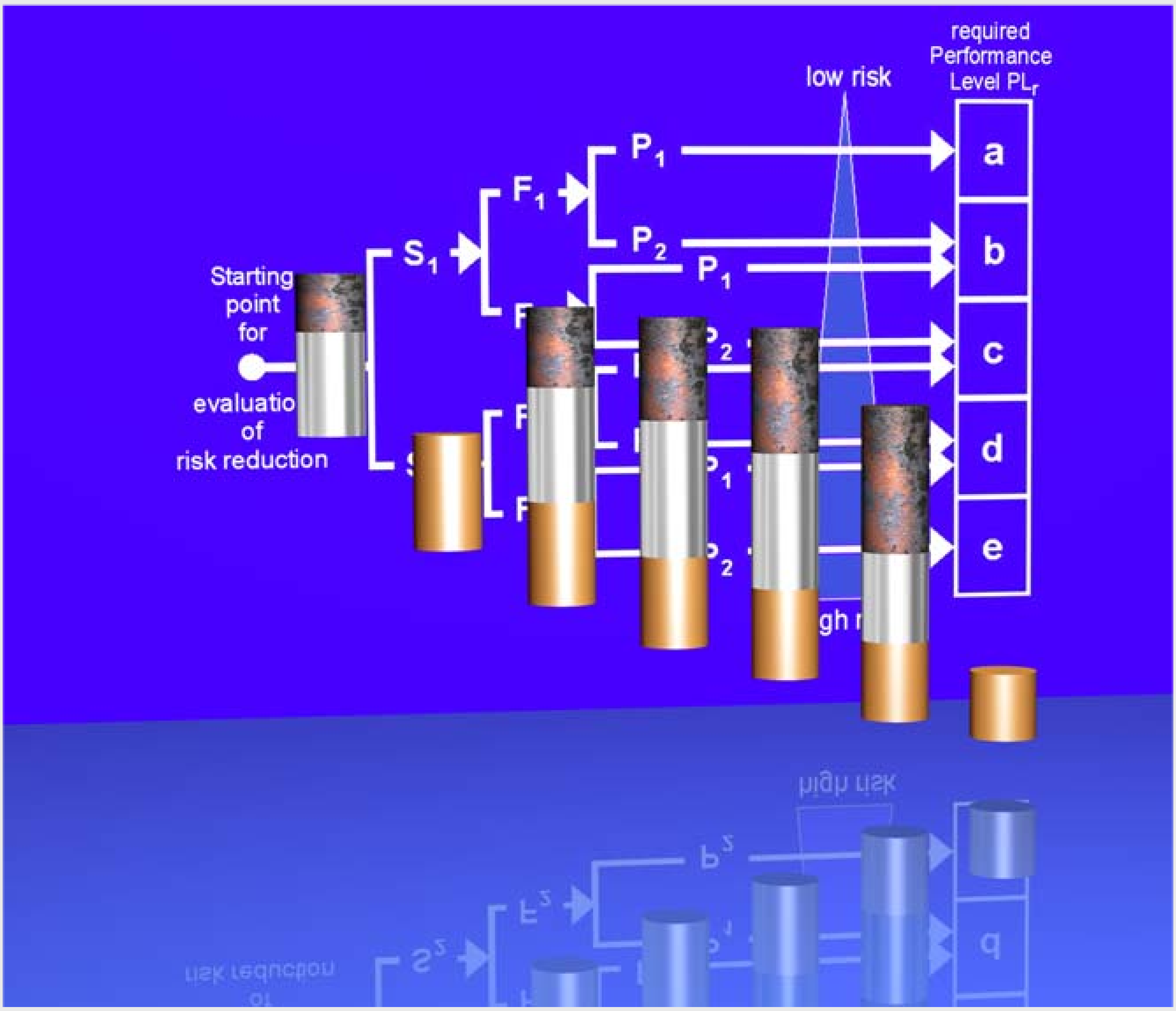
BGIA

Institut für Arbeitsschutz der
Deutschen Gesetzlichen Unfallversicherung

BGIA Report 2/2008e

Functional safety of machine controls – Application of EN ISO 13849 –



Care has been taken in the translation of this report from German. In case of any doubt consider the German version: Funktionale Sicherheit von Maschinensteuerungen – Anwendung der DIN EN ISO 13849 – (BGIA-Report 2/2008, 2nd ed. Dec. 2008, and Erratum as of June 2009)

Authors: Michael Hauke, Michael Schaefer, Ralf Apfeld,
Thomas Boemer, Michael Huelke, Torsten Borowski,
Karl-Heinz Büllesbach, Michael Dorra,
Hans-Georg Foermer-Schaefer, Wolfgang Grigulewitsch,
Klaus-Dieter Heimann, Burkhard Köhler, Michael Krauß,
Werner Kühlem, Oliver Lohmaier, Karlheinz Meffert, Jan Pilger,
Günter Reuß, Udo Schuster, Thomas Seifen, Helmut Zilligen
BGIA – Institute for Occupational Safety and Health of the
German Social Accident Insurance,
Sankt Augustin

Editorial office: Central Division of the BGIA – Institute for Occupational Safety and Health of the German Social Accident Insurance

Published by: German Social Accident Insurance (DGUV)
Mittelstr. 51
10117 Berlin
Germany
Tel.: +49 30 288763-800
Fax: +49 30 288763-808
Internet www.dguv.de
– June 2009 –

ISBN: 978-3-88383-793-2

ISSN: 1869-3491

Functional safety of machine controls
– Application of EN ISO 13849 –

Abstract

The EN ISO 13849 standard, “Safety of machinery – Safety-related parts of control systems”, contains provisions governing the design of such parts. This report describes the essential subject-matter of the standard in its heavily revised 2006 edition, and explains its application with reference to numerous examples from the fields of electromechanics, fluidics, electronics and programmable electronics, including control systems employing mixed technologies. The standard is placed in its context of the essential safety requirements of the Machinery Directive, and possible methods for risk assessment are presented. Based upon this information, the report can be used to select the required Performance Level PL_r for safety functions in control systems. The Performance Level PL which is actually attained is explained in detail. The requirements for attainment of the relevant Performance Level and its associated categories, component reliability, diagnostic coverage, software safety and measures for the prevention of systematic and common-cause failures are all discussed comprehensively. Background information is also provided on implementation of the requirements in real-case control systems. Numerous example circuits show, down to component level, how Performance Levels a to e can be engineered in the selected technologies with Categories B to 4. The examples also provide information on the safety principles employed and on components with well-tried safety functionality. Numerous literature references permit closer study of the examples provided. The report shows that the requirements of EN ISO 13849 can be implemented in engineering practice, and thus makes a contribution to consistent application and interpretation of the standard at national and international level.

Funktionale Sicherheit von Maschinensteuerungen
– Anwendung der DIN EN ISO 13849 –

Kurzfassung

Die Norm DIN EN ISO 13849 „Sicherheit von Maschinen - Sicherheitsbezogene Teile von Steuerungen“ macht Vorgaben für die Gestaltung von sicherheitsbezogenen Teilen von Steuerungen. Dieser Report stellt die wesentlichen Inhalte der Norm in ihrer stark überarbeiteten Fassung von 2007 vor und erläutert deren Anwendung an zahlreichen Beispielen aus den Bereichen Elektromechanik, Fluidtechnik, Elektronik und programmierbarer Elektronik, darunter auch Steuerungen gemischter Technologie. Der Zusammenhang der Norm mit den grundlegenden Sicherheitsanforderungen der Maschinenrichtlinie wird aufgezeigt und mögliche Verfahren zur Risikoabschätzung werden vorgestellt. Auf der Basis dieser Informationen erlaubt der Report die Auswahl des erforderlichen Performance Level PL_r für steuerungstechnische Sicherheitsfunktionen. Die Bestimmung des tatsächlich erreichten Performance Level PL wird detailliert erläutert. Auf die Anforderungen zum Erreichen des jeweiligen Performance Level und seine zugehörigen Kategorien, auf die Bauteilzuverlässigkeit, Diagnosedeckungsgrade, Softwaresicherheit und Maßnahmen gegen systematische Ausfälle sowie Fehler gemeinsamer Ursache wird im Detail eingegangen. Hintergrundinformationen zur Umsetzung der Anforderungen in die steuerungstechnische Praxis ergänzen das Angebot. Zahlreiche Schaltungsbeispiele zeigen bis auf die Ebene der Bauteile hinunter, wie die Performance Level a bis e mit den 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 Literaturhinweise dienen einem tieferen Verständnis der jeweiligen Beispiele. Der Report zeigt, dass die Anforderungen der DIN EN ISO 13849 in die technische Praxis umgesetzt werden können, und leistet damit einen Beitrag zur einheitlichen Anwendung und Interpretation der Norm auf nationaler und internationaler Ebene.

Sécurité fonctionnelle des commandes de machines – Application de la norme EN ISO 13849 –

Résumé

La norme EN ISO 13849 « Sécurité des machines – Parties des systèmes de commande relatives à la sécurité » émet des prescriptions pour la conception de parties de systèmes de commande relatives à la sécurité. Ce rapport présente les éléments essentiels de la norme dans sa version, largement révisée, de 2006 et explique son application à l'aide de nombreux exemples issus des secteurs de l'électromécanique, la fluidique, l'électronique et l'électronique programmable, mais aussi des commandes de technologies diverses. On y montre le lien existant entre la norme et les exigences de sécurité de base contenues dans la directive Machines et certaines procédures d'évaluation des risques y sont présentées. A partir de ces informations, le rapport permet de sélectionner le niveau de performance (required Performance Level PL_r) nécessaire pour les fonctions de sécurité de technique de commande. On y explique en détails comment déterminer le niveau de performance PL vraiment atteint. On y aborde dans les détails les exigences en matière d'obtention du niveau de performance et ses catégories respectives, la fiabilité des composants, la couverture du diagnostic, la sécurité des logiciels et les mesures contre les défaillances systématiques ainsi que les défaillances de cause commune. S'y ajoutent des informations générales concernant l'application des exigences dans la pratique de la technique des commandes. De nombreux exemples de montages montrent, en allant jusqu'au niveau des composants, comment appliquer techniquement le niveau de performance a à e avec les Catégories B à 4 dans les technologies respectives. Ils donnent ainsi des indications concernant les principes de sécurité utilisés et concernant les composants éprouvé en matière de technique de sécurité. Un grand nombre de documents complémentaires mentionnés permettent une meilleure compréhension des exemples donnés. Ce rapport montre que les exigences de la norme EN ISO 13849 peuvent être techniquement mises en pratique et apporte ainsi une aide pour une application et une interprétation cohérente de la norme au niveau national et international.

Aseguridad funcional de sistemas de mando de máquinas
– Aplicación de la norma EN ISO 13849 –

Resumen

La norma EN ISO 13849 “Seguridad de las máquinas - partes de sistemas de mando relativas a la seguridad” establece reglas para el diseño de partes de sistemas de mando relativas a la seguridad. El presente informe presenta los contenidos esenciales de la norma en su versión sustancialmente revisada de 2006 y explica su aplicación a través de numerosos ejemplos de los ramos de la electromecánica, ingeniería de fluidos, electrotécnica y tecnología informática, entre ellos también sistemas de mando de tecnología mixta. Se demuestra la relación de la norma con los requisitos fundamentales de seguridad de la directiva Máquinas, presentando posibles procedimientos para la evaluación de los riesgos. Sobre la base de estas informaciones, el informe permite seleccionar el nivel de prestaciones necesario (required Performance Level PL_r) para funciones de seguridad en la técnica de control. Se explica detalladamente la determinación del Performance Level PL realmente alcanzado. Se exponen en detalle los requisitos para alcanzar el respectivo Performance Level y sus respectivas categorías, la fiabilidad de los componentes, los grados de cobertura del diagnóstico, la seguridad del software y las medidas contra fallos sistemáticos, así como errores originados por una causa común. Informaciones de trasfondo sobre la implementación de los requisitos en la práctica de la ingeniería de control completan la oferta. Numerosos ejemplos de circuitos que abarcan hasta el nivel de los componentes muestran cómo se puede implementar técnicamente el Performance Level "a" a "e" con las Categorías B a 4 en las diversas tecnologías. Estos ejemplos dan indicaciones sobre los principios de seguridad aplicados y los componentes comprobados desde el punto de vista de la técnica de seguridad. Numerosas referencias bibliográficas ayudan a comprender mejor los diversos ejemplos. El informe demuestra que los requisitos de la norma EN ISO 13849 pueden implementarse en la práctica técnica y contribuye, de esta forma, a la aplicación e interpretación unitaria de la norma a nivel nacional e internacional.

Table of contents

1 Foreword

Ten years ago, BIA Report 6/97, “Categories for safety-related control systems in accordance with EN 954-1”, was published. Over the years, it has proved to be a bestseller. Since its appearance, over 6,000 copies of the printed English version have been dispatched, 12,000 copies of the German version. The number of downloads from the website of the BGIA – Institute for Occupational Safety and Health of the German Social Accident Insurance[1] is even higher. The report has even been translated into Japanese.

In the intervening ten years, safety-related machine controls, whether mechanical, pneumatic, hydraulic or electrical, have successfully been divided into five “Categories” according to EN 954-1. With the increasing use of programmable electronic systems, however, a need arose for thorough revision of this standard. This difficult task has now been completed with the publication of EN ISO 13849-1:2007-07. An essential new development is the introduction of concepts from probability theory for the safety analysis and design of control systems. This approach, which gives consideration to the probabilities of failure of components, is enshrined in the IEC 61508 series of electrical basic safety standards. In recognition of the need for all technologies to continue to be classified in an appropriate and above all practicable manner, the Categories have been successfully embedded in the broader concept of the Performance Level.

Not least thanks to the close involvement of experienced experts at the BGIA, the authors of the successor standard EN ISO 13849-1 have succeeded in presenting its content such that it remains practical in its application, despite the complexity of the subject-matter. The new standard has been available in harmonized form since May 2007. A position paper (see Annex I, page 359) by the German Engineering Federation (VDMA, Verband Deutscher Maschinen- und Anlagenbau) explicitly supports its application in machine construction and plant engineering in Germany. Now is therefore an appropriate time for a new, completely revised BGIA Report on safety-related machine control systems. Increasingly complex safety technology necessitates changes to the requirements for guides to application and the expectations of them. Together with the SISTEMA machine safety software (the acronym stands for “Safety Integrity Software Tool for the Evaluation of Machine Applications”) developed at the BGIA, this report aims to serve as the bridge between the “old” and the “new” standard.

The software and the report facilitate access to the new methodologies by users and readers. A team of 20 authors has developed, discussed and validated the text, and in particular the circuit examples, which are of great importance. The result is that the reader is guided step-by-step through the “secrets” of EN ISO 13849-1:2007 and its practical application. The report is not, of course, a substitute for the standard. However, it contains valuable advice, and in particular, enhancements and application

[1] Formerly the BG Institute for occupational safety (BIA)

aids which have already been proofed in the field. The report is intended as a tutorial and a reference work; it should and can fulfil both functions.

Prof. Dr. Helmut Blome
Director of the BGIA

2 Introduction

Since 1st January 1995, all machines placed on the market within the European Economic Area have been required to satisfy the essential requirements of the Machinery Directive [1]. In accordance with Article 1 of this directive, a machine is the 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. The scope of the codified version 98/37/EC [1] of the Machinery Directive covers not only machines, but also safety components which are placed on the market by the manufacturer to fulfil a safety function when in use, and the failure or malfunctioning of which endangers the safety or health of exposed persons.

The essential requirements of the Machinery Directive for machines and safety components can be found in Annex I of the directive. In addition to general principles for the integration of safety this annex contains dedicated sections governing controls for machines and the requirements placed upon protective devices. The essential safety requirements applicable to the design of machines and safety components oblige the manufacturer to conduct assessment in order to identify any hazards associated with the machine. Three principles are stated by which the accident risks associated with each hazard are to be reduced to an acceptable level:

- The elimination or reduction of risks by inherently safe design
- The taking of necessary measures for protection against risks which cannot be eliminated
- The informing of users of residual risks

Under Article 5, the observance of harmonized European standards “listed” in the Official Journal of the European Union gives rise to a presumption of conformity with the essential health and safety requirements of the Machinery Directive. Numerous draft European standards and standards which have now been harmonized as European standards detail and support the underlying philosophy set out in Annex I of the Machinery Directive for the attainment of occupational health and safety on machines. The EN ISO 12100 [2; 3] series of standards, for example, governs basic concepts and general principles for design for the safety of machinery. The procedure for the identification of hazards and for risk estimation and risk evaluation of each hazard is described in full in the new draft of EN ISO 14121-1 [4] and in its technical report, ISO/TR 14121-2 [5]. Based upon these two generic standards, the standards EN ISO 13849-1:2006 [6] and EN ISO 13849-2:2003 [7] describe the necessary risk reduction for the design, structure and integration of safety-related parts of control systems and protective devices, regardless of whether they are electrical, electronic, hydraulic, pneumatic or mechanical in nature. These standards present a generically applicable system of methods for machine controls and/or their protective devices. The Performance Levels described in the standards enhance the concept of Categories familiar from EN 954-1. The safety architectures can now be employed with significantly more flexibility. An essential advantage of EN 954-1 is its treatment of safety-related parts of control systems independently of the technology employed, as has already been mentioned. In EN ISO 13849-1: 2006 this procedure was retained and substantially enhanced. With the introduction of the Performance Level, combinations of different control structures employing different technologies can now be implemented easily. The new standard offers everything needed from a single source encompassing fewer than 100 pages. The methods are formulated neutrally with regard to the specific application or the technology employed, and can therefore be referenced by virtually all product standards (type C standards) and cited in the machine-specific standards.

With entry into force of the new Machinery Directive [8] on 29 December 2009, the harmonized standard acquires greater importance. An essential new element for example is the inclusion of safety-related logic (also described as the safety-related parts of control systems) in Annex IV of the new directive. Such Annex IV products are subject to special treatment under the directive unless they are manufactured to harmonized standards listed in the Official Journal. On the one hand, Annex IV products are no longer subject to compulsory EC type examination[2]; they can, for example, be placed on the market on the basis of an extended manufacturer's quality management (QM) system inspected by a notified body. However, the new directive places the spotlight on control systems with regard to the safety analysis [9; 10].

Together with Part 2 of the standard, EN ISO 13849-2:2003 [7], which has already been harmonized, EN ISO 13849-1:2006 [6] replaces EN 954-1:1996 [11]. Following the standard's initial appearance, a slightly amended version has been in force since June 2008[3]. For the first time a three-year transitional period has been laid down, ending in December 2009, during which EN 954-1:1996 remains in force simultaneously. Until the latter is withdrawn, the user may therefore choose to apply either standard. In order to simplify the transition from the familiar Categories required previously to the required Performance Level PL_r of the new standard, Chapter 5 of this report describes one possible procedure.

The purpose of the present BGIA Report is to describe the application of EN ISO 13849 and in particular its practical implementation with reference to numerous model solutions. Neither the explanations nor the examples should be regarded as an official national or European comment upon EN ISO 13849-1. Rather, the report is a compilation of almost thirty years' experience gained at the BGIA – Institute for Occupational Safety and Health of the German Social Accident Insurance in the assessment of safety and control facilities employing various forms of technology, and the institute's many years of involvement in relevant national and international standards committees.

[2] In addition to the EC type examination, provided a harmonized and listed standard exists, the current Machinery Directive enables the manufacturer: to declare that he has constructed his machine in accordance with this harmonized and listed standard, and to deposit the documentation with a notified body; or to declare that he has constructed his machine in accordance with this harmonized and listed standard, and to deposit the documentation with a notified body and to have the documentation inspected; or to have his product tested by a notified body and to deposit the relevant documentation there.

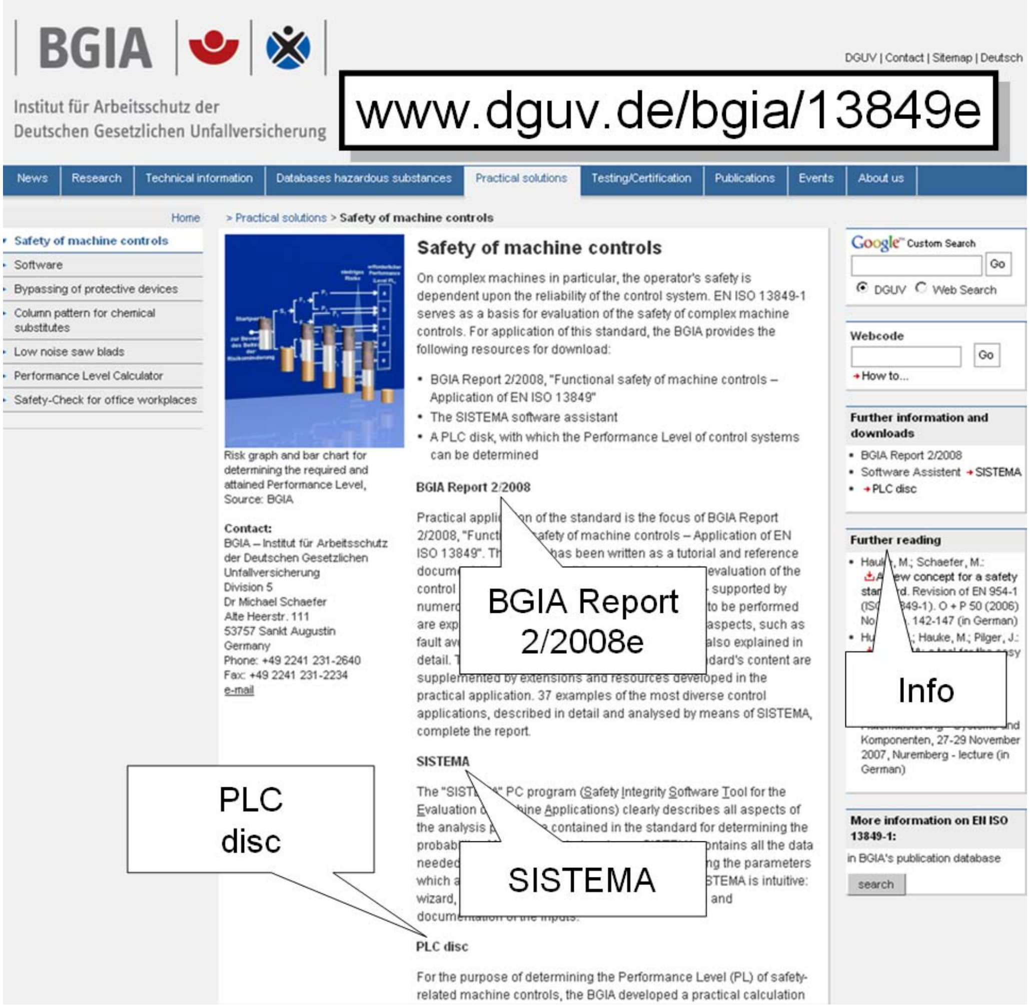
[3] Both parts of the standard were released in new versions EN ISO 13849-1:2008-06 and EN ISO 13849-2:2008-06. The changes with regard to the previous versions only affect the Annexes ZA and ZB, to implement the reference to the new Machinery Directive.

Chapter 3 deals with the generic standards governing functional safety on machines and machinery installations. Chapter 4 presents an overview of the structure of this report with regard to application of EN ISO 13849.

The authors hope that this report will be of genuine assistance to designers, operators and OSH experts in implementation of the requirements for the safety-related parts of control systems. The present interpretation of the standard has been tested in practice in the most diverse of applications, and the examples have been implemented in numerous actual cases.

The internet page "www.dguv.de/bgia/13849e" serves as a common entry to all information and help provided by the BGIA for the functional safety of machinery control systems (see Figure 2.1). In addition to the free BGIA-software SISTEMA (Safety Integrity Software Tool for the Evaluation of Machine Applications), the SISTEMA project files for the circuit examples of Chapter 8 can also be downloaded there. Future amendments will give up to date information to the user.

Figure 2.1:
The common entry page "www.dguv.de/bgia/13849e" links all practical help for safety of machinery control systems


BGIA
Institut für Arbeitsschutz der Deutschen Gesetzlichen Unfallversicherung
DGUV | Contact | Sitemap | Deutsch
www.dguv.de/bgia/13849e
News
Research
Technical information
Databases hazardous substances
Practical solutions
Testing/Certification
Publications
Events
About us
Home
> Practical solutions > Safety of machine controls
Safety of machine controls
Software
Bypassing of protective devices
Column pattern for chemical substitutes
Low noise saw blads
Performance Level Calculator
Safety-Check for office workplaces
Google Custom Search
Go
◉ DGUV ○ Web Search
Webcode
Go
How to...
BGIA Report 2/2008e
SISTEMA
PLC disc
Info
search

Risk graph and bar chart for determining the required and attained Performance Level, Source: BGIA

Contact:
BGIA – Institut für Arbeitsschutz der Deutschen Gesetzlichen Unfallversicherung
Division 5
Dr Michael Schaefer
Alte Heerstr. 111
53757 Sankt Augustin
Germany
Phone: +49 2241 231-2640
Fax: +49 2241 231-2234
e-mail

Safety of machine controls

On complex machines in particular, the operator's safety is dependent upon the reliability of the control system. EN ISO 13849-1 serves as a basis for evaluation of the safety of complex machine controls. For application of this standard, the BGIA provides the following resources for download:

- BGIA Report 2/2008, "Functional safety of machine controls – Application of EN ISO 13849"
- The SISTEMA software assistant
- A PLC disk, with which the Performance Level of control systems can be determined

BGIA Report 2/2008

Practical appli on of the standard is the focus of BGIA Report 2/2008, "Funct afety of machine controls – Application of EN ISO 13849". Th has been written as a tutorial and reference docum evaluation of the control supported by numer to be performed are exp aspects, such as fault av also explained in detail. T dard's content are supplemented by extensions and resources developed in the practical application. 37 examples of the most diverse control applications, described in detail and analysed by means of SISTEMA, complete the report.

SISTEMA

The "SIST A" PC program (Safety Integrity Software Tool for the Evaluation o hine Applications) clearly describes all aspects of the analysis p contained in the standard for determining the probab ontains all the data needed ng the parameters which a STEMA is intuitive: wizard, and documentation of the inputs.

PLC disc

For the purpose of determining the Performance Level (PL) of safety-related machine controls, the BGIA developed a practical calculation

Further information and downloads

- BGIA Report 2/2008
- Software Assistent → SISTEMA
- → PLC disc

Further reading

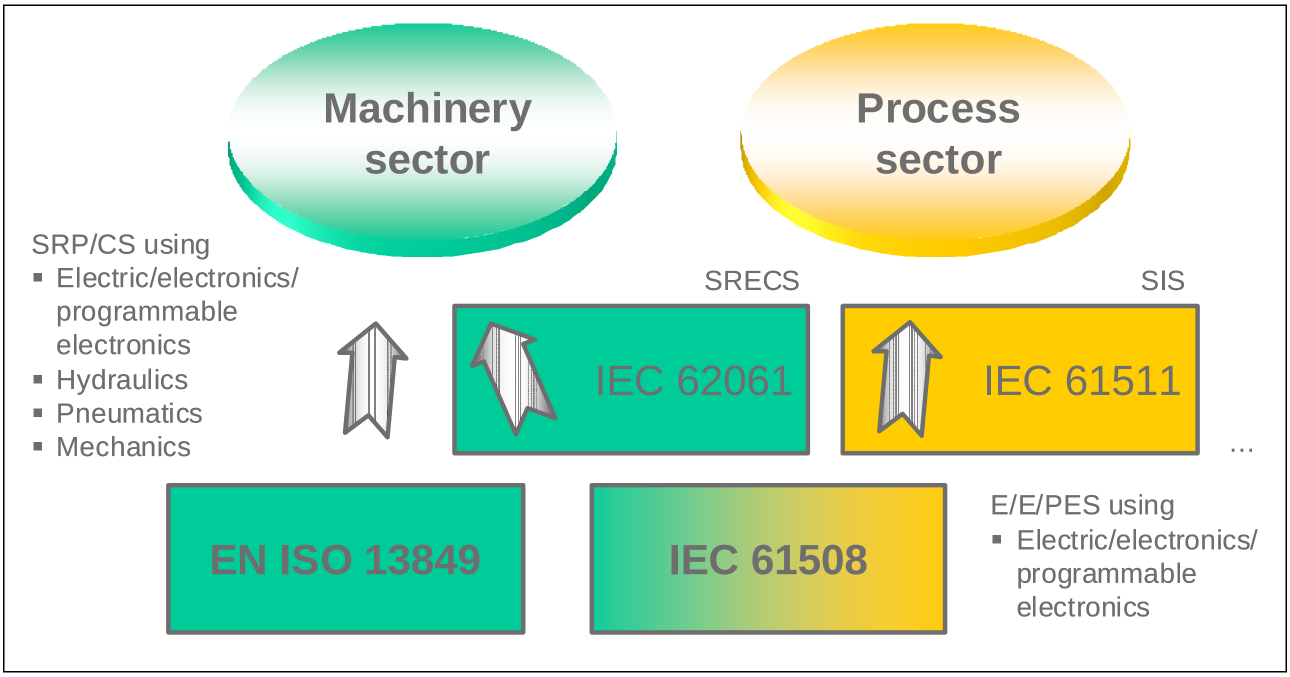
- Hau , M.; Schaefer, M.: A ew concept for a safety sta d. Revision of EN 954-1 (IS 849-1). O + P 50 (2006) No . 142-147 (in German)
- Hu ; Hauke, M.; Pilger, J.: sy nd Komponenten, 27-29 November 2007, Nuremberg - lecture (in German)

More information on EN ISO 13849-1:
in BGIA's publication database

3 Generic standards concerning the functional safety of machinery control systems

In addition to EN ISO 13849, which is discussed in this report, alternative standards of relevance exist in the area of functional safety[4]. As shown in Figure 3.1, these standards are those of the IEC 61508 series [12], and their sector standard IEC 62061 [13] for the machinery industry. Both of these are limited in their scope to electrical, electronic and programmable electronic systems.

Figure 3.1:
Scope of various generic standards concerning functional safety;
SRP/CS: safety-related parts of a control system; SRECS: safety-related electrical control system;
SIS: safety instrumented system; E/E/PES: electrical/electronic/programmable electronic system

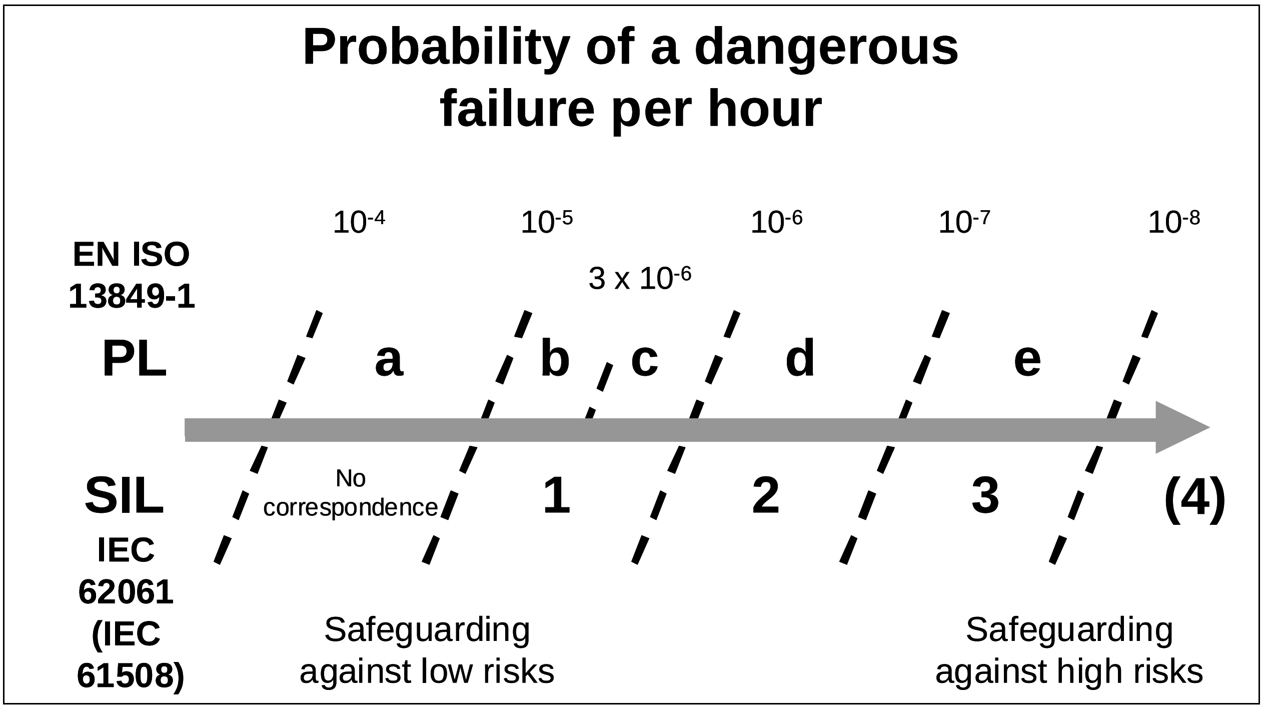


A classification system involving "Safety Integrity Levels" (SILs) is set out in IEC 61508 and IEC 62061. The SILs serve as indicators of the level of safety-related reliability. The associated values are target failure measures, each comprising a decade range[5]. In the low demand mode of operation, the measure is the *PFD* (average **p**robability of **f**ailure to perform the design function on **de**mand), whereas the definition for the high demand or continuous mode of operation is the *PFH* (**p**robability of a dangerous **f**ailure per **h**our) (for further information, refer also to [14]). In the area of machinery and therefore within the scope of IEC 62061, only the second definition is relevant. SIL 4 systems with higher risks are also unknown in the area of machinery, and are therefore not considered in IEC 62061 (Figure 3.2 on page 20).

[4] In this context, functional safety means that potential hazards which arise as a consequence of failures of a control system, i.e. a malfunction, are dealt with.

[5] For each level also the related deterministic and systematic requirements have to be fulfilled.

Figure 3.2:
The Performance Level (PL) and Safety Integrity Level (SIL) representing the probability of a dangerous failure per hour


Probability of a dangerous failure per hour
EN ISO 13849-1
PL
10⁻⁴
10⁻⁵
3 x 10⁻⁶
10⁻⁶
10⁻⁷
10⁻⁸
a
b
c
d
e
SIL
IEC 62061 (IEC 61508)
No correspondence
1
2
3
(4)
Safeguarding against low risks
Safeguarding against high risks

The essential approach of these standards, namely that of defining probabilities of failure as the characteristic parameter without the specific inclusion of architectures, initially appears to be more universal. The approach of EN ISO 13849-1, however, offers users the facility for developing and evaluating safety functions, ranging from a sensor to an actuator (e.g. a valve), under the umbrella of one standard, even though the functions may involve different technologies. Since 2003, Part 1 of EN 954 (and its ISO counterpart ISO 13849) has been accompanied by a Part 2 with the title of “Validation”. With the appearance of the revised Part 1, however, Part 2 requires revision and adaptation. Nevertheless, the requirements stated within it are already astonishingly well-suited to the revised Part 1. The Annexes A to D of Part 2 contain comprehensive material on the subjects of “basic safety principles”, “well-tried safety principles”, “well-tried components” and “fault lists” which continue to be valid under the new Part 1. Details can be found in Annex C of this report (page 301).

