Machinery Safety

Making industrial machinery safe for operators is the responsibility of every machine designer and builder. Over the years, a variety of regulations have been enacted to establish standards for safe machines. The primary European machine safety standards today are EN ISO 13849-2:2008 "Safety of machinery -- Safety-related parts of control systems -- Part2: Validation" and IEC 62061 "Safety of machinery – Functional safety of safety-related electrical, electronic and programmable electronic control systems." As of December 31, 2011 these standards superseded EN 954-1.

The two standards differ in the how a machine builder must document and analyze machinery to prove safety and compliance with the standard. Both standards have, in common, a need for safe components that support and simplify building a safe machine.

Many industry leaders are trying to eliminate the old approach of machine control with independent safety monitoring. The goal is to change from two designs to one integrated design. The old approach was to first design the machine control and then design safety monitoring and control around the machine control. The new approach only requires one design with both functions integrated. In addition to the benefits of 'one design' is the promise for better diagnostics, both machine and safety, that lead to more efficient and safer fault recovery.

ORMEC Servo Drive Safety Features

To aid in the design of safe machinery, ORMEC offers safety circuit options for the XD Indexer and S2D network servo drive families. These options provide a method to place the drive in a safe mode without the need for additional external components to power down the drive.

The EN ISO 13849:2008 and IEC 62061 standards detail a number of safe operational levels and functions. They differ in the amount of control and operation available and the cost to implement these options. The ORMEC servo drives have a Safe Torque Off function option. Additional safety function options are under development.

Safe Torque Off

With the Safe Torque Off (STO) function, power from the motor is safely removed and prevented. When active, no torque or force from the drive can be applied to cause motion in the motor. All current generating capability within the drive is removed. STO is designed to prevent the drive from causing motion, allowing an operator to safely access the machinery without needing to power down the drive.

If STO mode is activated while the motor is moving, torque will be removed and the motor will coast to rest. However, the motor is free to move under external forces. For example, a vertical

load supported by the drive could fall. Therefore, a brake or other external system may be needed to assure safety.

Designers may note that the ability to prevent motion existed in the past. Safe operation was often implemented using an external contactor that removed power from the servo drive. With power removed, the drive could not cause motion. What is the driving factor to change from this method of operation?

An implementation method that removes power from a drive takes additional components which use valuable space on a control panel and require extra wiring and control. Cycling power on a drive has a small impact on the long term life of the components as they experience power-up stresses more often. If power is removed from the drive, the machine controller losses valuable information about the state of the machine. This makes recovery more difficult.

The STO option in ORMEC servo drives offers an integrated approach to safety that:

- Eliminates the additional components
- Keeps the drive alive and communicating with the controller
- Reduces power-up cycling stresses and delays
- Enhances and simplifies the implementation of a machine safety strategy
- Requires no configuration and cannot be disabled by software

With STO, the drive is still communicating and safety related signals are available to the controller. This makes it much easier to design and control the recovery from a machine fault state.

Two safety options are available. One is best suited for Category 1 and 2 requirements. The second is designed for operation with Category 3 and 4 requirements.

<u>Safety Option 1</u>:
This option provides redundant inputs and control to safely remove power from the motor. However, fault detection, reporting and feedback associated with Category 3 and above are not present, resulting in a less expensive option.

This STO option uses two redundant inputs to control the torque producing capability of the drive. This reduces the likelihood of a failure of the safety function. Both inputs must be ON (sinking current) for the drive to command torque. Either input will disable the drive. These inputs are designed to react fast and independent of the drive processor. One input will remove torque in 1-5 microseconds, the other in a few milliseconds. A status output is provided that can be used as an interlock to the primary machine controller.

Figure 1 shows the STO functional circuit. The servo drive has two independent optically isolated inputs. A 12-24 VDC voltage is required on each input to allow the torque to be enabled. When allowed, the enable is still controlled by the normal drive enable and other faults. The safety inputs prevent torque regardless of the state of the drive enable input and will not cause torque if the normal drive enable is set to disable. Two LEDs are provided as visual feedback to aid in debugging of the system. An optically coupled output is available for use as feedback to the controller.

