BIA-Report 6/97e

Categories for Safety-related Control Systems in Accordance with EN 954-1

HVBG
Hauptverband der gewerblichen Berufsgenossenschaften

Authors: Werner Kleinbreuer, Franz Kreutzkampf,
Karlheinz Meffert, Dietmar Reinert
Berufsgenossenschaftliches Institut
für Arbeitssicherheit – BIA, Sankt Augustin

Translated by: Health and Safety Executive Translation Services
together with BIA

Publisher: Hauptverband der gewerblichen
Berufsgenossenschaften (HVBG)
Alte Heerstraße 111, D-53754 Sankt Augustin
Phone: (+49) 0 22 41 / 2 31 - 01
Fax: (+49) 0 22 41 / 2 31 - 13 33
Internet: http: / / www.hvbg.de

– September 1999 –

Typesetting and Layout: HVBG, Öffentlichkeitsarbeit

Printed by: DCM – Druck Center Meckenheim

ISBN: 3-88383-528-5
ISSN: 0173-0387

Abstract

This report describes the main elements of EN 954 “Safety of machinery – safety-related parts of control systems, Part 1: General design principles“ and deals with the application of this standard, drawing on numerous examples from electromechanics, fluid technology, electronics and computing.

Information is also provided on the link between EN 954 and the basic safety requirements laid down in the machinery directive, and possible means of risk assessment are also described. On the basis of this information, the report can be used as an aid in the selection of the category of safety-related parts for control systems for machinery. The requirements of each category are covered in detail and, where necessary, the relevant background information regarding the implementation of these requirements for control systems in practice is also provided. Three comprehensive tables depict the fundamental safety principles, those safety principles that have become established and component parts that have proved to be safe. The tables are partly broken down into specific applications. The examples show how categories B to 4 can be implemented in practice, going as far as giving examples of component parts. Information is also provided on the safety principles used and on component parts that have a proven track record in terms of safety. Numerous bibliographical references are also given for readers who want to look into individual examples in more depth.

As well as detailed electric, hydraulic and pneumatic error lists, the two appendices also contain several examples for assessing the risk presented by machinery.

The report shows that the requirements stipulated in EN 954-1 can be implemented in practice and therefore makes an initial contribution to promoting the uniform application and interpretation of categories throughout Europe.

Kurzfassung

Der vorliegende Report stellt die wesentlichen Inhalte der EN 954 „Sicherheit von Maschinen – Sicherheitsbezogene Teile von Steuerungen, Teil 1: Allgemeine Gestaltungsleitsätze“ dar und erläutert die Anwendung der Norm an zahlreichen Beispielen aus den Bereichen Elektromechanik, Fluidtechnik, Elektronik und Rechnertechnik.

Der Zusammenhang mit den grundlegenden Sicherheitsanforderungen der Maschinenrichtlinie wird aufgezeigt, und die möglichen Verfahren zur Risikoabschätzung werden vorgestellt. Auf der Basis dieser Informationen erlaubt der Report die Auswahl der Kategorie für sicherheitsbezogene Teile von Steuerungen an Maschinen. Auf die Anforderungen für die jeweilige Kategorie wird im Detail eingegangen, und da, wo notwendig, finden sich die erforderlichen Hintergrundinformationen zur Umsetzung der Anforderungen in die steuerungstechnische Praxis. In drei umfangreichen Tabellen werden die grundlegenden Sicherheitsprinzipien, die bewährten Sicherheitsprinzipien und sicherheitstechnisch bewährte Bauteile z.T. anwendungsabhängig aufgelistet. Die Beispiele zeigen bis auf die Bauteilebene, wie die Kategorien B bis 4 in den jeweiligen Technologien technisch umgesetzt werden können. Sie geben dabei Hinweise auf die verwendeten Sicherheitsprinzipien und sicherheitstechnisch bewährte Bauteile. Zahlreiche Literaturverweise dienen einem tieferen Verständnis der einzelnen Beispiele.

In zwei Anhängen finden sich sowohl ausführliche elektrische, hydraulische und pneumatische Fehlerlisten als auch mehrere Beispiele für die Risikoabschätzung an Maschinen.

Der Report zeigt, daß die Anforderungen der EN 954-1 in Technik umgesetzt werden können und stellt damit einen ersten Beitrag dar, eine einheitliche Anwendung und Interpretation der Kategorien in Europa zu fördern.

Résumé

Le présent compte rendu suivant présente les principaux contenus de la norme EN 954 «Sécurité des machines – Pièces de sécurité dans les commandes, Partie I : Principes généraux de construction» et explique l'application de la norme à l'aide de nombreux exemples tirés des domaines de l'électromécanique, de la technique des fluides, de l'électronique et le l'informatique.

Le lien avec les exigences de sécurité fondamentales définies dans la directive machines est mis en évidence, les méthodes envisageables pour l'évaluation des risques sont présentées. Sur la base de ces informations, le compte rendu permet de choisir la catégorie des pièces de sécurité dans les commandes de machines. Les exigences des différentes catégories sont exposées en détail et les informations de base sur leur transposition dans la pratique technique sont fournies là où elles sont nécessaires. Trois grands tableaux présentent, partiellement classés par application, les principes de sécurité fondamentaux, les principes de sécurité qui ont fait leurs preuves et les pièces de sécurité confirmées. Les exemples montrent jusqu'au niveau des pièces comment les catégories B à 4 peuvent être mises en pratique dans les différentes technologies. Ils donnent à cet égard des indications sur les principes de sécurité utilisés et sur les pièces de sécurité de fiabilité attestée. De nombreuses indications bibliographiques permettent d'approfondir la compréhension des différents exemples.

Deux annexes contiennent des listes détaillées de défaillances électriques, hydrauliques et pneumatiques, de même que plusieurs exemples d'évaluation des risques sur les machines.

Le compte rendu montre que les exigences de la norme EN 954-1 peuvent être mises en œuvre dans la technique et constitue ainsi une première contribution à une application et à une interprétation homogènes de ces catégories en Europe.

Resumen

El presente informe da a conocer los contenidos más importantes de la norma europea EN 954 sobre «Seguridad de las máquinas – Piezas en relación a la seguridad de sistemas de control, parte 1: Principios de configuración generales» y explica el empleo de la norma con muy variados ejemplos de los ramos de la electromecánica, la técnica de fluidos, la electrónica y la técnica de ordenadores.

Se muestra la relación con las exigencias de seguridad básicas de la directiva para máquinas y se dan a conocer los posibles procedimientos para el cálculo de riesgos. Mediante estas informaciones, el informe hace posible la selección de la categoría de piezas o elementos relacionados con la seguridad de los sistemas de control de las máquinas. Se hace referencia detallada de las exigencias de cada categoría y, siempre que resulte ello necesario, se cuenta con las informaciones básicas necesarias para la aplicación de las exigencias en la práctica real de la técnica de los sistemas de control. Los principios de seguridad básicos, los principios de seguridad ya aceptados por sus buenos resultados y las piezas de construcción de técnica de seguridad se alistan – en parte de acuerdo a su aplicación – en tres cuadros bien amplios. Los ejemplos muestran hasta al nivel de las piezas de construcción cómo las categorías de B a 4 pueden aplicarse técnicamente a cada una de las tecnologías correspondientes. En estos ejemplos se encuentran indicaciones sobre los principios de seguridad y sobre las piezas de construcción relacionadas a la técnica de seguridad y ya aceptadas por sus buenos resultados. Se ofrece numerosa información bibliográfica para la profundización de los ejemplos individuales mostrados.

En dos anexos se encuentran listas de errores exhaustivas en relación a la electricidad, la hidráulica y la neumática así como varios ejemplos en relación al cálculo de los riesgos propios de las máquinas.

El informe muestra que las exigencias de la norma EN 954-1 pueden tener sus aplicaciones técnicas y en este sentido viene a ser una primera contribución a la promoción de la aplicación unificada y de la interpretación de las categorías en Europa.

Table of Contents

Foreword

After nearly eight years' work, the European Standard, EN 954-1, entitled "Safety of Machinery – Safety-related Parts of Control Systems, Part 1: General Design Principles" was adopted in early 1996. The relatively long time which it had taken to draw up this standard becomes understandable, when you consider that this is an extremely complex standardization issue, which had no predecessors on either a European or a national level to serve as a pointer in the right direction.

The aim was to design a standard which was not application-specific (Type B standard), which could be referred to by other standards in the field of machinery safety (specific machinery or safety devices) in relation to the design of the respective safety-related parts of the control system. In addition to the requirement that the standard should not be concerned with specific applications, the standardization project was also particularly concerned with the need to apply irrespective of the technology used (electromechanical engineering, electronics, computing, hydraulics, pneumatics). It is precisely this approach, encompassing the whole spectrum of technologies, which constituted such a challenge to those involved in this project, representing more than ten European states.

The specification of five categories for safety-related parts of machinery control systems and safety devices lies at the heart of European Standard EN954-1. These categories can be applied irrespective of the application and the control system technology used, and are solely concerned with the risk in question which is posed by a machine.

The aim of the present BIA-Report is to explain the categories defined in EN 954-1 and, in particular, to demonstrate the practical implementation of this standard in a wide range of technologies by the use of many examples of circuits[1]. The explanations and examples should not be construed as an official national or European comment on EN954-1. This report is rather a collation of nearly twenty years of practical experience gained by the Institute of Occupational Safety of the German Berufsgenossenschaften (BIA) in the development and evaluation of safety-related control systems and devices, and the knowledge acquired from many years of collaboration in the relevant national, European and international standardization committees.

This collection of sample circuits, which have been well-tried in a wide range of applications and with the associated risks, is

[1] Some of the examples of circuits collated in this report have already been published by the BIA in other publications. Of particular note is the loose-leaf edition "BIA-Handbook", published by Erich Schmidt Verlag, Berlin, which also continues to update and supplement the circuit examples and comments on the categories.

intended to be of particular use for the machinery designer as a source of ideas and assistance in selecting suitable control system categories and for his own designs. In addition, this report represents an initial attempt to promote the standardized application and interpretation of the categories in Europe.

The authors would like to thank the Health and Safety Executive, Mr. Ray Ward, for the first translation of this report into English.

1 Introduction

The Directive on the Approximation of the laws of Member States to Machinery [1] (known as the Machinery Directive for short) came into force on 1.1.1993 with a transitional period of two years. Since 1.1.1995, all machinery which is brought into circulation within the European economic area must satisfy the basic requirements of the Machinery Directive. As defined in Article 1 of the above-mentioned Directive, machinery means an assembly of linked parts or components, at least one of which moves, with the appropriate actuators, control and power circuits, etc., joined together for a specific application, in particular for the processing, treatment, moving or packaging of a material. Safety components which are introduced by the manufacturer for the purpose of guaranteeing a safety function and which, if they failed or did not function correctly, could endanger the safety or health of the persons in the working area around the machinery under the scope of application of the Machinery Directive are also covered by the second amendment to this Directive dated 22 July 1993 [2].

The basic requirements of the Machinery Directive with respect to machinery and safety components are to be found in Annex I to the Directive. In addition to the general principles for the integration of safety, this Annex also contains individual sections on control systems and control stations for machinery and on the requirements with respect to safety devices. The basic safety requirements for the design of machinery and safety components require the manufacturer to undertake a hazard analysis, in order to determine all the hazards associated with the machinery. Three principles are specified with a view to reducing the accident risks associated with the individual hazards to an acceptable extent:

- ❒ elimination or minimisation of the hazards by the design itself,
- ❒ taking the necessary protection measures in relation to hazards which cannot be eliminated and
- ❒ training for users to protect against residual hazards.

According to Article 5, observance of harmonized European standards leads one to assume compliance with the basic safety requirements of the Machinery Directive. Several draft European standards and European Standards which have been harmonized in the meantime extend or lend concrete support to the philosophy underlying Annex 1 of the Machinery Directive with a view to achieving safe working conditions for machinery. The EN 292 series of standards [3] is concerned with the basic concepts and general design principles for machinery safety, amongst other things.

EN 1050 [4], "Principles for Risk Assessment" describes the entire process of identifying hazards and estimating and evaluating risks for the individual hazards. On the basis of these two basic standards, EN 954, Part 1 [5] describes the risk reduction which is necessary when designing and constructing safety-related parts of control systems and safety devices. For the first time, this standard provides a classification system which can be applied on a general basis throughout Europe for control systems for machinery and / or associated safety devices. The five categories described in this standard are formulated in such a way that they are not specific to certain technologies and are therefore referred to by almost all special standards for the individual safety devices and are also mentioned in machinery-specific standards.

The aim of this BIA Report is to explain the categories defined in EN 954, Part 1 [5] for safety-related parts of control systems and, in particular, to demonstrate the practical implementation of these categories by way of example by the use of a wide variety of solutions. Neither the explanations nor the examples should be construed as an official national or European comment on EN 954-1. This report is rather a collation of nearly twenty years of practical experience gained by the Institute for Occupational Safety of the German Berufsgenossenschaften – BIA in the assessment of safety and control devices in a wide range of technologies, incorporating many years of collaboration in the relevant national and European standardization committees.

The following chapter describes the basic method of hazard analysis by means of risk appraisal in order to select the safety-related parts of control systems. Without going into the standard's requirements in detail, Chapter 3 gives a brief overview of the categories and indicates the significance of the fault lists attached in the Appendix to the report. The main body of the report is concerned with the set of examples of control systems for the individual categories. Specific examples from the different technology sectors (electromechanical engineering, electronics, computing, hydraulics, pneumatics) are given, classified in accordance with the five categories specified in EN 954-1. Both detailed control circuits and basic principles are described. All the examples are arranged in the same way and contain numerous bibliographical references.

In addition to the fault lists, the Appendix also contains several examples of risk estimation for specific hazards with respect to different types of machinery.

The authors hope that this report will provide the designer with concrete assistance in using

the categories for safety-related parts of control systems. This interpretation of the standard has been put to the test in a wide variety of practical applications and the examples have been translated into a great many specific applications.

European Standard EN 1050 [4] – Principles for Risk Assessment – describes an iterative process to achieve machinery safety. Accordingly, the risk for each individual hazard can be determined in four stages. This thus provides the basis for the necessary risk reduction using the categories described in EN 954 [5]. As shown in Figure1, the iterative process begins by determining the limits of the machinery. This process not only specifies and describes the intended use in all situations, but also specifies the spatial and

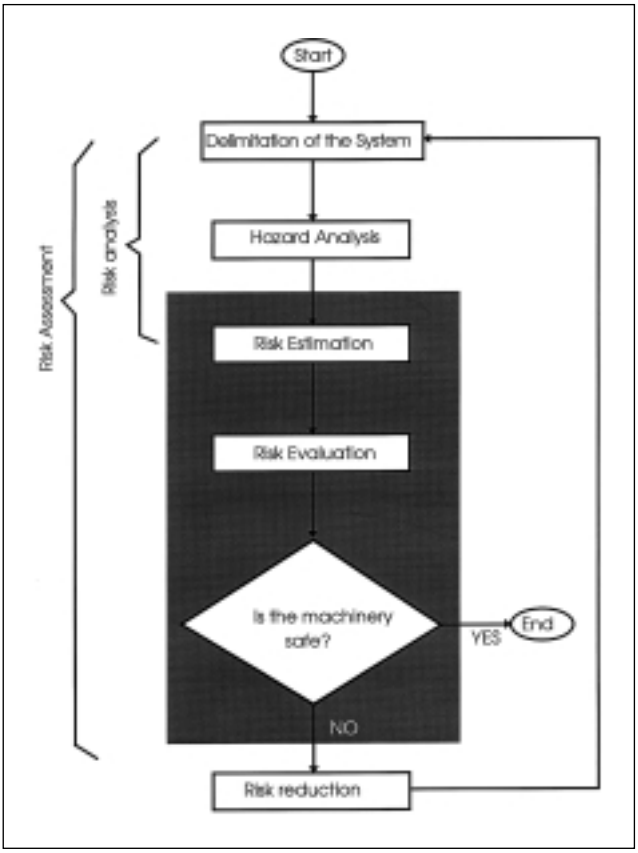


Figure 1:
The iterative process to achieve safety

time-related limits with respect to operation of the machinery.

In the second stage, the individual hazards for the machinery are identified and risk estimation is conducted for each of the hazards using four different elements of risk. This risk estimation, which could, for example, be conducted using the risk graphs in DIN V 19250 [6] or as defined in Appendix B of EN 954 [5], then constitutes the basis for a risk evaluation. Risk comparison is of vital importance in all of these processes, as the individual parameters for risk evaluation can only be specified by comparison with the solutions which are already in existence (risk evaluations and risk reduction measures). It is thus possible to use risk evaluation in order to establish, in a reasonably standard manner, the category to which safety-related parts of control systems belong.

The iterative process to achieve safety as described in EN 292 and EN 1050 will be applied to the safety-related parts of control systems in the three brief sections below.

2.1 Definition of Safety-related Parts of the Control System

In order to define a safety-related part of a control system, EN 954-1 refers to Appendix A of EN 292, Part 1. According to this standard, the control system begins with the component which processes an input signal issued

- ❒ by the controlled device and / or
- ❒ by the user or
- ❒ another person requiring protection

in such a way that safety-related output signals can be generated in conjunction with

- ❒ further input signals,
- ❒ data storage and
- ❒ logical processing of the various input signals.

The power control elements (main contactors, valves) are expressly included in the safety-related parts of a control system in the definition given in EN 954. Monitoring systems also come under the scope of application of EN 954. If Appendix A of EN 292 is used as a basis, the drive elements, power transmission elements and working parts, as well as the guards themselves, are excluded.

These comments show quite clearly that not only do logic units, such as programmable logic controllers or safety components for emergency stop operations form part of the concept of a “safety-related part of a control system“, but that complete safety devices, such as pressure sensitive mats with signal

processing [7], electrosensitive protective devices [8], two-hand control devices [9] or even interlocking devices in conjunction with guards [10], also come into this category if they contain safety-related parts of control systems. Most of the standards and draft standards published for the corresponding safety devices in the meantime relate to the classification scheme in EN 954-1 and define graduated requirements (often known as types) for the relevant safety device by specifying the relevant category. Thus, for example, in prEN 50100[2] [8], two types of electrosensitive protective devices are currently being standardized, relating to categories 2 and 4, whilst in EN 574 [9], five types of two-hand control devices are standardized, these being classified under categories 1, 3 and 4. As a general rule, the corresponding installation and operating instructions for all safety-related parts of control systems are included along with the control or safety device.

2.2 Identification of Hazards

Different risks can be estimated for one and the same piece of machinery, depending on the function and operating mode considered. This means that the appropriate category for a safety-related part of a control system is dependent on the safety function in question. Accordingly, there is normally no standard category for all safety functions with respect to a piece of machinery. In order to define the necessary categories for the machinery control system, the various hazards for the machinery must be established on a systematic basis. Appendix A of EN 1050 [4] offers valuable assistance in identifying the hazards for a piece of machinery by listing 37 types of hazards, each of which has up to 10 hazardous events or situations. Table 1 (see page 19) represents a check list of the major hazards which are listed in Appendix A of EN 1050. Mechanical hazards and hazards due to failure / malfunction in particular can be caused by incorrect design of safety-related parts of control systems.

There are many methods which are described in literature on this subject for the purpose of establishing the correlation between hazards and the failure of safety and control devices, and we shall give a brief explanation of three of these methods in the paragraphs below.

In fault tree analysis [11], we start with a known hazard and look for all the causes which may lead to this hazard. The individual possible faults are combined by elemen-

---

[2] With effect from 1997, prEN 50100 has been published as prEN 61496. The number had to be amended because this standard is also published as IEC 61496.

tary logical decisions (NOT, OR and / or AND). A logical zero means "operative", whilst a logical one stands for "failed". The fault tree is continued until a component's failure mode is established. This so-called primary failure cannot be traced back any further and is used as a starting point for the fault tree. Figure 2 (see page 20) shows an example of a fault tree for the hazard to eyes caused by the laser light emitted by a laser scanner (electro-sensitive protective device [12]) used for personal detection purposes[3].

This example is taken from the BIA's range of experience in the field of testing and its description is backed up by [11]. The entire method is described in detail in this standard and information on quantitative fault tree analysis is also provided in Part 2 of the standard. This method is frequently applied on a qualitative basis up to sub-assembly level.

In complete contrast to fault tree analysis, event tree analysis [13] seeks out those hazards which result from a specific cause. The hazards in question in this case are the result of the event tree analysis, whilst the primary events constitute the starting point for the event tree analysis. Figure 3 (see page 21) shows an event tree diagram for the failure of a position switch in upper dead centre in a paper cutting guillotine[4]. In principle, this method can also be quantified, however, it is usually performed on a qualitative basis for the purposes of hazard analysis.

[3] With a laser scanner, laser light is deflected into the plane of the protection field by a rotating mirror. In principle, it is possible that, during this operation, the laser beam may come into contact with the eyes of the person requiring protection. Eye protection can only be guaranteed by limiting the emission power to a corresponding degree and by ensuring a short eye exposure period by rotating the beam. The fault tree in Figure 2 is used to determine, on a systematic basis, whether individual component faults, amplitude or exposure period may have a critical effect on the safety of the eye.

[4] The safety functions for a paper cutting guillotine are described in detail in Appendix A. After each cutting operation, the blades and press crossheads reach the position in upper dead centre and remain there unless further cutting operations are initiated. This position must be notified to the control system for the paper cutting guillotine by means of a position switch, to ensure that unintentional movements of the blades and press crossheads do not occur. The user and, where applicable, a second operator are protected by a two-hand control device and a light grid, which operate independently of the position switch. There is a possible hazard if failure of the position switch renders the two-hand control device and the light grid inoperative simultaneously due to incorrect design of the control system. This is clarified quite succinctly by the event tree analysis in Figure 3.

Table 1:
Check list for machinery hazard analysis

Hazard	Event	Yes	No
mechanical	crushing		
	shearing / cutting		
	catching / drawing in		
	impact / puncture		
	friction		
	high pressure fluid injection		
	parts spinning		
	slipping / jerking / overturning		
electrical	direct contact		
	indirect contact		
	electrostatic phenomena		
	thermal / chemical reactions due to short-circuits / overloads		
thermal	burns / scalds		
	cold / heat in the environment		
noise	damage to hearing		
	stress / fatigue		
	interference with communication (warning signals)		
vibration	neurological and vascular disorders		
	circulation disorders		
	joint damage		
radiation	arcs		
	IR / UV radiation		
	lasers		
	electromagnetic radiation		
	high frequency magnetic fields (microwaves)		
	ionising radiation		
materials	by contact or inhalation		
	explosion / fire		
	biological / microbiological		
neglect of ergonomic principles	physiological strain		
	mental strain		
	abnormal behaviour (e.g.manipulation)		
failure / malfunction	failure of energy supply		
	component failure (failure of control system)		
	immunity		

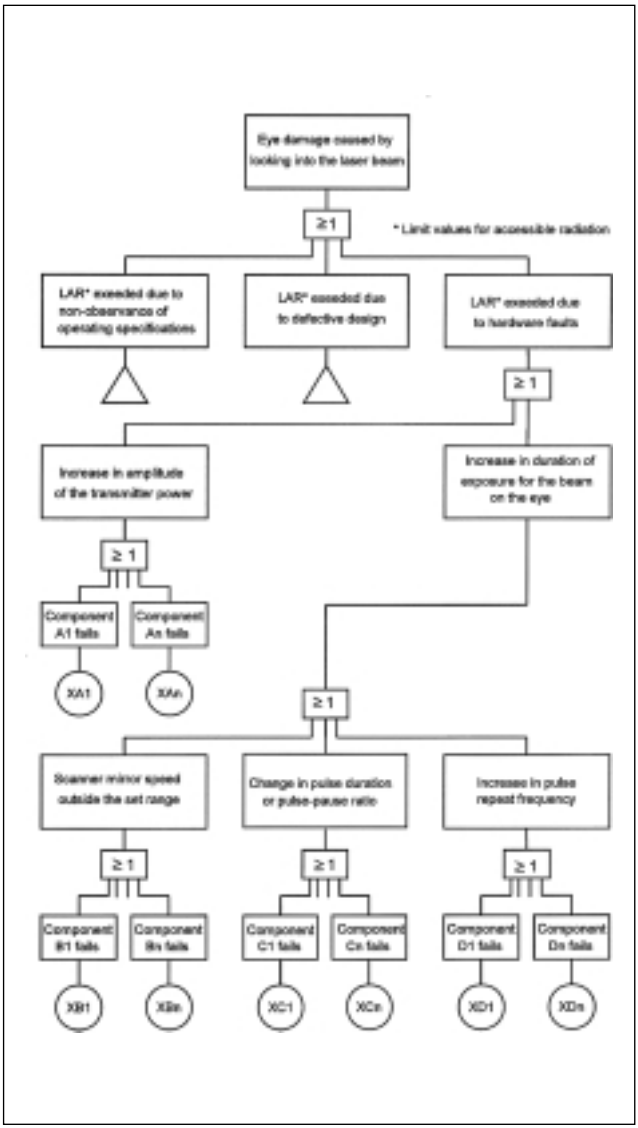


Figure 2:
Fault tree analysis for the hazard to eyes caused by laser light from a laser scanner

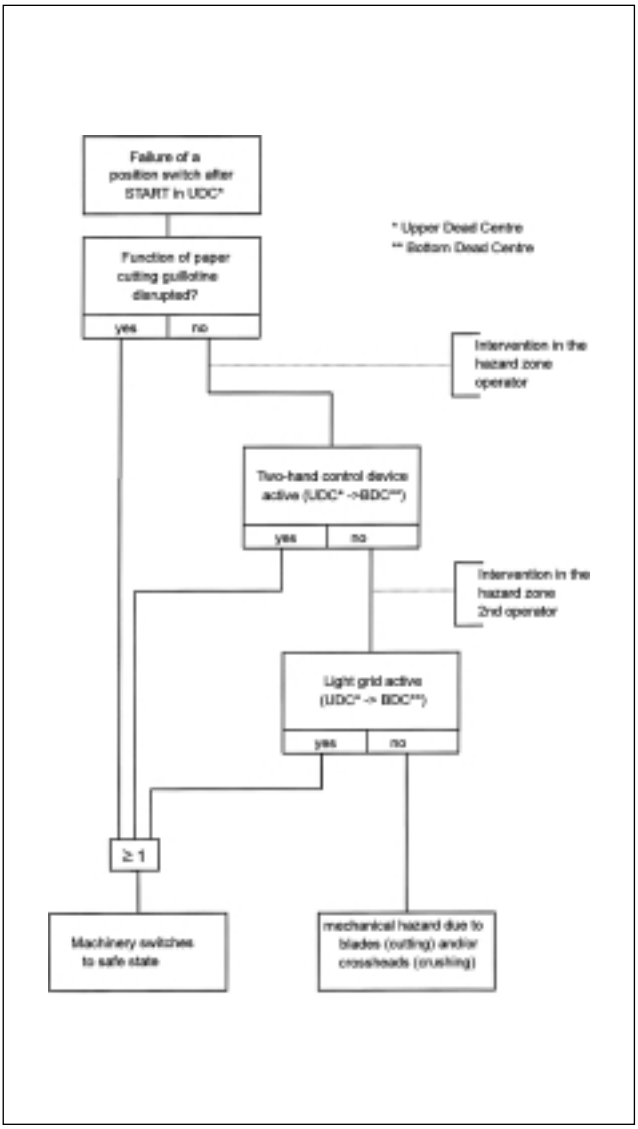


Figure 3:
Event tree analysis for the failure of a position switch in upper dead centre in a paper cutting guillotine

Failure mode and effects analysis [14] is a method used to examine the failure modes of all components in a system and their effects (effects on the safety-related parts of control systems). It starts with failures of individual components and analyses the possible hazards resulting from these failures. This method is often used to examine the effectiveness of specific measures taken within the control system. It forms the basis for the assessment of the categories defined in EN 954. By way of example, table 2 (see page 24) shows a failure mode and effects analysis form for various failure modes applicable to an integrated circuit in a light grid.

2.3 Risk Estimation and Description of Risk Parameters

2.3.1 The Concept of Risk

Once all the hazards for the safety-related parts of control systems in the machinery have been established, a risk analysis must be performed for each hazard. A few preliminary comments concerning the concept of risk should clarify the fundamental philosophy used in EN 1050.

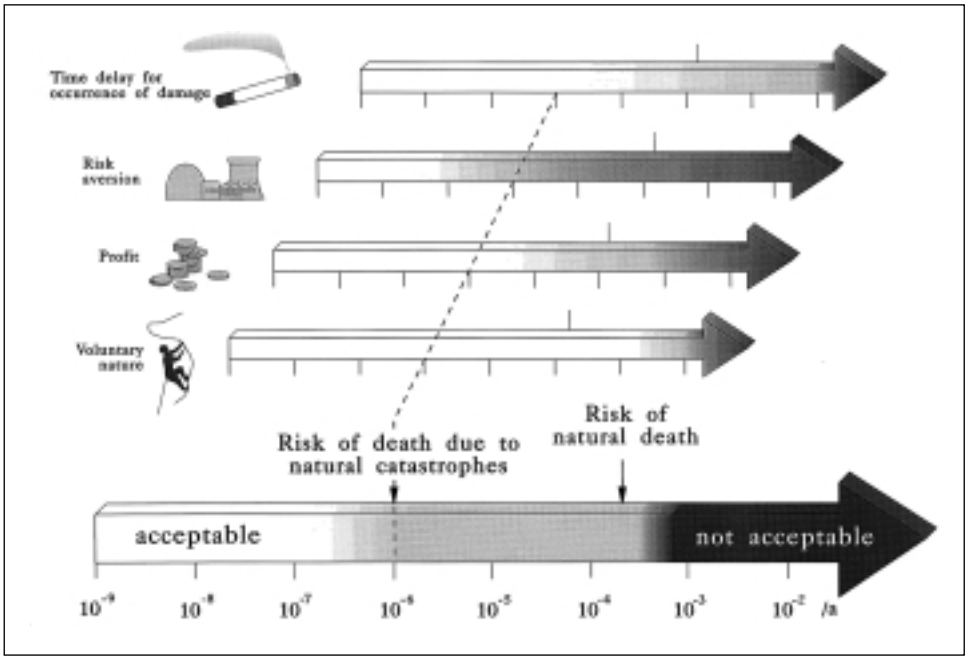
Annex 1 of the Machinery Directive specifies that risks of accidents must be ruled out for the foreseeable life-time of the machinery. As there is, in principle, no such thing as a zero risk[5] where technical installations are concerned, this requirement must be interpreted to mean that the remaining residual risks must be reduced to an extent which is generally acceptable. A risk is regarded as being acceptable in this light if it is generally accepted by the individuals in question after consideration of all aspects. The range of acceptable risks extends over about seven to eight decimal powers (Figure 4) [15]. A variety of factors influence risk acceptability, with the result that there may be huge differences in acceptability for risks which are comparable from an objective point of view but which have different origins or natures.

The most important factors and their influence on risk acceptability are shown in diagram form in Figure 4. The risks for death due to natural disasters (10^{-6}) per year and the lowest figure for the risk of death by natural causes (3×10^{-4}) are entered as clear reference points. The following are of crucial importance with respect to variable risk acceptability:

- whether a risk is taken voluntarily or is compulsory (difference of up to three decimal powers),

[5] A zero risk in this instance means the complete absence of any type of risk.

Figure 4:
Dependence of the acceptable risk on a variety of influences



- ❒ personal or business profit (up to four decimal powers for the same actual risk),
- ❒ aversion to potential catastrophic dangers (lower acceptability by about two to three decimal powers),
- ❒ discounting of risks which will have effects in the future (higher acceptability by one to two decimal powers).

It is often the case that the actual risk which is posed by a technical system and the risk which may be regarded as being acceptable for a system, are not only worlds apart in terms of figures. Both risks are also of a completely different nature: the actual risk can be established by experts and is for the most part defined by objective viewpoints. The acceptable risk is a convention reached

Table 2:
Example of failure mode and effects analysis on the transmitter in a light grid

Failure Mode and Effects Analysis								Page 1
System: light grid, Type 4, Component: Transmission element, integrated circuit U11, 4017								
Initial state:			Initial state:		Ambient conditions:			Documents:
Maintain safety function			two unobserved faults built in: First fault in U13 short-circuit pins 5-12 Second fault in U13 short-circuit pins 5-7		room temperature 20 to 30°C humidity < 80% dust-free atmosphere			circuit diagrams system specification
1	2	3	4	5	6	7		8
No.	Function element	Failure mode	Damage profile, possible causes	Failure detection	existing counter-measures	Effects of failure on the system and, where applicable, on its surroundings		Effect Comments
						Description	Document	
1.1	transmission beam selection	short-circuit pin 1-10	random fault	none, gap in protection field	emergency shut-down of machinery by user if fault observed in good time	gap in light curtain, due to irradiation, as two transmitters on	test report XXXX light grid	dangerous failure, finger protection no longer guaranteed, unobserved
1.2	transmission beam selection	short-circuit of all other pins with pins 1 or 10	random fault	output relays deenergize	none, as fault observed and safe state achieved	system switches over to safe state in the reaction time	test report XXXX light grid	fault observed, safe state achieved

Table 2
(continuation)

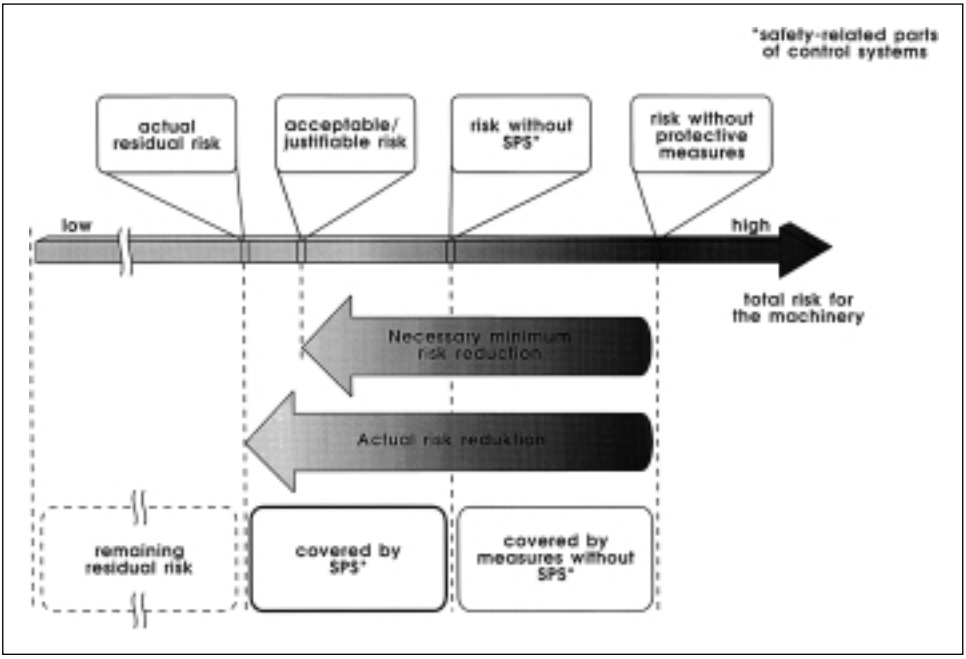
Failure Mode and Effects Analysis								Page 1
System: light grid, Type 4			Component: Transmission element, integrated circuit U11, 4017					
Initial state:			Initial state:		Ambient conditions:			Documents:
Maintain safety function			two unobserved faults built in: First fault in U13 short-circuit pins 5-12 Second fault in U13 short-circuit pins 5-7		room temperature 20 to 30˚C humidity < 80% dust-free atmosphere			circuit diagrams system specification
1.3	transmis-sion beam selection	short-circuit pin 5-12	random fault	none, gap in protec-tion field	emer-gency shut-down of machin-ery by user if fault observed in good time	gap in ligth cur-tain, due to irradia-tion, as two trans-mitters on	test report XXXX light grid	dangerous fail-ure, finger pro-tection no longer guaranteed, unobserved
1.4	transmis-sion beam selection	short-circuit of all other pins with pins 5 or 12	random fault	output relays deener-gize	none, as fault ob-served and safe state achieved	system switches over to safe state in the reaction time	test report XXXX light grid	fault observed, safe state achieved
1.5	transmis-sion beam selection	short-circuit of all other pins mutually	random fault	output relays deener-gize	none, as fault ob-served and safe state achieved	system switches over to safe state in the reaction time	test report XXXX light grid	fault observed, safe state achieved

by those responsible for social policy and, as such, it is not determined, but rather shaped by subjective and social viewpoints. The search for satisfactory safety solutions is first and foremost a question of bringing these two fundamentally different risk figures closer together. Thus, in the case of a specific application, a solution must be selected which leads to an actual risk which is smaller than or at most equal to the acceptable risk.

These preliminary comments are a straightforward explanation of the fundamental ideas behind EN 1050. The standard thus provides a method for determining the difference between the risk without safety measures and the acceptable risk, which is referred to in the standard as the "residual risk" (see figure 5).

To this end, the standard assumes that the risk which is associated with a specific technical

Figure 5:
The concept of acceptable risk



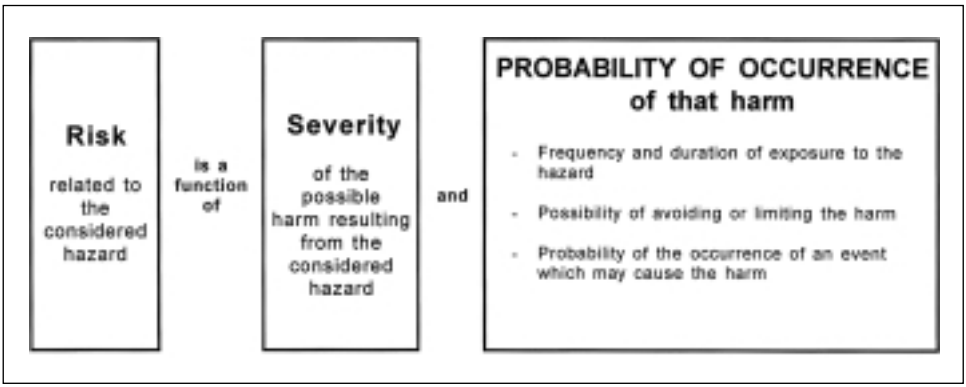
process or state can be described in outline by means of a probability statement, which takes account of the anticipated frequency of occurrence of an event leading to harm and the anticipated severity of the harm resulting from the occurrence of the event. Thus, the risk is defined by the two variables, "probability of occurrence of possible harm" (H) and "severity of the possible harm as a result of the considered hazard" (S). In the standard, these two elements are sub-divided into further elements and are split into separate stages in the Appendix to EN 954.

2.3.2 The Elements of Risk

Figure 6 explains the four elements of risk defined by standard EN 1050. The probability of occurrence of possible harm is characterised by three different elements of risk:

- ❒ the frequency and duration of exposure to the hazard (corresponds to exposure time "A" as defined in [6]),
- ❒ the probability of occurrence of a hazardous event (corresponds to the probability

Figure 6:
Elements of risk as defined in EN 1050



of occurrence of the undesirable event in the absence of a measurement and control safety device "W" as defined in [6]) and

- the possibility of avoiding or limiting the harm (corresponds to the possibility of avoiding the hazard "G" as defined in [6]).

Each element of risk from the above, all of which describe frequency, is sub-divided into several separate stages in the Appendix to EN 954.

When determining the risk, the frequency (or probability) of occurrence of a harmful event with a specified severity does not necessarily have to be quantified. The risk of the hazard in question can be characterised by means of qualitative statements with respect to the individual elements of risk. The risk which is inherent to the machinery can be established in this way. In this process, experimental values obtained from similar applications are used to a great extent when determining the elements of risk. A technical solution can be assessed after determining the elements of risk by comparing this solution with the solution for an application with the same elements of risk. Evaluation of elements of risk in this situation (see also Appendix A) is usually conducted differently for specific sectors[6], thus taking into account the variable nature of the acceptable residual risk.

Appendix A of this report explains how to establish the necessary risk reduction to achieve the acceptable risk by means of the elements of risk defined in EN 1050, making use of the risk graphs introduced in the informative Appendix B of EN 954-1 by way of example.

---

[6] Thus, for example, the frequency category "seldom to more often" is interpreted differently when talking about risks for machinery than in process control engineering.

3 Categories as defined in EN 954-1

3.1 General

The requirements for safety-related parts of control systems are specified by five categories in the context of EN 954-1 [4]. The categories represent a classification of the safety-related parts of a control system (STS) with respect to their ability to withstand faults and their behaviour in the event of faults, this being achieved on the basis of reliability and / or the structural architecture of the parts (table 3, see page 30). A greater ability to withstand faults signifies a higher possible risk reduction. For this reason, the categories are fundamentally suited to reducing the risk associated with a piece of machinery to an acceptable extent by means of measures at the level of the control system.

Category B is the basic category, the requirements of which must also be observed in the other categories. In categories B and 1, the ability to withstand faults is mainly achieved by the selection and use of appropriate components. If a fault occurs, the safety function may become inoperative. Category 1 has a greater ability to withstand faults than category B thanks to the use of special components which have been well-tried in safety applications.

In categories 2, 3 and 4, an improved performance with respect to the prescribed safety function is achieved, mainly as a result of structural measures. In category 2, execution of the safety function is checked at regular intervals (usually automatically by technical measures). However, the safety function may fail between the test phases if a fault occurs. By appropriate selection of the test intervals (e.g. once per shift), an appropriate risk reduction can be achieved when applying category 2. In categories 3 and 4, the occurrence of an individual fault cannot lead to the loss of the safety function. In category 4, and whenever reasonably practicable in category 3, such faults are detected automatically. Category 4 also offers the ability to withstand an accumulation of unobserved faults.

When considering faults it is necessary to reach an agreement as to the component faults which are implied and the component faults which can be reasonably ruled out. Information concerning the faults to be considered is given in the following sections and also in Appendix B.

Systematic faults[7] are barely mentioned at all in EN 954-1. Only in categories 3 and 4, does the sentence “Common mode faults shall be taken into account“ point to a type of systematic faults, namely common mode

[7] Systematic faults can creep into the product at any time during the product‘s life cycle.

Table 3:
Requirements for the categories of safety-related parts of machinery control systems

Category	Requirements (in brief)	System Behaviour	Principle
B	Safety-related parts of control systems and / or their safety devices and their components must be designed, constructed, selected, assembled and combined in accordance with the relevant standards such that they can withstand the expected influence.	The occurrence of a fault can lead to the loss of the safety function.	mainly characterised by the selection of components
1	The requirements of B shall apply. Well-tried components and well-tried safety principles shall be used.	The occurrence of a fault can lead to the loss of the safety function, but the probability of occurrence is lower than in category B.	
2	The requirements of B and the use of well-tried safety principles shall apply. The safety function shall be checked at suitable intervals by the machinery control system.	The occurrence of a fault can lead to the loss of the safety function between the checks. The loss of the safety function is deteced by the check.	mainly characterised by the structure
3	The requirements of B and the use of well-tried saftey principles shall apply. Safety-related parts shall be designed such that: 1. a single fault in any of these parts does not lead to the loss of the safety function, and 2. the single fault is detected whenever reasonably practicable.	If the single fault occurs, the safety function is still maintained. Some, but not all faults are detected. Accumulation of undetected faults can lead to the loss of the safety function.	
4	The requirements of B and the use of well-tried safety principles shall apply. Safety-related parts shall be designed such that: 1. a single fault in any of these parts does not lead to the loss of the safety function, and 2. the single fault is detected during or prior to the next demand on the safety function, or, if this is not possible, an accumulation of faults should not as a result lead to the loss of the safety function.	If faults occur, the safety function is still maintained. Faults are detected in good time to prevent the loss of the safety function.	

faults[8]. In category 4, diversity and the use of special test methods are mentioned as examples of measures used to counter systematic faults when validating the category. In principle, it can be said that many of the basic and well-tried safety principles do, of course, have the effect of preventing systematic faults (see tables 4 and 6, pages 32 and 39).

