

An Overview of “Daisy Chaining” Switches in Machine Guarding Safety Circuits

Copyright 2002, Schmersal Inc. Elmsford NY

Introduction

“Daisy chaining” is a widespread practice worldwide. However when using it in a machine guarding safety circuit, especially in higher risk applications, it is important to recognize its limitations and potential consequences.

This “white paper” has been prepared in the interest of creating a greater awareness of these limitations, and of the resultant potential compromises its use implies in the context of current popular risk assessment models. In addition it reviews its acceptability/compliance with our current understanding of safety system “control reliability” requirements.

Definition & Rationale:

“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 to achieve the desired safety control category. However, since there are a variety of fault conditions that might lead to a loss of the safety function, extreme care must be taken when designing the safety system with daisy-chained input switches.

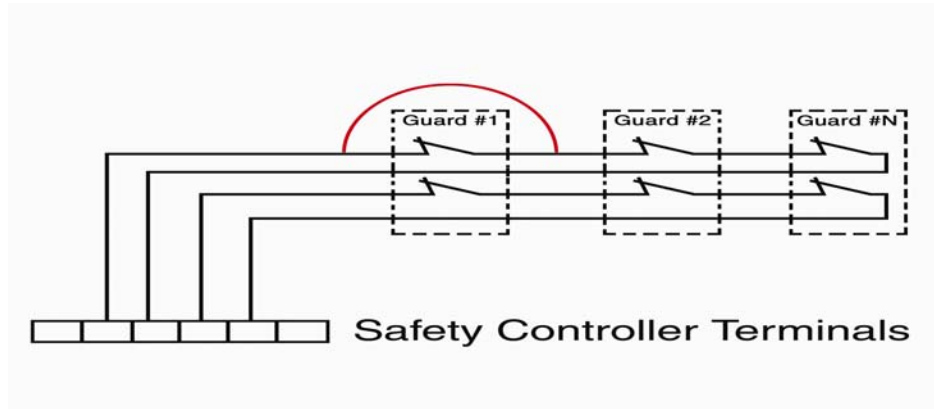
As an example, the following diagram shows a typical daisy chain solution for a multiple guard safety circuit using a single safety controller.



For this system the typical operating sequence would be:

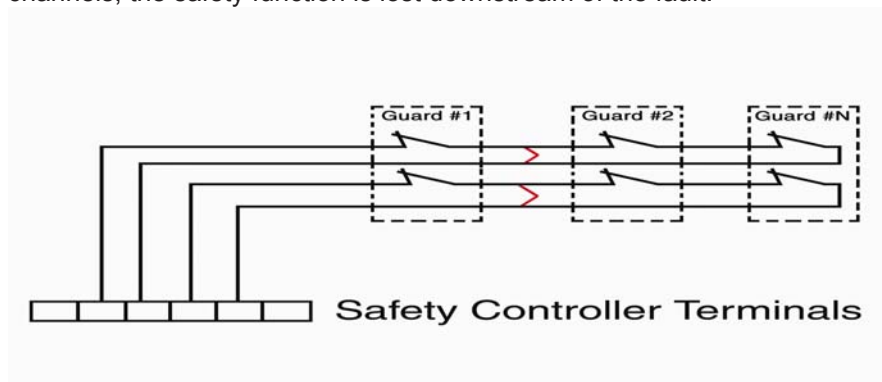
- 1) Guard #1 opens-safety controller outputs open and the machine stops.
- 2) Guard #2 opens-safety controller outputs remain open and the machine remains stopped.
- 3) Guard #2 closes-safety controller outputs remain open and the machine remains stopped.
- 4) Guard #1 closes-safety controller outputs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

The following diagram shows the same situation ... but with a short across the NC contact in guard #1. 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 #1 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. Depending on the characteristics of the safety controller used, this might require recycling power to the safety controller, or closing guard #1, then opening and closing another guard. The safety controller can also be reset by closing guard #1, then recycling power or pushing the reset button. This resetting can happen unintentionally, in which case the fault is undetected.
- (3) Once reset, the safety controller outputs will close and the machine can be restarted.
- (4) Opening guard #1 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 “shorts” on both channels, the safety function is lost downstream of the fault.



In this case, opening guard #1 results in the machine stopping. Guards #2 to #N are no longer being monitored and can be opened without detection ... thus allowing the machine continue to run. This demonstrates one of the problems that can be experienced when daisy chaining safety interlock switches.

