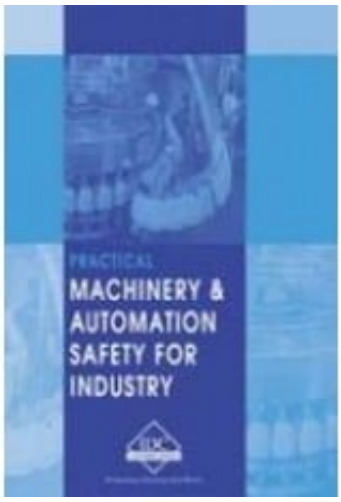
IDC Technologies - Books - 1031 Wellington Street West Perth WA 6005

Phone: +61 8 9321 1702 - Email: books@idc-online.com,publishing@eit.edu.au

SF-E - Machinery and Automation Safety for Industry



Availability: In Stock

Price: $139.94

Ex Tax: $127.22

Short Description

Safety regulations are now well established in industry but in many cases companies are taking inadequate measures laying themselves and their staff open to prosecution. And on the other hand many companies are taking safety measures to protect their staff; but are wasting a considerable amount of money in achieving ineffective partial compliance with the relevant standards and regulations.

Description

Safety regulations are now well established in industry but in many cases companies are taking inadequate measures laying themselves and their staff open to prosecution. And on the other hand many companies are taking safety measures to protect their staff; but are wasting a considerable amount of money in achieving ineffective partial compliance with the relevant standards and regulations.

This manual aims is to provide you with the tools to comply with the Safety legislation and ensure that your staff are. This manual familiarizes you with a wide variety of machinery hazards and shows you methods of making your equipment safe and complying with the applicable local safety Laws. Topics range from safeguarding of machinery, the Occupational Health and Safety Act, Safety Control Systems to Safe Fieldbus technology. This manual focuses on

giving you the tools to apply the principles of Machinery Safety to real equipment and systems. Practical case studies are a key part to ensure that you get a real world practical exposure to the topic.

Table of Contents
Download Chapter List

Table of Contents

First Chapter
Chapter 1: Introduction to Machinery Safety

1

Introduction to Machinery Safety

The safety of machinery affects all of us in everyday life, at home or at work or at leisure. Machines are part of our lives and our safety is dependent on the machines being safe for us to use at all times. So, how should a machine be made safe? There are some very basic aspects of safety that spring to mind. A machine should be:

Physically Safe: No sharp edges, spikes or projections we can bump into. No chance of it falling over on to somebody. No ways in which it can throw objects around or let out jets of steam or noxious gases No chance of explosions or radiation.

Mechanically safe: The moving parts must not be able to hurt someone. If there's a risk that this can happen then we need protection measures; fixed guards, movable guards, area sensing devices that stop the machine quickly if someone is in the danger zone.

Electrically safe: There must be no chance of an electrical shock or a dangerous electrical circuit arrangement.

Functionally safe: All the stops switches, guards and safety sensing devices that may be there to protect us must function properly. All safety controls that prevent movement at the wrong time must be reliable.

This workshop concentrates mainly on Functional Safety Systems; those safety measures that are based on sensors and control systems that are design to ensure safe working of the machines. These are also known as Safety-Related Electrical Control Systems (sometimes abbreviated as SRECS). The workshop training is intended for technicians and development engineers who will be concerned with designing and maintaining safety related control systems for automated machinery.

We shall also be looking at the general requirements for safety of machines including some aspects of mechanical guarding and electrical equipment safety.

As with all safety system applications, the technical requirements must be supported by a basic understanding of risk management principles. These principles provide guidance on the extent and complexity of essential safety measures for each application. Once a safety system has been devised its success depends on both the technical quality of the design and on the effective management of all aspects of the safety system throughout its lifecycle. This works shop therefore combines basic training in the principles of safety management with specialised chapters on the safety devices and techniques commonly seen in industry.

We shall to see that there is a common approach to most safety applications involving electrical/electronic control systems. If we can identify the ground rules and the common features that apply to most safety applications in machinery we shall have a basis or framework for tackling any particular project.

This is the basis of our workshop:

- Identify the common factors in most machinery safety applications.
- Outline the framework of regulations and standards that support good safety practices
- Develop a basic knowledge of design principles and design practices
- Develop a procedure for defining safety requirements and for selecting appropriate safety devices
- Learn about the most widely used safety techniques and see how they are used in practice.
- Introduce the current and newly developing technologies for safety systems

At the end of the workshop we hope that you will have sufficient knowledge to approach any machinery safety project or maintenance situation with confidence. You should feel that you have the background training to recognise the basic

features of safety systems, and to know the principles on which they should be built.

1.1 Scope and objectives of this chapter

This chapter provides an introduction to some key topics in machinery safety.

