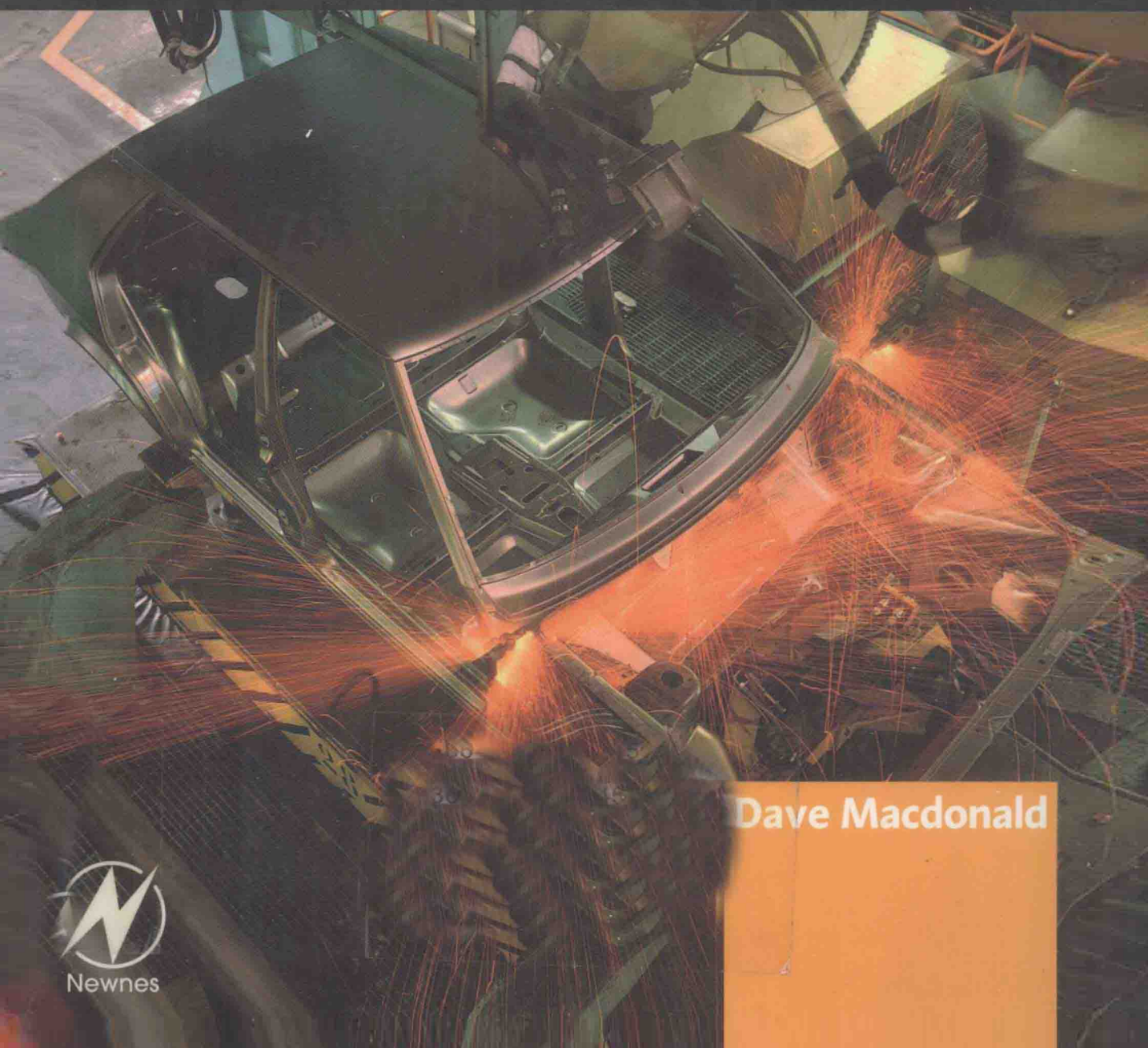
ELSEVIER

Practical Machinery Safety



Dave Macdonald

Newnes

Practical Machinery Safety

David M. Macdonald BSc (Hons) Inst. Eng., Senior Engineer,
IDC Technologies, Cape Town, South Africa

Series editor: Steve Mackay

ELSEVIER

AMSTERDAM ... LONDON
NEW YORK ... EGO
SAN FRANCISCO ... SINGAPORE ... SYDNEY ... TOKYO

Newnes is an imprint of Elsevier

Newnes

Newnes
An imprint of Elsevier
Linacre House, Jordan Hill, Oxford OX2 8DP
200 Wheeler Road, Burlington, MA 01803