The current overlap of the regulatory scope of the two standardization communities initially appears unfavourable to manufacturers of control systems and other users of standards. Both EN ISO 13849-1 and IEC 62061 are harmonized standards pursuant to the Machinery Directive. Parts 1 to 4 of IEC 61508 have the status of basic safety publication from the IEC[6] perspective (with the exception of low complexity systems); this series of standards cannot however be harmonized under the Machinery Directive, even as a European standard. This situation prompts for example the following questions:

[6] IEC = International Electrotechnical Commission

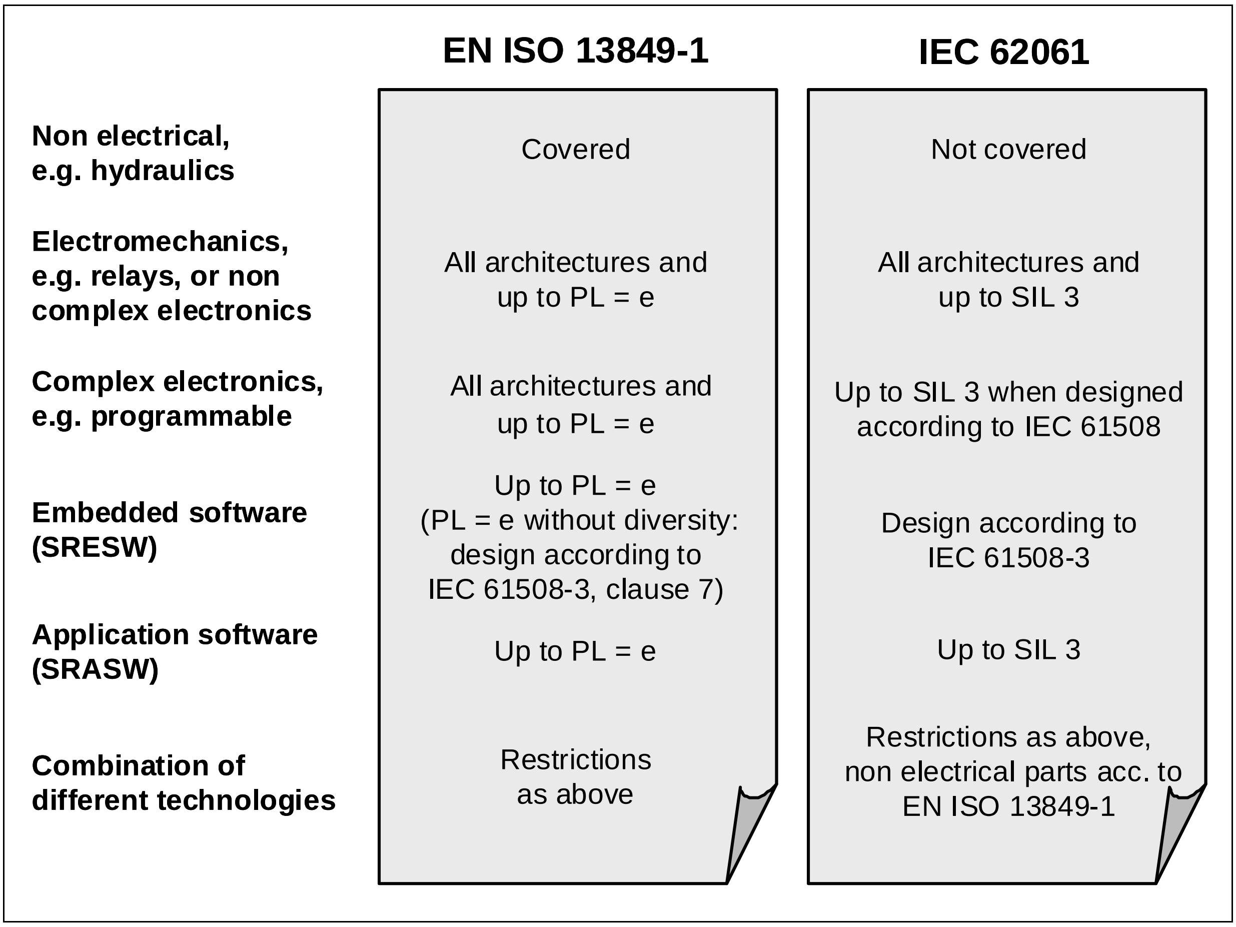
- What standard(s) should be applied for compliance with the Machinery Directive?
- Where they overlap in their scope, do the standards yield equivalent results?
- Are the classification systems of the standards, such as Categories, Performance Level (PL) and Safety Integrity Level (SIL), compatible?
- Can devices which have been developed in observance of one of the two standards be employed during implementation of a safety function in accordance with the other standard?

For the attainment of the greatest possible compatibility with IEC and, if possible, to permit merging of the two areas of standardization in the long term and also to enable the benefits of the probability approach to be exploited without abandonment of the proven Categories, the revised version of EN ISO 13849-1 attempts the balancing-act of uniting both the deterministic approach of the Categories and the aspect of safety reliability with the definition of the Performance Level (PL) (see also [15]). Numerically, as can be seen from Figure 3.2, corresponding classes exist which permit rapid preliminary estimations for practical day-to-day use.

Information on recommendations for application was drawn up by members of the standards committees at the draft stage of EN ISO 13849-1 and IEC 62061, and published virtually verbatim in the introductions to the standards. A key part of this is a Table which is intended to assist the user in selecting the appropriate standard for his particular application. This overview must however be considered obsolete, since it reflects the status of the draft version with regard to EN ISO 13849-1. The restrictions stated are no longer applicable to the current version of the published standard. Effectively, no restrictions now apply; the only requirement is that in the absence of full diversity, safety-related embedded software (SRESW) must satisfy Clause 7 of IEC 61508-3:1998 (refer also to Section 6.3 of this report). In the context of the standard, the designated architectures are also more an optional facility (simplified approach) than a requirement. They should however be regarded as a key element in simplification of the probabilistic approach which has now been implemented in EN ISO 13849, and their application is one of the main aspects of this report. With regard to IEC 62061, the Table indicates that complex, e.g. programmable electronics also falls within the scope of that standard. Although this is correct, the development of “SRECS” (see Figure 3.1) employing this technology must nonetheless be carried out in accordance with IEC 61508 to satisfy the requirements of the standard. Figure 3.3 (see page 22) shows an adapted recommendation which is consistent with the current status of the standard and of its scope.

Even though many experts point out that the results are approximately equivalent whichever of the standards is applied, the requirements are nevertheless quite different in their detail; as a sector standard of IEC 61508, IEC 62061 naturally describes the aspect of “management of functional safety” very explicitly. Development and verification of embedded software to EN ISO 13849-1 is based upon the essential requirements for safety-related software which are currently standard and are also described in IEC 61508. The presentation is based (probably intentionally) upon the “normal case”, without complexity. Broad agreement exists however that requirements from the two standards should not be mixed.

Figure 3.3:
“Adapted recommendation” for the application of EN ISO 13849-1 and IEC 62061



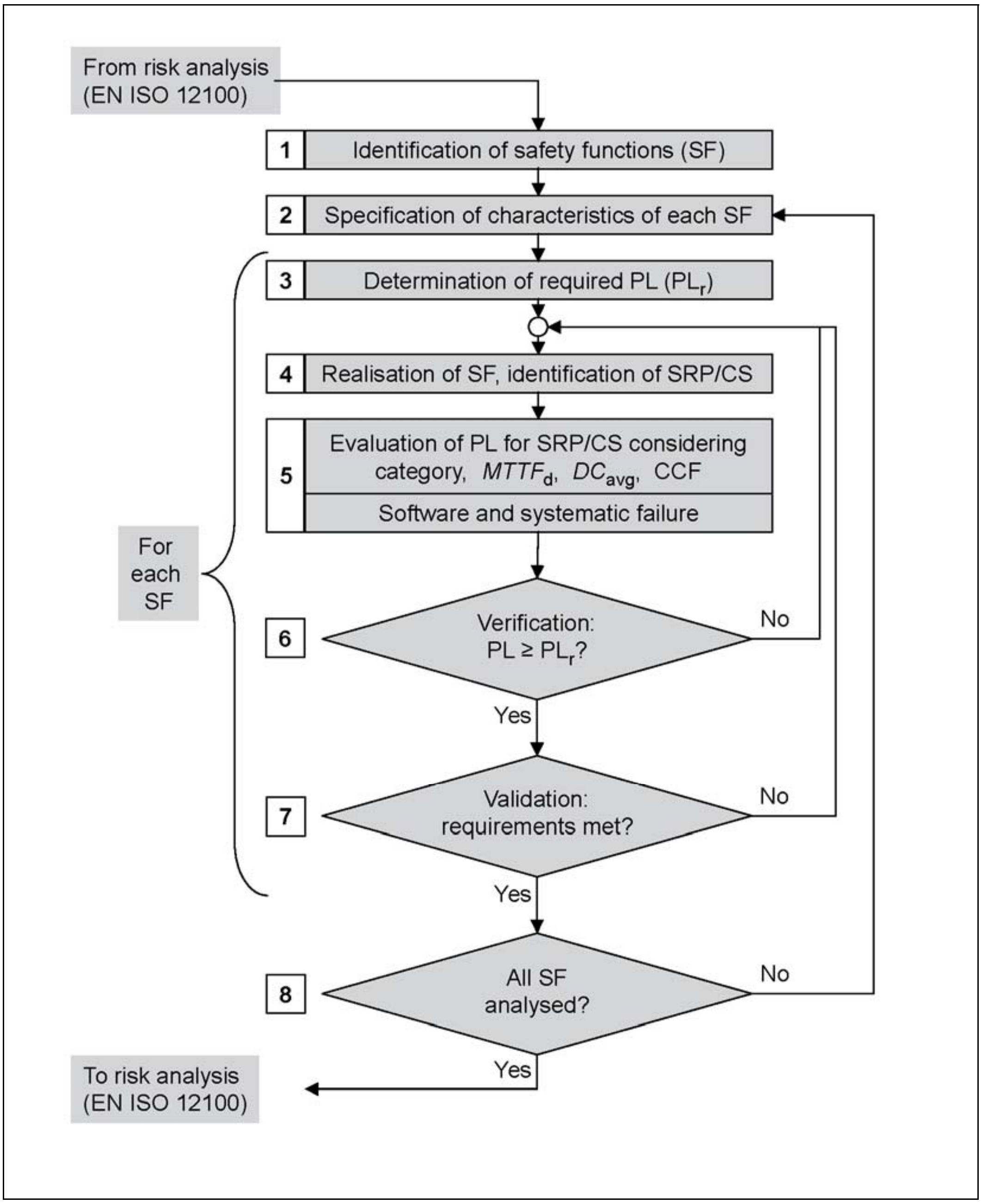
	EN ISO 13849-1	IEC 62061
Non electrical, e.g. hydraulics	Covered	Not covered
Electromechanics, e.g. relays, or non complex electronics	All architectures and up to PL = e	All architectures and up to SIL 3
Complex electronics, e.g. programmable	All architectures and up to PL = e	Up to SIL 3 when designed according to IEC 61508
Embedded software (SRESW)	Up to PL = e (PL = e without diversity: design according to IEC 61508-3, clause 7)	Design according to IEC 61508-3
Application software (SRASW)	Up to PL = e	Up to SIL 3
Combination of different technologies	Restrictions as above	Restrictions as above, non electrical parts acc. to EN ISO 13849-1

Decisive arguments from the user's point of view for the selection of EN ISO 13849 as a basis for the implementation of functional safety in the area of machinery may therefore be considered to be the generic approach with regard to technology, and the simplified approach with regard to quantification, with the use of the designated architectures. This includes the detailed consideration of non-electrical and electro-mechanical components. Manufacturers in particular of safety components which are produced in large quantities, such as a programmable logic controller (PLC) for safety applications, will of course wish to serve other markets in addition to that of machinery, and will therefore employ IEC 61508 in addition to EN ISO 13849 as the basis of their development activity.

4 Report and standard: an overview

This chapter relates the further chapters and annexes of this report to the standard for the reader's benefit. At the same time, it provides an overview of the iterative process for the design of the safety-related parts of control systems, and is therefore based upon Figure 4.1, which corresponds to Figure 3 of the standard.

Figure 4.1:
Iterative process for design of the safety-related parts of control systems;
SF = safety function, PL = Performance Level, PL_r = required Performance Level,
SRP/CS = safety-related parts of control systems, $MTTF_d$ = mean time to dangerous failure,
DC_{avg} = average diagnostic coverage, CCF = common cause failure


From risk analysis (EN ISO 12100)
1 Identification of safety functions (SF)
2 Specification of characteristics of each SF
3 Determination of required PL (PL_r)
4 Realisation of SF, identification of SRP/CS
5 Evaluation of PL for SRP/CS considering category, $MTTF_d$, DC_{avg}, CCF
Software and systematic failure
6 Verification: PL ≥ PL_r?
7 Validation: requirements met?
8 All SF analysed?
Yes
No
For each SF
To risk analysis (EN ISO 12100)

4.1 Identification of safety functions and their properties

The design and assessment process begins with a well-tried concept, i.e. the definition of one or more safety functions (SFs). The procedure is shown in Figure 4.1 by the blocks 1 to 3, and is described in greater detail in Chapter 5. The question to be answered is: In what way do the safety-related parts of the control system contribute towards reducing the risk of a hazard on a machine?

In the first instance, a machine should be constructed such that it is no longer capable of presenting a hazard to the user (inherent safety). The second step is then that of reducing the risk of any hazard which may still arise. This can be attained by protective measures, which are now generally implemented by the control system. In order for these protective measures (also described in their engineered implementation as protective devices) to attain a defined quality in consideration of the risk, an essential step is that of risk assessment. The protective device then serves as a safety-related part of a control system and as such executes the safety function in full or at least in part. It may for example prevent unexpected start-up when an operator enters a hazardous area. Since several safety functions can easily be present on a machine (for example for automatic and setup modes), it is important that careful consideration is given to each individual hazard and the associated safety function.

The safety function can be implemented by parts of the control system or by components which are required in addition to it. In both cases, these parts are safety-related parts of control systems. Although the same hardware may well be involved in the performance of different safety functions, the required quality of the risk reduction for each SF may differ. In the standard, the quality of the risk reduction is defined by the term “Performance Level” (PL). The result of the risk assessment determines the level of the PL value required for the safety function. This specification for the design of the control system is described as the “required Performance Level” PL_r. How is the PL_r obtained?

The risk of a hazard on a machine can be reduced not only by the control system, but also for example by a guard, such as a safety guard, or by personal protective equipment, such as safety goggles. Once it has been established what part is to be played by the control system, the required Performance Level PL_r is determined quickly and directly with the aid of a simple diagram, the “risk graph” (for examples, see Annex A, page 283). Is the associated injury irreversible (e.g. death, loss of limbs), or reversible (e.g. crushing injuries, which can heal)? Is the operator present frequently and for long periods in the hazardous area (e.g. more frequently than once an hour), or infrequently and briefly? Is the operator able to avoid an accident (e.g. owing to slow machine movements)? These three questions determine the PL_r. Details can be found in Section 5.4.

4.2 Design and technical implementation of the safety functions

Once the requirements concerning the safety-related parts of control systems have been defined, they are first designed, and then implemented. Finally, an inspection is conducted to ascertain whether the required risk reduction, the target PL_r value (block 6 in Figure 4.1), can be attained by means of the planned implementation (blocks 4 and 5 in Figure 4.1) with the actual PL value. The steps of blocks 4 and 5 are described in detail in Chapter 6. Following the tradition of BIA Report 6/97, Chapter 8 of this report also contains a large number of calculated circuit examples for all control technologies and each Category. In addition, the general descriptions contained in Chapters 5, 6 and 7 are accompanied by a comprehensively described circuit example. This provides the developer with an illustrative explanation of the methods and parameters described below.

Safety-related parts of control systems are likely to be only as good as the meaningfulness of their safety function. Further quality criteria are: the lifetime of the components employed, their interaction (dimensioning), the effectiveness of diagnostics (e.g. self-tests) and the fault tolerance of the structure. These parameters determine the probability of a dangerous failure and thus the attained PL. The revision of EN ISO 13849-1 places the methods by which the PL is calculated at the user's discretion. The highly complex Markov modelling method may therefore be used in consideration of the parameters stated above. The standard, however, describes a much simplified procedure, namely the use of a bar chart (see Figure 6.10), in which this modelling of the PL is already taken up. Experts interested in the bar chart's derivation will find it in Annex G (see page 347).

In the new version of the standard, the Categories continue to be the basis upon which the PL is determined. Their definition remains essentially unchanged; additional requirements are however now imposed concerning the component quality and the effectiveness of diagnostics. Adequate measures against common cause failure are required in addition for the Categories 2, 3 and 4 (see Table 4.1, page 26).

An overview of the Categories can be found in Table 6.2, the three right-hand columns of which show the new content in the revised standard. An essential aspect when the proposed simplified calculation method is used is the presentation of the Categories as logical block diagrams, the “designated architectures”.

Since the Categories require analysis of the faults (fault avoidance and control), further aspects arise which concern the reliability of the individual components, their fault-mode behaviour, and fault detection by automatic diagnostic measures. Fault lists and safety principles serve here as a basis (see Annex C). In addition to the traditional FMEA (failure mode and effects analysis), EN ISO 13849-1 makes provision for simplified methods of calculation such as the parts count method. A detailed description of this subject can be found in Annex B (see page 289).

One of the questions most frequently asked regarding the probability of failure concerns the sourcing of reliable failure data, the $MTTF_d$ (mean time to dangerous failure) values, for the safety-related components. The technical data sheet of the manufacturer of the parts or components should be given preference here over all other sources. Many manufacturers, including those of pneumatic components, have already indicated that they will make such data available in the future. Whereas, as yet, little is available in the way of data from manufacturers, typical example values can be obtained from established databases (such as SN 29500 or IEC/TR 62380). The standard and Annex D (see page 315) of this report also list a number of realistic values obtained from the field.

Table 4.1:
Deterministic and probabilistic characteristics of the categories;
additions due to the revision of the standard are highlighted in grey

Characteristic	**Category**				
	B	**1**	**2**	**3**	**4**
Design according to relevant standards, withstand the expected influence	X	X	X	X	X
Basic safety principles	X	X	X	X	X
Well-tried safety principles		X	X	X	X
Well-tried components		X			
Mean Time To dangerous Failure – $MTTF_\mathrm{d}$	low to medium	high	low to high	low to high	high
Fault detection (Checks)			X	X	X
Single-fault tolerance				X	X
Consideration of fault accumulation					X
Average diagnostic coverage – DC_avg	none	none	low to medium	low to medium	high
Measures against CCF			X	X	X
Mainly characterized by	Selection of components		Structure		

The effectiveness of diagnostics, in the form of the value for the average diagnostic coverage DC_avg, is easily determined: the test measures which monitor the block are compiled for each block. For each of these test measures, one of four typical DC values is determined from a table in the standard and then used for calculation. Further information can be found in Section 6.2.14 and Annex E. An averaging formula, which appears complex but is in fact simple, can be used to calculate the parameter DC_avg.

The final parameter, that of the CCF (common cause failure, Section 6.2.15) is very easy to calculate: for this parameter, it is assumed that a cause, such as fouling, overtemperature or short circuit, may under certain circumstances give rise to several faults which may for example simultaneously disable both control channels. For control of this source of hazard, it must be demonstrated for Category 2, 3 and 4 systems that adequate measures have been taken against CCF. This is achieved by means of a points system for eight typical counter-measures which are for the most part technical. At least 65 out of a possible 100 points must be attained (Annex F, see page 343).

The random hardware failures, which can be controlled by a good structure and by low probability of failure, are accompanied by the wide field of systematic faults – faults inherent to the system due to its design, such as dimensioning faults, software faults, or logical faults – against which protection is to be provided by measures for fault avoidance and control. The software faults account for a large proportion of such faults. As mentioned in the introduction, the requirements placed in the standard upon the safety-related software are new, but individual aspects of them are familiar from relevant standards. The actual measures are graded according to the required PL. Further information can be found in Section 6.1.2 for systematic failures and in Section 6.3 for software.

4.3 Verification and validation of the control system for each safety function

If the design has already reached an advanced stage by the time the achieved PL is determined, the question arises as to whether this PL is sufficient for each safety function executed by the control system. For this purpose, the PL is compared with the required PL_r (see Block 6, Figure 4.1). If the PL attained for a safety function is inferior to the required PL_r, design improvements on a greater or lesser scale are required (such as the use of alternative components with a superior $MTTF_d$), until the attained PL is adequate. Once this hurdle has been overcome, a series of validation steps are necessary. Part 2 of EN ISO 13849 comes into play for this purpose. This validation process systematically assures that all functional and performance requirements placed upon the safety-related parts of the control system have been attained (see Block 7, Figure 4.1). Further details can be found in Chapter 7.

4.4 Future development of EN ISO 13849-1

Following the appearance of the revised EN ISO 13849-1 in November 2006, a three-year transitional period now applies in which both it and its predecessor, EN 954-1, are valid. This addresses one of the most frequently voiced criticisms, that concerning the scale of the revisions which must first be taken on board by the developers and users. This process is supported once again by the BGIA through the provision of free tools, as was also the case with BIA Report 6/97. These tools take the form both of explanatory literature with examples, and of the "SISTEMA" free software program (the acronym stands for "Safety Integrity Software Tool for the Evaluation of Machine Applications"), which supports calculation and documentation of the PL_r and PL (see Annex H, page 355). The "Performance Level Calculator" [16] developed by the BGIA is already available free of charge; it presents the bar chart in the form of a rotating disc by means of which the PL can be determined simply and precisely at any time. Further tools and literature can be found on the BGIA website at www.dguv.de/bgia/13849e.

5 Safety functions and their contribution to risk reduction

This BGIA Report deals with safety functions and their contribution to reducing risks at hazardous zones on machinery. The design of such safety functions forms part of a process for the design of safe machines. This chapter therefore begins by addressing the requirements of the Machinery Directive, before describing the definition of safety functions and their properties. Section 5.7 then demonstrates implementation with reference to the practical example of a paper-cutting guillotine control.

5.1 Requirements of the EC Machinery Directive

The EC Machinery Directive [1] has been transposed into German law by the Geräte- und Produktsicherheitsgesetz (GPSG, the German Equipment and Product Safety Act). The directive sets out essential health and safety requirements for machines. The general provisions of the Machinery Directive are supported by standards. Particularly significant in this respect is the EN ISO 12100 [2; 3] series of standards, “Safety of machinery – Basic concepts, general principles for design”. A method is presented to the machine designer which is suitable for achieving machine safety. This method – a strategy for risk reduction – includes the design of safety-related parts of control systems[7].

Provided a harmonized product-specific standard (Type C standard) exists for the machine which is to be designed and the reference of the standard has been published in the Official Journal of the EU [17], it may be assumed that the essential health and safety requirements are satisfied. In such cases, the standard is said to give rise to a “presumption of conformity”, since its application justifies the assumption that the machine satisfies the requirements of the EC Machinery Directive. The strategy for risk reduction must however always be followed where a standard giving rise to the presumption of conformity does not exist, where a suitable standard exists but the design has deviated from it, or where additional aspects apply which are not covered by the product standard. In order for issues not covered by a product standard to be identified, the first two steps in the risk-reduction strategy described below must always be performed, i.e. the limits of the machinery must be defined and the hazards identified.

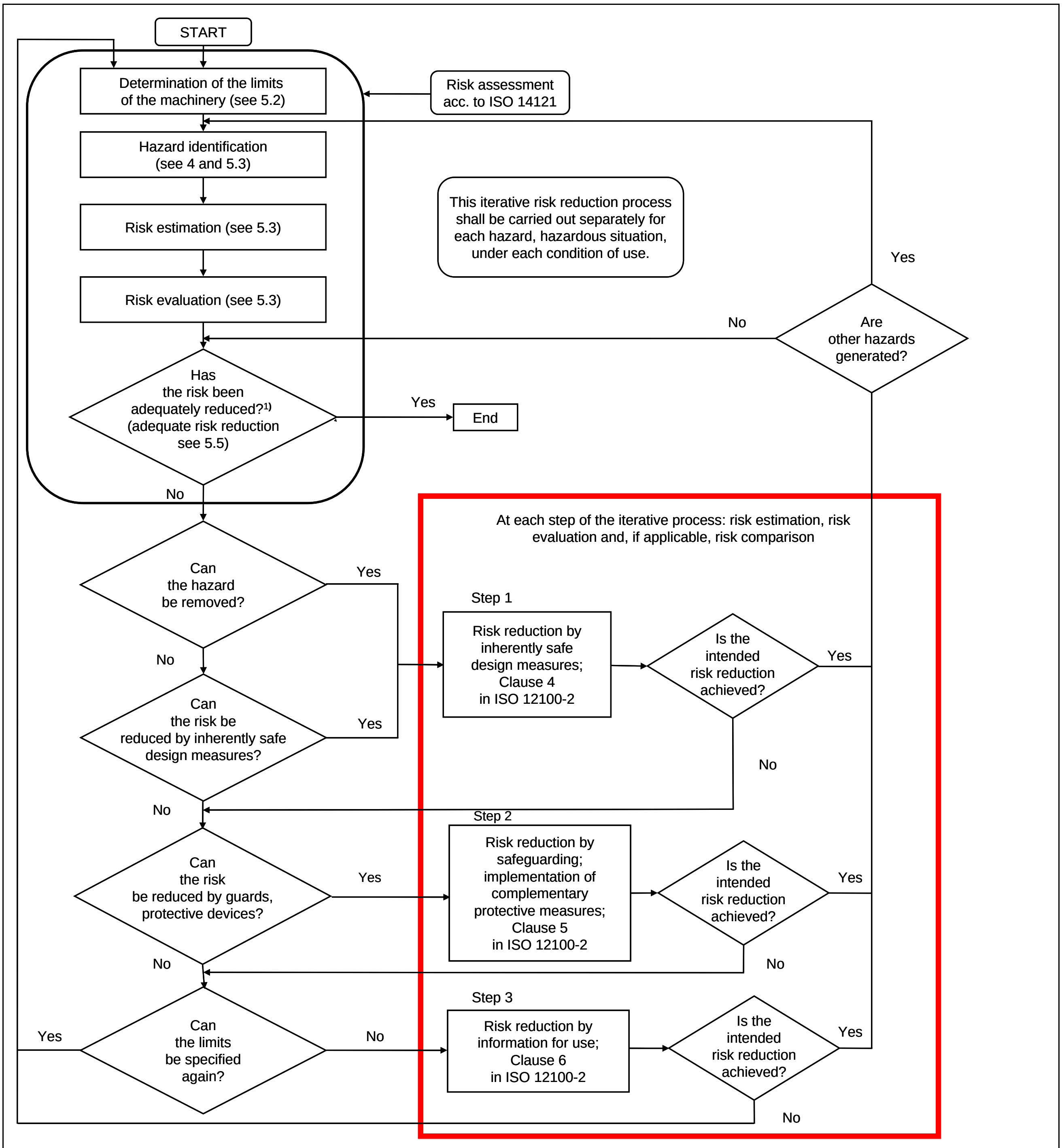
5.2 Risk-reduction strategy

The risk-reduction strategy presented in EN ISO 12100-1 was adopted in Figure 1 of EN ISO 13849-1 and enhanced by the aspects detailed in the latter standard (see Figure 5.1, page 30). A risk assessment is first performed. An important point is the

[7] Safety-related parts of control systems are one means by which a safety function is implemented. These systems begin by receiving safety-related input signals, for example by detecting the position of a safety guard by means of a Type 2 position switch, the separate actuator of which, fitted to the door, itself constitutes a safety-related part. Once received, the signals are processed, leading to generation of an output signal. This process might be performed by a contactor which connects a motor to the electrical system. The contactor constitutes a safety-related part of the control system, whereas the motor and the associated wiring do not.

assumption during the following steps that no protective measures have as yet been taken on the machine. Ultimately, the entire risk-reduction process has the function of determining the type and also the “quality” of the protective measure/protective device which is to be implemented.

Figure 5.1:
Iterative risk-reduction process


START
Determination of the limits of the machinery (see 5.2)
Risk assessment acc. to ISO 14121
Hazard identification (see 4 and 5.3)
Risk estimation (see 5.3)
Risk evaluation (see 5.3)
This iterative risk reduction process shall be carried out separately for each hazard, hazardous situation, under each condition of use.
Yes
No
Are other hazards generated?
Has the risk been adequately reduced?1) (adequate risk reduction see 5.5)
Yes
End
No
At each step of the iterative process: risk estimation, risk evaluation and, if applicable, risk comparison
Can the hazard be removed?
Yes
No
Step 1
Risk reduction by inherently safe design measures; Clause 4 in ISO 12100-2
Is the intended risk reduction achieved?
Yes
No
Can the risk be reduced by inherently safe design measures?
Yes
No
Step 2
Can the risk be reduced by guards, protective devices?
Yes
Risk reduction by safeguarding; implementation of complementary protective measures; Clause 5 in ISO 12100-2
Is the intended risk reduction achieved?
Yes
No
No
Step 3
Yes
Can the limits be specified again?
No
Risk reduction by information for use; Clause 6 in ISO 12100-2
Is the intended risk reduction achieved?
Yes
No

[1] The first time the question is asked, it is answered by the result of the initial risk assessment.

The risk-reduction process begins with definition of the limits of the machine. In addition to the space limits of the machine and its periods of use, particular attention must be paid to the use limits. Such constraints include the intended use of the machine (e.g. permissible materials which may be machined on it), including all service modes and the various facilities for operator intervention. Reasonably foreseeable misuse of the machine must also be considered.

The hazards are then identified; all phases of the machine's lifetime must be considered in this process. In addition to automatic mode, particular attention is paid to operating modes requiring manual intervention, e.g. for:

- Setup
- Testing
- Teaching-in/programming
- Commissioning
- Material charging
- Retrieval of the product
- Troubleshooting
- Cleaning
- Maintenance

Further details concerning this process step can be found in EN ISO 12100-1 and EN ISO 14121-1 [4]. A number of methods exist for systematic identification of the hazards; examples can be found in ISO/TR 14121-2 [5]. Possible hazards are also listed extensively in [4]. Figure 5.2 shows an excerpt.

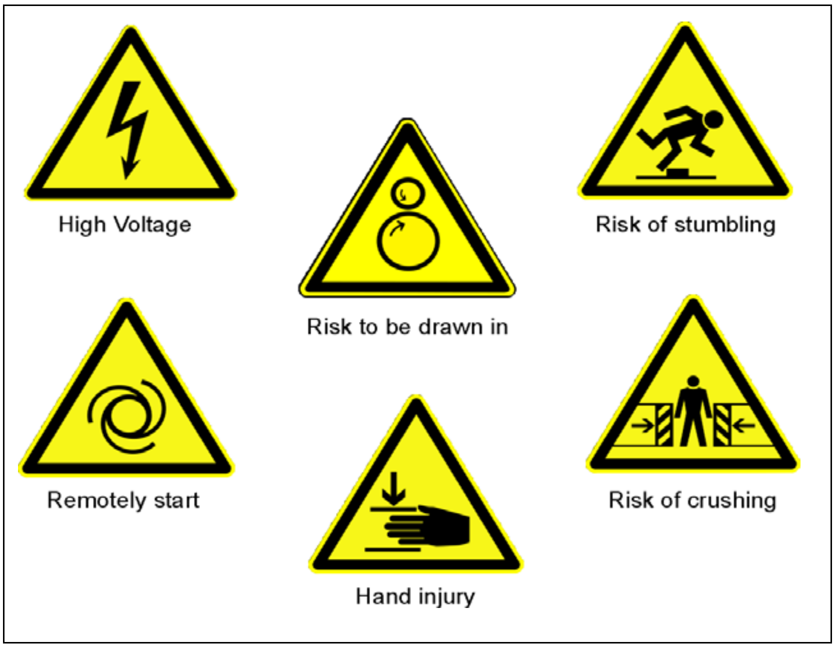


Figure 5.2:
Examples of hazards,
Source: Wikipedia

5.2.1 Risk estimation

Once all potential hazards which may be presented by the machine have been identified, the risk must be assessed for each hazard. The risk associated with a particular hazard situation can be determined from the following risk elements:

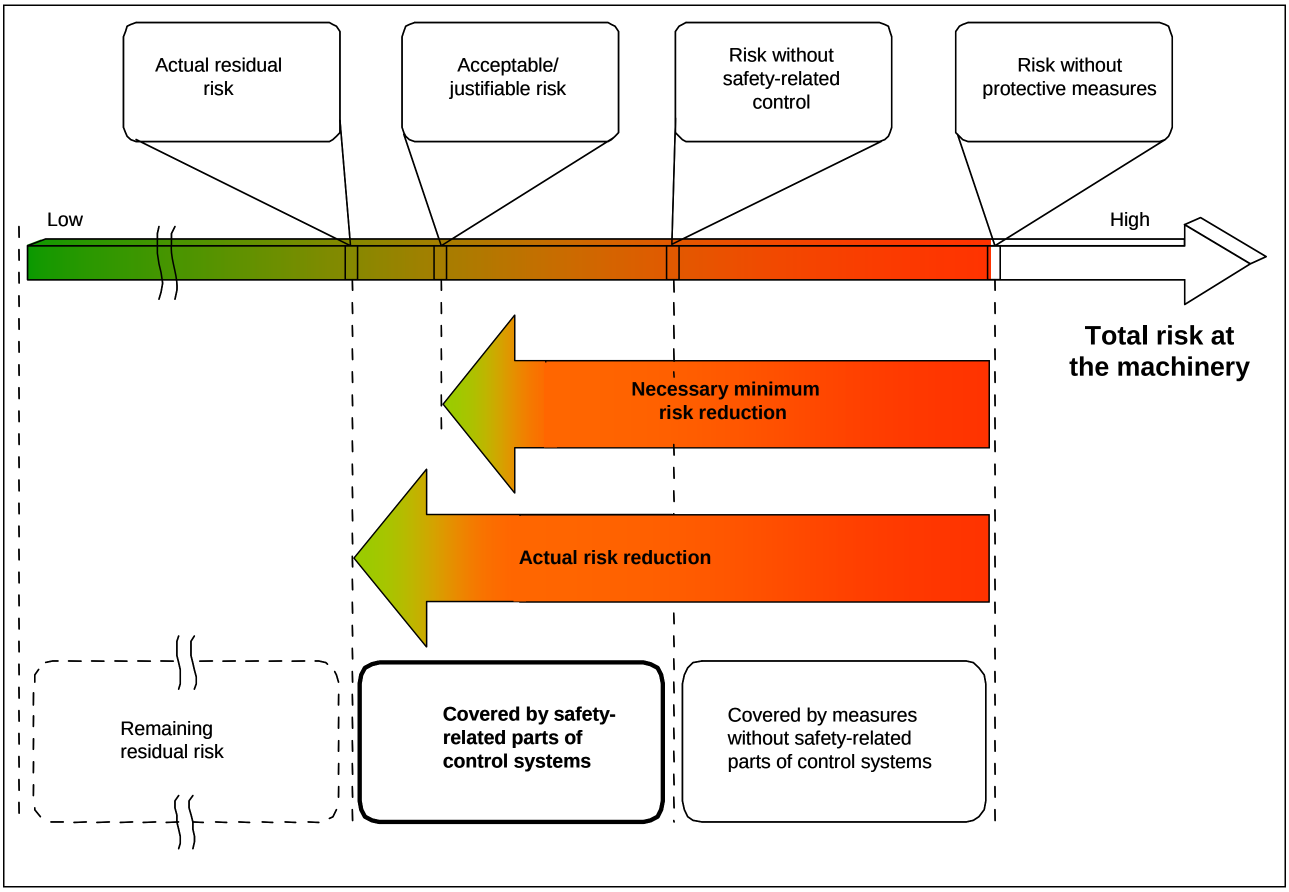
a) Severity of injury

b) Probability of this injury occurring as a function of

- the exposure of a person/of persons to the hazard
- a hazardous event occurring
- the technical and human possibilities for avoidance or limitation of the injury

The objective of the subsequent procedure is to reduce the risk to an acceptable level. For this purpose, Figure 5.3 shows the proportions of risk reduction with and without safety-related parts of a control system. Further information on the subject of risk can be found in the BGIA-Handbuch [18].