3.2 Category Specifications

3.2.1 Category B

Safety-related parts of control systems must be designed, constructed, selected, assembled and combined in accordance with the relevant standards and using the basic safety principles for the specific application, such that they are able to withstand:

- the anticipated operating stresses (e.g. reliability with respect to breaking capacity and frequency)
- the influence of the material used in the operating process (e.g. cleaning agents in a washing machine)
- other relevant external influences (e.g. mechanical vibrations, external electromagnetic fields, interruptions or disruptions to the energy supply).

These general principles are illustrated in general terms and with reference to specific technologies in the basic safety principles specified in table 4. In this table, the general basic safety principles apply in full for all technologies, whilst the technology-specific principles are also necessary for the relevant technologies. As category B represents a basic category for each of the other categories (see table 3), the basic safety principles should be applied as a general rule to the design of safety-related parts of control systems (STS) and / or safety devices.

No further specific safety-related measures are necessary for the components which comply with category B[9].

3.2.2 Category 1

In addition to the basic safety principles, safety-related parts in category 1 must be designed and constructed by using components and principles which are well-tried with respect to safety.

---

[8] Common mode faults are those faults which cause a multi-channel system to fail.

[9] If a component failure occurs, it may lead to the loss of the safety function.

Table 4:
Basic safety principles for the design of safety-related parts of control systems, Part 1

Principle	Description	Significant Criteria
General		
Ensure adequate dimensioning for all components	All components are selected such that they can withstand the anticipated operating stresses.	❒ breaking capacity, breaking frequency ❒ withstand voltage-strength ❒ pressure level, dynamic pressure behaviour, volume flow ❒ temperature and viscosity of pressure fluid ❒ type and condition of pressure fluid or compressed air
Resistance to relevant external influences	Safety-related parts of control systems (STS) are designed such that they can fulfil their function even in the event of the external influences which are usual for the application in question.	❒ mechanical effects (shock, vibration) ❒ climatic effects (temperature, humidity) ❒ leak-tightness of the housing (protection provided by enclosure) ❒ electromagnetic compatibility (fields, conducted disturbances)
closed circuit principle (positive signalling to start)	The safety-related switching position of the STS is achieved by removing the control signal (electrical voltage, pressure), i.e. by switching off the energy supply.	❒ safe state in the event of an interruption ❒ valves with working springs in the field of fluid technology
Control of fluctuations in the energy supply, failure and recovery of the energy supply	In the event of fluctuations in the energy supply (voltage or pressure), the STS should not initiate any unexpected reactions.	❒ faults in the power supply ❒ changes in pressure, pressure loss
Compliance with the applicable technical regulations	The applicable technical regulations associated with the application should be observed	❒ completeness ❒ accuracy
Quality assurance measures during production	General quality assurance measures, e.g. as defined in EN 45000, guarantee constant product quality for the STS.	❒ reproducibility during production
Comprehensible and complete installation, commissioning, operating and maintenance instructions	Well-structured instructions which are generally comprehensible are available for the installation, commissioning, operation and maintenance of STS.	❒ completeness ❒ comprehensibility ❒ accuracy
Formalization of modification procedure	All modifications to STS should be documented and the effects on the parts of the STS which have not been modified should be recorded. The modified STS will only be released following successful acceptance.	❒ accuracy of modifications ❒ no effect on parts which have not been modified

Table 4:
Basic safety principles for the design of safety-related parts of control systems, Part 2

Principle	Description	Significant Criteria
Fluid Technology		
Pressure control in the system	One or more pressure control valves usually prevent the pressure in a system or in parts of systems from rising beyond a specified level. Pressure control valves with secondary venting are used primarily for this purpose in pneumatic systems.	❒ check dimensioning ❒ position in the system (number) ❒ design
Filtration of the pressure medium (hydraulic fluid, compressed air)	The necessary purity class of the pressure medium during operation as specified by the manufacturer with reference to the components used is achieved by the use of a suitable device (usually a filter) after taking account of the application in question. Adequate drainage of the compressed air is also necessary for this to be achieved in the pneumatics sector.	❒ check dimensioning ❒ type of hydraulic fluid / compressed air state ❒ component manufacturers' requirements ❒ ambient conditions and conditions of usage ❒ position in the fluid technology system
Prevention of dirt intake	In open hydraulic systems, one particular way of preventing contamination from penetrating the fluid technology system is by using an active vent filter. In pneumatic systems, exhaust air filters (filter-silencer combinations) are used for this purpose (negative pressure).	❒ check dimensioning ❒ component manufactures' requirements ❒ ambient conditions and conditions of usage ❒ exhaust air discharge direction
Disconnection from the energy supply (if the energy supply is not required for the safety function, e.g. clamping devices)	Disconnection from the energy supply and discharge of the residual energy (if necessary) is facilitated by suitable main control devices (e.g. isolating valves).	❒ reliable disconnection / safe discharge (also in the case of storages) ❒ switch position and operating state should be recognisable

Table 4:
Basic safety principles for the design of safety-related parts of control systems, Part 3

Principle Description		
Computing		
Simple functional tests	Safety functions must be checked.	❒ normal functional and operating sequences ❒ tests should be representative
Transmission protocols with timed sequence monitoring for data transmission via buses	When transmitting usable data, compliance with a communication specification (e.g. parity bit) is monitored.	❒ accuracy of data communication
Timed monitoring via Watch-Dog	A timing element is periodically reset by the program. If the program no longer reacts after being reset, the STS is switched to a defined state by the timing element.	❒ monitoring program sequence
Technical modification protection (ROM, EPROM)	Modifications to the safety-related software by unauthorized persons are prevented by technical measures.	❒ no modifications by unauthorized persons
Minimisation of real-time effects	Real-time effects on the program make analysis more difficult and may cause certain properties of a program to become erratic. There should, therefore, be as few interrupts and multi-tasking areas as possible. Cyclic detection of process states should take place in a fixed sequence. Rules for approving interrupts should be drawn up.	❒ software should be able to be analysed ❒ software should be easy to modify
Structured programming	Control sequence flow in programs and data flow in these programs are designed to be transparent thanks to this method. This thus avoids non-systematic, complex and awkward program structures.	❒ case of testing, comprehensibility ❒ adaptability ❒ case of maintenance ❒ portability

A component which is well-tried with respect to safety for a safety-related application is a component which

- ❒ has been widely and successfully used in the past with successful results in similar applications or
- ❒ has been manufactured and verified by applying principles which demonstrate its suitability and reliability for safety-related applications.

Table 5 provides an overview of known components which are well-tried with respect to safety in the field of electrical engineering and components from the fluid technology sector which may be components which are well-tried with respect to safety.

Requirements with respect to the design and construction of valves which are well-tried with respect to safety and requirements concerning the condition of the pressure medium involved have not yet been specified. For this reason, only valve manufacturers and / or users are usually in a position to nominate valves which are well-tried with respect to safety for defined applications on the basis of their practical experience. A valve which is well-tried with respect to safety is, in particular, a valve with a sufficiently high level of safety-related reliability in practical conditions. This reliability relates solely to switching function into the safety-related position. A valve of this type must fulfil the component-specific basic and well-tried safety principles in Tables 4 and 6. Filtration for a valve which is well-tried with respect to safety must be performed specifically. In the case of a low risk combined with simple installations, the system filter which is always present in the installation may be sufficient for the necessary filtration operation. In the case of a higher risk and in complex installations, filtration should be performed immediately in front of the relevant valve and / or the relevant valves by means of a full-flow pressure filter (referred to as DF in the examples in Chapter 4). The filter's contamination level should be monitored. In pneumatic installations, a full-flow pressure filter may also be necessary immediately in front of the relevant valves in the case of larger pipework systems, several users and in the case of valves which require a higher filtration grade than other components in the installation.

In order to protect the valve as much as possible from contamination in the pressure medium from the cylinder side, specific measures are necessary with respect to the piston rod in the hydraulic / pneumatic cylinders (e.g. working wiper rings). In pneumatic control systems, it should also be noted that contamination can be drawn into the system via exhaust air apertures. For this reason, exhaust air (vent) apertures (e.g. on valves)

should be fitted with working filters, so-called filter-silencer combinations.

In the fields of electronics and computing, there are also no known components which are well-tried with respect to safety at the present time. As explained in [17], the method which is described in detail below to establish whether components are well-tried in operation, is used to prove that the components used, e.g. including software, are sufficiently free of systematic design faults. However, being well-tried in operation does not yet in itself enable a hardware module to be classified as a well-tried component, as, quite apart from systematic faults, the random error rate for a component must also be very low [16][10]. If a component is well-tried in operation, this tells us that no faults, or only insignificant faults, were established when using a considered unit, whereby this unit has been operated for the most part without any modifications over an adequate period of time in numerous different applications [17]. According to [17], a component is said to be well-tried in operation if, for an unaltered specification, the following conditions apply:

- ❒ 10 systems in different applications and
- ❒ 10^4 operating hours and
- ❒ at least one year of operation and
- ❒ no faults or no safety-related faults have been observed.
- ❒ There must be a statistical confidence level of 95%.

Proof must be provided by way of documentation from the manufacturer or user. The documentation must include the following at the very least: a precise description of the system and its components including the versions of the hardware and software used, the user and the usage period, operating hours, a method for selecting the systems and application cases used to provide this proof and a method to detect faults and to record and eliminate faults [17]. This is a particularly useful way of proving that software or complex electronic systems are well-tried in operation with respect to systematic faults. A correspondingly higher number of operating hours is required for higher categories [16].

Certain faults which are used for assessment purposes can also be ruled out for some well-tried components, because the fault rate for

[10] IEC Draft 1508 classifies the specified aims of a safety-related system in category 1 with a failure probability of 10^{-1} to 10^{-2} per demand for systems with a low demand rate and a probability of one dangerous failure per year of 10^{-1} to 10^{-2} for safety-related systems with a continuous or high demand rate. This probability limit is lower by one decimal power in each case for categories 3 and 4.

this failure mode is known to be very low (e.g. switches not opening when forcibly opened in category 3). Fault exclusions of this type are described for specific technologies in the fault lists in Appendix B to this Report.

The decision as to whether to accept a specific component as being well-tried with respect to safety is dependent on the application in question.

The following are examples of well-tried safety principles:

- ❒ avoiding specific faults (e.g. avoiding short-circuits by separation)
- ❒ reducing the probability of faults (e.g. by overdimensioning) or stress on the components below the design limit
- ❒ specifying the failure direction for a fault
- ❒ fault detection in good time (e.g. detecting earthing)
- ❒ limiting the consequences of a fault.

Table 6 illustrates currently known well-tried safety principles of a general and technology-specific nature. Some of these principles are very general and are in some cases used depending on the category in question. The principle of automatic monitoring exists as a well-tried principle in categories 3 and 4, for example, whilst touch operation, which is limited by time or distance, represents a principle which is dependent on the application in question. On the other hand, the principle of a "control system with self-locking" can be used for all categories on a very general basis. These reflections make it quite clear that, unlike the basic safety principles, well-tried principles cannot all be applied in all circumstances, but are specific to each technology, application or category.

In general terms, it can be said that there is a lower probability of a dangerous failure in category 1 than in category B. It follows that the loss of the safety function is less likely[11].

At present, there are no specified well-tried safety principles in the field of fluid technology. These safety principles relate to both the components and the pressure medium. Part 3 of Table 6 lists the major well-tried safety principles for fluid technology, which in our opinion, although, depending on the application in question cannot all be achieved at the same time.

[11] The occurrence of a fault can lead to the loss of the safety function.

Table 5:
Components which are well-tried with respect to safety for the design of safety-related parts of control systems

Components which are well-tried with respect to Safety	Aim / Function
Electrical Engineering	
Fuse / automatic switch	Cut-off in the event of a short-circuit or earthing
Mechanical position switch with personal protection function with forcibly actuated normally closed contact EN 60947-5-1, chapter 3	Control voltage interrupted when actuated
Positive locking (see EN 1088)	Preventing dangerous access
Forcibly actuated camshaft switch	Actuation of switching contacts
Control circuit contactors[5] as per EN 60947-4-1 Power contactors [5]	Release when de-energized
Emergency Stop keys / cable control switch with forcibly actuated normally closed contact (EN 60947-5-1, chapter 3)	Control voltage interrupted when actuated
Wiring, installation in control cabinet Light plastic sheathed cable, protected installation in machinery frame	Avoid short circuit of wires
Touch controls	Control voltage interrupted when released
Mechanically actuated compliance switch (see EN 292)	
Terminals in switching cabinet / terminal box in the machinery (with adequate protection system)	Avoid crosses (short circuits)
Fluid Technology [6]	
Directional control valves with discrete switching positions (slide and seat valves)	Safety-related switching position is taken up by means of durable, working springs and the control energy is interrupted
Continuous directional control valves	
Stop valves (non-return valves, controlled non-return valves)	Preventing the flow in the closed direction
Flow control valves (throttles and restrictors) as a fixed resistance in fluid engineering systems	Retention of the set volume flow
Pressure valves in the safety-related part of the control system	Proposed function in the event of pressure values being exceeded or not attained
Pressure switches, pressure sensors	
Mechanically positively actuated valves (forcibly actuated) Manual lever valves with spring return or spring centring	Interruption of volume flow or control signal
Pipework in the safety-related part of the control system and to consumer	Leak-tightness, breaking strength

[5] Whilst there is no doubt that control and power contactors do not respond if the control voltage is absent (fault exclusion), there is some controversy as to whether these contactors should be regarded as "well-tried components" with respect to the way in which they are released when de-energized. In the author`s opinion, no fault exclusion can in fact be made for these switching devices, but it is possible and justifiable to classify them as "well-tried components". Otherwise, contrary to many years of practical experience, a position monitoring device for a movable safety guard with only one power contactor for switching off the potentially hazardous movement would have to be classified under category B.

[6] This details components which may be components which are well-tried with respect to safety, as the current situation in the field of fluid technology is such that it is only possible to specify components which are well-tried with respect to safety in specific individual cases.

Table 6:
Well-tried safety principles for the design of safety-related parts of control systems, Part 1

Principle	Description	Aim
General		
Control system with self-lock	This type of control system goes into a self-locking state after a brief command, e.g. by touch controls and retains this state for as long as the control energy is provided (voltage, pressure).	Protection ❒ against unexpected restarting ❒ after energy failure and return
Separation / insulation	Adequate leakage distances and air gaps are ensured, and suitable insulating materials and thicknesses are used.	To avoid short-circuits
Earthing control circuits	A one-sided connection is made between control circuits and the equipment earth (see EN 60204-1, Section 9.1.4).	Fault detection in the event of earthing
Torque / power limiting (reduced pressure)	Forces which may lead to a hazard are limited by electrical, mechanical or fluid technology devices.	Risk reduction by improved hazard protection
Limited distance touch operation	The distance of a movement is limited to an admissible value in touch operation.	
Limited time touch operation	The time taken by a movement is limited to an admissible value in touch operation.	
Reduced frequency / speed (reduced volume flow)	The frequency or speed of a movement is limited to an admissible value in touch operation.	
Overdimensioning (underloading)	All equipment is loaded to less than the nominal value.	Reduction of the failure probability
Start-up testing	The protection function is compulsorily checked before initiating a potentially hazardous movement.	Fault detection before initiation
Self-actuated / automatic monitoring	Faults in components are detected in good time by monitoring.	Pick up faults in good time
Hardware diversity	Different types and designs of technical devices are installed.	Avoid common mode faults
Use of standard circuits	Standard circuits are circuits for special applications, which have been checked to determine their behaviour in the event of faults and which have been well-tried in practice.	Safety function by means of well-tried or tested devices

Table 6:
Well-tried safety principles for the design of safety-related parts of control systems, Part 2

Principle	Description	Aim
Use of type-tested modules (e.g. control devices)	Type-tested modules are factory-built devices which fulfil particular validated requirements.	
Normally closed / normally open contact combination	This is concerned with the arrangement of two mechanical position switches in a safety device with fundamentally different actuation modes. One switch is always actuated and the other is not actuated whatever the position of the safety device.	❒ Maintain the safety function of mechanical position switches in the event of individual faults in the mechanism ❒ Detection if the safety device is removed
Electromechanical engineering		
Connected movement of contacts	Connected movement implies a mechanical connection of contacts in contactors and relays which rules out the possibility of normally closed and normally open contacts closing simultaneously even in the event of a fault.	Monitoring control contactors
Interlocking	Several relays / contactors are connected in such a way that other components can no longer be actuated in the event of a fault in one component thanks to the connected movement system.	Prevention of undesirable states
Forcible / positive actuation	This is a reliable means of actuation by rigid, mechanical parts without non-positive and spring-actuated connections.	Safe actuation, e.g. for mechanical position switches
Electronics / Computing		
Dynamic techniques	All safety-related signals change their state on a regular basis, with the result that static faults automatically initiate a safety-oriented function.	Static component faults can be picked up and dealt with in good time
Separation of electrical energy transmission lines from information transmission lines	Resistance to interference is increased, especially with sensitive analog signals, by spatial separation.	No capacitive or inductive disturbances of signal transmissions by electrical energy transmissions

Table 6:
Well-tried Safety Principles for the Design of Safety-related Parts of Control Systems, Part 3

Principle	Description	Aim
Non-equivalent signal control	When processing redundant signals, one channel uses a logical l when the other uses a logical 0 and vice versa.	Increased resistance to interference with respect to common mode faults
Fault detection via the technical process	Faults are picked up by means of specific expected events which are prescribed by the technical process. It is not usually possible to pinpoint the fault in this method.	Early fault detection
Plausibility checks	Plausibility checks are used to achieve a defined reaction in the event of inadmissible or unusual inputs and states or those which are outside the specified values.	Defined reaction ❒ in the event of incorrect user specifications and ❒ in the event of component failures
Use of an external watchdog	A watchdog is a timed program run monitoring system in which an external component expects signals from the microcomputer at regular time intervals. If these signals are not received, the watchdog is required to initiate a safety-oriented reaction by means of a second independent cut-off path.	Defined reaction in the event of defective program sequence
Fluid Technology		
Positive overlap	There must be an adequate positive overlap for contacts to be closed when using slide valves.	to stop potentially hazardous movements to prevent unintentional starting up
Positive dynamic effect	The actuating forces have a direct effect (forcible) on the moving parts, i.e. without frictional connections.	Reliable actuation of moving parts
Specific selection of materials and material pairing	This selection takes place by considering the properties of the hydraulic fluid on the basis of corresponding experience and / or specific tests.	Reduction of failure probabilities
Definition of operating data	The principal variables which are defined are the operating temperature range and the operating viscosity range for the hydraulic fluid.	
Monitoring the hydraulic fluid	The state of the hydraulic fluid is monitored on a regular basis, e.g. by sampling.	

3.2.3 Category 2

The requirements of category B must be fulfilled. Well-tried safety principles must also be used. In addition, in category 2, the safety-related parts of the control system must compulsorily be tested by the machinery control system at suitable time intervals (see table 3). Testing the safety function must take place:

- ❒ when the machinery is started up and before a hazardous state is initiated
- ❒ periodically during operation, if risk analysis and the operating mode indicate that this is necessary.

This test can be initiated automatically or manually. However, a positive test result is a prerequisite for starting up or continuing to operate the machinery. Each safety function test must either approve operation, if no faults have been detected, or, if faults are detected, it must generate an output signal to enable appropriate control system measures to be initiated[12]. The test itself should not lead to a hazardous state. Once a fault has been detected, a safe state must be maintained until the fault has been rectified. The testing device may be a separate device or may be part of the safety-related part of the control system which executes the safety function.

In some cases, category 2 is not applicable, as it is not possible to test the safety functions of all components, e.g. pressure switches or temperature sensors. In general terms, category 2 can be achieved with electronic techniques, e.g. in safety devices or specific control systems[13]. However, in this case it must be possible to guarantee that the testing device and the STS cannot fail at the same time as a result of a single fault as listed in Appendix B (e.g. in that they are not implemented in a single programmable logic controller).

---

[12] In the latest version of the standard, this requirement is reduced in that it now states: „If it is not possible to initiate a safe state, e.g. welding the contact for the limit switch, the output signal must provide a warning of the hazard.“ To date, category 2 has been defined more stringently within the BIA and a second independent cut-off method was required. The additional requirement to maintain a safe state until the fault is rectified can only be fulfilled by means of the second independent cut-off method. This inconsistency must, in our opinion, be ironed out by the standard maker before the second independent cut-off method can be replaced by a warning.

[13] This system behaviour accepts that:
– the occurrence of a fault leads to the loss of the safety function between tests,
– the loss of the safety function is usually detected in good time by testing.

3.2.4 Category 3

The requirements of category B must be fulfilled. Well-tried safety principles must also be used. In addition, the safety-related parts in category 3 must be designed such that a single fault in one of these parts as defined by the fault list in Appendix B does not lead to the loss of the safety function (see table 3). Common mode faults must be taken into account if the probability of a fault occurring is high. The individual fault must be detected during or before the next demand on the safety function whenever reasonably practicable.

The requirement that individual faults should be detected does not mean that all faults are detected. zThis is why, in the case of certain types of machinery, an accumulation of unobserved faults can, in certain circumstances, lead to an unintentional output signal and to the machinery entering into a hazardous state. zTypical examples of practicable measures for fault detection purposes are scanning the relay contacts with connected movement or monitoring redundant electrical outputs. If necessary as a result of the technology and application in question, the Type C standard maker should specify additional details with respect to fault detection. "Whenever reasonably practicable" means that the necessary measures for fault detection purposes and the extent to which these are incorporated, are chiefly dependent on the consequences of a failure and on the probability of occurrence of an accident within the application. The technology which is used influences the possibilities for incorporating fault detection[14].

3.2.5 Category 4

The requirements of category B must be fulfilled. Well-tried safety principles should also be used. In addition, safety-related parts of control systems in category 4 must be designed such that (see also table 3):

- a single fault (see Appendix B of this report) in any of these safety-related parts does not lead to the loss of the safety function and
- the individual fault is detected during or before the next demand on the safety function, e.g. immediately after switching on or at the end of a machine cycle. If this type of detection is not possible, an

[14] This system behaviour accepts that
– the safety function is always retained if a single fault occurs,
– some, but not all faults are detected,
– an accumulation of undetected faults may lead to the loss of the safety function.

accumulation of faults should not lead to the loss of the safety function[15].

If it is not even possible to detect certain faults due to the technology or circuit design in question during the next test, the occurrence of additional faults must be assumed. In this case, an accumulation of faults should not lead to the loss of the safety function. Fault review should be suspended if the probability of further faults occurring can be regarded as being sufficiently low[16].

---

[15] This system behaviour accepts that
– the safety function is always retained if faults occur,
– faults are detected in sufficient time to prevent the loss of the safety function.

[16] According to the experience acquired by the BIA, fault accumulation can be suspended after the third fault, irrespective of the technology in question.

Fault review can be restricted to two combined faults, if

- ❒ the components' fault rates are low and
- ❒ the combined faults mainly occur independently of each other and
- ❒ the safety function is only interrupted if the faults occur in a specific sequence.

If additional faults occur as a result of an initial individual fault, the initial fault and all resulting faults must be regarded as a single fault. Common mode faults must be taken into account, e.g. by applying diversity or special methods for detecting faults of this type.

In the case of complex circuit structures (e.g. microprocessors, complete redundant systems), fault review is generally performed at structural level, i.e. based on sub-assemblies.

4 Collection of Examples of Control Systems for the Individual Categories

This chapter is a collection of technical implementation examples classified according to the five categories. When describing the examples, basic safety principles are assumed to apply and as such are not listed individually (see Chapter 3).

Each sample circuit is explained by the following four sections:

- ❒ functional description,
- ❒ design features,
- ❒ application and
- ❒ further references.

In the "Functional Description" section, the major safety-related functions are described in brief on the basis of an outline circuit diagram. Behaviour in the event of a fault is discussed. Fault detection measures are mentioned.

The special features of the design of the relevant example are listed under the heading "Design Features". Safety principles and the use of well-tried components are specified here amongst other things.

The "Application" section looks at the possible risk reduction which can be achieved by the use of the category. A decision as to application must, in the end, be dependent on the application in question. For this reason, the comments in the examples should only be regarded as recommendations.

The fact that the examples are limited to no more than three pages makes it necessary to specify "Further References". As a rule, this section contains a publication which is associated with the example mentioned. This can be consulted in order to read about the function of the example in detail.

The examples do not represent a binding interpretation of the categories. However, these examples have been assembled by the authors on the basis of many years of experience with safety-related machinery control systems and collaboration in national and European standardization committees with a view to providing the designer with useful assistance in developing his own designs.

A few basic observations are given for each technology sector in the following technology-specific sections so as to make the examples more comprehensible and to translate these in terms of categories.

4.1 Basic Technology-specific Observations concerning the Control System Examples

4.1.1 Electromechanical Control Systems

The main types of components which are used in electromechanical control systems are switches and / or control stations (e.g.: position switches, selector switches, keys) and switchgear (control contactors, relays, power contactors). These devices have definite switching positions. As a rule, they do not alter their switching state without being actuated by external or electrical triggers. When they are used in accordance with the specifications and selected appropriately, they are largely insensitive to ambient influences, such as humidity, temperature and electrical and electromagnetic interference phenomena. In this respect they are to some extent very different to electronic equipment (see also Section 4.1.3). By appropriate selection, dimensioning and configuration, it is possible to have an impact on durability and failure behaviour. This also applies to the wires used when installed accordingly both inside and outside the electrical housings.

For the above reasons, electromechanical components comply in most cases with the "basic safety principles" and can even be regarded as "components which are well-tried with respect to safety" in many instances. However, this only applies if the requirements of EN 60204-1 [18] for electrical equipment for the machinery / plant have been taken into account. In some cases, faults can also be ruled out, e.g. as in the case of a control contactor responding in the absence of control voltage or non-opening of a forcibly actuated normally closed contact in a switch as per EN 60947-5-1, Section 3 [19], see also Appendix B.

As category B requires that the relevant standards be observed and important "principles which are well-tried with respect to safety" are specified in the basic standard [18] for safety-related electromechanical parts of control systems, category B is identical to category 1 for this technology. This is why no electromechanical control systems are shown for category B in the sample circuits in this report.

4.1.2 Control Systems in the Field of Fluid Technology

In the case of fluid technology systems, it is the valve area, in particular, which should be regarded as the "safety-related part of the control system", especially those valves which control potentially hazardous movements or states. In hydraulic systems (see Figure 7), the measures taken to limit the

pressure in the system (VDB) and to filter the hydraulic fluid (RF) should also be regarded in this light. The components, LF, N and T, shown in Figure 7 are present in most hydraulic systems and are particularly important with respect to the state of the hydraulic fluid and thus for the valve functions. The vent filter, LF, which is located on the fluid tank prevents external contamination from entering the system. The level display, N, ensures that the liquid level remains within the specified limits. The temperature display, T, symbolizes appropriate measures to limit the operating temperature range and thus the operating viscosity range for the hydraulic fluid. If necessary, devices for cooling and / or heating pur-

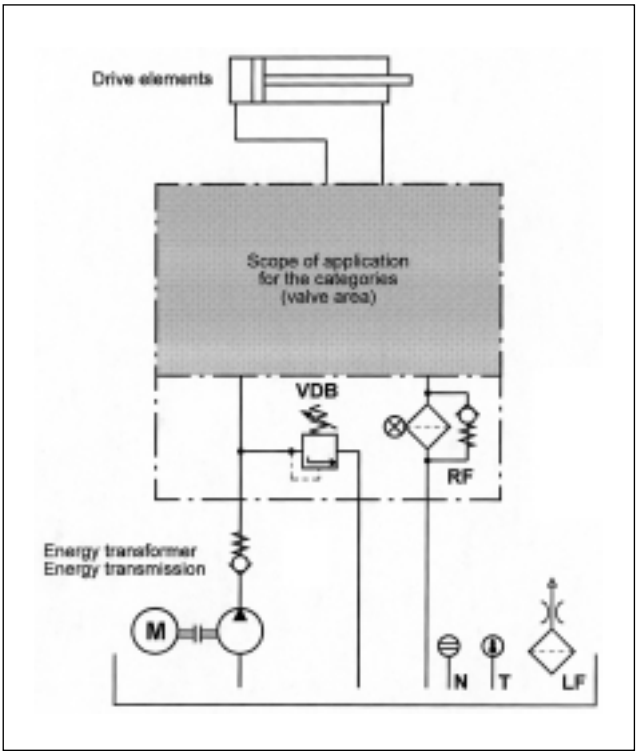


Figure 7:
Scope of application
for categories
in hydraulic systems

poses must be used in conjunction with a temperature control device (see also Table 6, Part 3 in this respect).

The drive elements and the energy transformation and energy transmission components are usually outside the scope of application of the categories in fluid technology systems.

In the case of pneumatic systems (see Figure 8), the components to prevent hazards in the event of energy fluctuations and the so-called maintenance unit for preparing the compressed air should be regarded in the same light, from a safety point of view, as the valve area. To enable possible energy fluctuations to be handled safely, a vent valve is often used in conjunction with a pressure switch. In the sample circuits in Section 4.2, these components are represented by the abbreviations EV (vent valve) and DS (pressure switch). The maintenance unit (see Figure 8) usually consists of a manual shut-off valve, HV, a filter with a water separator, FW, in which the filter's contamination level is monitored, and a pressure control valve, VDR, (with secondary venting with appropriate dimensions).

In addition to the safety-related part of the control system, the fluid technology circuits shown by way of example in Section 4.2 only include those additional components which are required in order to understand the fluid technology system or which have a direct bearing on the control system. All the requirements which must be fulfilled by fluid technology systems are specified in [20] and [21]. [22] to [25] are designated as additional applicable standards.

Most of the examples of control systems represent electrohydraulic or electropneumatic control systems. In these control systems, different safety requirements are executed by the electrical part of the control system, such as, for example, the requirements to control energy fluctuations in electrohydraulic control systems.

In all the control system examples, the required safety function is concerned with stopping a potentially hazardous movement or reversing the direction of movement. The concept of preventing unexpected starting up is implicitly included in this function.

Control systems in the field of fluid technology are usually designed in categories 1, 3 or 4, but the use of category 2 is also feasible. As category B already demands compliance with the relevant standards and the basic safety principles, fluid technology control systems in categories B and 1 cannot, for the most part, be distinguished by the design of the control system, but merely by the higher, safety-related reliability of the relevant valves. For this reason, no fluid

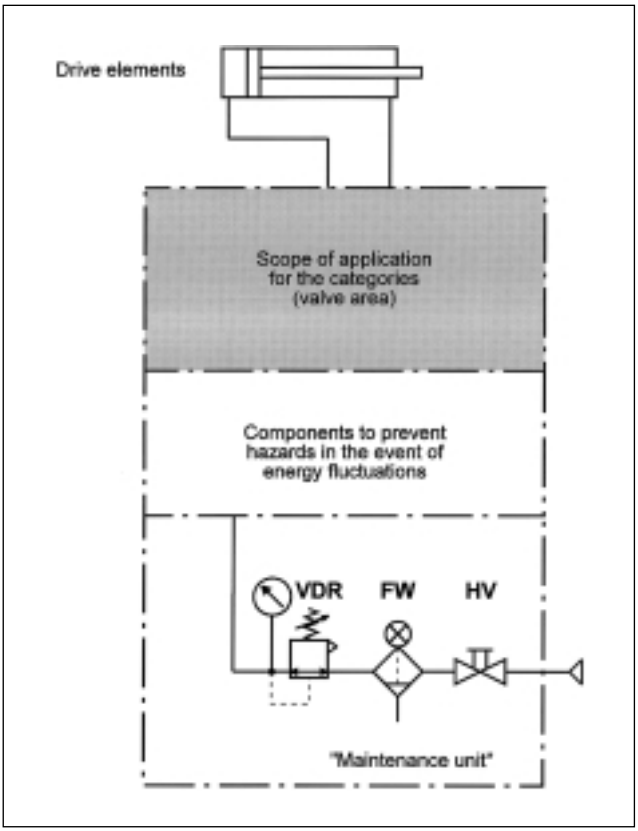


Figure 8:
Scope of application for categories in pneumatic systems

technology control systems from category B are shown in this report.

The term "pneumatic / hydraulic control systems" is used in the text below to mean only the safety-related parts of pneumatic / hydraulic control systems.

4.1.3 Electronic Control Systems

As a rule, electronic components are more sensitive to external ambient influences than electromechanical components. If no special measures are taken, the use of electronic components at temperatures below 0° C is

clearly subject to more restrictions than in the case of electromechanical components. There are also ambient influences which would have almost no significance when using electromechanical contact mechanisms, but which constitute a major problem in electronic systems. These include all electromagnetic interference phenomena, stray fields and the like, which are coupled into electronic systems via wires or via electromagnetic fields. Considerable measures need to be taken to protect against such influences in order to achieve an adequate level of resistance to interference for practical purposes.

There are hardly any possible fault exclusions for electronic components. This means that, in principle, the design of a specific component cannot guarantee safety, but that this can only be achieved by specific circuit designs and by the application of corresponding fault control measures. This is why there are no electronic systems in category 1.

Another point which is significant from a safety point of view is directly associated with the above comments: The failure behaviour of electronic components is usually more safety-critical than that of electromechanical components. Let us explain this by using an example: If a contactor is not triggered by electrical means, i.e. if the current does not pass through its coil, there is no reason why the contactor's contacts should close. This means that a relay or contactor which is disconnected does not cut in again of its own accord as a result of an internal fault. The situation is quite different in the case of most electronic components, e.g. a transistor. If a transistor is blocked, i.e. the base current is not high enough, we can still not rule out the possibility of the transistor suddenly becoming conductive without any external action as a result of an internal fault and thus initiating a hazardous movement under certain circumstances. An appropriate circuit design concept must also be used in order to overcome this safety disadvantage of electronic components.

In some cases, particularly when using large-scale integrated modules, it is no longer possible to establish, at the start of usage, i.e. when the system is handed over to the client, that the system is completely fault-free. Even at component level, this can no longer be proved 100% in certain circumstances, even by the manufacturers of the integrated circuits. This is where the error avoidance measures described in more recent draft standards [16] come in, whereby these, if they are performed in accordance with the control system category, are sufficient to guarantee the required safety at the start of usage in accordance with the current technical regulations.

4.1.4 Computer Control Systems

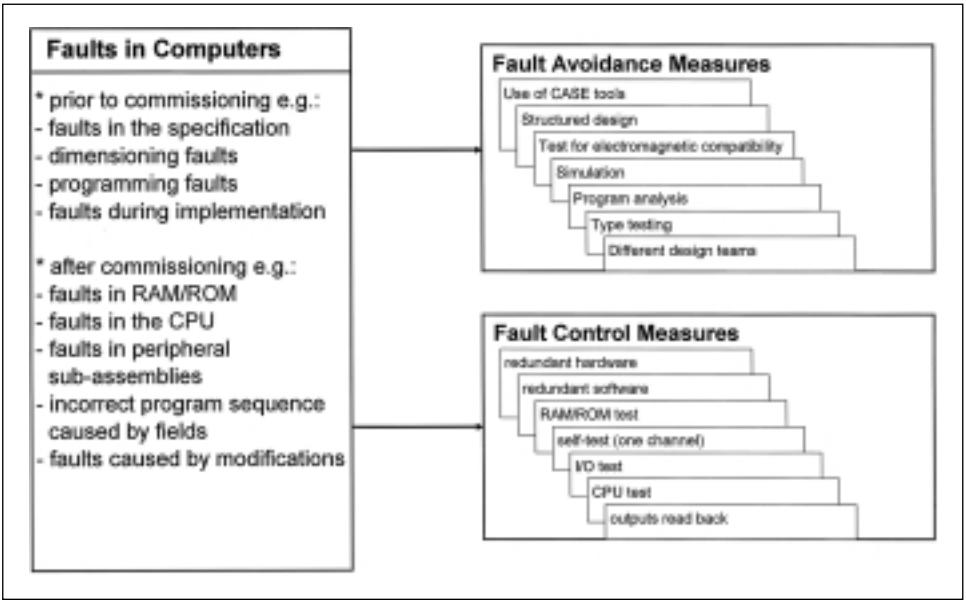
If we analyse the fault behaviour of microprocessor-controlled safety devices, we can see that random component failures are often not the cause of failure, but that this is rather caused by particular conditions during operation, which the programmer has not taken into account. Side effects of program modifications during system maintenance which are not immediately obvious represent a further source of faults. It follows on from these remarks that faults may exist, particularly in microprocessor-controlled machinery, whereby these faults were created when the system was designed, but may only lead to a hazardous situation during operation. Measures to counteract such faults must therefore be incorporated right back in the design process for the safety device. The Prestandard on Computer Safety [17] and Draft Standard IEC 1508 [16] take up this very point in distinguishing between fault avoidance and fault control measures (see Figure 9, page 52). Fault avoidance measures are taken by the manufacturer and testing body during the concept phase, and the development, installation and modification process, so as to avoid making specific faults completely or so as to reveal and correct these during the process. Fault control measures are hardware and software modules which are mainly responsible for detecting faults which occur during operation and for initiating safety-oriented reactions by the computer system.

The individual measures listed in [17] for the purpose of fault control and fault avoidance are assessed with respect to their effectiveness. A table sets out the level of effectiveness which is required for the possible faults and the relevant requirement classes in accordance with [6] (see table 7, page 53).

The lists of measures specified in [17] for the individual requirement classes show the correlation between the safety levels in the Prestandard for Computer Safety, the so-called "Safety Integrity Levels" standardized in [16] and the categories mentioned in [5], as illustrated in table 8, page 54. The descriptions listed in table 8 under the column entitled "Brief description" are given in many older national and international standards for machinery. With the aid of table 8, a requirement with regard to the level of effectiveness of the measures to be taken can be classified for each of the categories as compared with the described fault types in microprocessor-controlled systems with the aid of Table 7. The effectiveness of the different individual measures for computer systems is described in the Appendices to [16] and [17].

Random faults in computer-controlled safety-related control systems can to a great extent

Figure 9:
Fault avoidance and fault control measures



be controlled by the structure of the circuit as a whole. Thus, for example, a two-channel structure means that the safety device can still function safely even in the event of an undetected fault in one channel. These so-called system measures [17] or architectures help to allow faults to be tolerated. However, if it is deemed desirable to pick up faults in the individual computer components in good time, measures beneath system level will need to be taken. Examples of such measures include tests on the individual commands from the central processing unit or algorithms which provide information about program changes in the read-only memory. The measures to be taken at both system level and below system level are defined by the required category.

Fault control measures cannot, for example, prevent program faults which have been made in the software of both computer sys-

Table 7:
Effectiveness of measures with respect to faults as a function of the requirement class as defined in [17]

Failure caused by:		Safety-related Measures in accordance with Requirement Classes							
		1	2	3	4	5	6	7	8
Random faults in hardware	Single fault	fault control measures							
		low	medium			high			
		Effectiveness must be achieved by a combination of measures at system level and / or below system level							
	Multiple faults as a result of fault accumulation	fault control measures							
					low	medium		high	
		Effectiveness must be achieved by a combination of measures at system level and / or below system level and / or by non-technical measures							
Systematic faults with common mode faults	in hardware	fault avoidance measures							
		Basic measures			low	medium		high	
		fault control measures							
						low		high	
	in software	fault avoidance measures							
		Basic measures			low	medium		high	
		fault control measures							
					low	medium		high	
Handling faults, operation faults, manipulation		fault avoidance measures							
		Basic measures			low			high	
		fault control measures							
		Basic measures			low			high	
Faults due to operating and ambient influences		fault avoidance measures							
		Basic measures	low			medium		high	
		fault control measures							
		Basic measures				low		high	

Legend: low / medium / high = description of the effectiveness of the measures

Table 8:
Correlation between category, requirement classes and safety integritiy levels

Category as per [5]	Requirement Class as per [6]	Safety Integrity Level as per [16]	Brief Description
B	1	–	state of the art control systems
2	2 / 3	1	testing
3	4	2	single fault safety with partial fault detection
4	5 / 6	3	self-monitoring
–	7 / 8	4	not significant in machinery protection

tems and which therefore affect both parts of the system at the same time, from being able to cause a hazard. This is why there is also a series of fault avoidance measures which must be taken during the development process in addition to the fault control measures.

By way of example, Figures 10 and 11 (see page 55 and 56) are lists comprising a series of fault avoidance measures for categories B to 4. All of these measures should be taken for category 4, whilst, for category 3 requirements, all of the measures are significant with the exception of those which are required for category 4. This leaves only those fault avoidance measures which are required from category 2 upwards for categories 2 and 1. There are only a few fault avoidance measures to be taken for category B. These correspond to the basic safety principles as defined in EN 954.

4.2 Examples of Non-technology-specific Implementation of the Individual Categories

The following examples of circuits show the way in which the categories are realized with the relevant technologies. Both the development of safety-related parts of control systems and validation of such parts can be performed on this basis.

The following examples result from the BIA's many years of experience in developing and testing safety-related machinery control systems, without going into manufacturer-specific implementation proposals. Some of these examples have already been made available to the general public in a variety of publications, but this is the first time that they have been combined together for the purpose of translating the categories

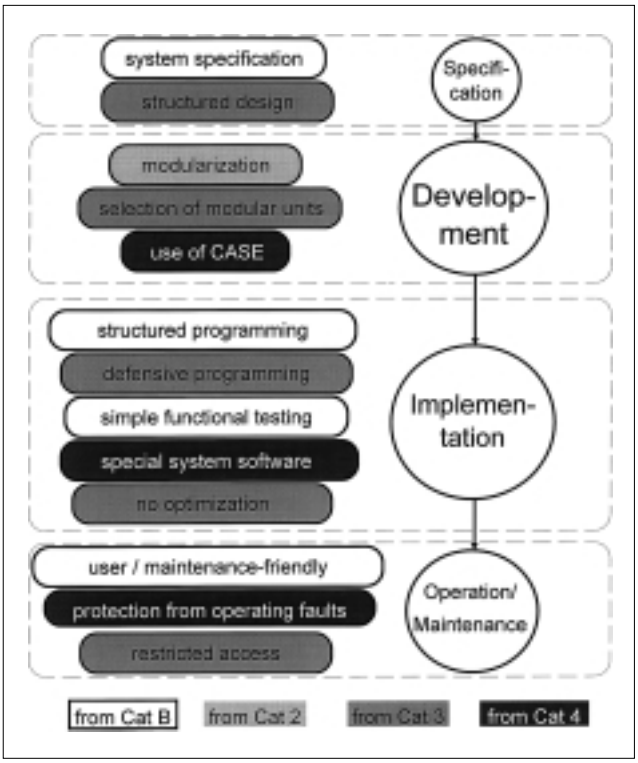


Figure 10:
Fault avoidance measures to be taken by the manufacturer

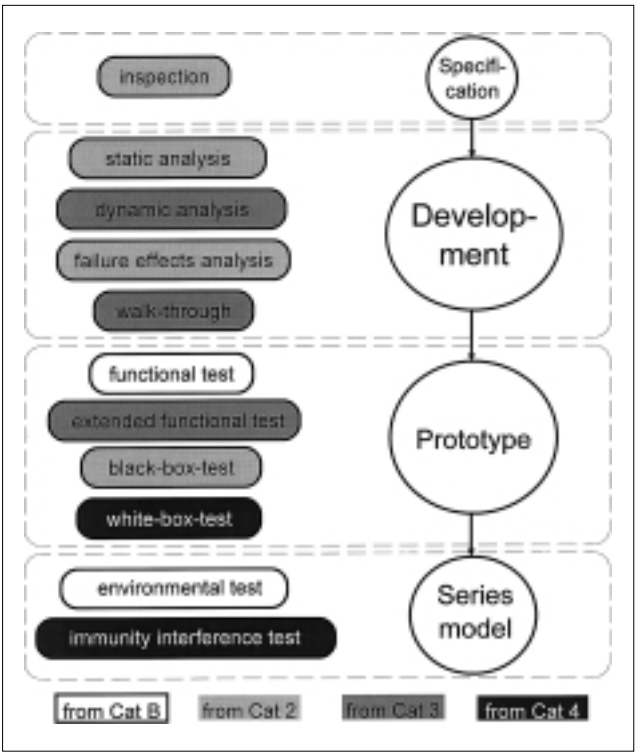


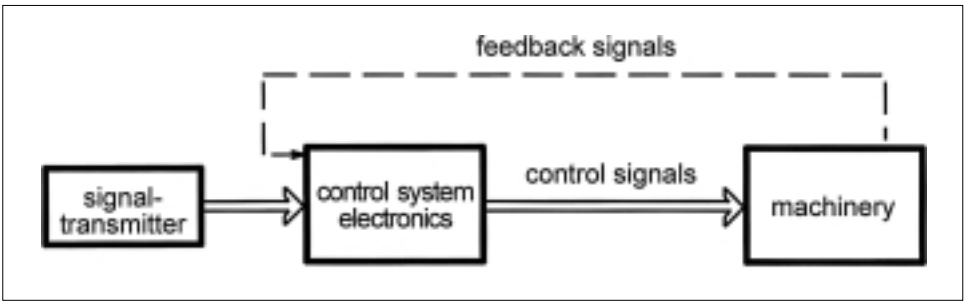
Figure 11:
Fault avoidance measures to be taken by the testing body

into practical applications. The principal source is given as the BIA Handbook (BIA-Handbuch), which is published by Erich Schmidt Verlag and is constantly being up-dated and expanded by loose-leaf editions.