There are, of course, faults that can occur other than those depicted in the above examples. These faults may or may not be detected depending upon the safety controller and circuit configuration. The use of safety interlock switches with 1NO & 1NC contacts may result in a safety circuit that is more reliable than one monitoring NC contacts only ... since certain "common mode" failures can be eliminated.

To better understand the implications of the above, let us examine them in the context of both current European and U.S standards/guidelines for risk assessment and related safety system requirements.

Risk Assessment Standards/Guidelines

European Standard EN954-1:

European standard EN954 presents a method of risk assessment that suggests at least one or more possibilities from the 5 different safety system characteristics depending upon the level of assessed risk. In this method the assessed level of risk is a function of:

- The frequency of exposure to the hazard.
- The severity of the potential injury from such exposure.
- The possibility of avoiding the hazard if exposed.

Each of the five safety categories is based on an assessment of each of these factors. Consequently, one can come to different conclusions regarding safety system/circuit requirements depending upon the resulting level of assessed risk.

The general safety system requirements and safety system behavior are summarized in Table I. below.

EN 954-1 Safety Categories:

Safety Category B has no special requirements for safety ... other than following good design practices and component selection consistent with the application parameters. However, it is the base of reference for the other safety categories.

For safety categories 1 and 2 we see that a single fault in the safety circuit is allowed to lead to a loss of the safety function. Since the loss of the safety function is allowed, one can infer that daisy chaining would be acceptable.

Safety Category 4 requires that there be no loss of the safety function with an accumulation of multiple faults. From this we infer that daisy chaining is not acceptable.

Safety Category 3 is less clear. For this category a single fault must not lead to loss of the safety function. However, all faults need not be detected and an accumulation of undetected faults that can lead to the loss of the safety function is permitted. From this we infer that daisy chaining may satisfy Safety Category 3 requirements - provided consideration is given to the types of faults possible in the application/safety circuit and appropriate steps are taken to minimize their possible occurrence.

**Table I.
Risk Assessment Categories per EN954**

Safety Category	General Safety System Requirements	General Safety System Behavior
B	<p>Safety system designed to meet operational requirements and withstand expected external influences.</p> <p>(This Category is usually satisfied by selecting components compatible with the application conditions ... e.g. voltage, load, temperature, etc.)</p>	<p>A single fault or component failure in the safety system can lead to the loss of the safety function.</p>
1	<p>Safety system must meet the requirements of Safety Category B, but must use "well-tried" principles and components.</p> <p>"Well-tried" principles and components include those which:</p> <ul style="list-style-type: none"> • Avoid certain faults ... e.g. short circuits. • Reduce the probability of faults ... e/g. overrating selected components, over-dimensioning for structural integrity. • Detects faults early ... e.g. ground fault protection. • Assures the mode of the fault ... e.g. ensure an open circuit when it is vital that the power be interrupted should an unsafe condition arise. • Limit the consequences of the fault. 	<p>A single fault or component failure can lead to the loss of the safety function. However, the use of "well-tried" principles and safety components results in a higher level of safety system reliability.</p>
2	<p>Safety system must meet the requirements of Safety Category B. In addition, the machine shall be prevented from starting if a fault is detected upon the application of machine power, or upon periodic checking during operation.</p> <p>(This suggests the use of a safety controller with a start-up test. Single-channel operation is permitted provided that the input devices ... such as machine guard interlocks, E-stop pushbuttons, et al ... are tested for proper operation on a regular basis.)</p>	<p>Here, too, a single fault or component failure can lead to the loss of the safety function. However, periodic checking may detect faults and permit timely maintenance of the safety system.</p>
3	<p>Safety system must meet the requirements of Safety Category B. In addition the safety system must be designed such that a single fault will not lead to the loss of the safety function. And, where practical, the single fault will be detected.</p> <p>(This requires redundancy in the safety circuit monitoring device ...safety controller... and the use of dual-channel monitoring of the input and output devices such as machine guard interlock switches, E-stop pushbuttons, safety relays, etc.)</p>	<p>Here a single fault or component failure in the safety system will not lead to the loss of the safety function and, where possible, will be detected.</p>
4	<p>Safety system must meet the requirements of Safety Category B. In addition the safety control system must be designed such that a single fault will not lead to the loss of the safety function and will be detected at or before the next demand on the safety system. If this is not possible, then the accumulation of multiple faults must not lead to the loss of the safety function.</p> <p>(This also requires redundancy in the safety circuit and the use of dual-channel monitoring of the input and output devices such as machine guard interlock switches, E-stop pushbuttons, etc. Here the application, technology used, and system structure will determine the number of allowable faults.)</p>	<p>Here a single fault or component failure in the safety system will not lead to the loss of the safety function and it will be detected in time to prevent the loss of the safety function.</p> <p>If detection of the fault is not possible, then an accumulation of faults will not lead to the loss of the safety function.</p>