First published 2004

British Library Cataloguing in Publication Data
Macdonald, D.M.
Practical machinery safety. – (Practical professional)
1. Machinery – Safety measures 2. Machinery – Safety appliances 3. Industrial safety
I. Title
621.8'0289

Library of Congress Cataloguing in Publication Data
A catalogue record for this book is available from the Library of Congress

ISBN 0 7506 6270 0

Typeset and edited by Integra Software Services Pvt. Ltd, Pondicherry, India
www.integra-india.com
Printed and bound in The Netherlands

Practical Machinery Safety

Other titles in the series

Practical Data Acquisition for Instrumentation and Control Systems (John Park, Steve Mackay)

Practical Data Communications for Instrumentation and Control (Steve Mackay, Edwin Wright, John Park)

Practical Digital Signal Processing for Engineers and Technicians (Edmund Lai)

Practical Electrical Network Automation and Communication Systems (Cobus Strauss)

Practical Embedded Controllers (John Park)

Practical Fiber Optics (David Bailey, Edwin Wright)

Practical Industrial Data Networks: Design, Installation and Troubleshooting (Steve Mackay, Edwin Wright, John Park, Deon Reynders)

Practical Industrial Safety, Risk Assessment and Shutdown Systems for Instrumentation and Control (Dave Macdonald)

Practical Modern SCADA Protocols: DNP3, 60870.5 and Related Systems (Gordon Clarke, Deon Reynders)

Practical Radio Engineering and Telemetry for Industry (David Bailey)

Practical SCADA for Industry (David Bailey, Edwin Wright)

Practical TCP/IP and Ethernet Networking (Deon Reynders, Edwin Wright)

Practical Variable Speed Drives and Power Electronics (Malcolm Barnes)

Practical Centrifugal Pumps (Paresh Girdhar and Octo Moniz)

Practical Electrical Equipment and Installations in Hazardous Areas (Geoffrey Bottrill and G. Vijayaraghavan)

Practical E-Manufacturing and Supply Chain Management (Gerhard Greef and Ranjan Ghoshal)

Practical Grounding, Bonding, Shielding and Surge Protection (G. Vijayaraghavan, Mark Brown and Malcolm Barnes)

Practical Hazops, Trips and Alarms (David Macdonald)

Practical Industrial Data Communications: Best Practice Techniques (Deon Reynders, Steve Mackay and Edwin Wright)

Practical Machinery Vibration Analysis and Predictive Maintenance (Cornelius Scheffer and Paresh Girdhar)

Practical Power Distribution for Industry (Jan de Kock and Cobus Strauss)

Practical Process Control for Engineers and Technicians (Wolfgang Altmann)

Practical Telecommunications and Wireless Communications (Edwin Wright and Deon Reynders)

Practical Troubleshooting Electrical Equipment (Mark Brown, Jawahar Rawtani and Dinesh Patil)

- Automation engineers
- Test engineers.

We would hope that you will be able to do the following as a result of reading this book:

- Identify hazards that occur with machinery and make them safe
- Describe the typical and widely used regulations for Safe Machinery use
- Apply the design procedures for Safety Controls
- Understand the Regulations that apply to manufacturers and users of equipment
- Apply safety rules to your next design involving guards, electrical and safety systems
- Perform simple risk assessment and hazard study methods to your project
- Understand machinery protection devices
- Know when to use Safety PLCs and how to apply them effectively
- Apply basic principles of Machinery Safety Management.

A basic working knowledge of electrical engineering concepts is useful but not essential as there will be a brief revision at the commencement of the class.

Preface

The technology of safety-related control systems plays a major role in the provision of safe working conditions throughout industry. Regulations require that suppliers and users of machines in all forms from simple tools to automated manufacturing lines take all necessary steps to protect workers from injury due to the hazards of using machines. Perhaps your company is wasting money on inappropriate safety measures that still do not deliver compliance with local safety regulations? This book aims to provide you with the knowledge to tackle machinery safety control problems at a basic and practical level whilst following the best available international standards. The book begins with an overview of machinery safety issues, introducing the concepts of hazard identification and risk reduction. The major international standards that are used to support compliance with EC regulations are highlighted and these standards are used as a basis for the design procedures. This approach will assist you to follow best practices for safety system applications wherever your plant is situated. The book looks at the risk assessment processes used to identify hazards and to quantify the risks inherent in a machine. This enables engineers to evaluate the need for risk reduction and hence define the safety functions to be provided by safety-related electrical controls. The book then introduces the concepts of safety categories as defined by standard EN 954 and illustrates the principles of failsafe design, fault tolerance and self-testing. With design procedures established the book now provides an introduction to machinery protection devices such as guards, enclosures with interlocks and guard monitoring relays, locking systems, safety mats, photo electric and electro sensitive principles and the application of light curtains.

