Automation, Inc.

www.automationinc.com
(763) 571-3336 | (800) 706-4775
4830 Azelia Ave N, Minneapolis, MN 55429

Why do I need dual channel safety?

Pete Archer - Product Specialist
June 2018

To answer this, we need some basic background information.

First why is safety needed? Here are 4 good reasons.

1. To Protect Employees
2. To Reduce insurance costs
3. To Satisfy government regulations
4. To Minimize liability and claims exposure

Second is the concept of Control Reliability.

> From ANSI B11.20-1991Paragraph 6.13, The control system shall be designed, constructed, and installed such that a single component failure within the system does *not* prevent stopping action from taking place - but will prevent successive system cycles until the failure has been corrected.
>
> - Any single fault shall be detected and shall not lead to a loss of the safety system. (Multiple faults can result in a loss of the safety system).
> - Successive machine cycles shall be prevented until the fault is corrected.
> - This strongly implies:
> - **Redundancy**
> - Cross Monitoring
> - Fault Detection

Redundancy leads to **dual channel safety**.

> The duplication of control circuits and/or components such that if one component or circuit fails, the other (redundant) unit will still be able to assure machine shut-down

Risk Assessment

> For those who do not want to go deep into Risk Assessments (will go a little deeper at the end of this discussion)
> - If an injury will heal to its original state then the risk is probably Safety Category 1
> - If an injury results in permanent damage then the risk is probably Safety Category 3
>
> **** Please note: The above 2 bullet points are not a substitute for a formal risk assessment. ****

For Safety Category 3 and above, you will need Control Reliability → Redundancy → Dual Channel

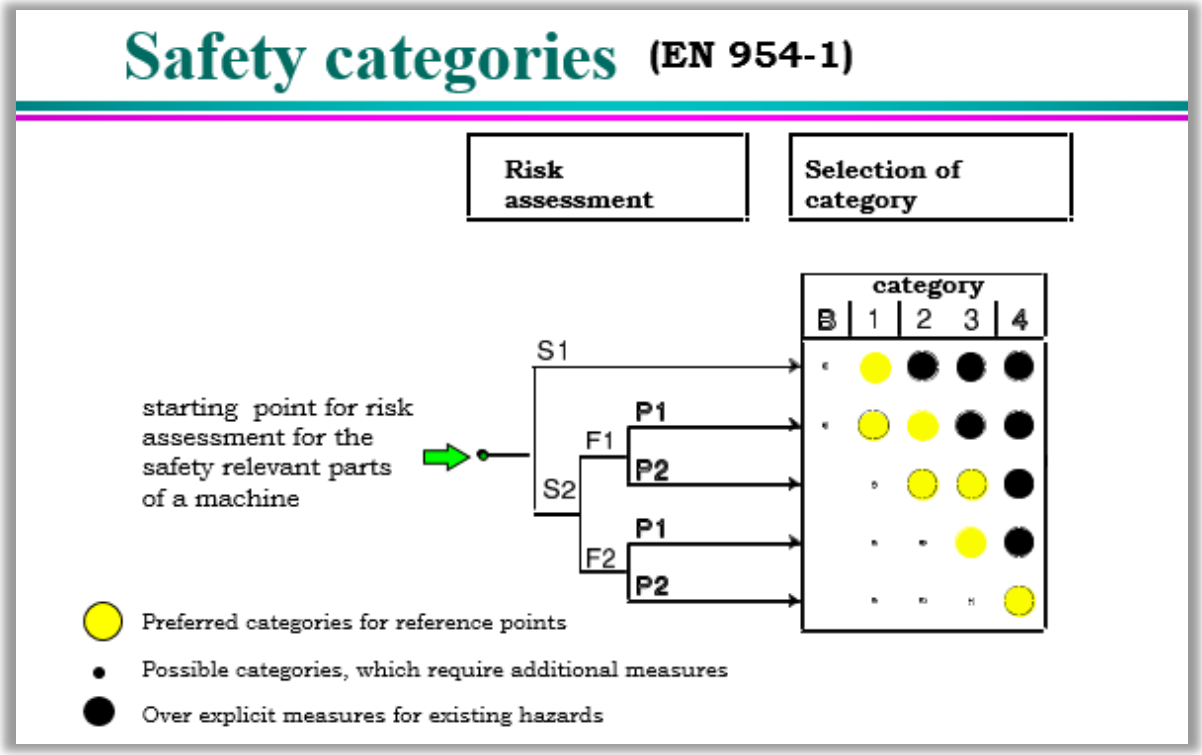
Automation, Inc.

www.automationinc.com
(763) 571-3336 | (800) 706-4775
4830 Azelia Ave N, Minneapolis, MN 55429

For those wanting to keep reading.

A little deeper discussion on Risk Assessments

Now that you have completed your formal risk assessment, this table should look familiar to you.



