Chapter 4

Risk Assessment

Contents

4.0 Background to risk assessment
4.1 Performing a risk assessment
4.2 Worked example
4.3 Control integrity
4.4 EN 954-1
  4.4.1 Category B
  4.4.2 Category 1
  4.4.3 Category 2
  4.4.4 Category 3
  4.4.5 Category 4
4.0 Background to risk assessment

Machinery must be safe to use, and the best way to achieve this is through good design and proper working practices. The regulations emphasize the need to assess the machine’s risk, both in its design stage and in its application. Different types of machine have different levels of associated risk. These risk levels must be determined at the design stage, so that any improvements necessary to the mechanical and electrical design of the machine can be identified, enabling it to meet the requirements of the regulations.

In simple terms, there are only 2 real factors to consider:

- The severity of foreseeable injuries (ranging from a bruise to a fatality)
- The probability of their occurrence.

There is very little that can be done about the severity of injury, should anyone happen to come into contact with moving parts, but much can be done to reduce the probability of contact occurring. EN 292 Parts 1 and 2 (Safety of machinery. Basic concepts, general principles for design) lists the main forms of hazards arising from machinery and requires that these be protected against. It recommends two approaches, which can be used separately or in tandem.

Firstly, the designer must look carefully at the initial design of the machine to assess the potential for avoiding or reducing as many hazards as possible. This can be achieved by selecting suitable design features. Secondly, the designer must look at the possibility of limiting exposure to the hazards by reducing the need for operator intervention in the danger zones. This is mainly achieved by
introducing automatic loading and unloading, possibly with the extended use of robots.

EN 1050 (Safety of machinery. Principles for risk assessment) describes risk assessment as a process intended to help designers and safety engineers define the most appropriate measures to enable them to achieve the highest possible levels of safety, according to the state of the art and the resulting constraints. The standard also defines several techniques for conducting a risk assessment, including the following:

- What-If method
- Failure Mode and Effect Analysis (FMEA)
- Hazard and Operability Study (HAZOPS)
- Fault Tree Analysis (FTA)
- Delphi technique
- Defi method
- Preliminary Hazard Analysis (PHA)
- Method Organised for a Systematic Analysis of Risks (MOSAR)

The standard also includes information on how to formulate documentation that will be useful for compiling the technical file, as required for CE certification.
EN 292 Parts 1 and 2 details the strategy for selecting safety measures, including those that are incorporated at the design stage and measures implemented by the operator. In all circumstances it requires designers to:

**Specify the limits of the machine**

This includes determining the intended use of the machine, the performance limits, space limits, range of movements, space requirements for installation and time limits for the foreseeable life of the machine or, if necessary, of some of its component parts (wear on faces, tools or control components).

![Conveyor diagram](image1)

Conveyor - The first idle roller is free to prevent drawing in

![Removal of shear trap diagram](image2)

Removal of shear trap by design

---

Fig. 5: Examples from BS 5304, demonstrating how safety can be included at the design stage
Identify the hazards and assess the risks
This should be considered over all phases of the machine’s life: in manufacture, transportation, assembly, installation, commissioning, normal use, foreseeable misuse, maintenance, dismantling and disposal. Again, the degree of injury and probability of occurrence must be assessed at this point.

Remove the hazards or limit the risk as far as possible
This can be achieved by taking out traps (see Fig. 5 below), reducing speed and force, employing good ergonomics and applying failsafe principles.

Design in safeguards against remaining risks
Where hazards cannot be designed out, safeguards must be designed in. These can include interlocked guards, light curtains, pressure mats, two-hand controls, trip devices etc.

Inform and warn the user about any residual risks
This can take the form of signs and symbols (both visual and audible) for all personnel including operators, installers and maintenance engineers etc.

Consider any other precautions
At this stage designers must determine whether additional requirements will be necessary for personnel, taking into account emergency situations.

It is important to emphasize that designers are required to consider the hazards, risks and required safety measures over all the phases of a machine’s life. Hazards must be identified and the associated risks assessed at each of the stages named above.