Figure 5.3:
Risk estimation and risk reduction


Actual residual risk
Acceptable/ justifiable risk
Risk without safety-related control
Risk without protective measures
Low
High
Total risk at the machinery
Necessary minimum risk reduction
Actual risk reduction
Remaining residual risk
Covered by safety-related parts of control systems
Covered by measures without safety-related parts of control systems

5.2.2 Risk evaluation

Following the risk estimation, a risk evaluation is performed in order to determine whether a risk reduction is necessary. The criteria for adequate risk reduction are set out in EN ISO 12100-1:

- Have all operating conditions and scope for operator intervention been taken into account?
- Have suitable protective measures been taken to eliminate the hazards or to reduce the risks to the extent practically possible?
- Has it been ensured that the measures taken do not give rise to new hazards?
- Have the users been adequately informed and warned of the residual risks?
- Has it been ensured that the protective measures taken do not impede the working conditions of the operating personnel and the machine's ease of use?
- Are the protective measures which have been taken mutually compatible?
- Has adequate consideration been given to the consequences of a machine designed for commercial/industrial use being employed in a non-commercial/ non-industrial environment?
- Has it been ensured that the protective measures taken do not impact negatively upon the working conditions of operating personnel or upon the machine's ease of use?

5.3 Identification of the required safety functions and their properties

Should the evaluation identify an as-yet unacceptable risk, appropriate protective devices must be provided. Priority is however to be given to efforts by which hazards are avoided (inherently safe design), or at least reduced to the greatest possible extent, by design modifications to the machine. In principle, information for use (including organizational measures) is also a possible means of risk reduction. Measures of this kind are acceptable however only in exceptional cases in which an economically reasonable risk reduction is not possible by means of engineered protective measures; in the majority of cases, protective devices will be required. In this context, safety functions are defined which are executed by the SRP/CS (safety-related parts of control systems) (see Figure 5.4).

EN ISO 13849-1:2006 [6] sets out an iterative process for design of the safety-related parts of control systems (Figure 4.1). Figure 5.5 (see page 34) shows the part relevant to this section of the report.

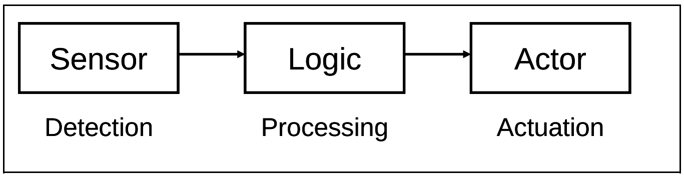
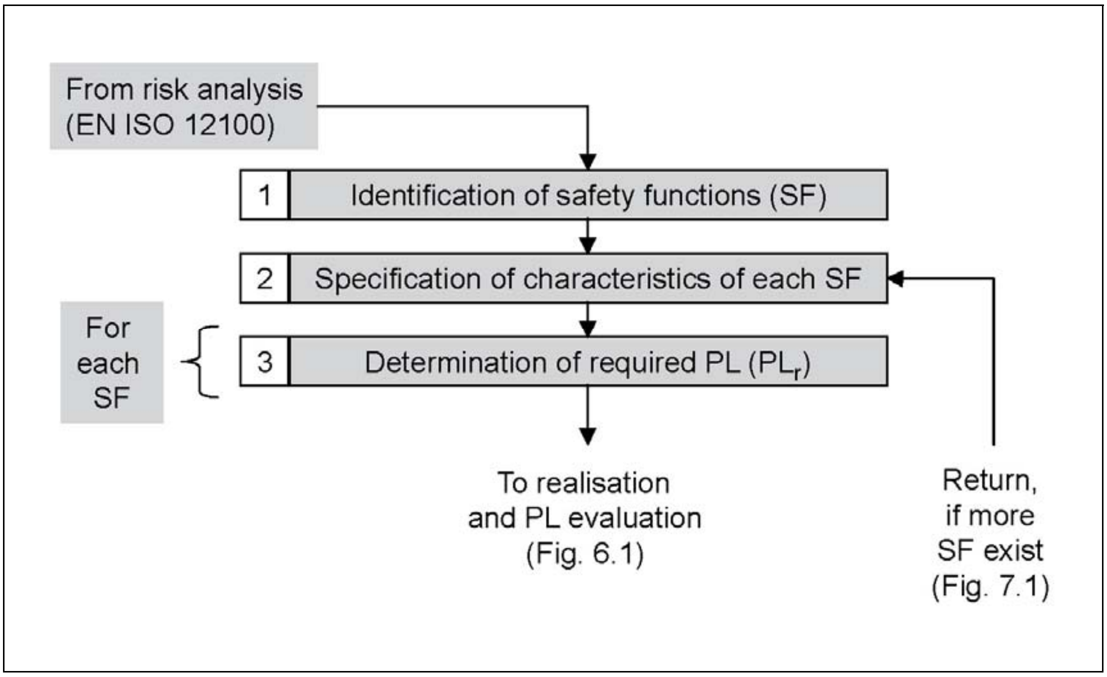


Figure 5.4:
Safety functions are executed by SRP/CS

Figure 5.5:
Excerpt from the iterative process for the design of the safety-related parts of control systems (SRP/CS)


From risk analysis (EN ISO 12100)
1 Identification of safety functions (SF)
2 Specification of characteristics of each SF
3 Determination of required PL (PL_r)
For each SF
To realisation and PL evaluation (Fig. 6.1)
Return, if more SF exist (Fig. 7.1)

5.3.1 Definition of safety functions

The necessary safety functions are defined in consideration of both the application and the hazard. For example, if projectiles must be anticipated, a light curtain will be an unsuitable solution, and an arrester (guard) will be required. A safety function is therefore a function involving measures (including measures in the control technology) which reduce the risk presented by a particular hazard to an acceptable level. In the absence of relevant provisions in a Type C standard, the safety functions are defined by the designer of the machine, e.g.:

a) Controlled stopping of the movement and application of the holding brake in the rest position

b) Prevention of a crushing point being caused by descending machine parts

c) Reduction of the power of a cutting laser where the eye is directly exposed

d) Prevention of dropping of the shaft in setup mode

e) Evasion of the robot when its hazardous area is entered

f) Prevention of entrapment of persons

g) Interruption of the closing movement controlled by two-hand operation in the event of penetration of the hazardous area by a second person (tripped by means of a light curtain)

Compound safety functions are frequently employed, as in the example in Section 5.7 (see page 44): the movement is initially braked to a halt by the electronic drive, after which a mechanical holding brake is applied. The Tables below provide information on possible safety functions. Table 5.1 summarizes the safety functions according to Section 5.1 of EN ISO 13849-1, and adds examples of possible applications.

Table 5.1:
Safety functions from EN ISO 13849-1

Safety function	Example application
Safety-related stop function initiated by safeguard	Response to tripping of a protective device, by STO, SS1 or SS2 (Table 5.2)
Manual reset function	Acknowledgement when areas behind the protective device are left
Start/restart function	Permissible only with interlocking guards with start function to EN ISO 12100-2
Local control function	Control of machine movements from a location within the hazardous area
Muting function	Temporary deactivation of protective devices, e.g. during material transport
Hold-to-run function	Machine movements controlled from a position within the hazardous area, e.g. during setup
Enabling device function	Machine movements controlled from a position within the hazardous area, e.g. during setup
Prevention of unexpected start-up	Manual operator intervention in hazardous area
Escape and rescue of trapped persons	Separation of rollers
Isolation and energy dissipation function	Opening of a hydraulic valve for pressure release
Control modes and mode selection	Activation of safety functions by an operating mode selector switch
Emergency stop function	Response to actuation of an emergency-stop device, by STO or SS1 (Table 5.2)

The “stopping in an emergency” function is also included: though not part of a protective device, it is used for implementation of a complementary protective measure (see Section 5.5). Table 5.2 (page 38) shows further safety functions for safe power drive systems to IEC 61800-5-2 (PDS/SR, power drive systems/safety related) [19]. The scope of this standard includes the safety functions frequently employed for prevention of unexpected start-up (STO, safe torque off; formerly safety related standstill), for safe stop SS1 and SS2 and for safely-limited speed (SLS, formerly safety-related reduced speed).

Table 5.2:
Safety function from IEC 61800-5-2

Abbreviation	**Term**	**Function**
STO	Safe torque off	Motor not receiving energy capable of generating rotary movement; stop category 0 to EN 60204-1.
SS1	Safe stop 1	Motor decelerating; monitoring of deceleration ramp and STO following standstill or STO following expiry of a deceleration time; stop category 1 to EN 60204-1
SS2	Safe stop 2	Motor decelerating; monitoring of deceleration ramp and SOS following standstill or SOS following expiry of a deceleration time; stop category 2 to EN 60204-1
SOS	Safe Operating Stop	Motor is stationary and resisting external forces
SLA	Safely Limited Acceleration	Violation of an acceleration limit value is prevented.
SLS	Safely Limited Speed	Violation of a speed limit value is prevented.
SLT	Safely Limited Torque	Violation of a torque/force limit value is prevented.
SLP	Safely Limited Position	Violation of a position limit value is prevented.
SLI	Safely Limited Increment	The motor is moved a specified step distance, after which it stops.
SDI	Safe Direction	The motor is prevented from running in the unintended direction.
SMT	Safe Motor Temperature	Violation of a motor temperature limit value is prevented.
SBC	Safe Brake Control	Safe actuation of an external brake
SCA	Safe Cam	A safe output signal is generated as long as the motor position remains within a specified range.
SSM	Safe Speed Monitor	A safe output signal is generated as long as the motor speed remains below a specified value.
SAR	Safe Acceleration Range	The acceleration of the motor is kept within specified limit values.
SSR	Safe Speed Range	The speed of the motor is kept within specified limit values.
STR	Safe Torque Range	The torque of the motor (the force in the case of linear motors) is kept within specified limit values.

The manner in which a safety function is executed may differ widely. For this reason, certain characteristics must be observed at selection, and specified on a case by case basis. These include:

- Use in different modes of operation (e.g. automatic mode, setup mode, troubleshooting)
- Response(s) to tripping of the safety function
- Response(s) to detection of a fault in the safety function
- Response time
- Frequency of actuation
- Priority, in cases where several safety functions may be active simultaneously
- Specification of safety-related parameters, such as the maximum permissible speed
- Required Performance Level PL_r

5.3.2 Examples in which the definition of the safety function has an influence upon subsequent calculation of the PL

Later chapters will show how the average probability of a dangerous failure per hour can be calculated for a safety function. The foundation for this is however laid at this stage, with definition of the safety function. By its nature, implementation of a safety function determines the type and scale of the components required for it. The definition of the safety function thus has a considerable influence upon determination of the safety-related reliability. This will be explained in the following examples.

Example 1: Safety function “Stopping when the safety guard is opened”

When the safety guard is opened, the machine operator has access to a hazardous area in which five drives control the movement of machine parts. Opening the safety guard causes all five drives to be brought to a halt as quickly as possible. The associated functional diagram is shown in Figure 5.6.

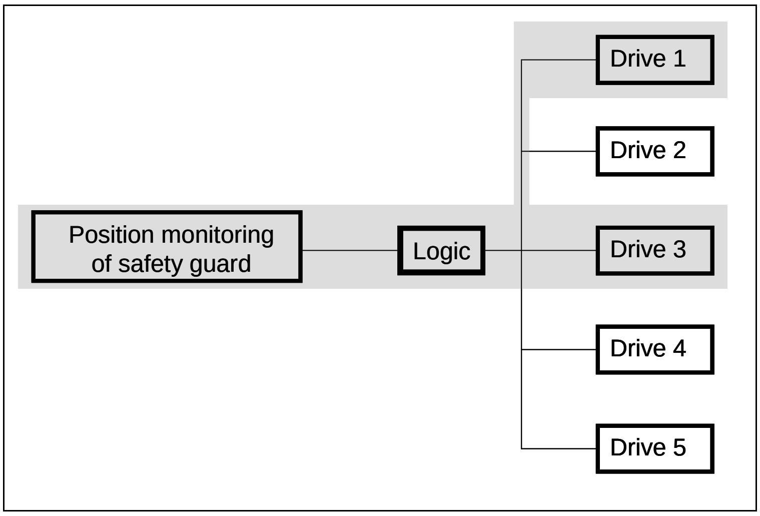


Figure 5.6:
Stopping when the safety guard is opened

During subsequent calculation of the PL of the safety function, the PLs of the following blocks[8] are therefore linked, for example as in Table 6.6:

- Position monitoring of the safety guard, including mechanical components
- Logic
- Drive x (x = 1, 2, … 5)

The result may be a PL which is no longer adequate for the application, even though it may be that only drives 1 and 3 trigger movements hazardous to the operator, and the remaining drives are halted purely “functionally”. In this case, it is recommended that only the movements actually presenting a hazard be considered for the purposes of the safety function.

Example 2: Safety function “Stopping when a safety guard is opened”

A hazardous movement is safeguarded by a fence fitted with five safety guards. Opening any of the guards halts the movement. For determining of the PL at a later stage, each guard forms part of a separate safety function SF1 to SF5, which is composed of the following blocks[8]:

- Position monitoring of safety guard x (x = 1, 2, ... 5) including mechanical components
- Logic
- Drive

Figure 5.7 shows the functional diagram and blocks of the safety function SF3.

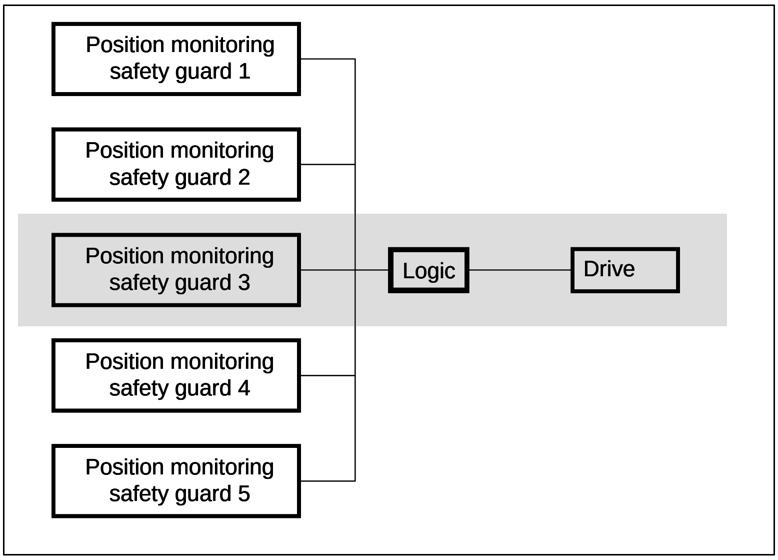

Position monitoring safety guard 1
Position monitoring safety guard 2
Position monitoring safety guard 3
Logic
Drive
Position monitoring safety guard 4
Position monitoring safety guard 5

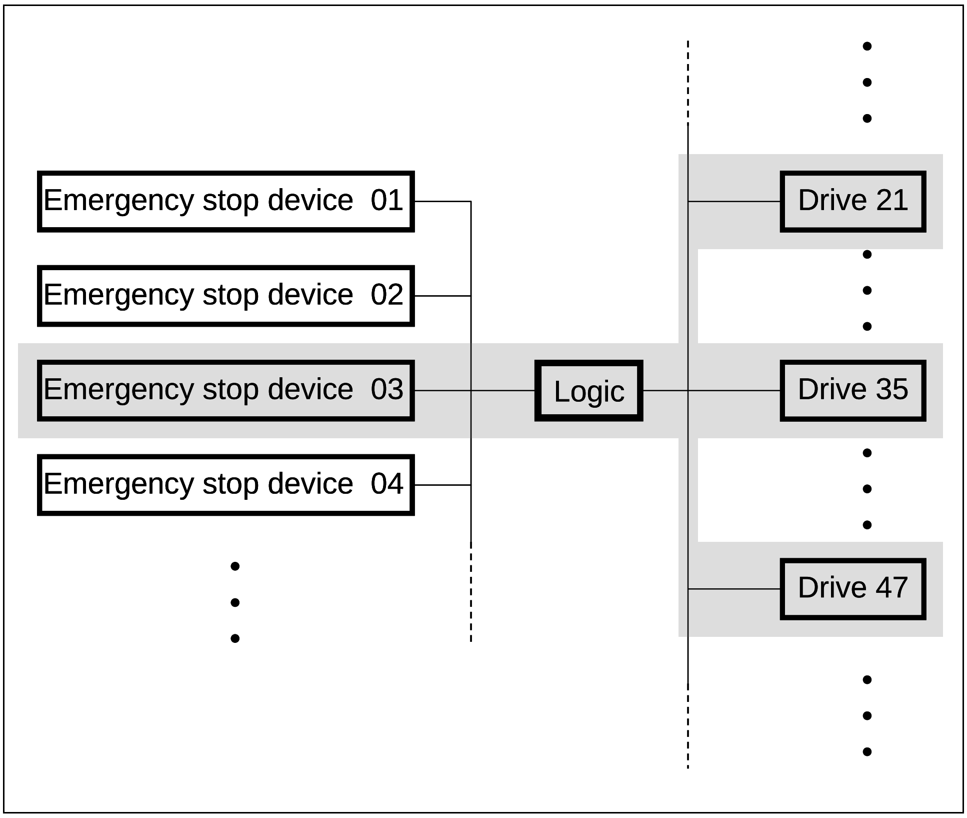
Figure 5.7:
Stopping when the safety guard 3 is opened

[8] Possible faults in the electrical system are assigned to the relevant blocks

Example 3: Safety function: "Emergency stop of an entire machine" (see Section 5.5)

Twenty emergency-stop devices are installed on a larger machine; when actuated, they bring all 50 drives to a halt as rapidly as possible. What components must be considered in this case for implementation of the safety function? It cannot be predicted which of the emergency-stop devices will be actuated for triggering of the safety function. Since the user only ever actuates one emergency stop device, safety functions SF1 to SF20 are defined. The location of an exposed person at the time of triggering of the emergency stop is not known. Regardless of where this person is located, however, not all 50 drives present a hazard. The worst case should therefore be considered representative for all conceivable situations. The worst case is determined by the worst PL, and is therefore partly dependent upon the number of drives in the safety chain which generate hazardous movements at the least favourable location, and upon the respective individual PL. The associated block diagram is shown in Figure 5.8.

Figure 5.8:
Emergency stop of the entire machine, worst case



During subsequent calculation of the safety function, the PL values of the following blocks must be taken into account, for example as shown in Table 6.6:

- Emergency stop device 03
- Logic
- Drive 21

- Drive 35
- Drive 47

The examples show the advantage of a “local approach” for definition of a safety function, in which the following are considered:

- At what location are persons to be found at the point in time under consideration?
- What movements present hazards at the location of the person(s)?
- What protective devices must tripped by the safety function? Multiple protective devices which may alternatively be used may also require consideration.

5.4 Determining of the required Performance Level PL_r

A required Performance Level PL_r[9] – technically the target value – must be specified for each intended safety function. The requirements are derived from the necessary risk reduction. The likelihood and severity of accident, if known, is among the aspects to be considered during definition of the risk reduction. ISO/TR 14121-2 describes methods for determining the necessary size of the risk reduction. EN ISO 13849-1 employs one of these methods, that of the risk graph.

5.4.1 Risk graph

The diagram in Annex A of the standard leads directly to the required Performance Level PL_r and is explained below (see Figure 5.9). Further examples for determining the PL_r can be found in Annex A (see page 283).

From the starting-point, the following risk parameters are evaluated[10]:

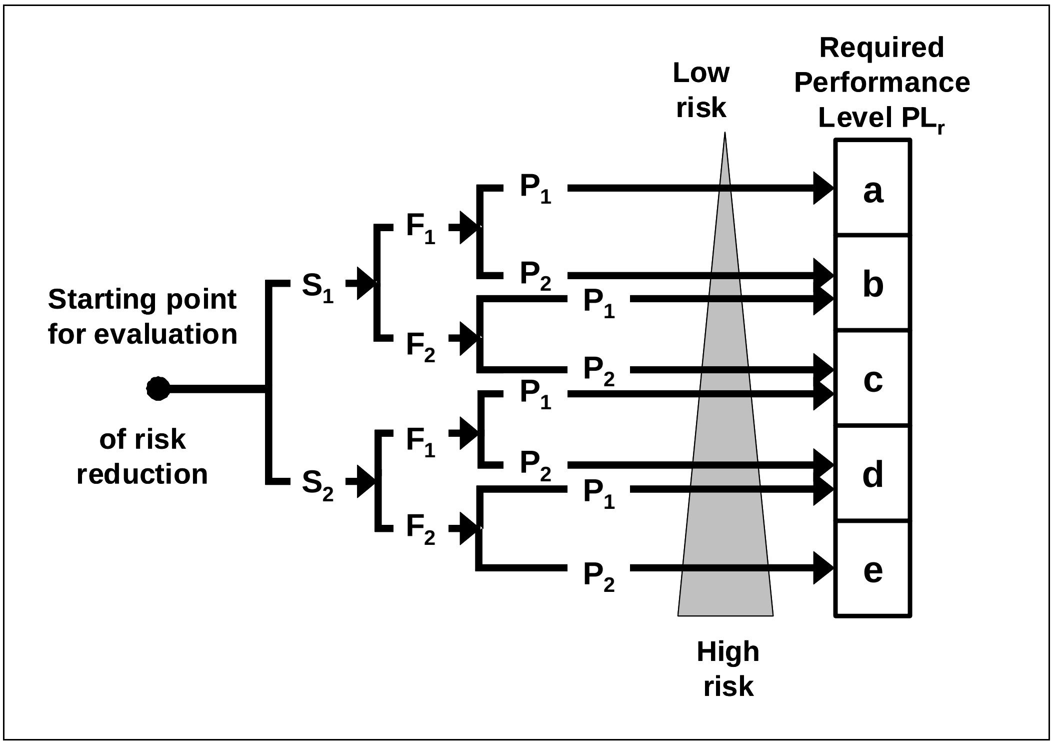
- S – severity of injury
- F – frequency and time of exposure to the hazard
- P – possibility of avoiding the hazard or limiting the harm

The risk graph thus leads to the necessary PL_r. This analysis must be performed for each safety function and without consideration of the risk reduction which is achieved as a result. Where other engineered measures are in place which are implemented independently of the control system, such as a mechanical guard or further safety functions, they can be assumed to be effective for the purpose of determining the PL_r.

[9] The index r (required) indicates that the Performance Level in this case is that required for the safety function (target value). Subsequent validation verifies whether the PL attained by the actual control system (actual value) is greater than or equal to PL_r. In this context, “greater than" means: PL = e > PL = d > PL = c > PL = b > PL = a.

[10] The probability of a hazardous event occurring is virtually impossible to determine in practice. For the purpose of simplification, the worst case is therefore already incorporated into the risk graph, and no further evaluation is required.

Figure 5.9:
Risk graph for determining the PL_r for each safety function


Required Performance Level PL_r
Low risk
High risk
Starting point for evaluation of risk reduction
S_1
S_2
F_1
F_2
P_1
P_2
a
b
c
d
e

Severity of injury S1 and S2

Generally, the severity of injury at a hazardous zone will be found to vary widely. For the requirements upon the control system, however, only the following distinction is relevant:

- S1 – slight (normally reversible injury)
- S2 – serious (normally irreversible injury or death)

The usual consequences of accidents and the healing processes which may normally be anticipated must be assumed for the purpose of selection between S1 and S2.

Frequency of and/or duration of exposure to hazard F1 and F2

The frequency of and/or duration of exposure to hazard are evaluated as:

- F1 – seldom-to-less-often and/or exposure time is short
- F2 – frequent-to-continuous and/or exposure time is long

Unfortunately, a clear boundary for selection between F1 and F2 cannot be stated. In a note, the standard contains the non-prescriptive instruction that in cases where operator interventions occur more frequently than once per hour, F2 should be selected; otherwise, F1. This instruction is however generally appropriate for all cases occurring in practice. During evaluation, an average value should be assigned for the hazard exposure which is commensurate with the overall time for which a machine is in use. Clear cases do however exist: for example, that of a manually charged metal-working press the operator of which must reach cyclically between the dies of the press (F2). Conversely, for a machining centre which is set up once each year and which then operates automatically, F1 will doubtless be selected. For evaluation of the frequency and duration of exposure to the hazard, cases in which the same person or different persons are exposed must be treated in the same way.

Possibility of avoiding the hazard P1 and P2

At this point, an evaluation must be made of whether avoidance of a hazardous situation:

- P1 – Is possible under specific conditions
- P2 – Is scarcely possible

For definition of this parameter, relevant aspects include the physical characteristics of the machine and the possible reaction of its operator. If, for example, the machine must be set up whilst running at limited speed, the parameter P1 will be the correct choice at the low setup acceleration values: with the slow emergence of the hazards and given sufficient room to move, the operator will be able to move out of the hazardous area. Conversely, P2 must be selected when higher speeds may rapidly be reached and the operator has no realistic opportunity of evading an accident. During this evaluation, consideration should be given only to hazard limitation by physically possible means and not to limitation by control components, since the latter could fail in the event of a fault. Rollers for example which are moving in the direction of the operator's hand cannot entrap it under fault-free conditions. In the event of a control-system fault, however, the direction of rotation could be reversed, and under worst-case conditions, the hand would be drawn in.

Chapter 6 (see page 51) describes the subsequent design of the safety functions.

5.4.2 Transition from a required Category in accordance with EN 954-1 to a PL_r

The application of EN ISO 13849-1:2006 requires that the PL_r is known. As described in the preceding section, a risk estimation is required for determination of the PL_r. For standards authors and machine manufacturers, it would however be easier if the PL_r could be derived from a known **required Category** to EN 954-1:1996. The PL_r can be derived in this way however only if a machine exhibits identical hazards with identical risks. Can the PL_r thus be determined without repetition of the risk estimation?

Both the required Category to EN 954-1 and the PL_r in accordance with the new standard are determined by means of a risk estimation. If the required Category is assumed to have been determined with the aid of the risk graph in EN 954-1, and the parameters S, F and P (see section 5.4.1) used for this purpose are transferred to the risk graphs of the new standard, it is found that a clear correlation to the PL_r does not exist for all required Categories.

It must also be considered that when a required Category to EN 954-1 is converted to a PL_r, the requirement concerning the structure to be implemented for the SRP/CS is lost. Chapter 6 explains the designated architectures associated with the Categories, e.g. testing with Category 2 and single-fault tolerance with Category 3. If a PL_r of d were to be assigned to a required Category 3 to EN 954-1, a safety function could then also be implemented in Category 2 (see Figure 6.10). By virtue of this simple transfer, a functionally single-channel structure with test equipment would be able to attain the previous high quality single fault tolerance of Category 3.

This is an intentional degree of freedom allowed for in the new standard, which however must be taken into account when the PL_r is determined. The risk arising in the event of a fault in the SRP/CS, for example, must therefore be observed during selection of a required Category (see EN 954-1, Section 6.3, and EN ISO 13849-1, Section 6.1). In the example considered here, this requirement could have resulted in a required Category of 3 being determined in accordance with EN 954-1.

From these considerations, it follows that when a required category in accordance with EN 954-1 is converted to a required PL_r, additional information may be necessary which is generally no longer available. If a new risk analysis is not conducted, one solution is a worst-case approach in which the PL_r and the required Category are determined at the same time, as shown in Table 5.3. A condition for this approach is that any additional measures which resulted in the “possible Category” being selected instead of the “preferred Category” in accordance with EN 954-1 must remain in place.

Table 5.3:
Worst-case approach for conversion from a required Category in accordance with EN 954-1 to a required Performance Level PL_r

Required Category to EN 954-1:1996		**Required Performance Level PL_r and required Category to EN ISO 13849-1:2006**
B	➔	b
1	➔	c
2	➔	d, Category 2
3	➔	d, Category 3
4	➔	e, Category 4

5.5 Complementary protective measures

The requirements for complementary protective measures are contained in EN ISO 12100-2 [3], Section 5.5. With regard to the control technology issues addressed in this report, these requirements particularly include

- Measures for stopping in an emergency
- Reversal of movements
- De-energization and energy dissipation

These are not by definition engineered protective measures of which the implementation would require a certain Performance Level. These complementary protective measures should however take effect when engineered protective measures (guards and other protective measures) have failed or have been disabled by tampering. In these cases in particular, an emergency stop function for example is expected actually to be serviceable. The requirements placed by EN 60204-1 [20] upon control circuits and the control functions of machines should therefore be observed. Section 9.4, “Control functions in the event of failure”, requires an appropriate standard of safety performance, which must be defined by the risk evaluation of the machine. Ultimately, the requirements of EN ISO 13849 therefore also apply to these complementary protective measures. Under no circumstances may complementary protective measures influence the function and standard of protective devices.

5.6 Treatment of old machinery

Old machinery in this context are machines which were placed on the market before the Machinery Directive came into force. The requirements of the directive were not applied to these machines. However, its application may become necessary should legacy machines be extended, modified, modernized, etc. In such cases, assessment must be made for whether an essential change has occurred. Should this be the case, the requirements of the EC Machinery Directive apply to “old” machines in the same way as to new machinery. These requirements include the application of EN ISO 13849. A diagram produced by the German Berufsgenossenschaft der chemischen Industrie[11] responsible for the chemical industry assists in determining whether an essential change has been made [21].

5.7 Risk reduction with reference to the example of a paper-cutting guillotine with diverse redundancy in the logic control (Category 4 – PL e)

The following example illustrates the application of EN ISO 13849-1 on a paper-cutting guillotine. Only certain aspects will be considered in detail, and not the entire process.

Guillotines (see Figure 5.10) are used to cut stacks of paper sheets or similar materials by means of a knife. The product to be cut is generally placed under the knife by hand. Immediately before the cutting action, a clamping bar is lowered at high force onto the stack in order to hold it in place during cutting. The knife and the clamping bar are driven hydraulically.

[11] Institution for statutory accident insurance and prevention in the chemical industry

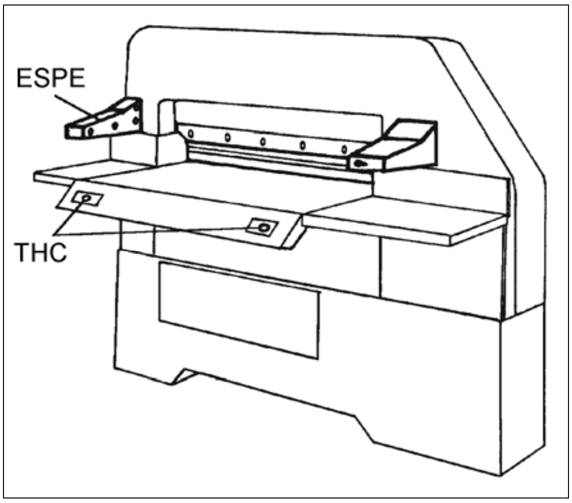


Figure 5.10:
Paper-cutting guillotine with two-hand control (THC) and electro-sensitive protective equipment (ESPE)

5.7.1 Definition of the limits of the machine

Space limits

Since paper-cutting guillotines are charged manually, sufficient space is required for the handling of product for cutting, onward transport/storage of the cut paper stack, and disposal of paper waste, in addition to space for the operator to move.

Time limits

Depending upon the application, the machine may be used for a period of approximately 20 years. Component wear may lengthen the time required for a movement to stop. The resulting violation of the overrun must therefore be detected and must result in the machine being stopped.

Use limits

The intended use of the machine is that of cutting stacked sheets of paper or similar materials. The machine is charged manually by a single person. However, depending upon the site of the installation and the width of the machine, the presence of other persons in the vicinity cannot be excluded.

Provision is made for the following modes of operation:

1. Pressing
2. Manual cutting (single cut)
3. Automatic sequence of cuts (automatic process following the first, manual cut)
4. Knife change

In the first three operating modes, movement of the clamping bar alone is possible in order for the line of cut to be indicated. For this purpose, the operator presses a pedal, and is able at the same time to alter the position of the paper stack with his hands within the hazardous area.

5.7.2 Identification of the hazards

The following mechanical hazards are significant for a paper-cutting guillotine:

G1 – crushing by the clamping bar

G2 – cutting by the knife during the cutting process

G3 – cutting by the knife in the rest position

Risk estimation

The dynamic press force of the clamping bar (hazard G1) is sufficiently great to cause not only reversible crushing, but also broken bones. For hazard G2, amputation of limbs must be assumed. During manual positioning of the paper stack, hazard G3 may lead to injury to the hands or forearms on the stationary knife. These injuries are however generally reversible.

The operators' exposure to hazard is very high, since they regularly (cyclically) intervene manually in the hazardous area in the course of routine work.

The drop speed of the clamping bar and knife (hazards G1 and G2) is very high, with the result that the operator has virtually no means of avoiding the hazard. With the knife stationary (hazard G3), the operator is able to avoid or limit injury.

The likelihood of injury as a function of the incidence of a hazardous event is not evaluated at this point, since the worst-case scenario is assumed below for this purpose.

Risk evaluation

In consideration of all operating conditions and all possibilities for operator intervention, a risk reduction is found to be required.

Inherently safe design

It is not possible for the dynamic press force of the clamping bar and the energy of the knife to be reduced, as this would impair the functionality of the machine. An arrangement and design of the machine which would prevent the operator from reaching into the hazardous area is also not possible, since this is precisely where he must align the stack of paper.