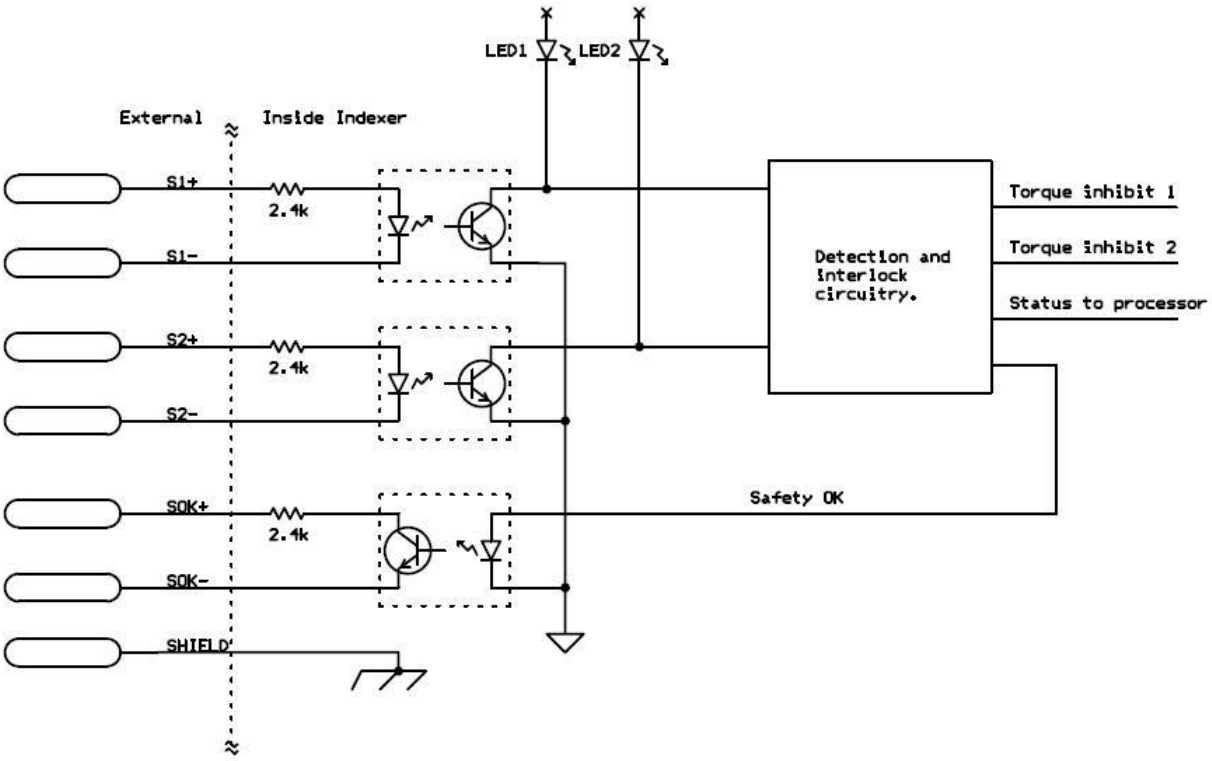

Figure 1: STO Functional Safety Circuit, up to Category 2

As shown in Figure 1, the STO circuitry provides redundant inputs and a redundant torque inhibit. There are two hardware interlocked torque inhibits outputs (Inhibit 1 and Inhibit 2). Either will prevent torque output of the drive to the motor. A status signal is provided to the processor in the servo drive which can then take further action. The processor will disable the drive and issue a fault.

By keeping the drive alive and providing the STO status to the drive processor, the machine controller has additional knowledge that was not available in the old safety model.

Safety Option 2:
This option adds the functionality required for Category 3 and 4 installations. Redundant inputs and control to safely remove power from the motor still exist.

