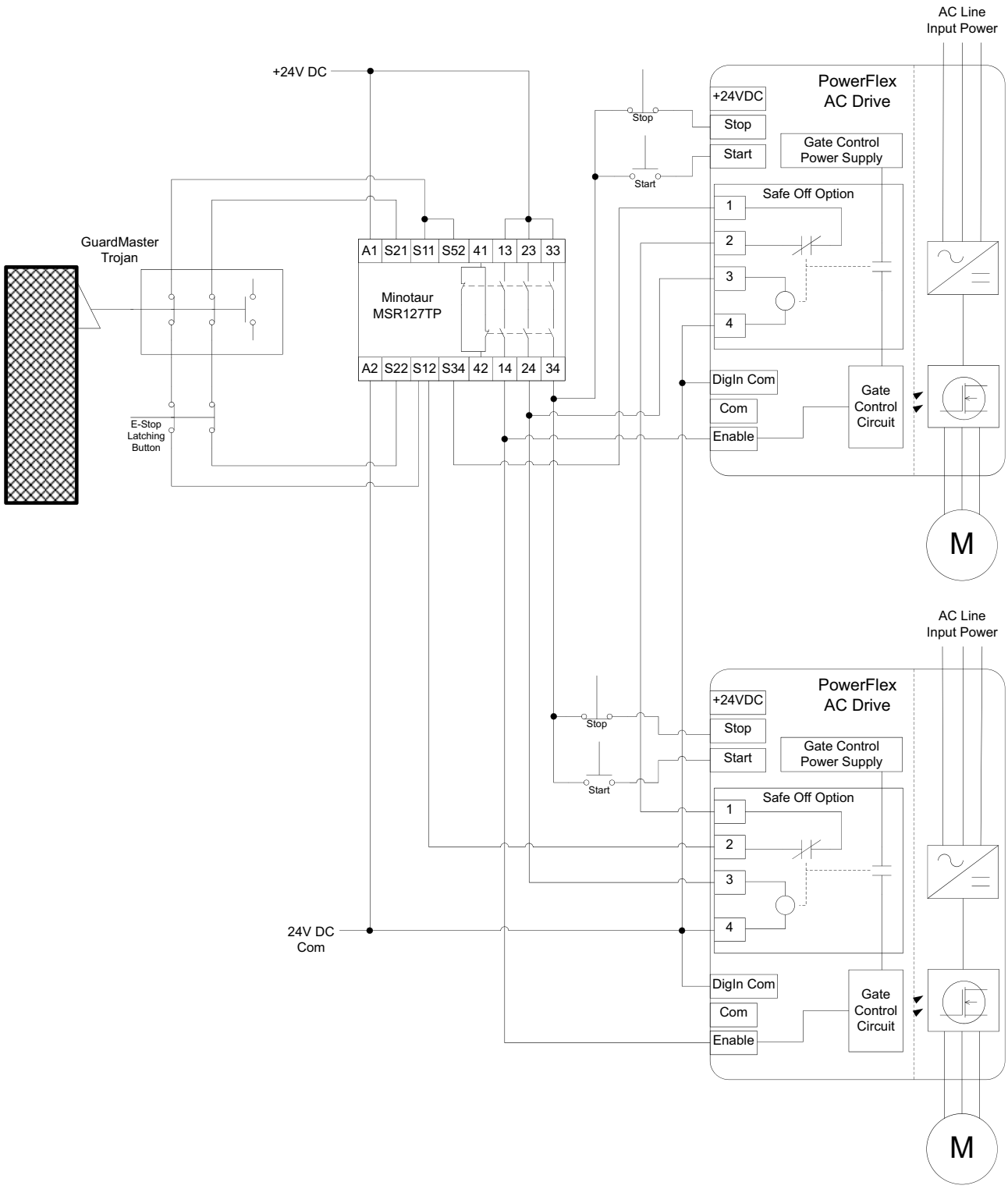
On PowerFlex® 40P AC drives the 24VDC is referenced to the digital common, jumper to Com does not apply. The hardware enable jumper in the drive must be removed if the Safe-off Option is installed. If not, the PowerFlex® 70 drive will fault (F111) when a start command is issued and the PowerFlex® 40P will fault on (F111) upon first removal of the enable.
Drives with hardware enable feature:

- -PowerFlex® 40P AC drives do not have programmable enable, this must be accomplished by removing hardware enable jumper and then programming one of the digital inputs as a stop.
- -PowerFlex® 70, 700, 700S or 700H drive hardware enable is not required but in general is recommended when the drive is interfaced with a safety relay.

