

III. Risk Assessment

26

What is “risk assessment”?

Various machines present different types of hazards and risks to the operator and/or maintenance personnel. Risk assessment is a systematic means of quantifying these

risk levels in order to determine the scope of the required safety system needed to protect personnel from possible injury.

27

How do I go about assessing the risk level presented by a machine or manufacturing process?

Different machines and processes have different levels of relative risk. Determining this relative risk level involves evaluating four major factors. These include:

- (1) Severity of the potential injury.
- (2) Frequency of exposure to the potential hazard.
- (3) Possibility of avoiding the hazard if it occurs.

One approach provides guidelines for risk assessment based upon five defined levels of risk. These levels range from the lowest risk (level B) in which the severity of injury is slight and/or there is relatively little likelihood of occurrence, to the highest risk (level 4) in which the likelihood of a severe injury (if the safety system fails) is relatively high.

This particular method is depicted in Figure 10, in which the following qualitative definitions apply:

- S: Severity of potential injury
 S1: slight injury (bruise)
 S2: severe injury (amputation or death)
- F: Frequency of exposure to potential hazard
 F1: infrequent exposure
 F2: frequent to continuous exposure
- P: Possibility of avoiding the hazard if it occurs (generally related to the speed/frequency of movement of hazard point and distance to hazard point)
 P1: possible
 P2: less possible

For further details of the above, the reader is referred to the EN 954-1 (Safety of Machinery: Principles for the Design of Related Control Systems).

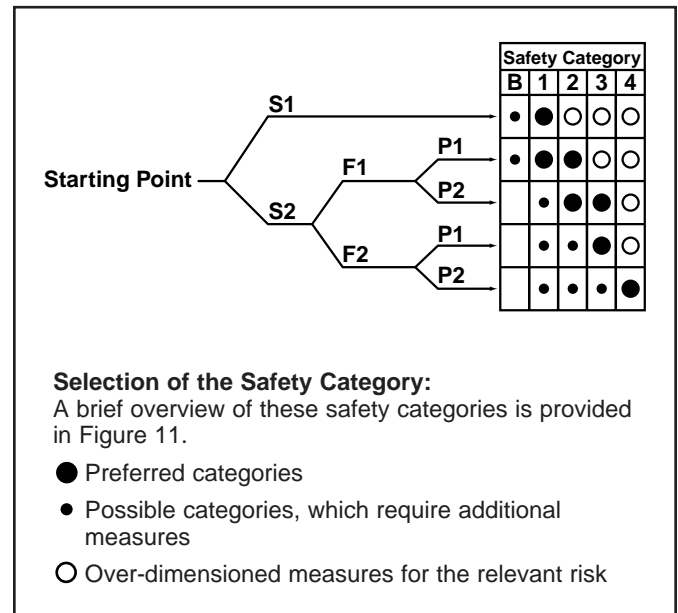


FIGURE 10

Another methodology is outlined in ANSI's Technical Report B11.TR3. This guideline suggests a “task-based” review of potential hazards by both the equipment designer and the ultimate end-user.

What are the defined levels of *relative risk* for machinery within which the *safety system* should be designed?

The European harmonized standard, EN954-1 (Safety of Machinery — Design of Safety Related Control Systems), outlines five relative levels of risk associated with the operation/maintenance of machinery. The greater the possibility and/or severity of injury, the

greater the requirements are on the design and integrity of the machine safety systems.

In general, these levels of risk are defined as follows:

Safety Cat.	General Safety System Requirements	General Safety System Behavior	Safety Cat.	General Safety System Requirements	General Safety System Behavior
B	Safety system designed to meet operational requirements and withstand expected external influences. (This category is usually satisfied by selecting components compatible with the application conditions ... e.g. temperature, voltage, load, etc.)	A single fault or failure in the safety system can lead to the loss of the safety function.	3	Safety system must meet the requirements of 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, where practical, the single fault will be detected. (This requires redundancy in the safety circuit monitoring module 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.)	Here a single fault or failure in the safety system will not lead to the loss of the safety function and, where possible, will be detected.
1	Safety system must meet the requirements of Category B, but must use "well-trying" safety principles and components. "Well-trying" principles and components include those which: <ul style="list-style-type: none"> ▪ avoid certain faults ... e.g. short circuits. ▪ reduce probability of faults ... e.g. over-rating selected components, over-dimensioning for structural integrity. ▪ detect faults early ... e.g. ground fault protection. ▪ assure the mode of the fault ... e.g. ensure an open circuit when it is vital that power be interrupted should an unsafe condition arise. ▪ limit the consequences of the fault. 	A single fault or failure in the safety system can lead to the loss of the safety function. However, the use of "well-trying" safety principles and safety components results in a higher level of safety system reliability.	4*	Safety system must meet the requirements of 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. (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, safety relays, etc. Here the number of allowable faults will be determined by the application, technology used, and system structure.)	Here a single fault or 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.
2	Safety system must meet the requirements of Category B. In addition the machine shall be prevented from starting if a fault is detected upon application of machine power, or upon periodic checking during operation. (This suggests the use of a safety relay module with redundancy and self-checking. 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.)	Here, too, a single fault or failure in the safety system can lead to the loss of the safety function between the checking intervals. However, periodic checking may detect faults and permit timely maintenance of the safety system.	<p>*Category 4 safety requirements are usually associated with extremely high-risk applications. Since general machine design practice respects classic safety hierarchy, in which most machine hazards are either:</p> <ul style="list-style-type: none"> ▪ designed out, ▪ guarded against (if they cannot be designed out), and, ▪ (as a last resort) warned against, <p>Category 4 requirements may arise relatively infrequently.</p>		

FIGURE 11

29

Which of these risk category safety system requirements is consistent with OSHA and ANSI's requirement for a "control reliable" safety circuit?

Within the above defined levels of risk, a Category 3 safety system would satisfy OSHA and ANSI's requirement for a "control reliable" safety circuit. Here use of an appropriate fail-to-safe, safety controller in combination with one or more safety interlock switches and/or coded-magnet sen-

sors will meet the single component failure detection and system shutdown criteria, while preventing a successive machine cycle from being initiated when a fault is detected.

30

How can the safety system requirements, and the requirement for machine safety system "control reliability," be satisfied?

Machine safety system control reliability can be achieved through use of:

- Safety components which feature fail-to-safe design.
- Electromechanical safety interlocks which feature positive-break N.C. contacts.
- Use of safety relays which feature positive-guided contacts.

- Use of self-checking safety controllers.
- Use of redundant monitoring/checking circuits and related safety system components.

The selection of these components will, of course, be a function of the application and its level of risk assessment. SCHMERSAL has available an *applications and safety circuit wiring handbook* to serve as a reference for selecting, designing and wiring the appropriate safety circuit for a given level of risk assessment.

31

Are safety controllers needed when addressing Category 1 or 2 safety system requirements?

Category 1 and 2 safety system requirements can be achieved without the use of safety controllers. However, this requires very careful design of the safety control circuit and a thorough understanding of the standards relat-

ed to the Machinery Directive. Use of a safety circuit controller ensures meeting Category 1 and 2 requirements without a time-consuming study of the machine control system.

How common are Category 4 safety system requirements and how can they be satisfied?

Category 4 safety system requirements are typically associated with extremely high-risk applications in which:

- (a) The severity of a potential injury is extremely high (e.g. amputation or death).
- (b) The employee/operator is exposed to the hazard highly frequently or continuously.
- (c) There is little possibility of the employee/operator avoiding the hazard.

Classic safety hierarchy states that dangers should be:

- (1) designed out;
- (2) guarded against, if they cannot be designed out; and then
- (3) (as a last resort) warned against.

Since this classic safety hierarchy reflects general machine design practice, few machines present Category 4 risk conditions.

When Category 4 safety requirements are encountered (that is, when the safety control system must be able to detect any single fault, or provide multiple fault tolerance, without loss of the safety function), it is important to remember these define the performance requirements of the overall safety system ... not of the individual components. (This, of course, is true for all safety categories ... not only Category 4.)

In this "system" context, it is clear that safety system component selection and design for equipment assessed as a Category 4 risk will be dictated by the number of faults the system can tolerate without loss of the safety function. Hence the appropriate safety system components are application-specific, requiring a thorough understanding of the operation of the machinery and its control system.

Use of a safety controller rated at Category 4 does not, in itself, assure the overall *safety system* meets this level of performance requirements.