Examples for EN 954

Electronic Control Systems
Example for EN 954 – Category B

Figure 12:
Electronic Control System as per EN 954 – Category B
for the control of potentially hazardous movements



Functional Description:

- ❒ Potentially hazardous movements or states are controlled by a single-channel integrated logic system as a function of the sensor.
- ❒ The safety function cannot be maintained in the event of all component failures and is dependent on the reliability of the components.
- ❒ No fault detection measures are specified.

Design Features

- ❒ The reaction is read back by the single-channel logic system and if plausibility is in doubt, a warning is issued and a cut-off reaction is initiated.
- ❒ The control system is able to withstand standard industrial ambient influences (shock, vibration, temperature, electromagnetic injection).

Application:

- ❒ In the case of low risks, e.g. if the hazard zone is only entered seldomly, if there is a relatively high probability that the hazard can still be averted by other measures and in conjunction with additional, e.g. organisational measures.

Further References:

- ❒ *Jürs, H.; Reinert, D.:* Elektronik in der Sicherheitstechnik. Sicherheitstechnisches Informations- und Arbeitsblatt 330 220. In: BIA-Handbuch 20. Lfg. V/93. Erich Schmidt Verlag, Bielefeld

Electromechanical Control Systems
Example for EN 954 – Category 1

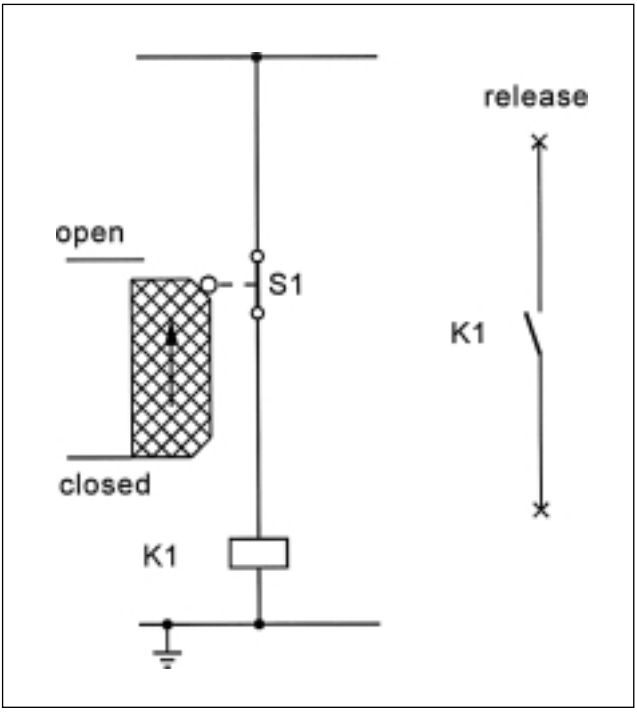


Figure 13:
Electromechanical Control System as per EN 954 – Category 1
Position monitoring for moving safety guards

Functional Description:

- ❒ Potentially hazardous movements or states are interrupted or prevented by contactor relay K1 when the safety guard is opened.
- ❒ The safety function cannot be maintained in the event of all component failures and is dependent on the reliability of the components.
- ❒ No fault detection measures are specified.
- ❒ Removal of the safety device is not detected.

Design Features:

- ❒ The closed circuit principle and control circuit earthing are used as well-tried principles.
- ❒ The switch, S1, is a forcibly opened position switch in accordance with EN 1088. If the safety device is not in the safety position, the normally closed contact must interrupt forcibly by mechanical means.
- ❒ Position monitoring is ensured by a contactor relay of a well-tried design.
- ❒ Actuating elements and position switches should be safeguarded against changes in position. Only rigid mechanical parts (no spring elements) may be used.
- ❒ The actuation stroke for the position switch shall be in accordance with the manufacturer's specifications.

Application:

- ❒ In the case of low risks, e.g. if the hazard zone is only entered seldomly and if there is a relatively high probability that the hazard can still be averted by other measures.

Further References:

- ❒ *Kreutzkampf, F.; Hertel, W.:* Zusammenstellung und Bewertung elektromechanischer Sicherheitsschaltungen für Verriegelungseinrichtungen. Sicherheitstechnisches Informations- und Arbeitsblatt 330 212. In: BIA-Handbuch 17. Lfg. X/91. Erich Schmidt Verlag, Bielefeld
- ❒ *Kreutzkampf, F.; Becker, K.:* Verriegelung beweglicher Schutzeinrichtungen. Sicherheitstechnisches Informations- und Arbeitsblatt 330 210. In: BIA-Handbuch 1. Lfg. IX/85. Erich Schmidt Verlag, Bielefeld

Electromechanical Control Systems
Example for EN 954 – Category 1

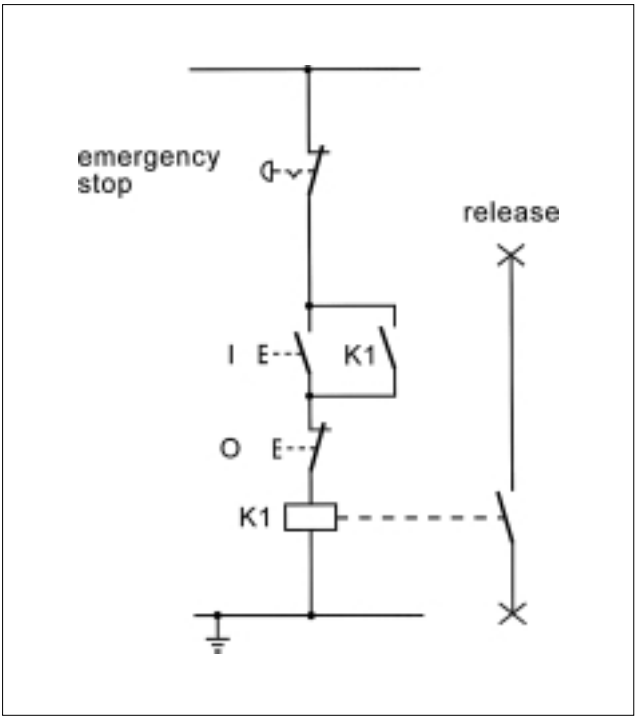


Figure 14:
Electromechanical Control System as per EN 954 – Category 1 emergency stop device

Functional Description:

- ❒ Potentially hazardous movements or states are shut down when the emergency stop device is actuated by contactor relay K1 and by interrupting the control voltage.
- ❒ The safety function cannot be maintained in the event of all component failures and is dependent on the reliability of the components.
- ❒ No fault detection measures are specified.

Design Features:

- ❒ The closed circuit principle and control circuit earthing are used as well-tried principles.
- ❒ The control station and operating element work on the principle of forcible actuation (EN 418).
- ❒ Signal processing is ensured by a contactor relay of a well-tried design.

Application:

- ❒ In the event of low risks, e.g. if switching off the energy supply suddenly does not lead to hazardous states (stop category 0 in accordance with EN 60204-1).
  Note:
  There are also possible applications in machinery in which the probability of hazards occurring is reduced by appropriate measures. Such measures may include safety devices with a corresponding control system category or covering and / or shielding hazardous areas.

Further References:

- ❒ not known.

Electromechanical Control Systems
Example for EN 954 – Category 1

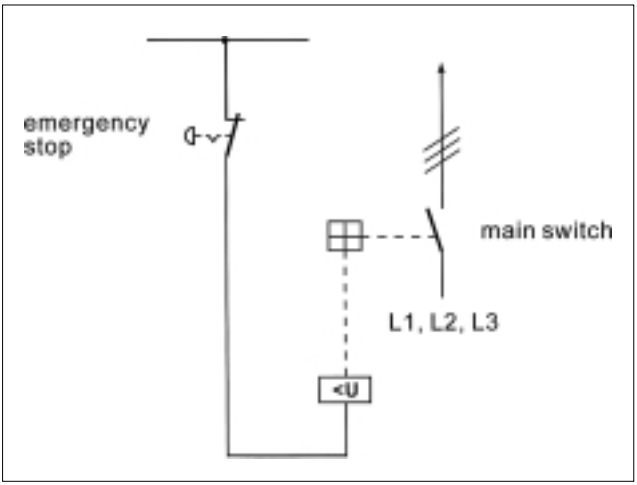


Figure 15:
Electromechanical Control System as per EN 954 – Category 1
Emergency stop device acting on the main switch undervoltage release

Functional Description:

- ❒ Potentially hazardous movements or states are interrupted when the emergency stop device is actuated by switching off the main switch by the undervoltage release.
- ❒ The safety function cannot be maintained in the event of all component failures and is dependent on the reliability of the components.
- ❒ No fault detection measures are specified.

Design Features:

- ❒ The closed circuit principle as applied to the undervoltage release is used as a well-tried principle.
- ❒ The control station and operating element work on the principle of forcible actuation (EN 418).
- ❒ The power supply to the whole machine is switched off.

Application:

- ❒ In the event of low risks, e.g. if switching off the energy supply suddenly does not lead to hazardous states (stop category 0 in accordance with EN 60204-1).
- ❒ There are also possible applications in machinery in which the probability of hazards occurring is reduced by appropriate measures. Such measures may include safety devices with a corresponding control system category or covering and / or shielding hazardous areas.

Further references:

- ❒ not known.

Electromechanical Control Systems
Example for EN 954 – Category 1

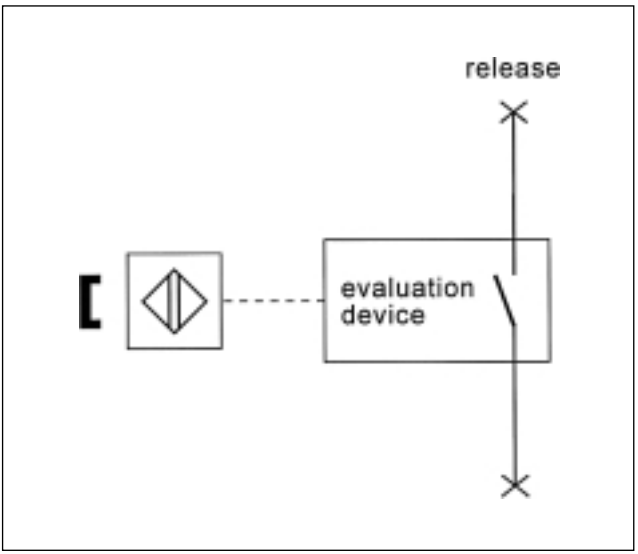


Figure 16:
Electromechanical Control System as per EN 954 – Category 1
Position monitoring for movable safety guards by proximity position switches for safety functions

Functional Description:

- ❒ Potentially hazardous movements or states are interrupted or prevented when the safety guard is opened by the evaluation device of a proximity position switch in accordance with DIN VDE 0660, Part 209.
- ❒ The safety function is comparable with mechanical position switches in accordance with EN 1088.
- ❒ The safety function is not affected by the occurrence of single faults. The safety function can be extended still further by appropriate design of the transmitter units, wires and evaluation devices.
- ❒ Removal of the safety device is detected.

Design Features:

- ❒ The switching states of various sensors (reed contacts) are evaluated by the evaluation device. The switching process is triggered by changes in magnetic, electromagnetic, optical, acoustic or other fields.
- ❒ Safe function cannot be easily suspended by evasion techniques; e.g. by using coded actuating magnets.

Application:

- ❒ In the case of low risks, e.g. if the hazard zone is only entered seldomly and if there is a relatively high probability that the hazard can still be averted by other measures. These may also be applied in situations in which the use of proximity systems is advantageous due to the absence of mechanisms and the high protection system class.

Further References:

- ❒ *Börner, F.; Foermer, H.-G.*; *Meffert, K.:* Magnetschalter in Sicherheitskreisen. BIA-Report 4 / 89. Hrsg.: Berufsgenossenschaftliches Institut für Arbeitssicherheit – BIA, Sankt Augustin 1989
- ❒ *Börner, F.; Meffert, K.:* Berührungslos wirkende Positionsschalter für Sicherheitsfunktionen, Positivliste. Sicherheitstechnisches Informations- und Arbeitsblatt 545 213. In: BIA-Handbuch 22. Lfg. V / 94. Erich Schmidt Verlag, Bielefeld

Hydraulic Control Systems
Example for EN 954 – Category 1

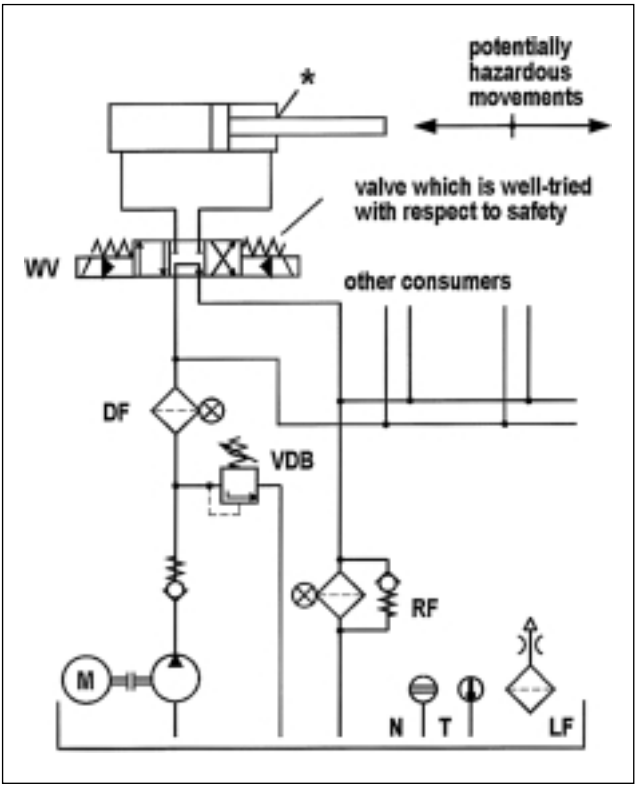


Figure 17:
Electrohydraulic Control System as per EN 954 – Category 1, for the control of potentially hazardous movements

Functional Description:

- Potentially hazardous movements or states are controlled by **one** directional control valve, WV, which is well-tried with respect to safety.
- Failure of the directional control valve may lead to the loss of the safety function. Failure is dependent on the reliability of the directional control valve.
- No fault detection measures are specified.

Design Features:

- WV is a directional control valve, with locked position, mid-position, adequate positive overlap, spring centring and durable springs.
- The safety-oriented switching position is achieved by removing the control signal. The manufacturer / user should, if necessary, confirm that the directional control valve is a component which is well-tried with respect to safety (sufficiently high degree of reliability).
- Specific measures to increase the reliability of the directional control valve by the use of a pressure filter, DF, in front of the directional control valve and by appropriate measures to prevent dirt being taken in through the piston rod in the cylinder (e.g. working wiper rings on the piston rod, see *) are necessary.

Application:

- In the case of low risks, e.g. if the hazard zone is only entered seldomly and if there is a relatively high probability that the hazard can still be averted by other measures.

Further References:

- *Kleinbreuer, W.:* Anwendung der Kategorien nach prEN 954-1 auf fluidtechnische Steuerungen. O+P "Ölhydraulik und Pneumatik" 38 (1994) Nr. 9
- *Kleinbreuer, W.:* Application of the Categories laid down in prEN 954-1 to fluid technology control systems. HEALTH & SAFETY EXECUTIVE LANGUAGE SERVICE, Transl. No. 15214 B, Information Centre, Broad Lane, Sheffield S37HQ, GB

Hydraulic Control Systems
Example for EN 954 – Category 1

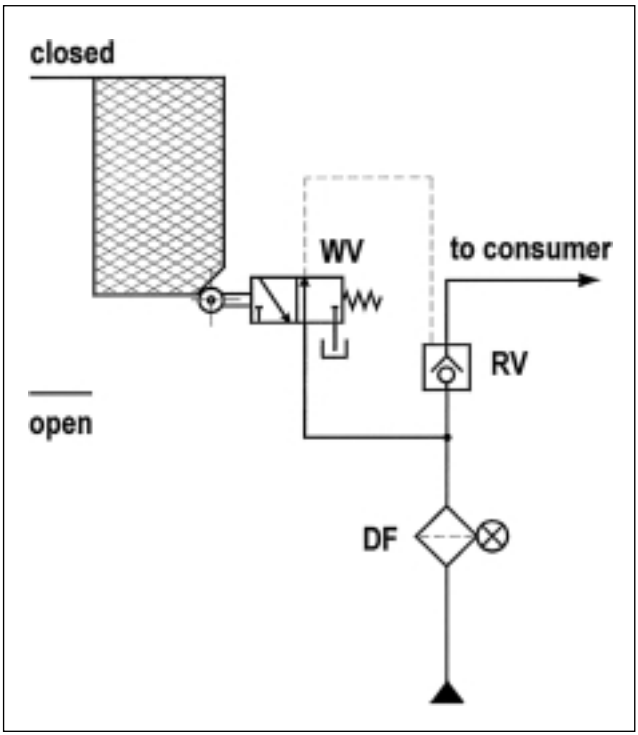


Figure 18:
Hydraulic Control System as per EN 954 – Category 1
Interlocking of movable safety guard (locking mechanism)

Functional Description:

- ❒ nterlocking of movable safety guard is monitored by a "hydraulic position switch", WV. This issues a control command to the stop valve, RV. Both valves are components which are well-tried with respect to safety.
- ❒ Energy supply (hydraulic) is only provided when the safety device is closed.
- ❒ Failure of the stop valve may lead to the loss of the safety function. Failure is dependent on the reliability of the stop valve.
- ❒ No fault detection measures are specified.

Design Features:

- ❒ WV is a hydraulic position switch (roller lever valve) with forcible actuation by movable safety guard, in accordance with EN 1088.
- ❒ The safety-oriented switching position of RV is achieved by removing the control signal.
- ❒ The manufacturer / user should, if necessary, confirm that the valves are components which are well-tried with respect to safety (sufficiently high degree of reliability).
- ❒ Specific measures to increase reliability by pressure filters, DF, in front of the valves are necessary.

Application:

- ❒ In the case of low risks, e.g. if the hazard zone is only entered seldomly and if there is a relatively high probability that the hazard can still be averted by other measures.

Further References:

- ❒ *Kleinbreuer, W.:* Anforderungen an hydraulische und pneumatische Maschinensteuerungen. Sichere Chemiearbeit (1992) Nr. 2 und Nr. 3
- ❒ EN 1088, Sicherheit von Maschinen – Verriegelungseinrichtungen in Verbindung mit trennenden Schutzeinrichtungen – Leitsätze für Gestaltung und Auswahl

Pneumatic Control Systems
Example for EN 954 – Category 1

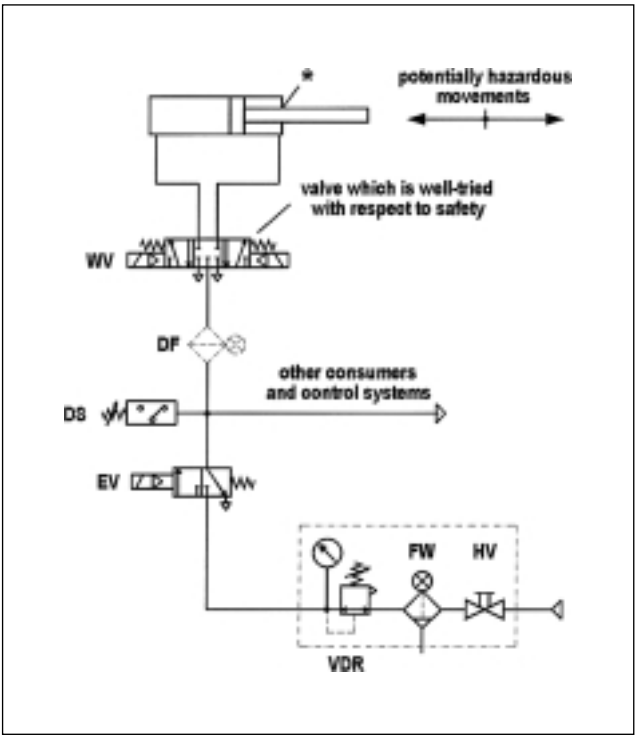


Figure 19:
Electropneumatic Control System as per EN 954 – Category 1, for the control of potentially hazardous movements

Functional Description:

- ❒ Potentially hazardous movements or states are controlled by **one** directional control valve, WV, which is well-tried with respect to safety.
- ❒ Failure of the directional control valve may lead to the loss of the safety function. Failure is dependent on the reliability of the directional control valve.
- ❒ No fault detection measures are specified.

Design Features:

- ❒ WV is a directional control valve, with locked position, mid-position, adequate positive overlap, spring centring and durable springs.
- ❒ The safety-oriented switching position is achieved by removing the control signal.
- ❒ The manufacturer / user should, if necessary, confirm that the directional control valve is a component which is well-tried with respect to safety (sufficiently high degree of reliability).
- ❒ Specific measures to increase the reliability of the directional control valve by the use of a pressure filter, DF, (may be required in extensive pipework systems) in front of the directional control valve and by appropriate measures to prevent dirt being taken in through the piston rod in the cylinder (e.g. working wiper rings on the piston rod, see *) are necessary.

Application:

- ❒ In the case of low risks, e.g. if the hazard zone is only entered seldomly and if there is a relatively high probability that the hazard can still be averted by other measures.

Further References:

- ❒ *Kleinbreuer, W.:* Anwendung der Kategorien nach prEN 954-1 auf fluid-technische Steuerungen. O+P "Ölhydraulik und Pneumatik" 38 (1994) No. 9
- ❒ *Kleinbreuer, W.:* Application of the Categories laid down in prEN 954-1 to fluid technology control systems. HEALTH & SAFETY EXECUTIVE LANGUAGE SERVICE, Transl. No. 15214 B, Information Centre, Broad Lane, Sheffield S37HQ, GB

Hydraulic Control Systems
Example for EN 954 – Category 2

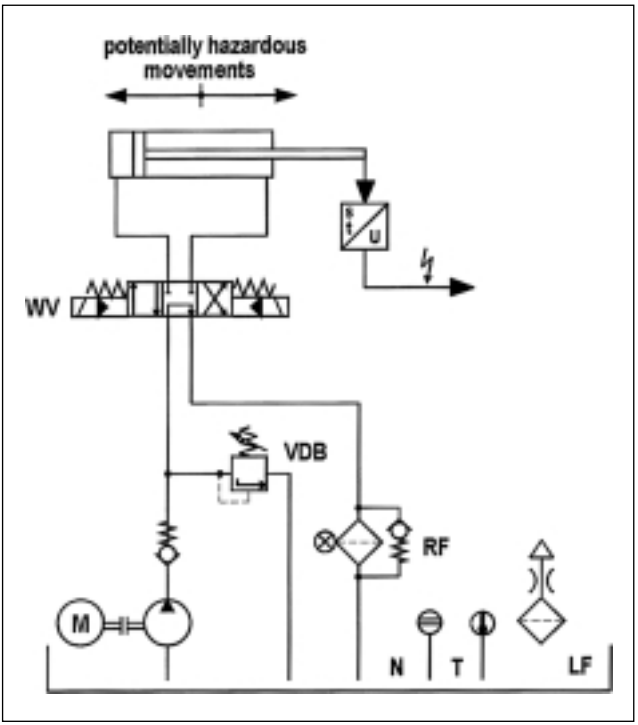


Figure 20:
Electrohydraulic Control System as per EN 954 – Category 2, for the control of potentially hazardous movements

Functional Description:

- ❒ Potentially hazardous movements or states are controlled by **one** directional control valve, WV.
- ❒ Failure of the directional control valve between the functional tests may lead to the loss of the safety function. Failure is dependent on the reliability of the directional control valve.
- ❒ Compulsory testing of the safety function at appropriate timed intervals is made. If the tests detect that the directional control valve has failed, this may, for example, lead to the machinery being switched off.
- ❒ The test function should not be impaired by failure of the directional control valve. Failure of the test function should not lead to a failure of the directional control valve.

Design Features:

- ❒ WV is a directional control valve, with locked position, mid-position, adequate positive overlap and spring centring.
- ❒ The safety-oriented switching position is achieved by removing the control signal.
- ❒ Testing is done, e.g. by checking the distance / time-related behaviour of the potentially hazardous movements in conjunction with the switching state of the directional control valve, evaluation in single-channel PLC.

Application:

- ❒ In the case of low risks, e.g. if the hazard zone is only entered seldomly and if there is a relatively high probability that the hazard can still be averted by other measures.

Further References:

- ❒ not known.

Pneumatic Control Systems
Example for EN 954 – Category 2

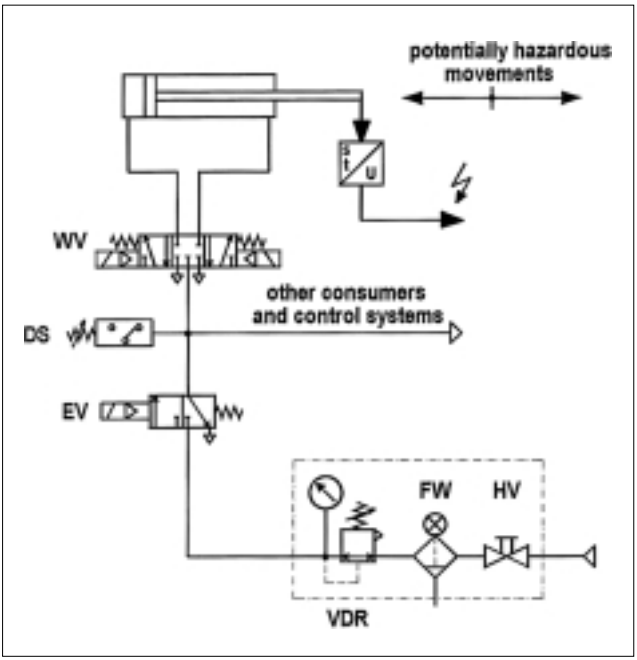


Figure 21:
Electropneumatic Control System as per EN 954 – category 2, for the control of potentially hazardous movements

Functional Description:

- ❒ Potentially hazardous movements or states are controlled by **one** directional control valve, WV.
- ❒ Failure of the directional control valve between the functional tests may lead to the loss of the safety function. Failure is dependent on the reliability of the directional control valve.
- ❒ Compulsory testing of the safety function at appropriate timed intervals is made. If the tests detect that the directional control valve has failed, this may, for example, lead to the machinery being switched off.
- ❒ The test function should not be impaired by failure of the directional control valve. Failure of the test function should not lead to a failure of the directional control valve.

Design Features:

- ❒ WV is a directional control valve, with locked position, mid-position, adequate positive overlap and spring centring.
- ❒ The safety-oriented switching position is achieved by removing the control signal.
- ❒ Testing is done, e.g. by checking the distance / time-related behaviour of the potentially hazardous movements in conjunction with the switching state of the directional control valve, evaluation in single-channel PLC.

Application:

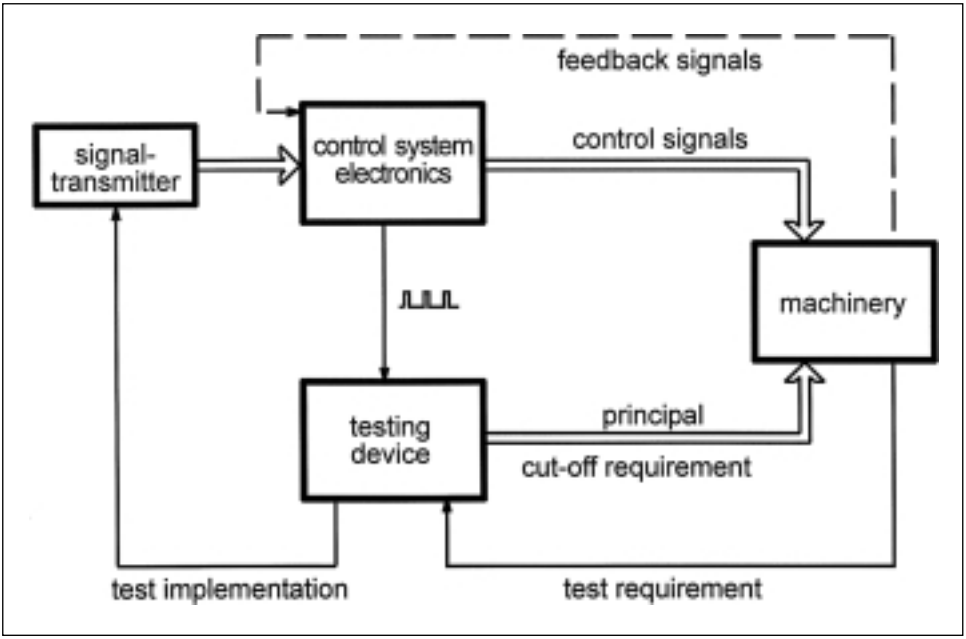
- ❒ In the case of low risks, e.g. if the hazard zone is only entered seldomly and if there is a relatively high probability that the hazard can still be averted by other measures.

Further References:

- ❒ not known.

Electronic Control Systems
Example for EN 954 – Category 2

Figure 22:
Electronic Control System as per EN 954 – Category 2
Outline structure of the control system



Functional Description:

- ❒ Potentially hazardous movements or states are controlled as a function of the signal transmitter.
- ❒ Compulsory testing of the safety function (by the system's own hardware, operating independently of the control system electronics) takes place either when the machinery is started up or on a cyclic basis.
- ❒ During the test, the safety function is checked thoroughly, i.e. release of the potentially hazardous movement is prevented when testing is underway.
- ❒ The testing or safety function must be maintained in the event of an individual component failure.
- ❒ Failure of the safety function is picked up during the next test.

Design Features:

- ❒ The second independent cut-off path makes it possible to shut down the system even if the normal cut-off path has failed.
- ❒ No further requirements are imposed on the testing device (failure does not have to be detected).
- ❒ The test covers the signal transmitter and the cut-off device.

Application:

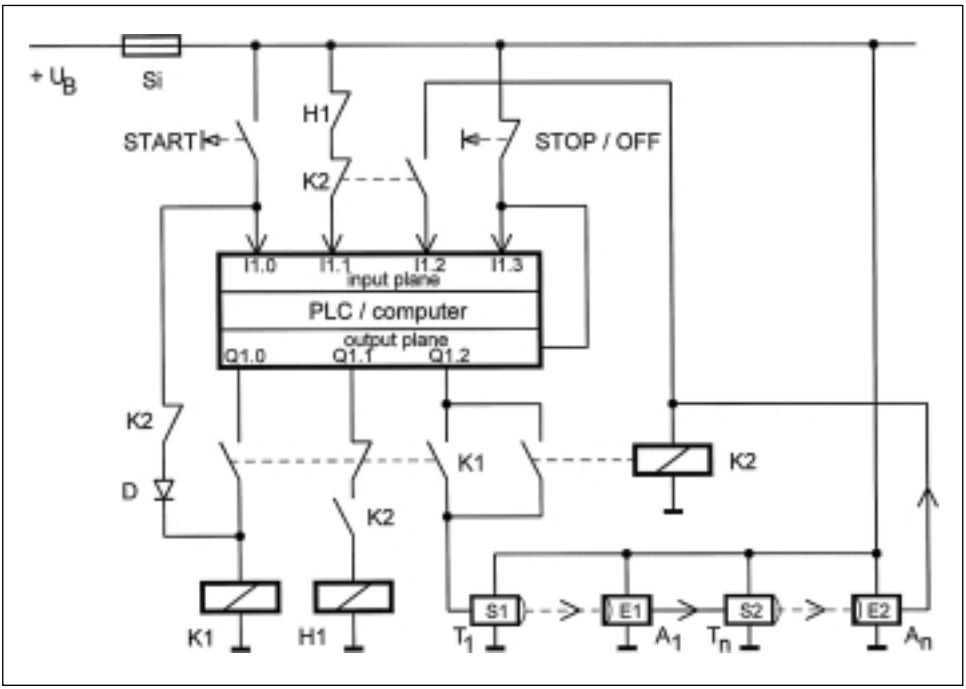
- ❒ In the case of low risks, e.g. if the hazard zone is only entered seldomy and if there is a relatively high probability that the hazard can still be averted by other measures. It must be possible to stop potentially hazardous movements or states on a regular basis as a function of the process in question.

Further References:

- ❒ *Jürs, H.; Reinert, D.:* Elektronik in der Sicherheitstechnik. Sicherheitstechnisches Informations- und Arbeitsblatt 330 220. In: BIA-Handbuch 20. Lfg. V/93. Erich Schmidt Verlag, Bielefeld
- ❒ *Grigulewitsch, W.; Reinert, D.:* Lichtschranken mit Testung. Sicherheitstechnisches Informations- und Arbeitsblatt 330 228. In BIA-Handbuch 22. Lfg. V/94. Erich Schmidt Verlag, Bielefeld

Computer Control Systems
Example for EN 954 – Category 2

Figure 23:
Computer Control System as per EN 954 – Category 2
Safety light barrier realized using a standard PLC



Functional Description:

- ❒ In the event of interrupting the light beam of the light barrier S1 / E1, potentially hazardous movements or states are shut down on a redundant basis by PLC output Q1.1 and relay / contactor K2.
- ❒ The light barrier safety function is tested after pressing the START key by software-controlled shutdown of the light barrier transmitter by PLC output Q1.2 and monitoring the receiver reaction by PLC inputs I1.1 and I1.2.
- ❒ The software is responsible for detecting a light barrier failure or a defective release delay.
- ❒ RELEASE is suspended for the duration of testing.

Design Features:

- ❒ Special light barriers with adequate optical characteristics as defined in EN 61496 must be used.
- ❒ K1 and K2 are relays with contacts with connected movement.
- ❒ Several transmitter / receiver systems can be cascaded and monitored with only one additional PLC input per light barrier.

Application:

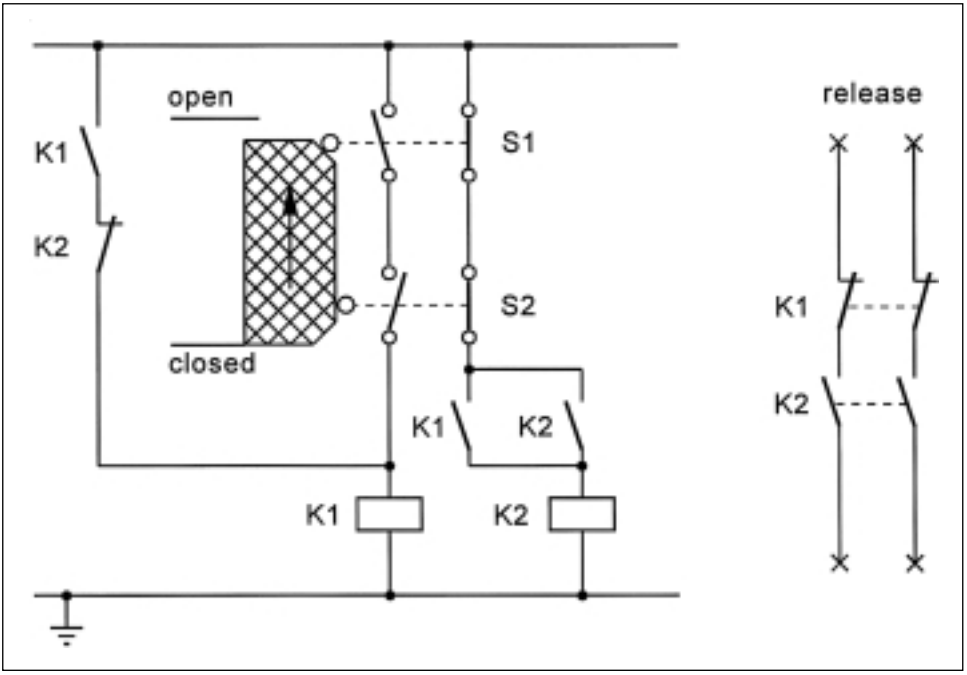
- ❒ In the case of low risks, e.g. if the hazard zone is only entered seldomly and if there is a relatively high probability that the hazard can still be averted by other measures. It must be possible to link the light barrier start-up test with regular initiation of the potentially hazardous movement (state).

Further References:

- ❒ *Grigulewitsch, W.; Reinert, D.:* Lichtschranken mit Testung. Sicherheitstechnisches Informations- und Arbeitsblatt 330 228. In: BIA-Handbuch 22. Lfg. V / 94. Erich Schmidt Verlag, Bielefeld

Electromechanical Control Systems
Example for EN 954 – Category 3

Figure 24:
Electromechanical Control System as per EN 954 – Category 3
Position monitoring for movable safety guards



Functional Description:

- ❒ Potentially hazardous movements or states are interrupted or prevented by a combination of normally closed and normally open contacts when the safety guard is opened.
- ❒ Release is only granted if the safety device is opened and then closed again (start-up testing).
- ❒ Removal of the safety device is detected immediately (by S2).
- ❒ If one component failure occurs, the safety function is still maintained.
- ❒ Most component failures are detected and lead to stoppage of operations.
- ❒ Faults in the starting and actuating mechanism are detected by the use of two position switches which are actuated using different principles (normally closed – normally open contact combination).
- ❒ There are few faults which are not detected (non-release of the control contactor, K2, when de-energized; non-interruption of the contacts in S1 or S2). An accumulation of faults of this type may lead to the loss of the safety function.

Design Features:

- ❒ The switch, S1, is a forcibly opened position switch in accordance with EN 1088.
- ❒ The control contactors, K1 and K2, have contacts with connected movement.
- ❒ The leads to the position switches are installed separately.

Application:

- ❒ In the case of medium to high risks, e.g. if the hazard zone is entered on a regular basis and if there is a relatively high probability that the hazard can still be averted by other measures.

Further References:

- ❒ *Kreutzkampf, F.; Hertel, W.:* Zusammenstellung und Bewertung elektromechanischer Sicherheitsschaltungen für Verriegelungseinrichtungen. Sicherheitstechnisches Informations- und Arbeitsblatt 330 212. In: BIA-Handbuch 17. Lfg. X/91. Erich Schmidt Verlag, Bielefeld
- ❒ *Kreutzkampf, F.; Hertel, W.:* Zusammenstellung und Bewertung elektromechanischer Sicherheitsschaltungen zur Stellungsüberwachung beweglicher Schutzeinrichtungen. BIA-Report 3/89

Electromechanical Control Systems
Example for EN 954 – Category 3

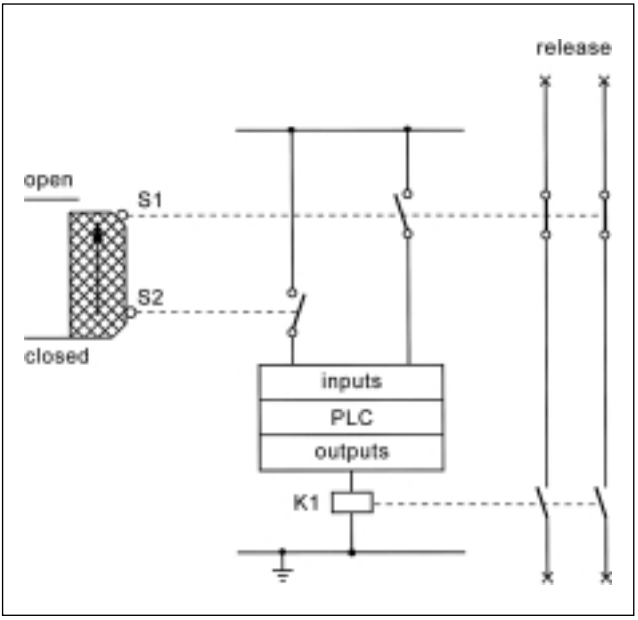


Figure 25:
Electromechanical Control System as per EN 954 – Category 3
Position monitoring for movable safety guards

Functional Description:

- ❒ Potentially hazardous movements or states are interrupted or prevented by a combination of normally closed and normally open contacts when the safety guard is opened.
- ❒ If one component failure occurs, the safety function is still maintained.
- ❒ Component failures in S1 and S2 are detected by the PLC and lead to stoppage of operations by K1.
- ❒ Faults in the starting and actuating mechanism are detected by the use of two position switches which are actuated using different principles (normally closed – normally open contact combination).
- ❒ Faults in the PLC and K1 are not detected. A further failure (e.g. failure of S1) causes the loss of the safety function.

Design Features:

- ❒ The switch, S1, is a forcibly opened position switch in accordance with EN 1088.
- ❒ The leads to the position switches are installed separately or take the form of protected wiring.

Application:

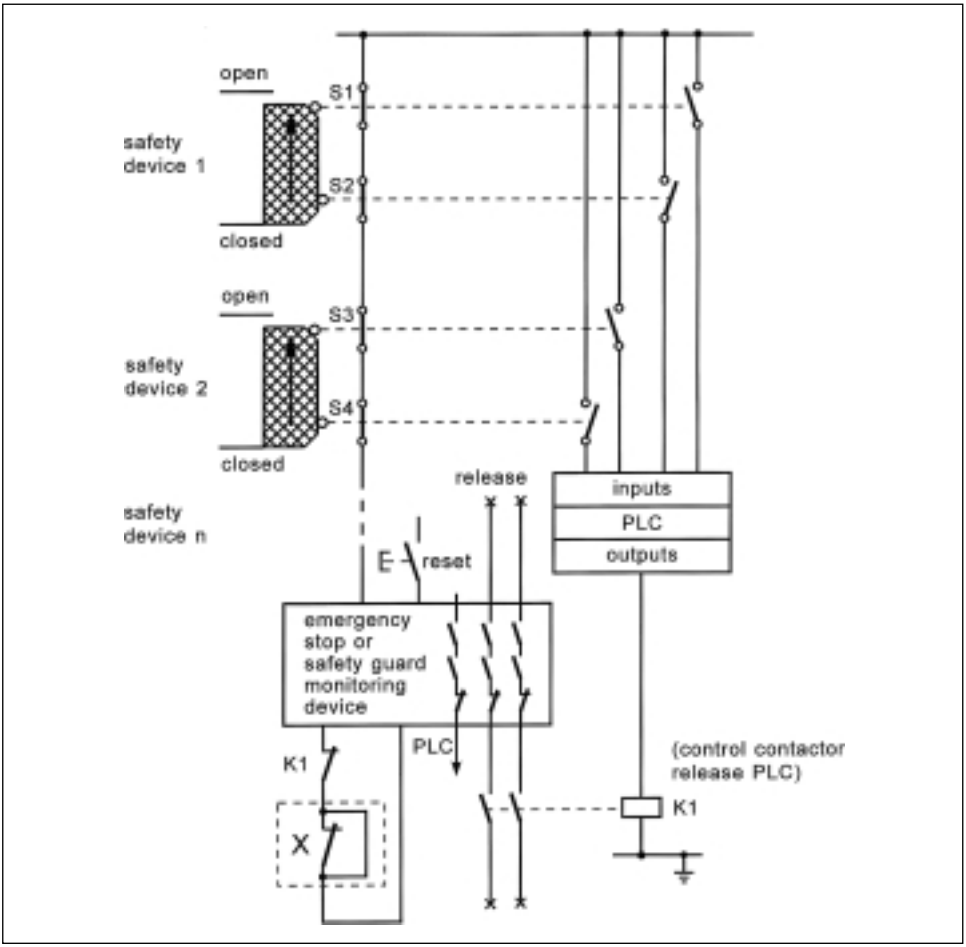
- ❒ In the case of medium to high risks, e.g. if the hazard zone is entered on a regular basis and if there is a relatively high probability that the hazard can still be averted by other measures.