The book continues with a study of Safety Control System techniques and introduces the principles of safety-certified PLCs focussing on practical useful information. Application examples such as guard door interlocking applications, two-hand controls, muting, area protection of robot installations and motion detection are then discussed.

The recently established standard IEC 61508 for functional safety of programmable systems is outlined. The concepts of safety integrity levels (SILs) are briefly explained and the key issues associated with software based safety applications are highlighted.

Typical people who will find this book useful include:

- Instrumentation and control engineers and technicians
- Process control engineers and technicians
- Electrical engineers
- Consulting engineers
- Process development engineers
- Design engineers
- Control systems sales engineers
- Maintenance supervisors
- Compliance engineers
- Machinery designers and system integrators
- Safety professionals, health and safety officers
- Production managers

Contents

1

Introduction to the machinery safety workshop

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 onto 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 stop 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 designed 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 the effective management of all aspects of the safety system throughout its life cycle. This workshop therefore combines basic training in the principles of safety

management, with specialized chapters on the safety devices and techniques commonly seen in industry.

We shall 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 recognize the basic features of safety systems and to know the principles on which they should be built.

1.1 Scope and objectives

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

- The definition of a machine and its safety-related controls
- Regulations and standards
- Hazards and risk assessment
- Concepts of risk reduction and tolerable risk
- An introduction to the safety life cycle 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 programmable logic controllers (PLCs) and bus networks.

The topics will be studied in more detail in the following 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 equipments which has moving parts can be considered a machine. Various definitions of machines are offered in engineering standards.

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 equipments. Typically we are interested in familiar types of machinery and there are some obvious groupings:

- Domestic applicances
- Lifts and escalators, cranes and hoists, forklift 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 centers
- Assembly lines and conveyor systems where multiple machines are coordinated to provide a complete manufacturing process
- Robots and robot-operated assembly or packing units
- Agricultural machines such as combined 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. Let us look at a simple diagram of a machine with its basic control system (see Figure 1.1) and then see where the safety system fits in.

Figure 1.1 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-molding 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 program of actions that will be decided by the operator and/or the stored program within the machine.

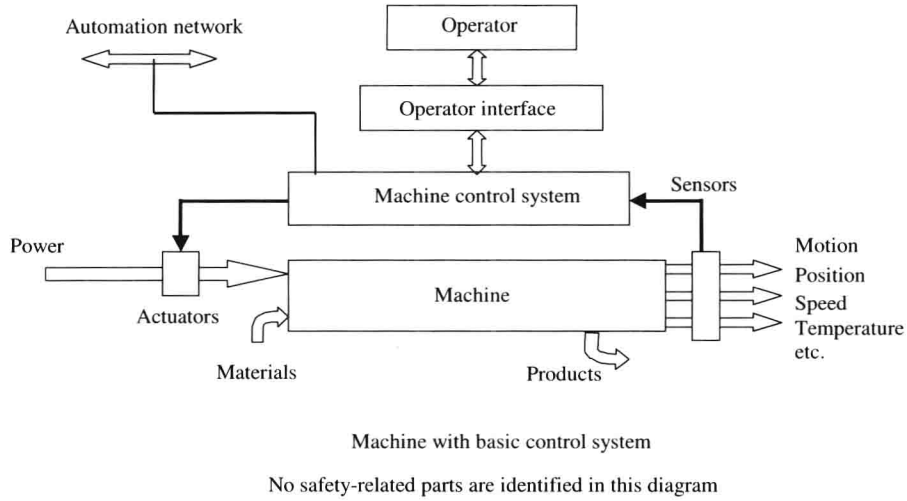


Figure 1.1
Block diagram model of a typical machine

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 coordination with several other machines. Hence we must recognize 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 programed.

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 in the wrong place at the time.

Fixed guards are usually the first line of defense 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 Figure 1.2 they are shown to consist of safety critical parts of the basic controls (e.g. emergency-stop controls) as well as separate sensors for devices such as the presence-sensing light curtains or safety mats.

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 an SRECS. The elements of an SRECS are as shown in Figure 1.3 and it is worth noting that these are very similar to those required for a process SIS.