“Fault Exclusion” per EN954:

European standards allow the process of “fault exclusion”. This provides a means of achieving a specific Safety Category by taking exception to the normal requirements for that Safety Category. Generally, this is accomplished by taking steps to minimize/preclude the occurrence of specific potential faults. One such example would be the exclusion of possible wiring faults (e.g. short circuits) in the interconnection wiring by running the wiring with sufficient protection (e.g. through conduit) to minimize the possibility of them occurring.

All such “fault exclusions” must be technically supported and properly documented in the machine/system technical file.

U.S. (ANSI) Guidelines for Risk Assessment

Risk Assessment per ANSI B11.TR3

ANSI’s recently published B11-TR3 Technical Report is a newly recognized guideline for conducting risk assessment and addressing the assessed risk with a suitable safety system. Unlike the frequently cited European Standard EN954, which is aimed primarily at the original equipment designer, TR3 is a “task-based” guideline.

As such, it encourages both the equipment designer and the end-user to conduct an audit of potential hazards. This recognizes that a high percentage of injuries occur during machine set-up and/or routine maintenance. Hence the end-user plays an important role in the hazard identification process.

Within this guideline the machine builder (OEM) and the end-user work together to identify the performed tasks and any associated risks. The level of risk is a function of the severity of the possible injury (the worst possible consequence of exposure to the hazard) and the probability of occurrence (as shown in the risk estimation matrix below):

Probability of Occurrence	Severity of Injury			
	Minor	Moderate	Serious	Catastrophic
Remote	Negligible	Negligible	Low	Low
Unlikely	Negligible	Low	Medium	Medium
Likely	Low	Medium	High	High
Very Likely	Medium	Medium	High	High

Shaded area shows level of assessed risk

The level of assessed risk suggests minimum standards of safety system performance to achieve the desired degree of risk reduction.

The following chart suggests the ANSI B11. TR3 guidelines for the safety system characteristics associated with each of the levels of assessed risk using this risk assessment model.

Assessed Level of Risk	Suggested Safety Control System Characteristics
Negligible	<ul style="list-style-type: none"> •Provides tactile or visual awareness of the hazard or minimal protection against inadvertent exposure (e.g. post and rope barrier, movable screen). •Safety control systems using single-channel (one safety contact configuration).
Low	<ul style="list-style-type: none"> •Barrier guard or protective device that provides simple guarding against inadvertent exposure to the hazard (e.g. fixed screen or movable guard with interlocking). •Physical devices that require adjustment for use (e.g. adjustable guard). •Dual-channel safety control system that may be manually checked to ensure the continuity of its performance.
Medium	<ul style="list-style-type: none"> •Barrier guard or protective device that prevents unintended exposure of any part of the body to the hazard and not removable or adjustable by unauthorized persons. •Physical devices that do not require adjustment or other operator intervention. •Dual-channel safety control system with self-checking upon start-up to ensure the continuity of its performance.
High	<ul style="list-style-type: none"> •Barrier guard or protective device that prevents unintended exposure of any part of the body to the hazard and secured with special fasteners or a lock. If barrier is movable, it should be equipped with a safety interlock. •Dual-channel safety control system with continuous self-checking to ensure the continuity of its performance.

It is important to understand that there are no specific (“canned”) solutions for any level of assessed risk. Rather each protective measure generally provides an incremental amount of risk reduction, with the final safety level attained a function of the combination of all the protective measures taken.

For example, during risk assessment:

- 1) A hazard, with it’s associated level of risk, is identified.
- 2) As a first step, a guard is added to protect against the hazard. However, access may be needed for routine maintenance.
- 3) The guard is designed to be movable, or alternatively, is equipped with a door/cover to permit access. The guard is then equipped with a safety interlock switch so that, when the guard is opened the machine stops (and the potential hazard is eliminated).
- 4) At this point the determination is made whether the risk of injury due to the recognized hazard has been reduced to an acceptable level.