The Drives I/O power supply may not have sufficient capacity to operate the safety relay. An external 24V DC power supply should be used.

Example: Safety Drive, Coast Stop, Multiple Drives

Stop Type: Category 0, Coast
Safety Level: EN954-1, Category 3
Drive Type: Drive with Safe-Off Option
Other: NFPA79 & EN60204 Emergency Stop Operation



Circuit Operation:

The gate will trigger the safety function. When triggered the safety relay outputs (Terminals 13 to 14, 23 to 24, and 33 to 34) open. This immediately removes +24vdc from the drives enable and Start/Stop inputs, and the Safe-off Option relay. The result is the drive is disabled, a stop signal is asserted, the Safe-Off Option goes to a safe state (off), and the motor will coast to stop. The Safe-off Option N.C. auxiliary contacts are monitored by the safety relay at terminals S52 & S34.

When the gate is restored and satisfies the safety relay inputs, the safety relay is reset. The safety relay outputs are energized restoring +24vdc to the drive Enable input and Drive Not Stop, and the Safe-off Option relay. A start command must be issued to the drive to restart.

If the Safe-off monitor contact is in an abnormal state, as monitored by the safety relay (S52 & S34) the safety relay will prevent operation at the next cycling of the "safety" circuit.

When the E-Stop is activated, the safety function is triggered and performs the same as the gate triggered function. Restoration of the E-Stop also recovers in the same manner as the gate restoration.

Other Considerations

A separate 24V supply must be used to drive the enable and safe-off option, when multiple drives are driven by a common safety relay.

The safe-off monitor contact of each drive must be connected in series.

The number of drives is limited by the current switching capability of the safety relay (e.g. MSR127TP) contacts.

The hardware enable jumper in the drive must be removed if the Safe-off Option is installed. If not, the PowerFlex® 70 drive will fault (F111) when a start command is issued and the PowerFlex® 40 or 40P drive will fault on (F111) upon first removal of the enable.