The following measures can however be taken:

1. Shrouding of all points of access to the hazardous area except on the operator side
2. Avoidance of sharp edges and corners

3. Assurance of a suitable working position and accessibility of the controls
4. Ergonomic design of the machine
5. Avoidance of electrical hazards
6. Avoidance of hazards presented by the hydraulic equipment

5.7.3 Required safety functions

In consideration of all operating modes and all manual interventions, the following safety functions are required:

SF1 – STO (safe torque off), for avoidance of unexpected start-up

SF2 – Controlled location of the operator's hands outside the hazardous area during a hazardous movement

SF3 – Detection by ESPE (electro-sensitive protective equipment), e.g. a light curtain, of intervention by further persons in the hazardous area, and immediate interruption of the cutting operation

SF4 – Automatic stopping of all movements following each single cut or following completion of the automatic cutting sequence

SF5 – Reduction of the dynamic press force for the clamping bar during the “indicate cut” function

SF6 – Automatic return of the clamping bar and knife to their initial positions following interruption of a cutting operation

SF7 – Covering of the knife by the clamping bar

Characteristics of the safety functions

Should the light curtain be penetrated, the cut must be interrupted immediately. The safety function SF3 therefore takes priority over SF2. For SF5, the maximum permissible force for the clamping bar during the “indicate cut” function must be specified (see EN 1010-3).

5.7.4 Determining of the required Performance Level PL_r

The PL_r must be determined for each safety function. If the situations in which the individual safety functions are used are analysed, evaluation of the risk parameters S, F and P yields similar results for the safety functions SF1 to SF6:

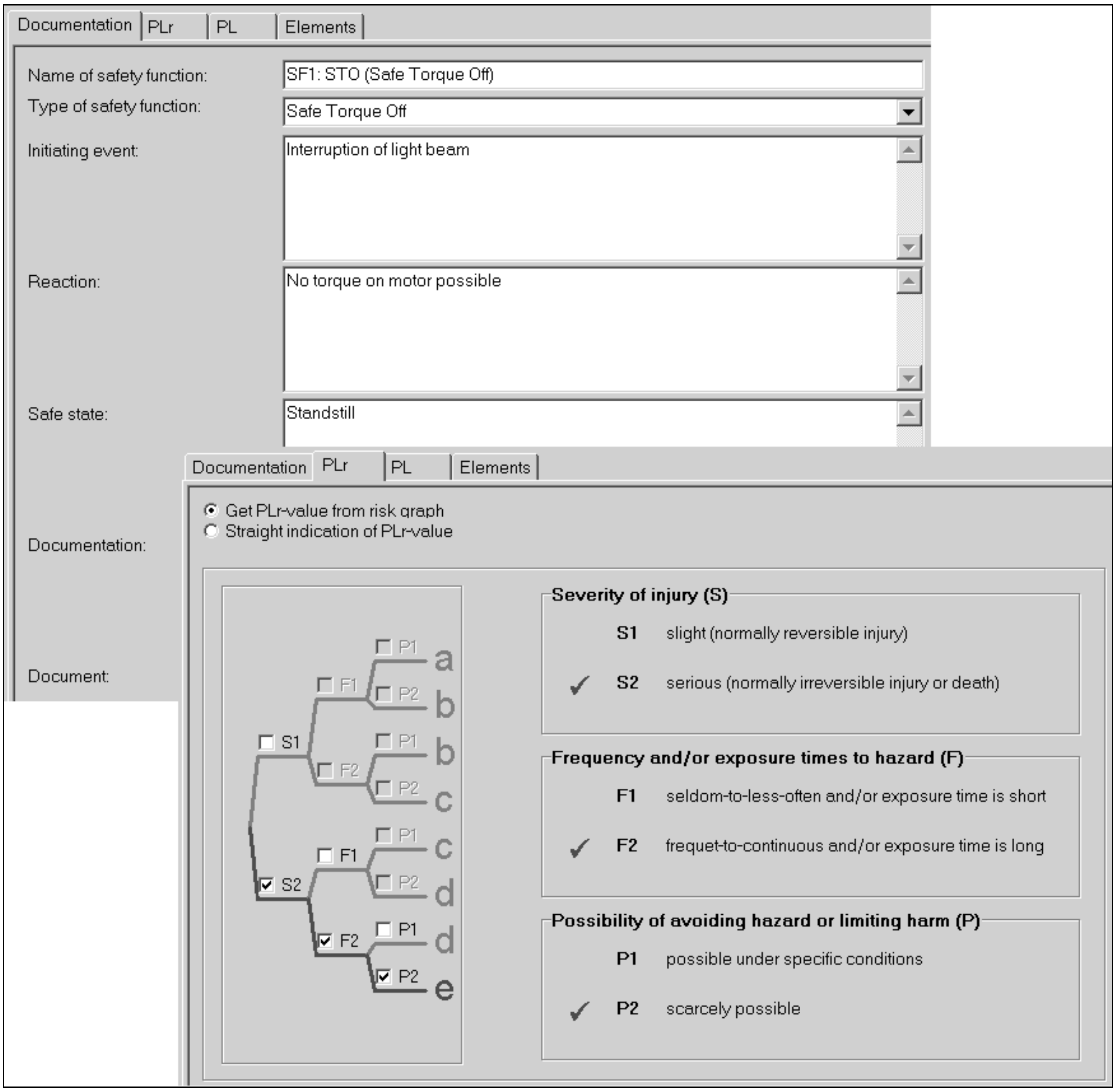
S2 – Serious, generally irreversible injury

F2 – Continuous presence in the hazardous area

P2 – Evasion of a hazardous situation is scarcely possible

In accordance with the risk graph in Figure 5.9, this evaluation results in a required Performance Level PL_r of e. Figure 5.11 shows the corresponding documentation and risk graph in the SISTEMA software for the safety function SF1.

Figure 5.11:
Documentation and risk graph for SF1



Name of safety function: SF1: STO (Safe Torque Off)

Type of safety function: Safe Torque Off

Initiating event: Interruption of light beam

Reaction: No torque on motor possible

Safe state: Standstill

Documentation:

Document:

● Get PLr-value from risk graph
○ Straight indication of PLr-value

Severity of injury (S)

	S1	slight (normally reversible injury)
✓	**S2**	serious (normally irreversible injury or death)

Frequency and/or exposure times to hazard (F)

	F1	seldom-to-less-often and/or exposure time is short
✓	**F2**	frequet-to-continuous and/or exposure time is long

Possibility of avoiding hazard or limiting harm (P)

	P1	possible under specific conditions
✓	**P2**	scarcely possible

The safety function SF7 is provided for the hazard G3, “cutting by the knife in the rest state”. The following risk parameters are specified for this purpose:

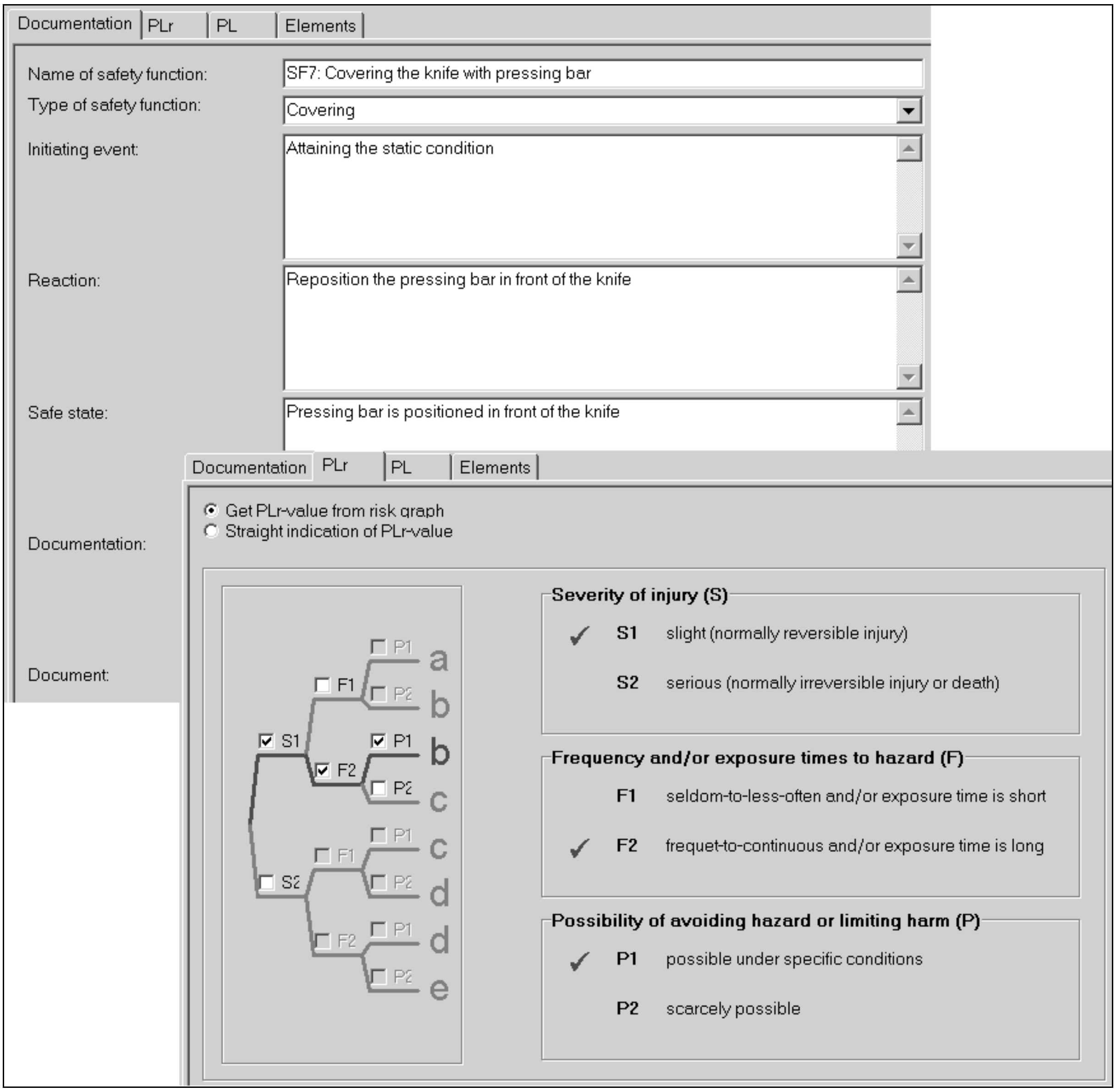
S1 – Slight, generally reversible injury

F2 – Exposure time is long

P1 – Evasion of a hazardous situation is possible under specific conditions

In accordance with the risk graph in Figure 5.9, this evaluation results in a required Performance Level PL_r of b. Figure 5.12 shows the corresponding documentation and risk graph in the SISTEMA software for the safety function SF7.

Figure 5.12:
Documentation and risk graph for SF7



Name of safety function: SF7: Covering the knife with pressing bar

Type of safety function: Covering

Initiating event: Attaining the static condition

Reaction: Reposition the pressing bar in front of the knife

Safe state: Pressing bar is positioned in front of the knife

Documentation:

Document:

● Get PLr-value from risk graph
○ Straight indication of PLr-value

☑ S1 □ F1 □ P1 □ P2 ☑ F2 ☑ P1 □ P2
□ S2 □ F1 □ P1 □ P2 □ F2 □ P1 □ P2

Severity of injury (S)

✓ **S1** slight (normally reversible injury)

S2 serious (normally irreversible injury or death)

Frequency and/or exposure times to hazard (F)

F1 seldom-to-less-often and/or exposure time is short

✓ **F2** frequet-to-continuous and/or exposure time is long

Possibility of avoiding hazard or limiting harm (P)

✓ **P1** possible under specific conditions

P2 scarcely possible

5.7.5 Complementary protective measures

The following measures are required:

1. Stopping in an emergency
   Suitable safety functions with a PL of e are already available in the machine control system and are used for the emergency stop. Provided the emergency-stop

control device features a two-channel circuit, stopping in an emergency therefore also satisfies a PL of e.

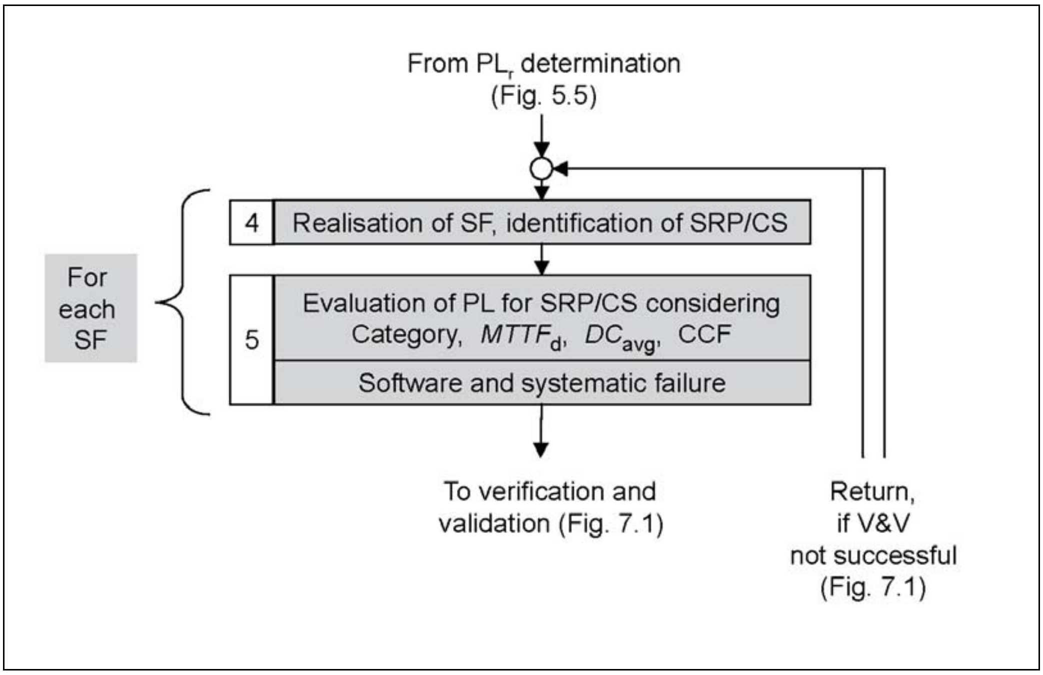
2. Freeing of a trapped person requires a reverse movement of the knife and clamping bar, which are achieved by spring force.

6 Design of safe control systems

6.1 Introduction

Once the precise safety function and its required risk reduction, the PL_r, have been defined, design proper begins of the safety-related parts of the control system (SRP/CS) which are to carry out the safety function(s). The corresponding section from the iterative design process of EN ISO 13849-1 is shown in Figure 6.1.

Figure 6.1:
Determining of the attained PL in the implementation phase of the SRP/CS: excerpt from the iterative design process, see Figure 4.1


From PL_r determination
(Fig. 5.5)
For each SF
4
Realisation of SF, identification of SRP/CS
5
Evaluation of PL for SRP/CS considering Category, $MTTF_d$, DC_{avg}, CCF
Software and systematic failure
To verification and validation (Fig. 7.1)
Return, if V&V not successful (Fig. 7.1)

The safety-related quality of the SRP/CS is indicated by one of five Performance Levels (PLs). Each of these PLs corresponds to a range of the probability of a dangerous failure per hour (Table 6.1, page 52). In addition to the average probability of a dangerous failure per hour (*PFH*), further measures, for example to enhance software robustness or to counter systematic failures, are required in order for the corresponding PL to be attained.

In principle, any method (e.g. Markov calculations, Petri nets) may be used to verify the probability of failure. The following criteria must however be observed:

- Quantifiable aspects (structure, component reliability, diagnostics in the form of self-tests, common cause failure)

- Non-quantifiable, qualitative aspects which influence the behaviour of the SRP/CS (fault-mode behaviour of the safety function, safety-related software, systematic failures and environmental conditions)

Table 6.1:
Correspondence between the probability of failure and the Performance Level

Performance Level (PL)	Average probability of a dangerous failure per hour (*PFH*) in h^{-1}
a	$\geq 10^{-5}$ to $< 10^{-4}$
b	$\geq 3 \times 10^{-6}$ to $< 10^{-5}$
c	$\geq 10^{-6}$ to $< 3 \times 10^{-6}$
d	$\geq 10^{-7}$ to $< 10^{-6}$
e	$\geq 10^{-8}$ to $< 10^{-7}$

For both groups of criteria, EN ISO 13849-1 proposes practical methods which produce a good and scientifically sound estimate of the attained PL. For each specific aspect, verification can be made coarser or finer as required, permitting both a fast approximation and a more detailed verification.

The development procedure is first described (see Section 6.1.1). This includes requirements upon the specification and upon the documentation within the life cycle of the SRP/CS. It is followed by measures necessary for the control of systematic failures (Section 6.1.2) and ergonomic design aspects (Section 6.1.3). Section 6.2 describes the Categories and the simplified method based upon them for evaluation of the quantifiable aspects. Section 6.3 then presents requirements upon the software. Finally, Section 6.4 shows the quantifiable aspects which must be observed where SRP/CS are used in combination. Figure 6.2 explains the need for this additional section.

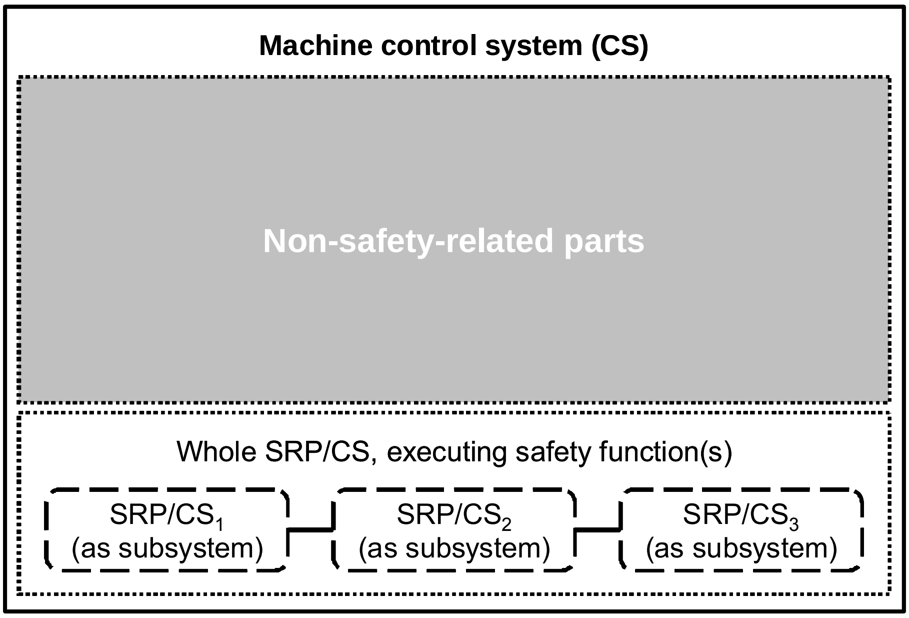

Machine control system (CS)
Non-safety-related parts
Whole SRP/CS, executing safety function(s)
SRP/CS$_1$ (as subsystem)
SRP/CS$_2$ (as subsystem)
SRP/CS$_3$ (as subsystem)

Figure 6.2:
SRP/CS and subsystems within the machine control system

The machine control system (CS) as a whole is divided into safety-related parts (SRP/CS) and the non-safety-related parts, which are generally substantially more comprehensive and which have the sole function of controlling normal operating functions. The combination of safety-related parts of a control system begins at the point at which safety-related signals are generated (these include, for example, the actuating cam and the roller of a position switch), and ends at the outputs of the power control elements (for example including the main contacts of a contactor). Where no hazards arise in the de-energized state (closed-circuit current principle), power components such as motors or cylinders are not regarded as SRP/CS. Should external forces take effect, however (for instance on vertical axes), the power elements must be enforced for functional safety (e.g. non-return valve on the cylinder, additional mechanical brake). Finally, Section 6.5 describes – like Section 5.7 before it – the actual implementation with reference to the practical example of a paper-cutting guillotine control.

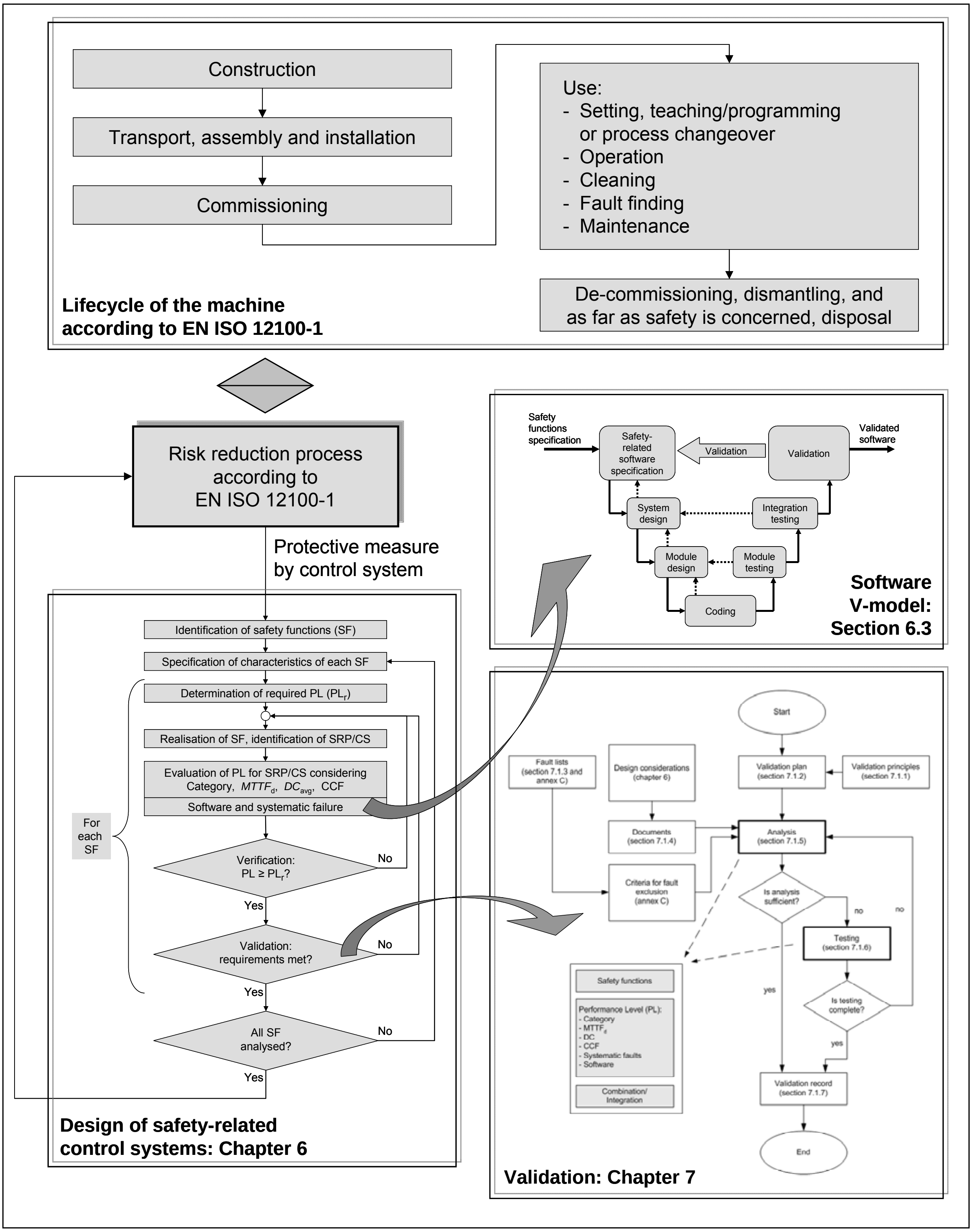
6.1.1 Design and development process

The objective of each activity during the design and integration of the safety-related parts of control systems (scope of the standard) is to develop and use products which are as free of faults as possible and which satisfy the requirements. Ultimately, the objective concerns the health of human beings and the avoidance of accidents. The motto for the design and development process must therefore be: **Structured** and **well-documented.**

The process of risk reduction in accordance with EN ISO 12100-1 must be geared to the entire life cycle of a machine, as shown in Figure 6.3. Although EN ISO 13849-1 contains no explicit provision to this effect, the concept of the life cycle must also be taken up in the design and integration of one or more SRP/CS, in order for the activities to be structured appropriately. The description of the standard in Section 4 also shows clearly that the iterative process described in the standard for the design of the safety-related parts of control systems is a process structured in discrete phases. As can be seen in Figure 6.3 (page 54), the validation phase is characterized by structured procedures of its own. These are described in greater detail in Chapter 7. Structuring into life-cycle phases is characterized very comprehensively by the V-model employed during development of safety-related software; this is explained in Section 6.3. For example, although the maintenance phase is not explicitly addressed by design process for an SRP/CS, it is taken into account by the required content of the information for use.

Since SRP/CS constitute parts of a machine, requirements in virtually any phase of the machine's life cycle may also have an influence upon it. All phases in the machine's life cycle must therefore be considered during the identification of safety functions and definition of their characteristics. In order for this process to be organized as comprehensibly and verifiably as possible, safety functions are specified first. SRP/CS which are not explicitly developed for a machine control system – examples include light curtains or safety PLC – therefore require a particularly precise description of their characteristic data and their interfaces in order for proper use to be assured.

Figure 6.3:
Life cycles of machines and SRP/CS


Construction
Transport, assembly and installation
Commissioning
Use:
- Setting, teaching/programming or process changeover
- Operation
- Cleaning
- Fault finding
- Maintenance
De-commissioning, dismantling, and as far as safety is concerned, disposal
Lifecycle of the machine according to EN ISO 12100-1
Risk reduction process according to EN ISO 12100-1
Protective measure by control system
Identification of safety functions (SF)
Specification of characteristics of each SF
Determination of required PL (PLr)
Realisation of SF, identification of SRP/CS
Evaluation of PL for SRP/CS considering Category, MTTFd, DCavg, CCF
Software and systematic failure
For each SF
Verification: PL ≥ PLr?
No
Yes
Validation: requirements met?
No
Yes
All SF analysed?
No
Yes
Design of safety-related control systems: Chapter 6
Safety functions specification
Safety-related software specification
Validation
Validation
Validated software
System design
Integration testing
Module design
Module testing
Coding
Software V-model: Section 6.3
Start
Fault lists (section 7.1.3 and annex C)
Design considerations (chapter 6)
Validation plan (section 7.1.2)
Validation principles (section 7.1.1)
Documents (section 7.1.4)
Analysis (section 7.1.5)
Criteria for fault exclusion (annex C)
Is analysis sufficient?
no
no
Testing (section 7.1.6)
yes
Safety functions
Performance Level (PL):
- Category
- MTTFd
- DC
- CCF
- Systematic faults
- Software
Combination/ Integration
Is testing complete?
yes
Validation record (section 7.1.7)
End
Validation: Chapter 7

The life cycle of the SRP/CS begins with specification of the safety functions. Besides particular aspects of various safety functions, EN ISO 13849-1 also lists general aspects which are a minimum requirement in such a specification.

A specification of this kind sets out, at the beginning of the development process, the framework for all parties involved. It constitutes a set of performance specifications; in no way is it a product specification produced post-development. A safety function is implemented by SRP/CS which are part of the machine control system and which possess interfaces to further SRP/CS and to the functional control system. A specification must therefore be drawn up. Text Box 6.1 shows a general arrangement template for a specification of the safety requirements. The arrangement also includes the specification of the safety functions. The arrangement template refers to an SRP/CS which executes the entire safety function. The specification must be adapted accordingly for SRP/CS in the form of subsystems.

Text box 6.1:
General arrangement template for a specification of the safety requirements

1 General product and project information

1.1 Product identification

1.2 Author, version, date, document name, file name

1.3 Contents

1.4 Terminology, definitions, glossary

1.5 Version history and changes

1.6 Directives, standards and technical rules relevant to development

2 Functional information on the machine, where relevant to safety

2.1 Intended use and reasonably foreseeable misuse

2.2 Process description (operating functions)

2.3 Operating modes (e.g. setup mode, automatic mode, operation of localized relevance or of parts of the machine)

2.4 Characteristic data, e.g. cycle times, response times, overrun distances

2.5 Other characteristics of the machine

2.6 Safe state of the machine

2.7 Interaction between processes (see also 2.2) and manual actions (repair, setup, cleaning, troubleshooting, etc.)

2.8 Emergency operations

3 Required Performance Level(s) (PL_r)

3.1 Reference to existing documentation concerning the hazard analysis and risk assessment for the machine

3.2 Results of the risk assessment for each identified hazard or hazardous situation and specification of the safety function(s) required in each case for risk reduction

Text box 6.1: continued

4 Safety functions (information applies to each safety function)

- Description of the function ("input – logic – output") including all functional characteristics (refer also to Tables 5.1 and 5.2)
- Activation/deactivation conditions or events (e.g. operating modes of the machine)
- Behaviour of the machine when the safety function is triggered
- Conditions to be observed for re-starting
- Performance criteria/performance data
- Process (timing behaviour) of the safety function, including response time
- Frequency of actuation (i.e. demand rate), recovery time following demand
- Other data
- Adjustable parameters (where provided)
- Classification and assignment of priorities in the event of simultaneous demand for and processing of multiple safety functions
- Functional concept for separation or independence/freedom of reciprocal action from non-safety functions and further safety functions

5 Required information for the SRP/CS design

5.1 Allocation of the SRP/CS and the form of technology by which the safety function is to be implemented; intended equipment

5.2 Selection of the Category, designated architecture (structure) in the form of a safety-related block diagram and description

5.3 Description of the interfaces (process interfaces, internal interfaces, user interfaces, control and display elements, etc.)

5.4 Behaviour at switch-on, implementation of the required starting and restarting behaviour

5.5 Performance data: cycle times, response times, etc.

5.6 Behaviour of the SRP/CS in the event of component failures and faults (achieve and maintain the safe state), including timing behaviour

5.7 Failure modes of components, modules or blocks which are to be considered; where applicable, reasoning for fault exclusions

5.8 Concept for implementation of the detection and control of random and systematic failures (self-tests, test circuits, monitoring arrangements, comparisons, plausibility tests, fault detection by the process, etc.)

5.9 Quantitative aspects

5.9.1 Target values for $MTTF_\mathrm{d}$ and DC_avg

Text box 6.1: continued

5.9.2 Switching frequency of components subject to wear

5.9.3 Frequency of measures for fault detection

5.9.4 Mission time, where different from the assumption upon which the intended architecture is based (20 years)

5.10 Operating and limit data (operating and storage temperature range, humidity class, IP degree of protection, resistance values for shock/vibration/EMC, supply data with tolerances, etc.)

5.11 Generic standards to be applied for design (for the equipment, for protection against electric shock/hazardous shock currents, for resistance to environmental conditions, etc.)

5.12 Technical and organizational measures for protected access to safety-related parameters and to SRP/CS characteristics (protection against tampering, access protection, program/data protection) and for protection against unauthorized operation (key switch, code, etc.), for example in non-standard operating modes

5.13 General technical requirements and organizational framework for commissioning, testing and acceptance, and for maintenance and repair

In order to be valid, such a specification must be verified prior to the next development step. Verification must cover completeness, correctness, intelligibility and freedom from contradictions. It is clearly advantageous for verification, for example in the form of an inspection, to be performed by a party not involved in the project. If safety-related software is employed, these specifications of the safety requirements must form the basis for a dedicated software specification; see Section 6.3.2.

The specification is the first document to be created in the procedure of the design of an SRP/CS. The documentation is of great importance in the interest of verifiable development. It must be considered that future responsibility for a product may lie with a party other than the developer. Details concerning the necessary documentation in the context of the iterative design process of an SRP/CS can be found in Section 6.3.8 concerning software, and in Sections 7.1.4 ff. The reader is reminded at this point that the documents must be clearly identifiable; version management is therefore essential. The contents of the information for use are ultimately of major importance for the proper implementation of safety functions. Chapter 11 of EN ISO 13849-1 lists the minimum information which must be included in the information for use. The content of the manufacturer's internal technical documentation for an SRP/CS is listed in Chapter 10 of the standard. Legislation also lays down requirements concerning the documentation. Text Box 6.2 (see page 58) shows the content of the technical documentation for machines which is required by the future (new) European Machinery Directive (2006/42/EC) [8], which comes into force on 29 December 2009.

Text Box 6.2:
Technical documentation for machines: excerpt from the future Machinery Directive (2006/42/EC), Annex VII, A

1. The technical file shall comprise the following:

   a) a construction file including:

   – a general description of the machinery,

   – the overall drawing of the machinery and drawings of the control circuits, as well as the pertinent descriptions and explanations necessary for understanding the operation of the machinery,

   – full detailed drawings, accompanied by any calculation notes, test results, certificates, etc., required to check the conformity of the machinery with the essential health and safety requirements,

   – the documentation on risk assessment demonstrating the procedure followed, including:

     i) a list of the essential health and safety requirements which apply to the machinery,

     ii) the description of the protective measures implemented to eliminate identified hazards or to reduce risks and, when appropriate, the indication of the residual risks associated with the machinery,

   – the standards and other technical specifications used, indicating the essential health and safety requirements covered by these standards,

   – any technical report giving the results of the tests carried out either by the manufacturer or by a body chosen by the manufacturer or his authorised representative,

   – a copy of the instructions for the machinery,

   – where appropriate, the declaration of incorporation for included partly completed machinery and the relevant assembly instructions for such machinery,

   – where appropriate, copies of the EC declaration of conformity of machinery or other products incorporated into the machinery,

   – a copy of the EC declaration of conformity;

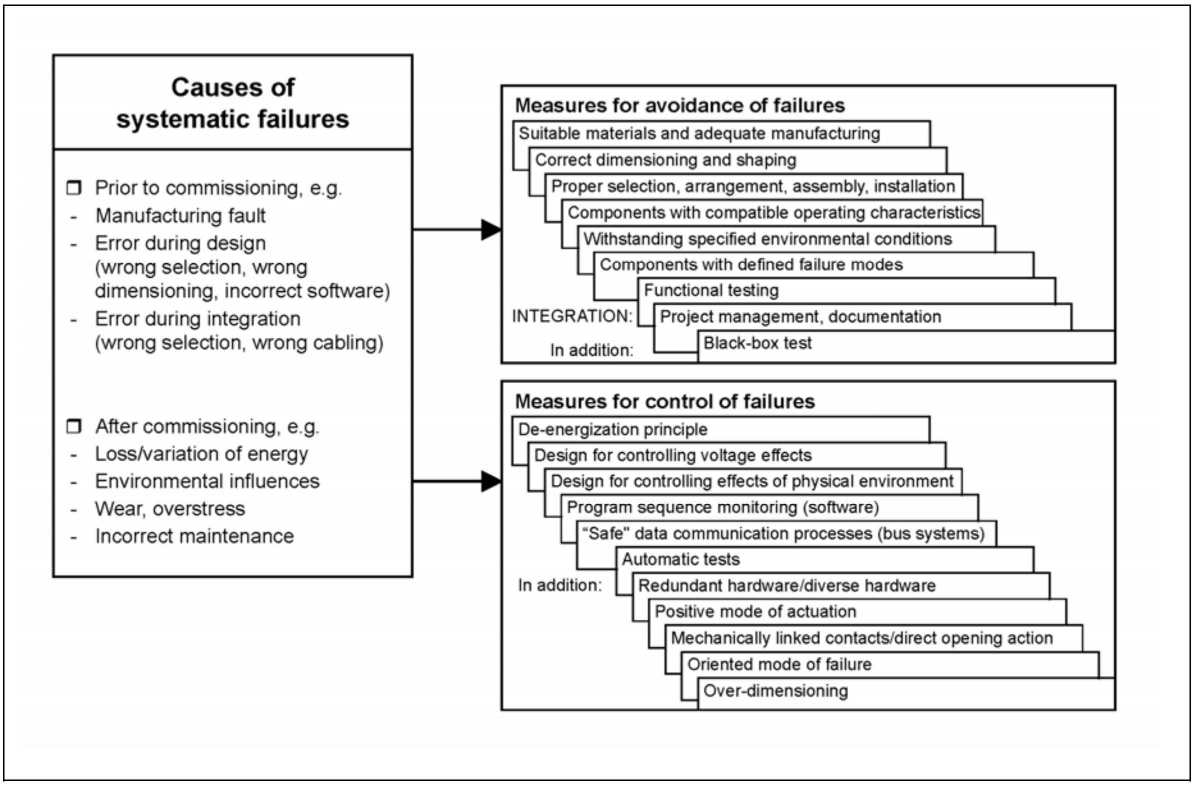
   b) for series manufacture, the internal measures that will be implemented to ensure that the machinery remains in conformity with the provisions of this Directive.

