

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-tried" safety principles and components. "Well-tried" 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 tried" 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