This systematic method for identifying and eliminating risks is shown in the flowchart in Fig. 6 overleaf.
Fig. 6: Flowchart for systematic identification and reduction of risks
Please note:
BS 5304 1988 is not a harmonised European standard. However, most interested observers consider it an important document for use in the design of safe machinery. As yet it has not been superseded or replaced by any other standard, but many of the ideas and concepts it contains are being applied in some of the B2 standards, including:

- **EN 1088 (Safety of machinery. Interlocking devices associated with guards. Principles for design and selection)**
- **EN 953 (Safety of machinery. Guards. General requirements for the design and construction of fixed and movable guards).**

Many of the C standards will also draw upon this standard for advice and information. When deciding whether the safety level of a machine is adequate, designers must be certain that the intended level of safety has been achieved and that safety measures neither prevent the machine performing its intended function, nor generate additional hazards.

The Management of Health and Safety at Work Regulations (MHSWR) were introduced in 1992 and require employers to carry out a “suitable and sufficient assessment” of the risks their employees are exposed to while at work. Employers are also required to record the findings of their assessment and, where the risks are considered unacceptable, to introduce control measures to reduce the risks. At this stage it would be beneficial to outline some definitions on the subject of risk assessment, as stated in the harmonised standards (in particular EN 1050):
**Risk assessment**
This is defined as a series of logical steps to enable the hazards associated with work equipment to be reduced and eliminated in a systematic way. Risk assessment is an essential part of the interactive process of risk reduction.

**Hazard**
This is defined as something with the potential to cause harm.

**Risk**
The likelihood that harm from the particular hazard could be realised. Essentially, risk is a combination of the nature of the hazard and the probability of occurrence.

**Exposed person**
Anyone who could be affected by the hazard.

**Control measures**
Measures taken to eliminate the hazard or to minimise the likelihood of occurrence to acceptable levels (these levels are well defined in law).
4.1 Performing a risk assessment

Many people are frightened by the words “risk assessment”, believing they do not understand what it entails. However, everyone carries out risk assessment as part of everyday life. Crossing the road requires a risk assessment based on simple hazard analysis, the hazard being the traffic and the risk the likelihood of reaching the other side without being run over. Three different control measures could be suitable, depending on the amount of traffic:

- **Light traffic on a little-used road**
  Control measure: cross using judgement and experience

- **Heavy traffic on the high street**
  Control measure: cross using the pedestrian crossing

- **Continuous fast traffic on the M1**
  Control measure: cross using the footbridge.

EN 1050 outlines several risk assessment methods and techniques. Some are based on mathematical models and require access to failure rates and reliability data. It is important to remember that quantitative methods can only be as reliable as the data used in the calculations, and failure data is generally scarce for risk assessments involving work equipment.

The risk assessment method used in this guide is not intended as a substitute for these scientifically proven systems. However, used with practice and an open mind, it will enable most engineers, supervisors and managers to produce sufficient risk assessment data to guide the user towards compliance with the regulations. Essentially it is an attempt to quantify what is very much a qualitative technique, similar to the one described in the HSE booklet “Five Steps to Risk
Assessment”. It is important to note that this assessment is based on making appropriate choices from a list of possibilities, and as such the user is expected to exercise sound judgement.

This method takes into account four criteria, seeking to quantify a level of risk and qualify it as:

- **Negligible**
  Presenting very little risk to health and safety

- **Low but significant**
  Containing hazards that require control measures

- **High**
  Having potentially dangerous hazards, which require control measures to be implemented urgently

- **Unacceptable**
  Continued operation in this state is unacceptable.