Further References:

- ❒ not known.

Electromechanical Control Systems
Example for EN 954 – Category 3

Figure 26:
Electromechanical Control System as per EN 954 – Category 3
Position monitoring for movable safety guards



Functional Description:

- ❒ Potentially hazardous movements or states are interrupted or prevented by a combination of normally closed and normally open contacts when the safety guard is opened.
- ❒ If one component failure occurs, the safety function is still maintained.
- ❒ Most component failures are detected and lead to stoppage of operations.
- ❒ Faults in the starting and actuating mechanism are detected by the use of two position switches which are actuated using different principles (normally closed – normally open contact combination).
- ❒ A few faults are not detected (e.g. non-interruption of contacts in S1 to S4).
- ❒ Several safety devices can be connected in series (cascading).
- ❒ The circuit can be extended in the area marked "X" for the purpose of monitoring power contactors and contactors for duplicating the release path.

Design Features:

- ❒ Switches S1 and S3 are forcibly opened position switches in accordance with EN 1088.
- ❒ Contactor K1 has contacts with connected movement.
- ❒ The leads to the position switches are installed separately or take the form of protected wiring.
- ❒ Emergency stop or safety guard monitoring device corresponds to category 4.

Application:

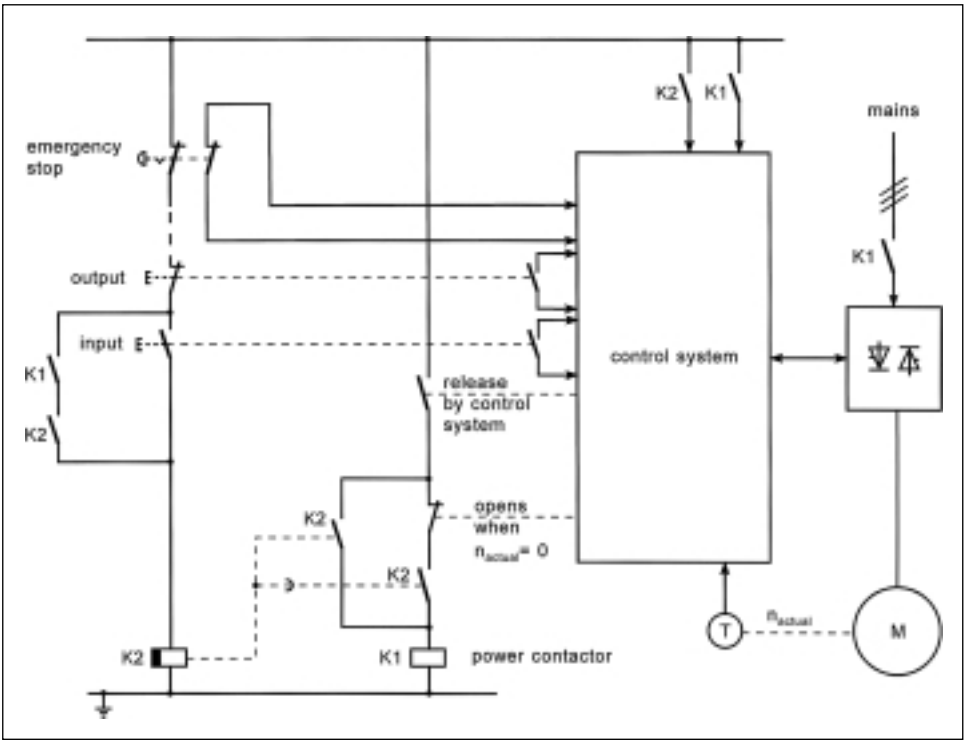
- ❒ In the case of medium to high risks, e.g. if the hazard zone is entered on a regular basis and if there is a relatively high probability that the hazard can still be averted by other measures.

Further References:

- ❒ not known.

Electromechanical Control Systems
Example for EN 954 – Category 3

Figure 27:
Electromechanical Control System as per EN 954 – Category 3
Emergency stop device for converter with regenerative braking by energy feedback



Functional Description:

- After actuating the emergency stop device, the drive mechanism is braked by energy feedback. The power contactor, K1, must remain in the on position until the drive mechanism is at standstill. When n_{actual} is equal to zero, the power contactor is switched off by the standstill message from the converter.
- If this switching off action does not take effect, switching off is achieved no later than after the usual braking time by the delayed contact from K2.

Design Features:

- The emergency stop device is designed on a redundant basis. Braking is initiated via a normally closed contact and the drive mechanism is brought to a standstill (stop-category 2 in accordance with EN 60204-1). K2 and the power contactor, K1, are switched off after a delay via the emergency stop device's other normally closed contact (stop category 1 in accordance with EN 60204-1).
- Redundant shutdown of the drive mechanism is achieved in a different way by the emergency stop device. Depending on the position in which a fault occurs, the drive mechanism is either not braked, but switched off after a delay by K2 and K1, or the power supply is not cut off by K1 after braking by the converter.
- Most faults can be detected by the control system and start-up of the drive mechanism can be prevented.

Application:

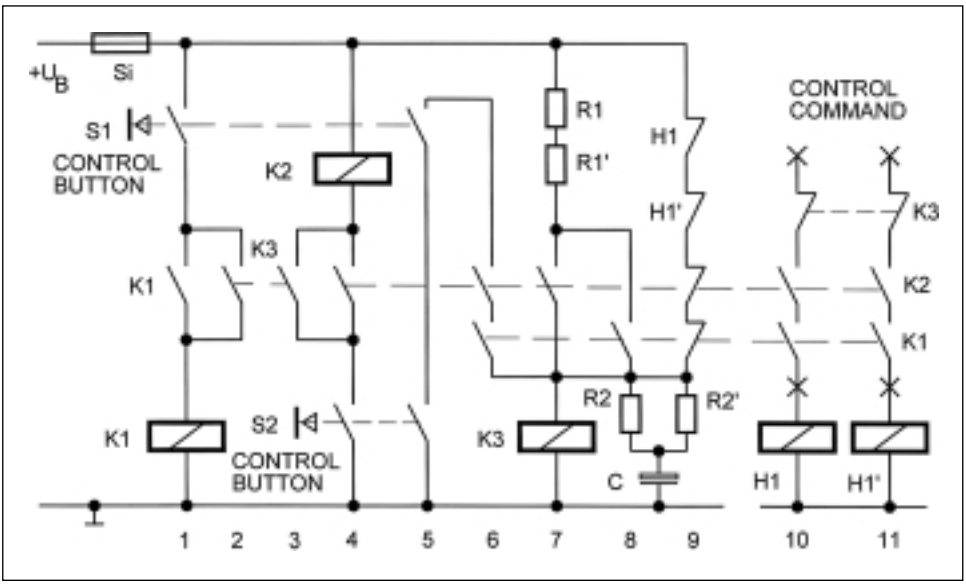
- In the case of medium to high risks, e.g. if the hazard zone is entered on a regular basis and if there is a relatively high probability that the hazard can still be averted by other measures. This can only be applied if using converters with regenerative braking (stop category 1) in which failure of the electronic brake in the event of a fault can be tolerated when the emergency stop device is actuated.

Further References:

- not known.

Electromechanical Control Systems
Example for EN 954 – Category 3

Figure 28:
Electromechanical Control System as per EN 954 – Category 3
Two-hand control circuit in systems using contacts as per prEN 574 type II **without** time settings for synchronous actuation



Functional Description:

- A potentially hazardous movement or state can only be initiated by actuating both controls, S1 and S2 (current path 1, 4 and 5), in that K3 drops out after K1 and K2 respond via paths 5 and 6 and this thus issues the control command.
- Even if only one input command is cancelled by S1 or S2, this leads to the control command being cancelled immediately via K1 or K2 as K3 dropped out when the command was issued (see current path 10 and 11).
- Reset monitoring is achieved via K3 (current paths 2 and 3) and the two normally closed contacts of K1 and K2 in current path 9.
- In the event of a fault, single-handed control is not possible. When the system is resting, K3 has responded and is preparing to trigger K1 and K2 in current paths 2 and 3. At the same time, K3 blocks any control commands from being output in the output circuit. If one of relays K1 or K2 does not drop out after an input command is cancelled, K3 also remains in the dropped-out position via R1 / R1'.

Design Features:

- The offset coil arrangement of K1 and K2 detects short circuits in the wiring to the controls with the aid of the fuse, Si.
- Buttons with double contacts are provided for both controls, which means that even if one of the contacts does not open, intentional actuation of the buttons remains a prerequisite for a valid control command.
- K3 is wired with a delayed release to bridge the contact switching intervals for relays K1 and K2. The resistors, R2 / R2', limit the starting current of the capacitor, C, to approx. 0.5 A.
- K1 – K3, H1 / H1' are relays or contactors with contacts with connected movement.
- All relay / contactor coils have been fitted with arc suppressors to ensure safe function of the circuit.

Application:

- In the case of medium to high risks, e.g. if the hazard zone is entered on a regular basis and if there is a relatively high probability that the hazard can still be averted by other measures.

Further References:

Grigulewitsch, W.; Reinert, D.: Zweihandschaltungen nach Anforderungsstufe II in DIN 24980. Sicherheitstechnisches Informations- und Arbeitsblatt 330229. In: BIA-Handbuch 17. Lfg. X / 91. Erich Schmidt Verlag, Bielefeld

Hydraulic Control Systems
Example for EN 954 – Category 3

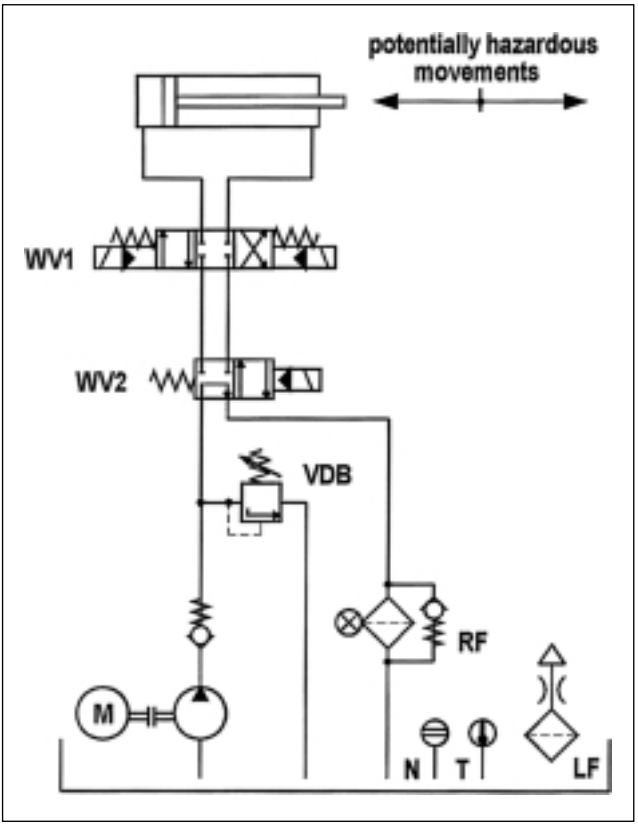


Figure 29:
Electrohydraulic Control System as per EN 954 – Category 3, without fault detection measures, for the control of potentially hazardous movements

Functional Description:

- ❒ Potentially hazardous movements or states are controlled by **two** directional control valves (WV1 and WV2).
- ❒ Failure of one of the directional control valves does not lead to the loss of the safety function.
- ❒ Both directional control valves are triggered cyclically.
- ❒ No fault detection measures are specified (in accordance with a risk evaluation). Some faults are detected as a function of operation. An accumulation of undetected faults may lead to the loss of the safety function.

Design Features:

- ❒ Both directional control valves (WV1 and WV2), have locked position in mid-position, adequate positive overlap and spring centring and / or return.
- ❒ The safety-oriented switching position is achieved by removing the control signal.

Application:

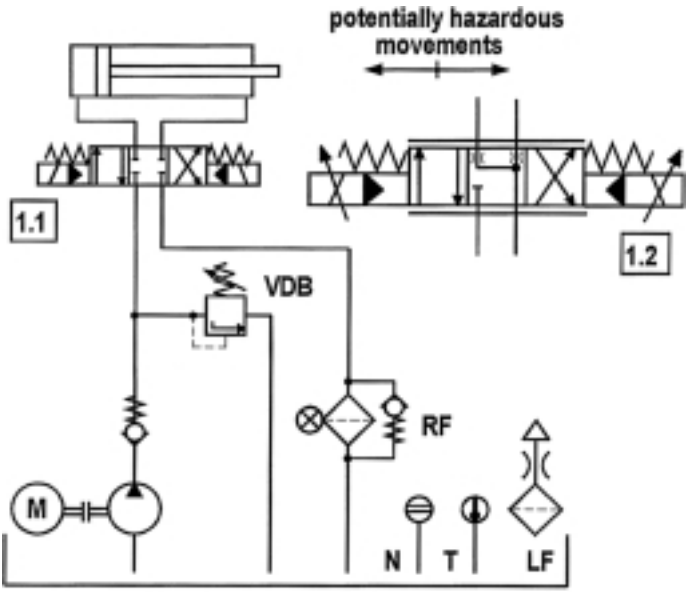
- ❒ In the case of medium to high risks, e.g. if the hazard zone is entered on a regular basis and if there is a relatively high probability that the hazard can still be averted by other measures.

Further References:

- ❒ *Kleinbreuer, W.:* Konstruierte Sicherheit, Anforderungen an hydraulische und pneumatische Maschinensteuerungen. fluid (1992) Nr. 11 / 12.

Hydraulic Control Systems
Example for EN 954 – Category 3

Figure 30:
Electrohydraulic Control System as per EN 954 – Category 3,
for the control of potentially hazardous movements



1.1 Valve suitable for Category 3 and disconnection of the pump drive motor by an appropriate power contactor.

1.2 Valve which is not suitable for Category 3, but disconnection of the pump drive motor in accordance with Category 3.

Functional Description:

- ❒ Potentially hazardous movements or states are controlled by **one** directional control valve and by disconnecting the pump drive motor (Solution 1.1) or by redundant disconnection of the pump drive motor (Solution 1.2).
- ❒ One component failure (directional control valve or power contactor or one of the two power contactors) does not lead to the loss of the safety function.
- ❒ All the specified components are triggered cyclically.
- ❒ No fault detection measures are specified in the hydraulic part of the control system (in accordance with a risk evaluation). Some faults are detected as a function of operation. An accumulation of undetected faults may lead to the loss of the safety function.

Design Features:

- ❒ Directional control valve 1.1 has locked position in mid-position, adequate positive overlap and spring centring. Directional control valve 1.2 is not suitable for Category 3 (e.g. servo valve with zero overlap).
- ❒ In both solutions, the safety-oriented state is achieved by removal of the control signal in each instance.

Application:

- ❒ In the case of medium to high risks, e.g. if the hazard zone is entered on a regular basis and if there is a relatively high probability that the hazard can still be averted by other measures.

Further References:

- ❒ *Kleinbreuer, W.:* Hydraulische und pneumatische Maschinensteuerungen mit abgestuften sicherheitstechnischen Maßnahmen für den Fehlerfall (Allgemeine Anforderungen, Schaltungsbeispiele, Fehlerliste).16. Internationales Kolloquium, Berichtsband P. 69-76, Hrsg.: ISSA, Heidelberg.

Hydraulic Control Systems
Example for EN 954 – Category 3

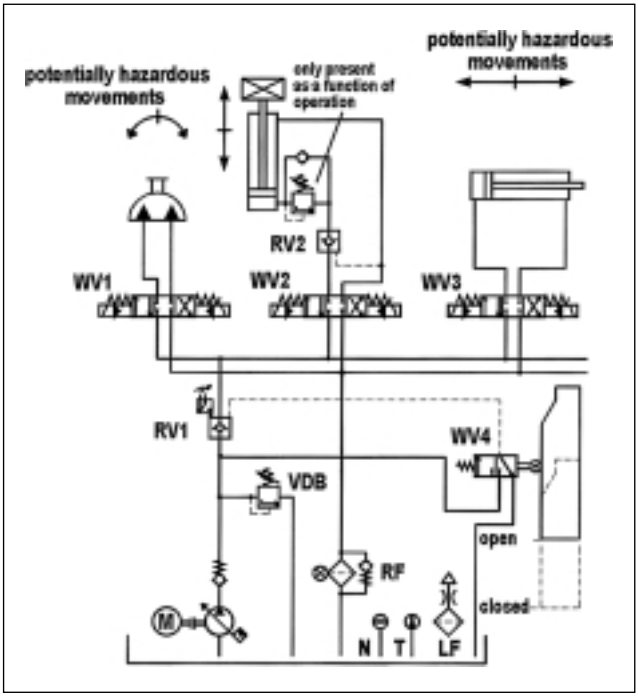


Figure 31:
Electrohydraulic Control System as per EN 954 – Category 3, with fault detection measures, for the control of potentially hazardous movements

Functional Description:

- Potentially hazardous movements or states are controlled by **two** directional control valves in each instance (RV1 operating with one WV in each instance). There exists an additional stop valve RV2 to prevent closing movement due to forces of gravity.
- Failure of one of the two named valves in each case does not lead to the loss of the safety function.
- WV1 to WV3 are triggered cyclically, RV1 closes only when the movable safety guard is opened.
- A fault detection measure is only specified in the case of RV1. Some faults in the valves which are not monitored are detected as a function of operation. An accumulation of undetected faults may lead to the loss of the safety function.

Design Features:

- Directional control valves WV1 to WV3 have a locked position in mid-position, adequate positive overlap and spring centring. RV1 with electrical position monitoring, as RV1 does not switch cyclically.
- The safety-oriented switching position is achieved by removing the control signal (electrical or hydraulic) in each instance.
- Signal processing for electrical position monitoring may, for example, take place in a single-channel PLC.

Application:

- In the case of medium to high risks, e.g. if the hazard zone is entered on a regular basis and if there is a relatively high probability that the hazard can still be averted by other measures.

Further References:

- *Kleinbreuer, W.:* Hydraulische und pneumatische Maschinensteuerungen mit abgestuften sicherheitstechnischen Maßnahmen für den Fehlerfall (Allgemeine Anforderungen, Schaltungsbeispiele, Fehlerliste). 16. Internationales Kolloquium, Berichtsband S. 69-76, Hrsg.: ISSA, Heidelberg.

Pneumatic Control Systems
Example for EN 954 – Category 3

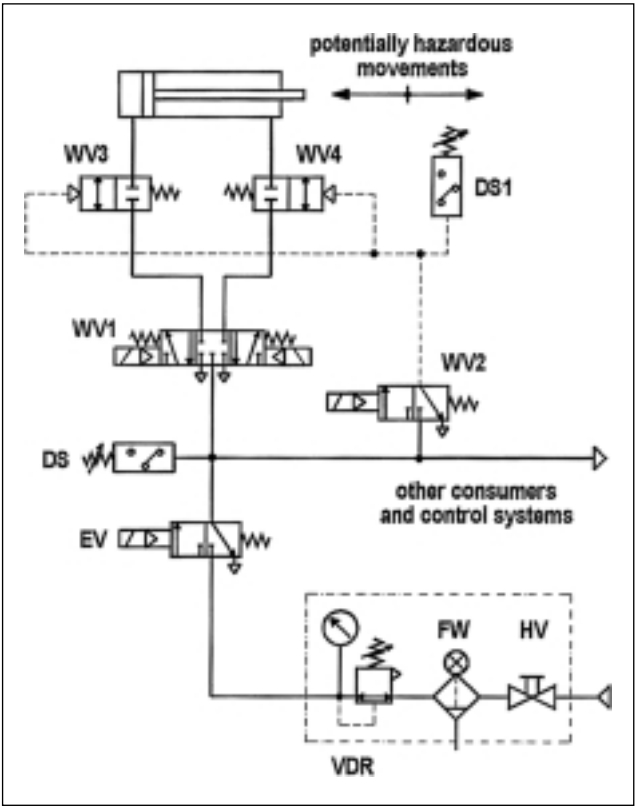


Figure 32:
Electropneumatic Control System as per EN 954 – Category 3, for the control of potentially hazardous movements

Functional Description:

- ❒ Potentially hazardous movements or states are controlled by **two** directional control valves in each instance (WV1 and WV3 or WV1 and WV4).
- ❒ Failure of one of the directional control valves does not lead to the loss of the safety function.
- ❒ All directional control valves are triggered cyclically.
- ❒ Operation of the pilot valve, WV2, is monitored by pressure switch DS1. Some faults may be detected in the valves which are not monitored as a function of operation. An accumulation of undetected faults may lead to the loss of the safety function.

Design Features:

- ❒ Directional control valve WV1 has a locked position in mid-position, adequate positive overlap and spring centring.
- ❒ Stop valves WV3 and WV4 are screwed as far down in the cylinder as possible, pilot-controlled by valve WV2.
- ❒ The safety-oriented switching position is achieved by removing the control signal in each case.
- ❒ Signal processing for pressure monitoring (DS1) may take place in a single-channel PLC for example.

Application:

- ❒ In the case of medium to high risks, e.g. if the hazard zone is entered on a regular basis and if there is a relatively high probability that the hazard can still be averted by other measures.

Further References:

- ❒ *Kleinbreuer, W.:* Konstruierte Sicherheit, Anforderungen an hydraulische und pneumatische Maschinensteuerungen. fluid (1992) Nr. 11/12.

Pneumatic Control Systems
Example for EN 954 – Category 3

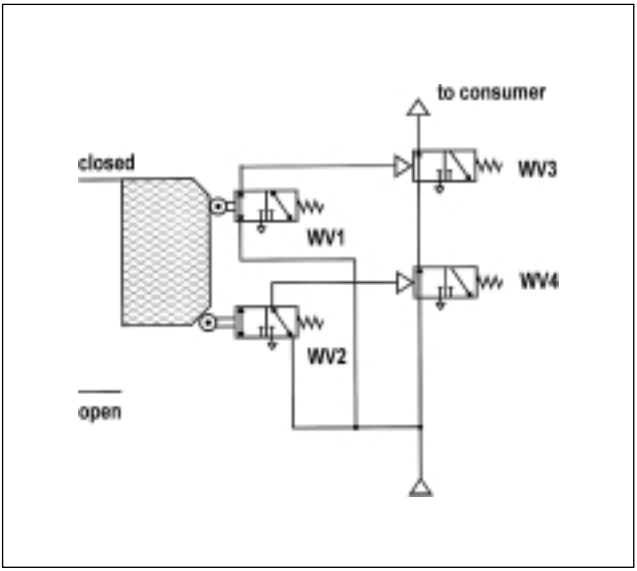


Figure 33:
Pneumatic Control System as per EN 954 – Category 3
Interlocking of movable safety guards

Functional Description:

- ❒ Interlocking of movable safety guard is monitored by two "pneumatic position switches" (WV1 and WV2). These each issue a control command to the directional control valves, WV3 and WV4.
- ❒ Energy supply (pneumatic) is only provided when the safety device is closed.
- ❒ Failure of one of the directional control valves does not lead to the loss of the safety function.
- ❒ No fault detection measures are specified (in accordance with a risk evaluation). Some faults are detected as a function of operation. An accumulation of undetected faults may lead to the loss of the safety function.

Design Features:

- ❒ WV2 is a pneumatic position switch, with forcible actuation by the movable safety guard, in accordance with EN 1088.
- ❒ The safety-oriented switching position of the directional control valves, WV3 and WV4, is achieved by removing the control signals.

Application:

- ❒ In the case of medium to high risks, e.g. if the hazard zone is entered on a regular basis and if there is a relatively high probability that the hazard can still be averted by other measures.

Further References:

- ❒ *Kleinbreuer, W.:* Anforderungen an hydraulische und pneumatische Maschinensteuerungen. Sichere Chemiearbeit (1992) Nr. 2 und Nr. 3.
- ❒ EN 1088: Sicherheit von Maschinen – Verriegelungseinrichtungen in Verbindung mit trennenden Schutzeinrichtungen – Leitsätze für Gestaltung und Auswahl

Pneumatic Control Systems
Example for EN 954 – Category 3

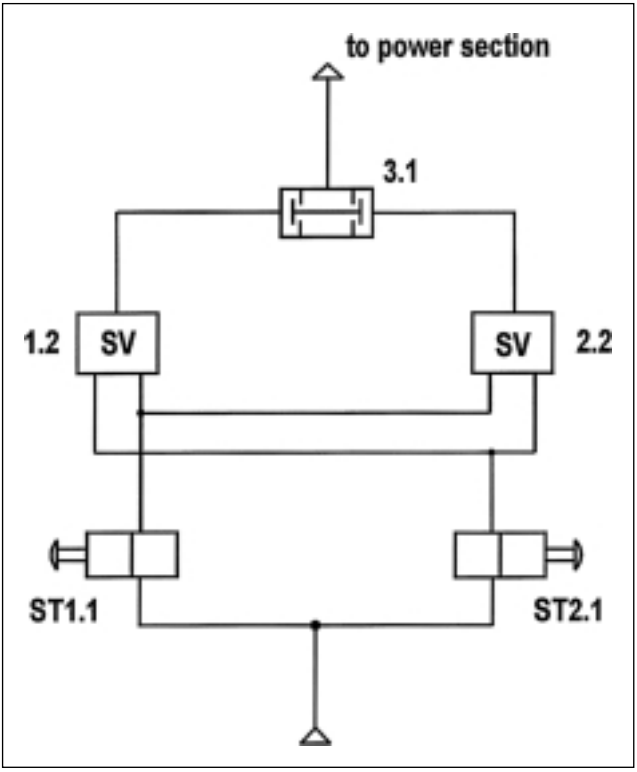


Figure 34:
Pneumatic Control System as per EN 954 – Category 3, for two-hand control, achieved by two "commercially available two-hand modules"

Functional Description:

- Potentially dangerous movements and states are controlled by synchronous actuation of operating elements ST1.1 and ST2.1 via the signal processing devices, SV, by a control signal at the output of the AND element 3.1.
- Failure of one signal processing device, SV, does not lead to the loss of the safety function.
- No fault detection measures are specified (in accordance with a risk evaluation). Some faults are detected as a function of operation. An accumulation of undetected faults can lead to the loss of the safety function.

Design Features:

- Pneumatic signal processing devices SV1.2 and SV2.2 consist of "commercially available two-hand modules".
- The safety-oriented switching position for the pneumatic components is achieved by removing the control signals.
- Signal processing devices SV1.2 and SV2.2 fulfil the requirements with respect to the relationship between input signals and output signal, termination of the output signal, regeneration of the output signal and synchronous actuation in accordance with prEN 574.

Application:

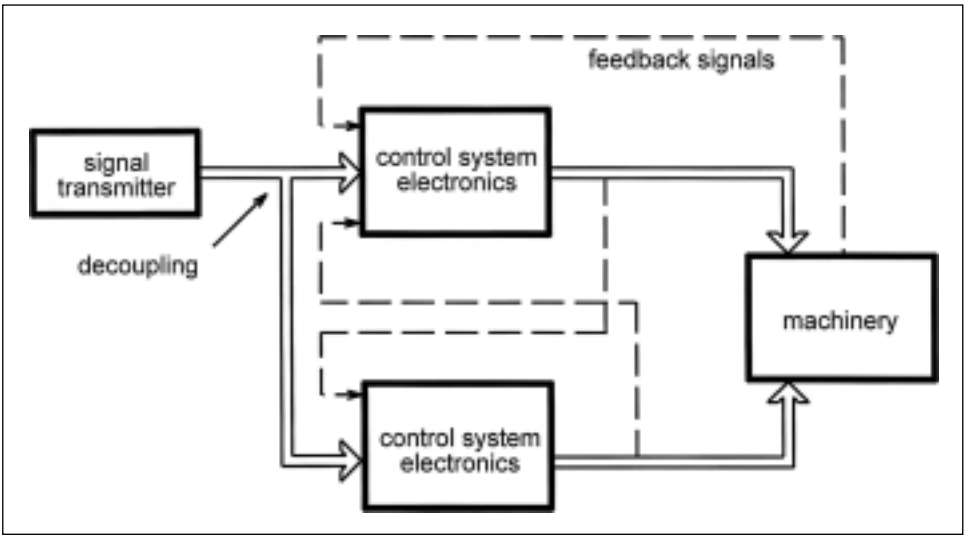
- In the case of medium to high risks, e.g. if the hazard zone is entered on a regular basis and if there is a relatively high probability that the hazard can still be averted by other measures.

Further References:

- *Kleinbreuer, W.; Kühlem, W.:* Pneumatische Zweihandschaltungen, Technische Realisierung und Ergebnisse von experimentellen Untersuchungen. Sicherheitstechnisches Informations- und Arbeitsblatt 330 242. In: BIA-Handbuch 18. Lfg. VI/92. Erich Schmidt Verlag, Bielefeld
- prEN 574: Sicherheit von Maschinen, Zweihandschaltungen, Funktionelle Aspekte – Gestaltungsleitsätze

Electronic Control Systems
Example for EN 954 – Category 3

Figure 35:
Electronic Control System as per EN 954 – Category 3
Outline structure of the control system



Functional description:

- ❒ Potentially dangerous movements or states are controlled by two channels, working independently of each other but as a function of the signal transmitter.
- ❒ Fault detection is performed for the peripheral elements.
- ❒ An unbalance in the output signals or detection of a fault in the peripheral elements causes the safety function to be triggered.

Design Features:

- ❒ Machinery reaction monitored with respect to its safety-related behaviour via the feedback signals.
- ❒ Feedback possible via contacts with connected movement
- ❒ Depending on the machinery reaction, many plausibility checks can often be used for fault detection purposes.
- ❒ Static signal transmitters must also be designed on a redundant basis.
- ❒ When wiring the signal transmitters in both channels, care should be taken to ensure that the inputs are decoupled (e.g. by decoupling diodes) in such a way that a fault in one channel does not cause the other channel to fail in the same way.

Application:

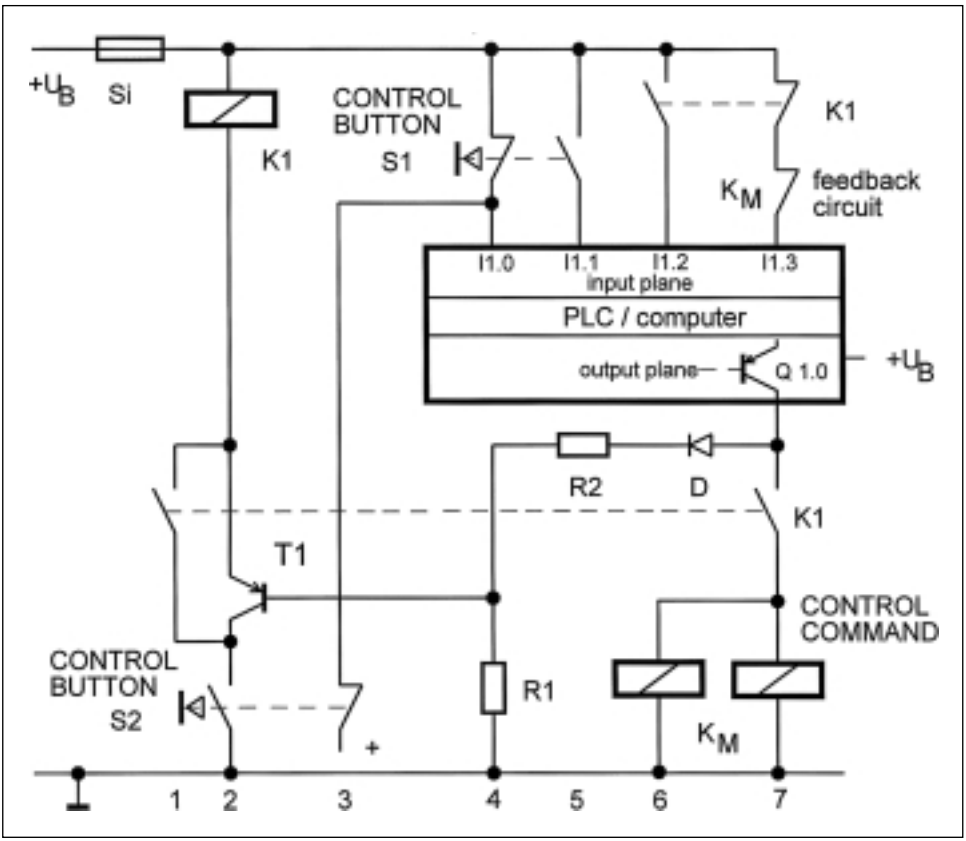
- ❒ In the case of medium to high risks, e.g. if the hazard zone is entered on a regular basis and if there is a relatively high probability that the hazard can still be averted by other measures.

Further References:

- ❒ *Jürs, H.; Reinert, D.:* Elektronik in der Sicherheitstechnik. Sicherheits-technisches Informations- und Arbeitsblatt 330 220. In BIA-Handbuch 20. Lfg. V/93. Erich Schmidt Verlag, Bielefeld
- ❒ *Grigulewitsch, W.; Meffert, K.:* Redundante Schaltungstechniken. Sicherheitstechnisches Informations- und Arbeitsblatt 330 226. In BIA-Handbuch, 10. Lfg. X/88. Erich Schmidt Verlag, Bielefeld

Computer Control Systems
Example for EN 954 – Category 3

Figure 36:
Computer Control System as per EN 954 – Category 3
Two-hand control circuit achieved by a standard PLC as per prEN 574 type II **without** time settings for synchronous actuation



Functional Description:

- A potentially hazardous movement or state can only be initiated by actuating both controls, S1 and S2, by causing K1 to go into self-locking mode and switching on Q 1.0 (the two-hand condition is achieved solely by the software).
- Before pressing controls S1 and S2, the output, Q 1.0, is switched to LOW potential and K1 is de-energized. This thus prevents a control command being issued on a redundant basis.
- An incorrect HIGH potential at Q 1.0 causes K1 to drop out permanently after the release of S2-transistor T1 blocks – and not only prevents a control command from arising but also prevents further control commands being issued when S2 is actuated again.
- Single-handed control is not possible as a result of any fault in the fault list.
- Almost complete fault detection in the peripheral elements is achieved by inputs I1.1, I1.2 and I1.3.

Design Features:

- Buttons with double contacts are provided for both controls, which means that an intentional actuation of the buttons remains a prerequisite for a valid control command even in the event of a contact not opening. Mechanical failure of one of the controls is picked up by reset monitoring.
- K1 is a relay with contacts with connected movement.
- All relay / contactor coils have been fitted with arc suppressors to ensure safe function of the circuit.

Application:

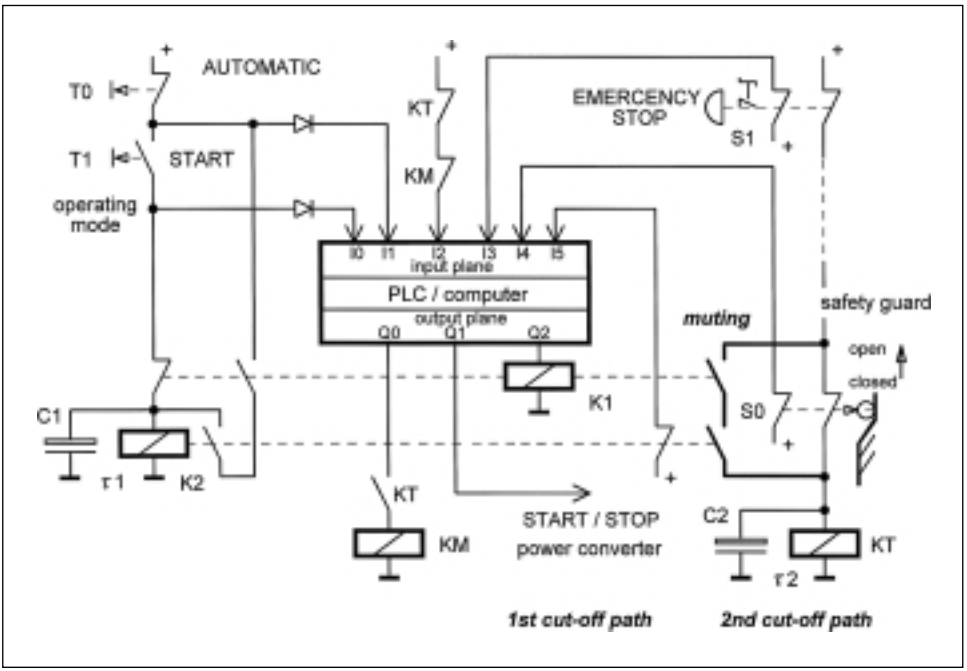
- In the case of medium to high risks, e.g. if the hazard zone is entered on a regular basis and if there is a relatively high probability that the hazard can still be averted by other measures.

Further References:

- *Grigulewitsch, W.; Reinert, D.:* Zweihandschaltungen nach Anforderungsstufe II in DIN 24 980. Sicherheitstechnisches Informations- und Arbeitsblatt 330 229. In: BIA-Handbuch 17. Lfg. X / 91. Erich Schmidt Verlag, Bielefeld

Computer Control Systems
Example for EN 954 – Category 3

Figure 37:
Computer Control System as per EN 954 – Category 3
Permanent muting of a safety guard contact during setting-up mode when using a standard PLC, e.g. when keying at a speed which has been reduced to a safe level



Functional Description:

- Potentially hazardous movements or states are prevented or interrupted with the aid of a programmable logic controller (PLC) and separate hardware when the safety guard is opened. The forcibly actuated position switch, S0, is then actuated and the relay / contactor, KT, is de-energized after a delay. As KT drops out, the mains contactor, KM, is de-energized and thus the power supply to the drive mechanism for the power converter, which is not illustrated in the diagram, is interrupted.
- Muting the normally closed contact, S0, which causes de-energization of relay / contactor KT, is performed on a redundant basis, i.e. on the one hand, it is controlled by the PLC (output Q2) with relay K1, whilst on the other hand, it is performed independently of the PLC with relay K2.
- Contactors KT and KM having dropped out and the opened safety guard are prerequisites for keying at a safely reduced speed. When the START key, T1, is actuated, K2 only switches to self-locking mode if K1 has first dropped out and then responded again within a set time of $\tau 1$, as controlled by the PLC. Only when both relays have responded is muting of the safety guard monitoring contact, S0, achieved and the START key, T1, can be released. When contactor KT responds, the mains contactor, KM, can also be energized. This is the precondition for triggering a machinery movement by setting the PLC output, Q1 (START signal for power converter).
- Fault detection is performed for the peripheral elements, K1, K2, KT and KM, via the PLC software and leads to operations being halted. Permanent muting of the safety guard is thus effectively prevented.

Design Features:

- Switch S0 is a forcibly opening position switch in accordance with EN 1088.
- Relays K1, K2, KT and KM have contacts which have connected movement.
- Programming follows a modular structure documented in ladder diagramms.

Application:

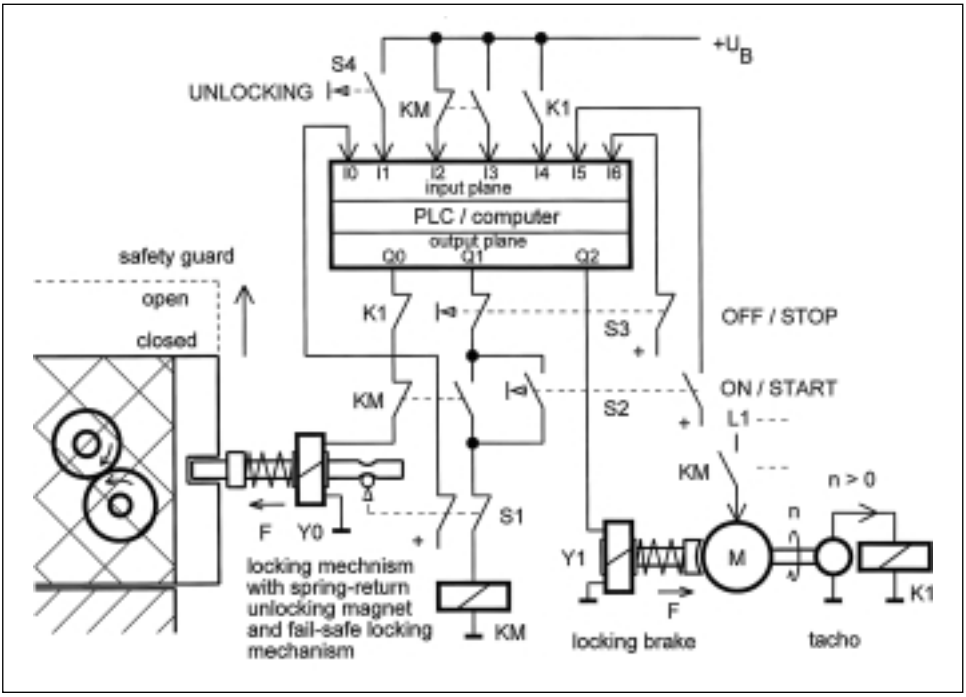
- In the case of medium to high risks, e.g. if the hazard zone is entered on a regular basis and if there is a relatively high probability that the hazard can be averted by other measures.

Further References:

- *Grigulewitsch, W.; Reinert, D.:* Schaltungsbeispiele mit speicherprogrammierbaren Steuerungen zur Umsetzung der Steuerungskategorie 3. Sicherheitstechnisches Informations- und Arbeitsblatt 330 227. In: BIA-Handbuch 24. Lfg. I / 95. Erich Schmidt Verlag, Bielefeld

Computer Control Systems
Example for EN 954 – Category 3

Figure 38:
Computer Control System as per EN 954 – Category 3
Locking a safety guard with a standard PLC



Functional Description:

- The safety guard must be closed as a prerequisite for initiating a potentially hazardous machinery movement. Opening the guard is only possible by drawing back the bolt when the unlocking magnet, Y0, is energized.

- Position monitoring for the locking bolt is achieved solely via the forcibly opening position switch, S1. A normally closed contact, S1, is scanned directly by the PLC via input I0. The other normally closed contact acts directly on the motor contactor, KM, which has normally open and normally closed contacts which are each connected to an input of the PLC (I2 / I3).

- When the ON / START key, S2, is actuated, the PLC first activates the output, Q2, responsible for releasing the blocking brake via input I5, then the motor contactor, KM, is triggered by setting the output, Q1. When KM responds, S2 can be released. KM switches to self-locking mode, both in the PLC output plane and in the PLC input plane via scanning of the normally open contact, KM, with input I3. The tacho signal which is activated when KM has responded energizes the connected relay, K1, at a speed in excess of n > 0, which displays the motor's regulation rotation at input I4 of the PLC.

- An OFF / STOP command which is issued by actuating key S3 has the direct effect of stopping the motor contactor, KM, from triggering, and thus self-locking, in output circuit Q1 of the PLC. Closing the normally closed contact, KM, at input I2 starts a pre-set braking period in the user program, after which the magnetic coil, Y1, is switched out of circuit by resetting the PLC output, Q2. The motor brake engages due to spring tension and finds its resting position. The pre-set braking period is measured such that the machinery movement has always come to a standstill, even under the most unfavourable operating conditions, before the brake engages.

- Prerequisites for opening the safety guard, before which the locking mechanism must be unlocked by the PLC, are that the motor contactor, KM, should have dropped out before actuating key S4 (UNLOCKING) (input I2 controls HIGH potential), the pre-set braking period incorporated in the PLC user program should have expired and a signal should have been issued confirming that the movement has come to a standstill (input I4 controls LOW potential). Only then does the PLC user program activate output Q0 and cause the magnetic coil, Y0, to be energized, and thus the locking bolt to be drawn back, by the flow of current through the normally closed contacts, KM and K1.

- In the event of the PLC failing, the safety guard is prevented from opening, because the current required to unlock the locking mechanism cannot flow through the magnetic coil, Y0, because of relay K1, which is energized in this situation.

- A single failure of the locking mechanism is picked up – as is the failure of the tacho generator and / or relay K1 or motor contactor KM – by plausibility checks and time settings in the PLC user program and the safety guard is locked or the potentially hazardous movement is stopped as a result.