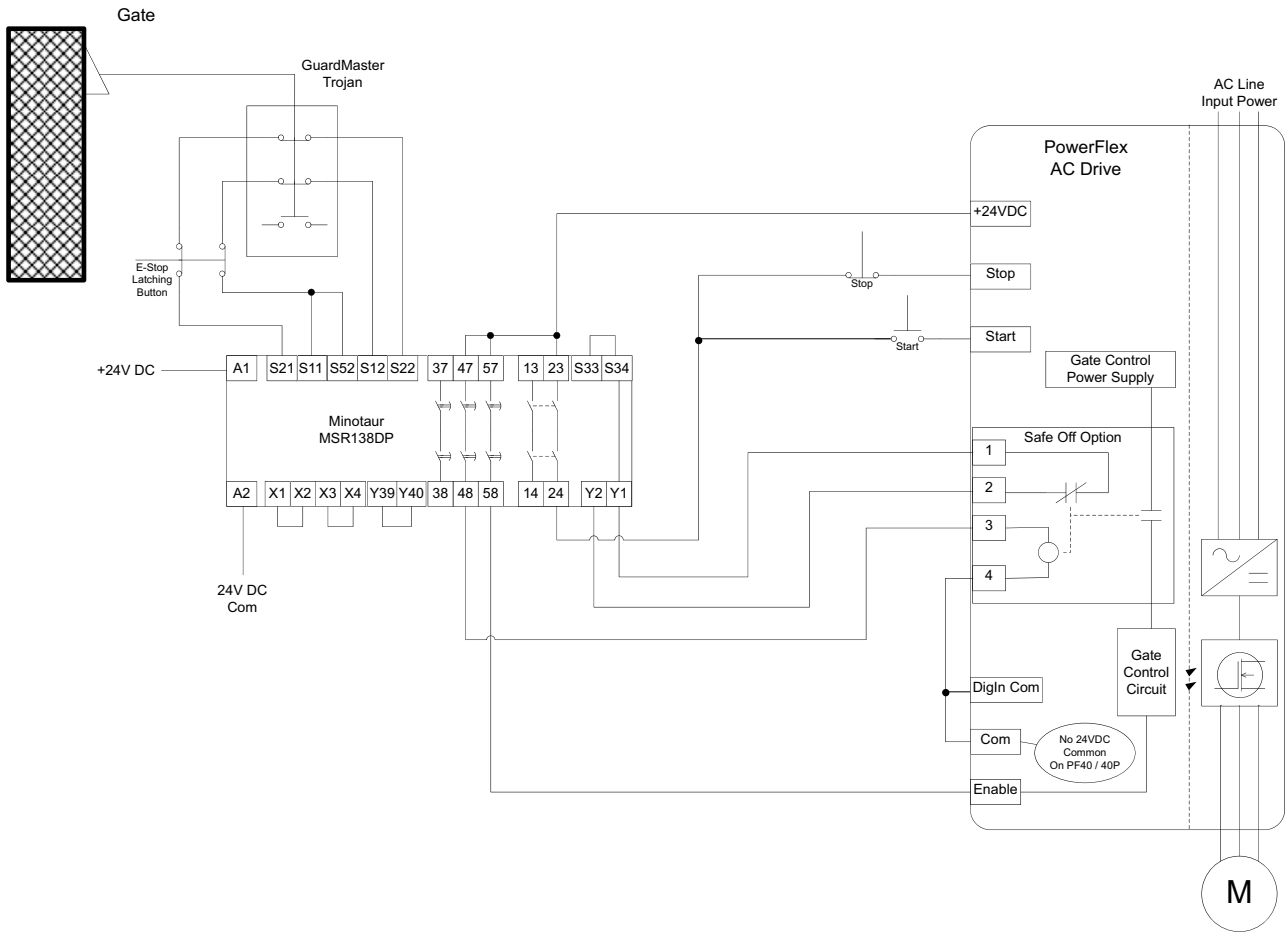
Drives with hardware enable feature:

- -PowerFlex® 40 or 40P drives do not have programmable enable, this must be accomplished by removing hardware enable jumper and then programming one of the digital inputs as a stop.
- -PowerFlex® 70, 700, 700S or 700H drive hardware enable is not required but in general is recommended when the drive is interfaced with a safety relay.

Example: Safety Drive, Controlled Stop

OVERVIEW:
This example shows how to provide Controlled Stop and protection against restart (Category 3 per EN954-1) on a drive with a safe-off feature.

Stop Type: Category 1, Controlled
Safety Level: EN954-1, Category 3
Drive Type: Drive with Safe-off Option
Other: NFPA79 & EN60204 Emergency Stop Operation



Circuit Operation:

The gate will trigger the safety function. When triggered the safety relay outputs (Terminals 13 to 14 and 23 to 24) open. This immediately removes +24vdc from the drive Start/Stop input. The result is the drive stop signal is asserted and a ramp to stop is issued.

Once the time delay in the safety relay expires, the safety relay time delayed contacts (Terminals 37 to 38, 47 to 48, and 57 to 58) open. The +24vdc is then removed from the drive Enable input as well as the Safe-off Option. The Safe-off Option goes to a safe state (off).

Note: The time delay of the safety relay must be greater than the deceleration ramp time of the drive otherwise a coast stop will occur when the timer expires.

When the gate is restored and satisfies the safety relay inputs, the safety relay is reset (terminals Y39 and Y40 are N.C.). The safety relay outputs are energized restoring +24vdc to the drive Enable input, the Safe-off Option and the Drive Start/Stop. A start command must be issued to the drive to restart.

If the Safe-off monitor contact is in an abnormal state, as monitored by the safety relay (Y1 & Y2) the safety relay will prevent operation at the next cycling of the "safety" circuit.

Other Considerations:

On PowerFlex® 40P AC drives the 24VDC is referenced to the digital common, jumper to Com does not apply.

The hardware enable jumper in the drive must be removed if the Safe-off Option is installed. If not, the PowerFlex® 70 drive will fault (F111) when a start command is issued and the PowerFlex® 40P AC drive will fault on (F111) upon first removal of the enable.