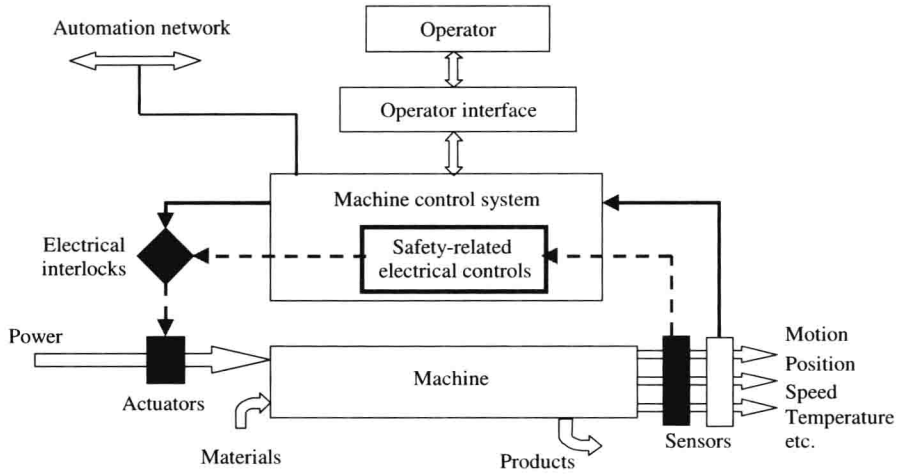


Figure 1.2
Block diagram of machine showing safety-related parts

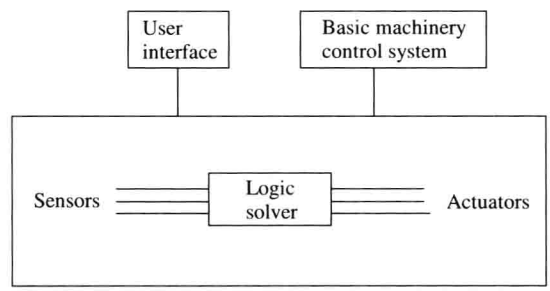


Figure 1.3
Basic elements of a safety-related control system

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.

Figure 1.4 represents a very simple safety control scheme typically required for a machine tool to protect operators against getting entangled in rotating parts.

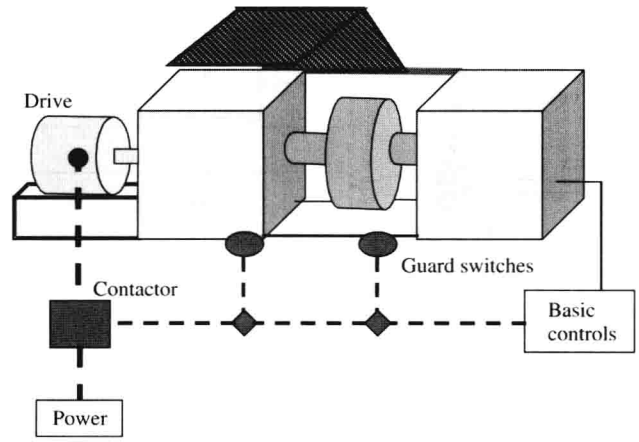


Figure 1.4
Elementary guard position interlock with guard open, drive stopped

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 E-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.

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.

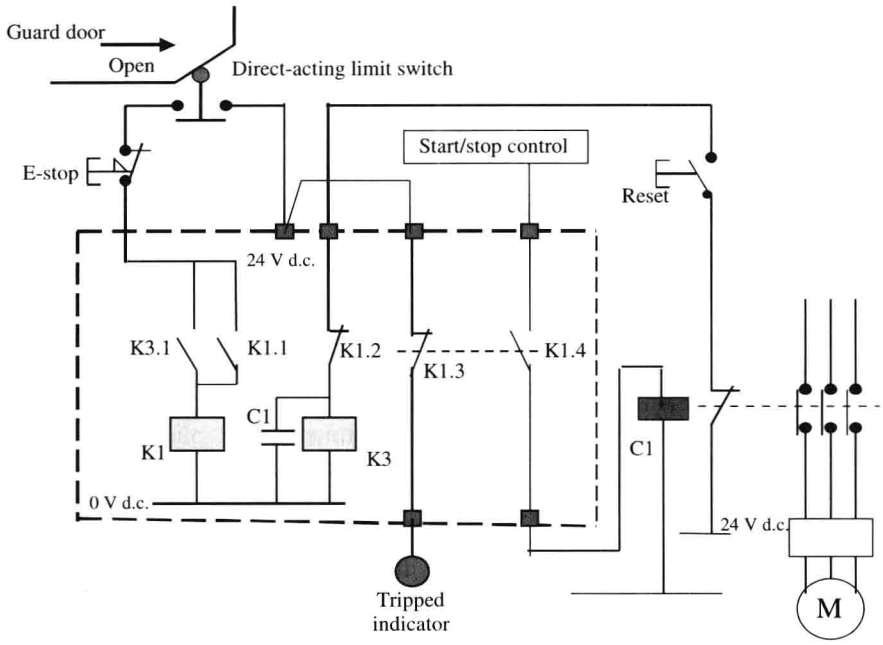


Figure 1.5
Simplified circuit of an E-stop and guard-monitoring relay

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 a 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 (SILs).
- Machinery safety systems are 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?