The criteria used to arrive at these levels are identified below. A numeric value is assigned to each option. The sum of the value of the chosen options will identify a risk level as:

<table>
<thead>
<tr>
<th>Risk Level</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Negligible</td>
<td>0-5</td>
</tr>
<tr>
<td>Low but significant</td>
<td>5-50</td>
</tr>
<tr>
<td>High</td>
<td>50-500</td>
</tr>
<tr>
<td>Unacceptable</td>
<td>500+</td>
</tr>
</tbody>
</table>
Likelihood of occurrence (LO) / contact with hazard

Almost impossible - possible only under extreme circumstances 0.033
Highly unlikely - though conceivable 1
Unlikely - but could occur 1.5
Possible - but unusual 2
Even chance - could happen 5
Probable - not surprising 8
 Likely - only to be expected 10
Certain - no doubt 15

Frequency of exposure to the hazard (FE)

Annually 0.5
Monthly 1
Weekly 1.5
Daily 2.5
Hourly 4
Constantly 5

Degree of possible harm (DPH), taking into account the worst possible case

Scratch/bruise 0.1
Laceration/mild ill-effect 0.5
Break minor bone or minor illness (temporary) 2
Break major bone or major illness (temporary) 4
Loss of one limb, eye, hearing loss (permanent) 6
Loss of two limbs, eyes (permanent) 10
Fatality 15
Number of persons exposed to the hazard (NP)

1-2 persons 1
3-7 persons 2
8-15 persons 4
16-50 persons 8
50+ persons 12

The calculation is as follows:

$$LO \times FE \times DPH \times NP = \text{Risk level}$$

Any risk not considered trivial will need to be identified and assessed. If required, control measures must be introduced. Clearly this method relies on the judgement of the assessor, who not only must decide what constitutes a non-trivial risk, but must also select the most appropriate option from the lists. This being the case, the publishers of this guide can take no responsibility for the validity of the assessment made. However, the following points may prove useful:

- Always take into account the skill, awareness and boredom factors of the exposed person. People working on repetitive jobs may not notice that equipment is deteriorating or starting to fail.
- Never conduct a risk assessment without the co-operation of operators and supervisors. They will probably be more aware of the hazards than the assessor.
- If a hazard needs to be measured in order to decide its level (e.g. noise), make sure the correct equipment is used.
- Hazards from machinery are mainly mechanical. These include (but are not limited to) crushing, shearing, entanglement, stabbing, friction, loss of stability and the feed/ejection of parts.
All these must be considered. The best approach is to check all the hazards identified in the regulations.

Non-mechanical hazards will also need to be assessed if relevant. These include (but are not limited to) high or low temperature, noise, electric shock, effect of chemical contact or inhalation, fire, explosion and the effects of laser light. Again, it is important to read the requirements of the regulations.

Details of risk assessments must be documented to include findings as well as recommendations.

Any recommendations that involve upgrading control measures must be implemented with the minimum possible delay.

Risk assessments are always on-going. If the work equipment or the work itself changes, the risks must be re-assessed.

If the assessment shows that training is a significant measure, this must be structured accordingly and continuously assessed.

If setting, cleaning and maintaining equipment presents risks other than those faced by the operators, these must be addressed separately and, if necessary, specific control measures must be put in place.
4.2 Worked example

Equipment: Production machine
Main hazard: Trapping between the tool post and the chuck as parts are loaded.

The assessment will be performed in two stages. The first step is to ignore whatever safety measures are already in place in order to arrive at a “conceptual” control measure, where hazards are assessed in their “raw” state. The second step is to compare this conceptual measure with the existing control measures. If these are as good as or better than the concept, no further action will be required. However, if the existing measures are shown to be inadequate, work must be done to bring it up to standard.

Initial assessment, without control measures:

- **Likelihood of occurrence: Possible**
  This was selected because the event would be unusual and would probably only occur if the operator was distracted during the loading operation.

- **Frequency of exposure: Constant**
  The machine cycle time is less than two minutes.

- **Degree of possible harm: Loss of one limb**
  The machine feed is hydraulic and the pressure could crush the whole forearm.

- **Number of persons at risk: 1-2**
  Only the operator is at risk from this hazard.