Design Features:

- In the safety position, the guard is connected positively with the locking bolt of the locking mechanism which protrudes into the frame of the gate and is thus held in the locked position.

- Switch S1 is a forcibly opening position switch in accordance with EN 1088. The wiring to the position switch is protected.

- Relays K1, KM, have contacts with connected movement.

- Programming follows a modular structure as documented in ladder diagrams.

Application:

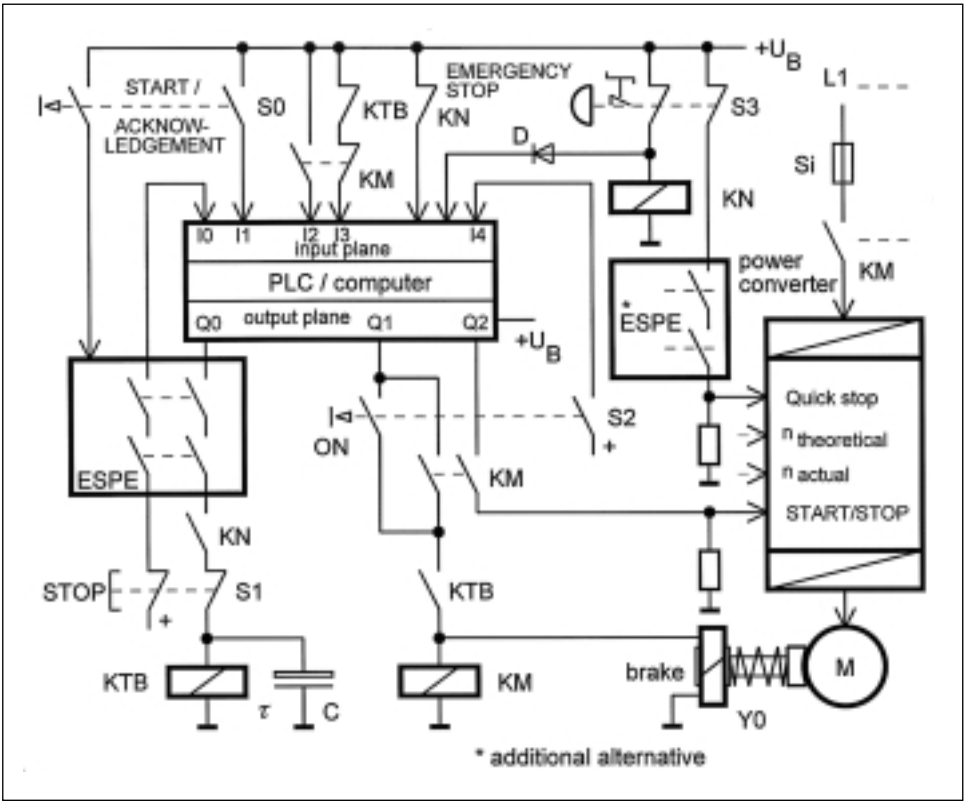
- In the case of medium to high risks, e.g. if the hazard zone is entered on a regular basis and if there is a relatively high probability that the hazard can still be averted by other measures.

Further References:

- *Grigulewitsch, W.; Reinert, D.:* Schaltungsbeispiele mit speicherprogrammier- baren Steuerungen zur Umsetzung der Steuerungskategorie 3. Sicherheits-technisches Informations- und Arbeitsblatt 330 227. In: BIA-Handbuch 24. Lfg. I/95 Erich Schmidt Verlag, Bielefeld

Computer Control Systems
Example for EN 954 – Category 3

Figure 39:
Computer Control System as per EN 954 – Category 3
Stopping an PLC-controlled converter drive mechanism in accordance with STOP category 1 in EN 60 204:
– after an emergency stop command,
– after a stop command or
– when a safety device has responded (in this case, electrosensitive protective device ESPD).



Functional Description:

- A potentially hazardous movement is prevented or interrupted on a redundant basis if one of the safety devices or the emergency stop switch has been actuated. In an emergency, after actuating an emergency stop switch, the drive mechanism is stopped as quickly as possible by, in the first instance, the "quick stop" input which is provided on the converter. Only after the expiry of a period of time which is pre-set in the PLC (start of pre-set time with LOW potential at input I5), is the mains contactor, KM, de-energized and the brake, Y0, engaged by re-setting the PLC outputs, Q0 to Q2. In parallel with these processes, the contactor, KN, is de-energized by opening the normally closed contact for the emergency stop switch, as a result of which first the timing element, KTB / C and then, in turn, KM are caused to drop out independently of the PLC as a function of the contacts.
- Stopping the drive mechanism correctly during operation after a STOP command or when a safety device has responded, is initiated by cancelling the START / STOP signal for the converter (LOW potential) with PLC output Q2 (1st cut-off path!). Breaking the circuit at contactor KTB / C, which is associated with a safety device responding or with a STOP command, starts a pre-set braking period and once this has expired, the trigger mechanism for the mains contactor, KM, is interrupted (2nd cut-off path!). The pre-set time is selected such that the machinery movement comes to a standstill before the mains contactor, KM, drops out, even under unfavourable conditions.
- In the event of failure of the PLC, the converter or the timing element, KTB, the drive mechanism is guaranteed to stop in each instance because there are always two independent cut-off paths.
- If the contactors, KM, KN or KTB, do not drop out, this is picked up no later than before a further machinery movement is initiated thanks to the system which exists within the PLC for scanning the normally closed contacts with connected movement.

Design Features:

- All the safety devices used correspond to at least Category 3.
- The relays / contactors, KN, KTB and KM, have contacts with connected movement.
- Programming follows a modular structure documented in ladder diagrams.

Application:

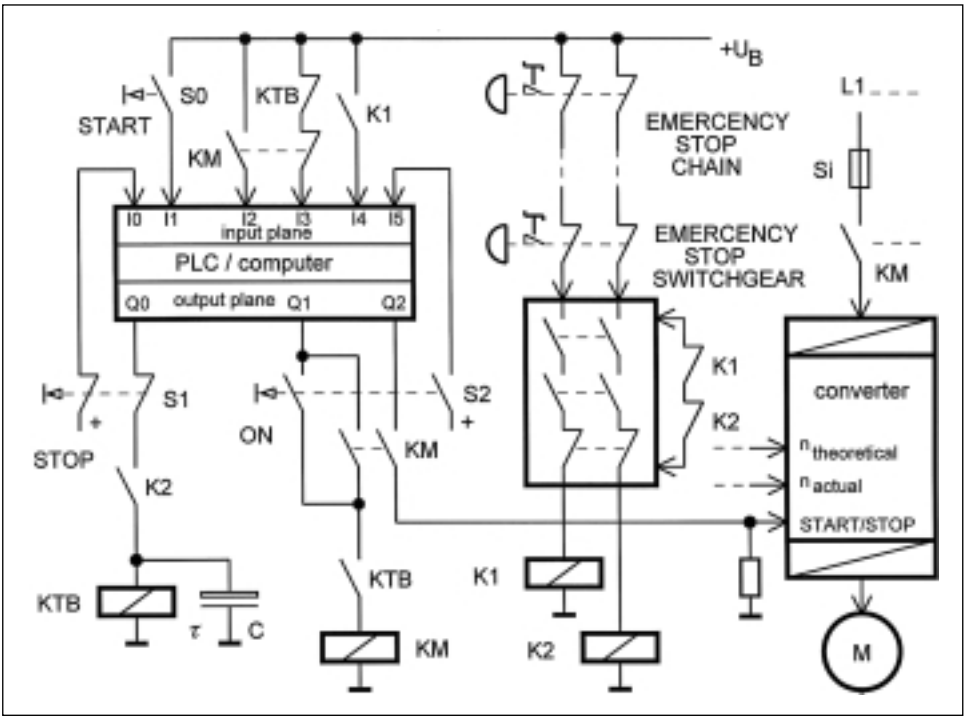
- In the case of medium to high risks, e.g. if the hazard zone is entered on a regular basis and if there is a relatively high probability that the hazard can still be averted by other measures.

Further References:

- *Grigulewitsch, W.; Reinert, D.:* Schaltungsbeispiele mit speicherprogrammierbaren Steuerungen zur Umsetzung der Steuerungskategorie 3. Sicherheits-technisches Informations- und Arbeitsblatt 330 227. In: BIA-Handbuch 24. Lfg. I / 95. Erich Schmidt Verlag, Bielefeld

Computer Control Systems
Example for EN 954 – Category 3

Figure 40:
Computer Control System as per EN 954 – Category 3
Stopping an PLC-controlled converter drive mechanism in accordance with STOP category 1
in EN 60 204 after an emergency stop command



Functional Description:

- A potentially hazardous movement is prevented or interrupted on a redundant basis if one of the safety devices or the emergency stop switch is actuated. In an emergency, after actuating an emergency stop switch, the drive mechanism is stopped as quickly as possible by first de-activating the emergency stop switchgear, whilst at the same time de-energizing the contactors, K1 and K2. Opening the normally open contact, K1, at PLC input I4 causes the START signal for the converter to be cancelled (PLC output Q2 controls LOW potential; 1st cut-off path!). Opening the normally open contact, K2, in front of the timing element, KTB / C starts a pre-set braking period and once this has expired, the trigger mechanism for the mains contactor, KM, is interrupted (2nd cut-off path!). The pre-set time is selected such that the machinery movement comes to a standstill before the mains contactor, KM, drops out, even under unfavourable conditions. Stopping the drive mechanism correctly during operation after a STOP command is initiated by opening the normally closed contacts for STOP key S1 and scanning these by PLC input I0. The shutdown of the converter begins by re-setting the PLC output, Q2, in the same way as when stopping in an emergency.
- In the event of a single failure of the PLC, the converter, the timing element, KTB / C, or the contactors, K1 / K2, the drive mechanism is guaranteed to stop on each occasion because there are always two independent cut-off paths. If the contactors, KM or KTB, do not drop out, this is picked up no later than before a further machinery movement is initiated thanks to the existing system of feedback of normally closed contacts with connected movement to PLC input I3. If contactors K1 and K2 do not drop out, this is picked up no later than after unlocking the actuated emergency stop switch by monitoring the normally closed contacts within the emergency stop switchgear.

Design Features:

- All the safety devices used correspond to at least Category 3.
- The relays / contactors, KN, KTB and KM, have contacts with connected movement.
- Programming follows a modular structure documented in ladder diagrams.

Application:

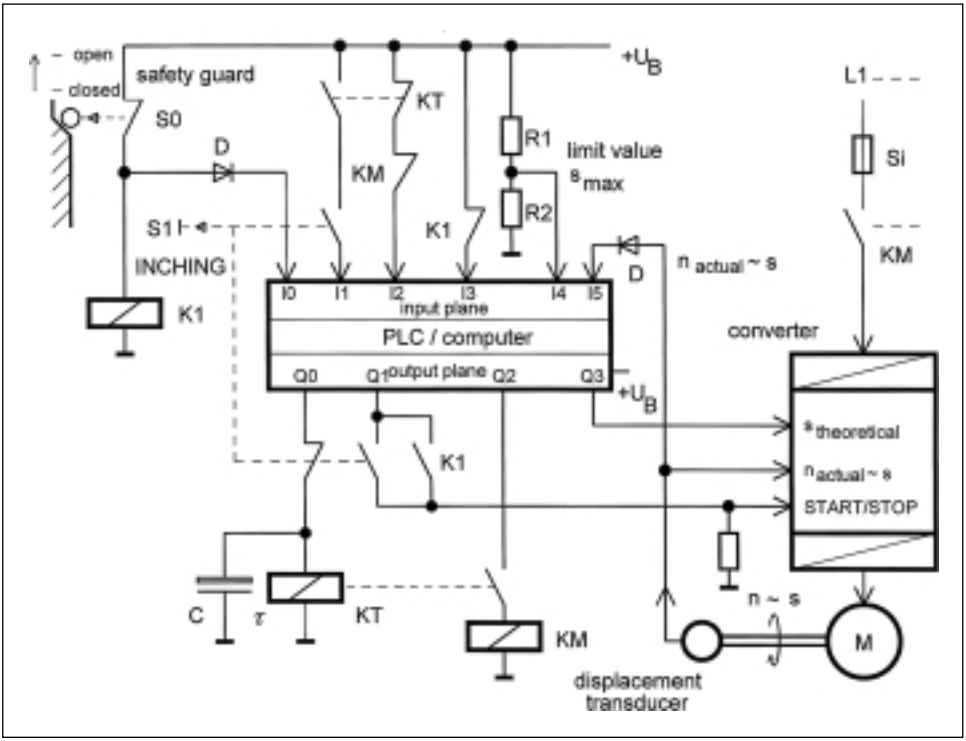
- In the case of medium to high risks, e.g. if the hazard zone is entered on a regular basis and if there is a relatively high probability that the hazard can still be averted by other measures.

Further References:

- *Grigulewitsch, W.; Reinert, D.:* Schaltungsbeispiele mit speicherprogrammierbaren Steuerungen zur Umsetzung der Steuerungskategorie 3. Sicherheitstechnisches Informations- und Arbeitsblatt 330 227. In: BIA-Handbuch 24. Lfg. I / 95. Erich Schmidt Verlag, Bielefeld

Computer Control Systems
Example for EN 954 – Category 3

Figure 41:
Computer Control System as per EN 954 – Category 3
Limited distance inching mode with PLC and separate timing element for monitoring the distance during setting-up operation



Functional description:

- A potentially hazardous movement is prevented or interrupted on a redundant basis when the safety guard is opened. When the safety guard is opened, limited distance inching mode is actuated. The forcibly opening position switch, S0, is then actuated and the relay / contactor, K1, is de-energized. The START / STOP signal for the converter can only be activated by the PLC output, Q1, if the INCHING key, S1, is actuated. The theoretical limit value specified for the distance, s_{max}, at PLC output I4 only appears once and is passed on to the converter in the form of digital information via PLC output Q3. The timing element, KT / C, which takes the form of separate hardware, is also triggered whenever the INCHING key, S1, is actuated as a redundant means of determining the distance travelled.
- In the event of failure of the PLC, the converter, the displacement transducer or in the event of an incorrect theoretical limit value specification, the motor drive mechanism is guaranteed to shut down no later than after the expiry of the set time thanks to the timing element, KT / C, which overrides these devices. Failure of the timing element, KT / C (e.g. in the event of KT not dropping out) is picked up by the PLC (input I2), as is a situation in which KM does not drop out, by scanning of the normally closed contacts with connected movement. These relays / contactors must drop out after each occasion on which the converter is gradually shut down as a condition for the drive mechanism to be started up again.

Design Features:

- K1, K2, KT and KM are relays / contactors with contacts with connected movement.
- Programming follows a modular structure documented in ladder diagrams.

Application:

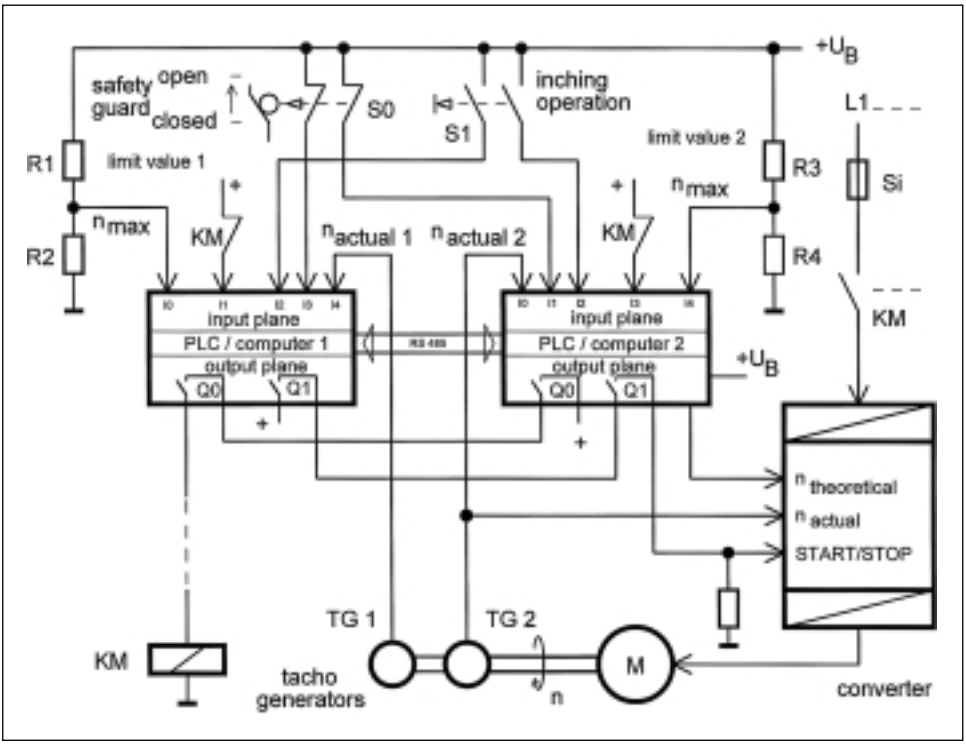
- In the case of medium to high risks, e.g. if the hazard zone is entered on a regular basis and if there is a relatively high probability that the hazard can still be averted by other measures.

Further References:

- *Grigulewitsch, W.; Reinert, D.:* Schaltungsbeispiele mit speicherprogrammierbaren Steuerungen zur Umsetzung der Steuerungskategorie 3. Sicherheitstechnisches Informations- und Arbeitsblatt 330 227. In BIA-Handbuch 24. Lfg. I / 95. Erich Schmidt Verlag, Bielefeld

Computer Control Systems
Example for EN 954 – Category 3

Figure 42:
Computer Control System as per EN 954 – Category 3
PLC redundancy for the purpose of generating a safely reduced speed with a separate theoretical / actual value comparison in each of the processing channels and separate frequency limit value specifications



Functional Description:

- A potentially hazardous movement is prevented or interrupted on a redundant basis when the safety guard is opened. A reduced speed is actuated when the safety guard is opened. Both processing channels receive theoretical limit value specifications which are completely independent of each other at inputs I0 (PLC1) and I4 (PLC2). Scanning of the actual frequency of the reduced speed is also performed by independently operating tacho generators at inputs I4 (SPC1) and I0 (SPC2). Each channel performs the comparison of theoretical / actual values on an independent basis.
- A serial interface (e.g. RS 485) is provided for the purpose of exchanging data, including safety-related data, e.g. for fault detection by comparing the states of the two PLCs and / or computers.
- In the event of one of the processing channels failing, the converter and the mains contactor are switched down by the other channel which is still operational. A failure of the converter, which may, for example, lead to unexpected starting up, continued operation or to an increase in the frequency, is detected via the separate frequency recording systems by tacho generators TG1 and TG2 in both processing channels. If the mains contactor, KM, does not drop out, this is picked up by the normally closed contacts in both PLCs and / or computers (inputs I1 or I3) and causes the START / STOP signal for the converter to be blocked by both processing channels. Faults or malfunctions of the interface are controlled with a medium degree of effectiveness by test patterns or tests in the transmission protocol, for example.

Design Features:

- KM is a relay / contactor with contacts with connected movement.
- Programming follows a modular structure documented in ladder diagrams.

Application:

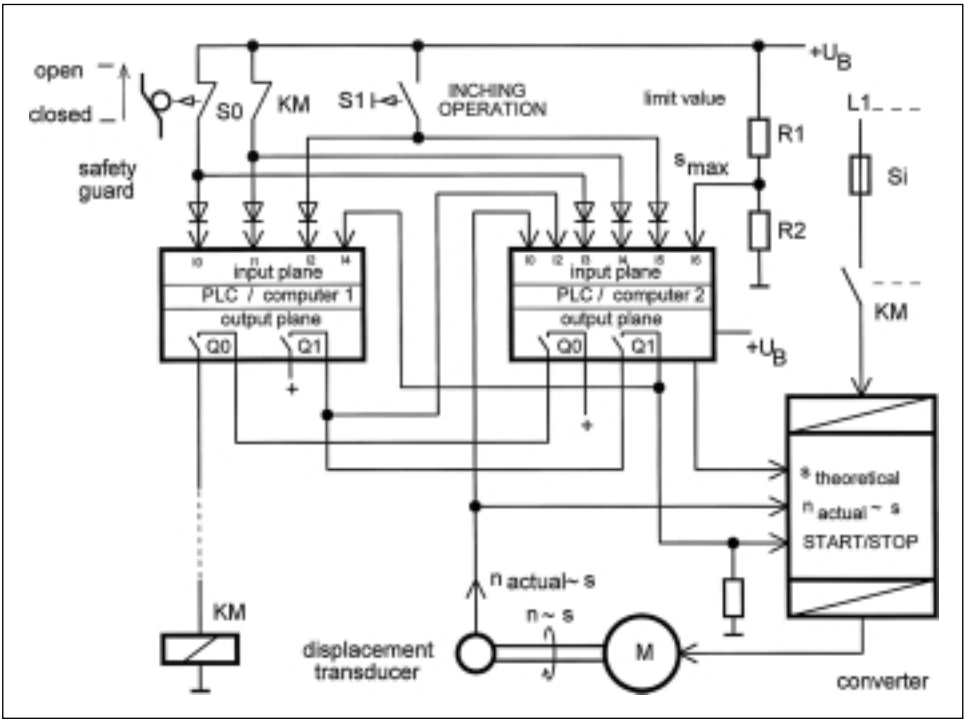
- In the case of medium to high risks, e.g. if the hazard zone is entered on a regular basis and if there is a relatively high probability that the hazard can still be averted by other measures.

Further References:

- *Grigulewitsch, W.; Reinert, D.:* Schaltungsbeispiele mit speicherprogrammierbaren Steuerungen zur Umsetzung der Steuerungskategorie 3. Sicherheitstechnisches Informations- und Arbeitsblatt 330 227. In: BIA-Handbuch, 24. Lfg. I / 95. Erich Schmidt Verlag, Bielefeld

Computer Control Systems
Example for EN 954 – Category 3

Figure 43:
Computer Control System as per EN 954 – Category 3
Limited distance INCHING MODE with PLC redundancy and output comparison



Functional Description:

- A potentially hazardous movement is prevented or interrupted on a redundant basis when the safety guard is opened. Limited distance inching operation is actuated when the safety guard is opened. The theoretical limit value specified for the distance, s_{max}, only appears once and is passed on to the converter by PLC2 in the form of digital information at output Q2. Only the time is specified in PLC1 as a redundant measure for distance recording in PLC2.
- If the distance is exceeded, the converter is first switched down via output Q1 of PLC2 by cancelling the START / STOP signal for the converter. Within its pre-set time, PLC1 waits for this START / STOP signal to be cancelled. If shut-down by PLC2 does not occur, PLC1 takes over this operation by resetting output Q1. The mains contactor, KM, is also de-energized by PLC1 via output Q0.
- In the event of failure of PLC2, the converter, the displacement transducer or in the event of an incorrect theoretical limit value specification, the motor drive mechanism is guaranteed to shut down no later than after the expiry of the set time in PLC1 via outputs Q1 and Q0.
- Failure of one of the PLCs or of a computer is picked up by plausibility checks in both processing channels thanks to feedback of the outputs and due to the fixed sequence for triggering and gradually shutting down the converter. If the mains contactor, KM, does not drop out, this is picked up by the normally closed contact, KM, which is scanned by the two processing channels (inputs I1 to I3). By switching off the START / STOP input for the converter (LOW potential!) by both PLC outputs, Q1, the machinery movement is brought to a standstill in the event of a fault and starting up again is prevented by storing the defective state.

Design Features:

- The necessary decoupling (no feedback) between the processing channels is ensured by the diodes which are marked at the inputs.
- KM is a relay / contactor with contacts with connected movement.
- Programming follows a modular structure documented in ladder diagrams.

Application:

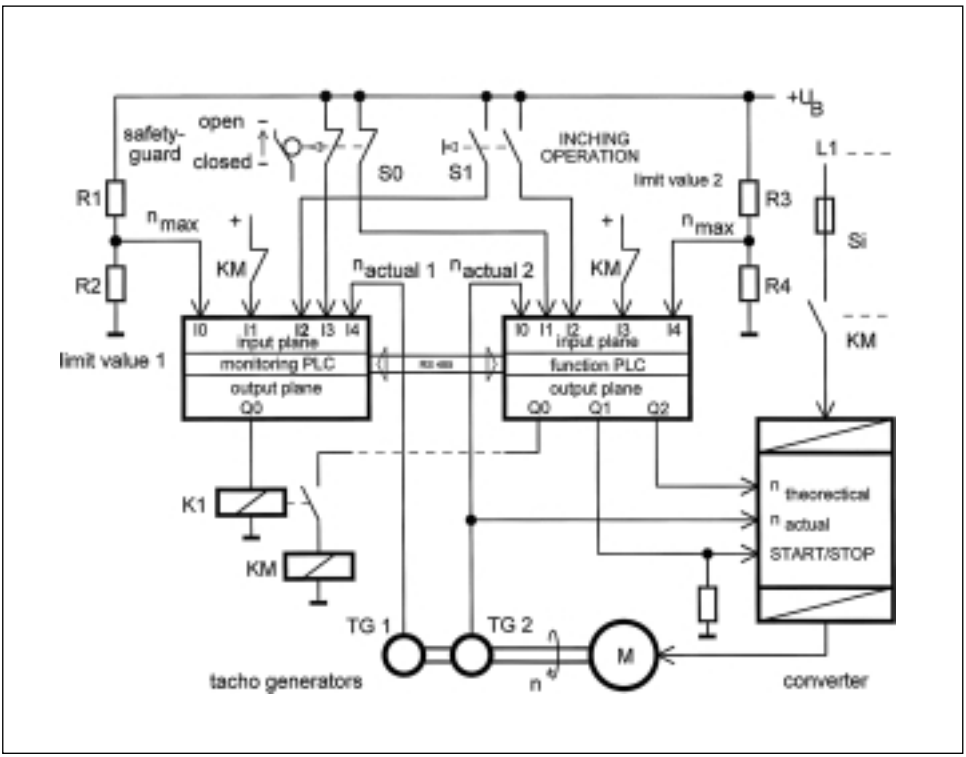
- In the case of medium to high risks, e.g. if the hazard zone is entered on a regular basis and if there is a relatively high probability that the hazard can still be averted by other measures.

Further References:

- *Grigulewitsch, W.; Reinert, D.:* Schaltungsbeispiele mit speicherprogrammierbaren Steuerungen zur Umsetzung der Steuerungskategorie 3. Sicherheitstechnisches Informations- und Arbeitsblatt 330 227. In: BIA-Handbuch, 24. Lfg. I / 95. Erich Schmidt Verlag, Bielefeld

Computer Control Systems
Example for EN 954 – Category 3

Figure 44:
Computer Control System as per EN 954 – Category 3
"cold" stand-by, i.e. non-functional PLC redundancy



Functional Description:

- A potentially hazardous movement is prevented or interrupted on a redundant basis when the safety guard is opened. Limited distance inching operations is actuated when the safety guard is opened. All safety-related input signals are provided on a redundant basis and are read in by both the function PLC and by the monitoring PLC. All safety-related signals are checked for plausibility (correct time and value within specified tolerances) in the monitoring PLC.
- The monitoring PLC is also in a position to scan status information in the different operating modes and to check its correctness by means of a serial interface (RS 485).
- In fault-free operation, the contactor, K1, always stays in the responded position, in other words, after de-energization of the mains contactor, KM, for example. Only when faults or malfunctions occur during the course of the production process will the monitoring channel intervene actively in operation of the machinery, de-energize K1 and thus KM, and hence finally cause the entire piece of machinery to come to a standstill.
- Fault detection is only possible for the function PLC by the monitoring PLC. Automatic testing of the monitoring PLC's cut-off ability is **not** possible, as the monitoring PLC only executes its safety-related function when the function PLC fails. The safety function of the monitoring PLC must be checked within the specified testing and maintenance intervals when the machinery or plant is at a standstill.

Design Features:

- Faults in connecting the two channels via the serial interface are detected by test patterns (signature) and thus prevent incorrect data from being output to the monitoring PLC.
- As communication takes place without feedback, a fault which has occurred in one channel cannot lead to the failure of the other channel and thus to the failure of the entire system.
- KM / K1 are relays / contactors with contacts with connected movement.
- Programming follows a modular structure documented in ladder diagrams.

Application:

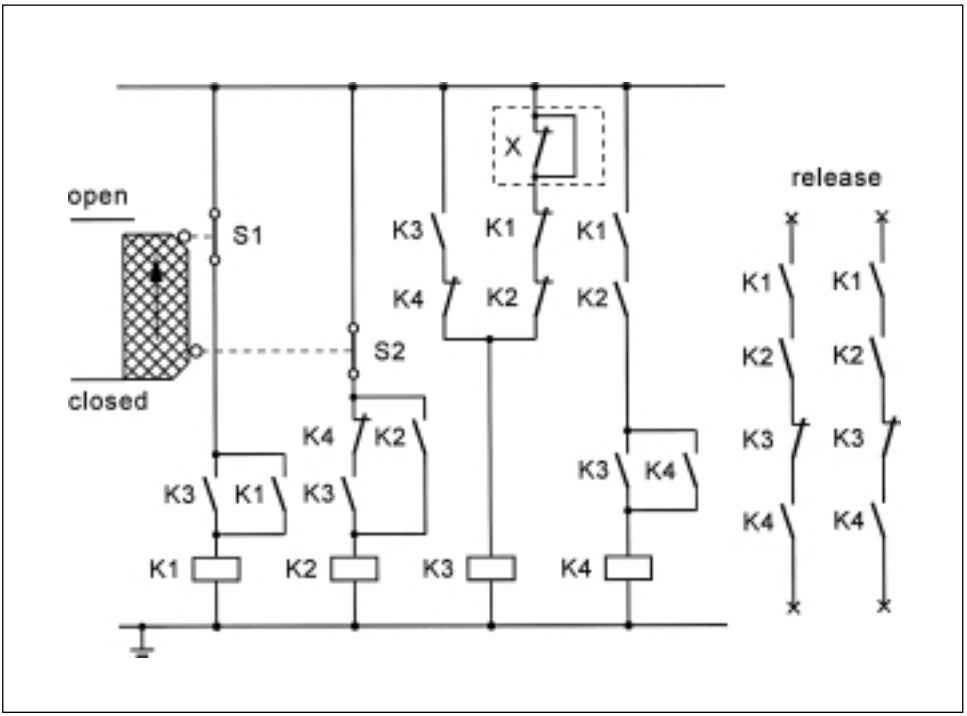
- In the case of medium to high risks, e.g. if the hazard zone is entered on a regular basis and if there is a relatively high probability that the hazard can still be averted by other measures.

Further References:

- *Grigulewitsch, W.; Reinert, D.:* Schaltungsbeispiele mit speicherprogrammierbaren Steuerungen zur Umsetzung der Steuerungskategorie 3. Sicherheitstechnisches Informations- und Arbeitsblatt 330 227. In: BIA-Handbuch, 24. Lfg. 1 / 95. Erich Schmidt Verlag, Bielefeld

Electromechanical Control Systems
Example for EN 954 – Category 4

Figure 45:
Electromechanical Control System as per EN 954 – Category 4
Position monitoring of movable safety guards



Functional Description:

- ❒ Potentially hazardous movements or states are interrupted or prevented by a combination of normally closed and normally open contacts when the safety guard is opened.
- ❒ It is not necessary to perform a start-up test by opening and closing the safety device.
- ❒ The safety function is also fulfilled if a component failure occurs. All faults, in accordance with the fault list, are detected during operation or when the safety device is actuated (opened and closed) by interrupting release.
- ❒ An accumulation of faults between two consecutive actuation times may lead to the loss of the safety function.
- ❒ The circuit can be extended in the area marked with an "X" for the purpose of monitoring power contactors and contactors to duplicate the release path.

Design Features:

- ❒ All safety-related parts of the control system are designed on a redundant basis.
- ❒ Switch S1 is a forcibly opening position switch in accordance with EN 1088.
- ❒ The control contactors, K1 / K2 / K3 / K4 have contacts with connected movement.
- ❒ Separate wiring is installed for the position switches S1 / S2.
- ❒ Category 4 is only observed if several mechanical position switches for various safety devices are not connected in series (cascading), as otherwise fault detection in switches and wires is not possible.

Application:

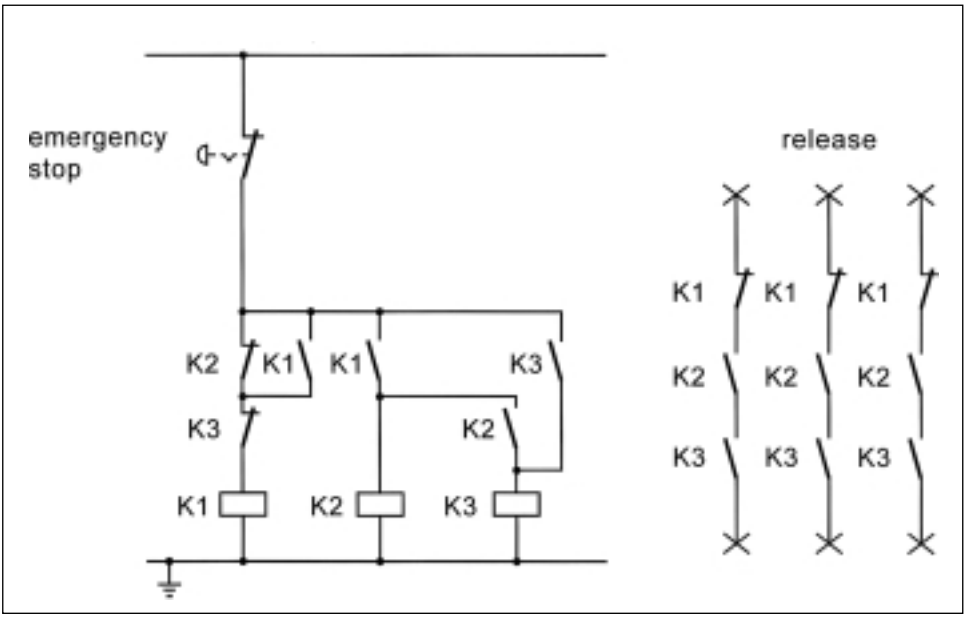
- ❒ In the case of high risks, e.g. if the hazard zone is entered on a regular basis and if there is a low probability that the hazard can still be averted by other measures.

Further References:

- ❒ *Kreutzkampf, F.; Hertel, W.:* Zusammenstellung und Bewertung elektromechanischer Sicherheitsschaltungen für Verriegelungseinrichtungen. Sicherheitstechnisches Informations- und Arbeitsblatt 330 212. In: BIA-Handbuch 17. Lfg. X / 91. Erich Schmidt Verlag, Bielefeld

Electromechanical Control Systems
Example for EN 954 – Category 4

Figure 46:
Electromechanical Control System as per EN 954 – Category 4
Emergency stop device
Fault exclusion for emergency stop switches and wires



Functional Description:

- ❒ Potentially hazardous movements or states are stopped by a self-monitoring contactor combination when the emergency stop devices are actuated.
- ❒ The following fault exclusions are made when assessing the category:
  – non-interruption of the emergency stop switching contact on actuation,
  – bridging of the emergency stop switch by a short-circuit in the wiring.
- ❒ The safety function of the contactor combination is fulfilled if a component failure occurs. All faults, in accordance with the fault list, are detected during operation or when the emergency stop switch is actuated by interrupting release.
- ❒ An accumulation of faults between two consecutive actuation times may lead to the loss of the safety function.

Design Features:

- ❒ The control station and operating element work according to the principle of forcible actuation (EN 418).
- ❒ The control contactors, K1 / K2 / K3, have contacts with connected movement.
- ❒ Fault exclusion is only possible if emergency stop switches and wires are not exposed to any particular hazards.

Application:

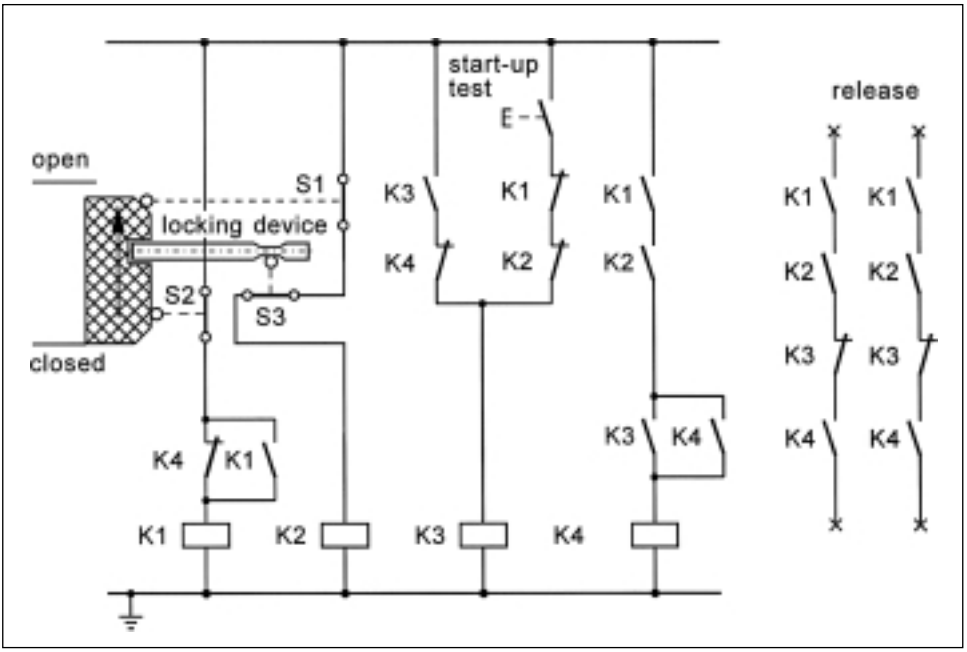
- ❒ In the case of high risks, if disconnecting the power supply suddenly does not lead to hazardous states (stop-category 0 as per EN 60204-1).
- ❒ If fault exclusion (see above) is not possible, control stations and wires may be designed on a redundant basis (double-pole). In this case, signal processing must be extended or replaced by a double-pole emergency stop monitoring device.

Further References:

- ❒ not known.

Electromechanical Control Systems
Example for EN 954 – Category 4

Figure 47:
Electromechanical Control System as per EN 954 – Category 4
Position monitoring of movable safety guards with locking and start-up testing



Functional Description:

❒ Potentially hazardous movements or states are interrupted or prevented by a combination of normally closed and normally open contacts when the safety guard is opened.

- ❒ Locking devices (locking mechanisms) are also monitored by position switches which are operated forcibly.
- ❒ There is a start-up test procedure which must be performed when the safety device is opened.
- ❒ The safety function is also fulfilled if a component failure occurs. All faults, in accordance with the fault list, are detected during operation or when the safety device is actuated (opened and closed) by interrupting release.
- ❒ An accumulation of faults between two consecutive actuation times may lead to the loss of the safety function.
- ❒ If the position of the safety device is also detected forcibly at the same time by the position monitoring system for the locking device (S3) (failsafe locking mechanism), S1 may be dropped.

Design Features:

- ❒ All safety-related parts of the control system for monitoring the position of the safety device are designed on a redundant basis.
- ❒ Switches S1 and S3 are forcibly opening position switches in accordance with EN 1088.
- ❒ The control contactors, K1 / K2 / K3 / K4 have contacts with connected movement.
- ❒ Separate wiring is installed for position switches S1 / S2 / S3.
- ❒ Category 4 is only observed if several mechanical position switches for various safety devices are not connected in series (cascading), as otherwise fault detection in switches and wires is not possible.
- ❒ The locking device may, for example, be controlled by time-related systems (threaded bolts, time switch) or movement-dependent systems (trouble indicators).

Application:

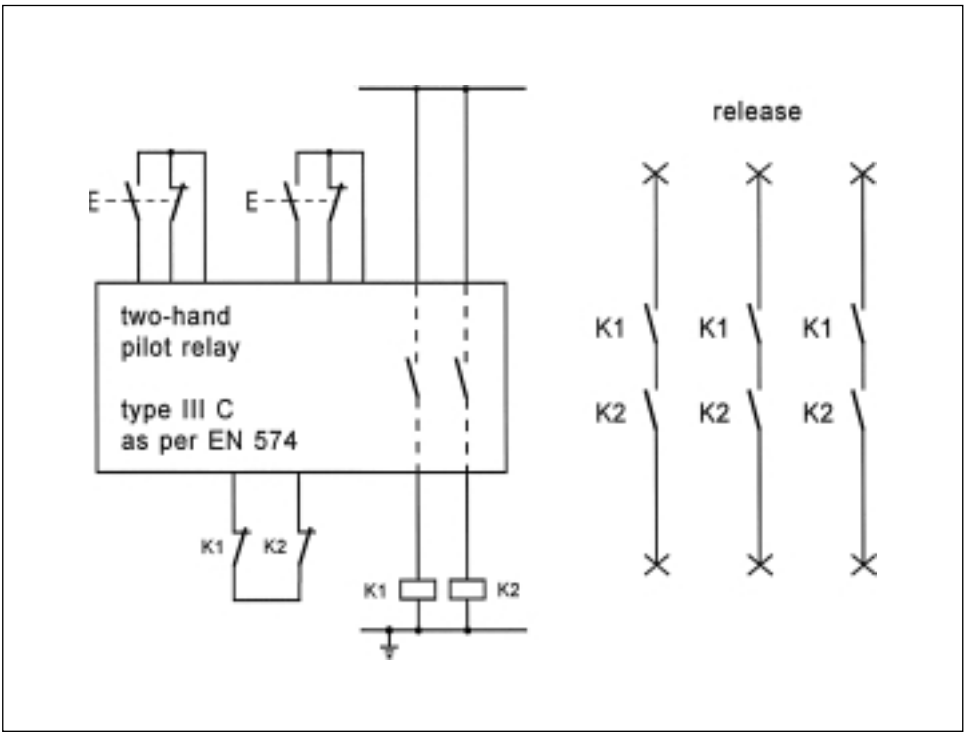
- ❒ In the case of high risks, e.g. if the hazard zone is entered on a regular basis and if there is a low probability that the hazard can still be averted by other measures. The circuit can be used with guards which must be closed and remain locked for long enough to ensure that there is no longer any risk of injury as a result of hazardous machine functions.

Further References:

- ❒ *Kreutzkampf, F.; Hertel, W.:* Zusammenstellung und Bewertung elektromechanischer Sicherheitsschaltungen für Verriegelungseinrichtungen. Sicherheitstechnisches Informations- und Arbeitsblatt 330 212. In: BIA-Handbuch 17. Lfg. X / 91. Erich Schmidt Verlag, Bielefeld
- ❒ ZH1 / 153 / 10.95: Merkblatt für die Auswahl und Anbringung elektromechanischer Verriegelungseinrichtungen für Sicherheitsfunktionen. Carl Heymanns Verlag, Köln 10 / 1995

Electromechanical Control Systems
Example for EN 954 – Category 4

Figure 48:
Electromechanical Control System as per EN 954 – Category 4
Two-hand control circuit, signal processing by relay unit with series-connected control contactors



Functional description:

- ❒ Potentially hazardous movements are controlled by two-hand relay unit.
- ❒ Contact duplication is provided by K1 and K2.

Design Features:

- ❒ Relay unit corresponds to Type III C in accordance with EN 574.
- ❒ Fault detection of K1 and K2 by normally closed contacts in the feedback circuit.