The topics include:

- The definition of a machine and it’s safety related controls
- Regulations and standards.
- Hazards and risk assessment
- Concepts of risk reduction and tolerable risk
- An introduction to the safety lifecycle and its relevance to safety management
- A simple example of a machine safety system and its development steps
- Safety equipment, sensors, logic solvers and actuators.
- Standards for programmable systems.
- Application of safety PLCs and Bus networks

The topics will be studied in more detail in succeeding chapters but the objective here is to achieve the broadest possible view of the subject before diving into particular details.

1.2 Machinery and Controls

What do we mean by machinery?

As you might expect almost any assembly of mechanical and electrical equipment that has moving parts can be considered a machine. Various definitions of machines:

This definition of machinery is taken from the European standard EN 292-1*: Safety of machinery –Basic concepts, general principles for design.*

“Machinery (machine)”

An assembly of linked parts or components, at least one of which moves, with the

appropriate machine actuators, control and power circuits, etc., joined together for a specific application, in particular for the processing, treatment, moving or packaging of a material.

The term machinery also covers an assembly of machines, which, in order to achieve a common function or deliver a product, are arranged and controlled so that they function as an integral whole."

The electrical safety standard IEC 60204-1 adds the following detail. (In paragraph 3.33)

"Machinery also means interchangeable equipment modifying the function of a machine, which is placed on the market (supplied) for the purpose of being assembled with a machine or a series of different machines, or with a tractor by the operator himself insofar as this equipment is not a spare part or a tool."

It can be seen that this definition will embrace a vast range of equipment. Typically we are interested in familiar types of machinery and there are some obvious groupings.

- Domestic appliances
- Lifts and escalators, cranes and hoists, fork-lift trucks
- Basic cutting, sawing and drilling tools
- Machine tools such as lathes, milling machines, metal working drills, circular saws.
- Press tools ranging from small ones for components to large presses for motor vehicle body parts.
- Multi-station machining centres
- Assembly lines and conveyor systems where multiple machines are co-ordinated to provide a complete manufacturing process.
- Robots and robot operated assembly or packing units.
- Agricultural machines such as combine harvesters and baling machines

In all the above machines it is the responsibility of the builder and supplier to ensure that the machine is designed to be safe to use in its intended manner. This very often requires that the machine be fitted with essential safety measures to minimize the risk of injury to people near to the machines, particularly those operating and maintaining the machines.

What is a machinery safety system?

Any assembly of devices designed to protect people from hazards or injuries that

could arise from the use of the machine can be considered to be a **machinery safety system**. The machinery safety system may also provide protection for the machine itself or other machines against damage due to malfunctioning of the machine. Lets look at a simple diagram of a machine with its basic control system and then see where the safety system fits in.

Figure1.1: *Block diagram model of a typical machine.*

The diagram here depicts a machine with a basic control system. It may for example have drives creating movements of assemblies and cutting tools, if it is an injection moulding machine it may have hydraulic pumps with hydraulic valves controlling linear actuators. The actions of the machine will have physical parameters that can be measured with sensors and evaluated by the control system. The control system will operate drives and actuators to follow a programme of actions that will be decided by the operator and/or the stored programme within the machine.

In automation systems it may be that the machine controls will exchange data with a larger control network, enabling this machine to be operated in co-ordination with several other machines. Hence we must recognise that there are several sources of commands for the machine to respond with controlled actions. Sources of commands are:

- The operator via a control interface
- The machine control logic from a fixed logic control or from a stored program
- The automation cell control system

To these we must add “false commands” from malfunctions:

- The machine goes wrong, mechanically or electrically.
- The operator does something wrong.
- The control system goes wrong or is incorrectly programmed.

Any of these commands could cause the machine to start moving and hence there is a possible hazard if a person or another machine is the wrong place at the time.

Fixed guards are usually the first line of defence to prevent a person being hurt by the machine but in many cases the situation will require a logical action from the control system to prevent movement or other physical events from happening until safe conditions are proved to exist. These protective measures are the “safety functions” to be provided by the control system. Those parts of the basic control system as well as any specially provided safety parts are known as the **“safety related parts of the control system”.** In the next diagram they are shown to consist of safety critical parts of the basic controls (for example Emergency Stop controls) as well as separate sensors for devices such as presence sensing light curtains or safety mats.

Figure 1.2:*Block diagram of machine showing safety related parts*

It is important to bear in mind that the safety related controls include all parts involved in the safety function. Hence the sensors, logic or evaluation units and the final drive interlocks and contactors or valves belong to the safety control system.

Whilst some safety devices can simply be passive guards such as shields or covers, it is most likely that many of the safety functions will be provided by a combination of mechanical devices and a *safety related electrical control system*. (Sometimes abbreviated as SRECS).

The elements of a safety-related electrical control system are shown below and it is worth noting that these are very similar to those required for a process safety instrumented system.