This gives the following calculation:

\[ (LO = 2 \times FE = 5 \times DPH = 6 \times NP = 1) = 60 = \text{HIGH} \]
Clearly, the score from this hazard indicates a high risk, so control measures will need to be applied in order to reduce this risk to an acceptable level. This can be regarded in two ways. If at all possible, the first step should be to reduce or remove the hazard. However, on most machines the hazard will either be fixed by design or cannot be removed or reduced. In this case, the only available action will be to protect against it.

To protect the operator from this hazard, a suitable guard must be fitted to prevent access while the machine is in motion and to prevent the machine moving while the operator is loading parts. The next thing to consider is the type of guard. A fixed, bolted guard would clearly be unacceptable because access is required on a regular basis and, because of the time it takes to remove it, the operator may be tempted to take it away altogether. The choice would therefore seem to lie between an electrosensitive or non-contact system (light curtain or pressure mat) and an interlocked fast-access mechanical guard.

Once the type of guard has been selected, the hazard needs to be reassessed with the control measure in place. To do this we need to return to the four factors listed above. In this case, there is little that can be done about the number of people at risk or the frequency of exposure, unless of course the selected control measure includes an automatic loading system. The degree of harm is also difficult to change. The only factor that is affected by the addition of an interlocked guard is the likelihood of occurrence.
Reassessment:

- Likelihood of occurrence: Almost impossible
  The machine cannot move if the guard is open.
- Frequency of exposure: Constant
- Degree of possible harm: Loss of one limb
- Number of persons at risk: 1-2

The new score from this hazard suggests that this solution reduces the risk to acceptable levels:

\[(LO = 0.033 \times FE = 5 \times DPH = 6 \times NP = 1) = 0.99 = NEGLIGIBLE\]

If control measures are in place, the mechanical aspects will need to be compared with the conceptual requirements and the recommendations of the guarding standards. If they match, no action is necessary. If no guards are present, or the quality of the guards is not as required, remedial action will be necessary. If physical means are not sufficient to bring the risk to an acceptable level, warning notices and special training may be the only way forward. These are regarded as acceptable control measures, but should be the final items considered in the hierarchy of preventive measures.
4.3 Control integrity

The risk assessments we have looked at so far have dealt with mechanical control measures, which are often required to interact with the machine’s control system, either by preventing all dangerous machine movement or by stopping a specific operation. The following key factors should be considered when assessing the integrity of the control system:

- **Part identification**
  Determine how the safety-related part that will be interlocked contributes to the operation of the machine.

- **Demand rate**
  Determine the demand placed on that particular part during the machine’s operation and establish whether its failure would lead to a hazardous situation.

- **Technology used**
  Establish what technology is to be used on the protective system.

- **Probability of a fault occurring**
  Establish the probability of a fault occurring in the safety-related part and whether this would lead to a hazardous situation.

- **Fault detection**
  Consideration must be given to how faults will be detected and, should faults accumulate, to the number of faults that will be tolerated before a hazardous situation arises.

These simple considerations show that the integrity of a safety-related control may vary.
4.4 EN 954-1

The harmonised standard EN 954-1 is concerned with the safety-related parts of a control system and looks at their ability to resist faults, something that will obviously affect how far risks can be reduced. Section 6 of this standard lists 5 categories (category B, 1, 2, 3 and 4) to act as guidance for safety-related controls.

It is important to note that these categories are not risk levels, nor are they intended to be used in any given hierarchy.

4.4.1 Category B

In this category, a single fault can lead to the loss of the safety function. The component parts of the control system must be able to withstand the expected operating stresses and any influences from materials that are processed; reliability in use should also be taken into account, as should any other external influences. The use of standards and test data is a good check for conformity. As a single fault can lead to the loss of the safety function, measures in addition to those provided by the safety-related controls may need to be installed in order to meet the requirements of Annex A in EN 292-1.