Added are:

- Outputs for feedback of the input state
- A more fault tolerant design
- Fault detection and reporting
- A fault output to aid in system diagnostics

This STO option uses two redundant inputs to control the torque producing capability of the drive. This reduces the likelihood of a failure of the safety function. Both inputs must be ON (sinking current) for the drive to command torque. Either input will disable the drive. These inputs are designed to react fast and independent of the drive processor. One input will

remove torque in 1-5 microseconds, the other in a few milliseconds. Each input has an associated output to support monitoring by an external Safety PLC or monitoring safety relay. A no-fault output contact is provided to indicate when a safety circuit fault is detected.

In addition to performing a STO function this option contains circuitry to monitor the safety function for faults. If a fault is detected the servo drive is placed into a safe mode and the no-fault output is released. Fault detection includes a full check at power up of the drive. During operation various functions are continuously checked. For example, S0 and S1 must match within a 20ms window.

Figure 2 shows a simplified diagram of the safety circuit. Figure 3 shows a typical implementation in a machine to achieve a Category 4 rating. It is the machine designers' responsibility to verify that the combination of all components meets the safety requirements.

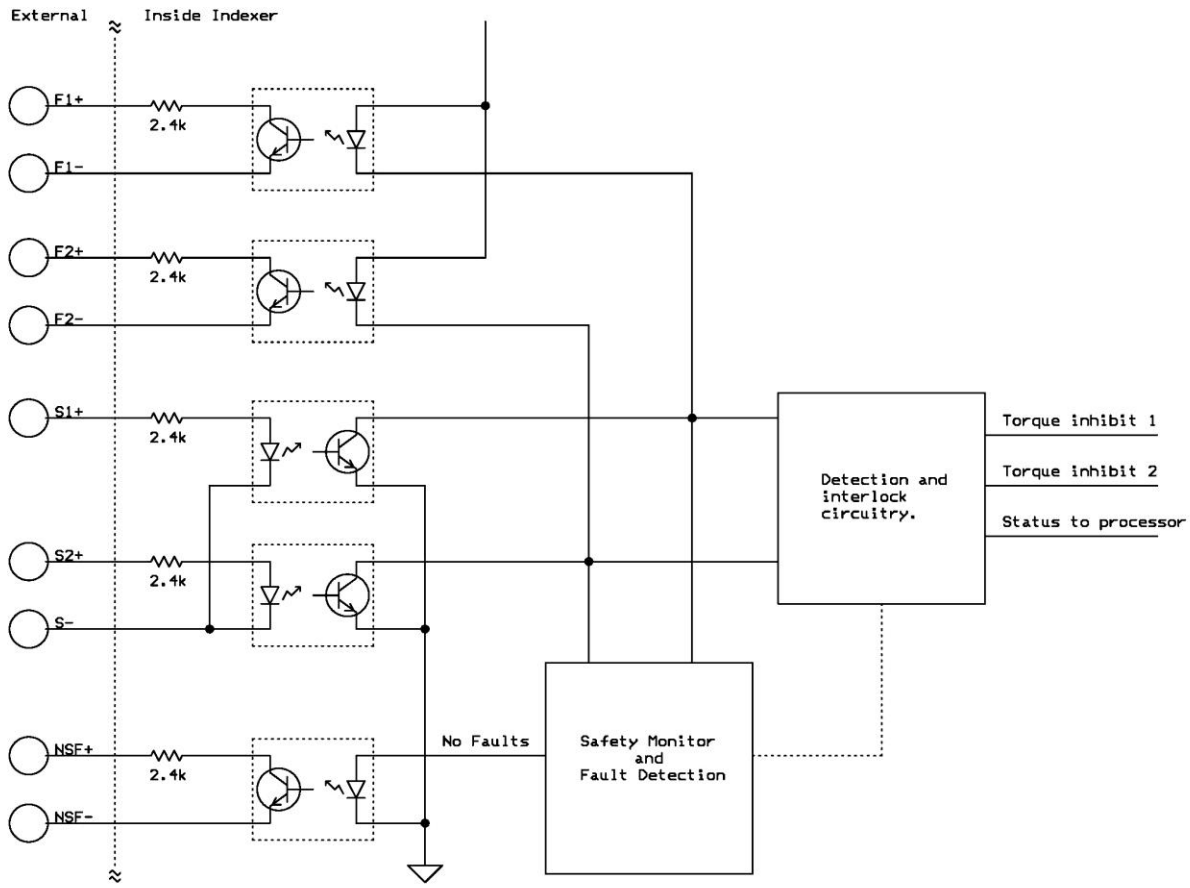

