Fault Masking

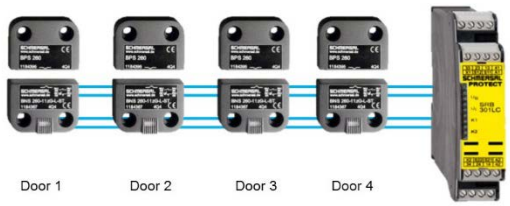
A problem that leads to a better solution for Interlocking guards.

Fault masking is the potential result from “daisy chaining” electromechanical switches. “Daisy chaining” is a widespread practice worldwide. However, when practicing it in a machine guarding safety circuit, especially in higher risk applications, it is important to recognize its limitations and potential consequences.

"Daisy chaining" is defined as a series connection of multiple switches in a circuit. It is accomplished by wiring NC contacts in series and NO contacts in parallel. Commonly used in single-channel designs, "daisy chaining" is often casually applied in higher risk safety applications without a full understanding and consideration of its limitations and their potential consequences. Daisy chaining of electrical safety interlocks is an attractive lower cost alternative for the designer, especially on higher risk machines that might otherwise require multiple safety controllers or safety I/O for programmable controllers to achieve the desired safety control category. Since there are a variety of fault conditions (I.E. A short circuit across one of the channels of a normally-closed contact in an interlock switch due to a contact weld or moisture) that may lead to a loss of the safety function, extreme care must be taken when designing the safety system with daisy-chained input switches.

Example of Fault Masking

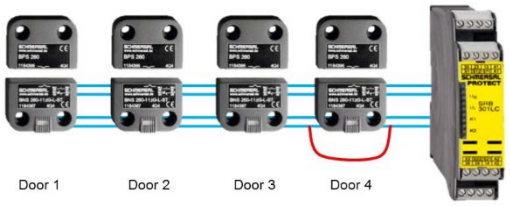
As an example, the following diagrams show a typical daisy chain solution for a multiple guard safety circuit using a single safety controller.



For this system the typical operating sequence would be:

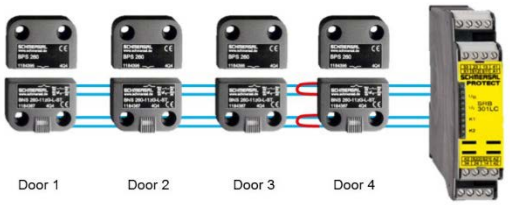
1. Guard door #1 opens - safety controller outputs open and the machine stops.
2. Guard door #2 opens - safety controller outputs remain open and the machine remains stopped.
3. Guard door #2 closes - safety controller outputs remain open and the machine remains stopped.
4. Guard door #1 closes - safety controller outputs close and the machine can restart.

The following diagram shows the same situation … but with a short across the NC contact in guard #4. In this case, some safety controllers may not detect the fault, but the safety function is not lost. This is illustrated by the following typical operating sequence that is possible under this condition:



1. Guard door #4 opens causing the safety controller outputs to open and the machine to Stop …not because of detection of the “short”, but rather because there was a change of state in only one channel.
2. Some safety controllers will go to a fault condition requiring reset.
3. Depending on the characteristics of the safety controller used, this might require cycling power to the safety controller, and closing guard door #4. The safety controller can also be reset by closing guard #4, and opening and closing another guard. This resetting can happen unintentionally, in which case the fault is undetected.
4. Once reset, the safety controller outputs will close and the machine can be restarted.
5. Opening guard door #4 again will stop the machine. Hence the safety function is still present, although the fault remains undetected.

If a second fault now occurs, for example, as shown below with a short on each channel, the safety function is lost when opening guard #4.



This occurrence of failure is called “Fault Masking”.

Relevant Standards

ISO 13849-1 clause 6.2.6 for Control Category 3 defines SRP/CS (Safety Related Parts of the Control System) shall be designed so that a single fault in any of these parts shall not lead to a loss of safety function. Important to note ISO 13849-1 also refers to Diagnostics Coverage (DC_{avg}) of the SRP/CS shall be at least “low” which translates in to minimum 60 percent according to table 6 from clause 4.5.3. This means 60 percent of the faults shall be detected.

ISO 14119, is the standard which deals with design principles and selection of interlocking devices associated with guards. In Clause 8.6, the standard talks about logical series connection of interlocking devices and fault masking, and the effect on the diagnostics coverage (DC_{avg}) value. To clarify this, the standard refers to ISO/TR24119, which is a technical report specific to fault masking and resulting diagnostic coverage.

ISO/TR 24119 goes in to more detail on evaluation of fault masking in a serial connection of guard interlocking devices with dry contacts and possible DC values. When there is series connection of guard door switches with dry contacts and if there is one or more guard door used frequently (more than once per hour) then the Diagnostics Coverage is considered to be none. Thus, the maximum achievable PL (performance level) is PL_c as per ISO13849-1 table 6.

A simplified method for determination of maximum achievable DC is located in section 6 and 6.2. Table 1 provides guidance for DC coverage and the limitation when series connections are utilized. Section 6.3 and table 2 gives guidance on the probability of Fault Masking. The probability of fault masking is dependent on several parameters that should be considered, including:

- Number of series connected devices
- Actuation frequency of each movable guard
- Distance between the movable guards
- Accessibility of the movable guards
- Number of operators

Table 1 - Maximum achievable DC (simplified)

Number of frequently used moveable guards [a) b)]	+	Number of additional movable guards [c)]	Maximum Achievable DC [d)]
0	+	2 to 4	Medium
		5 to 30	Low
		> 30	None
1	+	1	Medium
		2 to 4	Low
		≥ 5	None
>1	+	0	None

a) If the frequency is more than once per hour.

b) If the number of operators capable of opening separate guards exceeds one, then the number of frequently used movable guards shall be increased by one.

c) The number of additional movable guards may be reduced by one if one of the following conditions is met:

- when the minimum distance between guards is more than 5 meters.
- when none of the additional moveable guards is directly reachable.

d) In any case, if it is foreseeable that a fault masking will occur (multiple guards will be open at the same time as part of normal operation or service), then DC is limited to "none".