6.1.2 Systematic failures

In contrast to random component failures, systematic failures have causes which can be eliminated only by modification, for example, of the design, the manufacturing process, the operating methods or the documentation. They arise at some point in the life cycle of a product, for example as a result of faults in the specification or the design, or during modification of an SRP/CS. The implementation of multi-channel structures and analysis of the probability of component failures are important elements in the design of safety technology. Should fundamental aspects not be considered, even the most favourable figures for the probability of failure are of no benefit. If, for example, a product is not used correctly or is used in the wrong environment, a risk of systematic failure may exist. This fact is addressed by EN ISO 13849-1 in conjunction with Part 2, when it requires that possible systematic failures also be considered for attainment of a PL. Essentially, it can be said that many of the basic and well-tried safety principles are already effective in preventing systematic failures (see Annex C, page 301). These principles, which supplement Annex G of the standard, should be considered in accordance with EN ISO 13849-2.

The informative Annex G of the standard contains a list of measures, and therefore indirectly also of influences which are to be considered. The measures are divided into those for the avoidance of failures (G.3 and G.4) and those for their control (G.2). Figure 6.4 provides an overview. The measures for the avoidance of failures must be effective throughout all phases of a product's lifetime, and are addressed accordingly to some degree in Chapter 7 of this report, under the aspect of validation. Although not stated explicitly, appropriate care must be taken specifically during modifications, troubleshooting and maintenance. It is during these phases in particular that the details of development are not (or no longer) evident. Conversely, measures for the control of failures must be implemented within a product, and take full effect during operation. Besides basic requirements, the standard also lists measures for selection, one or more of which are to be applied in consideration of the complexity of the SRP/CS and of the PL (marked as “in addition” in Figure 6.4).

Figure 6.4:
Measures against systematic failures in accordance with Annex G of the standard


Causes of systematic failures
❒ Prior to commissioning, e.g.
- Manufacturing fault
- Error during design (wrong selection, wrong dimensioning, incorrect software)
- Error during integration (wrong selection, wrong cabling)
❒ After commissioning, e.g.
- Loss/variation of energy
- Environmental influences
- Wear, overstress
- Incorrect maintenance
Measures for avoidance of failures
Suitable materials and adequate manufacturing
Correct dimensioning and shaping
Proper selection, arrangement, assembly, installation
Components with compatible operating characteristics
Withstanding specified environmental conditions
Components with defined failure modes
Functional testing
INTEGRATION:
Project management, documentation
In addition:
Black-box test
Measures for control of failures
De-energization principle
Design for controlling voltage effects
Design for controlling effects of physical environment
Program sequence monitoring (software)
"Safe" data communication processes (bus systems)
Automatic tests
In addition:
Redundant hardware/diverse hardware
Positive mode of actuation
Mechanically linked contacts/direct opening action
Oriented mode of failure
Over-dimensioning

Most of the measures are explained in brief in the standard. Attention is drawn to the fact that in the daily practice of the BGIA, diversity is assumed to be of major benefit in general, and not only as shown for hardware in Figure 6.4. Refer in this context also to the information concerning the requirements upon software in Section 6.3.10.

The astute reader of this report may wonder in what way these measures differ from those against common cause failure (CCF, see Section 6.2.15). Common cause failures are of course also to be regarded as systematic failures. The analysis of CCF however addresses only structures which are multi-channel in form or which at least possess test equipment (Categories 2, 3 and 4). A further difference is the "attempt" to consider CCF aspects numerically (quantitatively); by contrast, the analysis described in Annex G of the standard is purely qualitative. Given adequate measures against systematic failures in accordance with Annex G of the standard and observance of basic and well-tried safety principles, it would not appear particularly difficult to satisfy the requirements for measures against common cause failure (CCF).

Three examples will show that actual requirements may indeed vary according to application and technology, and that an explanation of the general requirements may therefore also be necessary at times.

Example 1:
Measures for control of the effects of a power failure

The design of safety-related parts of control systems must also give consideration to faults in the power supply (electric power, air pressure in pneumatic systems, hydraulic fluid pressure) (see Section 5.2.8 and Annex G of the standard). Voltage breakdown, voltage fluctuations and overvoltage or undervoltage may for example endanger the safe state of a machine. This particularly applies to the raised holding of loads by means of electrical and hydraulic drives (vertical axes). Such disturbances may be caused by component faults within the SRP/CS. In this case, their effects upon the Performance Level are considered during verification. Should the cause lie in the mains supply however, or if the mains disconnecting device (main switch) of the machine has been actuated, these cases lie beyond the scope of quantitative analysis. They can be considered only as systematic failures – and in some cases even as operating states – which must be controlled by the SRP/CS such that the safe state is achieved and/or maintained. Reducing the requirements to a lower PL_r, for example because failure of the power supply is rare, is not permissible, since consideration of a power failure has no effect upon the parameters S, F and P, which are relevant for the risk assessment.

Example 2:
Failure of pneumatic or hydraulic valves

Among the requirements of EN ISO 13849-2, Table B.1 "Basic safety principles" and Table B.2, "Well-tried safety principles" for pneumatic systems are that attention must be paid to the "use of suitable materials and adequate manufacturing" and the "proper avoidance of contamination of the compressed air" during the design and manufacture of pneumatic components. These requirements apply above all to the selection of materials, the processes of manufacture and treatment in consideration of factors such as stresses, durability, abrasion, wear, corrosion and temperature, and the consideration of highly effective filtration of the compressed air and the removal of solids and water. Table C.1 and C.2 similarly specify the requirements for hydraulic systems. Attention must in the same way be paid to “proper avoidance of contamination of the fluid” and to “correct dimensioning and shaping”.

Greater resistance to operating movement may nevertheless arise in fluid power components which are operated infrequently, owing to their design characteristics (gap between the valving element and the enclosure):

- On pneumatic valves with soft seals which remain in the same switching position for a longer period, the seals may swell owing to chemical influences caused by the lubricant (oil with additives in the compressed air, introduced by the compressor, lubricator, or lubrication for life), or the lubricating film may collapse under the pressure of the seal edge, resulting in increased resistance to operation.
- On hydraulic valves, silting may occur when the valve remains in the same switching position for a longer period. In this case, fine dirt particles are deposited in the sealing gap between switching operations, causing the valving element to stick.

For these reasons, a high force surplus (e.g. spring force) is generally required to return the valving element to the “safety-oriented switching position”. On non-mechanical springs, retention of the reset function must be assured by suitable measures. In addition, the effects described above must be prevented by suitable switching cycles/test cycles at intervals for example of less than 8 hours.

Example 3:
Separation of safety-related and non-safety-related functions

Standards governing functional safety generally address the separation of safety-related functions from other (non-safety-related) functions. This is also the case for EN ISO 13849-2, for example as a well-tried safety principle for electrical systems under the heading “Minimise possibility of faults”. This requirement applies to both hardware and software. At the same time, reasons may exist which make complete separation disadvantageous. In such cases, clearly defined functional and technical interfaces must at least be implemented which enable influences upon the safety-related part to be avoided and/or controlled.

This requirement is illustrated well by the example of the development of application software. The most far-reaching form of separation between standard application software and safety-related application software (SRASW, see Section 6.3) is of course for them to be written with separate programming systems (engineering suites) and run on separate PLC. For economic reasons in particular, however, it is desirable for the entire application software to be written by means of a single programming system, possibly in the same engineering process. A number of aspects must be considered here, however. These include the requirement that safety-related variables, results or outputs must not be overwritten by non-safety-related parts of software (program, function block, function/instruction, etc.). Links between the two environments are permissible, but only with the observance of specified conventions.

One such convention is that safety-related signals and functions must always retain priority: linking by means of an OR operation, for example, is not permitted under any circumstances. Software development tools nowadays support such approaches, and have implemented defined functions and rules with automatic checking (in the editors and compilers). Errors in logic operations which may have an effect only in unexpected operational situations or which may not be detectable with reasonable effort at the time of acceptance/commissioning can thus be prevented in a user-friendly manner.

This does not mean that the designer will be spared a complete analysis of the influence exerted by functional standard components of a control system upon the safety-related parts, including that of the influence of the safety-related functions upon each other. The analysis of where (technically) and how (functionally) such influences may arise will however be considerably simplified and accelerated by the use of the development tools referred to above. The even more pertinent question, namely that of how the influences which are detected are to be eliminated (avoided or controlled), may not even arise.

6.1.3 Ergonomics

Annex I Section 1.1.2d of the European Machinery Directive 98/37/EC requires that, at the design stage of the machine, manufacturers of machines reduce the discomfort, fatigue and psychological stress faced by the operator to the greatest possible extent, taking into account ergonomic principles. This therefore also applies to the interfaces between the operator of a machine or installation and the SRP/CS. These interfaces include both specific protective devices, such as a safety guard with position switch, and the operation of a safety function, for example by a pushbutton or even by a software display interface which is suitable for this purpose.

The importance of ergonomic principles for SRP/CS, and the fact that not all cases of intended use or foreseeable misuse of an SRP/CS are necessarily considered during the design of a machine, is demonstrated by the HVBG Report on the bypassing of protective devices on machinery [22].

EN ISO 13849-1 therefore requires that ergonomic principles be applied, and lists a number of useful standards for this purpose in Section 4.8. In order for designers of machines to be able to check the design of the human-machine interface of the SRP/CS, a checklist for ergonomic machine design was drawn up by the BGIA. In October 2006, this checklist and further documents were published in the form of the BG Information BGI 5048-1 and BGI 5048-2 [23]. Among the subjects addressed more specifically are: manually operated actuators; keyboards, keys and input devices; displays; visual danger signals; and the software ergonomics of user interfaces. VDI/VDE guideline 3850 [24] for example serves as an aid to the user-friendly design of useware for machines.

6.2 Quantification of the probability of failure

The numerical quantification of the probability of failure required by the standard for determination of the PL, often referred to (including in other standards) simply as “quantification”, can strictly speaking never be determined exactly, but only by approximation with the aid of statistical methods or other estimations. The main influencing variables which must be considered during this process of determination are stated; the method by which the probability of failure is actually determined from them is however at the user's discretion. Any validated and recognized method is permitted here. Such methods include reliability block diagrams, fault tree analysis, Markov modelling or Petri nets. Depending upon the party determining the probability of failure, i.e. the manufacturer of the control system, the user of the machine, or a test body, preferences for and experience with different methods may vary. For this reason, any suitable method is explicitly permitted in this context.

At the same time, parties lacking prior experience in quantification of the probability of failure will require a certain amount of support in the use of EN ISO 13849-1. This need has been considered by the development of a simplified approach which, whilst being based upon sound scientific principles (Markov modelling), describes a simple method for quantification in successive steps. At certain points, the description makes estimates erring on the safe side which could result in a greater figure for the probability of failure being estimated when compared to more precise methods; the method is, however, suitable for practical application even by non-mathematicians, and the procedure is largely transparent and therefore verifiable. This simplified method is presented below in detail, both in general terms and with reference to a calculated practical example (see Section 6.5). Further details on selected specific subjects can be found in the Annexes.

6.2.1 Designated architectures ...

The structure or architecture of a safety control system determines its tolerance to faults and constitutes the framework upon which all other quantifiable aspects are based, by which the PL of the safety-related parts of control systems is ultimately formed. The experience gained by the BGIA with industry since 1985 confirms that the greater part of all implemented controls can be assigned to a very limited number of basic types of safety-related control systems (or to combinations of these basic types, see below). These types are: at one end of the spectrum, the single-channel untested system with components of differing reliability; in the middle of the spectrum, the same type, but enhanced by testing; and at the other end, the two-channel systems featuring high-quality testing. Systems with more than two channels and other “exotic” structures are extremely rare in machine construction, and the simplified method is of only limited use for their assessment. Even where more than two channels are present, however, it is generally sufficient for the two most reliable channels to be considered in order for the PL to be estimated with sufficient precision by means of the simplified method involving designated architectures. Therefore, systems employing more than two channels are not considered in EN ISO 13849-1. In addition to this “horizontal” division into various functional or testing channels, a “vertical” division into a sensor level (input devices, “I”), a processing level (logic, “L”) and an actuator level (output devices, “O”) is generally also advantageous.

Continuity is assured, fully intentionally, to the Categories of EN 954-1 which are established in the machine construction industry and the associated standards.
In accordance with this system, EN 954-1 defines five structures as Categories.
EN ISO 13849-1 supplements the former Category definition slightly with quantitative requirements for the component reliability ($MTTF_d$), the diagnostic coverage of tests (DC_{avg}) and the resistance to common cause failures (CCF). In addition, the Categories are mapped to five basic structural types, termed designated architectures. Identical Categories may still take different structural forms; the generalization which their mapping to the associated designated architecture represents is still permissible as an approximation within the simplified approach, however. The number of “vertical” blocks (input, logic, output) in a channel is for example generally of little relevance to determination of the PL from a mathematical and safety technology perspective.

Where more complex safety functions are involved, it may no longer be possible to map the entire safety chain to any one of the five basic types alone. In this case, the solution is generally for the safety chain to be dismantled into several sections, each of which can be mapped to a particular designated architecture. The method by which these sections (subsystems) are then recompiled and an overall value determined from the individual Performance Levels is explained in greater detail in Section 6.4. The following information relates to control systems (SRP/CS) which can be assigned to a Category without being dismantled into subsystems.

6.2.2 ... and Categories

The Categories classify safety-related parts of a control system (SRP/CS) in respect of their resistance to faults and their subsequent behaviour in the fault condition, based upon the reliability and/or the structural arrangement of the parts (see Table 6.2). A higher resistance to faults translates into a greater possible risk reduction. For definition of the probability of failure and of the PL, the Categories therefore form the backbone, complemented by the component reliability ($MTTF_d$), the tests (DC_{avg}), and the resistance to common cause failures (CCF).

Category B is the basic Category, the requirements of which must also be observed in all other categories. In Categories B and 1, the resistance to faults is attained primarily by the selection and use of suitable components. The safety function may be rendered ineffective by the incidence of a fault. Category 1 has a greater resistance to faults than Category B owing to the use of special components and principles which are well-tried in a safety context.

In Categories 2, 3 and 4, superior performance in terms of the specified safety function is attained primarily by structural measures. In Category 2, performance of the safety function is generally checked automatically at regular intervals by self-tests performed by technical test equipment (TE). The safety function may fail however should a fault arise between the test phases. By appropriate selection of the test intervals, a suitable risk reduction can be attained with application of Category 2.
In Categories 3 and 4, the occurrence of a single fault does not result in loss of the safety function. In Category 4, and, whenever reasonably practicable, also in Category 3, such faults are detected automatically. In addition, the resistance to an accumulation of undetected faults is also assured in Category 4.

Table 6.2:
Summary of the requirements for Categories; the three right-hand columns show the essential changes from the Category definition of the previous version of the standard

Category	Summary of the requirements	System behaviour	Principle for attainment of safety	*MTTF*$_d$ of each channel	*DC*$_{avg}$	CCF
B	SRP/CS(s) and/or their protective equipment, as well as their components, shall be designed, constructed, selected, assembled and combined in accordance with relevant standards so that they can withstand the expected influences. Basic safety principles shall be used.	The occurrence of a fault can lead to the loss of the safety function.	Mainly characterized by selection of components	Low to Medium	None	Not relevant
1	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 for Category B.	Mainly characterized by selection of components	High	None	Not relevant
2	Requirements of B and the use of well-tried safety principles shall apply. Safety function shall be checked at suitable intervals by the machine 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 detected by the check.	Mainly characterized by structure	Low to High	Low to Medium	Measures required, see Annex F
3	Requirements of B and the use of well-tried safety principles shall apply. Safety-related parts shall be designed so that: – a single fault in any of these parts does not lead to the loss of the safety function, and – whenever reasonably practicable, the single fault is detected.	When a single fault occurs, the safety function is always performed. Some, but not all, faults will be detected. Accumulation of undetected faults can lead to the loss of the safety function.	Mainly characterized by structure	Low to High	Low to Medium	Measures required, see Annex F

Table 6.2: continued

Category	Summary of the requirements	System behaviour	Principle for attainment of safety	$MTTF_d$ of each channel	DC_{avg}	CCF
4	Requirements of B and the use of well-tried safety principles shall apply. Safety-related parts shall be designed, so that: – a single fault in any of these parts does not lead to a loss of the safety function, and – a single fault is detected at or before the next demand upon the safety function, but that if this detection is not possible, an accumulation of undetected faults shall not lead to the loss of the safety function.	When a single fault occurs the safety function is always performed. Detection of accumulated faults reduces the probability of the loss of the safety function (high *DC*). The faults will be detected in time to prevent the loss of the safety function.	Mainly characterized by structure	High	High including accumulation of faults	Measures required, see Annex F

Consideration of the faults must include an assessment of what component faults may be assumed, and what faults may (with reasoning) be excluded. Information on the faults to be considered is provided in Annex C (see page 301).

In Categories 3 and 4, common cause failures capable of causing simultaneous failure of several channels must also be adequately controlled. The same applies to Category 2, since the test equipment and its dedicated deactivation path likewise constitute a two-channel system. Essentially, it can be said that many of the basic and well-tried safety principles are effective not only against random hardware failures, but also against systematic failures which may creep into the product at some point in the course of the product life cycle, e.g. faults arising during product design or modification.

6.2.3 Category B

The SRP/CS must be designed, constructed, selected, assembled and combined for the intended application in accordance with the relevant standards with application of the basic safety principles in such a way that they can resist:

- The anticipated operating stresses (e.g. reliability with regard to breaking capacity and frequency)
- The influence of the processed material (e.g. aggressive chemical substances, dusts, chips)

- Other relevant external influences (e.g. mechanical vibration, electromagnetic interference, interruptions or disturbances in the power supply)

These general principles can be presented, both in general terms and with regard to specific technologies, in the basic safety principles listed in Annex C. The general basic safety principles apply in full here to all technologies, whereas the technology-specific principles are required in addition for the technology concerned. Since Category B is the basic category for all other categories (see Table 6.2), the basic safety principles must be applied generically during the design of safety-related parts of control systems and/or protective devices.

For components which satisfy Category B, no further special safety measures are required. The $MTTF_d$ of each channel may therefore be low or medium (see below for the definition of "Low" and "Medium"). Should a component failure occur, it may lead to loss of the safety function. No monitoring measures are required, including DC_{avg}. Common cause failures also cannot be considered on single-channel control systems; no requirements therefore exist with regard to CCF.

Owing to this very rudimentary resistance to failure, the maximum attainable PL of Category B systems is limited to PL b.

The designated architecture for Category B in Figure 6.5 corresponds to a single-channel system with input (I), logic (L) and output (O) levels.

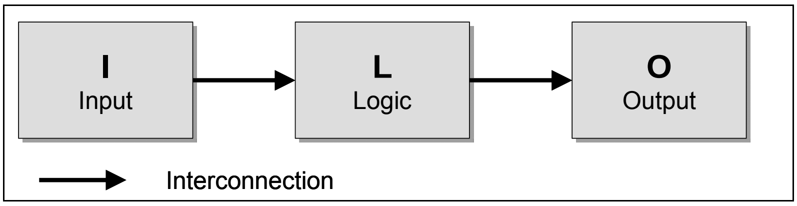


Figure 6.5: Designated architecture for Category B and Category 1

6.2.4 Category 1

In addition to the requirements for Category B, for example the application of basic safety principles, Category 1 SRP/CS must be designed and constructed with the use of components and principles which are well-tried for safety-related applications.

A well-tried component for a safety-related application is a component which either

- has been widely used in the past with successful results in similar applications, or
- has been made and verified using principles which demonstrate its suitability and reliability for safety-related applications.

Annex C (page 301) provides an overview of known well-tried components embodying various technologies for safety-related applications.

Newly developed components and safety principles may be considered as equivalent to "well-tried" if they fulfil the second condition stated above. The decision to accept a particular component as well-tried depends on the application. Complex electronic components, such as programmable logic controllers (PLCs), microprocessors or application-specific integrated circuits (ASICs) cannot be considered as equivalent to well-tried. Conversely, simple electronic components such as transistors, diodes, etc. may be regarded as well-tried.

The well-tried property of a component is dependent upon its application, and indicates only that a dangerous failure is improbable. It follows that the anticipated dangerous failure rate is greater than zero, and is considered in the form of the $MTTF_d$ during calculation of the PL. Conversely, the assumption of a fault exclusion (see Section 6.2.10) gives rise to assumption of an “infinitely high” $MTTF_d$ which is not incorporated into the calculation.

Owing to the expected higher component reliability, the $MTTF_d$ of the single channel in Category 1 must be high; as in Category B, however, no requirements are placed upon the DC_{avg} and CCF. The incidence of a fault may lead to loss of the safety function. The $MTTF_d$ of the channel in Category 1 is however greater than that in Category B. In consequence, the loss of the safety function is less probable, and the maximum PL that can be attained with Category 1 is PL c.

The designated architecture for Category 1 is the same as for Category B (see Figure 6.5), since the differences lie in the component reliability and not in the structure.

6.2.5 Category 2

In addition to the requirements for Category B (e.g. the application of basic safety principles), Category 2 SRP/CS must employ well-tried safety principles and be designed such that their safety functions are tested at reasonable intervals by the machine control system. The safety function(s) must be tested

- at start-up of the machine, and
- prior to initiation of a hazardous situation, e.g. the start of a new cycle, start of other movements, and/or periodically during operation, where the risk assessment and the kind of operation indicate that this is necessary.

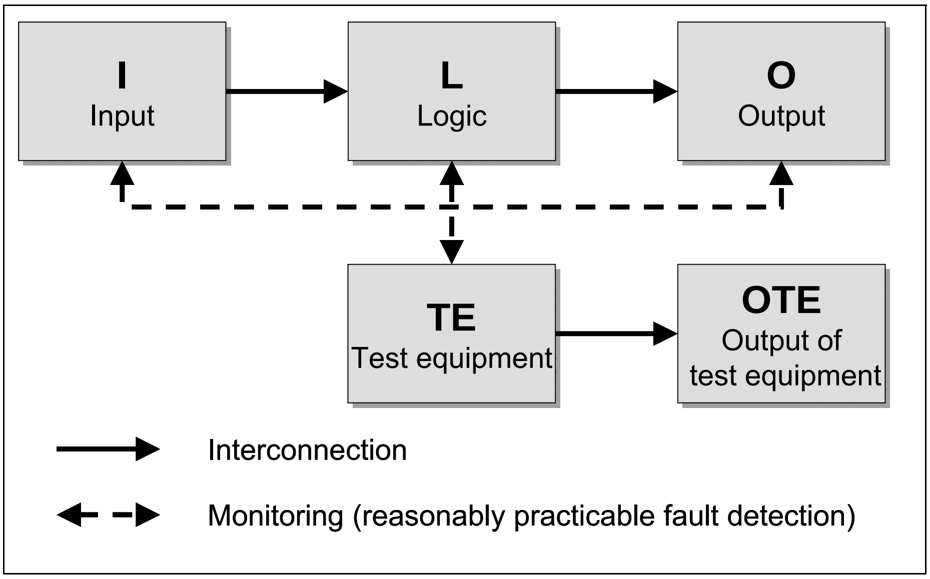
These tests can be initiated automatically. Each test of the safety function(s) must either

- permit operation, if no faults have been detected, or
- should a fault have been detected, generate an output for the initiation of appropriate control action. Whenever possible, this output must initiate a safe state. The safe state must be maintained until the fault is cleared. Should initiation of a safe state not be possible (e.g. owing to welding of the contact in the final switching element), the output must provide a warning of the hazard.

For the designated architecture of Category 2 (Figure 6.6), calculation of the $MTTF_d$ and DC_{avg} considers only the blocks of the functional channel (i.e. I, L and O), and only indirectly the $MTTF_d$ of the blocks of the test channel (i.e. TE and OTE). Values from “Low” to “High” are permitted for the $MTTF_d$ of the functional channel.

DC_{avg} must be at least “Low”. Adequate measures against CCF must be applied (see Section 6.2.15 and Annex F).

Figure 6.6:
Designated architecture for Category 2; broken lines indicate reasonably practicable fault detection



The check must not itself give rise to a hazardous situation (e.g. owing to an increase in the response time). The checking equipment may be implemented either as a part of the functional channel, or separate from it. In some cases, Category 2 is not applicable, since the test of the safety functions cannot be performed on all components. Since the safety function can fail unnoticed between tests, the interval between tests is a critical parameter. In addition, the test equipment could itself fail before the functional channel fails. For simplified quantification of the PL by means of the designated architecture and the bar chart (Figure 6.10), the following requirements are therefore imposed:

- The $MTTF_d$ value of the test equipment TE must not be lower than half the $MTTF_d$ value of the logic L (refer also to the last page of Annex E).
- The test rate must be at least 100 times the mean demand rate upon the safety function (see Section 6.2.14).

Owing to these restrictions and to the fact that with the designated architecture, a *DC_{avg}* of over 90% is difficult to attain in practice with external test equipment, undetected first faults may result in loss of the safety function. For these reasons, the maximum PL which can be attained with Category 2 is limited to PL d.

6.2.6 Category 3

In addition to the requirements for Category B (e.g. the application of basic safety principles), Category 3 SRP/CS must apply well-tried safety principles and be designed such that a single fault does not result in loss of the safety function. Where implementation is reasonably practicable, a single fault must be detected at or prior to the next demand upon the safety function.

Values ranging from low to high may be selected for the $MTTF_d$ of each channel. Since not all faults need be detected or the accumulation of undetected dangerous faults may lead to a hazardous situation, a low DC_{avg} suffices as a minimum requirement. Adequate measures must be taken against common cause failure (CCF).

The requirement for single-fault tolerance does not necessarily mean that a two-channel system must be implemented, since single-channel components with no potential for dangerous failure (fail-safe design), for example, may also be tolerant of single faults. The same applies to systems with a high standard of monitoring which respond to a fault with a dedicated deactivation path sufficiently quickly for a dangerous state to be avoided. Nevertheless, the majority of Category 3 systems are implemented in two-channel form. A corresponding designated architecture was selected for this reason (Figure 6.7). A purely "logical two-channel arrangement", for example employing redundant software on single-channel hardware, would however not generally offer single-fault tolerance of hardware failures.

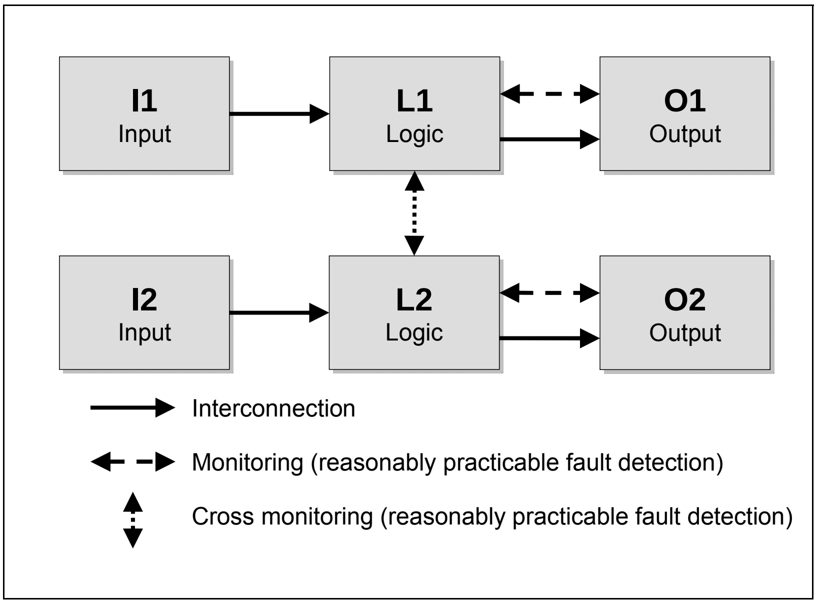

I1
Input
L1
Logic
O1
Output
I2
Input
L2
Logic
O2
Output
Interconnection
Monitoring (reasonably practicable fault detection)
Cross monitoring (reasonably practicable fault detection)

Figure 6.7: Designated architecture for Category 3; broken lines indicate reasonably practicable fault detection

6.2.7 Category 4

In addition to the requirements for Category B (e.g. the application of basic safety principles), Category 4 SRP/CS must apply well-tried safety principles and be designed such that:

- a single fault does not result in loss of the safety function, and
- the single fault is detected at or prior to the next demand upon the safety function, for example immediately upon switching-on of the machine or at the end of a machine operating cycle. Should such detection not be possible, the

accumulation of undetected faults must not result in loss of the safety function (in practice, consideration of a fault combination for two faults may be sufficient).

Since this is the Category with the greatest resistance to faults (the greatest contribution to risk reduction), both the $MTTF_d$ of each channel and the DC_{avg} must be high, and adequate measures must be taken against CCF.

Because the differences between this Category and Category 3 lie primarily in the $MTTF_d$ and the DC_{avg}, the designated architecture for Category 4 (Figure 6.8) is similar to that for Category 3. The unbroken lines for monitoring symbolize the higher DC_{avg}, however.

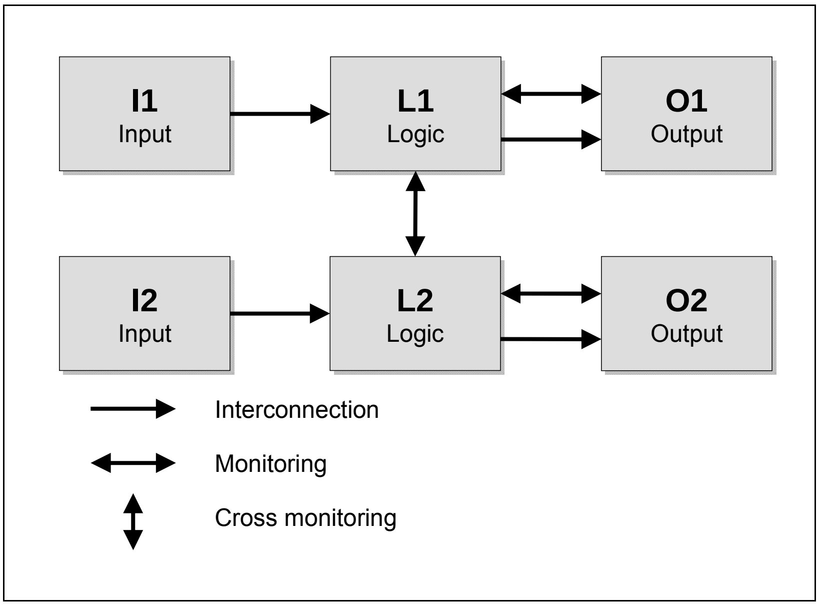


Figure 6.8:
Designated architecture for Category 4

6.2.8 Blocks and channels

For simplified quantification of the probability of failure, it is useful for the safety-related control to be presented in the form of abstracted blocks and channels. The term “blocks” has a defined meaning in this context. It refers to function blocks only in the sense that the safety function is executed in smaller units arranged in series and in parallel. The following rules can be stated for mapping of the hardware structure to a safety-related block diagram:

- The blocks should map, in abstract form, all control elements which relate to execution of the safety function.
- If the safety function is executed in multiple redundant channels, they should be presented in separate blocks. This reflects the fact that should one block fail, execution of the safety function by the blocks of the other channel is not impaired.
- Division of the blocks within a channel is more arbitrary; although EN ISO 13849-1 proposes three blocks per channel (input level I, logic level L and output level O), the chief purpose of this arrangement is clarity. Neither the

precise boundary between I, L and O, nor the number of blocks in a channel significantly affects the probability of failure calculated in the form of a PL.

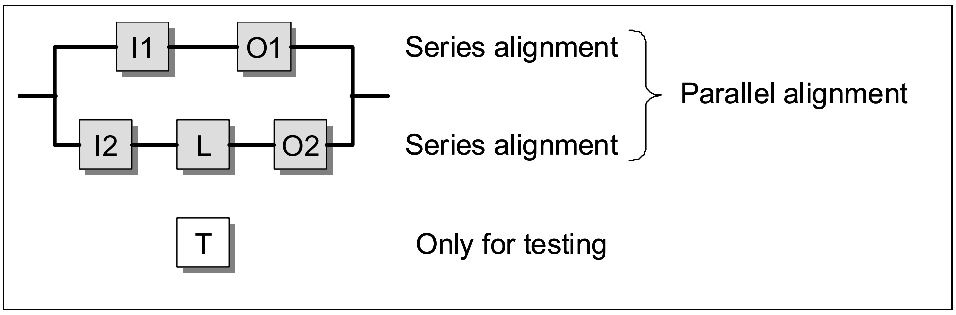
- The block assignment of each hardware unit relevant to safety must be clearly specified (e.g. in the form of a parts list). This permits calculation of the mean time to dangerous failure ($MTTF_d$) of the block, based upon the $MTTF_d$ of the hardware units belonging to the block concerned (e.g. by the failure mode and effects analysis (FMEA) or the parts count method, see Section 6.2.13).
- Hardware units employed purely for test purposes, the failure of which cannot directly impair execution of the safety function in the various channels, may be grouped as separate blocks of a supplementary test channel.

For Categories 3 and 4, the standard does not set out direct requirements for the reliability of external test equipment; with reference to Category 2, however, the $MTTF_d$ of the test equipment should be at least half that of the individual (symmetrized, see below) channel, and consideration should also be given to systematic failures and CCF.

6.2.9 Safety-related block diagram

The safety-related block diagram is based upon the more familiar reliability block diagram [25]. Common to both diagrams is the principle that the (safety) function may continue to be performed provided a chain of blocks which have not failed dangerously remains intact from left to right along the functional connecting lines. However, the safety-related block diagram presents further test mechanisms, such as the cross-check of redundant channels, or tests performed by separate test units. A general example of a safety-related block diagram is shown in Figure 6.9.

