Fault Exclusion

An important concept within the category requirements of ISO 13849-1 is the probability of the occurrence of the failure, which can be decreased using the "fault exclusion" method. This method assumes that the possibility of certain well-defined failure(s) can be reduced to a point where the resulting fault(s) can be disregarded.

Fault exclusion is a tool a designer can use during the development of the safety-related part of the control system and the risk assessment process. It allows the designer to eliminate the possibility of various failures and justify it through the risk assessment process to meet the requirements of Categories 2, 3 or 4. See ISO 13849-1/-2 for further information.

Monitoring of Safety Devices

Requirements vary widely for the level of control reliability or safety category per ISO 13849-1 (EN954-1) in safety applications. While Banner Engineering always recommends the highest level of safety in any application, it is the responsibility of the user to safely install, operate and maintain each safety system and comply with all relevant laws and regulations.

Although only two applications are listed, the Module can monitor a variety of devices as long as the input requirements are complied with (see Electrical Installation and Specifications). The Safety Module does not have 500 ms simultaneity between inputs and thus cannot be used for monitoring a two-hand control. In all cases, the safety performance (integrity) must reduce the risk from identified hazards as determined by the machine's risk assessment .

WARNING: Emergency Stop Functions
Do not mute or bypass any Emergency Stop device. ANSI B11.19, ANSI NFPA79 and IEC/EN 60204-1 require that **the Emergency Stop function remain active at all times.**

Emergency Stop Push Buttons and Rope/Cable Pull Switches

The safety inputs can be interfaced with positive-opening switches to monitor an emergency-stop (E-stop) push button or rope/cable pull. The switch must provide one or two contacts for safety which are closed when the switch is armed. Once activated, the E-stop switch must open all its safety-rated contacts, and must require a deliberate action (such as twisting, pulling, or unlocking) to return to the closed-contact, armed position. The switch must be a "positive-opening" (or direct-opening) type, as described by IEC 60947-5-1.

Standards ANSI NFPA 79, IEC/EN 60204-1, and ISO 13850 specify additional emergency stop switch device requirements, including the following:

- Emergency-stop push buttons shall be located at each operator control station and at other operating stations where emergency shutdown is required.
- Stop and emergency-stop push buttons shall be continuously operable and readily accessible from all control and operating stations where located. Do not mute or bypass E-stop buttons or rope/cable pulls.
- Actuators of emergency-stop devices shall be colored red. The background immediately around the device actuator shall be colored yellow (where possible). The actuator of a push-button-operated device shall be of the palm or mushroom-head type.
- The emergency-stop actuator shall be a self-latching type.

For Rope/Cable Pull Installations Only:

- The wire rope should be easily accessible and visible along its entire length. Markers or flags may be fixed on the rope to increase its visibility.
- Mounting points, including support points, must be rigid.
- The rope should be free of friction at all supports. Pulleys are recommended.

Some applications may have additional requirements; comply with all relevant regulations. See the device manufacturer installation instructions for complete information (such as ES-..A-5A p/n 122365, SSA-EB..-.. p/n 111880, or RP-RM83F.. p/n 141245 data sheets).

WARNING: Emergency Stop Functions
Do not mute or bypass any Emergency Stop device. ANSI B11.19, ANSI NFPA79 and IEC/EN 60204-1 require that **the Emergency Stop function remain active at all times.**

Interlocked Guards (Gates)

The safety inputs can be interfaced with positive-opening safety switches to monitor the position of an interlock guard or gate. Each switch must provide electrically isolated contacts: at minimum, one normally closed (N.C.) contact from each individually mounted switch.

The contacts must be of "positive-opening" (direct-opening) design, as described by IEC 60947- 5-1, with one or more normally closed contacts rated for safety. In addition, the switches must be mounted in a "positive mode," to move/disengage the actuator from its home position and open the normally closed contact when the guard opens.

In higher levels of safety performance, the design of a dual-channel coded magnetic switch typically uses complementary switching, in which one channel is open and one channel is closed at all times. **The inputs of the Safety Module do not support complementary switching, and thus should not be used with coded magnetic safety switches.**

The design and installation of the interlocked guard and the safety switches should comply with ANSI B11.19, ISO14119, and other applicable standards. See the device manufacturer installation instructions for complete information (such as GM-FA-10J p/n 60998, SI-LS83/-LS100 p/n 59622, or SI-HG63 p/n 129465 datasheets).

Mechanical Installation

The Safety Module must be installed inside an enclosure.
It is not designed for exposed wiring. It is the user's responsibility to house the Safety Module in an enclosure with NEMA 3 (IEC IP54) rating, or better. The Safety Module mounts directly to standard 35 mm DIN rail.

Heat Dissipation Considerations. For reliable operation, ensure that the operating specifications are not exceeded. The enclosure must provide adequate heat dissipation, so that the air closely surrounding the Module does not exceed the maximum operating temperature stated in the Specifications. Methods to reduce heat build-up include venting, forced airflow (e.g., exhaust fans), adequate enclosure exterior surface area, and spacing between modules and other sources of heat.

Electrical Installation

WARNING: Shock Hazard and Hazardous Energy
Always disconnect power from the safety system (for example, device, module, interfacing, etc.) and the machine being controlled before making any connections or replacing any component.

Electrical installation and wiring must be made by Qualified Personnel and must comply with the relevant electrical standards and wiring codes, such as the NEC (National Electrical Code), ANSI NFPA79, or IEC 60204-1, and all applicable local standards and codes.

Lockout/tagout procedures may be required. Refer to OSHA 29CFR1910.147, ANSI Z244-1, ISO 14118, or the appropriate standard for controlling hazardous energy.

It is not possible to give exact wiring instructions for a Safety Module that interfaces to a multitude of machine control configurations. The following guidelines are general in nature.

The Safety Module has no delay function. Its output relay contacts open within **25 milliseconds** after a safety input opens. This classifies the Safety Module as a functional stop "Category 0" control, as defined by ANSI NFPA 79 and IEC/EN 60204-1.

The safety inputs can be connected to:

- A +24V dc source that is switched by a hard/relay contact in single-channel hookup configuration, or
- Hard/relay contacts in a dual-channel hookup configuration using terminals S11-S12 and S21-S22.

Safety Input Device Hookup Options

The operation of all dual-channel hookup options is concurrent, meaning that input channel 1 and input channel 2 must be in the same state in both the STOP and RUN condition, but with no simultaneity (i.e. timing) requirement between the channels.

The **dual-channel hookup configuration** is able to detect certain failures and faults, such as short circuits, that could result in a loss of the safety function. Once such a failure or fault is detected, the Safety Module will turn OFF (open) its safety outputs until the problem is fixed. This circuit can meet ISO 13849-1 Category 2, 3, or 4 requirements, depending on the safety rating and the installation of the safety input device. This circuit can detect a short circuit between channels or to another source of power, at a minimum, when the device is actuated.

A single device with redundant outputs that can fail in such a manner to lose the safety function, such as a single safety interlocking switch, can typically meet only a Category 2. See below for means to eliminate or minimize the possibility of failures and faults that could result in the loss of the safety function(s).

The **single-channel hookup configuration** cannot detect short circuits to secondary sources of +24V dc or detect the loss of the switching function of the safety input device (i.e., it is not redundant) and thus this circuit typically can meet only ISO 13849-1 Category 2.