Figure 1.3*:Basic elements of a safety related control system*

Figure 1.3 depicts the essential elements of all safety related control systems. These comprise:

- The safety control equipment comprising sensors, logic solvers and actuators

- An interface to the basic control system that must not allow the basic controls or operator settings to interfere with or corrupt the safety function
- An interface to the users; these will be operators, machine setters, technicians, engineers. This interface must also be secure against corruption of the safety function.
- Functional separation: We want to keep the safety systems functionally independent from the basic controls to protect them against being accidentally or deliberately defeated by action of the basic controls.
- Avoidance of common cause failures. We want to avoid the possibility that a malfunction or electrical defect in the basic machinery controls can at the same time override or corrupt the safety controls. For example if one PLC output stage controlled the starter for a drive and also controlled a safety interlock it would be useless as a safety device if the PLC failed with all outputs on.

The next diagram represents a very simple safety control scheme typically as required for a machine tool to protect operators against getting entangled in rotating parts.

Figure 1.4:*Elementary guard position interlock with guard open, drive stopped*

The interlocks prevent the spindle drive from starting unless the guard is closed. Failure of any part of this interlock system increases the risk of an accident. It is easy in this example to see that the limit switches and final contactor form part of the safety function.

A typical hardware based implementation of the guard door safety function will link the guard door switches in series with an emergency stop switch to provide an input to a latching relay. The latching relay will trip when the guard door is opened or when the E-Stop is pressed.

To improve the safety of the circuits an additional relay is used to prevent the latching relay from being reset unless the safety control circuits are healthy (i.e. free of dangerous faults). For example in figure 1-5 a simplified safety relay design is shown where K3 is a relay that must be energized before the latching relay K1 can be set. K3 will not energize unless the power control contactor(s) C has been released, proving that it is not held in by another stray circuit or by a mechanical defect.

In practice relay K1 is usually duplicated by a second channel or redundant relay K2 and both relays must be energized and latched to close the output circuits. K3 is often arranged with multiple contacts and expansion units to enable many drives to be interlocked from the same logic.

Figure 1.5: *Simplified circuit of an E-stop and guard monitoring relay*

The example shown in figure 1.5 uses a safety monitoring relay unit to perform the essential logic functions required to provide safety integrity. These are: Checks on the state of input signals, detection of stuck contactors, wiring faults in the input and output circuits, timing and logic for interlocking control etc. The safety monitoring relay modules ensure that the safety interlocks and E-Stop functions are able to operate independently of the basic control system actions at all times.

These are some of the key design features we shall be keeping in mind throughout the workshop. Later in the workshop we shall be looking at ways of achieving functional independence for the safety systems whilst achieving the cost and performance benefits of a physically integrated control and safety system.

1.3 Distinction between Machinery and Process Safety Control Systems

There are important parallels between process safety systems and machinery safety. These are worth noting because many technicians and engineers will have to deal with safety systems in both categories. There is also an increasing trend to share the technical standards across these industries and some vendors offer safety equipment that is suitable for both.

For process technology the identification of unacceptable risks leads to set of risk reduction measures that often include what is known as a safety-instrumented system. (SIS) or emergency shutdown system.

- Process plant shutdown systems define the grade or performance of their applications in terms of safety integrity levels or SILs.
- Machinery safety systems are have been traditionally defined for

performance by “safety categories” but will in future be moving to the same basis of SILs for complex and/or programmable safety systems.

Process plant safety is subject to different regulations and design standards from those applicable to machinery safety but the basic principles are essentially the same.

Some interesting questions arise when a section of process plant has a large and dangerous machine in the plant.

- Is the hazard coming from the process or from the machine?
- Which regulations are applicable?
- What design standard shall we apply?

If the hazard is due to the process the plant safety systems can deal with it. If the machine presents hazards of its own the safety requirements will fall under machinery safety regulations.

1.4 International Standards and Practices

It is a characteristic of safety legislation in most industrialized countries to have an overall requirement for safety at work in the form of general occupational health and safety regulations. The regulations then refer to a subset of regulations directed at particular aspects of hazards at work.

Regulations such as OHSA (in USA) and ESHWR (in Europe) requires all companies to ensure the safety of workers, environment and plant. Safety practice begins in all industries with the practice of risk assessment, requiring companies to identify and evaluate risk in the workplace and to record the measures if any that they have taken to minimize the risks. When it comes to the provision of measures to improve safety there is a difference in approach for some industries as noted below.

1.4.1 Safety engineering methods in process plants

In the case of process plants such as refineries or chemical works the laws leave the details of the engineered safety systems to be satisfied by a set of widely applied “best practices” to be used at the discretion of the end user. There are

some standards (such as IEC 61511) that set down the principles for management and design of the safety systems for process plants. The owner or operating company is then obliged to justify the details of the safety measures for each application.

1.4.2 Safety engineering methods in machinery

In machinery applications, the legislation either prescribes adherence to a set of named standards (USA practice) or it allows us to presume compliance if we follow the relevant standards (EU practice). If there are no standards applicable for a particular machine, a safety case can be established by using the general principles applied in all safety applications. These principles are set down in higher level, general-purpose standards. It is these high level standards that are of particular interest to us in this workshop since they provide a good basis for essential training in the subject.

1.4.3 International standards

Both process and machinery safety methods are part of a growing trend to set common standards for safety practices that will be acceptable all across the world. Our next figure shows some of the major regulations and standards that have become established in Europe and in the USA.