Figure 6.9:
General example of a safety-related block diagram; I1 and O1 constitute the first channel (series alignment), whilst I2, L and O2 constitute the second (series alignment); with both channels together, the safety function is executed redundantly (parallel alignment). T is used only for testing



In accordance with this definition, the following rules can be formulated for presentation of a safety control system in the form of a safety-related block diagram:

- The arrangement of blocks in series in the form of a “channel” (e.g. blocks I, L and O) expresses the fact that failure of one block may lead to failure of the entire chain. Should, for example, a hardware unit in a channel fail dangerously, the entire channel becomes incapable of executing the safety function.
- A parallel arrangement of blocks/channels symbolizes the multiply redundant execution of the safety function, or of relevant parts of it. For example, a safety function executed by multiple channels is maintained provided at least one channel has not suffered failure.
- Blocks employed for test purposes only, which do not impair execution of the safety function in the different channels should they fail, can be displayed as a separate test channel. Although failure of test measures causes the reliability of the system as a whole to be reduced, the effect is only minor, provided execution of the pure safety function in the individual channels remains assured.

The definition of the blocks and channels goes hand-in-hand with determination of the Category, and is the first step in quantification of the PL. Further values are required for this purpose: the evaluation of the component reliability ($MTTF_d$), of the tests (DC_{avg}), and of the relevance of common cause failures (CCF).

6.2.10 Fault considerations and fault exclusion

In a real-case control system, there is no limit whatsoever to the number of theoretically possible faults. It is therefore necessary for evaluation to be limited to the faults which are relevant. Certain faults can be excluded if the following points are considered:

- The technical improbability of their occurrence (a probability which is several orders of magnitude lower than that of other possible faults and the risk reduction which is to be attained)
- Good engineering practice, independent of the application under consideration
- The technical requirements relating to the application and to the specific hazard

The component faults which may occur are described in EN ISO 13849-2. The following points must be observed:

- The fault lists constitute a selection only. Where necessary, new fault models must therefore be created (for example for new components), or further fault types considered, depending upon the application. An FMEA for example may be performed for this purpose.
- Secondary faults are evaluated as a single fault together with the initial fault giving rise to them, in the same way as multiple faults with a common cause (CCF, common cause failures).
- The simultaneous incidence of two or more faults differing in their cause is regarded as extremely improbable, and does not therefore need to be considered.

Further information on fault exclusion can be found in Annex C and in Part 2 of EN ISO 13849. Should faults be excluded without the reason for exclusion being immediately apparent (such as the peeling-off of tracks on a properly dimensioned circuit-board layout), precise reasoning must be stated in the technical documentation.

Provided the requirements are met, fault exclusions are also possible for components, for example for the electrical break contacts and the mechanical actuation of electromechanical position switches or emergency stop devices. If fault exclusion applies, failure rates (*MTTF*$_d$) and monitoring measures (*DC*) need not be considered for such components.

6.2.11 Mean time to dangerous failure – *MTTF*$_d$

The reliability of the individual components from which the control system is constructed has a decisive bearing upon the overall reliability of the system. The *MTTF*$_d$ (mean time to dangerous failure) is thus also considered in the PL as a reliability value. It is clear that "failure" refers to component defects which result in the intended function not or no longer being performed. The other parts of the term *MTTF*$_d$ require explanation, however:

- "Mean" indicates that the value is a statistical mean which does not refer to a single component, but is defined as an anticipated value for the mean lifetime of the typical component. In this context, the anticipated value for the individual component can be considered equal to the mean value of a large number of components of the same type. The value is not therefore a guaranteed minimum lifetime in the sense of failure-free period. This approach employing a mean value is also reflected in the fact that the lifetime values are not normally adapted to the conditions of use (e.g. load, temperature, climate), provided the components are employed within the conditions of use specified for them. It is generally assumed here that the higher load in one application of a device is averaged out by a lower load in another application. Should higher loads be anticipated in all applications (e.g. owing to extreme temperatures), however, these conditions must be considered when the *MTTF*$_d$ is determined.

- "Time" indicates that the reliability is expressed in terms of a time in the sense of a lifetime. The *MTTF*$_d$ is generally indicated in years (abbreviated "a"). Other forms of notation which may be converted to an *MTTF*$_d$ include failure rates or switching operations. Failure rates are generally indicated by the small Greek letter λ (lambda) and expressed in the unit "FIT" (= 10^{-9} per hour, i.e. failures per billion component hours). The relationship between λ_d and *MTTF*$_d$ is expressed, at a constant failure rate λ_d over the lifetime, as *MTTF*$_d$ = $1/\lambda_d$. The conversion from hours to years must of course be considered. For components which wear primarily as a result of their mechanical actuation, the reliability is usually expressed in operation cycles, for example as a B_{10d} value, i.e. the mean number of cycles after which 10% of the components fail dangerously. In this case, the *MTTF*$_d$ can be calculated by inclusion of the mean number of operations per year n_{op} which are anticipated in the application. For more details, refer to Annex D (see page 315).

- “Dangerous” indicates that only failures which impair execution of the safety function are ultimately considered for the PL (unsafe failure). By contrast, safe failures may well cause the safe state to be assumed (operating inhibition) or reduce the availability or productivity of a machine, but the safety function is nevertheless executed properly, or the safe state initiated/maintained. In redundant structures, however, the “dangerous” attribute refers to each individual channel. Should a failure in one channel result in the safety function being rendered inoperative, the failure concerned is considered dangerous, even where a further channel is still able to execute the safety function successfully.

Both an individual component, such as a transistor, valve or contactor, and a block, a channel, or the control system as a whole, may possess an $MTTF_d$. This overall $MTTF_d$ represents the value for a channel, possibly symmetrized over several channels, and is based upon the $MTTF_d$ of all components involved in the SRP/CS. In accordance with the bottom-up principle, the unit under consideration is successively enlarged. In the interests of minimizing effort, it is often advantageous that only safety-related components need be considered in the analysis, i.e. components the failure of which could have an indirect or direct negative influence upon performance of the safety function. For simplification purposes, fault exclusions are also possible which take account of the fact that certain failures are extremely improbable and their contribution to the overall reliability negligibly small. The assumption of fault exclusions is, however, subject to certain conditions; these are set out in detail in EN ISO 13849-2 and described more comprehensively in Section 6.2.10. Provided, therefore, that certain conditions are met, conductor short-circuits or certain mechanical failures for example can be excluded on the basis of the design.

6.2.12 Data sources for individual components

One of the questions most frequently posed in this context concerns the sourcing of reliable failure data for the safety-related components. The manufacturer, and for example his technical data sheet, should be given preference here over all other sources. Many manufacturers, for example of electromechanical or pneumatic components, have already indicated that they will make such information available in the future. Where data from the manufacturer is not (yet) available, typical example values can still be obtained from established databases (see Annex D). However, since such sources generally do not distinguish between dangerous and safe failures, it may be assumed as a general approximation that on average, only half of all failures are dangerous. With consideration for the problem of obtaining reliability values, EN ISO 13849-1 lists a number of typical values. These are however very conservative estimates, and their use is therefore recommended only if the data sources indicated above are not available. In addition to MTTF_d values for mechanical, hydraulic and electronic components, the standard also contains B_{10d} values for pneumatic and electromechanical components. Details are described in Annex D (see page 315).

6.2.13 FMEA versus the parts count method

Once the MTTF_d values of all safety-related components have been obtained, certain simple rules can be used to calculate the MTTF_d value of the control system from them. A number of methods can be used for this purpose: complex, with the use of a precise failure mode and effects analysis (FMEA), or fast and simple by means of the parts count method, involving some estimations erring on the safe side. This begins with the small difference between *MTTF* and *MTTF*$_d$: what proportion of failures of a certain component are dangerous? All conceivable failure types can be listed in a complex FMEA, evaluated as either “safe” or “dangerous”, and the proportional frequency of their occurrence estimated. Since the effects of a component failure upon the block determine whether the failure mode is safe or dangerous, detailed analyses of the effect caused by a failure may be necessary. However, a greater number of failure types may prove to be “safe” than is the case with a simplified assessment, as proposed by EN ISO 13849-1: if the parts count method is used, a conservative approach assumes that overall, the safe and dangerous failures are similar in number. In the absence of more detailed information, the *MTTF*$_d$ is therefore assumed with this method to be double the *MTTF*. Once again, the principle is that of the statistical mean, i.e. an excessively favourable evaluation of one component is cancelled out by an overly pessimistic evaluation of another. It is quite possible for the parts count method and an FMEA to be combined. Where the values produced by a parts count alone yield a sufficiently low PFH, an FMEA need not be performed. Should this not be the case, however, a study of the failure modes is advantageous, for example by means of a partial FMEA, particularly on the components which exhibit poorer MTTF$_d$ values. Further explanations of this subject can be found in Annex B (see page 289).

As with other methods of quantification, evaluation to EN ISO 13849-1 assumes a constant failure rate throughout the mission time of the component for all MTTF$_d$ values. Even if this does not directly reflect the failure behaviour, as for example in the case of components subject to heavy wear, an approximate *MTTF*$_d$ value which remains valid throughout the component's mission time is nevertheless determined in this way by an estimation erring on the safe side. Early failures are generally disregarded, since components exhibiting pronounced early failure patterns do not satisfy the availability requirements for a machine control system and are therefore not generally significant on the market. The advantage of this procedure is that the *MTTF*$_d$ is always equal to the reciprocal of the associated dangerous failure rate λ_d. Since the dangerous failure rates λ_d of the components in a block can simply be added together, the MTTF$_d$ values of the components involved (N components with running index i) give rise to the *MTTF*$_d$ of the block as follows:

$$\lambda_d = \sum_{i=1}^{N} \lambda_{di} \qquad \text{i.e.} \qquad \frac{1}{MTTF_d} = \sum_{i=1}^{N} \frac{1}{MTTF_{di}} \tag{1}$$

The same relationship applies to calculation of the *MTTF*$_d$ of each channel from the MTTF$_d$ values of the associated blocks. Once the *MTTF*$_d$ for each channel is known, a further simplification is made in the form of a classification. The calculated values are assigned to three typical classes (Table 6.3).

Table 6.3:
Classification of the $MTTF_d$ of each channel

$MTTF_d$ of each channel	
Description	**Range**
Not acceptable	0 years ≤ $MTTF_d$ < 3 years
Low	3 years ≤ $MTTF_d$ < 10 years
Medium	10 years ≤ $MTTF_d$ < 30 years
High	30 years ≤ $MTTF_d$ ≤ 100 years
Non-applicable	100 years < $MTTF_d$

A mean (important: not guaranteed) lifetime of less than three years is deemed not reasonable for safety engineering components. Values exceeding 100 years may not be substituted, in order for the component reliability not to be overstated in comparison with the other main influencing variables such as the structure or tests. Should a figure of less than three years actually be produced for a channel, the components should be replaced with more reliable alternatives, since even PL a cannot otherwise be achieved. Values over 100 years for the mean lifetime are not unusual, but owing to “capping”, do not have any bearing upon the PL above this value, since the maximum value of 100 years is substituted in this case for the component reliability.

If several channels are involved in a control system, it is not initially clear which value should be employed as representative for the entire system. A cautious approach would of course be to take the lower value; results which are still safe, but better, are however produced by the following averaging formula (C1 and C2 refer here to the two channels, which are symmetrized):

$$MTTF_d = \frac{2}{3}\left[MTTF_{dC1} + MTTF_{dC2} - \frac{1}{\frac{1}{MTTF_{dC1}} + \frac{1}{MTTF_{dC2}}}\right] \qquad (2)$$

Where the channels concerned are balanced, the $\mathrm{MTTF_d}$ value calculated in this way corresponds to the $\mathrm{MTTF_d}$ value of a channel. Where they are imbalanced, the result is an average $MTTF_d$ the minimum value of at least two-thirds of the better value. A further possible scenario here is that the better value had already been capped to an $MTTF_d$ of 100 years, and the symmetrized value is thus less than 100 years as a result. It is therefore generally more effective to implement channels of balanced reliability wherever possible. Regardless of the number and form of the channels, the result of this method is always an $\mathrm{MTTF_d}$ value for a single control channel which, averaged over the control system, indicates the level of component reliability.

6.2.14 Diagnostic coverage of test and monitoring measures – *DC*

A further variable with a major influence upon the PL are the (self)test and monitoring measures in an SRP/CS. Effective tests for example permit some compensation to be made for poor reliability of the components. The quality of the tests is measured in EN ISO 13849-1 by the diagnostic coverage *DC*. The *DC* is defined as the proportion of detected dangerous failures among all conceivable dangerous failures. The reference quantity may be a component, a block, or the entire SRP/CS. In the last of these cases, the DC is the average diagnostic coverage DC_{avg}, which has an important function in simplified calculation of the PL by means of the bar chart.

As at many other points in the standard, two methods exist for calculation of the DC_{avg}: one more precise but more complex; the other simpler, involving a series of estimations erring on the safe side. The precise, complex method involves a failure mode and effects analysis (FMEA) and is based upon the DC definition. In this case, the dangerous detectable (dd) and dangerous undetectable (du) failure types for each component are determined, together with their proportions of the total failure rate of the component. Finally, summation and formation of the ratio produces the DC value for the unit under consideration:

$$DC = \frac{\sum \lambda_{dd}}{\sum \lambda_{dd} + \sum \lambda_{du}} = \frac{\sum \lambda_{dd}}{\sum \lambda_{d}} \qquad (3)$$

The method favoured by EN ISO 13849-1 is based upon a reasoned conservative estimate of the *DC* directly on the component or block level, followed by calculation of the DC_{avg} from the individual DC values by means of an averaging formula. Many tests can be classified as typical standard measures for which estimated DC values are listed in Annex E of the standard. These measures are classified in a coarse system comprising four marker values (0%, 60%, 90% and 99%). A comprehensive list of the typical test measures stated in the standard can be found in Annex E. Application is explained with reference to the example of the control system for a paper-cutting guillotine (see Section 6.5).

A number of boundary conditions must be observed for calculation of the *DC* of a component or block:

- Detection of a dangerous failure is only the beginning. For successful conclusion of a test, a safe state must be initiated which does not present any further danger. This includes an effective shut-off path, which for example in the case of single-channel tested systems (Category 2) entails a requirement for a second shut-off element. This is required in order to initiate and maintain the safe state when the test has detected failure of the normal shut-off element (block "O" on the safety-related block diagram).

- The triggering of a test, its performance, and the necessary deactivation should ideally all be performed automatically by the SRP/CS. Only in exceptional cases would it appear advisable to rely here upon manual intervention, for example by the machine operator: in practice, it is sadly often the case that the necessary measures are not adequately implemented, whether out of idleness, or owing to pressure of work or poor information or organization. The effective implementation of manual tests entails considerable organizational effort and discipline. Calculation of the *DC* for two-channel systems nonetheless takes account of fault detection when a demand is made upon the safety function, i.e. consideration is not limited to tests triggered automatically by programmable electronics; electromechanical components such as relays or contactors constitute classic cases in which the “failure to drop out” fault can typically be detected only when a demand is made upon the safety function. Where faults are to be detected in the event of a demand, the frequency must be considered with which a demand is made upon the safety function.

- A further aspect is the question of the necessary test frequency. A test which is not executed sufficiently frequently may under certain circumstances be overtaken by the incidence of a hazardous event, and may therefore give a false impression of safety. As a rule of thumb, the test frequency is always in competition with other frequencies; for this reason, a generic adequate frequency cannot be stated. In the two-channel Category 3 and 4 systems, the test frequency is in competition with the frequency of incidence of a second dangerous failure, since only if the second channel fails before a test has detected the failure of the first channel does a danger exist of the safety function not being executed. As per the definition, Category 4 systems even tolerate the accumulation of undetected faults. In two-channel systems, a frequency of one test per shift has proved appropriate in practice. The situation is different in the case of Category 2 single-channel tested systems. Here, the test must be passed before the next demand upon the safety function – i.e. a potential hazard – occurs. In this case, the test frequency is therefore in competition with the frequency of the demand upon the safety function. In both cases, a factor of 100 is regarded as adequate, i.e. a test frequency which is at least 100 times the dangerous failure rate λ_d (= 1/$MTTF_d$) (for Category 3 or 4) or the mean demand rate upon the safety function (for Category 2). By contrast, down to a factor of 25, the maximum increase in the probability of failure is approximately 10%. Below this level, the synchronization of demand and testing essentially determines whether testing is even relevant. Should, in single-channel tested systems, the tests be executed with the demand on the safety function so quickly that the safe state is attained before a hazard arises, no conditions are imposed upon the frequency of testing.

- A further point is the reliability of the test equipment itself: a general requirement is that the test equipment should not fail prior to the components which it monitors. At the same time, it is inefficient for much greater investment to be made in the reliability of the test equipment than in the safety equipment which performs the safety function proper. EN ISO 13849-1 therefore imposes only limited requirements upon the reliability of the test equipment. For Categories 3 and 4, reliance is upon single-fault tolerance, since inclusive of failure of the test equipment, a total of three dangerous failures must occur before the safety function ceases to be executed. The occurrence of such a case unobserved is considered extremely improbable and not therefore critical. For Category 2, a secondary condition exists, at least with the simplified procedure for determining of the PL by means of the bar chart, which was set out for calculation of the “Category 2 bars”: in this case, the dangerous failure rate of the test equipment should not exceed twice the dangerous failure rate of the components which it monitors. In cases of doubt, this comparison can be performed on a per-channel basis, with the result that the $\mathrm{MTTF_d}$ value of the entire test channel should not be lower than half of the $\mathrm{MTTF_d}$ value of the functional channel.

- The effectiveness of a given test measure, for example fault detection by the process, may depend heavily upon the application, and can vary anywhere between 0 and 99%. Particular care must be taken here during selection of one of the DC marker values.

- A situation is possible in which components or blocks are monitored by several tests, or in which different tests act upon different components, with the result that an overall *DC* must be determined for the components or the block. Annex E (see page 333) provides assistance in these issues.

- In the case of programmable electronic systems in particular, a large number of complex faults is conceivable, with the result that corresponding requirements must be placed upon the complexity of the tests. In this case, should a *DC* of over 60% be required for the (programmable or complex) logic, EN ISO 13849-1 calls for at least one measure for variant memory, invariant memory and the processing unit – where present – with a *DC* of at least 60% in each case.

Once the DC values of all blocks are known, the $\mathrm{DC_{avg}}$ value for the system is calculated by means of the approximation formula (4). This formula weights the individual *DC* values with the associated $MTTF_\mathrm{d}$ values, since very reliable parts (high $MTTF_\mathrm{d}$) are less reliant upon effective tests than unreliable parts (the sums in numerators and denominators are formed across N blocks of the entire system):

$$DC_\mathrm{avg} = \frac{\dfrac{DC_1}{MTTF_\mathrm{d1}} + \dfrac{DC_2}{MTTF_\mathrm{d2}} + \ldots + \dfrac{DC_\mathrm{N}}{MTTF_\mathrm{dN}}}{\dfrac{1}{MTTF_\mathrm{d1}} + \dfrac{1}{MTTF_\mathrm{d2}} + \ldots + \dfrac{1}{MTTF_\mathrm{dN}}} \qquad (4)$$

Once obtained, the DC_avg constitutes a value describing the quality of the test and monitoring measures averaged over the entire SRP/CS. Before this value can be substituted in the simplified quantification of the PL together with the Category (five classes) and the $MTTF_\mathrm{d}$ of each channel (three classes), it must be assigned to one of the four classes in Table 6.4.

When the DC_avg is subsequently used in the simplified quantification involving the bar chart (see Section 6.2.16), only the respective lower marker value of a $\mathrm{DC_{avg}}$ class (0%, 60%, 90% or 99%) is used. A further simplification thus takes effect here, based upon an estimation erring on the safe side.

In specific cases, this coarsely simplified system may however give rise to paradoxes, if for example an unreliable component with an above-average *DC* for the SRP/CS is replaced by a more reliable component (for a more detailed explanation, refer to the end of Annex G on page 352).

DC (diagnostic coverage)	
Description	**Range**
None	$DC < 60\%$
Low	$60\% \leq DC < 90\%$
Medium	$90\% \leq DC < 99\%$
High	$99\% \leq DC$

Table 6.4:
The four levels of diagnostic coverage in accordance with the simplified approach of EN ISO 13849-1

6.2.15 Measures against common cause failure (CCF)

The final parameter relevant to the simplified quantification of the probability of failure concerns common cause failures (CCF). Such failures are related dangerous failures, for example in both channels of a redundant SRP/CS, which are attributable to a common cause. Examples include unfavourable environmental conditions or overloads which were not adequately addressed during design of the control system. Should the channels not be adequately separated, dangerous secondary faults may occur which render the intended single-fault tolerance ineffective. The quantitative relevance of these effects in a specific system is difficult to estimate (refer also to Annex F). In Annex D of IEC 61508-6 [27], the “beta-factor” model is used for this purpose. In this model, the rate of common cause failures is placed as $\beta \times \lambda_d$, in relation to the dangerous failure rate of a channel λ_d. Without a precise FMEA, β can at best only be estimated for a real-case SRP/CS, however. For this purpose, EN ISO 13849-1 contains a checklist of eight important counter-measures, which are evaluated with between 5 and 25 points:

- Physical separation between the signal paths of different channels (15 points)
- Diversity in the technology, the design or the physical principles of the channels (20 points)
- Protection against possible overloading (15 points) and the use of well-tried components (5 points)
- Failure mode and effects analysis during development for the identification of potential common cause failures (5 points)
- Training of designers/maintainers in CCF and its avoidance (5 points)
- Protection against common cause failures triggered by contamination (mechanical and fluidic systems) and electromagnetic interference (electrical systems) (25 points)
- Protection against common cause failures triggered by unfavourable environmental conditions (10 points)

The points stated for a given counter-measure are to be awarded either in full, or not at all. No points are awarded for a “partial” implementation of the counter-measures. Different packages of measures may however be effective against CCF at subsystem level. Should all eight counter-measures be satisfied, a maximum total of 100 points is awarded. However, EN ISO 13849-1 requires only a minimum total of 65 points – and even then, only for SRP/CS in Categories 2, 3 and 4. In Category 2 systems, the objective is the avoidance of dangerous common cause failures in test and functional channel which could give rise to an undetected occurrence of a dangerous fault. During creation of the bar chart for simplified quantification, the 65 points were equated to a beta factor of 2%. The coarse approximation with regard to the five Categories and the three $\mathrm{MTTF_d}$ and four $\mathrm{DC_{avg}}$ classes was carried further and reduced to a simple yes/no decision. Whereas the benefits of a redundant structure are eliminated almost completely even at a beta factor of almost 10%, a beta factor not exceeding 2% reduces the relevance of common cause failures to a justifiable level.

6.2.16 Simplified determining of the PL by means of the bar chart

Even after the four essential quantitative parameters for calculation of the probability of failure have been resolved, determining the attained PL for the SRP/CS from them remains a difficult task. Although in principle, any suitable method is permitted, EN ISO 13849-1 proposes a simple graphical method which is based upon more complex calculations and estimations erring on the safe side: the bar-chart method (see Figure 6.10).

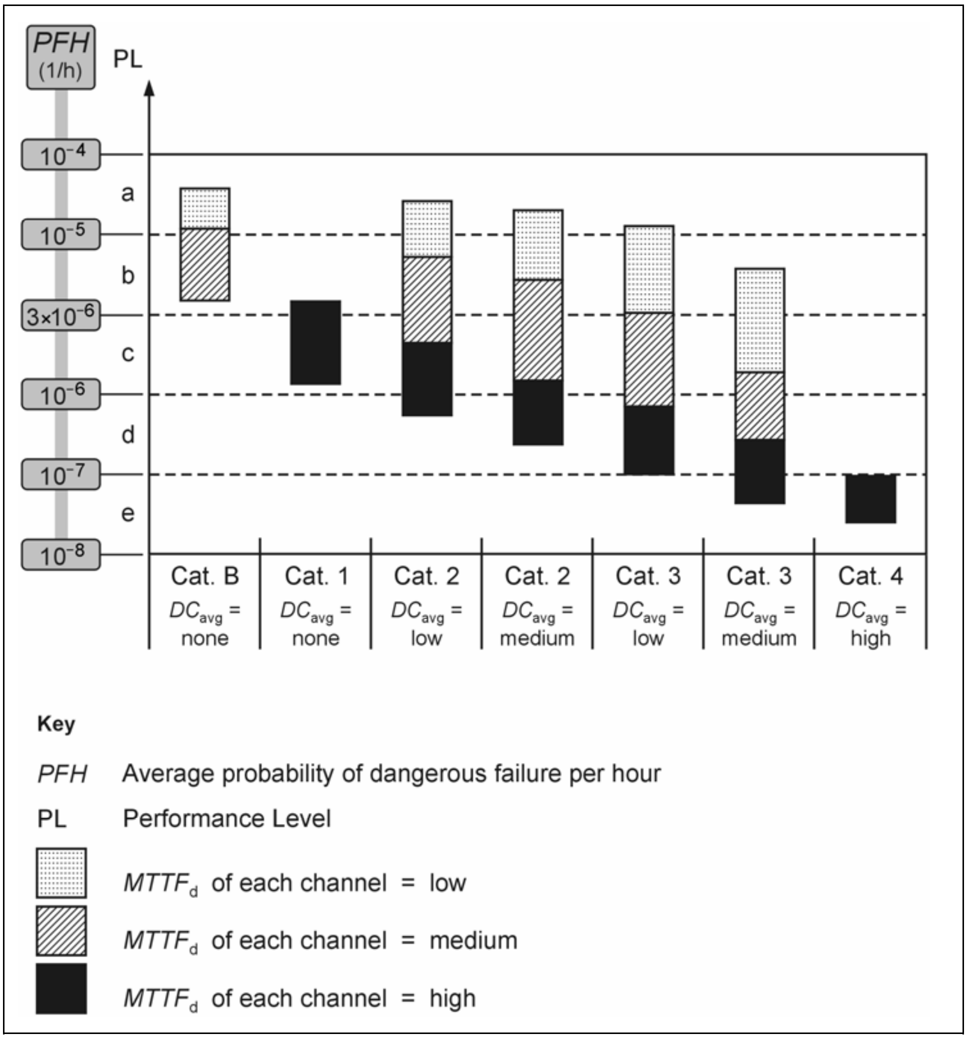
This diagram was generated by Markov modelling based upon the designated architectures for the Categories; further details can be found in Annex G (see page 347). When the bar chart is used, the relevant bar is first determined on the horizontal axis from the attained Category – adequate measures against CCF must be provided in this case for Categories 2, 3 and 4 – in combination with the attained $\mathrm{DC_{avg}}$ class. The level of the $MTTF_\mathrm{d}$ attained by the SRP/CS on the selected bar determines the PL, which can be read off on the vertical axis. This method permits rapid qualitative estimation of the attained PL even in the absence of precise quantitative data. Should more precise values be required, for example not only the PL, but also a value for the average probability of a dangerous failure per hour, the tables contained in Annex K of the standard are useful. Similar assistance is also provided by the BGIA SISTEMA software (see Annex H), which analyses the bar chart quantitatively.

During creation of the bar chart, consideration was not only given to designated architectures; certain conditions were also laid down which are to be observed during the chart's application:

- A mission time of 20 years is assumed for the SRP/CS, within which the component reliability can be described or approximated by constant failure rates. The actual mission time may be reduced to below the assumed 20 years owing to the use of components subject to severe wear (refer to the $\mathrm{T_{10d}}$ value in Annex D) or for other reasons. Application of the bar chart is justified in this case by preventative replacement of the affected components or SRP/CS. This information must be made available to the user in a suitable form, for example in the information for use and by marking on the SRP/CS.

- In the bars for Category 2, it has been assumed that the test frequency is at least 100 times the mean frequency of the demand upon the safety function, and also that the test equipment is at least half as reliable as the logic (refer also to Annex E).

Figure 6.10:
Bar chart for simplified determining of the PL from the Category (including measures against CCF), the DC_{avg} and the $MTTF_d$



Owing to capping of the allowable $MTTF_d$ of each channel to 100 years, a high PL can be attained only with certain Categories. Although this is related to the simplified approach of the designated architectures and the bar chart, the associated limitations also apply to an unrelated calculation of the average probability of a dangerous failure per hour by means of other methods. As already mentioned, the architecture imposes the following limitations upon certain Categories. The limitations are intended to prevent the component reliability being overstated in comparison with the other influencing variables:

- In Category B, a maximum PL of b can be attained.
- In Category 1, a maximum PL of c can be attained.

- In Category 2, a maximum PL of d can be attained.
- In Categories 3 or 4, a maximum PL of e can be attained.

Besides the quantitative aspect of the probability of failure, qualitative aspects must also be considered for attainment of a given PL. Such aspects include systematic failures (see Section 6.1.2) and software faults. These will be discussed in greater detail in Section 6.3.

6.2.17 Bus systems as "interconnecting means"

The discrete blocks input unit, logic and output unit of a designated architecture must be connected together not only logically, but also physically. For this purpose, the standard defines "interconnecting means", which are regarded as part of the SRP/CS. The term "interconnecting means" may initially appear strange to an expert from the field of electrical or fluid power technology. However, it serves as a generic term for electrical and fluidic lines, and even for such components as mechanical plungers. All requirements of the standard therefore also apply to these forms of "interconnecting means". In the context of fault consideration, a conductor short-circuit for example is an assumed fault. What, however, is the situation when bus systems are used to transmit safety-related information? Detailed consideration of such a complex subject is of course outside the scope of the standard, particularly since BG test principles (GS-ET-26, [28]) exist on the subject and a corresponding international standard is available (IEC 61784-3 [29]). Bus systems which satisfy the requirements described in these publications can also be readily employed in the context of EN ISO 13849-1. Several bus systems suitable for safety-related use already exist on the market.

The publications referred to above employ a special fault model by which consideration is given to the use of a black-box channel for the transmission of safety-related data: in other words, no particular requirements for fault detection, for example, are placed upon this transmission channel itself. The model assumes the repetition, loss, insertion, incorrect sequence, corruption, wrong addressing and delay of safety-related messages and the coupling of safety-related and non-safety-related messages as possible faults. Further possible aspects include faults which systematically corrupts messages, for example by completely inverting them. Measures in "safety layers" which are then implemented in safety-related parts of control systems enable transmission faults to be excluded with sufficient probability. Suitable measures include for example sequence number, time stamp, time expectation, connection authentication, feedback message and data integrity assurance. Data integrity assurance in particular frequently entails complex calculations. The purpose of these calculations is to determine the "residual error probability" *R*, and from it the "residual error rate" Λ (derived from the lower-case λ for the failure rate for components). This is the value which, with regard to the average probability of a dangerous failure per hour required for a PL, can then be substituted as the component for the transmission of safety-related messages. Both of the above publications limit the residual error rate to 1% of the maximum value permitted for the probability of a dangerous failure per hour. Values stated by manufacturers are in fact frequently related to an SIL (see Chapter 3); in practice, however, these values are compatible for use under a required PL (see also Figure 3.2). The 1% rule results in the contribution to the probability of a dangerous failure per hour being virtually negligible, i.e. enables it to be added to the values determined for the SRP/CS. Comprehensive information on bus systems for the transmission of safety-related information can be found for example in [30].

Where a bus system, which is generally tested by an independent body, or its components are employed for the implementation of safety functions, planning of its use and proper implementation with regard to fault avoidance are of great importance. A large number of parameters must be set; this process is supported to a greater or lesser degree by relevant tools.

6.3 Development of safety-related software

Comments such as the following are frequently heard: “Of course, a software programmer with years of experience no longer makes mistakes”. This overrating of one's own ability is in fact the greatest mistake of all. Software is generally complicated, which is why the number of failures caused by software faults is on the increase, in contrast to the situation for hardware. How often are “power PC users” surprised when a computer peripheral ceases to work, and how often does the problem turn out to have been caused by a part of the software which is not compatible with another piece of software, such as a driver? Hardware faults are comparatively rare. According to [31], normal software, i.e. simple software for simple functions, contains approximately 25 faults per 1,000 lines of code. Also according to [31], well-written software contains around two to three faults per 1,000 lines of code, and the software employed in the Space Shuttle has (according to NASA) fewer than one fault per 10,000 lines. What this means in practice is that a mobile telephone, with up to 200,000 lines of code, has up to 600 software faults. A PC operating system has 27 million lines of code and therefore up to 50,000 faults; the Space Shuttle up to 300 faults; and the software for the Space Defence Initiative (SDI) up to 10,000 faults. These program faults lie dormant in the products until, under certain conditions and in certain situations, they impact upon their function. Like no other technology, software and therefore also its programmers assume a greater responsibility than ever before.

Programmable SRP/CS had already been included within the scope of EN 954-1. One of the essential changes in the revision of EN ISO 13849-1 was the introduction of requirements concerning their software and its development. For the sake of emphasis at this point: the requirements in Section 4.6 of the standard enable safety-related software to be developed for all SRP/CS in the machinery sector and for all required Performance Levels from a to e. This section is intended primarily for application programmers who develop the safety functions for a machine, for example in an application-oriented language on a programmable logic controller (PLC). By contrast, these requirements in EN ISO 13849-1 are not particularly new to developers of SRESW (safety-related embedded software), i.e. firmware or software tools for electronic safety components. Such “embedded software” developments for the components, which are generally certified, are often subject to the very complex requirements of the basic safety standard EN/IEC 61508-3 [32] (and the other seven parts), which is binding for IEC safety standards governing functional safety.

The basic principles of this section can be applied to both software types. Individual requirements tend to be formulated in detail more for application programmers of SRASW (safety-related application software). Conversely, the example described in Section 6.5 of a control system for a paper-cutting guillotine shows the development of an SRESW.

The requirements governing software development are geared to the software type used (SRASW or SRESW) and the language type. As in other current standards containing requirements for software, a distinction is drawn between the language types FVL (full variability language) and LVL (limited variability language). SRASW is generally programmed in LVL, for example in a graphical language as defined in IEC 61131-3. The requirements contained in Section 4.6.3 of EN ISO 13849-1 apply in this case.

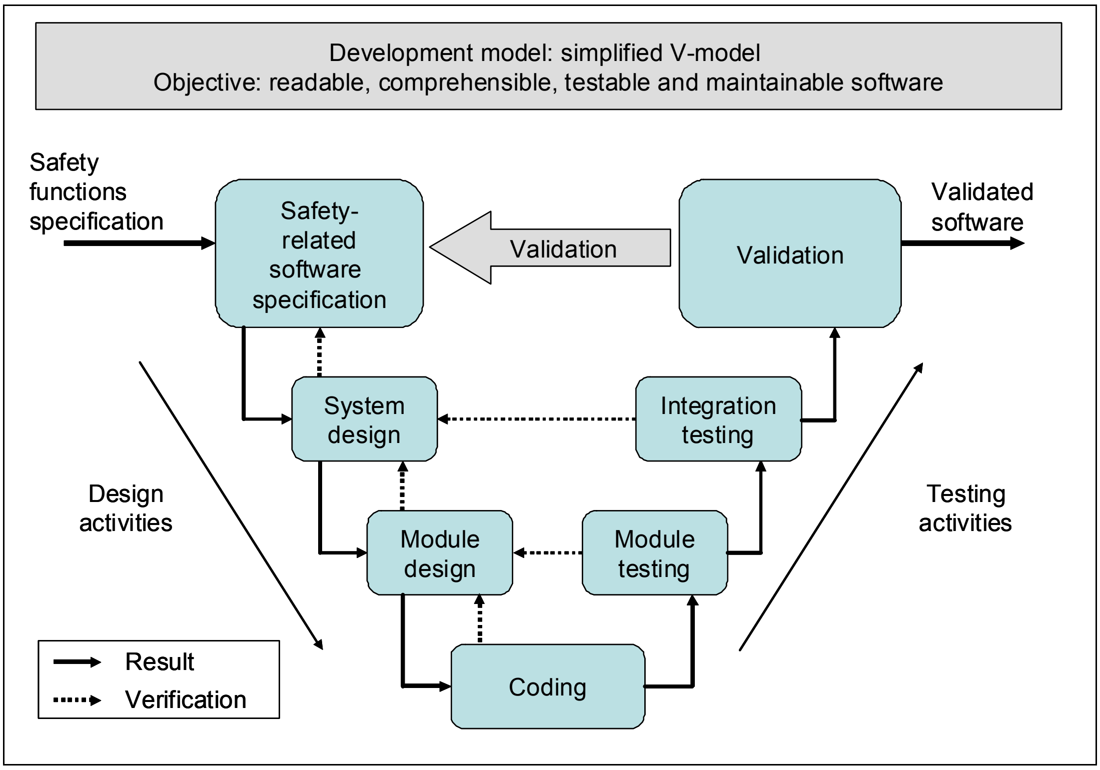
As soon as SRASW is programmed in FVL (for example, a PLC in the high-level language "C"), however, the requirements for SRESW contained in Section 4.6.2 of the standard must be met. If the SRASW is required to satisfy a Performance Level of e in this case, EN ISO 13849-1 refers at the end of Section 4.6.2, once only, but with exceptions, to the requirements of IEC 61508-3:1998.