4.4.2 Category 1

All the requirements of category B apply, in addition to the use of well-tried components and safety principles. Increased reliability aims to eliminate the likelihood of a fault occurring. For example, life testing and positive mode operation help to avoid certain types of faults, while failure mode definition helps to detect potential faults before they occur.

The likelihood of failure is less than category B, but a single fault can still lead to the loss of the safety function. This means that measures
in addition to those provided by the safety-related controls may need to be installed in order to meet the requirements of Annex A in EN 292-1. For categories B and 1, it is fair to say that the safety of the system relies on the components.

4.4.3 Category 2
All the requirements of category B apply, in addition to the use of well-tried components, safety principles and a safety function check. This check should be performed as the machine starts up and, if required, periodically during operation. The safety function check may be automatic or manual and will allow the system to operate if no fault is detected. If a fault is found, the safety function check will generate a fault output, which will initiate a safe state whenever possible. This check may be performed by the machine control system or by a dedicated monitoring device. If a fault occurs, the safety function may be lost between checks, but the fault will be detected by the next check.

It is fair to say that a manual check is the only effective way to detect faults. The frequency of this particular check will depend on the initial risk assessment of the component during the machine’s operation.

4.4.4 Category 3
All the requirements of category B apply, in addition to the use of well-tried components and safety principles. A further requirement of category 3 is that a single fault shall not cause the loss of the safety function. Whenever practicable, a safety-critical single fault shall be detected at or before the next demand upon the safety function. However, this does not mean that all faults will be detected, so an accumulation of faults could still cause the loss of the safety function. A practical way to avoid this is to use redundant devices.
4.4.5 Category 4
All the requirements of category B apply, in addition to the use of well-tried components and safety principles. A further requirement of category 4 is that a single fault in any of the safety-related parts of the system shall not cause the loss of the safety function. The single fault must be detected at or before the next demand upon the safety system. If this is impossible, an accumulation of faults shall not lead to the loss of the safety function. An accumulation is normally regarded as two faults, but this depends largely on the complexity and technology of the system. Common faults must be eliminated by using diversity and by implementing special procedures that will identify them. It must not be possible for the safety function to be lost if a fault is detected.

It is clear, therefore, that categories B and 1 have a lower integrity than categories 2, 3 and 4. However, it is important to remember that the requirements of B and 1 are included in each category and have also to be applied to the peripheral parts of the safety-related control system, such as switches and housings. This means that a complete safety-related control system may combine a number of categories. The chart in Fig. 7 is taken from Annex B of EN 954-1 and is an informative guide to the selection of safety-related controls. This chart should be used in conjunction with the recommendations for risk assessment given in EN 1050.

For further reference please read:
CR 954-100, Guide on the use and application of EN954-1, published by CEN.
**Preferred categories for reference points**
- Possible categories which can require additional measures
- Measures which can be overdimensioned for the relevant risk

\[\begin{array}{c}
\text{Categories} \\
\hline
\text{B} & 1 & 2 & 3 & 4 \\
\hline
\bullet & \bullet & \bigcirc & \bigcirc & \bigcirc \\
\bullet & \bullet & \bullet & \bigcirc & \bigcirc \\
\bullet & \bullet & \bullet & \bullet & \bigcirc \\
\bullet & \bullet & \bullet & \bullet & \bullet \\
\end{array}\]

\[\begin{array}{c}
\text{Categories} \\
\hline
\text{S} = \text{Severity of injury} \\
\text{S1 Slight injury (normally reversible) i.e. slight cut or bruise.} \\
\text{S2 Serious (normally irreversible) injury including death.} \\
\hline
\text{F} = \text{Frequency and/or exposure time to the hazard} \\
\text{F1 Seldom to quite often and/or the exposure time is short.} \\
\text{F2 Frequent to continuous and/or the exposure time is long.} \\
\hline
\text{P} = \text{Possibility of avoiding the hazard} \\
\text{P1 Possible under specific conditions.} \\
\text{P2 Scarcely possible.} \\
\end{array}\]

Fig. 7: Extract from EN 954-1: risk assessment chart