Drives with hardware enable feature:

-PowerFlex® 40 or 40P drives do not have programmable enable, this must be accomplished by removing hardware enable jumper and then programming one of the digital inputs as a stop.

-PowerFlex® 70, 700, 700S or 700H drive hardware enable is not required but in general is recommended when the drive is interfaced with a safety relay.

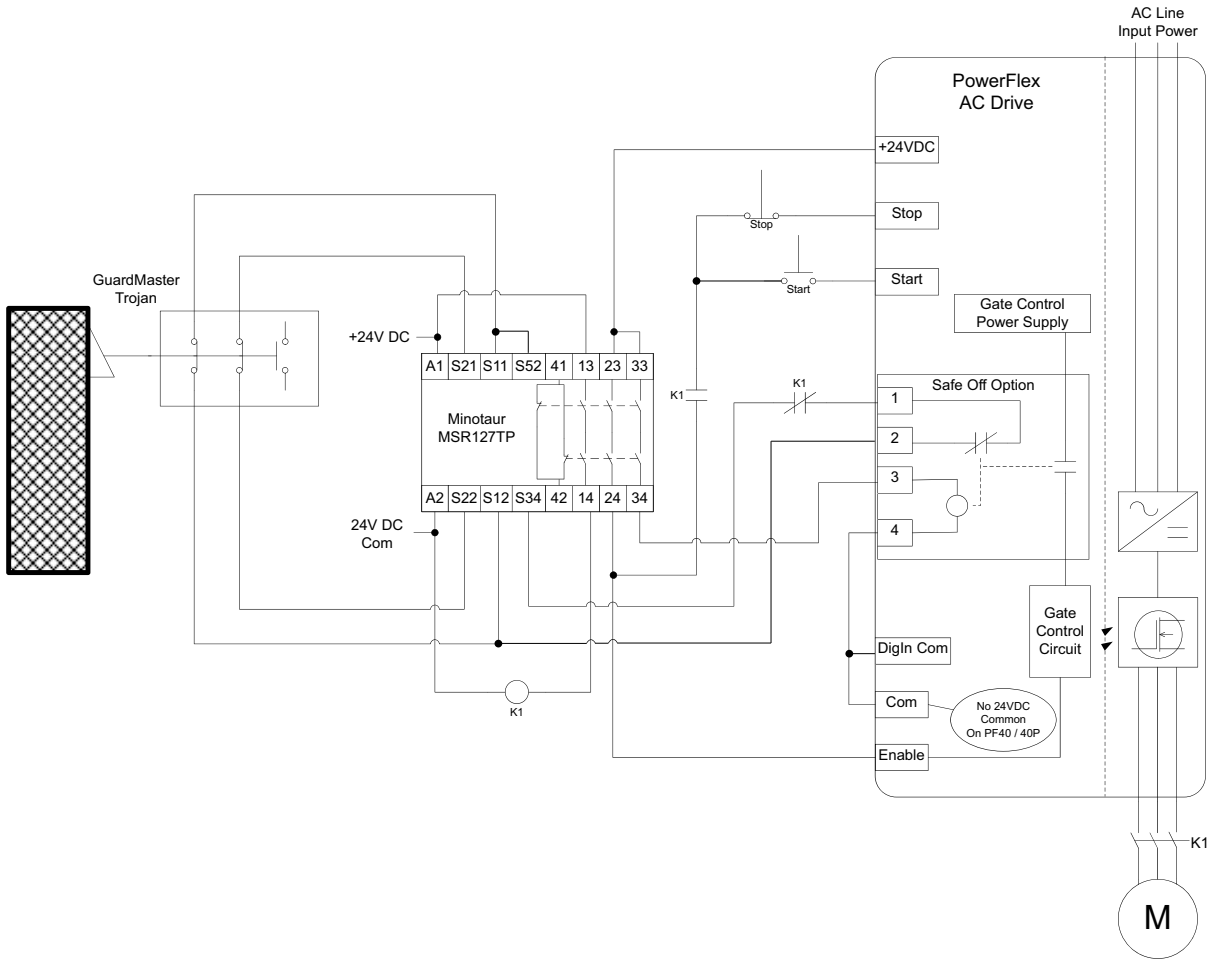
The Drives I/O power supply may not have sufficient capacity to operate the safety relay. An external 24V DC power supply should be used.