Should this not be the case, protective measures continue to be taken until an acceptably low level of risk has been achieved.

U.S. (ANSI) Standards - Control Reliability

In addition to the TR3 risk assessment guideline, the ANSI B11 community has proposed a revised definition of control reliability and the subsequent performance requirements. Since they are not yet finalized we offer them only for your reference.

Control Reliability (current definition per ANSI B11.20)

Control reliability as originally defined by ANSI essentially states that a safety system be designed, constructed and installed such that the failure of a single component within the system does not prevent stopping action from taking place; but shall prevent a successive machine cycle from being initiated until the failure is corrected.

Since the failure must be detected, and there is no reference to risk assessment, we conclude that daisy chaining would not be permissible at any level of assessed risk. (This appears unreasonable since a hazard that poses the potential for a minor injury (e.g. a bruise) would require the same level of protection as a hazard which poses the threat of serious injury.

Control Reliability (proposed ANSI B11. definition):

Control reliability is the capability of the machine control system, the safeguarding, other control components, and related interfacing, to achieve a safe state in the event of a failure within their safety-related functions.

Control reliability is one of the design strategies that may be used to meet the performance requirements shown below. Control reliability cannot prevent a repeat cycle in the event of a major mechanical failure, or in the presence of multiple simultaneous failures, and is not provided by simple redundancy. In addition, there must be monitoring to assure that redundancy is maintained.

Performance Requirements (Proposed):

When a component, module, device or system failure occurs, such that it or a subsequent failure of another component, module, device or system would lead to the inability of the safety-related function(s) to respond to a normal stop command or an immediate stop command, the safety-related function shall:

- Prevent initiation of hazardous machine motion until the failure is corrected or until the control system is manually reset; or
- Initiate an immediate stop command and prevent re-initiation of hazardous machine motion until the failure is corrected or until the control system is manually reset; or
- Prevent re-initiation of hazardous machine motion at the next normal stop command until the failure is corrected or until the control system is manually reset.

In the presence of a failure, the user shall be responsible to ensure that repetitive manual reset of the system or device is not used for production operation.

These requirements suggest that a single fault need not be detected prior to the next machine cycle provided it does not compromise the ability of the safety system to perform when called upon to do so.

The above definition and performance requirements suggest that daisy chaining may be acceptable at all risk levels. We at Schmersal believe that the use of daisy chaining becomes questionable at high risk levels. Since the U.S. standards are still evolving, we need to await their finalization before coming to a final conclusion.

Conclusions Regarding Use Of Daisy Chaining

Regardless of the finalization of the domestic Standards/Guidelines, we believe the use of "daisy chaining" is a personal decision of the system designer. Therefore, we neither recommend nor discourage its use. However, based on current domestic and European standards, we believe the following conclusions are reasonable at this time:

For Low levels of assessed risk ... we believe daisy chaining is acceptable.

For High levels of assessed risk ... we believe daisy chaining is unacceptable.

For Intermediate levels of assessed risk ... we believe daisy chaining may be acceptable with due diligence given to the design criteria utilized in overall safety system design.

Safety Circuit Design Suggestions:

Should the system designer choose to "daisy chain", consideration should be given to (but not be limited to) the following:

Methods of interconnection wiring (important since it is the most common source of faults when daisy chaining):

- Run wires in protected channels
- Consider running wires in one switch entry and out another
- Run wires in grounded metallic conduit
- Use solid wires
- If using stranded wires, install ferrules or tin the wires to prevent shorts from loose strands

Safety controller selection:

- Choose a safety controller with a finite delay between channels. (Safety controllers with infinite delay between channels can operate as single channel monitors. Thus a short occurring in one channel only may not be detected)
- Choose a safety controller with cross short monitoring ... thus providing detection of a short between channels

Other:

- Monitor two (2) safety interlock switches per guard using a daisy chain consisting of 1 contact from the first switch as one channel and 1 contact from the second switch as a second channel.
- Use switches with 1NO/1NC contacts to reduce the risk of "common mode" failure

Compromises associated with "daisy chaining":

When using daisy chaining, be aware that:

- Some safety system faults may not be detected.
- It may be difficult to identify which guard is opened or to identify where within the safety circuit a fault has occurred.
- Production downtime may be greater while maintenance personnel locate and attempt to correct the cause of machine stoppage.

#