The simplified method is easier to apply and use compared to the regular method.

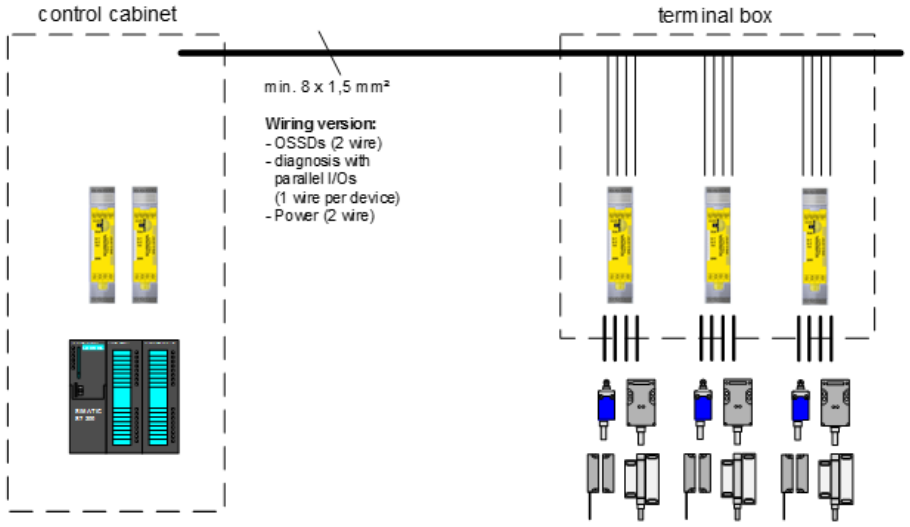
Now, this raises a question of how to overcome the issue of fault masking. Section 7 provides guidance on avoiding fault masking of interlocking devices with dry contacts, which include:

- Use of smart network technologies like AS-interface (AS-i) to be able to connect safety devices on a safety network
- Use of smart switches with self-diagnostics feature with RFID technology which can be series connected without losing the diagnostics coverage and still be able to reach the highest performance level of up to PL_e according ISO13849-1.
- Use of extra contacts to add diagnostics wired to individual monitoring device
- Use safety relays with multiple inputs so the dry contacts of the switches can be wired individually on to a safety input module or wire them individually to programmable safety controllers.

Solutions to fault masking

There are many solutions in the industry that will comply with the requirements of ISO 14119.

Using SRB-E series safety controllers (safety relay) with microprocessor provides the highest level of performance level to up to PL_e according to ISO 13849-1. SRB-E 204ST with multi-input safety relay can take up to 4 dry contact switches with providing “high” DC coverage. Also, the SRB-E series enables you to cascade several SRB-E-204PE input modules and wiring up to 4 dual channel safety switches per module. Additionally, it provides greater problem-solving possibility due to microprocessor based technology which makes for easier troubleshooting.



Electronic switches with microprocessor based technology also provide the ability to series connect with a “high” Diagnostic Coverage and able to achieve up to PL_e. Various models with locking or non-locking non contacts devices AZM, MZM, RSS, CSS are coded with RFID coding or a Schmersal developed pulse echo frequency technology. The self-monitored outputs provide two OSSD type of outputs, which monitors for shorts to voltage, ground as well as cross shorts. Any number of standard diagnostic devices can be connected in series within the maximum cable length of 200 meters (656 feet) or up to 31 serial diagnostic versions of RFID and Pulse echo devices can be wired in series - without loss of safety category or performance level.

A safety network like AS-interface is a great solution as well. SCHMERSAL Safety Solutions utilizes AS Interface Safety at Work (ASI SAW), is a safety bus system based upon the open standard of AS International. It is a simple and flexible solution to quickly, efficiently and cost effectively integrate a vast safety system. The AS Interface is an open system, allowing integrators to realize custom safety solutions with components from multiple suppliers. SCHMERSAL offers a diverse range of compatible safety devices with integrated AS Interface. Included are a variety of keyed interlocks, solenoid interlocks, safety sensors, E-Stop button, control panels, emergency cable pull switches, limit switches, and safety foot switches.

ISO14119 is a great tool to help end users and machine builders (OEMs) to understand and utilize more flexible, advanced technologies when using interlocking guards. It helps the designers with the problem of fault masking when series connecting dry contact switches by providing guidance through the ISO/TR24119 technical report. There are several other aspects in ISO14119 which were not recognized by the previous standard, EN1088, such as the locking function to be considered as a separate safety function from the interlock function, new requirements for safety sensors, and specifically addressing tamper resistance protection.

Schmersal has TÜV Rheinland certified FS Engineers who are available to assist end users, machine builders and system integrators in meeting the requirements of ISO14119 and understand this industry standard. Schmersal can help with required safety interlocks and any other safety hardware to work toward meeting the requirements for machine safety.

Author:
Kartik Vashi
Functional Safety Engineer
TÜV Rheinland ID-No. 10045/15 Machinery
Schmersal Canada

SCHMERSAL USA
15 Skyline Drive
Hawthorne, NY 10532

Tel: 914-347-4775
salesusa@schmersal.com
www.schmersalusa.com

SCHMERSAL Canada
15 Regan Road, Unit # 3
Brampton, ON L7A 1E3

Tel: 905-495-7540
salescanada@schmersal.com
www.schmersalcanada.com