Application:

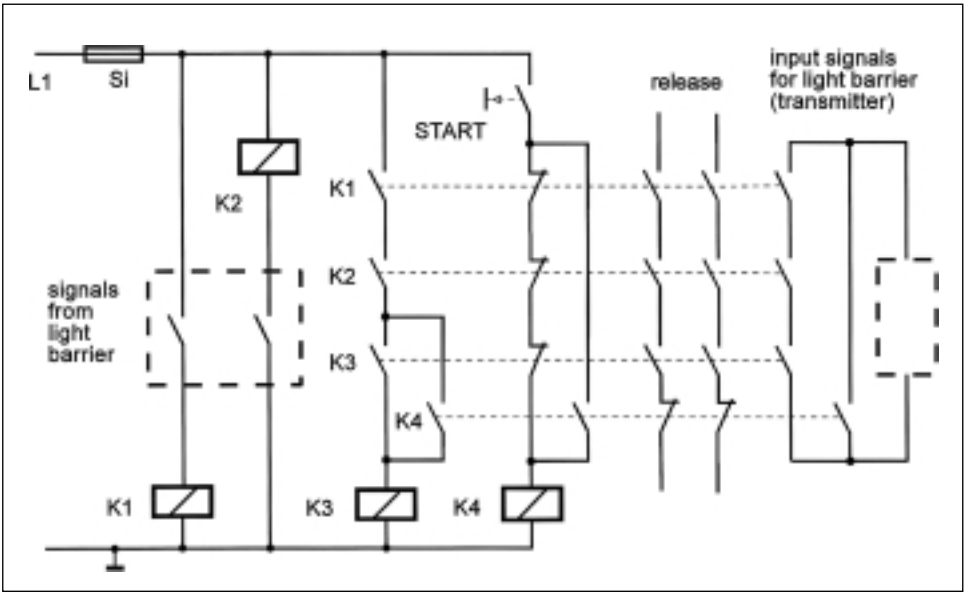
- ❒ In the case of high risks, e.g. if the hazard zone is entered on a regular basis and if there is a low probability that the hazard can still be averted by other measures.

Further References:

- ❒ not known.

Electromechanical Control Systems
Example for EN 954 – Category 4

Figure 49:
Electromechanical Control System as per EN 954 – Category 4
Integration of safety-related signals in the machinery control system using a light barrier by way of example



Functional Description:

- ❒ The safety-related signals from the light barrier (2 normally open contacts) switch the control contactors, K1 and K2, which have a different coil connection.
- ❒ One normally open contact from each of K1 and K2 is located in the release path and also in the input circuit for starting the light barrier transmitter.
- ❒ When the light barrier signals have been interrupted, the contactors, K1, K2, K3, must be deliberately tested by the start key and the transmitter must receive a new start command.
- ❒ Faults in the control contactors, K1, K2, K3 (welding together) and K4 (dropping out) and bridging of the start key are detected and cause release to be prevented no later than at the "start" stage.
- ❒ An accumulation of faults between two consecutive start times may lead to the loss of the safety function.

Design Features:

- ❒ The control contactors, K1, K2, K3 and K4 have contacts with connected movement.
- ❒ Short-circuits between different signal lines cause the fuse (Si) to respond as a result of the different coil connections for K1 and K2. This is why it is not necessary to have a separate wiring route for each signal.

Application:

- ❒ In the case of high risks, e.g. if the hazard zone is entered on a regular basis and if there is a low probability that the hazard can still be averted by other measures.

Further References:

- ❒ not known.

Hydraulic Control Systems
Example for EN 954 – Category 4

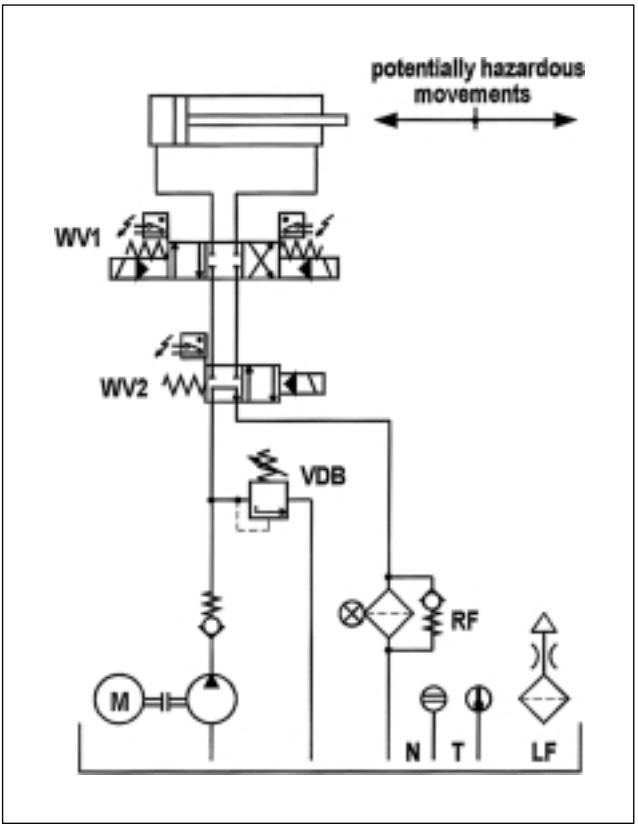


Figure 50:
Electrohydraulic Control System as per EN 954 – Category 4 for the control of potentially hazardous movements

Functional Description:

- ❒ Potentially hazardous movements or states are controlled by **two** directional control valves (WV1 and WV2).
- ❒ Failure of one of the directional control valves does not lead to the loss of the safety function.
- ❒ Both directional control valves are triggered cyclically.
- ❒ A fault detection measure is specified for each of the two directional control valves. Failure of both directional control valves is detected; after a fault, initiation of the next potentially hazardous movement is prevented.

Design Features:

- ❒ Both directional control valves (WV1 and WV2) have locked position in mid-position, adequate positive overlap, spring centring and return and also electrical position monitoring.
- ❒ The safety-oriented switching position is achieved by removing the control signal in each instance.
- ❒ Signal processing for electrical position monitoring devices complies with the corresponding requirements for the fault in question.

Application:

- ❒ In the case of high risks, e.g. if the hazard zone is entered on a regular basis and if there is a low probability that the hazard can still be averted by other measures.

Further References:

- ❒ *Kleinbreuer, W.:* Sicherheitstechnisch abgestufte Steuerungen in der Fluidtechnik. Die BG (1994) Nr. 3
- ❒ *Gorgs, K.-J.; Kleinbreuer, W.*; *Kühlem, W.:* Fehlerlisten für hydraulische und pneumatische Bauelemente – Bei der Prüfung unterstellte Fehlerarten. Sicherheitstechnisches Informations- und Arbeitsblatt 340 225. In: BIA-Handbuch, 14. Lfg. VI/90 und 15. Lfg. XI/90. Erich Schmidt Verlag, Bielefeld

Pneumatic Control Systems
Example for EN 954 – Category 4

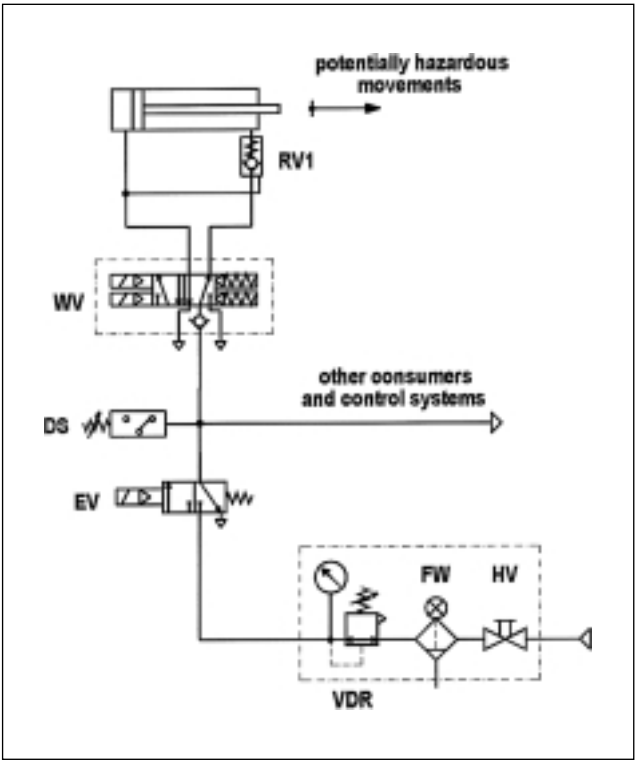


Figure 51:
Electropneumatic Control System as per EN 954 – Category 4 for the control of potentially hazardous movements

Functional Description:

- A potentially hazardous movement or a potentially hazardous state is controlled by a self-monitoring valve combination, WV, in conjunction with an unlockable non-return valve, RV1 (important if compressed air and external power supplies fail).
- One component failure within the valve combination does not lead to the loss of the safety function.
- Both pilot valves in the valve combination are triggered separately. When one control signal / both control signals have been removed, the movement is always reversed.
- A single fault within the valve combination is detected; initiation of the next potentially hazardous movement is prevented.

Design Features:

- WV is a self-monitored valve combination with mechanically separate pilot valves and fault detection by pneumatic / mechanical means with integrated non-return valve in the P-line.
- The safety-oriented switching position is achieved by removing the control signals.
- The unlockable non-return valve, RV1, should be screwed as far down in the cylinder as possible.
- Fault detection within the valve combination complies with the corresponding requirements against faults.

Application:

- In the case of high risks, e.g. if the hazard zone is entered on a regular basis and if there is a low probability that the hazard can still be averted by other measures.

Further References:

- *Kleinbreuer, W.:* Sicherheitstechnisch abgestufte Steuerungen in der Fluidtechnik. Die BG (1994) Nr. 3
- *Gorgs, K.-J.; Kleinbreuer, W.*; *Kühlem, W.:* Fehlerlisten für hydraulische und pneumatische Bauelemente – Bei der Prüfung unterstellte Fehlerarten. Sicherheitstechnisches Informations- und Arbeitsblatt 340 225. In: BIA-Handbuch 14. Lfg. VI / 90 and 15. Lfg. XI / 90 Erich Schmidt Verlag, Bielefeld

Pneumatic Control Systems
Example for EN 954 – Category 4

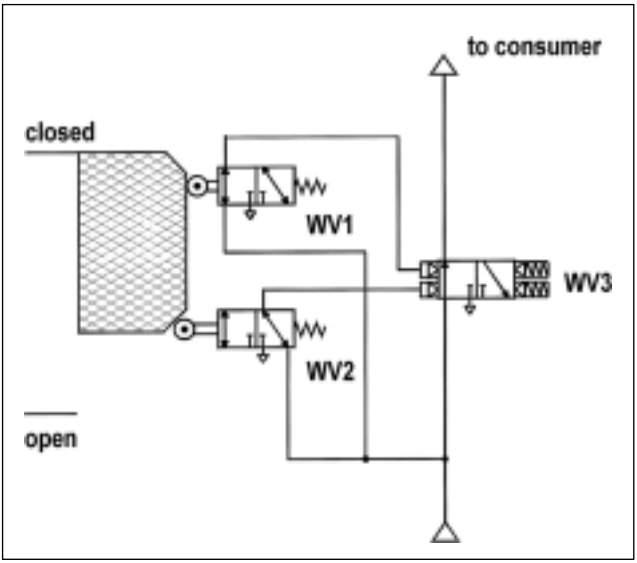


Figure 52:
Pneumatic Control System as per EN 954 – Category 4
Interlocking of movable safety guard

Functional Description:

- ❒ Interlocking of movable safety guard is monitored by two "pneumatic position switches" (WV1 and WV2). These each issue a control command to the self-monitoring valve combination, WV3.
- ❒ Energy supply (pneumatic) is only provided when the safety device is closed.
- ❒ Failure of one component does not lead to the loss of the safety function.

Design Features:

- ❒ WV2 is a pneumatic position switch with forcible actuation by the movable safety guard, in accordance with EN 1088.
- ❒ The safety-oriented switching position of the valve combination, WV3, is achieved by removing one control signal / both control signals.
- ❒ WV1 / WV2 is a self-monitored valve combination with mechanically separate pilot valves and fault detection by pneumatic / mechanical means.
- ❒ Fault detection within the valve combination complies with the corresponding requirements against faults.

Application:

- ❒ In the case of high risks, e.g. if the hazard zone is entered on a regular basis and if there is a low probability that the hazard can still be averted by other measures.

Further References:

- ❒ *Kleinbreuer, W.:* Anforderungen an hydraulische und pneumatische Maschinensteuerungen. Sichere Chemiearbeit (1992) Nr. 2 und Nr. 3
- ❒ EN 1088: Sicherheit von Maschinen – Verriegelungseinrichtungen in Verbindung mit trennenden Schutzeinrichtungen – Leitsätze für Gestaltung und Auswahl
- ❒ *Gorgs, K.-J.; Kleinbreuer, W.; Kühlem, W.:* Fehlerlisten für hydraulische und pneumatische Bauelelemente – Bei der Prüfung unterstellte Fehlerarten. Sicherheitstechnisches Informations- und Arbeitsblatt 340 225. In: BIA-Handbuch 14. Lfg. VI / 90 und 15. Lfg. XI / 90. Erich Schmidt Verlag, Bielefeld

Pneumatic Control Systems
Example for EN 954 – Category 4

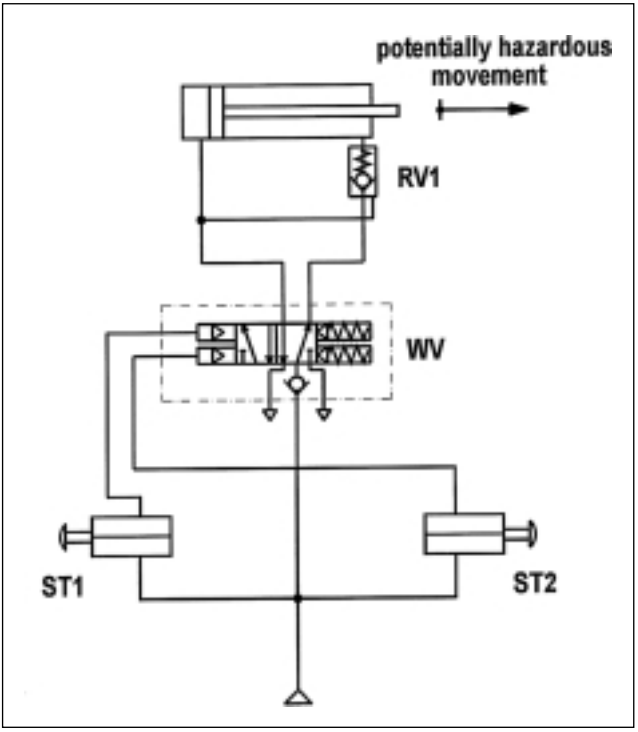


Figure 53:
Pneumatic Control System as per EN 954 – Category 4
For two-hand control, achieved by a special valve combination for direct control of the cylinder

Functional Description:

- A potentially hazardous movement or a potentially hazardous state is controlled by synchronous actuation of operating elements ST1 and ST2 by a self-monitoring valve combination, WV, in conjunction with an unlockable non-return valve, RV1 (important if compressed air and external power supplies fail).
- One component failure within the valve combination does not lead to the loss of the safety function.
- Both pilot valves in the valve combination are triggered separately. When one control signal / both control signals have been removed, the movement is always reversed.
- A single fault within the valve combination is detected; initiation of the next potentially hazardous movement is prevented.

Design Features:

- WV is a self-monitored valve combination, with mechanically separate pilot valves and fault detection by pneumatic / mechanical means with integrated non-return valve in the P-line.
- The safety-oriented switching position is achieved by removing the control signals.
- The unlockable non-return valve, RV1, should be screwed as far down in the cylinder as possible.
- The self-monitored valve combination fulfils the requirements for fault detection and with respect to the relationship between input signals and output signal, termination of the output signal, regeneration of the output signal and synchronous actuation in accordance with EN 574. The operating elements ST1 and ST2 together with their signal convertors have to release the control signal for the valve combination if the input signal is released or in the case of a fault.

Application:

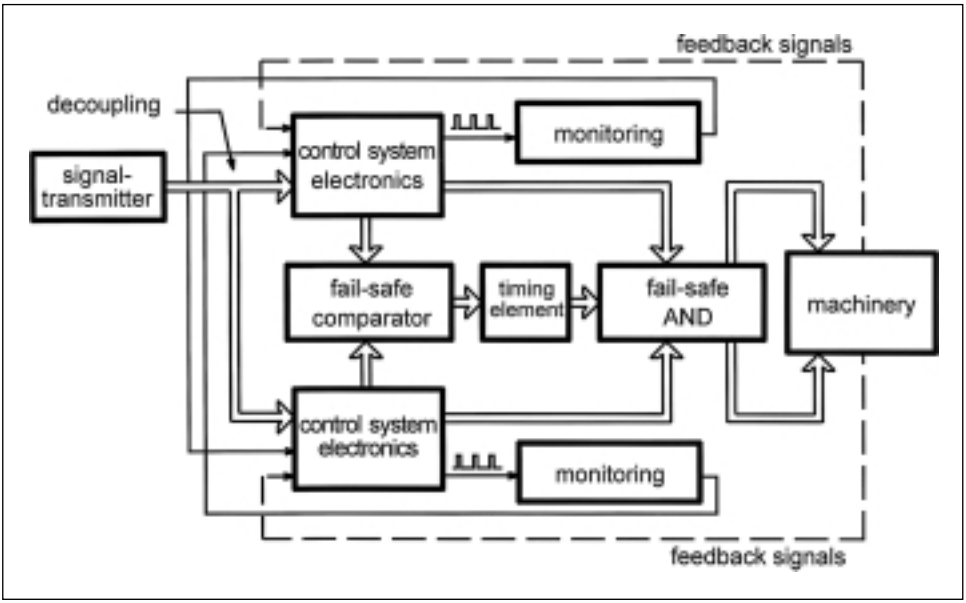
- In the case of high risks, e.g. if the hazard zone is entered on a regular basis and if there is a low probability that the hazard can still be averted by other measures.

Further References:

- *Kleinbreuer, W.:* Sicherheitstechnisch abgestufte Steuerungen in der Fluidtechnik. Die BG (1994) Nr. 3

Electronic Control Systems
Example for EN 954 – Category 4

Figure 54:
Electronic Control System as per EN 954 – Category 4
Outline structure of the control system



Functional Description:

- ❒ Potentially dangerous movements or states are controlled by two channels, working independently of each other but as a function of the signal transmitter.
- ❒ Fault detection is performed (within one hour maximum) for all components in the control system electronics by numerous inter-comparisons.
- ❒ An unbalance in the output signals or detection of a fault in one of the components causes the safety function to be triggered.

Design Features:

- ❒ The machinery reaction can be monitored on a redundant basis with respect to its safety-related behaviour via the feedback signals.
- ❒ Depending on the machinery reaction, many plausibility checks can often be used for fault detection purposes.
- ❒ Static signal transmitters are designed on a redundant basis and these components are actuated dynamically.
- ❒ When wiring the signal transmitters in both channels, care was taken to ensure that the inputs are decoupled (e.g. by decoupling diodes) in such a way that a fault in one channel does not cause the other channel to fail in the same way.

Application:

- ❒ In the case of high risks, e.g. if the hazard zone is entered on a regular basis and if there is a low probability that the hazard can still be averted by other measures.

Further References:

- ❒ *Jürs, H.; Reinert, D.:* Elektronik in der Sicherheitstechnik. Sicherheitstechnisches Informations- und Arbeitsblatt 330 220. In: BIA-Handbuch 20. Lfg. V/93. Erich Schmidt Verlag, Bielefeld
- ❒ *Grigulewitsch, W.; Meffert, K.:* Redundante Schaltungstechniken. Sicherheitstechnisches Informations- und Arbeitsblatt 330 226. In: BIA-Handbuch 10. Lfg. X/88. Erich Schmidt Verlag, Bielefeld

Computer Control Systems
Example for EN 954 – Category 4

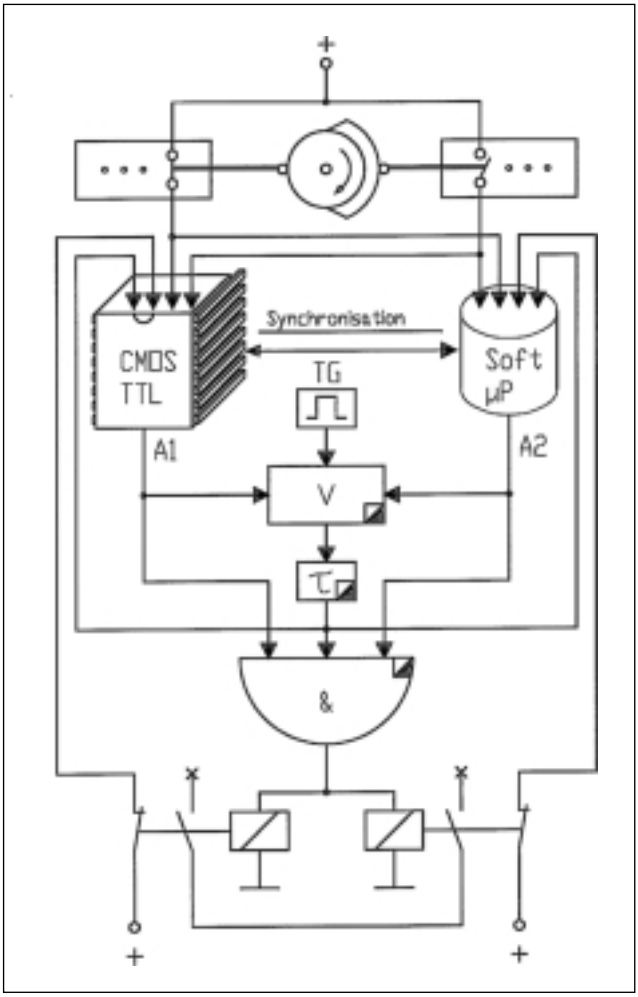


Figure 55:
Computer Control System as per EN 954 – Category 4
Control of a process with diverse redundancy with microprocessor and CMOS/TTL logic

Functional Description:

- ❒ Potentially hazardous movements or states are interrupted or prevented by two diverse channels (computer technology and TTL logic). Both channels operate independently of each other, but are synchronized.
- ❒ The process input signals are processed by both channels. It is also only possible to consider the safety-related signals in this operation.
- ❒ In the event of a component failure occurring, the safety function is still retained.
- ❒ A single component failure in one channel is picked up within one hour. To this end, a separate clock generator generates pulses which are only passed on by an equivalence comparator if signals A1 and A2 are identical. The comparator output signal and the signals from the channels are fed to the devices for triggering the potentially hazardous movements via a fail-safe AND module.

Design Features:

- ❒ The diversity of the two processing channels helps to control and avoid systematic failures in the hardware.
- ❒ However, decoupling of the processing channels also makes it necessary to obtain permission for a small time delay in addition to synchronization. The timing element, t, allows both channels non-equivalent operation for the corresponding time so as to compensate for different processing times within the channels.
- ❒ The final control elements for the potentially hazardous movements are read back via the contacts for the relays with connected movement in order to ensure a permanent shutdown by the channel.

Application:

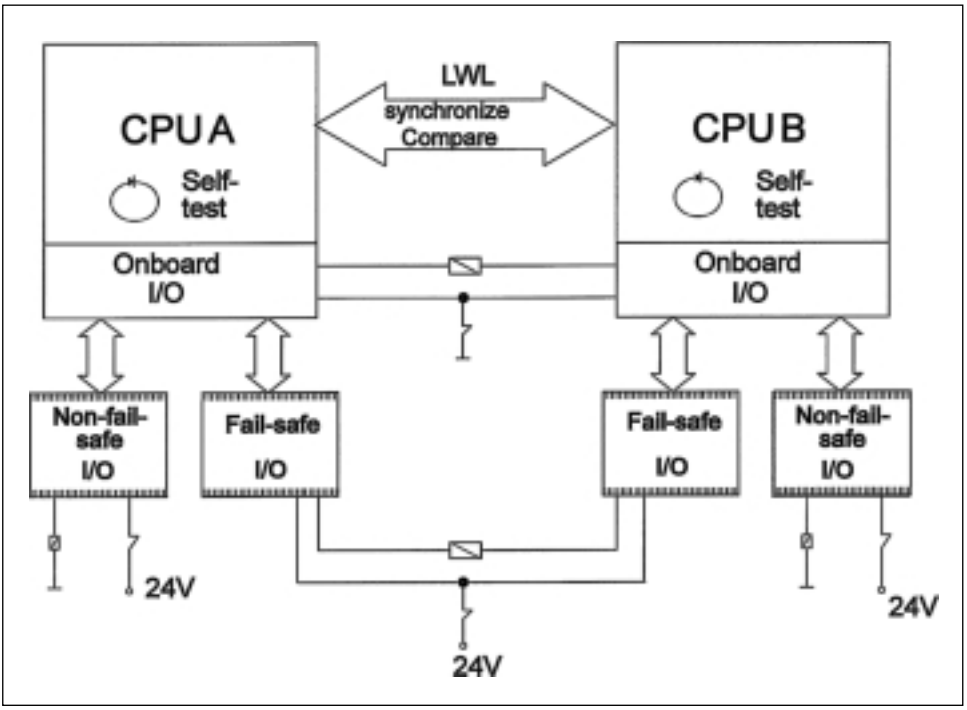
- ❒ In the case of high risks, e.g. if the hazard zone is entered on a regular basis and if there is a relatively high probability that the hazard can still be averted by other measures.

Further References:

- ❒ *Grigulewitsch, W.; Meffert, K.; Reuß, G.:* Aufbau elektrischer Maschinensteuerungen mit diversitärer Redundanz. BIA-Report 5/86. Hrsg.: Berufsgenossenschaftliches Institut für Arbeitssicherheit - BIA, Sankt Augustin.

Computer Control Systems
Example for EN 954 – Category 4

Figure 56:
Computer Control System as per EN 954 – Category 4
Freely programmable logic controller



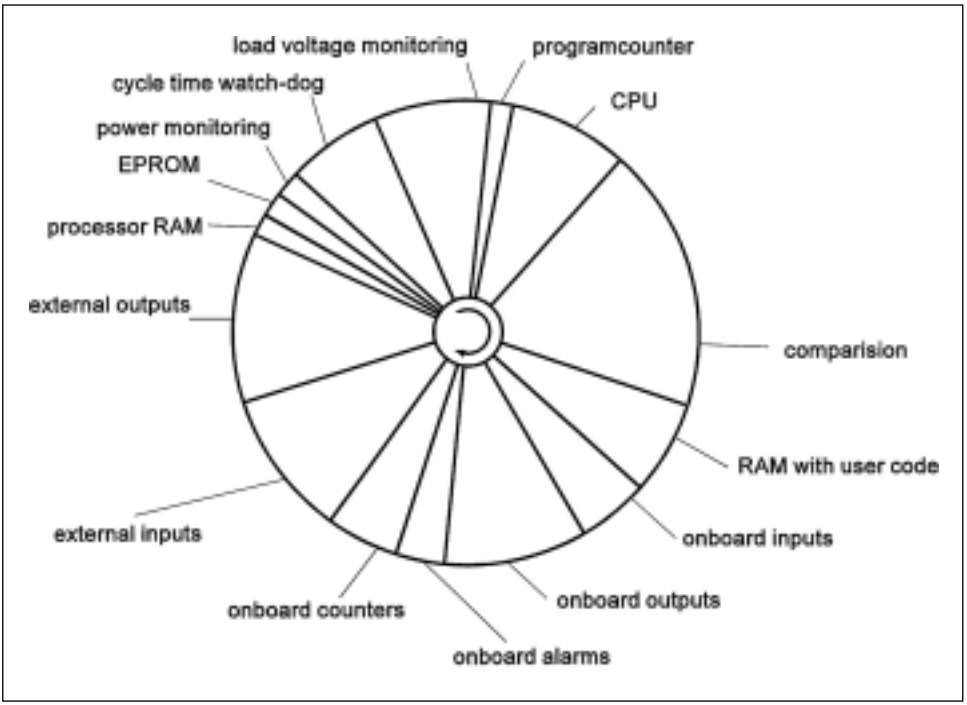
Functional Description:

- ❒ Potentially hazardous movements or states are interrupted or prevented by two identical central processing units. The central processing units can be extended by external peripheral sub-assemblies and by additional programmable logic controllers systems via a BUS system.
- ❒ In the event of a component failure occurring, the safety function is still retained.
- ❒ A single component failure in one channel is picked up within one hour. Once the fault has been detected, both channels switch all their outputs to zero potential within less than 10 ms.
- ❒ All safety-related functions are programmed in the same way in both channels. An optical fibre transmission is necessary in order to synchronize the results of the two channels. The optical fibre transmission is also used for a highly dynamic exchange and comparison process for fault detection purposes. If a comparison detects a difference, the outputs of both central processing units are set to 0 and all output cards are disconnected from the supply voltage along with their contacts.

Design Features:

- ❒ So-called on-line tests are performed for all modular units in order to monitor the correct function of each unit. All tests are performed in the background in a time slice operation. The operating system for the programmable logic controller guarantees that all sub-assemblies will have been checked completely after one hour. All tests are performed fully in each channel. Whenever the programmable logic controller system is switched to the stop state by the stop run switch or the mains switch or alternatively by a fault state, all tests are performed en bloc. Figure 57 shows the time units for the various background tests.
- ❒ CPU: Test of all registers by a walking 1 or 0, test internal processor RAM via a Galpat test divided into 16 byte units; test all CPU commands; test program counter and address calculation by the response of program islands in EPROM; time-related program run monitoring via synchronization every 5 ms.
- ❒ EPROM: signature with a width of one word via the generator polynomial $X^{16} + X^{15} + X^{12} + X^{1}$; comparison of the entire EPROM content of both channels within one hour.
- ❒ RAM with application program: Walking 0 and walking 1 and comparison with the content of the RAM memory in the second channel, part of this having been stored inversely.

Figure 57:
Background tests for computer components



- Input / output units: test all digital inputs via a walking 1 and a walking 0 using special digital outputs; the input and output data is compared by fibre optic coupling; all outputs are issued in two channels and inversely. All outputs are monitored.

- Data lines (internal communication): Special transmission protocols; information redundancy (partially inverse) with comparison in each channel.

- Power supply: All supply voltages are monitored; power down routine with storage of all safety-related data; the buffer battery for the RAM is monitored continuously.
- Cycle and program sequence: tested watchdog with separate time base without time window; mutual time and logical program run monitoring for the individual channels within 5 ms and by exchange of a program-dependent variable.
- External communication: Each data exchange via the bus system between different PLCs is monitored via a signature with a double word width (CRC) and comparison in both channels; communication with the programming device is monitored by a modification comparator and a falsification comparator; filters have been installed to protect against external electromagnetic interference phenomena and all communication is safeguarded by a transmission protocol (dynamic principle).
- All safety-related inputs and outputs must be projected before the application software can be designed. The following must be specified for each input and output on each sub-assembly: whether it is a redundant input / output, how the input is triggered, how long are the discrepancy period for the redundant inputs and outputs (i.e., the time during which redundant inputs and outputs may have different potentials) and whether a test output is used to monitor a relatively static input. All inputs / outputs are projected in this way via a menu-controlled program with which the projection exercise can also be documented accordingly. If, for example, an output, which has been projected as a redundant output, is connected in a way which is not redundant, the operating system prevents the PLC from starting the entire user program. The same thing happens if, in the two channels, the same input does not assume the same state during the discrepancy period.
- In addition, the reaction of each signal group (i.e. a group of signals which belong together from a logical point of view) in the event of a fault being detected must be specified (see Figure 58). There are five possible different reactions: switching off the signal group via an internal relay (S), ignoring all signals from this group (all inputs and outputs are set to 0) (P); continuing with the old value (L); inputting the defective signal as 0 (A) or 1 (0).

- The closed circuit principle is used for sensors. Faults are also revealed by performing an input comparison together with a test pattern for static inputs (this also detects interference from neighbouring signal lines). Faults in final control elements are detected using the closed circuit principle and mutual monitoring of redundant control elements (interference from neighbouring signal lines) is revealed.

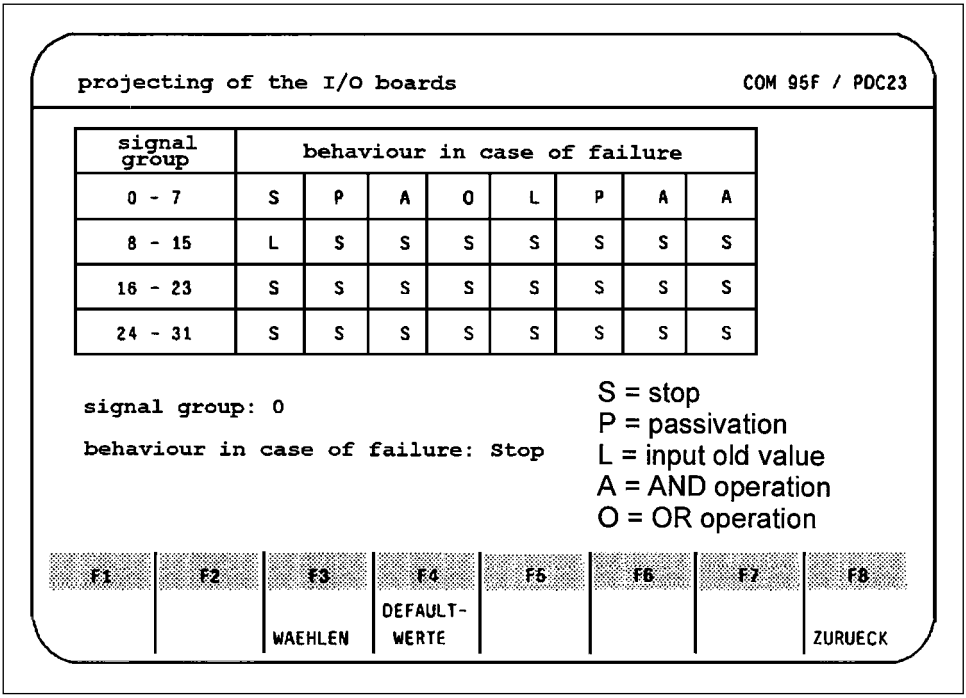
- As to simplify safety-related user programming, standard software modules have been integrated together with a specific input / output configuration. The execution of an emergency stop via the "Emergency stop" function module can be cited as an example. The two contacts for the emergency stop switch are connected to the redundant input lines of the PLC. They are also connected to an output line, to enable short-circuits in the signal lines for the emergency stop button to be revealed. The redundant contactors for the shutdown operation are triggered by redundant output channels in the PLC (one contactor with a positive output and the other with a negative output). Two normally closed contacts are used to monitor that the contactors function correctly. The function module guarantees a reaction time of 14 ms for the onboard peripherals and 135 ms for the external input / output sub-assemblies. Detailed user instructions give a detailed description of the way in which the sensors and control elements for this function module should be connected, how the various inputs / outputs must be projected and how the function module must be called by the program. Other function modules are available. None of these modules can be modified by the user. Fault during application of these function modules are minimized and it is very easy to integrate these standard modules in the safety-related application.

- Modifications to the software are often the source of hazardous faults. For this reason, a so-called modification comparator has been implemented, with the ability to check the safety-related software. This firmware compares the modified software with the previous version and marks all modified areas, thus enabling a review of the modifications to be documented.

Application:

- In the case of high risks, e.g. if the hazard zone is entered on a regular basis and if there is a low probability that the hazard can still be averted by other measures.

Figure 58:
Projecting inputs / outputs for the SPC



signal group	behaviour in case of failure							
0 - 7	S	P	A	O	L	P	A	A
8 - 15	L	S	S	S	S	S	S	S
16 - 23	S	S	S	S	S	S	S	S
24 - 31	S	S	S	S	S	S	S	S

Further References:

- *Reinert, D.; Reuß, G.:* Sicherheitstechnische Beurteilung und Prüfung mikroprozessorgesteuerter Sicherheitseinrichtungen. Sicherheitstechnisches Informations- und Arbeitsblatt 310 222. In: BIA Handbuch 17. Lfg. X/91. Erich Schmidt Verlag, Bielefeld

- *Reinert, D.; Reuß, G.; Jürs, H.; Faller, R.; Hammerschall, J.:* Validation of functional safety of programmable electronic systems according to IEC 1508 in: Pre-prints of fifth international working conference on dependable computing for critical applications. Urbana-Champaign 1995
- *Barradange, W.; Cluang, A.; Sohl, W.:* Techniques for testing the microprocessor family, in: Proceedings of the IEEE 64, H. 6, P. 943-950
- *Maehle, E.:* Entwurf von Selbsttestprogrammen für Mikrocomputer. In: Microcomputing. Berichte der Tagung III / 79 des German Chapter of the ACM / Remmele, W.; Schecher, H. (Hrsg.), Stuttgart, Teubner 1979, S. 204-216
- *Vasa, S.:* Calculating an error checking character in software. Computer Design (1976) Nr. 5

5 Conclusion

This report leaves the specialist sector in no doubt that the publication of EN 954, Part 1, does not represent a complete change in direction for safety technology for safety devices and control systems in Germany. Well-tried components and principles have already been in use in the past, circuit structures have had "start-up testing", the principle of "single fault safety" has been applied in accident prevention specifications and "self-monitoring" control systems and safety devices which correspond to Category 4 have been constructed and assessed. Therefore, the examples given in this report are the result of the BIA's many years of experience. The standard has systematically classified and, in some cases, re-designated many basic measures which have already been applied in Germany for many years. Thus, for example, the basic safety principles represent the essence of a well-designed safety control system. The well-tried safety principles are found scattered throughout the different national standards issued over recent years. The risk-related approach has already been under discussion in Germany for over ten years and has shaped the technology behind safety and control devices for much longer, especially after publication of DIN V 19250 [6]. The new version of EN 954 [5] will therefore allow significant aspects of the safety technology which has been applied to machinery in Germany to be transferred to a European-wide level.

At present, work is underway on a Part 2 to EN 954, which is intended to define the way in which the individual categories are validated for the different technology sectors. It is proposed that specific fault lists will be incorporated in this future Part 2 and that it will provide additional details on implementing the categories. This would thus represent an official interpretation of the standard. However, it may be many years before Part 2 is finalized. Until such a time, this report may stimulate further standardization work and provide assistance in interpreting the standard in the meantime.

Plans are also in hand to take the European Standard to the international level of ISO standardization. If this project is successful, the categories will also become standard throughout Europe. German manufacturers would therefore do well to adopt this way of thinking as from today and to incorporate this in their products.

Bibliography

[1] Richtlinie des Rates vom 14. Juni 1989 zur Angleichung der Rechtsvorschriften der Mitgliedsstaaten für Maschinen (89/392/EWG). ABl. EG S. 9-32

[2] *Massimi P.; Van Gheluwe, J.-P.:* Die Rechtsvorschriften der Gemeinschaft für Maschinen. Erläuterungen zu den Richtlinien 89/392/EWG und 91/368/EWG. Bundesanzeiger Verlag. Luxemburg 1993

[3] EN 292: Sicherheit von Maschinen – Grundbegriffe, allgemeine Gestaltungsleitsätze. Teil 1: Grundsätzliche Terminologie, Methodik. Beuth-Verlag, Berlin 1991

[4] EN 1050: Sicherheit von Maschinen – Leitsätze zur Risikobeurteilung. Beuth-Verlag, Berlin 1996

[5] EN 954-1: Sicherheit von Maschinen – Sicherheitsbezogene Teile von Steuerungen. Teil 1: Allgemeine Gestaltungsleitsätze. Beuth-Verlag, Berlin 1996

[6] DIN V 19250: Leittechnik. Grundlegende Sicherheitsbetrachtungen für MSR-Schutzeinrichtungen. Beuth-Verlag, Berlin 1994

[7] prEN 1760-1: Sicherheit von Maschinen – Druckempfindliche Schutzeinrichtungen. Teil 1: Allgemeine Leitsätze für die Gestaltung und Prüfung von Schaltmatten und Schaltplatten. Beuth-Verlag, Berlin 1995

[8] prEN 50 100: Sicherheit von Maschinen – Berührungslos wirkende Schutzeinrichtungen. Teil 1: Allgemeine Anforderungen und Prüfungen. Brüssel 1994

[9] EN 574: Sicherheit von Maschinen – Zweihandschaltungen. Funktionelle Aspekte – Gestaltungsleitsätze. Beuth-Verlag, Berlin 1995

[10] EN 1088: Sicherheit von Maschinen – Verriegelungseinrichtungen in Verbindung mit trennenden Schutzeinrichtungen – Leitsätze für Gestaltung und Auswahl. Beuth-Verlag, Berlin 1996

[11] DIN 25 424-1: Fehlerbaumanalyse: Methode und Bildzeichen. Beuth-Verlag, Berlin 1981

[12] *Bömer, T.; Reinert, D.:* Empfehlungen für die Prüfung scannender opto-elektronischer Taster. Sicherheitstechnisches Informations- und Arbeitsblatt 310 242. In: BIA-Handbuch 27. Lfg. VI/96. Erich Schmidt Verlag, Bielefeld 1996

[13] DIN 25 419: Ereignisablaufanalyse: Verfahren, graphische Symbole und Auswirkung. Beuth-Verlag, Berlin 1985

[14] DIN 25 448: Ausfalleffektanalyse. Beuth-Verlag, Berlin 1990

[15] *Meffert, K.:* Klassifikation von Risiken und technischen Maßnahmen. Die BG (1993) Nr. 7, S. 406-412

[16] DIN VDE 0801 (IEC 1508): Entwurf: Funktionale Sicherheit. Sicherheitssysteme, Teile 1-7. Beuth-Verlag, Berlin 1996

[17] DIN V VDE 0801: Grundsätze für Rechner in Systemen mit Sicherheitsaufgaben, mit Anhang A1. Beuth-Verlag, Berlin 1990 und 1994

[18] DIN EN 60 204: Sicherheit von Maschinen – Elektrische Ausrüstung von Maschinen. Teil 1: Allgemeine Anforderungen. Beuth-Verlag, Berlin 1993

[19] EN 60 947-5-1: Niederspannungs-Schaltgeräte – Teil 5-1: Elektromechanische Steuergeräte. Beuth-Verlag, Berlin 1995

[20] DIN EN 982: Sicherheit von Maschinen – Sicherheitstechnische Anforderungen an fluidtechnische Anlagen und deren Bauteile – Hydraulik. Beuth-Verlag, Berlin 1996

[21] DIN EN 983: Sicherheit von Maschinen – Sicherheitstechnische Anforderungen an fluidtechnische Anlagen und deren Bauteile – Pneumatik. Beuth-Verlag, Berlin 1996

[22] DIN EN 1037: Sicherheit von Maschinen – Vermeidung von unerwartetem Anlauf. Beuth Verlag, Berlin 1996

[23] ISO 1219-1: Fluid power systems and components - Graphic symbols and circuit diagrams – Part 1: Graphic symbols. ISO-Verlag, Genf 1991

[24] DIN ISO 1219-2: Fluidtechnik – Graphische Symbole und Schaltpläne. Teil 2: Schaltpläne. Beuth-Verlag, Berlin 1994

[25] DIN ISO 8573-1: Druckluft für allgemeine Anwendungen. Teil 1: Verunreinigungen und Qualitätsklassen. Beuth-Verlag, Berlin 1995

[26] *Felgendreher, K.; Meffert, K.:* Klassifikation von Risiken – Beispiel zur Anwendung von DIN V 19 250 Kraftbetätigte Fenster, Türen und Tore. Sicherheitstechnisches Informations- und Arbeitsblatt 320 190. In: BIA-Handbuch 11. Lfg. V/89. Erich Schmidt Verlag, Bielefeld 1989

[27] *Bock, H.; Bömer, T.:* Klassifikation von Risiken – Beispiel zur Anwendung von DIN V 19 250 Auffahrschutz an fahrerlosen Flurförderzeugen. Sicherheitstechnisches Informations- und Arbeitsblatt 320 121. In: BIA-Handbuch 19. Lfg. X/92. Erich Schmidt Verlag, Bielefeld 1992

[28] *Meffert, K.; Schwind, H.:* Klassifikation von Risiken - Beispiel zur Anwendung von DIN V 19 250 Planschneidemaschine. Sicherheitstechnisches Informations- und Arbeitsblatt 320 180. In: BIA-Handbuch 11. Lfg. V/89. Erich Schmidt Verlag, Bielefeld 1989

[29] *Grigulewitsch, W.; Meffert, K.; Reuß, G.:* Fehlerliste für elektrische Bauelemente. Bei der Prüfung unterstellte Fehlerarten. Sicherheitstechnisches Informations- und Arbeitsblatt 340 220. In: BIA-Handbuch 13. Lfg. XI/89. Erich Schmidt Verlag, Bielefeld 1989

[30] *Gorgs, K.-J.; Kleinbreuer, W.; Kühlem, W.:* Fehlerlisten für hydraulische und pneumatische Bauelemente. Bei der Prüfung unterstellte Fehlerarten. Sicherheitstechnisches Informations- und Arbeitsblatt 340 225. In: BIA-Handbuch 14. Lfg. I/90. Erich Schmidt Verlag, Bielefeld 1990

Appendix

Appendix A: Example of Risk Estimation for Machinery

There are many known methods for performing a risk estimation and evaluation on technical systems [5], [6], [16] [1]. All the methods make use of the two elements of risk, namely "severity of the possible harm" and "probability of occurrence of this harm". In the risk evaluation, these define the risk reduction required in order to achieve a tolerable residual risk for a technical application.