Figure 1.6:*Global legislations and standards for machinery and process safety*

Control of Major Accident Hazards regulations. COMAH is a European Union (EU) requirement for managing safety in large hazardous processes. Similar requirements exist in the USA under the process safety rules of OHS regulations (OSH 29 CFR 1910.119).

Control of Substances Hazardous to Health regulations. COSHH is a UK regulation to ensure that any factory handling or processing hazardous substances takes steps to minimize the risk of substances harming people or the environment. This is similar to the USA’s clean air act requirements of the

Environmental Protection Agency (EPA). (EPA 40 CFR 68).

The EU Machinery Directive defines machinery safety requirements to be observed in EU states by manufacturers, suppliers and users of machines. It references a wide range of general and detailed engineering standards that have been “Harmonized”. This means that they have been accepted by each of the member states as a national standard in that country. The great value of working to the requirements of a Harmonized standard is that it creates a “presumption of compliance “ with the relevant EC Directive. This simplifies the task of proving that the machine will meet the requirements of the Safety Directive.

There are other EU directives that impact on machinery equipment such as the Low Voltage Directive (LVD) and we shall look more closely at this in chapter 3.

In the United States there is general intention to achieve uniformity with European standards so that there can be free interchange of products and services. The OHSA regulations incorporate and require compliance with the **ANSI B 11 series of standards** produced by the Association of Manufacturing Technology (AMT), a trade association of the machine tool industry.

1.4.4 Supplier’s responsibility for safety

An important point to note about machinery safety legislation is that the designer and builder of a machine has a major responsibility to make the machine safe to use within a foreseeable range of applications. Since the machine may find its way into a wide variety of workplaces and into domestic homes in the case of home appliances, safety must be built into the machine as a unit. This makes the supplier of the machine responsible for proving it is safe to use. The supplier can be prosecuted for supplying an unsafe machine

1.4.5 Owners responsibility for safety

Once the machine is installed in a factory it becomes the owners responsibility to see that it is used in a safe manner and that all safety measures are properly maintained and applied. The owner will of course want to buy a machine that comes with all the safety measures in place. However as soon as two or more machinery devices are assembled to form a production unit the user has created

a new and often unique machine. Hence there will always be a need for the user to do risk assessment and to implement additional safety measures whenever the need is found.

It follows that both the suppliers and the end users should have a good knowledge of the range of applicable regulations and their supporting standards.

1.5 Introduction to hazards and risks

The first step in any safety related project is to identify the hazards and to consider the level of the risks they present. ***So what are hazards and what is risk?***

1.5.1 Hazard

In the broadest terms, a *hazard is* an inherent physical or chemical characteristic that has the potential for causing harm to people, property, or the environment. In machinery usage EN 292-1 describes Hazard as "*A source of possible injury to damage to health*" and it goes on to describe some elementary forms of mechanical hazard in the following list of hazard types:

-
- Cutting or severing
- Entanglement
- Impact
- Stabbing or puncture
- Friction or abrasion
- High pressure fluid ejection

Other types of hazard may also be present such as the primary chemical process hazards:

- Explosion
- Fire
- Toxic release

And we have already mentioned electrical hazards. The first task of any risk assessment is to identify the potential hazards of a machine and then move on to

evaluate the level of risk they present.

1.5.2 Risk

Risk is usually defined as the combination of the severity and probability of an event. In other words, how often can it happen and how bad is it when it does happen? Risk can be evaluated qualitatively or quantitatively.

Roughly: Risk = Frequency of the event x consequence of hazard

In EN 1050 a simple diagram similar to figure 1-7 shown here describes the elements of risk.

Figure 1.7*: Elements of risk are combined to produce a qualitative or quantitative value*

Qualitative descriptions of risk use terms such as “Low”, or “High” or “Severe”

Quantitative descriptions of risk use numerical values such as “1 irreversible injury per 1000 years” this might be the equivalent of a “Medium but unacceptable risk”. If the quantitative risk is reduced to say “1 irreversible injury per 100 000 years” we might describe this as a “Low and acceptable risk”.

1.6 Risk reduction

The reduction of risk can sometimes be achieved by design improvements but if this not practicable it often requires protection measures. In some cases this will be an alternative way of doing things or it can be a protection system such as a safety-related electrical control system. The design principle is shown in the diagram below.

Figure. 1.8 *Risk reduction steps*

As the diagram shows we have to evaluate the risks due to the hazards and then compare them with the target risk levels. To design a protection system we have to specify what safety function it has to perform and then define how good it must be (define the safety integrity).

The objective is to reduce the risk from the **unacceptable** to at least the **tolerable.** This seems simple enough as long as we can work out what is tolerable. Here's an example of risk reduction principles applied on the cricket field:

Figure 1.9*: Sporting example for risk reduction*

Safety systems are all about risk reduction. If we can't take away the hazard we shall have to reduce the risk.