Example: Safety Drive, Coast Stop, Category 4

OVERVIEW:
This example shows how to provide Stop and protection against restart (Category 4 per EN954-1) on a drive with a safe-off feature.

Stop Type: Category 0, Coast
Safety Level: EN954-1, Category 4
Drive Type: Drive with Safe-Off Option

NOTE: A PowerFlex safety drive, when used with suitable safety components, provides protection according to EN 954-1:1996; safety performance Category 3 for safe-off and protection against restart. However, by adding the redundant component the system is capable of meeting category 4. The safe-off option is just one element of a complete safety control system. All components in the system must be chosen and applied correctly to achieve the desired level of operator safeguarding.



Circuit Operation:

The gate will trigger the safety function. When triggered the safety relay outputs (Terminals 13 to 14, 23 to 24, and 33 to 34) open. This immediately removes +24vdc from the drives enable and Start/Stop inputs, K1's contactor coil, and the Safe-off Option relay. The result is the drive is disabled, a stop signal is asserted, the Safe-off Option goes to a safe state (off), K1 contactor opens, and the motor will coast to stop. The N.O. auxiliary contact of K1 opens to prevent a drive Start before the contactor closes. The N.C. auxiliary contacts are monitored by the safety relay at terminals S52 & S34.

When the gate is restored and satisfies the safety relay inputs, the safety relay is reset. The safety relay outputs are energized restoring +24vdc to the drive Enable input and Drive Not Stop, the coil of the K1 contactor, and the Safe-off Option relay. A start command must be issued to the drive to restart.

If Safe-off monitor contact and/or K1's contactor N.C. auxiliary contact are in an abnormal state, as monitored by the safety relay (S52 & S34) the safety relay will prevent operation at the next cycling of the "safety" circuit.

Other Considerations:

On PowerFlex® 40P AC drives the 24VDC is referenced to the digital common, connection from "DigIn Com" to "Com" does not apply.

The hardware enable jumper in the drive must be removed if the Safe-off Option is installed. If not, the PowerFlex® 70 drive will fault (F111) when a start command is issued and the PowerFlex® 40P AC drive will fault on (F111) upon first removal of the enable.

Drives with hardware enable feature:

-PowerFlex® 40P AC drives do not have programmable enable, this must be accomplished by removing hardware enable jumper and then programming one of the digital inputs as a stop.

-PowerFlex® 70, 700, 700S or 700H drive hardware enable is not required but in general is recommended when the drive is interfaced with a safety relay.

The Drives I/O power supply may not have sufficient capacity to operate the safety relay. An external 24V DC power supply should be used.

When considering the categories, you need to look at all aspects of the system, as each portion has it's own risk reduction requirements. With these considerations, the machine designer can evaluate the cost / benefit tradeoffs to achieve the desired risk reduction.

1. Input devices
To achieve category 4, connect only one device to one safety relay. If you add multiple devices in series (a very common practice), the category drops to 3. If a safety PLC is used, then typically, the input devices are connected to separate inputs and this will achieve category 4.

2. Logic device:
The safety relay or Safety PLC must be rated for category 4 on both immediate and delayed (when used) outputs.

3. Output devices
The Drive, by itself is rated for category 3. The Drive plus one contactor achieves category 4, as long as both the drive and contactor are monitored.

4. Monitoring
Category 3 requires monitoring of at least one output device
Category 4 requires monitoring of two output devices.

www.rockwellautomation.com

Power, Control and Information Solutions Headquarters

Americas: Rockwell Automation, 1201 South Second Street, Milwaukee, WI 53204-2496 USA, Tel: (1) 414.382.2000, Fax: (1) 414.382.4444
Europe/Middle East/Africa: Rockwell Automation, Vorstlaan/Boulevard du Souverain 36, 1170 Brussels, Belgium, Tel: (32) 2 663 0600, Fax: (32) 2 663 0640
Asia Pacific: Rockwell Automation, Level 14, Core F, Cyberport 3, 100 Cyberport Road, Hong Kong, Tel: (852) 2887 4788, Fax: (852) 2508 1846

DRIVES-AP003A-EN-P–April 2007