Figure 2: Simplified Safety Circuit Diagram

As shown in Figure 2, S1 and S2 provide redundant inputs. These inputs are detected and control the redundant torque inhibits. There are two hardware interlocked torque inhibits outputs (Inhibit 1 and Inhibit 2). Either will prevent torque output of the drive to the motor. The state of S1 is reflected in F1 and the state of S2 is reflected in F2. A status signal is provided to the processor in the servo drive which can then take further action. The processor will

disable the drive and issue a fault. This fault provides notification to the non-safety controller of a Safe Off Demand. This integration of safety and control aids in machine diagnostics and recovery.

Circuitry is provided to monitor for faults within the safety circuits. The NSF (No Safety Fault) outputs are provided for use in either the safety monitoring or the non-safety control. When inactive it indicates that the drive has detected a fault in the safety circuits. The drive will be prevented from applying power to the motor and the output will be inactive.

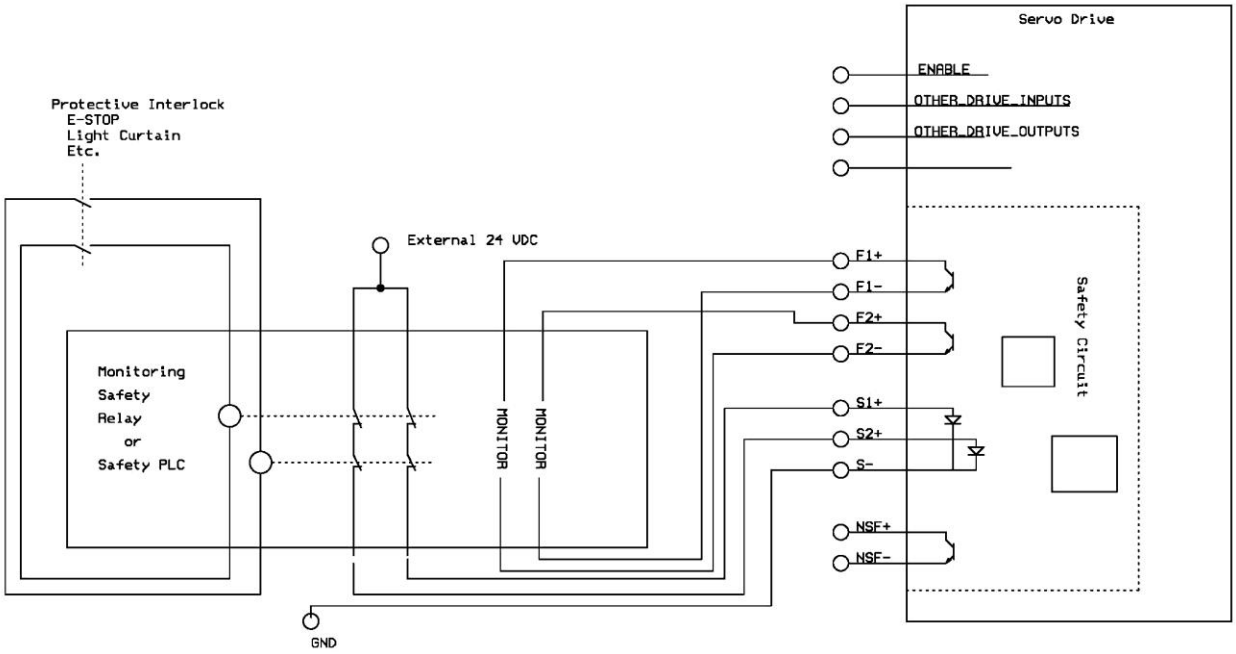

Figure 3: Typical connections for Category 4 installation

Summary

ORMEC servo drives are continually being enhanced with additional options with features and functions to help meet the emerging industry safety standards. These options provide the knowledge for control machinery that integrates both machine control design and machinery safety design.