This report is intended to provide a description, by way of example, of the method which is based on [6], which can be found in Appendix B (for information) to EN 954-1. This method is applied to specific examples taken from the field of machinery safety and the required category for these examples is determined.

A.1 The Risk Graph

The risk graph which was introduced by the informative Appendix B of EN 954-1 provides a method for illustrating the risk which is inherent to the process by the elements of risk defined in EN 1050 in relation to the categories as risk reduction measures (see Figure A1, page 164). The probability of occurrence of a hazardous event influences whether a category which is lower or higher than the preferred category must be selected.

We can see straightaway that combining of the "severity of injury", S, and the "frequency", H, is not done by multiplication, but rather that the elements "frequency and / or duration of exposure to the hazard", F, "possibility of avoiding the hazard", P, or merely S are incorporated in the assessment of risk as a function of the "severity of the injury", S. This is e.g. because characterising frequency by the parameters F and P would not lead to any further useful graduation of the risk for the S1 element of risk.

The risk graph gives rise to different categories, whereby the partial risk to be controlled by the safety-related part of a control system increases in line with the category number. As the report has shown, the measures to be taken also increase in line with the category level, to enable the partial risk to be reduced to a tolerable extent.

[1] Part 5 of [16] describes quantitative and qualitative methods for risk estimation and risk evaluation. Appendix C of this part describes the quantitative procedure which requires a quantitative specification of the acceptable residual risk. Appendix D outlines the method which has been standardized in Germany for risk estimation using the risk graphs in accordance with [6]. Appendix E illustrates a qualitative method from the process industry sector in the USA.

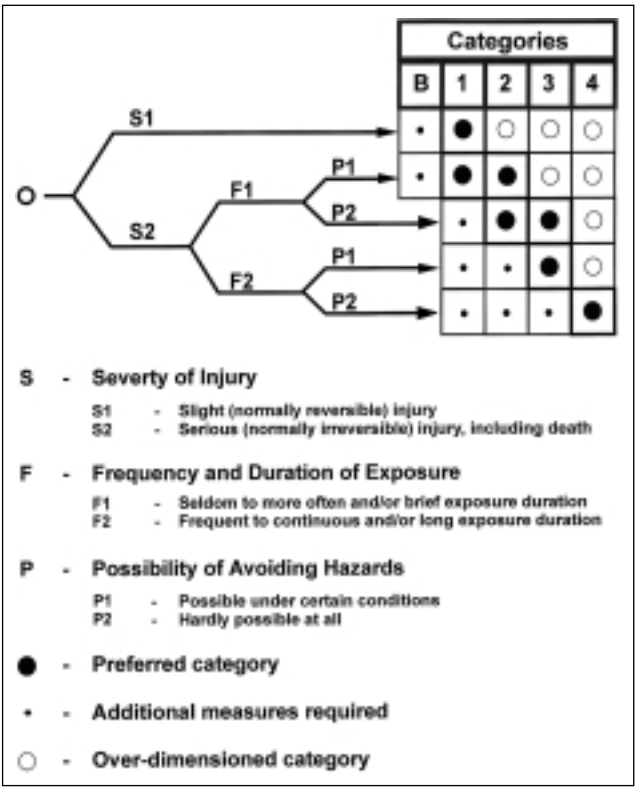


Figure A1:
Notes for the selection of categories

However, individual risks are only allocated directly to control system categories if the required risk reduction has been achieved solely by measures at control system level. A reduction of the category is possible if additional non-technical measures are taken, e.g. operation only after a key switch has been actuated by persons with special training.

Table A1:
Complete risk reduction process

Specified by	Action	Resources used
Design of the machinery as a whole / comparison with existing solutions, EN 1050	Description of the relevant hazard posed by the machinery	Fault tree analysis (FTA) Failure Mode and Effects Criticality Analysis (FMECA) Hazard and Operability Studies (HAZOP)
EN 1050, EN 954 Appendix B	Definition of elements of risk without any safety measures	Risk graph
System requirements specification	List of measures which are not related to the control system	Event tree analysis (ETA)
existing solutions, iterative process	Which of the measures which are not related to the control system have an effect on which elements of risk?	–
EN 954 Appendix B	Definition of the category for the relevant safety-related parts of control systems	Risk graph
Standards for specific applications	Description of non-technical safety measures	Event tree analysis (ETA)
EN 954, IEC 1508	Description of the remaining measures for the safety-related parts of control systems	IEC 1508, this report, DIN V 19251, DIN V VDE 0801

A decision as to the extent to which the overall risk reduction can be broken down into technical and non-technical measures can be made in each individual case on the basis of experience with equivalent applications. Table A1 represents an overview of the complete risk reduction process using the principle outlined above.

A.2 Application Examples for the Risk Graph

Figure A2 illustrates the risk estimation process for the safeguards of closing edges[2] on power-operated windows, doors or gates [26]. As a rule, the formation of crushing and shearing zones is associated with the movement of power-operated windows, doors and wings of gates (see Figure A2). These hazard zones are generally only formed when the wing approaches its end positions. Injuries in hazard zones of this type can be avoided by the use of safeguards of closing edges, for example. Safeguards of closing edges, e.g. safety edges, are placed on the closing edges of the gate wings.

The crushing and shearing zones on the wings of power-operated windows, doors and gates may cause serious or, under certain circumstances, fatal injuries, with the result that S2 must be assumed for the severity of harm. Persons are only rarely and only for short periods in the vicinity of the crushing and shearing zones which occur for only a limited time (F1). Under normal circumstances, persons who are at risk have the option to remove themselves from the hazard zone represented by the moving wing (P1). This option is restricted in the case of gates which close quickly (P2). As shown in Figure A2, the safeguards of closing edges should thus correspond to control system category 2 even in the case of rapid action gates.

As a driverless transport vehicle can, under certain circumstances, be carrying a load weighing several tonnes as it moves along, a serious, irreversible injury is probable in the event of a collision with the vehicle, if this takes place at full speed (S2). People have free access to the vehicle's travel routes and it must therefore be assumed that people will be present in the hazard zone on a relatively frequent basis (F2). As the vehicle drives at very low speeds (generally 3-5 km / hour), a pedestrian approaching such a vehicle usually has the option of getting out of the vehicle's way (P1). Crash protection for driverless floor conveyors should thus correspond to control system category 3 [27] (Figure A3, see page 168).

The paper cutting guillotine illustrated in Figure A4, see page 169, [28] is used to first compress and then cut thick piles of paper

[2] Safeguards of closing edges currently still come under the Construction Product Directive. However it is intended that safeguards of closing edges will be incorporated in the Machinery Directive when this is next revised. The safeguards of closing edges on a power-operated gate is a classic example of the application of Category 2 and has been incorporated in this Appendix for this reason.

once the cutting operation has been released by a two-hand control device. The user is required to access the hazard zone before each cutting operation. The light grid, together with the two-hand control device and a safely designed control system for the machinery as a whole, prevents the possibility of injuries during loading.

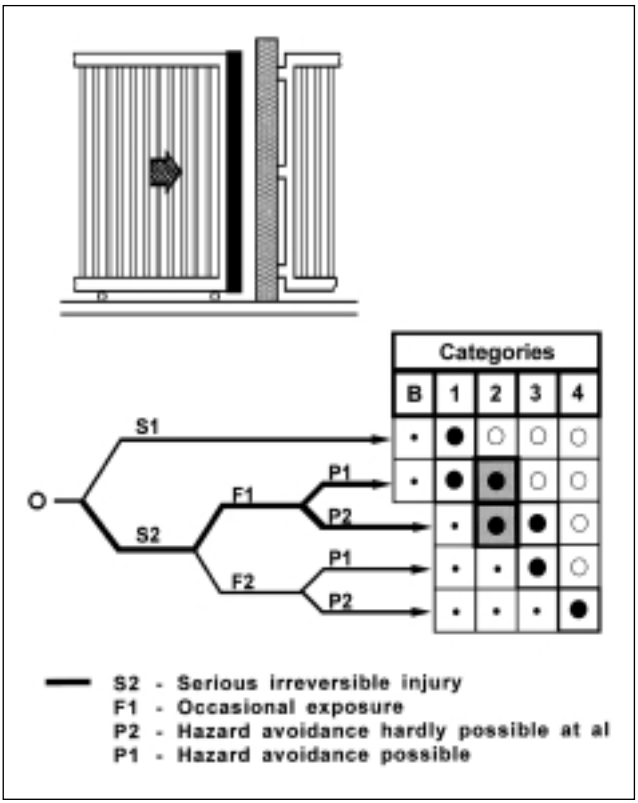


Figure A2:
Risk estimation for safequards of closing edges on power-operated windows, doors and gates

The user of the paper cutting guillotine is exposed on a very frequent basis to the risk of a serious hand injury (S2) (namely during each loading operation (F2)) and has hardly any chance of avoiding the hazard in the event of the machine control system malfunctioning (P2). The safety device and the overall safety control system for a system of this type

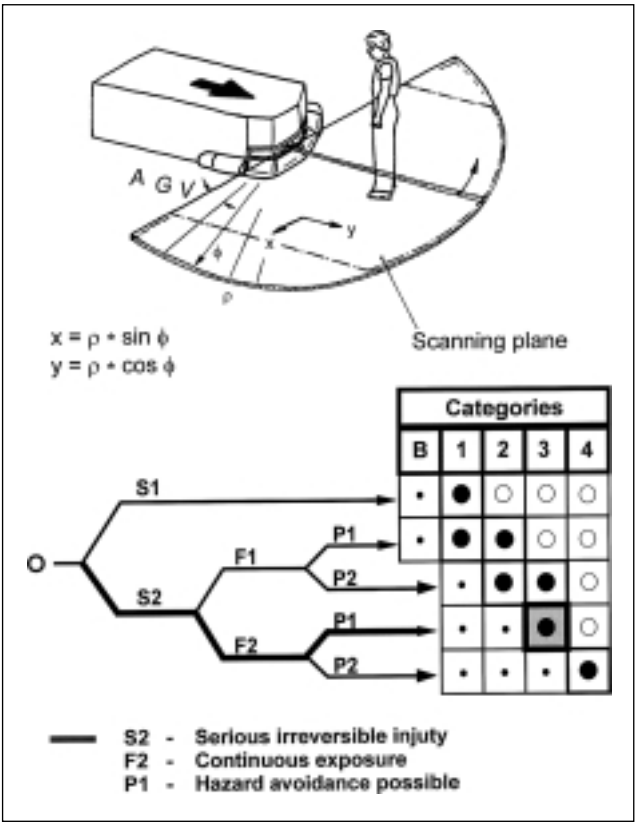


Figure A3:
Risk estimation for crash protection for a driverless floor conveyor

should thus correspond to control system category 4 (Figure A4).

These examples show that there may be very different risks for the same level of severity of harm and these then lead to different control system categories.

All of these examples are taken from the BIA-Handbook, which contains many more applications from the field of machinery safety. The results, which are also used as a basis for the risk graphs in DIN V 19250, can be transferred to the categories given in EN 954-1 using Table 8 in Chapter 4.

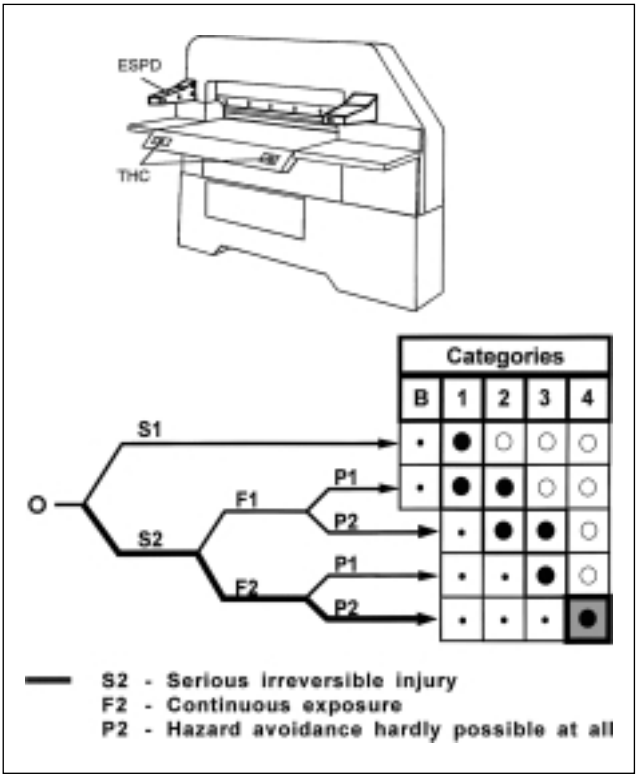


Figure A4:
Risk estimation for control of a paper cutting guillotine

Appendix B: Fault Lists

The categories represent a way of classifying the safety-related parts of a control system (STS) with respect to their ability to withstand faults and their behaviour in the event of a fault. This classification system having been achieved on the basis of reliability and / or the structural arrangement of the parts (see table 3).

This conclusion, as reached in Chapter 3 of this report, shows the significance of a fault list, which is binding for all those involved and which lists the fault modes used as a basis for the different electrical and fluid technology components with specific reference to industrial machinery and plant design.

The authors have published faults lists of this type, which have been revised many times over the course of time and supplemented by information from relevant literature and technical regulations, in the BIA-Handbook [29], [30]. Significant concepts from the BIA fault lists have in the meantime found their way into European working papers or even into initial draft standards [8]. The basic principle of listing fault assumptions, fault exclusions and comments on the latter for each component in a form which can easily be reproduced, has been retained. Some faults and fault exclusions have been modified. Nevertheless, the authors believe that the BIA fault lists represent a sound basis for the design and evaluation of safety-related parts of control systems and safety devices before the final publication of the working papers and draft standards. For this reason, and due to the high demand for these lists in conjunction with the application of EN 954-1, the BIA fault lists are published in this Appendix.

Safety-technology Information and Worksheet

Fault Lists for Electrical Components – faults to be assumed in testing –

1 Introduction

Specified safety requirements with reference to behaviour in a fault condition are provided for technical devices where, in the event of a failure of the controls, persons may be injured. Examples are to be found in the areas of

Machinery and systems engineering, e.g. [1 to 8],

The technical protective devices and safety-relevant components, e.g. [9 to 13],

Traffic and transport engineering, e.g. [14 to 21]

Medical engineering, e.g. [22],

Power engineering, e.g. [23;24].

The effects that can arise as a result of failures in safety-relevant controls are described in the "safety-technology information and worksheet" 330250 in the BIA-Handbook.

The safety requirements which are included in the Technical Regulations and Accident Prevention Rules depend very strongly on the relevant application and extend, in the simplest case from organisational measures, such as regular, functional testing dependant on its purpose through automatic test circuits up to so-called self-monitoring controls, with which faults that occur are automatically made known. The whole of the considerations that are necessary to describe the safety behaviour of a device in the event of a fault and also to check this behaviour in practice is referred to as the fault consideration. One of the most important problems within the scope of fault consideration is that of which faults in electrical components are to be covered. Such fault agreement [25] is necessary as a basis in order to provide the developer with obligatory criteria for the drafting of his control-engineering safety concepts. On the other hand, with this fault agreement the intention is to ensure that different Test Houses and testers do not produce different results with the same test object.

Now which faults are to be included in such a fault list? If all theoretically possible conceivable faults of a component were to be covered in the fault consideration, this would not only lead to an extremely high cost of testing, but to some extent it would no longer be possible to carry out the testing. In many cases it would even be impossible to build a safe control, as the principle of circuits that are safe in the event of a fault assumes that components are available in which it is possible to rule out certain faults (fault exclusion).

For applications in the area of railway signalling engineering, fault catalogues have been produced [26;27] in the past. From the literature, e.g. [28], and from the Technical Rules and Guidelines, e.g. [3;14;15;23;29] it is possible to derive information concerning the faults that are covered and fault exclusions. These fault lists are, however, only conditionally transferable to general industrial applications and even contradict themselves, to some extent in the detailed requirements. In the majority of the Standards and Safety Rules, however, no statements are included as to which faults are actually to be covered in the fault consideration.

2 Requirements for a Fault List

In order always to provide the same assumptions for control-engineering safety testing, the types of faults in electrical components to be taken as basis for the testing have been summarised by the Institute of Occupational Safety of the German Berufsgenossenschaften (BIA). This summary – specially directed towards the design of industrial machines and systems – has been repeatedly revised and extended over the course of time using information from the current literature and the Technical Rules. The lists – proven over several years of testing practice – represent a compromise between differing, and to some extent contradictory, requirements which will be illustrated in the following:

High degree of fault coverage

The faults covered in the testing when faults are present should cover as many as possible of all of the possible faults. The higher the degree of fault coverage the lower is the risk of overlooking hazardous types of faults under certain circumstances.

Feasibility

The more complex a component, the greater is the number of possible faults. So for example, in [27] for the transistor alone 51 types of faults are described; and with LSI assemblies the number of different fault possibilities becomes astronomically high. In order to implement the testing in the event of faults the theoretically possible types of faults must therefore be limited. This limitation must be carried out in such a way that, despite what can happen as the result of a fault, a high degree of coverage of faults is achieved. One good possibility, on the one hand to be able to implement the fault testing in a simple manner, but on the other hand to have a high degree of fault coverage, is the assumption of a "worst case" fault for a complex integrated component or even for a complete integrated component assembly. Here a "worst-case" fault means that at the output terminals of the component or component assembly the most unfavourable fault, from a safety point of view – usually a logical or sequential fault – is assumed.

Possibility of inserting faults

Where it is possible, faults should be covered which are also capable of being inserted into the original circuit to be tested. This is not always possible, when consideration is given, for example, to certain internal drift processes in semiconductor components. Depending on the principle in the circuit and on the circumstances, here nothing else remains but to determine the effect of such faults with the help of theoretical calculation procedures.

Reproducibility

The inserted faults should, as far as possible, be selected so that a reproducible test result is produced. This is not always self evident, when for example considering how to cover the breakage of an input connection pin of a CMOS component. Here, depending on the circumstances, it is necessary to use special test procedures, as for example "potential pulling" (stuck-at-fault).

Economics

The faults covered should allow a simple insertion of faults. The installation of faults in the original circuit takes up the greatest time with experimental methods.

Independence from the manufacturer

The type of the faults to be inserted should be largely independent of the component manufacturer. An exception to this arises when it is claimed that a fault is excluded.

Realistic fault exclusion

It has already been mentioned that, without the assumption of real fault exclusions, safe controls cannot be realised. Now these fault exclusions – apart from certain physically based particular cases – represent a compromise between the safety-engineering requirements and the technical / economic possibilities. For example, fault exclusions can be based on:

- ❒ the physical impossibility of a certain type of fault (Example: large increase in the capacitance of a capacitor),
- ❒ generally recognised – independent of the application – technical rules (Example: forced guidance of relay contacts),
- ❒ technical / economic aspects that depend on the application and which are consequently dependent on the actual risk level of the application (Example: cable short circuits on external cables).

The two first-quoted bases for exclusion of a fault represent the general case. However, in certain applications further fault exclusions can be made. These additional fault exclusions – mostly laid down in the Technical Rules – depend on the risk level of the corresponding application and are based in particular on the probability of the occurrence of a fault. This probability can be verified by means of actual failure rates or estimated from experience based on operational performance testing.

3 Components and assemblies dealt with

For the tests, the types of faults taken as well as the constructional boundary conditions for fault exclusions, are summarised in the following lists. The following electrical components are dealt with:

1 Conductors and connections
1.1 Conductors / cables
1.2 Printed circuit board
1.3 Clamping units
1.4 Multipolar plug connector

2 Control switches
2.1 Mechanical position switches
2.2 Hand-operated switches and push-buttons
2.3 Proximity limit switches
2.4 Relay / contactor

3 Discrete electronic components
3.1 Transformer, transmitter
3.2 Wire-wound resistor
3.3 Composition resistor
3.4 Resistance network
3.5 Potentiometer
3.6 Capacitor, trimmer

4. Electronic components
4.1 Discrete semiconductors (e.g. diode, transistor)
4.2 Optocoupler
4.3 Integrated circuit (SSI, MSI)
4.4 Integrated circuit (LSI, e.g. memory, mP)

Bibliography

[1] DIN VDE 0113 Teil 1: Elektrische Ausrüstung von Industriemaschinen – Allgemeine Festlegungen

[2] DIN VDE 0160: Ausrüstung von Starkstromanlagen mit elektronischen Betriebsmittel

[3] Sicherheitsregeln für Steuerungen an kraftbetriebenen Pressen der Metallverarbeitung (ZH 1 / 457)

[4] Richtlinien für kraftbetriebene Fenster, Türen und Tore (ZH 1 / 494)

[5] Richtlinie für Lagereinrichtungen und -geräte (ZH 1 / 428)

[6] Sicherheitsregeln für Schwenkarmstanzen mit Schwenkhilfe (ZH 1 / 505)

[7] Sicherheitsregeln für Stapelautomaten, Setzmaschinen und automatische Abtragegeräte in der Baustoffindustrie (ZH 1 / 520)

[8] Accident prevention regulation Druck und Papierverarbeitung (VBG 7i)

[9] Sicherheitsregeln für berührungslos wirkende Schutzeinrichtungen an kraftbetriebenen Arbeitsmitteln (ZH 1 / 597)

[10] Sicherheitsregeln für berührungslos wirkende Schutzeinrichtungen an kraftbetriebenen Pressen der Metallverarbeitung (ZH 1 / 281)

[11] Sicherheitsregeln für Zweihandschaltungen an kraftbetriebenen Pressen der Metallverarbeitung (ZH 1 / 456)

[12] DIN 24980: Zweihandschaltungen

[13] DIN VDE 0660 Teil 209: Niederspannungsschaltgeräte - Zusatzbestimmungen für berührungslos wirkende Positionsschalter für Sicherheitsfunktionen

[14] DIN VDE 0831: Elektrische Bahnsignalanlagen

[15] DIN VDE 0832: Straßenverkehrssignalanlagen (SVA)

[16] Sicherheitsregeln für Verschiebewagen in Stetigförderanlagen (ZH 1 / 158)

[17] Richtlinien für fahrerlose Flurförderzeuge (ZH 1 / 473)

[18] TRA 200: Personenaufzüge, Lastenaufzüge, Güteraufzüge

[19] EN 115: Fahrtreppen

[20] Richtlinien für Fahrtreppen und Fahrsteige (ZH 1 / 484)

[21] Richtlinien für Funkfernsteuerung von Kranen (ZH 1 / 547)

[22] DIN IEC 601 VDE 0750: Sicherheit elektromedizinischer Geräte. Allgemeine Festlegungen (sowie Teile 2 ...)

[23] DIN VDE 0116: Elektrische Ausrüstung von Feuerungsanlagen

[24] DIN 25434: Reaktorschutzsystem und Überwachungseinrichtungen des Sicherheitssystems

[25] VDI / VDE 3541 Blatt 2: Steuerungseinrichtungen mit vereinbarter gesicherter Funktion

[26] *Ore*: Frage A 118: Verwendung von elektronischen Bauelementen in der Signaltechnik, Bericht Nr. 2. Forschungs- und Versuchsamt des internationalen Eisenbahnverbandes

[27] Allgemeine Richtlinien für signaltechnisch sichere Schaltungen und Einrichtungen der Elektronik. Ausfall-Liste 43120 Entwurf. Bundesbahn-Zentralamt München

[28] *Bajenescu, T.I.:* Zuverlässigkeit elektronischer Komponenten. VDE-Verlag

[29] TRA 101: Richtlinie für die Prüfung von Bauteilen

Authors

Dipl.-Ing. W. Grigulewitsch, Dr.-Ing. K. Meffert and Dipl.-Ing. G. Reuss
Department Machinery Safety / Control technology

1 Conductors and connections

1.1 Conductors/cables

Fault assumption	Fault exclusion	Remarks
short circuit between any two conductors	short circuit between conductors in the electric installation zone provided that conductors and installation zone are in accordance with the valid DIN VDE-regulations short circuits between conductors belonging to different sheated wires short circuit between conductors being protected by special measures against damages from the outside (cable conduits, armor pipe[1,2])	[1] circuits being metalbraided and connected [2] This fault exclusion can only be made at facilities with a relatively low risk compare VBG 5 § 15.
interruption of any conductor	no	
short circuit to ground and earth short circuit of a conductor	no	

1.2 Printed circuit board

Fault assumption	Fault exclusion	Remarks
short circuit between adjoining conductor ways	short circuit between adjoining conductor ways if the printed circuit board is constructed according to the appropriate Rules of Technics[1] and protected against conductive foreign bodies (also cuts of the conductor ways[2]).	[1] if base material used according to IEC 249-1 and the striking distance and creep distances are dimensioned at least to pollution degree 2 / installation category III, according to IEC 664 (1980) and IEC 664 A (1981). Also for striking distances and creep distances between conductor path and placed components, especially for those conductor path below components e.g. using SMD technology [2] conveniant measures can be e.g. installation of printed circuit board in enclosure with IP > = 54 and covered with a varnish or protective coat.
open circuit of any conductor	no	

1.3 Clamping units (for e.g. terminal strip)

Fault assumption	Fault exclusion	Remarks
open circuit of single plug pins short circuit between adjoining plug pins	no short circuit between adjoining plug pins[1)]	[1)] if versions according to appropriate DIN VDE regulations and adequate connecting methods are used

1.4 Multipolar plug connectors

Fault assumption	Fault exclusion	Remarks
open circuit of single terminals short circuit between adjoining terminals	no short circuit between adjoining terminals[1)]	[1)] ensured by constructive measures for e.g. – profiling, shrinkage hose above the point of connection … creep- and striking clearances chosen with regard to stress of insulation according to classification in IEC 664 (1980) and IEC 664A (1981) and pollution degree 3 / installation category III

2 Control switches

2.1 Mechanical position switches

Fault assumption	Fault exclusion	Remarks
non-closure of a contact non-opening of a contact non-actuation of the switch due to mechanical failure (for e.g. break of plunger, wear of the actuating file, disadjustment) remaining actuation of the switch due to mechanical failure short circuits of contacts being insulated from each other simultaneous short circuit between the three poles of a change-over contact	no non-opening of a contact which has to open itself constraintly[1)] non-actuation…[2)] no short circuit…[3)] simultaneous short circuit…[1,3)]	[1)] In case of auxiliary circuit switches according to DIN VDE 0660, part 206 [2)] mechanically sufficient fixation, actuation of switch according to manufacturer's specifications. This fault exclusion is only allowed for facilities with a relatively low risk, compare VBG 5 § 15 [3)] sufficient creep and striking distances between the contacts. Parts loosening themselves and being conductive may not bridge the insulation between the contacts. Compare DIN VDE 0660 part 206

2.2 Hand-operated switches and push-buttons

Fault assumption	Fault exclusion	Remarks
non-closure of a contact	no	[1] parts loosening themselves and being conductive must not bridge the contact. Form-closed connections between adjusting part and electric contact [2] in case of positive mechanical action from the adjusting part to the electric contact [3] sufficient creep and striking distances between the types of contact. Parts loosening themselves and being conductive must not bridge the insulation between the contacts [4] this fault is accepted in many cases especially at a relatively low risk (e.g. hold to run operation)
non-opening of a contact	non-opening of a contact which has to open itself constraintly[1]	
non-actuation of contacts due to mechanical failure	non-actuation…[2]	
short circuits of contacts being insulated from each other	short circuit…[3]	
remaining actuation of the switch[4] due to mechanical failure	remaining actuation…[2]	
simultaneous short circuit between the three poles of a change-over contact	simultaneous short circuit…[1,3]	

2.3 Proximity limit switch

Fault assumption	Fault exclusion	Remarks
output permanently on low-resistance[2] (cut through)	defective transition of output in the unsafe switching condition[1,2]	[1] switch has to correspond to testing principle GS-ET-14 resp. DIN VDE 0660 part 209 [2] according to construction the low-or high resistant initial state can signal the safe switching position [3] mechanically sufficient fixation of switch and counterpart. This fault exclusion is only allowed at facilities with a relatively low risk. Compare VBG 5 § 15
output permanently on high-resistance[2] (not cut through)	defective transition of output in the unsafe switching condition[1,2]	
voltage supply interrupted	no	
non-actuation of switch due to mechanical failure (for e.g. loss of the counterpart, disadjustment)	non-actuation…[3]	
short circuit between the three connections of a change-over contact (in case of reed contact)	no	

2.4 Relay / contactor

Fault assumption	Fault exclusion	Remarks
does not de-energise	no	[1] if relais / contactors with positively guided contacts are used the non-opening of a contact can be interrogated due to the strict antivalence of opener and closer contacts (control of tightening-and drop). At the examination a total guide rings on a projectile is assumed, that means if a closing contact does not open all other contacts remain closed. This counts analogously for the non-opening of openers. [2] if creep and striking distances are chosen in respect to the stress of insulation according to classification in IEC 664 (1980) and IEC 664 A (1981) with pollution degree 3 / installation category III and convenient connection methods are used.
does not energise	no	
open circuit of the coil or the way of contact	no	
non-opening of single contacts[1]	no	
simultaneous short circuit between the three poles of a make-and-break contact	simultaneous short circuit…[1]	
equivalent switching state of opener and closer (being closed simultaneously)	equivalent switching state of opener and closer (being closed simultaneously)[1]	
short circuit between types of contact under each other and contacts and coiling.	short circuit…[2]	

3 Discrete electronic components

3.1 Transformers, transmitters

Fault assumption	Fault exclusion	Remarks
open circuit of coiling	no	[1] either those requirements according to IEC 742 (1983) have to be fulfilled. In the last case the insulation for at least 2.500 V test alternating voltage has to be measured also for nominal voltage lower than 500 V. A secondary short circuit must not lead to such a high temperature. Interturn short circuits and winding short circuits have to be avoided by convenient measures e.g. by: – inpreguation of the windings, so that all cavities between coil form and winding are filled. – application of winding wires for elevated requirements for insulation and heat-resistance
short circuit between coilings	short circuit between coilings[1]	

3.2 Wire-wound resistor

Fault assumption	Fault exclusion	Remarks
open circuit	no	[1] single layer winding and glazed or casted
short circuit	(short circuit[1]	[2] will be examined if it is expected that the circuit is critical to drift failure. This must normally not be assumed at digital signal processing.
drift[2]		
a) reduction of resistance $0\ \Omega \le R \le R_N$	a) reduction of resistance[1] $0{,}8 \cdot R_N \le R \le R_N$	
b) increase of resistance $R_N \le R \le 10 \cdot R_N$	no	

3.3 Composition resistor

Fault assumption	Fault exclusion	Remarks
open circuit	no	[1] layer of resistance reversed with axial wire connection and varnish sheating. The admissible limiting values such as continuos voltage or power must not be exceeded even at the worst case.
short circuit	short circuit[1]	[2] versions as mentioned under[1] but with a resistance tolerance $\le \pm 5\%$, operating voltage $\le 0{,}5 \cdot$ maximum permissible continuous voltage. In case of higher resistance tolerances the drift range is enlarged
drift[3]		[3] is tested if it can be expected that the connection is critical to drift failure. In case of digital signal conversion this must normally not be assumed.
a) reduction of resistance $0{,}5 \cdot R_N \le R \le R_N$	a) reduction of resistance[2] $0{,}8 \cdot R_N \le R \le R_N$	
b) Increase of resistance $R_N \le R \le 10 \cdot R_N$	no	

3.4 Resistance network

Fault assumption	Fault exclusion	Remarks
open circuit of single connections	no	[1] is only assumed if it has to be expected that the circuit is critical to drift failure
short circuits between various connections	no	
drift of single resistor[1] $0\ \Omega \le R_N \le 10 \cdot R_N$	no	

3.5 Potentiometer

Fault assumption	Fault exclusion	Remarks
open circuit of single connections	no	[1] concerning the wire potentiometer short circuit is only assumed between tap and one of the external connections
simultaneous short circuit between all connections	simultaneous short circuit between all connections[1]	
drift		
a) reduction of resistance $0\ \Omega \leq R \leq R_N$	no	
b) increase of resistance $R_N \leq R \leq 10 \cdot R_N$	no	

3.6 Capacitor, trimmer

Fault assumption	Fault exclusion	Remarks
open circuit	no	[1] exclusion of faults even not at self-healing MP-capacitors
short circuit[1]	no	[2] is only assumed if it has to be expected that the circuit is critical towards drift failure.
drift[2] $0\ F \leq C \leq 2 \cdot C_N$[3] tan δ[2]	no	[3] if the examination shows that the increase of capacitor is critical concerning the safety so only the maximum capacity according to the indications of manufacturer is assumed

4 Electronic components

4.1 Discrete semi conductors (for e.g. diode, tansistor)

Fault assumption	Fault exclusion	Remarks
short circuit between any two connections	no	[1] is only assumed if it has to be expected that the circuit is critical to drift failures
open circuit of each single connection	no	
drift of output values and characteristic values[1]	no	

4.2 Opto coupler

Fault assumption	Fault exclusion	Remarks
open circuit of single connections	no	[1] requirements according to draft DIN VDE 0884 have to be fulfilled
short circuit between various connections		
a) on the side of input (transmitter)	no	[2] by means of a suitable wiring of the optocoupler it can be granted that the minimum energy required for the charge to be put in mot at the output is not available at the input side
b) on the side of output (receiver)	no	
c) between input and output[2]	c) short circuit between various connections of the side of input and output[1]	

4.3 Integrated circuit (SSI, MSI)

Fault assumption	Fault exclusion	Remarks
open circuit of each single connection	no	[1] due to the assumed short circuits resp. the simultaneous failure of all partial functions in an IC all safety signals have to be separated from each other and processed in different ICs
short circuit between any two connections[1]	no	
stuck-at-fault (static "0" and "1" signal at all in- and outputs single or simultaneous[1,2])	no	[2] is only assumed if it has to be expected that the circuit is critical towards this fault assumption
drift of output potentials[2,4]	no	[3] frequency and duty cycle is dependant on the technique of connection and the external wiring. At the examination the driving stages in question will be disconnected
oscillation of outputs[2,3,4]	no	[4] is only assumed for facilities with increased risk, compare VBG 5, § 15 (2)

4.4 Integrated circuit (LSI, e.g. storage, µP)

Fault assumption	Fault exclusion	Remarks
failure of the total or partial function[1)] The failure can – be static – modify the logic – be dependant on the bit sequences	no	[1)] incorrect bit- and word combinations as well as wrong program working are assumed to µP. This means in the "worst-case" that e.g. the programmed self-tests are correctly executed but the results are incorrectly determined
undetected faults in the hardware which are not recognised due to the complex construction of the IC[1)]	no	
undetected faults in the stored program[1)]	no	

Safety-technology Information and Worksheet

Fault Lists for Hydraulic and Pneumatic Components – faults to be assumed in testing –

1 Introduction

Accident prevention regulations, directives and safety rules as well as various regulations of private standards-making bodies (e.g. in [1 to 11]) include, among other things, safety-technology requirements for control systems, protective devices and systems. Some of these requirements are formulated independent of a particular technology, and thus apply also for hydraulic and pneumatic, i.e. fluidic control systems and protective equipment and systems.

In some regulations and directives, the safety-technology requirements also directly or indirectly address the response in the event of a fault or failure. Thus, e.g. [5] mandates dependant of specific conditions a hydraulic or pneumatic control system that is "single-fault-tolerant". In order to fulfill such requirements, it is first necessary to examine the faults. As defined by [12], such an examination comprises the totality of all considerations required to enable the safety-technology behaviour of a device in the event of a fault to be described and practically tested. A decisive factor in this fault examination is the determination, i.e. specification of the faults which are to be assumed. For the developers, such a fault specification is an important prerequisite for enabling the design and realization of the required safety of the control system (with existing components). In addition, a fault specification can also ensure that different testing groups and testers do not produce different results for one and the same testing object.

Up to now, only a few directives and regulations (e.g. [5; 6; 11]) describe the faults which are to be assumed for hydraulic and pneumatic components, and which are to be excluded. The professional literature for fluidics (e.g. [13; 14]) also contains little information on possible technical failures of the components under consideration. To date, no comprehensive, detailed fault list for fluidic components is known. Such a list already exists for electronic components in the "safety-technology information and worksheet" No. 340220 of the BIA-Handbook.

2 Requirements for a fault list

The Institute of Occupational Safety of the German Berufsgenossenschaften (BIA) has compiled a list of the fault assumptions and exclusions for the respective components which form the basis for safety-technology testing of hydraulic and pneumatic control systems, protective equipment and systems. This fault list, created especially for the industrial mechanical-engineering and plant engineering industries, is based in particular on experience gained in over ten years of testing practice. Relevant information contained in directives, regulations and professional literature have been taken into account. Just like the fault list for electrical components, this list represents a compromise between different and sometimes contradictory requirements, as described below.

High degree of fault coverage

The faults covered in the testing when faults are present should cover as many as possible of all of the possible faults. The higher the degree of fault coverage the lower is the risk of overlooking hazardous types of faults under certain circumstances.

Practicality

Hydraulic and pneumatic components are often less complex in their structure than electrical components, particularly integrated circuits. In spite of this, however, the fault test usually cannot cover all faults which are theoretically possible. One good approach for conducting the fault test relatively simply while still covering a high level of possible faults is to assume the most unfavorable state of the output component from the point of view of safety technology. For example, in pneumatic circuits assembled using information-processing elements (e.g. AND, OR and NOT elements), it is often sufficient to assume corresponding faults in the output valve.

Possibility of inserting faults

Where possible, faults should be assumed which can also be built into the component or circuit to be tested. The cause of the fault, e.g. contamination of the pressure medium with solid matter, often cannot be realistically simulated without a disproportionate amount of time and effort. However, the effects of this cause, e.g. jamming of the moving component, can generally be built in as a fault. For this reason, those

faults (effects of faults) which can also be built in during testing were given preference in compiling this list.

Reproducibility

As far as possible, the built-in faults should be selected so as to obtain a reproducible test result.

Economy

The assumed faults should allow faults to be built into the system in an efficient manner. However, the insertion of the faults in the respective component or original circuit under study requires a great deal more time than the theoretical examination of faults. For this reason, examination should remain on the theoretical level for readily comprehensible components and circuits.

Manufacturer-independence

The assumed faults should be largely independent of the component manufacturer. However, fault exclusions can generally only be formulated in design terms and are thus sometimes indirectly manufacturer-dependent.

Realistic fault exclusions

Safe control systems cannot be realized without concrete fault exclusions. With the exception of a few physically justified individual cases, these fault exclusions represent a compromise between the requirements of safety technology and the technical and economic possibilities. In particular, fault exclusions are justified by:

- ❒ the physical impossibility of a defined fault type (e.g. increase in the volumetric flow of a fixed displacement pump with no change in the operating and drive parameters);
- ❒ generally recognized, application-independent technical experience (e.g. sudden fracture of a valve slide piston into numerous pieces);
- ❒ technical / economic aspects determined by the application and thus dependent on the specific risk of the application (e.g. spontaneous switching of a valve without activation in a relatively low-risk application).

The first two reasons for excluding a fault are the most common case. However, farther-reaching fault exclusions can be made for defined applications. These additional fault exclusions depend on the risk of the respective application and focus primarily on the probability that this type of fault will occur. The probability of occurrence can be substantiated by concrete failure rates or estimated through experience on the basis actual operation. Actual failure rates of fluidic components under industrial conditions are practically unknown, so that corresponding operating experience must be substituted in this case.

3 Components investigated

An overview of the fault lists for hydraulic and pneumatic components is presented below. Although these lists have a great deal in common, a single list with specification of the respective special characteristics for hydraulic and pneumatic components would make use of the lists too cumbersome for most practitioners.

For each component, the lists specify the fault assumptions, the fault exclusions plus corresponding remarks. These remarks contain reasons, explanations and notes of a general nature. The following hydraulic and pneumatic components are dealt with:

1 Valves
1.1 Directional control valves
1.2 Stop valves
1.3 Flow valves
1.4 Pressure control valves

2 Ducts
2.1 Pipework
2.2 Hoses
2.3 Connecting elements

3 Cylinders

4 Pressure transmitter / pressure medium transducer

Plus the following hydraulic components:

5 Filter

6 Accumulators (pressure vessels)

7 Pumps / motors

8 Sensors

Plus the following pneumatic components:

5 Compressed air treatment
5.1 Filter
5.2 Oiler
5.3 Muffler

6 Accumulators (pressure vessels)

7 Motors

8 Sensors

9 Information processing
9.1 Logical switching element
9.2 Time lag devices
9.3 Converters

Bibliography

[1] Accident-prevention regulation „Kraftbetriebenes Arbeitsmittel“ (VBG 5). Carl Heymanns Verlag, Cologne (10 / 1985 and 4 / 1987)

[2] Accident-prevention regulation „Hydraulische Pressen“ (VBG 7n 5.2). Carl Heymanns Verlag, Cologne (4 / 1987)

[3] Accident-prevention regulation „Giessereien“ (VGB 32). Carl Heymanns Verlag, Cologne (4 / 1979 and 4 / 1986)

[4] Richtlinien für kraftbetätigte Fenster, Türen und Tore (ZH 1 / 494). Carl Heymanns Verlag, Cologne (10 / 1989)

[5] Sicherheitsregeln für die Steuerungen von Druck- und Papierverarbeitungsmaschinen (ZH 1 / 170). Carl Heymanns Verlag, Cologne (10 / 1988)

[6] Sicherheitsregeln für Steuerungen an kraftbetriebenen Pressen der Metallbearbeitung (ZH 1 / 457). Carl Heymanns Verlag, Cologne (2 / 1978)

[7] Sicherheitsregeln an Zweihandschaltungen an kraftbetriebenen Pressen der Metallbearbeitung (ZH 1 / 456). Carl Heymanns Verlag, Cologne (2 / 1978)

[8] DIN 24 980 Zweihandschaltung, Sicherheitstechnische Anforderungen, Prüfung. Beuth Verlag, Berlin (8 / 1987)

[9] DIN 24 346 Hydraulische Anlagen, Ausführungsgrundlagen. Beuth Verlag, Berlin (12 / 1984)

[10] VDI 3229 Technische Ausführungsrichtlinien für Werkzeugmaschinen und andere Fertigungsmittel, P-Pneumatische Ausrüstung. Beuth Verlag, Berlin (5 / 1967)

[11] VDI 2854, Entwurf: Sicherheitstechnische Anforderungen an automatische Fertigungssysteme. Beuth Verlag, Berlin (10 / 1989)

[12] *Grigulewitsch, W., K. Meffert und G. Reuss:* Fehlerliste für elektrische Bauelemente – Bei der Prüfung unterstellte Fehlerarten. Sicherheitstechnisches Informations- und Arbeitsblatt 340 220 in: BIA-Handbuch, 7. Lfg. VI / 87 und 13. Lfg. XI / 89. Erich Schmidt Verlag, Bielefeld

[13] *Böinghoff, O:* Ursachen und Folgen der Verschmutzung von Hydraulikflüssigkeiten. Grundlagen der Landtechnik 24 (1974), Nr. 2, S. 46-50

[14] *Weule, H:* Sicherung der Verfügbarkeit hydraulischer Anlagen in Planung und Betrieb. 8. Aachener Fluidtechnisches Kolloquium, März 1998, Fachgebiet Hydraulik, Band 1, S. 5-47. Hrsg.: Verein zur Förderung der Forschung und Anwendung der Hydraulik und Pneumatik e.V., Aachen

Authors

Dipl.-Ing. K.-J. Gorgs, Dr.-Ing. W. Kleinbreuer and Dipl.-Ing. W. Kühlem
Department Machinery Safety / Control technology

List of faults occurring in hydraulic components (Status 2/90)

1 Valves (hydraulic components ≙ Hy)

1.1 Directional control valves (Hy)

Fault assumed	Fault exclusion	Remarks
Modification (extension) of the switching times	no[1] yes, in case of positive actuation of the moving component[2] insofar as the actuation force is sufficient and if sizing and construction of the operating mechanism have been to recognised rules of technology, and state of the art	[1] For example, due to wear, material fatigue (among other things, springs), external influences, blokkage of slits and nozzles, it is not possible to exclude a fault. [2] A positive actuation of the moving component is possible in the case of mechanical, form-locking actuation and can, for example, occur through guides in a movable protection device. In the case of manual operation (hand, foot) the activation force for valves according[3] is usually not sufficiently large. [3] This applies generally to gate valves and seat valves with similar commands on the moving component (cartridge construction), but or usually also in the case of ball seat valves because in this case the commands of the actuation mechanism (e.g. driver rod) have to be considered. In this case, because of 1) it is not possible to exclude a fault. [4] The spring tension remains largely intact, if the wire diameter is larger than the winding spacing (coiling after wire rupture is prevented) and the spring is sufficiently guided (sharp bending after wire rupture, is prevented). [5] Normal assembly and operating conditions occur, if circumstances foreseen by the manufacturer are respected and when the gravity force of the moving component does not have any negative technical safety implications (e.g. horizontal assembly), if no particular mass force acts on the moving component (e.g. direction of motion when installing on moved machine parts) and no extreme vibration and shock loading occur.
Failure to switch (sticking of the moving component in a final position or zero position) or Incomplete switching (sticking of the moving component in arbitrary intermediate position)	no[3] yes, in case of positive actuation	
Automatic change of the initial switching position of the moving component (without control)	no, for specification levels "Single failure safety" and "Self-monitoring". If, however, the spring tension is largely retained in the case of spring fracture[4] and normal assembly and operating conditions occur[5], it is possible to exclude faults yes, in the case of lower specification level, when normal assembly and operating conditions occur[5] yes, in case of positive actuation of the moving component[2] if sizing and construction of the operating mechanism have been to recognised rules of technology and state of the art.	