Risk reduction can be achieved by reducing either the frequency of a hazardous event or its consequences or by reducing both them. Generally the most desirable approach is to first reduce the frequency since all events are likely to have cost implications even without dire consequences. So for a typical problem of physical harm from moving parts of a machine the risk reduction is achieved by reducing the possibilities that a person can get in the way of the moving the parts. If we can reduce the chance of trapping a hand in the moving parts from say once per week to perhaps once per hundred years we may feel that this is an acceptable solution. In this case we have settled for what is known as a **tolerable risk**.

1.7 The ALARP principle for tolerable risk

The next diagram illustrates the concept of tolerable risk and is known as the ALARP diagram.

Figure. 1.10*: Typical ALARP diagram*

The ALARP (as low as reasonably practicable) principle recognizes that there are three broad categories of risks:

Negligible Risk: broadly accepted by most people as they go about their everyday lives, these would include the risk of being struck by lightning or of having brake failure in a car.

Tolerable risk: We would rather not have the risk but it is tolerable in view of the benefits obtained by accepting it. The cost in inconvenience or in money is balanced against the scale of risk and a compromise is accepted. This would apply to travelling in a car, we accept that accidents happen but we do our best to minimize our chances of disaster. Does it apply to Bungee jumping?

Unacceptable risk: The risk level is so high that we are not prepared to tolerate it. The losses far outweigh any possible benefits in the situation.

Essentially this principle guides the design engineer and the safety specialist into setting tolerable risk targets for a hazardous situation. This is the first step in setting up a standard of performance for any safety system. The problem here is that it is difficult to determine what is a tolerable risk.

Some of the engineering standards simply state that the machine must be "safe". If we look in the standards for a definition of safety we get:***" Freedom from unacceptable harm"***

This seems to be the same thing as acceptable risk but doesn't get us any further. We shall take a more detailed look at "acceptable" or "tolerable" risk criteria in Chapter 3 as we follow the risk reduction steps described in the standard EN 1050.

1.7.1 Risk assessment procedure

The process for a risk assessment for the handling and use of machines follows the same general rules for all risk assessments. These rules are most clearly

described in a widely used brochure published by the UK Health and Safety Executive (HSE) called ‘Five steps to risk assessment’. We recommend readers to take a free download of this leaflet from the HSE website: www.hse.org.

The 5 steps recommended in the leaflet are shown in figure 1.11 below.

These simple risk assessment steps define the basis for our work on machinery safety just as they will apply to a wide variety of activities in the work place.

Figure 1.11*: 5 steps in the risk assessment procedure*

If we decide that the precautions are not adequate it will be clear that certain steps would be taken to improve the situation. Typically these steps are to be based on the following responses given in order of preference:

1. Try a less risky option
2. Prevent access to the hazard (e.g. by guarding)
3. Organize work to reduce exposure to the hazard
4. Issue personal protective equipment
5. Provide welfare facilities (e.g. washing facilities for removal of contamination and first aid).

In particular items 2 and 3 above will be relevant to our work on the development of machinery safety systems.

1.8 Development example for a machinery safety system

Here we take a typical example of machinery safety practices by looking at a commonly used machine: The metalworking or wood working Centre Lathe. One of the most widely used of all machine tools, the centre lathe presents some basic hazards. For example:

- The spinning chuck or spindle presents hazards: entanglement of clothes, abrasion,
- The cutting of metal can produce flying chips. An impact hazard including

damage to eyes
- An exposed lead screw presents a hazard of entanglement for clothes or trapping of hands

Figure 1.12 *Metal working lathe for risk assessment*

These three hazards present various levels of risk to the person using the lathe. The machinery safety systems are provided to reduce the risks presented by these hazards to levels that are considered reasonable or tolerable.

1.8.1 Risk Assessment Example

Here is an elementary risk assessment for the lathe example: The risks might be evaluated as shown before the application of measures to reduce the risks.

Hazard	Probability of event	Consequence	Risk
Operator contact with spinning chuck	High Avg. 1 per week	Abrasion wounds	Abrasion wounds once per week
Flying chips hit face	Very High Avg. 1per day	1 in 10 chance of eye damage	Eye damage once eve 10 days
Entanglement of clothes with exposed rotating lead screw	Moderate Avg. 1 per year	1 in 5 chance of broken arm	One broken arm per 5 years.

Clearly the risks shown in this table are unacceptable and they have to be reduced. Risk reduction options consist of ways of reducing the probability of the event and/or reducing the consequence. In chapter 3 we study risk assessment methods and ways of deciding what is tolerable.

1.8.2 Propose Safety Functions

For the moment if we assume that the risks have to be reduced it is easy to see that some typical safety measures can be applied. For example:

- The exposed lead screw can be made safer by a telescopic or flexible cover that remains in place at all times except when the machine is stripped for service. This is a mechanical guard that normally has no requirement for interlocking to the electrical drives.
- Where there is danger from flying chips it may be acceptable to wear protection equipment, (usually abbreviated: PPE) in this case; safety glasses.
- A lathe guard can be provided to cover the spinning chuck. In the slide shown here a simple hinged cover can be mounted to be put in place by the operator after he or she has set up the work piece and tightened the chuck jaws.