S: Severity of potential injury
- S1: slight injury (bruise)
- S2: severe injury (amputation or death)

F: Frequency of exposure
- F1: infrequent
- F2: frequent to continuous

P: Possibility of avoiding the hazard
- P1: Probable
- P2: Unlikely

- Category 1

  All conditions of category B apply, but the safety related system must use “well-tried” principles and components:
  - Avoid certain faults
  - Reduce probability of faults
  - Detect faults early
  - Assure the mode of a fault
  - Limit the consequences of a fault

- Category 2
  - All conditions of Category B apply. In addition, the machine shall be prevented from starting if a fault is detected upon application of machine power.
  - Single channel monitoring is permitted provided input devices are periodically checked. This check may be manual.

- Category 3
  - All conditions of Category B apply. 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, where practical, the single fault will be detected. An accumulation of undetected faults may lead to a loss of the safety function. In addition, successive machine cycles shall be prevented until the fault is corrected.
  - This requires redundancy and self-checking in the interface relay and dual channel monitoring of the input devices.

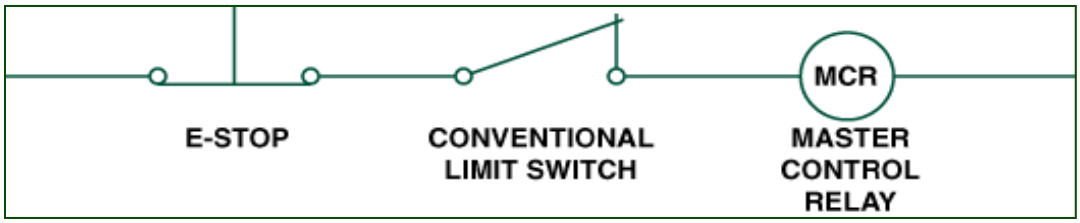
- Category 4
  - All conditions of category B apply. In addition, every single fault must be detected at or before the next demand on the safety system. If this is not possible, then the accumulation of undetected faults must not lead to the loss of the safety function.
  - The number of allowable multiple faults will be determined by the application, technology, and system structure.

Automation, Inc.

www.automationinc.com
(763) 571-3336 | (800) 706-4775
4830 Azelia Ave N, Minneapolis, MN 55429

A bit on Safety Circuits:

A simple safety circuit: Safety Category B if components selected properly

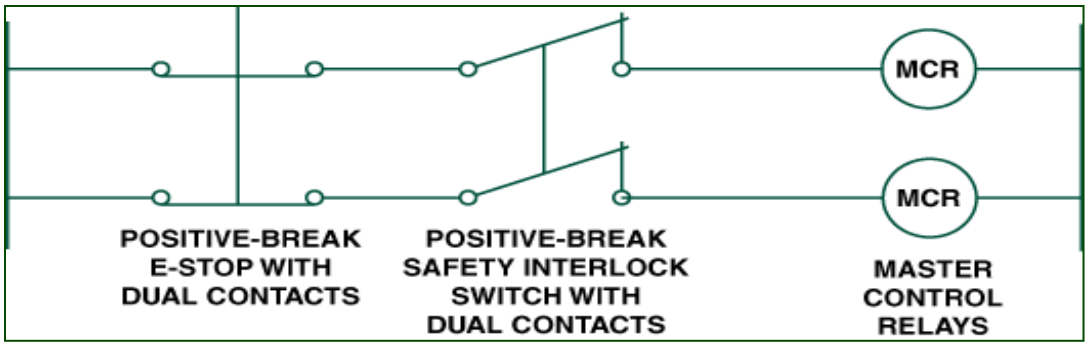


Possible failure modes:

- Switch contact weld
- Contact spring failure
- Short in wiring
- Break in wiring
- Actuator failure/Key break
- Switch manipulation
- Motor contactor/control relay weld

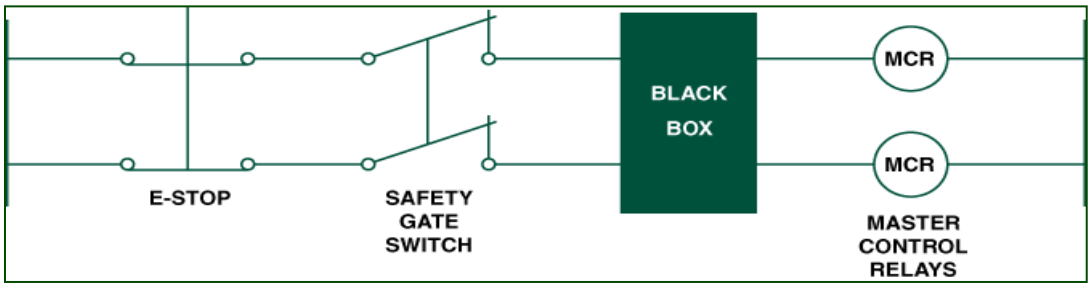
Improved Safety control system: Safety Category 1

Improve reliability by adding another positive break contact to the switches-----Redundancy



- Lacks fault detection
- Still not control reliable

Control Reliable



- Fault recognition
- Cross monitoring
- Self-Checking

Black Box (Safety Controllers—really should be discussed in a separate discussion)

- Safety system fault detection and control modules which detect (and locate) open machine guards and safety system component faults.
- Typically feature redundant, self- checking circuit design and positive-guided control relays.

**Drawings and Diagrams are complimentary of Schmersal Safety Solutions
http://www.schmersal.com/en/home/

SCHMERSAL