Fault assumed	Fault exclusion	Remarks
Leakage	no, in the case of gate valves[6)] yes, for seat valves in normal conditions of use and if sufficient filtration is available no, for seat valves in abnormal circumstances[7)]	[6)] In the case of gate valves (metallic sealing) there will be leakage because of the gap due to construction. [7)] Abnormal conditions of use will occur, e.g. in the case of considerable solid loading of the pressure medium (internal or external causes) and / or high humidity content of the atmosphere in the case of insufficient filtration; in addition, if there is a danger of cavitation erosion at the valves seat (unfavourable flow conditions).
Modification of the leakage volume flow	no[8)]	[8)] Changes in the fit or valve seat (e.g. by wear) are assumed over a long time-period. In addition, partial deformations of the valve seat in abnormal conditions of use are assumed (see 7). Material breaking off from leading edges, valve stems and valve seats is not assumed.
Bursting of the valve housing and breaking of the moving component as well as fracture of the fixing and cover screws.	yes, when design, sizing and construction have been to recognised rules of technology and state of the art.	
Uncontrolled command and control behaviour of servo- and proportional valves by hydraulic faults, in particular without control. (This fault assumption occurs for these valves in addition to those faults already assumed. If in addition to the safe switch position (middle or end position) there are arbitrary safety-relevant intermediate positions, then the electronic control must also be subject to safety evaluation, see "Faults list for electric components").	no, for servo-valves and proportional directional control valves with servo driving stage yes, for proportional directional control valves if their safety can be evaluated in the same manner as for conventional directional control valves[9)] as a result of their construction	[9)] Important assessment criteria in this respect are, for example: – occupying the safe switching position upon failure of the control energy by means of sufficiently large mechanical return forces (springs) – safe electrical segregation of the control energy as a

Fault assumed	Fault exclusion	Remarks
Note: If valve functions (switch symbols) are fulfilled by operation of several moving parts (individual valves) (e.g. 4 / 3 directional function by four individual 2 / 2 built-in valves) then the fault evaluation has to be carried out for each one of the individual moving components. The same procedure has to be followed for pilot valves.		– requirement for occupying the safe switching position – sufficient positive overlap in the safe switching position – construction of the pilot valve in multistage proportional directional control valves (the pilot valve must be mechanically similar to a conventional valve or if the pilot valve is designed like a servo-valve then there must be a separation in the safe switching position by means of a conventional directional control valve between the first stage and the main stage).

1.2 Stop valves (seat valves) (Hy)

Fault assumed	Fault exclusion	Remarks
Modification (extension) of the switching time	no[1)]	[1)]Because, for example, of wear, material fatigue (e.g. springs), external influences, blokkages of slits and nozzles, it is not possible to exclude faults. [2)]This applies e.g. to check valves in cartridge form but also usually for controlled ball seat valves (e.g. unlatchable check valve) because in this case one also has to consider the control of the actuating mechanism (e.g. actuating piston). In these cases, because of[1)] it is not possible to exclude faults. [3)]For non-controlled ball seat valves, sticking of the moving component is usually sufficiently improbable because of[1)].
Non-opening, incomplete opening, non-closure as well as insufficient closure (sticking of the moving component in a final position or in an arbitrary intermediate position)	no, when the control of the moving component is similar to the case of valve pistons[2)] yes, when the control of the moving component is similar to the case of ball seat valve[3)] and there is a specification level below that of "self-monitoring"	

Fault assumed	Fault exclusion	Remarks
Automatic change of the initial switching position (without control)	yes, for normal assembly and operating conditions[4] and when there is sufficient closure force on the basis of available pressure and areas	[4] Normal assembly and operating conditions occur, if the conditions foreseen by the manufacturer are respected, no particular mass force acts on the moving component and no extreme vibration or shock loading occur.
Simultaneous closure of both inlet connections in two-way valves	yes, when, because of construction and design of the moving component, the simultaneous closure is sufficiently improbable	
Leakage	yes, when normal operating circumstances occur and there is sufficient filtration no, for abnormal circumstances[5]	[5] Abnormal conditions of use will occur, e. g. in the case of considerable solid loading of the pressure medium (internal or external causes) and / or high humidity content of the atmosphere in the case of insufficient filtration; in addition, if there is a danger of cavitation erosion at the valve seat (unfavourable flow conditions)
Modification of the leakage volume flow	no[6]	[6] It is assumed over a long period that changes in the valve seat occur (e. g. due to wear). In addition, partial deformation of the valve seats in abnormal conditions are assumed (see [5]. Material breakaway at valves seats is not assumed.
Bursting of the valve housing and breaking of the moving component as well as fracture of the fixing and cover screws	yes, when design, construction and sizing have been to recognised rules of technology and state of the art	

1.3 Flow valves (Hy)

Fault assumed	Fault exclusion	Remarks
Change in volume flow without change in regulating device	yes, for flow valves without moving parts[1] (fixed resistances, throttle valves) when normal operating circumstances occur and there is sufficient filtration[2], [4] no, for flow valves with moving parts, e.g. flow control valves[3],[4]	[1] The regulating device is not considered as a moving part. Changes in volume flow due to changes in pressure differential and viscosity are physically limited in this type of valve and are not covered of this assumed fault. [2] Normal operating conditions occur when conditions foreseen by the manufacturer are observed and no abnormally high abrasion and no large

Fault assumed	Fault exclusion	Remarks
		solid particle (in relation to the cross-section of the hydraulic resistance) in the system are expected. 3)Due, e.g. to wear, material fatigue (among other things springs), external influences, blokkage of slits and nozzles, an uncontrolled behaviour of the moving component (pressure compensator) has to be assumed. 4)If a stop valve is integrated in the flow valve, the additional fault assumptions for stop valves have to be considered. 5)Since the required nominal value is given by the electronics and since moving components exist3), it is usually not possible to exclude a fault.
Change in volume flow in the case of non-adjustable circular slits and nozzles	yes, when the diameter is greater than 0,8 mm, normal circumstances2) and sufficient filtration are available	
Change in volume flow by unwanted change of the setting value in proportional flow valves. (This fault assumption occurs in these valves in addition to the other fault assumptions)	no5)	
Automatic modification of the regulating device	yes, for effective protections of the regulating device, adapted to the particular case, under consideration of technically safe immobilisation (e.g. lead seals)	
Unintentional screwing out of the operating element in the regulating device	yes, when an effective positive locking protection against unscrewing is available	
Bursting of the valve housing and breaking of the moving component as well as fracture of the fixing and cover screws	yes, when design, construction and sizing have been to recognised rules of the technology and state of the art	

1.4 Pressure valves (Hy)

Fault assumed	Fault exclusion	Remarks
Non-opening or insufficient opening (spatially and temporally) when exceeding the set pressure or non-closure or insufficient closure (spatially and temporally) if pressure drops below the set value (sticking or difficult movement of the moving component1))	no, when the control of the moving component is similar to the case of valve pistons2), 3) yes, when the control of the moving component is similar to the case of a ball seat valve4) and there is a specification level below that of "self-monitoring"	1)This fault assumption applies only it the function of pressure valves is determining, in particular for dynamic effects (e.g. section indicator, clamp) and the control of hazardous movements (e.g. keeping a load in a lifted position, pressure build-up in tool closure systems).

Fault assumed	Fault exclusion	Remarks
		It does not apply for its normal function in hydraulic systems (e.g. pressure limitation, pressure decrease). It also does not apply to the application of type-approved pressure limitation valves. In the latter application there is only an occasional actuation of the valve so that influences as per[2] are less probable. [2]E.g. wear, external influences, blockage of slits and nozzles mean that sticking of the moving component cannot be excluded. [3]This applies e.g. for pressure valves in cartridge or gate form but also usually for controlled ball seat valves with damping devices because in this case one also has to consider the control of the damping device. In these cases, because of[2] it is not possible to exclude faults. [4]In the case of ball seat valves without damping devices, the control is usually such that sticking of the moving component because of[2] is sufficiently improbable.
Modification of the pressure control behaviour without modification of the regulating device[1]	no[5] yes, in the case of direct actuation of pressure limitation valves if the spring force is largely retained after break of the spring[6]	[5]Due, e.g. to material fatigue (control spring), blockage of slits and nozzles, it is not possible to exclude faults. [6]The spring tension remains largely intact, if the wire diameter is larger than the winding spacing (coiling after wire rupture is prevented) and the spring is sufficiently guided (sharp bending after wire rupture is prevented).
Modification of the pressure control behaviour by unwanted modification of the control value in the case of proportional pressure valves[1]. (This fault assumption occurs in these valves in addition to the other fault assumptions.)	no[7]	[7]Because the required set point is given by the electronics and because there are moving components[2], it is usually not possible to exclude faults.

Fault assumed	Fault exclusion	Remarks
Automatic modification of the regulating device	yes, for effective protection of the regulating device, adapted to the particular case, under consideration of technically safe immobilisation (e.g. lead seals)	
Unintentional screwing out of the operating element in the regulation device	yes, when an effective positive locking protection against unscrewing is available	
Leakage	no, in the case of gate valves[8)] yes, for seat valves in normal conditions of use and if sufficient filtration is available no, for seat valves in abnormal circumstances[9)]	[8)]In the case of gate valves (metallic sealing) there will be leakage because of the gap due to construction. [9)]Abnormal conditions of use will occur, e.g. in the case of considerable solid loading of the pressure medium (internal or external causes) and / or high humidity content of the atmosphere in the case of insufficient filtration; in addition, if there is a danger of cavitation erosion at the valve seat (unfavourable flow conditions).
Modification of the leakage volume flow	no[10)]	[10)]Changes in the fit or valve seat (e.g. by wear) are assumed over a long time-period. In addition, partial deformations of the valve seat in abnormal conditions of use are assumed (see[8)]). Material breaking off from leading edges, valve stems and valve seats is not assumed.
Bursting of the valve housing and breaking of the moving component as well as fracture of the fixing and cover screws	yes, when design, sizing and constructions have been to recognised rules of technology and state of the art	

2 Ducts (Hy)

2.1 Pipework (Hy)

Fault assumed	Fault exclusion	Remarks
Bursting and leakage	yes, when in particular the sizing, choice of materials, manufacture, configuration and attachment have been to recognised rules of technology, and state of the art	
Rupture at the connecting element	yes, when using usual connecting elements, when no particular safety requirements are placed[1] and if sizing, choice of materials, manufacture, configuration and attachment have been to recognised rules of technology, and state of the art no, when using cutting ring union pieces or in particular cases when specific safety requirements are placed[2] yes, when using welded bolting, welded flanges and flange connections, if sizing …	[1]There are no particular safety requirements if, e.g. the pipework fails without any hazardous machine movement being expected and if the time persons spend in potentially dangerous areas near the pipework is short. [2]Specific safety requirements exist if, e.g. masses are hydraulically maintained in a lifted position or are decelerated (at high kinetic energy) or there is an immediate risk to persons from the escaping pressure medium.
Clogging (blockage)	yes, in ducts in the power circuit yes, in the case of control and measurement lines when no particular safety requirements are placed on the control or measurement signal no, in the case of control and measurement lines if particular safety requirements are placed on the control and measurement signal[3] and the nominal diameter is < 3 mm	[3]Specific safety requirements exist if a faulty control or measurement signal can create a hazard, e. g. in the case of valve monitoring using a pressure switch.

2.2 Hose assemblies (Hy)

Fault assumed	Fault exclusion	Remarks
Bursting, tearing out of attachment and leakage	yes, when there are no particular safety requirements[1] and when in particular the sizing, choice of materials, manufacture, configuration and attachment have been to recognised rules of technology, and state of the art	[1] There are no particular safety requirements if, e.g. the hose assembly fails without any hazardous machine movement being expected, and if the time persons spend in potentially dangerous areas near the hose assembly is small.

Fault assumed	Fault exclusion	Remarks
	no, when in particular safety requirements are placed[2] (also when sizing …)	[2] Specific safety requirements exist, if. e.g. masses are hydraulically maintained in a lifted position or are decelerated (at high kinetic energy) or there is an immediate risk to persons due to failure of the hose assembly (escaping pressure medium, whipping of pipe). In this case, mainly manufacturing defects in the hose assembly and age-induced decreases in performance have to be assumed.
Clogging (blockage)	yes, in ducts in the power circuit yes, in the case of control and measurement lines when no particular safety requirements are placed on the control or measurement signal no, in the case of control and measurement if particular safety requirements are placed on the control and measurement signal[3] and the nominal diameter is <3 mm	[3] Specific safety requirements exist if a faulty control or measurement signal can create a hazard, e.g. in the case of valve monitoring using a pressure switch.

2.3 Connecting elements (Hy)

Fault assumed	Fault exclusion	Remarks
Bursting, failure of attachment screws or tearing out of screws	yes, if sizing, material choice, manufacture, configuration and connection to the pipework or fluid-technological component have been to recognised rules of technology, and state of the art	
Leakage (failure of leaktightness)	no[1]	[1] Due to wear, ageing, deterioration of the elasticity, etc. it is not possible to exclude faults over a long period. A sudden major failure of the leaktightness is not assumed.
Clogging (blocking)	yes, for use in the power circuit yes, in the case of control and measurement lines when no particular safety requirements are placed on the control or measurement signal	

Fault assumed	Fault exclusion	Remarks
	no, in the case of control and measurement lines if particular safety requirements are placed on the control and measurement signal[2] and the nominal diameter is < 3 mm	[2] Specific safety requirements exist if a faulty control or measurement signal can create a hazard, e.g. in the case of valve monitoring using a pressure switch.

3 Cylinders (Hy)

Fault assumed	Fault exclusion	Remarks
Loss of the leaktightness of pressure chambers or change in leaktightness	no[1]	[1] Because of wear of seals, wipers and guides it is not possible to exclude faults over a long time period. Sudden major failure of leaktightness is not assumed.
Failure of the end of course damping	yes, if no failure of the stop valve at the end of course damping is assumed[2] no, if failure of the stop valve available at the end of course damping is assumed[2]	[2] See 1.2 Stop valves (Hy) ("failure to close")
Loosening of the connection piston / piston rod as well as piston rod / machine	yes, if design and manufacture have been to recognised rules of technology and state of the art and possibly answer specific safety requirements	
Bursting of the pressure chambers as well as fracture of the attachment and cover screws	yes, if sizing, material choice, configuration and attachment have been to recognised rules of technology and state of the art	
Buckling of piston rods	yes, if sizing, material choice, configuration and attachment have been to recognised rules of technology and state of the art	

4 Pressure tansmitter / pressure medium transducer (Hy)

Fault assumed	Fault exclusion	Remarks
Loss of the leaktightness of pressure chambers or change in leaktightness	no[1]	[1] Because of wear of seals, wipers and guides it is not possible to exclude faults over a long time period. Sudden major failure of leaktightness is not assumed.

Fault assumed	Fault exclusion	Remarks
Bursting of the pressure chambers as well as fracture of the attachment and cover screws	yes, if sizing, material choice, configuration and attachment have been to recognised rules of technology and state of the art	

5 Filter (Hy)

Fault assumed	Fault exclusion	Remarks
Blockage of the filter element	no[1)]	[1)] In particular after initial or restart, after repair and maintenance, blockage of the filter due to "original dirt" is to be expected even if correctly sized.
Rupture of the filter element	yes, if the filter element is sufficiently resistant to pressure and if there is an effective bypass valve or an effective dirt monitoring	
Failure of the bypass valve	yes, if the control of the bypass valve is similar to that of a ball seat valve[2)] yes, when no particular safety requirements must be fulfilled in connection with the location of the filter no, if particular safety requirements in connection with the location of the filter have to be fulfilled[3)] and failure of the bypass valve has to be assumed[2)]	[2)] See 1.2 Stop valves (Hy) ("Failure to open") [3)] There are particular safety requirements if, for example, increase of the pressure upstream of the filter could cause dangerous movements (loosening of brakes, increase of slowing down paths, switching of valves) [4)] In exceptional cases (high pressure, large volume) it can be necessary in addition to consider the requirements of the pressure vessel ordinance including all relevant rules.
Failure of the dirt indicator or dirt monitor	no, for conventional design	
Bursting of the filter housing and fracture of the cover screws or connecting screws	yes, when sizing, material choice, location in the system and securing have been to recognised rules of technology and state of the art[4)]	

6 Accumulators (pressure vessels) (Hy)

Fault assumed	Fault exclusion	Remarks
Bursting of the pressure vessel and breach of connecting and cover screws as well as tearing out of attachment screws	yes, when construction, equipment and location in the system respond to requirements[1)] and are to recognised rules of technology and state of the art	[1)] Requirements on construction and equipment are laid down in particular in the pressure vessel ordinance and relevant rules.

Fault assumed	Fault exclusion	Remarks
Loss of leaktightness of the connecting element between gas and pressure fluid	no[2)]	[2)] Wear of seals and guides (piston accumulator) as well as ageing of membrane and accumulator bags (membrane and bubble accumulator) mean that faults cannot be excluded over a long time period. [3)] Sudden major failure of seals is not assumed.
Failure of the connecting element between gas and pressure fluid	no, in the case of membrane and bubble accumulator yes, in the case of piston accumulators[3)]	
Failure of the fill-up valve on the gas side	yes, when the fill-up valve is to recognised rules of technology and state of the art and there is sufficient protection against external events	

7 Pumps / motors (Hy)

Fault assumed	Fault exclusion	Remarks
Modification of the volume / absorption stream in the case of constant pumps and motors	yes, for short time periods[1)]	[1)] For longer time periods one has to assume a modification through wear of the moving parts and seals. [2)] There are particular requirements if, for example, speeds or rotational speeds have to be maintained to the standard required for single failure safety or self-monitoring. Modification of the switching times and sticking of the moving components, clogging of slits and nozzles as well as change of the spring forces in the control or regulation device have to be assumed, see 1.1 "Directional control valves", remarks[1), 4)]
Automatic change of the volume / absorption setting without actuation of the regulating device in the case of adjustable pumps / motors	yes, in the case of mechanically adjustable pumps and motors yes, in the case of pressure volume controlled pumps and motors if no particular requirements are placed on the adjustment parameters being kept constant no, in the case of pressure and volume controlled pumps and motors if particular requirements are placed on the adjustment parameters being kept constant[2)]	
Rupture of loosening of the drive / output connecting elements (couplings) as well as bursting of the housing and rupture of the cover and attachment screws	yes, of design, construction and sizing are to recognised rules of technology and state of the art	

8 Sensors (Hy)

Fault assumed	Fault exclusion	Remarks
Failure of the sensor[1)]	no[2)]	[1)] This definition encompasses in the case signal capture, processing and output in particular of pressure, volume flow, temperature and direction.
Modification of the coverage and output characteristic	no[2)]	[2)] Because, for example, of wear, material fatigue (among other things, springs) external influences, blockage of slits and nozzles as well as failure and / or modification in the behaviour of the electrical / electronic components it is not possible to exclude failure.

List of faults occuring in pneumatic components (Status 2/90)
1 Valves (pneumatic components)
1.1 Directional control valves (Pn)

Fault assumed	Fault exclusion	Remarks
Modification (extension) of the switching times	no[1)] yes, in case of positive actuation of the moving component[2)] insofar as the actuation force is sufficient and if sizing and construction of the operating mechanism have been to recognised rules of technology, and state of the art	[1)] For example, due to wear, material fatigue (among other things, springs), external influences, blockage of slits and nozzles, it is not possible to exclude a fault. [2)] A positive actuation of the moving component is possible in the case of mechanical, form-locking actuation and can, for example, occur through guides in a movable protection device or by manual operation (hand, foot).
Failure to switch (sticking of the moving component in a final position or zero position) or incomplete switching (sticking of the moving component in arbitrary intermediate position)	no[1)] yes, in case of positive actuation …[2)]	
Automatic change of the initial switching position of the moving component (without control, by stresses due to vibration or shocks, or both).	yes, in the case of gate valves with elastic packing no, in the case of gate valves with metallic packing and in the case of seat valves if the specification level "Single failure safety" or "self-monitoring" is required. If however the spring tension is largely retained in the case of spring fracture[3)] and normal assembly and operating conditions occur[4)], it is possible to exclude faults. yes, in the case of gate valves with metallic packing and seat valves in the case of lower specification level, when normal assembly and operating conditions occur.	[3)] The spring tension remains largely intact, if the wire diameter is larger than the winding spacing (coiling after wire rupture is prevented) and the spring is sufficiently guided (sharp bending after wire rupture, is prevented). [4)] Normal assembly and operating conditions occur, if circumstances foreseen by the manufacturer are respected and when the gravity force of the moving component does not have any negative technical safety implications (e.g. horizontal assembly), if no

Fault assumed	Fault exclusion	Remarks
	yes, in the case of positive actuation of the moving components[2] if sizing and construction of the operating mechanism have been to recognised rules of technology and state of the art.	particular mass force acts on the moving component (e.g. direction of motion when installing on moved machine parts) and no extreme vibration and shock loading occur.
Automatic change of the initial switching position of the moving component (without control, due to leakage).	yes, for valves which because of their construction can only be switched by air fed signals (positive signals, pressure increase) no, in the case of valves which because of their construction are switched by air release signals (negative signals, pressure decrease)	
Leakage	yes, in the case of gate valves with elastic packing in so far as a sufficient positive overlap is present[5] and in the case of seat valves when normal operating conditions occur and sufficient treatment of the compressed air takes place no, in the case of gate valves with metallic packing[6] no, in the case of gate valves with elastic packing and for seat valves when normal operating conditions do not apply[7]	[5] In the case of gate valves with elastic packing, leakage with unfavourable safety consequences can usually be excluded. A small leakage over a large timespan does however take place. [6] In the case of gate valves with metallic packing there will be leakage because of the gap due to construction. [7] Abnormal conditions of use will occur, e.g. in the case of considerable solid loading and / or high humidity content of the atmosphere in the case of insufficient filtration and / or high lubricant fraction in the compressed air. [8] Changes in the fit or valve seat due to wear (metallic packing) or due to chemical changes in the packing material (e.g. volume decrease) as well as wear of elastic packing are assumed over a long time-period. In addition, partial deformations of the valve seat in normal conditions of use are assumed (see[7]).
Modification of the leakage volume flow	no[8]	

Fault assumed	Fault exclusion	Remarks
Bursting of the valve housing and the breaking of the moving component as well as fracture of the fixing and cover screws.	yes, when design, construction and sizing have been to recognised rules of technology and state of the art	
Uncontrolled "command and control behaviour" of servo- and proportional valves by pneumatic faults, in particular without control. (This fault assumption occurs for these valves in addition to those faults already assumed. If in addition to the safe switching position (middle or end position) there are arbitrary safety-relevant intermediate positions, then the electronic control must also be subject to safety evaluation, see "Faults list for electric components".) **Note:** If directional control valves are composed of several individual valves (e. g. 5 / 4 directional function by four individual 2 / 2 directional valves) then the fault evaluation has to be carried out for each one of the individual valves. The same procedure has to be followed for pilot valves.	no, for servo-valves yes, for proportional directional control valves if their safety can be evaluated in the same manner as for conventional directional control valves[9)] as a result of their construction	[9)] Important assessment criteria in this respect are for example: – safe electrical segregation of the control energy as a requirement for occupying the safe switching position – occupying the safe switching position upon failure of the control energy by means of sufficiently large mechanical return forces (springs) – sufficient positive overlap in the safe switching position

1.2 Stop valves (check, quick action ventilating and shuttle valves) (Pn)

Fault assumed	Fault exclusion	Remarks
Modification (extension) of the switching times	no[1)]	[1)] Because, for example, of wear, material fatigue (e.g. springs), external influences, chemical effects of lubricants on seals, blockages of slits and nozzles, it is not possible to exclude faults.

Fault assumed	Fault exclusion	Remarks
Non-opening, incomplete opening, non-closure as well as insufficient closure (sticking of the moving component in a final position or in an arbitrary intermediate position)	no, when the control of the moving component is similar to the case of valve pistons[2)] yes, when the control of the moving component is similar to the case of ball seat valve[3)] and there is a specification level below that of "self-monitoring"	[2)] This applies e.g. to check valves in cartridge form but also usually for controlled ball seat valves (e.g. unlatchable check valve) because in this case one also has to consider the control of the actuating mechanism (e.g. actuating piston). In these cases, because of[1)] it is not possible to exclude faults. [3)] For non-controlled ball seat valves, sticking of the moving component is usually sufficiently improbable because of[1)]. [4)] Normal assembly and operating conditions occur, if the conditions foreseen by the manufacturer are respected, no particular mass force acts on the moving component and no extreme vibration or shock loading occur. [5)] Abnormal conditions of use will occur, e.g. in the case of considerable solid loading and / or high humidity content of the atmosphere and / or high lubricant fraction in the compressed air. [6)] It is assumed over a long period that changes in the valves seat occur (e.g. due to wear, chemical changes in the packing material). In addition, partial deformation of the packing and / or valve seats in abnormal conditions are assumed (see[5)]).
Automatic change of the initial switching position (without control)	yes, for normal assembly and operating conditions[4)] and when there is sufficient closure force on the basis of available pressure and areas	
Simultaneous closure of both inlet connections in two-way valves	yes, when, because of construction and design of the moving component, the simultaneous closure is sufficiently improbable	
Leakage	yes, when normal operating circumstances occur and there is sufficient treatment of the compressed air no, for abnormal circumstances[5)]	
Modification of the leakage volume flow	no[6)]	
Bursting of the valve housing and breaking of the moving component as well as fracture of the fixing and cover screws	yes, when design, construction and sizing have been to recognised rules of technology and state of the art	

1.3 Flow valves (Pn)

Fault assumed	Fault exclusion	Remarks
Change in volume flow without change in regulating device	Yes, for flow valves without moving parts[1] (fixed resistances, throttle valves) when normal operating circumstances occur and there is sufficient treatment of the compressed air[2] no, for flow valves with moving parts[3]	[1] The regulating device is not considered as a moving part. Changes in volume flow due to changes in pressure differential are physically limited in this type of valve and are not covered by this assumed fault. [2] Normal operating conditions occur when conditions foreseen by the manufacturer are observed and no abnormally high abrasion and no large solid particles (in relation to the cross-section of the throttle) in the systems are expected. [3] Due, e.g. to wear, material fatigue (among other things springs), external influences, an uncontrolled behaviour of the moving component (one-way restrictor) has to be assumed.
Automatic modification of the regulating device	yes, for effective protection of the regulating device, adapted to the particular case, under consideration of technically safe immobilisation (e.g. lead seals)	
Unintentional screwing out of the operating element in the regulating device	yes, when an effective positive locking protection against unscrewing is available	
Bursting of the valve housing and breaking of the moving component as well as fracture of the fixing and cover screws	yes, when design, construction and sizing have been to recognised rules of technology and state of the art	

1.4 Pressure valves (Pn)

Fault assumed	Fault exclusion	Remarks
Non-opening or insufficient opening (spatially and temporally) when exceeding the set pressure or non-closure or insufficient closure (spatially and temporally) if pressure drops below the set value (sticking or difficult movement of the moving component[1])	no, when the control of the moving component is similar to the case of valve pistons[2), 3)] yes, when the control of the moving component is similar to the case of a ball seat or membrane valve (e. g. for pressure reducing valve with secondary pressure relief)[4)] and if there is a specification level below that of "self-monitoring"	[1)]This fault assumption applies only if the function of pressure valves is determining, in particular for dynamic effects (e.g. clamp). It does not apply for its normal function in pneumatic systems (e.g. pressure limitation, pressure decrease). It also does not apply to the application of type-approved pressure limitation valves. In the latter application there is only an occasional actuation of the valve so that influences as per[3)] are less probable. [2)] This applies for example to pressure regulating piston type valves. Because of 3) it is not possible to exclude a fault. [3)] E.g. wear, external influences, blockage of nozzles, chemical effect of lubricants on packing, mean that sticking of the moving component cannot be excluded. [4)]In the case of ball seat and diaphragm valves, the control is usually laid out in such a way that sticking of the moving part because of[3)] is sufficiently improbable. [5)] Due, e.g. to material fatigue (control spring, membrane), blokkage of nozzles, it is not possible to exclude faults. [6)] The spring tension remains largely intact, if the wire diameter is larger than the winding spacing (coiling after wire rupture is prevented) and the spring is sufficiently guided (sharp bending after wire rupture, is prevented). [7)] Because the required set point is given by the electronics and because there are moving components[3)], it is usually not possible to exclude faults.
Modification of the pressure control behaviour without modification of the regulating device[1)]	no[5)] yes, in the case of direct actuation of pressure limitation valves and pressure switch valves if the spring force is largely retained after break of the spring[6)]	
Modification of the pressure control behaviour by unwanted modification of the control value in the case of proportional pressure valves[1)]. (This fault assumption occurs in these valves in addition to the other fault assumptions)	no[7)]	

Fault assumed	Fault exclusion	Remarks
Automatic modification of the regulating device	yes, for effective protection of the regulating device, adapted to the particular case, under consideration of technically safe immobilisation (e.g. lead seals)	
Unintentional screwing out of the operating element in the regulating device	yes, when an effective positive locking protection against unscrewing is available	
Leakage	yes, for seat and diaphragm valves and piston valves with elastic packing in normal conditions of use and if sufficient treatment of the compressed air is available no, for seat valves in abnormal circumstances[8)]	[8)] Abnormal conditions of use will occur, e.g. in the case of considerable solid loading of the compressed air (internal or external causes) and / or high humidity and / or high lubricant content of the compressed air. [9)] Changes in the valve seat (e.g. by wear, chemical changes in seal material) are assumed over a long time period. In addition, partial deformations of the packing and / or valve seat in abnormal conditions of use are assumed (see[8)]).
Modification of the leakage volume flow	no[9)]	
Bursting of the valve housing and breaking of the moving component (except control spring, membrane) as well as fracture of the fixing and cover screws	yes, when design, sizing and construction have been to recognised rules of technology and state of the art	

2 Ducts (Pn)

2.1 Pipework (Pn)

Fault assumed	Fault exclusion	Remarks
Bursting and leakage	yes, when in particular the sizing, choice of materials, manufacture, configuration and attachment have been to recognised rules of technology and state of the art[1)]	[1)] When using plastic pipes, it is necessary to consider the manufacturer's data, in particular with respect to operational environmental influences, (e.g. thermal influences, chemical influences, influences due to radiation). When using steel pipes that have not been treated with corrosion retardant media, it is particularly important to provide sufficient drying of the compressed air.

Fault assumed	Fault exclusion	Remarks
Rupture at the connecting element	yes, when using usual connecting elements, when no particular safety requirements are placed[2] and when sizing, choice of materials, manufacture, configuration and attachment have been to recognised rules of technology and state of the art	[2] No specific safety requirements exist if, for example, no hazardous machine motion can be expected, e.g. resulting from the failure of the pipework.
	no, when using connecting elements for plastic pipe (bayonet-crimp system among others) if specific safety requirements are placed[3]	[3] Specific technical requirements exist if, for example, masses are held pneumatically in a high position or decelerated (at large kinetic energies) and personnel may be in the danger area.
	yes, when using cutting ring union pieces or threaded pipe (i.e. steel pipes) if sizing, choice of materials, manufacture, configuration and attachment have been to recognised rules of technology and state of the art	
Clogging (blockage)	yes, for pipework in the power circuit as well as for control and measurement lines when no particular safety requirements are placed	
	yes, when the nominal diameter of the line is ≥ 2 mm	[4] Specific safety requirements exist if a faulty control signal can create a hazard, e.g. in the case of valve monitoring using a pressure switch.
	no, if specific safety requirements are placed[4] and the nominal diameter of the line is < 2 mm	
Kinking of the plastic pipes with a small nominal diameter	yes, for pipework in the power circuit as well as control and measurement lines when no specific safety requirements are placed[4]	
	yes, when a properly protected displacement of the pipes takes place taking account of the relevant manufacturer's data (e.g. minimum curvature radius)	

Fault assumed	Fault exclusion	Remarks
	no, if specific safety requirements are placed[4] and no properly protected displacement of the pipes takes place taking account of the relevant manufacturer's data (e.g. minimum curvature radius)	

2.2 Hose assemblies (Pn)

Fault assumed	Fault exclusion	Remarks
Bursting, tearing out of attachment and leakage	yes, when there are no particular safety requirements[1] and when in particular the sizing, choice of materials, manufacture, configuration and attachment have been to recognised rules of technology and state of the art no, when particular safety requirements are placed[2] (also when the sizing, choice of materials, manufacture, configuration and attachment have been to recognised rules of technology and state of the art) yes, if specific safety requirements are placed, if one uses hose assemblies manufactured to DIN 20066 made of relevant hoses (at least hoses with fabric insets, Type 2 TE as per DIN 20021, Part 2 with the corresponding hose fittings[3]	[1] There are no particular safety requirements if, e.g. the hose assembly fails without any hazardous machine movement being expected, and if the time persons spend in potentially dangerous areas near the hose assembly is small. [2] Specific safety requirements exist if, e.g. masses are pneumatically maintained in a lifted position or are decelerated (at high kinetic energy), with persons in the danger zone or there is an immediate risk to persons due to failure of the hose assembly (whipping of pipe). In this case, mainly manufacturing defects in the hose and hose assembly and age-induced or environmentally-induced decreases in performance have to be assumed. [3] Failure of the hose assembly can be considered sufficiently improbable if the hose assembly is manufactured and installed according DIN 20066.
Clogging (blockage)	yes, for hose assemblies in the power circuit and in the case of control and measurement lines when no particular safety requirements are placed	

Fault assumed	Fault exclusion	Remarks
	yes, when the nominal diameter of the line is ≥ 2 mm no, when there are no specific safety requirements[4)] and the nominal diameter is < 2 mm	[4)] Specific safety requirements exist if a faulty control signal can create a hazard, e.g. in the case of valve monitoring using a pressure switch.

2.3 Connecting elements (Pn)

Fault assumed	Fault exclusion	Remarks
Bursting, failure of attachment screws or tearing out of screws	yes, if sizing, material choice, manufacture, configuration and connection to the pipework or fluid-technological component have been to recognised rules of technology and state of the art	
Leakage (failure of leaktightness)	no[1)]	[1)] Due to wear, ageing, deterioration of the elasticity, etc. it is not possible to exclude faults over a long period. A sudden major failure of the leaktightness is not assumed.
Clogging (blocking)	yes, for use in the power circuit and in the case of control and measurement lines when no particular safety requirements are placed on the control or measurement signal yes, if the nominal diameter is ≥ 2 mm no, if particular safety requirements are placed[2)] and the nominal diameter is < 2 mm	[2)] Specific safety requirements exist if a faulty signal can create a hazard, e.g. in the case of valve monitoring using a pressure switch.

3 Cylinders (Pn)

Fault assumed	Fault exclusion	Remarks
Loss of the leaktightness of pressure chambers or change in leaktightness	no[1)]	[1)] Because of wear of seals, wipers and guides it is not possible to exclude faults over a long time period. Sudden major failure of leaktightness is not assumed. [2)] See 1.3 "Valves – Flow valves" (Pn) (change in volume flow with no change in control element)
Failure of the end of course damping	yes, if no failure of the flow valve (one-way restrictor) at the end of course damping is assumed[2)] no, if failure of the flow valve (one-way restrictor) at the end of course damping is assumed[2)]	
Loosening of the connection piston / piston rod as well as piston rod / machine	yes, if design and manufacture have been to recognised rules of technology and state of the art and possibly answer specific safety requirements	
Bursting of the pressure chambers as well as fracture of the attachment and cover screws	yes, if sizing, material choice, configuration and attachment have been to recognised rules of technology and state of the art	
Buckling of piston rods	yes, if sizing, material choice, configuration and attachment have been to recognised rules of technology and state of the art	

4 Pressure transmitter / pressure medium transducer (Pn)

Fault assumed	Fault exclusion	Remarks
Loss of the leaktightness of pressure chambers or change in leaktightness	no[1)]	1)Because of wear of seals and guides it is not possible to exclude faults over a long time period. Sudden major failure of leaktightness is not assumed.
Bursting of the pressure chambers as well as fracture of the attachment and cover screws	yes, if sizing, material choice, configuration and attachment have been to recognised rules of technology and state of the art	

5 Compressed air treatment (Pn)

5.1 Filter (Pn)

Fault assumed	Fault exclusion	Remarks
Blockage of the filter element	no[1)]	[1)] In particular after work on the compressed air generating plant and on the pipework in the compressed air network, as well as in the case of compressed which has not been or only incompletely been treated, one can expect blockage of the filter even if correctly sized. [2)] In exceptional cases (large volume) it can be necessary to also consider the requirements of the pressure vessel ordinance including all relevant rules.
Rupture of the filter element	yes, if the filter is sufficiently resistant to pressure	
Failure of the dirt indicator or dirt monitor	no	
Bursting of the filter housing and fracture of the cover screws or connecting screws	yes, when sizing, material choice, configuration and attachment have been to recognised rules of technology[2)] and state of the art	

5.2 Oiler (Pn)

Fault assumed	Fault exclusion	Remarks
Change in the set value (oil volume per unit time) without modification of the regulating device	no[1)]	[1)] As a result of clogging of slits and nozzles, it is not possible to exclude a fault.
Automatic modification of the regulating device	yes, if there are no extreme vibration loads	
Unintentional screwing out of the operating element in the regulating device	yes, when an effective, positive locking protection against unscrewing is available	
Bursting of the housing and fracture of the fixing and cover screws	yes, when design, sizing and construction have been to recognised rules of technology and state of the art	

5.3 Muffler (Pn)

Fault assumed	Fault exclusion	Remarks
Blockage of muffler	yes, if no particular safety requirements exist no, if particular safety requirements[1] exist yes, if because of the construction and design, a clogging of the muffler element can be excluded[2]	[1] Specific safety requirements exist if an increased pressure in the offgas can result in a hazard, e.g. by failure to switch or unwanted switching or delayed switching of a valve. [2] Clogging of the muffler element or the increase in the pressure in the offgas above a certain critical value is sufficiently improbable for a corresponding diameter and / or corresponding design of the muffler element.
Unintentional screwing out of the muffler / muffler element	yes, if an effective guard against unscrewing exists	
Fracture / bursting of the muffler housing and fracture of the attachment thread	yes, if sizing and construction are to recognised rules of technology and state of the art	

6 Accumulators (pressure vessels) (Pn)

Fault assumed	Fault exclusion	Remarks
Bursting of the pressure vessel and breach of connecting and cover screws well as tearing out of attachment screws	yes, when construction equipment and location in the system respond to requirements[1] and are to recognised rules of technology and state of the art	[1] Requirements on construction and equipment are laid down in particular in the pressure vessel ordinance and relevant rules.

7 Motors (Pn)

Fault assumed	Fault exclusion	Remarks
Modification of the suction stream in compressed air motors	yes, for short time periods[1]	[1] For longer time periods one has to assume a modification through wear of the moving parts and seals.

Fault assumed	Fault exclusion	Remarks
Automatic change of the suction setting without actuation of the regulating device in compressed air motors	yes, in the case of compressed air motors if no particular requirements are placed on the adjustment parameters being kept constant no, in the case of compressed air motors if particular requirements are placed on the adjustment parameters being kept constant[2)]	[2)] There are particular requirements if, for example, speeds, rotational speeds or torque have to be maintained to the standard required for single failure safety or self-monitoring. Corresponding fault assumption, see 1.3 "Valves – Flow valves" (Pn) and / or 1.4 "Valves – Pressure valves" (Pn).
Rupture or loosing of the drive / output connecting elements (couplings) as well as bursting of the housing and rupture of the cover and attachment screws	yes, if design, construction and sizing are to recognised rules of technology and state of the art	

8 Sensors (Pn)

Fault assumed	Fault exclusion	Remarks
Failure of the sensor[1)]	no[2)]	[1)] This definition encompasses in this case signal capture, processing and output in particular of pressure, volume flow, temperature and direction.
Modification of the coverage and output characteristic	no[2)]	[2)] Because, for example, of wear, material fatigue (among other things, springs) external influences, blockage of slits and nozzles as well as failure an / or modification in the behaviour of the electrical / electronic components it is not possible to exclude failure.

9 Information processing (Pn)

9.1 Logical switching element (Pn)

Fault assumed	Fault exclusion	Remarks
Failure of the logical switching element[1] due to e.g. modification of the switching times, failure to switch or incomplete switching	no[2] yes[2]	[1] This covers pneumatic logical switching elements such as e.g. AND-element, OR-element, storage-element [2] Corresponding fault assumptions as well as fault exclusions see 1.1 "Valves – Directional control valves" (Pn) 1.2 "Valves – Stop valves" (Pn) 1.3 "Valves – Flow valves" (Pn)

9.2 Time lag devices (Pn)

Fault assumed	Fault exclusion	Remarks
Failure of time lag device[1] or Modification of the detection and output characteristic	no[2] yes, for time lag devices without moving components (e.g. fixed resistances), if normal conditions of use apply and there is sufficient treatment of the compressed air[3]	[1] This covers pneumatic as well as pneumatic / mechanical time and counting elements. [2] Due e.g. to wear, material fatigue (among others springs), external influences, chemical influences of lubricants on seals, clogging of nozzles and slits, it is not possible to exclude a fault.
Bursting of the housing and fracture of the fixing and cover screws	yes, if construction and sizing have been to recognised rules of technology and state of the art	[3] Normal operating conditions occur when conditions foreseen by the manufacturer are respected and when no larger solid particles (in relation, e. g. to the cross-section of the fixed resistance) can be expected in the system.

9.3 Converters (Pn)

Fault assumed	Fault exclusion	Remarks
Failure of converter[1)] or Modification of the detection and output characteristic	no[2)] yes, for converters without moving components (e.g. reflex nozzle) if normal conditions of use apply and there is sufficient treatment of the compressed air[3)]	[1)] This covers elements for the conversion of a pneumatic signal into an electrical one, the detection of positions (cylindrical switch, reflex nozzle), for the amplification of pneumatic signals. [2)] Due e.g. to wear, material fatigue (among others springs), external influences, chemical influences of lubricants on seals, clogging of nozzles and slits, it is not possible to exclude a fault. [3)] Normal operating conditions occur when conditions foreseen by the manufacturer are respected and when no larger solid particles (in relation, e.g. to the cross-section of the fixed resistance) can be expected in the system.
Bursting of the housing and fracture of the fixing and cover screws	yes, if construction and sizing have been to recognised rules of technology and state of the art	