But now we have to be sure that the operator always swings or slides the cover into position. We want to be sure that the lathe cannot be operated if the cover is out of position.

This means we shall want to arrange an electrical interlock to make sure that the lathe will not start turning until the guard is in place. To do this we need to have a position-sensing switch, perhaps a mechanical limit switch, set up to ensure the guard is in position before it will close its contact. Here we have the beginnings of a safety related electrical control system. This particular safety function requires that electrical power to the lathe drive will be switched off if the guard is not in position.

Figure 1.13: Elementary guard position interlock with guard open, drive stopped:

Figure 1.14*: Elementary guard position interlock with guard closed, drive can be started:*

1.8.3 Risk assessment after adding protection measures

The table we saw at the start of this exercise can now be updated to show the

effect of protection measures. This is a typical risk assessment reporting method.

Hazard	Probability of event	Consequence	Risk before	Safety measure	Risk after
Operator contact with spinning chuck	High	Abrasion wounds	High	Interlocked guard	Low
Flying chips hit face	Very High	1 in 10 chance of eye damage	Severe	Interlocked guard and PPE goggles	Very Low
Entanglement of clothes with exposed rotating lead screw	Moderate	1 in 5 chance of broken arm	Medium	Flexible cover	Very Low

1.8.4 Evaluate expected risk reduction

It looks as if the safety interlock and guards we have specified will do the job very well. If we follow the risk reduction procedures what we need to do now is check to see if the new level of risk is acceptable or tolerable. This seems simple enough at first. But to be sure that we have got it right we have to consider possible problems due to failures of the equipment or due to incorrect design. This takes us into the subject of “safety integrity” and how it can be determined. We shall look at the whole subject of failure modes, reliability analysis and safety integrity at relevant points throughout the workshop.

Consider failure modes and limitations of the protection measures

Lets look again at the lathe guard example . What could go wrong? What are the chances? No safety device can achieve 100% reliability. For example:

- The limit switch must be good enough to always do its job even when the guard gets a bit worn and doesn’t locate so well. So it has to have a good range of tolerance for positioning errors.
- We don’t want someone to jam a matchstick into the switch so that the guard function can be defeated. So it must be tamper proof.
- If the cover is lifted or moved away whilst the chuck is spinning, the rundown time may not be fast enough to avoid an accident. So maybe the cover should be locked in place until the chuck has stopped. This will require some timing or speed sensing device and an electronic lock. Is this expense and complexity justified? How do we decide?

- If the limit switch does develop a fault we want to be sure that the safety of the guard function is not lost. So it should be fail-safe or it should be able to carry on protecting us even when it has a fault. (Fault tolerant). Better still we would like to know about the fault as soon as it develops. We may want the safety system to be self-testing (also known as having diagnostics).

The guard and its sensing system have to be designed such that it will not be an obstacle to high productivity. It must not get in the way of efficient use of the machine. It must not present temptations or incentives for people do without it (bypassing).

The cost of the equipment must not be so high that users are heavily penalised for ensuring safety.

Similar possible problems arise with the circuits and relays or programmable controllers that may be used in linking the limit switch to the drive interlock. Finally we have to make sure that the power break contacts to the drive control cannot be defeated by either a fault or by the actions of another control system or even by the maintenance technician.

So it is the designer’s responsibility to see that the safety devices are fit for purpose and it’s the maintenance technician’s job to keep the devices in good working order. Both parties must understand the design principles and safety functions of the devices.

1.8.5 Equipment Choices for the Safety Systems

The workshop will examine some of the features of the equipment and devices available to us. We must to be able to recognize the benefits and any weaknesses of our equipment choices. In particular the choices must balance safety performance, capital cost and the effect on productivity.

1.8.6 Standard solutions to standard problems

In many practical projects, the writers of machinery safety standards and the suppliers of components have done a lot of the design job for us for the most common types of machines and for most applications. So our job is to find out

what’s out there and how to make the best use of it. We get a lot of help form the industry specialists.

- Standards such EN 954, define safety categories suitable for graded levels of risk reduction service.
- Manufacturers offer safety products designed specifically for the most widely needed safety functions.
- Testing authorities certify that safety devices are fit for the designated tasks and certify the safety category that can be achieved.

The following are some of the electrical and electronic control equipment available in the market for machine safety, arranged in approximate categories:

- Emergency-Stop switches,
- Safety gate position limit switches, tongue or cam operated
- Monitoring safety relays for:
    - Emergency stops
    - Guard positions,
    - Two hand controls
    - Speed monitors and timers.
- Muting systems
- Locking safety switches, interlocking devices, trapped key systems
- Electro sensitive presence sensing devices including:
    - Edge sensing
    - Safety mats
    - Safety light screens/curtains
    - Programmable Logic Controllers for safety applications
    - Certified software applications for commonly used safety functions
    - Bus networking of sensors and logic controllers for complex safety applications.