6.3.1 Error-free software …

… unfortunately does not exist in the real world. In contrast to hardware faults, which occur as a result of random component failure, the causes of software are systematic. It is therefore all the more important that all reasonable steps be taken to avoid errors during the development of safety-related software, the purpose of which is after all that of minimizing risks. What is considered reasonable is determined on the one hand by the required Performance Level PL_r. At the same time, safety-critical faults tend to creep into particular phases of software development, where they remain undetected until they cause a failure in operation, with particularly devastating effects. These phases are known to be those of specification, design and modification. The requirements of EN ISO 13849-1 – and the explanations provided in this section – are therefore aimed in particular at fault avoidance in these phases. Sadly, it is often the case that less attention is paid in practice to these phases of application programming.

In order for safety-related software of high quality to be attained, it is clear that suitable up-to-date and well-tried development models of "software engineering" should be followed. For safety-related systems, reference is generally made in this context to the "V model" [32]. Since the V model familiar from the literature is generally used for very complex software, EN ISO 13849-1, Section 4.6.1 requires only a more simplified form of it (Figure 6.11). This form is considered to be appropriate for the practical conditions and the objectives for safety-related SRP/CS in the machinery sector and specifically for the development of SRASW. The actual objective here is the creation of readable, comprehensible, testable and maintainable software. Programmers who do not generally develop safety-related software are likely to consider these requirements tedious. However, they provide them with the certainty of having developed the software to an adequate standard.

Figure 6.11:
Simplified V model for the development of safety-related software


Development model: simplified V-model
Objective: readable, comprehensible, testable and maintainable software
Safety functions specification
Safety-related software specification
Validation
Validation
Validated software
System design
Integration testing
Design activities
Testing activities
Module design
Module testing
Coding
Result
Verification

In addition to the phases, Figure 6.11 also shows important terminology which must first be defined (in a software context).

Result

Refers to the product of a phase, for example the specification, the design document, the code, and in the case of the final result, the tested, validated software. It may however also refer to the result of a specification phase in the form of a test plan which is not required until a much later phase, at which it can be used for systematic validation of the software. The result(s) of the previous phases serve as inputs for the following phases. This is indicated by the arrow.

Verification

Describes the quality assurance activity by which the result of a phase is checked against the specification of the preceding phase. During or at the end of the coding phase, for example, verification is performed of whether the code actually implements the specified module design, and of whether the programming guidelines have been observed in the process.

Validation

In this context, software validation is a concluding, special form of verification of the entire software. A check is performed of whether the requirements of the software specification governing the functionality of the software have been implemented.

Selected phases of the simplified V model, and thus at the same time the “roadmap” for software development, are described below. The downward-pointing part of the “V” describes the design activities of development, the upward-pointing part the test activities.

6.3.2 Overall safety interface: software specification

Based upon the higher-level specification of the safety functions of the SRP/CS, the sub-functions of the specification which are to be implemented by the software are described in this document. In addition, the following are presented:

- Functions which detect and control hardware faults
- Performance characteristics, such as the maximum response time
- Fault-mode responses
- Interfaces provided to other systems, etc.

Besides these functional requirements, the PL to be attained – the PL_r – by the safety functions must be indicated, in order to permit selection of the necessary measures for fault avoidance (see further below).

This specification (or “safety-related software requirements specification”) must be verified, for example by a review performed by a person not involved in its creation. The reviewer must confirm first that the requirements specification complies with the higher-level specification, and second that it satisfies the formal requirements governing how a software specification is to be written. The specification should be structured and generated in detail in such a way that it can also serve as a checklist for later validation.

The overall safety of a machine or machinery installation is assured by all safety-related parts of the control system and their functions (components of all technologies, electronics, and software). A description is therefore required here, in the form of a specification, of the safety for the machine/machinery installation. The document needs not run into the hundreds of pages; it is acceptable for it to be limited to the essential points in a comprehensible form. The specifications for the machine or machinery installation as a whole will be followed by a subset of tasks for the programmer. The software specification thus forms a part of the overall concept, and can therefore be regarded as a “contract” with a “subcontractor”, i.e. the programmer.

The software specification begins with provisions concerning the design and coding of the software. The other elements relating to safety must be able to rely upon implementation of the functions in the software. The specification is thus also the point of reference for acceptance of the software: the validation of the software functions must demonstrate whether the “contractual obligations” have been met. In the area of SRASW, this must be taken literally, since the engineering and programming of a control system are often assigned by the parties responsible for safety as a whole to other companies or corporate divisions. In this case, the specification is also to constitute a contractually binding interface to external or internal service providers.

6.3.3 System and module design for the "safety-related technical specification"

The software architecture is generally already defined by the operating system or the development tool. The design further defines the structure and modules to be employed for implementation of the specified safety sub-functions. What existing library functions are to be employed must be determined, and whether new functions may have to be developed specifically for the project. In this section, the term software function/module also refers in all cases to a function block.

The software design document should describe the structure and process of the software, supported by diagrams, in a way which makes these aspects comprehensible to outside parties. The more the program is based upon re-used software functions which have already been validated and are already documented elsewhere, the more compact the document can be. The module design also specifies the new software functions which are to be created specifically for the project, their interfaces, and test cases for their module test. For less complex SRP/CS, the system and module design can be summarized in a "safety-related software technical specification".

6.3.4 Finally: programming

Coding work proper then begins, to the relief of the programmer. In the interests of fault avoidance, the following three aspects must be considered:

- Code must be readable and clear, in order to facilitate testing and fault-free modification at a later stage. Binding programming guidelines facilitate, among other things, better commenting of the program and the assignment of self-explanatory names to variables and modules.
- Defensive programming, i.e. the assumption that internal or external errors may always be present, and identification of them. If the characteristic of input signals over time is known, for example, this anticipatory approach can be used to detect errors in the peripheral circuitry. If a finite-state machine is programmed, the state variable is monitored against a valid value range, etc.
- The code must be analysed statically, i.e. without execution: for low PLs, a code review is sufficient; for PLs d and e, the data and control flow should also be examined, ideally with the use of tools. Typical questions are: is the code consistent with the previous software design? Do any points exist at which signals with a lower PL (for example from a standard PLC) override a signal with a higher PL? Where and by what modules are variables initialized, written to, and then assigned to the safety output? What software functions are executed conditionally?

6.3.5 Module test, integration test and validation

In the module test, the new software functions specifically developed for the project are tested and simulated in order to test whether they are coded as specified in the module design. At the integration test at the latest, the complete software is tested for proper operation on the hardware (integration) and compliance with the system design (verification), for example during the typical commissioning of a machine's PLC. Both are still verification measures, i.e. they involve looking “into” the software. Whether the safety-related sub-functions of the software perform as specified is determined by software validation, which has already been described. For the higher PLs d and e, an extended functional test is also required.

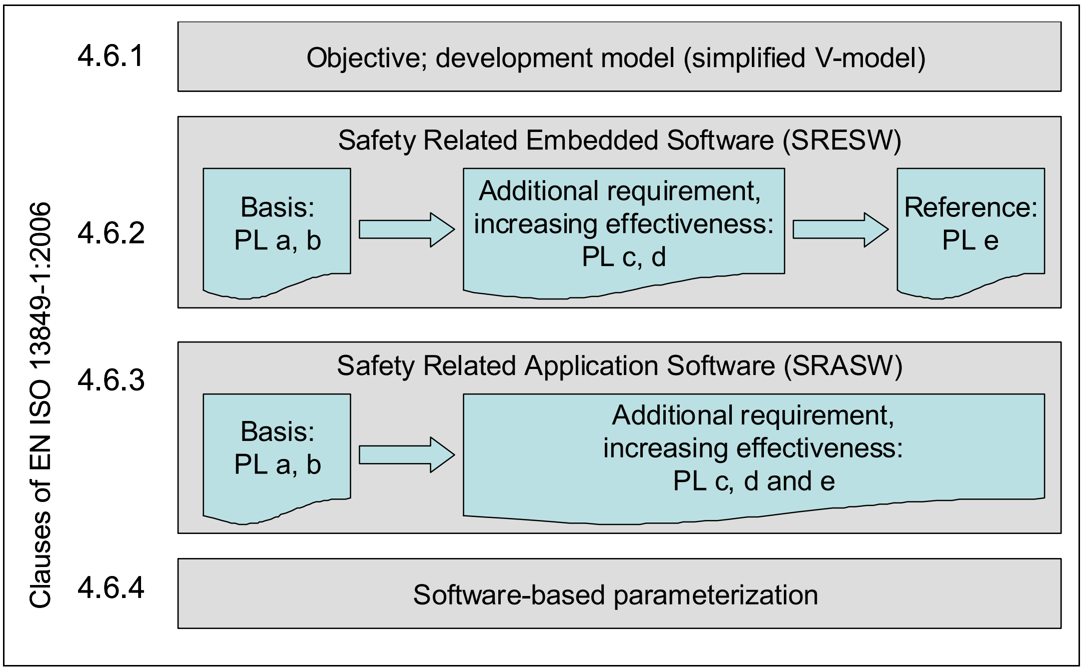
Discrete software functions which have been certified or validated by quality assurance measures do not need to be verified again. As soon as a number of these functions are combined for a specific project, however, the resulting new form of safety sub-function must be validated. Even on certified modules, dangerous systematic faults may be caused by errors in parameterization and logic.

6.3.6 Structure of the normative requirements

Once the development process has been outlined, normative requirements are described for the software itself, for the development tools used, and for the development activities. These requirements also contribute towards fault avoidance. The effort involved should be commensurate with the required risk reduction, in the same way as for the hardware of the programmable SRP/CS. The requirements and their effectiveness therefore rise in line with increasing PL_r.

Figure 6.12 shows that a suitable package of basic measures exists for all PLs, for both SRASW and SRESW.

Figure 6.12:
Grading of the requirements for safety-related software


Clauses of EN ISO 13849-1:2006
4.6.1
Objective; development model (simplified V-model)
4.6.2
Safety Related Embedded Software (SRESW)
Basis: PL a, b
Additional requirement, increasing effectiveness: PL c, d
Reference: PL e
4.6.3
Safety Related Application Software (SRASW)
Basis: PL a, b
Additional requirement, increasing effectiveness: PL c, d and e
4.6.4
Software-based parameterization

These basic measures are sufficient for the development of software for PL a or b. For software which is employed in SRP/CS for PL c to e, the basic measures are supplemented by further measures for fault avoidance. The latter are required for PL c with lower effectiveness, for PL d with medium effectiveness and for PL e with higher effectiveness. Irrespective of whether the software now acts in only one or in both channels of a desired Category, the PL_r of the implemented safety function(s) is always the yardstick for the requirements.

The aspect of “higher effectiveness” refers to the rising level of fault avoidance. This may be illustrated by the important task of production of the specification. For PL c, for example, it may be sufficient for the programmer to write the specification him or herself and for it to be reviewed by another programmer (internal review). Should the same software be employed for PL e, however, a higher level of fault avoidance must be attained. It may then be necessary for the specification to be written by the software project manager, for example, rather than the programmer. In addition, the review of this specification could also be performed jointly by the programmer and a more independent person, such as the hardware engineer. More eyes (generally) detect more faults.

A comprehensive discussion of the individual requirements and of their greater or lesser effectiveness is unfortunately beyond the scope of this BGIA Report. Discussion will therefore be limited to certain particular cases:

- It is not uncommon for the integral software of an SRP/CS to implement several safety functions (SFx) of differing PL_r (e.g. SF1 and SF2 with PL_r c, SF3 with PL_r e). In practice, however, it is unlikely to be possible to differentiate between the safety functions of differing PL_r in the development cycle, the tools, or the effectiveness of the activities (e.g. during modifications). In this case, the requirements for fault avoidance are therefore geared towards the highest PL_r (in the example given, PL e).
- Redundant SRP/CS, in which only one channel is programmable: although the programmable electronics only constitute a single channel, the overall structure corresponds to Category 3 or 4. Safety functions with a higher PL_r, such as d or e, are frequently implemented by means of these structures. Accordingly, the requirements of the highest PL_r also apply to the software of this one channel (see also Section 6.3.10).
- The use of standard PLCs: the circuit examples in this BGIA Report (see Chapter 8, page 131) demonstrate that safety-related control systems can in principle also be created with the use of standard PLCs. With PL e only, it is likely to be very difficult to attain the required “High” level of diagnostic coverage *DC* (not less than 99%) for the hardware of a PLC – at least if this diagnostic coverage is to be implemented by the SRASW. For PL a to d, the requirements for the standard PLC are described in Section 6.3.10. In addition, the application programmer must satisfy the requirements for fault avoidance with SRASW (Sections 4.6.1 and 4.6.3 of the standard) in accordance with the PL_r.
- A bonus with diverse SRESW is that on a two-channel SRP/CS for a safety function(s) with a PL_r of e, the SRESW of the two channels can be implemented differently. Should the degree of this diversity be so great that the code, the design, and even the specification have been created differently, this software can also be developed in accordance with the requirements for PL d set out in

EN ISO 13849-1. It is then irrelevant whether the SRP/CS have two different or identical hardware channels.

6.3.7 Suitable software tools

No software without tools: this particularly holds true for safety-related software. The selection and quality of these tools are therefore decisive factors for fault avoidance and thus for the quality of the safety function. EN ISO 13849-1 emphasizes four elements:

- Development tools:
  Tools are required for development which are suitable and well-tried for the intended use. Certified tools for safety components are generally employed for SRASW. Features such as the avoidance and detection of semantic errors, the observance of language subsets or the monitoring of programming guidelines relieve the programmer of tasks and enhance the quality of the software.

- Libraries of software functions:
  The design of the system should consider existing or supplied libraries and, where practicable, employ validated functions. The following principle applies: the more the program is based upon functions which are already validated or indeed certified, the fewer project-specific software components remain which must be validated by the commissioning body or an external organization. For typical recurring functions, the system integrator is well advised to invest the necessary effort in developing suitable modules himself to EN ISO 13849-1 such that they can also be re-used and tested by independent persons routinely and without error. Discrete library functions also require a specification, design, test plan, validation, etc.

- Suitable programming languages:
  For SRASW, application-oriented languages are recommended, for example in accordance with EN/IEC 61131-3 [33]. Even these languages are more comprehensive than necessary, and contain constructs which in some cases are error-prone. Programmers should therefore limit the use of the syntax. Corresponding language subsets are generally specified by the tool.

- Programming guidelines:
  Suitable programming guidelines must be observed for coding of the software functions [34; 35]. The guidelines should be the existing, accepted rules of a recognized organization. Alternatively, a company may draw up suitable programming guidelines of its own, provided they have a sound practical or theoretical basis. Programming guidelines govern the use of critical language constructs, the scope and interface of software functions, the formatting and commenting of the code, symbolic names of functions and variables, etc.

These tools and guidelines should be specified in the design document.

6.3.8 Unloved, but important: documentation and configuration management

Before the manufacturer issues the EC declaration of conformity for a machine, he must draw up its technical documentation. Where safety-related software is concerned, this refers in the first instance to specification of the implemented safety functions (requirements specification), the design document (technical specification), and the well-commented program. In addition, the certified or self-validated library functions used must be listed together with their identification (version number, author, date, etc.). Application of the manufacturer's own programming guidelines and language subsets must also be documented. Should these already be contained in the tool, an appropriate reference to these properties is sufficient. Finally, the test activities must be documented. The integration test and validation of the safety functions are often performed at the same time. These tests must obviously be planned and documented together with the test results.

What is meant by configuration management? For safety-related software in particular, it is obvious and therefore a requirement that its development be transparent to all parties involved and for subsequent inspections:

- Who specified, programmed, commissioned, verified and validated, and when?
- What was used for development, e.g. tools and their settings, re-used functions and their identification, programming guidelines?
- What program versions are loaded on which SRP/CS?

This and other necessary information must be recorded and suitably archived together with all relevant development documentation for later use, for example for modification after five years in operation.

6.3.9 Software is in a constant state of change: modification

Experience has shown that an SRASW which has already been tested will still be the subject of busy extension and adaptation work during commissioning of an installation or machine. This procedure is termed “modification”. These changes are often so extensive that not only the code, but even the original specification is no longer appropriate and should in fact be revised. Changes to safety functions at one end of the installation or machine may have an impact on the safety functions which at this stage have not been modified at the other end. Alternatively, the modifications may reveal gaps in the safety concept. This possibility should be examined, and the necessary phases of the V model repeated if appropriate.

Practical experience also shows however that even after it has already been put into service, a machine or installation may still require an additional emergency stop facility or safety guard. The machining process is also frequently improved: the safety concept must then be adapted accordingly. The existing software must be “modified”. Note: this may be the case on SRP/CS which have already been operated for a longer period of time and for the most part without failures caused by software faults – which may merely mean that a present but “hidden” fault has not yet taken effect. Following a modification, however, this situation may change, for example if the software was not adequately structured and individual modules/functions are not therefore completely without reciprocal impact.

In the situations described, “Murphy's Law” often takes effect: the program was written many years previously, but the original programmer has more pressing tasks or is already working for a different company. In this case, it is in the interests of both the safety and economy of the machine or installation for the software to possess the properties stated above: legibility, structure, intelligibility, and also conduciveness to straightforward, non-error-prone modification – independently of whatever programmer happens to be available.

In principle, a modification means that the development process must be resumed, i.e. in the V model, at the point at which a change was made (Figure 6.11), for example:

- When the code has been changed, the module and integration test must be repeated, as must validation.
- If changes were also required to the specification, it too must be verified again, for example by review by a colleague, in order to ensure that no faults have crept in at a different point in the specification. Accordingly, all development and verification measures and also validation of the affected safety functions must be repeated.

In view of the effort described, it is understandable that the influence of a modification upon the safety functions must be studied and documented systematically. Since modifications may have a not inconsiderable effect upon proper execution of the safety function, a suitable procedure must be set out at an early stage. If appropriate, this should include appointment of the persons responsible.

6.3.10 Requirements for the software of standard components in SRP/CS

Safety-related controls are often implemented by means of standard components for industrial applications. Since the standard formulates requirements for the implementation of SRESW and SRASW, these must also be satisfied with regard to electronically programmable standard components. Restrictions exist however which do not apply to tested safety components. The following Categories/Performance Levels (PLs) cannot be claimed by electronically programmable standard components:

- Category 1: excluded by the standard
- Category 4/PL e cannot generally be attained in practice with the use of standard components owing to the required high degree of diagnostic coverage (*DC*). Evaluation is necessary on a case-by-case basis.

Requirements for SRESW

All standard components under consideration must have been developed for industrial use. For the SRESW (firmware, operating system), the basic measures for PL a to b are a minimum requirement. In the majority of applications (see Table 6.5), this can be demonstrated in two ways:

- By confirmation by the component manufacturer that the basic measures have been satisfied
- By indication by the component manufacturer that he has conducted development within a QA process (e.g. to ISO 900x) in accordance with relevant product standards (e.g. EN/IEC 61131-2 for PLCs). This will be the case for the majority of standard components.

Table 6.5:
Requirements for the SRESW of standard components

No.	PL	Category, Redundancy	SRESW
1	a b	Category B/2/3	The basic measures for PL a to b apply. Two alternatives: i) Confirmation by the manufacturer, or ii) Covered by development within a QA system in accordance with relevant product standards; in this case, the manufacturer need not confirm observance of the requirements to EN ISO 13849-1
2	c d	Two components for two channels in Category 2/3 Diverse SRESW or diverse technology	Bonus by diversity of the SRESW or the technologies. The basic measures for PL a to b apply. Two alternatives: i) Confirmation by the manufacturer, or ii) Covered by development within a QA system in accordance with relevant product standards; in this case, the manufacturer need not confirm observance of the requirements to EN ISO 13849-1
3	c d	Two components for two channels in Category 2/3 SRESW homogeneous	No bonus owing to diversity. The basic measures for PL a to b apply, and additional measures for PL c/d. The manufacturer must confirm that all requirements to EN ISO 13849-1 have been observed.

“Diverse SRESW” is stated as a requirement in some places below. The SRESW of two components is considered “diverse” in this context when

- they are different components with different operating systems from two different manufacturers, or
- they are different components from different series/product families from the same manufacturer, who confirms that they differ significantly in their SRESW. Examples for PLCs: the first component is a compact PLC (e.g. 16-bit CPU, proprietary operating system), the second a modular PLC (e.g. 32-bit CPU, embedded Windows). A further example: a PLC and a programmable switching relay.

Should the manufacturer not confirm the diversity, the SRESW of the two components is considered in all other cases (two identical PLCs or two similar PLCs from the same product range from the same manufacturer) to be not diverse, and therefore to be homogeneous. Where necessary for attainment of the required *DC*, the manufacturer must also confirm the *DC* of the fault detection/control measures implemented in the SRESW. The $MTTF_d$ of the components obviously forms part of the information which must be provided by the manufacturer.

Should only one standard component in Category 2 or 3 be used in combination with another technology and where diverse standard components are employed for each channel, the requirements are lowered owing to the low probability of a dangerous failure being caused by systematic faults in the SRESW. Table 6.5 shows the various combinations and the way in which the requirements for SRESW are met.

To summarize, the use of electronic programmable standard components in SRP/CS is assessed as follows with regard to the requirements for the SRESW:

- At the current state of the art, PL e cannot generally be attained by implementtation involving software-based standard components.
- With diversity of the SRESW/diverse technology of two channels, PL c/d can be implemented with reduced requirements upon the SRESW. Although the benefit of diversity is not formulated explicitly in the standard, it is common practice and is also presented in similar terms in the future, second version of IEC 61508.
- PL a/b can be implemented with suitable standard components.

Requirements for SRASW

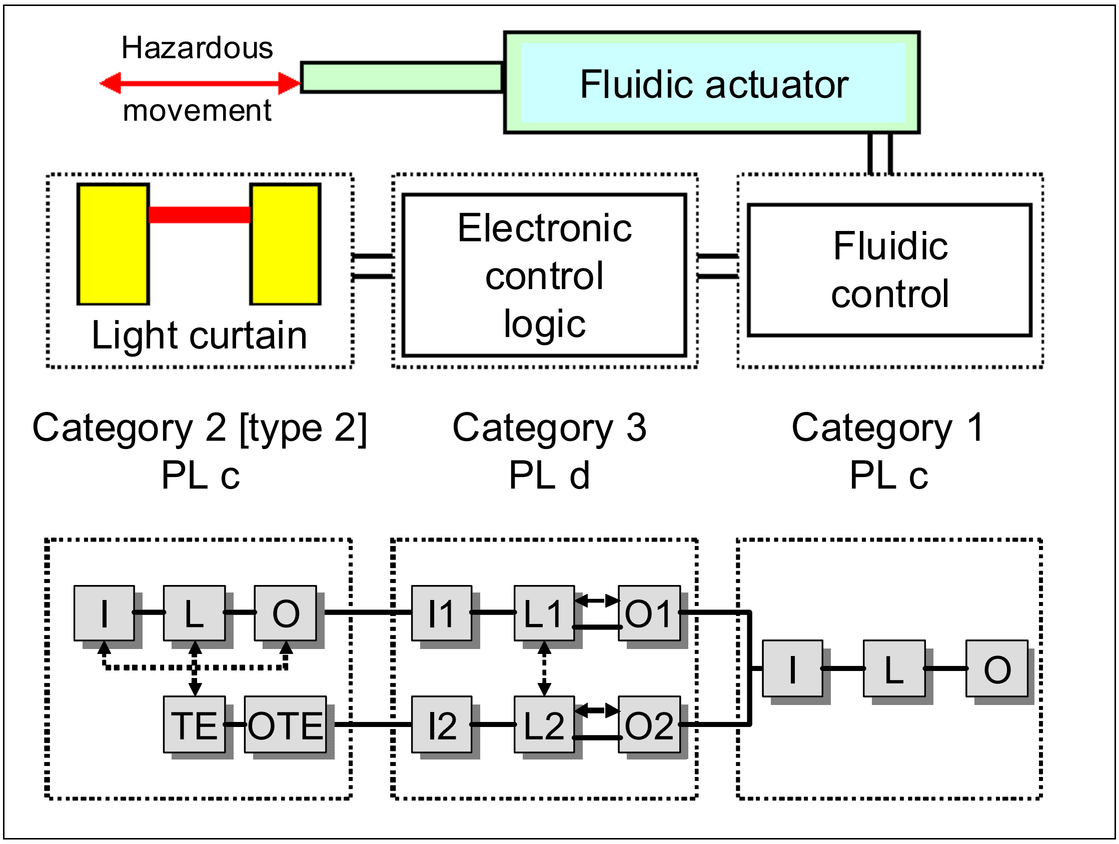
The requirements for SRASW are geared to the PL which must be attained by the subsystem containing the programmable standard component. If a standard component is employed in one channel in diverse redundancy with another technology (e.g. fluid power) in the other channel, the requirements in the PL for SRASW are lowered by one level (e.g. from PL d to PL c) owing to the lower probability of a dangerous failure caused by systematic faults in the SRASW.

6.4 Combination of SRP/CS as subsystems

Up to this point, this chapter has considered an SRP/CS only in the form of a complete control system which can be mapped in its entirety to a Category/designated architecture with a corresponding Performance Level. The safety function is executed exclusively by such a control system, beginning with a triggering event through to attainment of the safe state. In reality, however, it is often necessary for several SRP/CS, each of which executes parts of the safety function, to be arranged in series as subsystems. Such subsystems may employ different technologies and/or implement different Categories/Performance Levels. Frequently, for example, different technologies are employed on the sensor/logic level (e.g. electronics in Category 3) to those on the drive level (e.g. hydraulics in Category 1), or bought-in devices are interlinked, e.g. light curtains, electronic controls and pneumatic valve level as shown in Figure 6.13. One of the major advantages of the PL concept over the Categories is that a method now exists by which subsystems of differing Category but similar Performance Level can be combined to form an overall system of mixed Categories but with a defined overall PL. In practice, different constellations may occur. These will now be discussed in greater detail:

- The entire control system in one Category, no subsystems: for this case, the explanations given above apply, e.g. regarding the designated architectures.
- Control subsystem in one Category: for this case, the above explanations also apply, for example with regard to the designated architectures; the contribution to the safety function and the interfaces to which further subsystems can be connected must however be defined in order for the safety function to be completed (see below).
- Arrangement of subsystems (e.g. of differing Category) in series: a method is described below by which the PL of the overall system can be calculated from the values of the subsystems (PL, average probability of a dangerous failure per hour). Here too, the precise definition of the contribution to the safety function and of the interfaces must be observed.
- Treatment of special cases, such as the arrangement of subsystems in parallel or the use of subsystems in only one channel of an entire control system.

Figure 6.13:
Arrangement of subsystems in series for implementation of a safety function



The arrangement in series of several subsystems, including subsystems differing in their technology, typically takes the form outlined by the example shown in Figure 6.13: the light curtain, electronic control system and pneumatic valve are arranged in series in order for them to execute the safety function (stopping of the hazardous movement in the event of interruption of the light beam) together. The pneumatic cylinder itself is not a control component and is not therefore subject to a PL assessment.

A chain is only ever as strong as its weakest link; this rule also applies to the interlinking of control components both of different Categories and of different Performance Levels. As has often been observed in practice, a Category 1 hydraulic control system may, owing to the high $MTTF_d$ of its components, exhibit safety comparable to that of a Category 3 electronic control system with a medium DC_{avg} and low $MTTF_d$. Since positive and negative correction values for the Category resulting from the $MTTF_d$ and the DC_{avg} are already reflected in the PL, the PL for the combination is geared to the frequency with which the lowest PL occurs in the series arrangement, and not to the lowest individual Category. The overall probability of failure rises with the number of control elements; the PL of the series arrangement may therefore be a level lower than the lowest subsystem PL if, for example, more than three of these elements are arranged in series. The following method in EN ISO 13849-1 can be used to obtain a rough approximation of the overall PL attained based upon the subsystem PL:

- The lowest PL of all subsystems in the series arrangement is first determined. This is PL_{low}.
- The number of instances of PL_{low} in the series arrangement of the subsystems is counted. This is N_{low}.
- The overall PL can then be calculated from PL_{low} and N_{low} according to Table 6.6.

PL_{low}	N_{low}	Overall PL
a	≥ 4	No PL, not permitted
	≤ 3	a
b	≥ 3	
	≤ 2	b
c	≥ 3	
	≤ 2	c
d	≥ 4	
	≤ 3	d
e	≥ 4	
	≤ 3	e

Table 6.6:
Simplified calculation of the PL for series arrangements of subsystems

This simplified method supports the determining of the overall PL when only the PL of the subsystems is known, and not the average probability of a dangerous failure per hour upon which it is based. As an approximation, a value for the probability of failure is assumed for the subsystems which is exactly in the middle of the valid range for the PL_{low} in question. Conversely, should the values be available for the average probability of a dangerous failure per hour for all subsystems (values for SIL and probability of failure to IEC 61508 [12] or IEC 62061 [13] are also suitable), the relevant value for the overall PL can be obtained from them by summation:

$$PFH_{\text{total}} = \sum_{i=1}^{N} PFH_{\text{i}} = PFH_1 + PFH_2 + \ldots + PFH_{\text{N}} \qquad (5)$$

where

N = number of subsystems involved in the safety function

PFH_{i} = average probability of a dangerous failure per hour of the *i*th subsystem

Since all subsystem PLs are always at least as great as the overall PL, it is also ensured that all measures for non-quantifiable, qualitative aspects (e.g. systematic failures or software) are adequately considered in the combination. Particular attention must however be paid here to the interfaces between the subsystems:

- All connections (e.g. conductors or data communication over bus systems) must already be considered in the PL of one of the subsystems involved, or faults in the connections must be excluded or be negligible.

- The safety subsystems arranged in series must be compatible at their interfaces. In other words, each output status of an actuating subsystem which signals the demand upon the safety function must be suitable as a triggering event for initiation of the safe state of the downstream subsystem.

In cascaded two-channel systems, addition of the subsystem PFH values may lead to minor arithmetic errors on the unsafe side. Strictly speaking, the two outputs of the first subsystem should additionally be read crossed over into the inputs of the second subsystem, and compared. Crossed-over doubling of the input information, however, is often already implemented internally at the input level. In order to avoid unnecessarily excessive cabling work, the minor underestimation of the PFH during addition is tolerable.

The rules described up to this point already enable subsystems to be combined much more flexibly than was possible on the basis of Categories prior to the revision of EN ISO 13849-1. These subsystems may differ widely in nature, for example with regard to their technology or Category, and may also be developed against other standards for the safety-related parts of machine controls which are based upon an SIL rather than a PL (cf. Figure 3.2).

Two-channel and (tested) single-channel parts may alternate in linked subsystems. As an example, Figure 6.14 shows a logic subsystem (e.g. a safety PLC) to which two-channel input and output elements are connected.

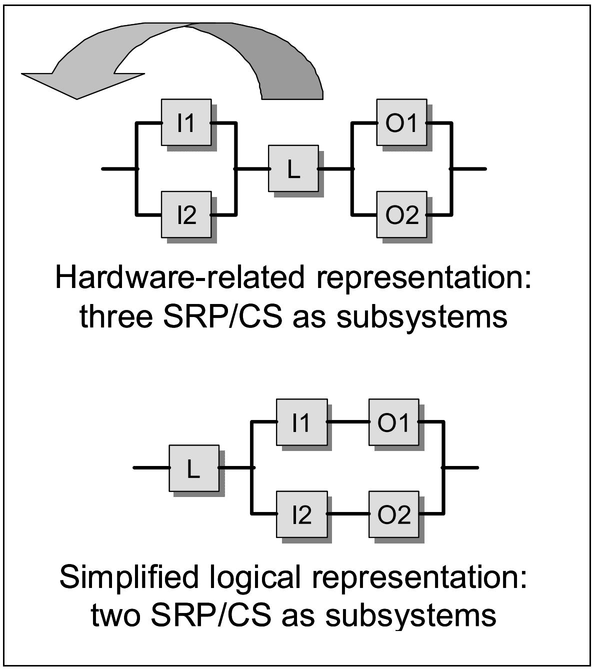

I1
I2
L
O1
O2
Hardware-related representation: three SRP/CS as subsystems
L
I1
O1
I2
O2
Simplified logical representation: two SRP/CS as subsystems

Figure 6.14:
Mixed subsystems can be re-sorted in the safety-related block diagram

Since an abstraction of the hardware level is already performed in the safety-related block diagram, the sequence of the subsystems is in principle interchangeable. It is therefore recommended that subsystems sharing the same structure be grouped together, as shown in Figure 6.14. This makes calculation of the PL simpler, and unnecessary truncation effects, such as multiple capping of the $MTTF_d$ of a channel to 100 years, are avoided.

Special cases nevertheless remain for which only rough rules, if any, can be given at this time. One special case concerns the arrangement of subsystems in parallel. In this case, simple, generally valid rules cannot be formulated either for the quantifiable aspects (e.g. Category 1 twice in parallel still does not equate to Category 3, since it lacks fault detection), or with regard to the qualitative aspects (e.g. systematic failures, software, common cause failure). The only solution is a reassessment of the entire system. It may be possible to exploit the intermediate results in part (e.g. the $MTTF_d$ or *DC* of blocks). A further special case is the integration of subsystems which already possess a PL (or SIL) or an average probability of dangerous failure per hour in the form of a block in an SRP/CS. As an approximate rule and without inspection of the internal structure of the subsystem, the reciprocal of the average probability of a dangerous failure per hour may be employed as the $MTTF_d$ for the block. Since any diagnostics measures of the subsystem which may have been implemented internally have already been considered in the probability of failure, only supplementary diagnostics measures acting externally upon the subsystem may be considered for the *DC* of the block.

A further issue which may arise in this context concerns the assignment of a Category for a complete system which is in turn created from subsystems for which the only available information is the average probability of dangerous failure per hour.