In the workshop we shall be looking at the principles of the different protection methods and will hope to see the factors that will help us to make the best choices for any application.

1.8.7 Programmable systems for automation safety

Programmable systems have become established in machinery safety and there are many new developments taking place at the high tech end of the market. We shall take a look at the technologies later in the workshop. For the moment we

can just list some of the reasons why we would want to use programmable electronics and networks in safety systems:

- Sequencing of shutdown actions in large machines
- A manufacturing line consisting of several closely linked machines will have many safety functions. For efficiency they need to be implemented under one centralised logic system with efficient monitoring and fault detection.
- Software driven safety functions provide powerful logic tools with flexibility for coping with changing automation functions.
- Efficient diagnostics software speeds up troubleshooting and reduces downtime.
- Networked input/output systems simplify cabling and reduce installation costs
- Selective shutdown facilities reduce the impact of safety trips on the rest of the plant.
- Cost benefits of re-using software for multiple copies of the same machines.

As stated earlier, the publication of IEC 61508 and the development in progress of a machinery sector version of this standard has set down a firm basis for the use of programmable systems. We shall outline this standard later in the workshop.

1.8.8 Development of Integrated Safety Systems

We have seen that there is a need for the safety systems to be functionally independent of the basic machine control systems. However from the manufacturing point of view there are cost penalties in having to build two control systems for each machine. If you are making, say, several hundred injection moulding machines it would be better if one complete control system could handle both safety and basic control. If you could place all the regular sensors and the safety sensors on one bus network feeding one control box this would be even better.

To a large extent this approach is now becoming feasible without breaking the rules of functional independence and with out any loss of safety integrity. Some of the reasons why this approach is gaining ground:

- Safety PLCs can be made with internal separation of safety and non-

safety sections.
- Bus systems can achieve safety rated performance for all sensors.
- Continuous diagnostics can ensure fail safe behaviour
- Safety certified software function blocks can operate in secure partitions of the PLC operating system.

We shall take a brief look at this technology after covering the basics of programmable safety systems

1.9 The Engineering Tasks

1.9.1 Introduction to the Safety Lifecycle

The safety products are a great help but they do not relieve the applications engineer of the duty to see that the complete safety function has been designed to meet the original objective. It is always necessary to examine the complete design to see that it meets all aspects of the required safety function and satisfies the required safety category or risk reduction capability. The key to managing this task properly is to plan and execute what is known as the “Safety Life Cycle”. This simply means all the phased activities from the beginning of the design to the day that someone disposes of the machine.

Figure 1.15*: Elements and information flow in the safety lifecycle*

Here is a rough and informal description of the main steps of design for the safety-related parts of the control system. Lets recap the thinking process we have just been through for the centre lathe protection so we can identify some of the steps in that application.

S**tep 1: Obtain information**

Obtain information about the machine and its intended use.. (In our case a centre lathe used for machining metal objects)

Step 2: Conduct a hazard identification exercise.

For each hazard and analyse the level of risk in terms of consequence of the accident and likelihood of the event. (We listed the hazards, we also decided the consequences and estimated the exposure of the operator and frequency of the possible accident assuming there are no safe guards)

Step 3 : Decide on the measures to be taken to reduce the risk.

This involves defining the safety functions to be provided both by design of the machine and by design of safeguarding functions. (We are stuck with the design, so we chose to provide a safety function, which will prevent the drive from running unless the guard is in position). This step includes defining all the essential safeguards such as being tamper proof.

Step 4: Outline the design of the safety system to identify the subsystems involved in the safety related electrical control system.

We can see there will be a position sensing device with critical requirements and a fail-safe interlocking system to prevent the drive from running unless the sensor circuit is closed.

Step 5: Specify the equipment and its safety categories.

For each subsystem, specify the equipment type you want to use and the level of safety integrity it must have.

This is also known as the safety category; the higher the category, the greater the assurance that the subsystem will not fail in a dangerous way. Finding the right category is a matter of knowing the level of risk reduction needed for each application. The standards provide us with further assistance in the way of selection charts. We are referring here to standard EN 954-1 for safety categories. This is a subject we are going to examine in some detail in Chapter 4.

Step 6: Design verification

Carry out a verification check to see that the results we have achieved so far have not been deviated from the original requirements through some misunderstanding or through changes to the original problem analysis. To ensure this is true we need to have a record of all our design work showing how each decision is based on information that is still correct.

Step 7: Detailed Design and Building

Proceed with detailed design, equipment selection and implementation of the solution. Also define the maintenance and regular testing requirements. Make sure proper test facilities are provided with the equipment.

Step 8 Validation

Check that the design documents and the testing plan are aligned and up to date

Carry out proper testing to demonstrate that the safety functions are fully operational and perform as intended under all foreseeable conditions. Record the results.

Step 9: Provide a design history file or “Technical file “

Describing how the safety system design has been developed, reporting the results of assessments and assumptions and demonstrating how the design satisfies risk reduction requirements.

Step 10: Use and maintain the safety systems

As intended by the designers, implement a programme of regular testing. Keep a record of all tests and enforce strict change control to ensure that the safety system and its design records remain up to date.

The above steps are based on the procedures mapped out in the relevant European Standards but are only an approximate description. We shall look more carefully at the standard procedures in chapter 3 of the workshop.

1.9.2 Importance of change control

Its one thing to have a well documented track record for the safety system but the next step in the safety life cycle requires that a procedure be maintained for trapping any changes to the machine that will affect the validity of the present safety design. The basis of change control is that all machinery modifications will be subject to a hazard review against the original hazard analysis documents to see if it has impact on the present safety functions.

If a change is required it must be processed through the relevant steps of the

safety life cycle and all updates must be done and recorded properly. This is a hard discipline to follow but it is the best way to maintain or improve the standard of safety that was achieved for the original machine.

Is all of this relevant to maintenance work?

Yes it is. For those involved in maintenance rather than in design it is still important to understand the design processes that should (in theory) lie behind the products you are working with. The latest safety standards require that persons working on safety systems are competent to do so. Competence includes being aware of the design rules and understanding the performance requirements of the safety devices.

It is important for a maintenance technician to fully understand the safety function of the subject equipment and to know the reasons why it has been given a particular safety category. If anything changes in the design of the equipment or in the way the machine is being used the performance requirements of the safety device may be affected. The end user has a continuing responsibility to ensure that adequate safety levels are maintained. This responsibility cannot be properly fulfilled if the reasons for the existing safety measures are not known.

1.10 Benefits of the Systematic Approach

One of best advocates for a systematic approach to safety engineering is the UK Health and Safety Executive (HSE): Their publication: “ Out of Control” is a very useful little book about “Why control systems go wrong and how to prevent failure ” The following analysis of 34 accidents attributed to control system failures has been widely published.

Figure 1.16*: Analysis by UK Health and Safety Executive of causes of safety control system failures.*

HSE’s summary of the problems causing accidents due to control systems includes some useful paragraphs:

“The analysis of the incidents shows that the majority were not caused by some

subtle failure mode of the control system, but by defects which could have been anticipated if a systematic risk-based approach had been used throughout the life of the system. It is also clear that despite differences in the underlying technology of control systems, the safety principles needed to prevent failure remain the same.

Specification

The analysis shows that a significant percentage of the incidents can be attributed to inadequacies in the specification of the control system. This may have been due either to poor hazard analysis of the equipment under control, or to inadequate assessment of the impact of failure modes of the control system on the specification. Whatever the cause, situations which should have been identified are often missed because a systematic approach had not been used. It is difficult to incorporate the changes required to deal with the late identification of hazards after the design process has begun, and more difficult, (and expensive), to make such changes later in the life of the control system. It is preferable to expend resources eliminating a problem, than to expend resources in dealing with its effects.

Design

Close attention to detail is essential in the design of all safety-related control systems, whether they are simple hard- wired systems, or complex systems implemented by software. It is important that safety analysis techniques are used to ensure that the requirements in the specification are met, and that the foreseeable failure modes of the control system do not compromise that specification. Issues of concern, which have been identified, include an over-optimistic dependence on the safety integrity of single channel systems, failure to adequately verify software, and poor consideration of human factors. Good design can also eliminate, or at least reduce, the chance of error on the part of the operator or maintenance technician.

Maintenance and modification

The safety integrity of a well-designed system can be severely impaired by inadequate operational procedures for carrying out the maintenance and modification of safety-related systems. Training of staff, inadequate safety analysis, inadequate testing, and inadequate management control of procedures were recurring themes of operational failures."

We can conclude that being systematic:

- Helps us to benefit from previously acquired knowledge and experience.
- Minimizes the chances of errors
- Demonstrates to others that we have done the job properly… they recognize our way of doing things is legitimate
- Makes it easier to compare one solution or problem with another and hence leads to generally accepted standards of protection
- Allows continuity between individuals and between different participants in any common venture. Makes the safety system less dependent on any one individual.
- Encourages the development of safety products that can be used by many.
- Assists suppliers to achieve compliance with regulations.

1.11 Conclusions

This overview has shown us that machines come in all shapes and forms and they can present us with a number of characteristic hazards. We have seen that there is a systematic method of identifying the hazards and assessing the risks based on the judgement of experienced persons who are needed to estimate the risks, i.e. the likelihood of an accident and the severity of the consequences.

Regulations require that we carry out risk assessments to decide the need for safeguards and the same regulations require that we install and maintain safeguarding equipment to an acceptable design. Engineering standards exist to guide us on what is considered to be acceptable practice both in the design of solutions and in the way we manage the safety life cycle of the machine.

Safeguarding methods range from passive guards to sophisticated safety related controls but all have the task of reducing risk. The amount of risk reduction needed depends on the original unguarded risk and the perception of what is safe or tolerable. This leads us to the concept that the quality of the solution or the quantity of risk reduction to be applied defines the performance needs of the safety system.