Besides information on the internal structure, information on the $MTTF_d$ of each channel and on the DC_{avg} is lacking in this case, for which minimum requirements apply depending upon the Category. The same principle therefore applies as to parallel arrangements: the only alternative to a very rough estimation is re-evaluation, possibly with exploitation of intermediate results obtained.

6.5 Determining the PL with reference to the example of a paper-cutting guillotine with diverse redundancy in the logic control (Category 4 – PL e)

This section supplements the general description with an illustration of how the PL is determined in practice. At the same time, the example which is described here in detail facilitates the reader's access to Chapter 8, which contains a large number of circuit examples for diverse PLs, Categories and forms of technology.

The text boxes with grey background shown below correspond to the brief descriptions in the form presented in Chapter 8. Additional explanations are also provided; reference to them for each circuit example in Chapter 8 would however be too protracted.

6.5.1 Safety functions

The example control system for a paper-cutting guillotine described in Section 5.7 is taken up again here. Of the seven safety functions stated there, the implementation of SF2 is described as an example, for which the required Performance Level was found to be PL_r e. Since the various safety functions may make use of the same components, all safety functions must be considered during implementation. For example, for safeguarding on the operator side, the product standard governing paper-cutting guillotines, EN 1010-3, requires electro-sensitive protective equipment (ESPE, not shown here) for the safety function SF3, in addition to a two-hand control (THC).

Safety function (SF2):

- Controlled location of the operator's hands outside the hazardous area during a hazardous movement

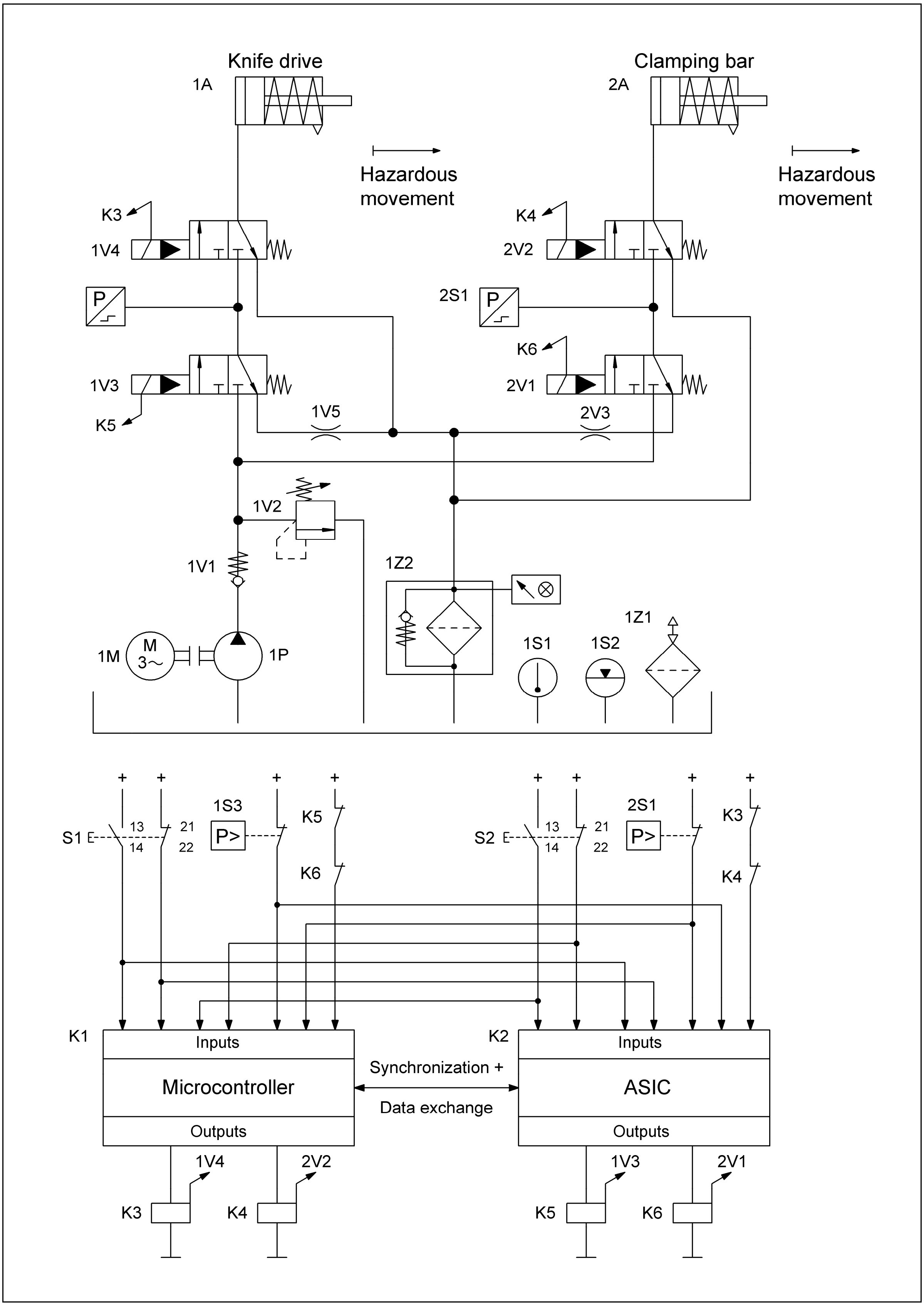
6.5.2 Implementation

Where implementation takes the form of a two-hand control, this safety function can be described as follows: when at least one of the two actuators S1 and S2 is released, the hazardous movement of the clamping bar and knife is interrupted, and both the clamping bar and the knife are returned to their initial positions by spring force. A restart is prevented until both actuators have been released and a new cycle initiated by the two-hand control. Controlled location of the operator's hands is achieved by means of two actuators which must be operated simultaneously for the machine to be started (for details, e.g. concerning immunity to bypassing, see EN 574). The electrical signals must be evaluated with regard to their timing and logic. For this purpose, a programmable electronic control system is a suitable arrangement. Such a system will generally also control the movement of the clamping bar and knife. Owing to the high forces required, these parts are driven hydraulically. As described in Chapter 5 (see Section 5.3.2), the safety function encompasses both actuators – clamping bar and knife – since they are located at the same hazardous zone.

Figure 6.15 represents an electrohydraulic conceptual schematic diagram showing how the safety-related control components are implemented in practice. In the conceptual schematic diagram shown here, as in Chapter 8, many details are of course omitted in the interests of greater clarity. Besides the majority of functional control components required for operation of the machine within the process, certain safety-related details such as protective circuits (fuses, EMC) and “peripherals” (power supply, clock signals etc. for the logic) have also been omitted.

Owing to the required single-fault tolerance and tolerance of an accumulation of undetected faults, decoupling elements are for example also required in practice between the interconnected inputs of the two logic channels, in order for a defective input on one channel not to cause interference on the other channel. It must therefore be appreciated that a conceptual schematic diagram such as this does not constitute documentation from which a replica could be fabricated; its purpose is instead that of illustrating the structure of the safety technology.

Figure 6.15:
Conceptual schematic diagram of the electronic drive of a hydraulic knife drive and a hydraulic clamping bar (essential components)



6.5.3 Functional description

A functional description explaining the circuit structure and signal paths is essential for an understanding of the circuit diagram. It is intended to permit identification of the functional process during execution of the safety function (which may take place in different channels) and the implemented test measures.

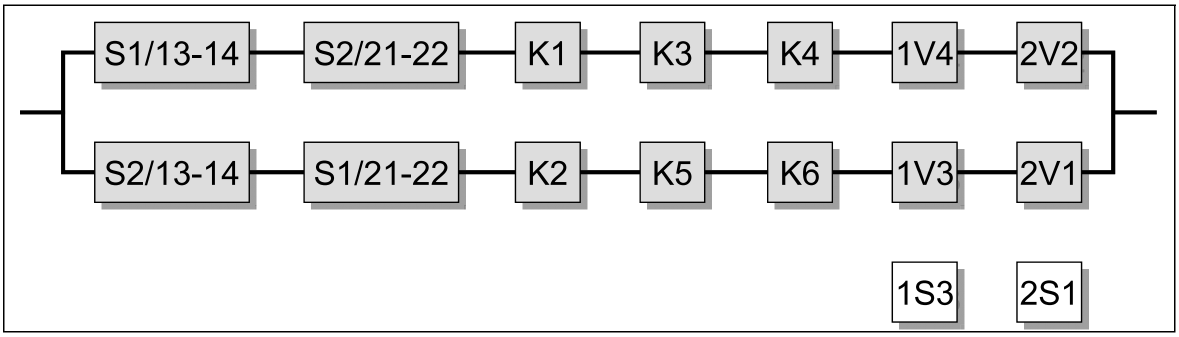
Functional description:

- Operation of the actuators S1 and S2 of the two-hand control initiates the hazardous movements (processing cycle) of the clamping bar and the knife. Should either of the actuators of the two-hand control be released during this cycle or a signal change occur in the peripheral system of the machine which is not expected by the control system, the cycle is halted and the machine assumes the safe state.
- Pressing the actuators S1 and S2 causes the rising edges of the signals to be fed to the two processing channels K1 (microcontroller) and K2 (ASIC). Provided these signals satisfy the requirements for simultaneity in accordance with the relevant standard, EN 574, the two processing channels set the outputs (contactor relays K3 to K6) for a valid cut request.
- The two processing channels act synchronously and also mutually evaluate internal intermediate states of the cyclical signal processing operations. Deviations from defined intermediate states cause the machine to be halted. One processing channel is formed by a microcontroller (K1), the other by an ASIC (K2). K1 and K2 perform background self-tests during operation.
- Faults in the actuators S1/S2 and in contactor relays K3 to K6 (with mechanically linked readback contacts) are detected by cross-checking in the processing channels.
- Failure of the valves 1V3/1V4 and 2V1/2V2 is detected by means of the pressure switches 1S3 and 2S1.
- Failure of the valves or sticking open of 1V4 or 2V2 is detected by a strong reduction in the return speed of the hydraulic cylinders. This situation can also be detected by the control system by suitable evaluation of the pressure signals (duration of pressure drop).
- Failure of the valves or sticking open of 1V3 or 2V1 is detected directly by monitoring of the signal change of the pressure switches 1S3 and 2S1: in the event of valve sticking, a pressure would be signalled although no pressure should be present.
- All machine states are monitored by both processing channels. The cyclical nature of the cut cycle causes all system states to be cycled through, and faults can thus be detected.

6.5.4 Safety-related block diagram

The description of the circuit arrangement in conjunction with the circuit diagram and if appropriate other descriptive documents (comprehensive specification) enables a control category to be determined and the actual circuit to be mapped to an abstracted safety-related block diagram (Figure 6.16). This example soon shows that the safety function is executed in two-channel mode. Category 3 or 4 may therefore be considered. The high-quality test measures, by which combinations of faults can also be controlled, suggest Category 4. Actual verification is obtained in Chapter 7, as is checking of the quantitative requirements for the $MTTF_d$, DC_{avg} and CCF (see below). The explanations provided in Sections 6.2.8 and 6.2.9 are helpful for implementation in the safety-related block diagram. A proven procedure is to trace the signal path, beginning at the actuator side, by asking: “How is the hazardous movement driven/prevented?”, and then to follow the logic through to the sensors. Note in this example that actuators S1 and S2 are not mutually redundant, even though they may initially appear so, since each button independently protects one of the user's hands. Rather, the redundancy begins within each button by the use of electrical make/break contact combinations. Each control channel monitors both hands/actuators by evaluation of at least one electrical switching contact in each actuator. The safety-related block diagram therefore contains a make contact, e.g. S1/13-14, and a break contact, e.g. S2/21-22, in each channel. The safety-related block diagram differs substantially in this respect from the functional circuit diagram.

Figure 6.16:
Safety-related block diagram of the SRP/CS for the selected safety function SF2 on the paper-cutting guillotine



Under certain circumstances, implementation of the safety function in practice may result in restrictions or recommendations for the application. For example, the effectiveness of fault detection by the work process is by definition closely related to the application.

Remark

- Application for example on paper-cutting guillotines (EN 1010-3)

6.5.5 Input variables for quantitative evaluation of the attained PL

All basic information for evaluation of the attained PL is available at this point. With knowledge of the Category and of the safety-related block diagram, the $MTTF_d$ and DC can first be determined for the individual blocks, and the measures against CCF also evaluated for existing redundancies. This is followed by the “mathematical” steps for determining the $MTTF_d$ of each channel, the DC_{avg}, and finally the PL.

Calculation of the probability of failure

- $MTTF_d$: at 240 working days per year, 8 working hours per day and a cycle time of 80 seconds, n_{op} is 86,400 cycles per year. For S1 and S2 and for K3 to K6, a B_{10d} value of 2,000,000 cycles [M] produces an $MTTF_d$ of 232 years. For the microcontroller alone, an $MTTF_d$ of 1,142 years is calculated [D]. The same value is also substituted for the ASIC [D]. Together with the associated circuit arrangement, this results in an $MTTF_d$ of 806 years in each case for the blocks K1 and K2. An $MTTF_d$ of 150 years [S] is assumed for each of the valves 1V3, 1V4, 2V1 and 2V2. These values result in an $MTTF_d$ for each channel of 31.4 years (“high”).

- DC_{avg}: in accordance with EN ISO 13849-1, Annex E, the DC values produced for S1/S2 are: 99% (cross monitoring of input signals without dynamic test with frequent signal change); for K1/K2: 90% (self-test by software and cross monitoring); for K3 to K6: 99% (direct monitoring by mechanically linked contact elements); for 1V3/2V1: 99% (indirect monitoring by the pressure sensor); and for 1V4/2V2: 99% (indirect monitoring by the function and measurement of a change in the duration of the pressure drop). These values yield a DC_{avg} of 98.6% (“high”).

- Adequate measures against common cause failure (65 points): separation (15), over-voltage protection etc. (15) and environmental conditions (25 + 10)

- The combination of control elements corresponds to Category 4 with a high $MTTF_d$ per channel (31.4 years) and a DC_{avg} of 98.6%, within the tolerance range for DC_{avg} “high”. This results in an average probability of dangerous failure of 9.7×10^{-8} per hour. This corresponds to PL e.

In order to elucidate calculation of the $MTTF_d$, block “K1” will first be considered: although the conceptual schematic diagram (Figure 6.15) only shows the microcontroller, this block includes further elements which are necessary for operation in practice (e.g. crystal oscillator). The dangerous failure of all elements which could prevent execution of the safety function in the affected channel must be considered. This generally encompasses all elements in the signal path critical to safety, e.g. for decoupling, readback, EMC protection or protection against overvoltage. These elements are generally necessary in the interests of basic and well-tried safety principles or for attainment of the DC. Figure B.2 (page 293) shows this approach with reference to a further simple example. The parts count method shown in Table 6.7 is suitable for use as a simple tabular method for determining the block $\mathrm{MTTF_d}$ based upon the element $\mathrm{MTTF_d}$. (For comparison, Figure B.3 on page 295 shows the procedure of a failure mode and effects analysis.)

Table 6.7:
Parts count method for the “microcontroller” block K1, based upon failure rates λ taken from the SN 29500 collection of data [36] (stated in FIT, i.e. 10^{-9} per hour)

Component	Failure rate λ [FIT] to SN 29500	Number	Total failure rate λ [FIT]	Total dangerous failure rate λ_d [FIT]	$MTTF_d$ in years as the reciprocal of the total rate λ_d
Resistor, metal film	0.2	7	1.4	0.7	163,079
Capacitor, no power	1	4	4	2	57,078
Diode, general purpose	1	3	3	1.5	76,104
Optocoupler with bipolar output	15	2	30	15	7,610
Microcontroller	200	1	200	100	1,142
Crystal oscillator	15	1	15	7.5	15,221
Transistor, low-power bipolar	20	1	20	10	11,416
Plastic-sealed relay	10	1	10	5	22,831
Total for the “microcontroller” block K1				141.7 FIT	806 years

The failure rates stated in the second column for the elements were determined by means of the SN 29500 **d**atabase [35], as is indicated by the code [D] under “calculation of the probability of failure” (see Chapter 8). Validation is described in greater detail in the continuation of this example in Section 7.6. Since identical elements may occur more than once (third column), the total failure rate for each element type is calculated and indicated in the fourth column. The global approximation that only half of the failures are dangerous yields the halved value in column 5. Finally, simple summation produces the total rate of dangerous failures for block K1. Column 6 shows the associated $\mathrm{MTTF_d}$ values in years, derived as the reciprocals of the dangerous failure rates (in column 5, following conversion from hours to years). Following rounding, this value is 806 years for block K1. Since the database employed states identical failure rates for the microcontroller and the ASIC and the circuitry is similar, the $\mathrm{MTTF_d}$ value of 806 years also applies to block K2.

Manufacturers' data (“[M]”) are used for blocks S1/S2 and K3 to K6. Since reliability data are available only for S1/S2 overall (operating mechanism **and** break and make contact), these values can be used as an estimation erring on the safe side for each of the channels, even though only either the make contacts (e.g. S1/13-14) **or** the break contacts (e.g. S2/21-22) are considered in each channel beside the operating mechanism. The assumed B_{10d} values are converted to $MTTF_d$ values by means of the formulae familiar from Annex D:

$$n_{op} = \frac{d_{op} \text{ x } h_{op}}{t_{cycle}} \text{ x } 3{,}600 \frac{s}{h} = \frac{240 \text{ days/year x } 8 \text{ h/day}}{80 \text{ s/cycle}} \text{ x } 3{,}600 \frac{s}{h} = 86{,}400 \frac{\text{cycles}}{\text{year}} \qquad (6)$$

$$MTTF_d = \frac{B_{10d}}{0.1 \text{ x } n_{op}} = \frac{2{,}000{,}000 \text{ cycles}}{0.1 \text{ x } 86{,}400 \text{ cycles/year}} = 231.5 \text{ years} \qquad (7)$$

The operating time of electromechanical components is limited to the T_{10d} value (mean time at which 10% of the components under analysis fail dangerously). Since in this case, however, the T_{10d} value is greater than the assumed mission time of 20 years, it is not relevant for further analysis.

$$T_{10d} = \frac{B_{10d}}{n_{op}} = \frac{2{,}000{,}000 \text{ cycles}}{86{,}400 \text{ cycles}} = 23.15 \text{ years} \qquad (8)$$

The $MTTF_d$ values for the valves 1V3, 1V4, 2V1 and 2V2 can be derived by means of the good engineering practice method described in the **s**tandard itself ("[S]"), provided the conditions stated there are met.

In accordance with Section 6.2.13, the total for one channel (S1, S2, K1, K3, K4, 1V4, 2V2) yields an $MTTF_d$ of 31.4 years, i.e. "high":

$$\frac{1}{MTTF_d} = \frac{1}{232 \text{ years}} + \frac{1}{232 \text{ years}} + \frac{1}{806 \text{ years}} + \frac{1}{232 \text{ years}} + \frac{1}{232 \text{ years}} + \frac{1}{150 \text{ years}} + \frac{1}{150 \text{ years}}$$
$$= \frac{1}{31.4 \text{ years}} \qquad (9)$$

Since the second channel exhibits the same $MTTF_d$, the usual symmetrization is superfluous.

Validation of the assumed DC values is also described in greater detail in Chapter 7. High-quality self-tests, for example, are performed for K1 and K2 by software and cross-checks, including the special measures for variant and invariant memory and the processor unit which are required for microprocessor systems. Altogether, a DC_{avg} of 98.6% is produced for the SRP/CS according to Section 6.2.14. With exploitation of the 5% tolerance, this value is in the "high" range:

$$DC_{\text{avg}} = \frac{2\times\left(\frac{99\%}{232\ \text{years}}+\frac{99\%}{232\ \text{years}}+\frac{90\%}{806\ \text{years}}+\frac{99\%}{232\ \text{years}}+\frac{99\%}{232\ \text{years}}+\frac{99\%}{150\ \text{years}}+\frac{99\%}{150\ \text{years}}\right)}{2\times\left(\frac{1}{232\ \text{years}}+\frac{1}{232\ \text{years}}+\frac{1}{806\ \text{years}}+\frac{1}{232\ \text{years}}+\frac{1}{232\ \text{years}}+\frac{1}{150\ \text{years}}+\frac{1}{150\ \text{years}}\right)} = 98.6\% \quad (10)$$

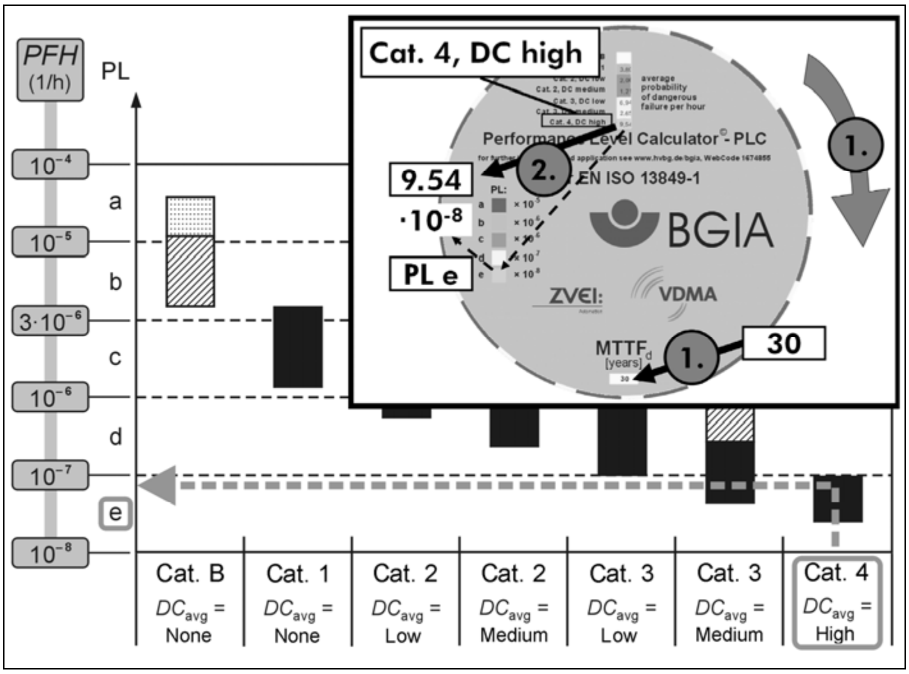
The four measures against common cause failure (CCF) stated above (see grey box on page 108 are largely self-explanatory. Validation is nonetheless explained in greater detail in Chapter 7. In addition, the “diversity” measure and the “use of well-tried components” measure take effect in the electrical and hydraulic subsystems respectively, see Annex F. With satisfaction of the requirements for CCF, DC_{avg} “high” and $MTTF_{\text{d}}$ “high”, the quantitative requirements for Category 4 are also met.

6.5.6 Several approaches for quantitative calculation of the PL

At this point, little is still required for determining of the PL on the basis of quantifiable aspects. The results for the Category, DC_{avg} and $MTTF_{\text{d}}$ can be used for graphical confirmation by means of the bar chart that PL e is attained (see Figure 6.17). The tabular values in Annex K of the standard or the BGIA's PLC disk [16] based upon them yield the following result:

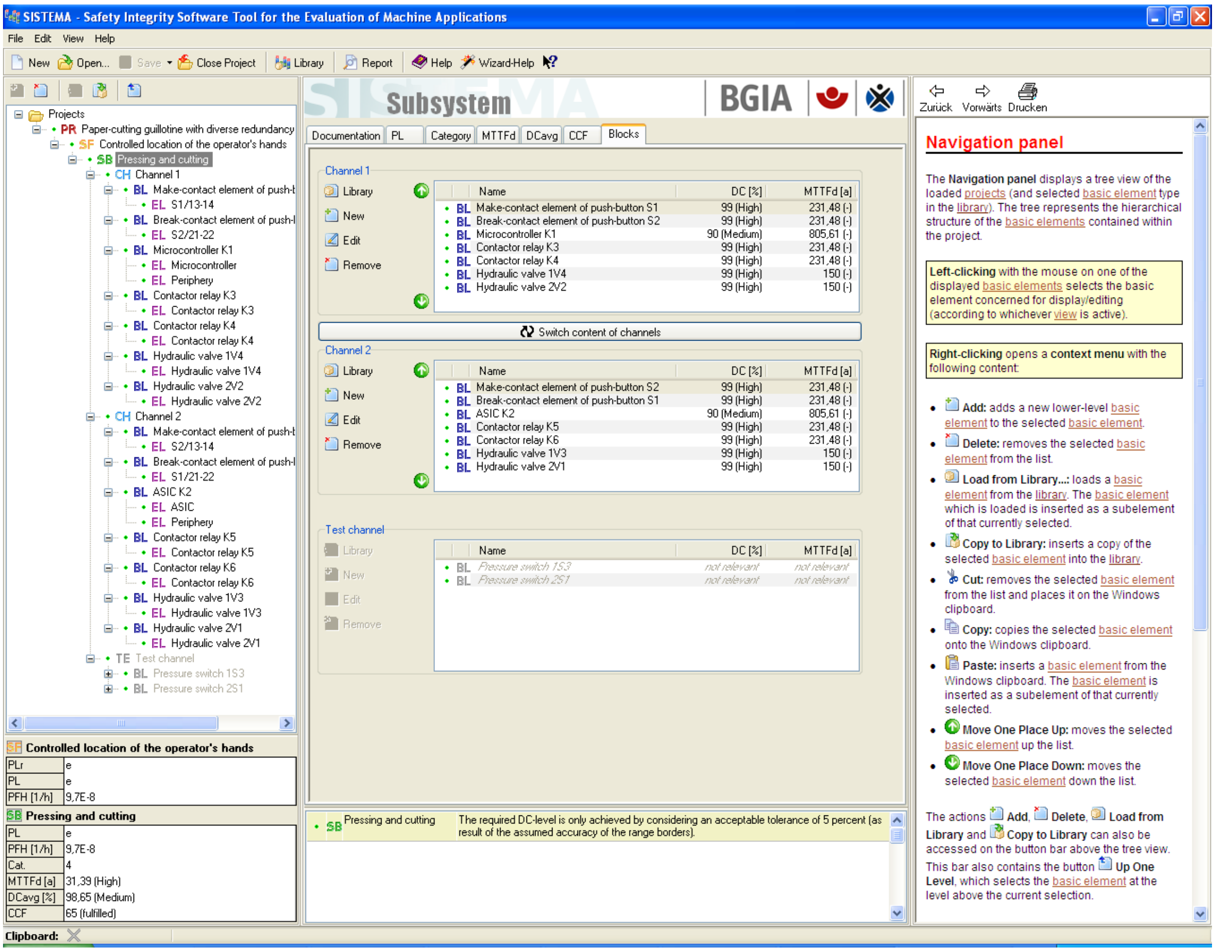
Category	CCF	DC_{avg}	$MTTF_{\text{d}}$	Average probability of a dangerous failure per hour
4	OK	“High”	“High” (rounded: 30 years)	9.54×10^{-8} per hour (PL e)

Figure 6.17:
Determining of the PL by means of the bar chart



The SISTEMA software, available free of charge from the BGIA (see Annex H), is much more convenient for the administration, documentation and calculation of all intermediate results. All quantitative requirements for determining of the PL which have been described thus far can be handled easily with this software, and all calculations including mathematical determining of the PL are automated. Use of the exact $\mathrm{DC}_{\mathrm{avg}}$ and MTTF_d values for calculation is possible as a special option. For DC_{avg}, the more exact (in this case poorer) value of 98.6% is employed for calculation rather than exploitation of the 5% tolerance for DC_{avg} “high” and substitution of a rounded 99% (for the tolerances for DC and $MTTF_\mathrm{d}$, cf. Note 2 in Tables 5 and 6 of the standard). Dropping below the 99% mark for Category 4, still within the tolerance range, triggers a warning message by SISTEMA, however. Conversely, use of the exact MTTF_d value of 31.4 years for calculation yields a slight improvement compared to the rounded value of 30 years for $MTTF_\mathrm{d}$ “high”. The resulting mean probability of a dangerous failure per hour is 9.7 × 10^{-8} per hour (see Figure 6.18), which differs only slightly from the value calculated above.

Figure 6.18:
Determining of the PL by means of SISTEMA


SISTEMA - Safety Integrity Software Tool for the Evaluation of Machine Applications
File Edit View Help
New Open... Save Close Project Library Report Help Wizard-Help
Subsystem
BGIA
Documentation PL Category MTTFd DCavg CCF Blocks
Zurück Vorwärts Drucken
Library
New
Edit
Remove
Switch content of channels
Clipboard:

- Projects
  - PR Paper-cutting guillotine with diverse redundancy
    - SF Controlled location of the operator's hands
      - SB Pressing and cutting
        - CH Channel 1
          - BL Make-contact element of push-b
            - EL S1/13-14
          - BL Break-contact element of push-b
            - EL S2/21-22
          - BL Microcontroller K1
            - EL Microcontroller
            - EL Periphery
          - BL Contactor relay K3
            - EL Contactor relay K3
          - BL Contactor relay K4
            - EL Contactor relay K4
          - BL Hydraulic valve 1V4
            - EL Hydraulic valve 1V4
          - BL Hydraulic valve 2V2
            - EL Hydraulic valve 2V2
        - CH Channel 2
          - BL Make-contact element of push-b
            - EL S2/13-14
          - BL Break-contact element of push-b
            - EL S1/21-22
          - BL ASIC K2
            - EL ASIC
            - EL Periphery
          - BL Contactor relay K5
            - EL Contactor relay K5
          - BL Contactor relay K6
            - EL Contactor relay K6
          - BL Hydraulic valve 1V3
            - EL Hydraulic valve 1V3
          - BL Hydraulic valve 2V1
            - EL Hydraulic valve 2V1
        - TE Test channel
          - BL Pressure switch 1S3
          - BL Pressure switch 2S1

SF Controlled location of the operator's hands

PLr	e
PL	e
PFH [1/h]	9,7E-8

SB Pressing and cutting

PL	e
PFH [1/h]	9,7E-8
Cat.	4
MTTFd [a]	31,39 (High)
DCavg [%]	98,65 (Medium)
CCF	65 (fulfilled)

Channel 1

	Name	DC [%]	MTTFd [a]
BL	Make-contact element of push-button S1	99 (High)	231,48 (-)
BL	Break-contact element of push-button S2	99 (High)	231,48 (-)
BL	Microcontroller K1	90 (Medium)	805,61 (-)
BL	Contactor relay K3	99 (High)	231,48 (-)
BL	Contactor relay K4	99 (High)	231,48 (-)
BL	Hydraulic valve 1V4	99 (High)	150 (-)
BL	Hydraulic valve 2V2	99 (High)	150 (-)

Channel 2

	Name	DC [%]	MTTFd [a]
BL	Make-contact element of push-button S2	99 (High)	231,48 (-)
BL	Break-contact element of push-button S1	99 (High)	231,48 (-)
BL	ASIC K2	90 (Medium)	805,61 (-)
BL	Contactor relay K5	99 (High)	231,48 (-)
BL	Contactor relay K6	99 (High)	231,48 (-)
BL	Hydraulic valve 1V3	99 (High)	150 (-)
BL	Hydraulic valve 2V1	99 (High)	150 (-)

Test channel

	Name	DC [%]	MTTFd [a]
BL	*Pressure switch 1S3*	*not relevant*	*not relevant*
BL	*Pressure switch 2S1*	*not relevant*	*not relevant*

SB Pressing and cutting — The required DC-level is only achieved by considering an acceptable tolerance of 5 percent (as result of the assumed accuracy of the range borders).

Navigation panel

The **Navigation panel** displays a tree view of the loaded projects (and selected basic element type in the library). The tree represents the hierarchical structure of the basic elements contained within the project.

Left-clicking with the mouse on one of the displayed basic elements selects the basic element concerned for display/editing (according to whichever view is active).

Right-clicking opens a **context menu** with the following content:

- **Add:** adds a new lower-level basic element to the selected basic element.
- **Delete:** removes the selected basic element from the list.
- **Load from Library...:** loads a basic element from the library. The basic element which is loaded is inserted as a subelement of that currently selected.
- **Copy to Library:** inserts a copy of the selected basic element into the library.
- **Cut:** removes the selected basic element from the list and places it on the Windows clipboard.
- **Copy:** copies the selected basic element onto the Windows clipboard.
- **Paste:** inserts a basic element from the Windows clipboard. The basic element is inserted as a subelement of that currently selected.
- **Move One Place Up:** moves the selected basic element up the list.
- **Move One Place Down:** moves the selected basic element down the list.

The actions **Add**, **Delete**, **Load from Library** and **Copy to Library** can also be accessed on the button bar above the tree view. This bar also contains the button **Up One Level**, which selects the basic element at the level above the current selection.

This is now followed by evaluation of the non-quantifiable qualitative aspects for determining the PL, firstly for systematic failures.

6.5.7 Systematic failures

With its diversity-oriented approach for the logic control, the selected design of the control system employs a highly effective measure against the influence of systematic failures. Further measures are of course required in the course of implementation, for example in order to control the effects of a voltage breakdown, fluctuations in voltage, overvoltage and undervoltage. Some of the necessary measures are already evident in the selected design. These include:

- Use of the closed-circuit current principle: this ensures that the de-energized state cannot give rise to an actuation signal (e.g. in the event of wire breakage).
- Failure recognition by automatic tests: in this case tests, which differ between the two channels, are performed which are capable of detecting faults at an early stage and of initiating the safe state independently of the adjacent channel.
- Testing by redundant hardware: the diversity by design assists, in addition, in the control of faults caused by environmental influences which act in different ways upon the different channels.
- The use of contactor relays with mechanically linked contacts: status detection of relevant contacts enables dangerous failures of the contactor relays and in some cases of other circuit components to be detected.
- Monitoring of the program sequence: the ASIC for example is used to monitor the program sequence of the microcontroller channel.

The reader's attention is drawn in particular to two details concerning systematic failures, the first of which concerns the application, the second the design process:

- During design of the hydraulic system for paper-cutting guillotines, consideration must be given to the incidence of paper dust. Contamination of hydraulic fluid with paper dust for example may jeopardize the safe function of a paper-cutting guillotine. For this reason, particular attention must be paid to effective filtration of the pressure medium. In addition, the ingress of paper dust into the hydraulic system from outside must be prevented, for example by wiper rings on cylinder rods and by tank vent filters.
- Fault-avoidance measures during development of the ASIC in accordance with the ASIC development life cycle of the IEC 61508-2:2005 (CD) draft standard. This draft standard makes provision for a V model for the development of an ASIC, following the V model familiar from software development.

6.5.8 Ergonomic aspects

In this example, a safety-related interface exists between the user and the control system: the two-hand control (THC) device, with actuators S1 and S2. Certain ergonomic aspects must be considered here in order to prevent any person from being endangered, either directly or over time as a result of strain, during the intended use and reasonably foreseeable misuse of the machine. For the majority of machines, these user interfaces can be checked by means of BG Information 5048, “Ergonomische Maschinengestaltung” (ergonomic machine design), Parts 1 and 2 [23]. Aspects to be observed in this context include the following:

- Height and orientation of the actuators in relation to the operator
- Legroom and area of reach during operation, normally in a standing position
- Arrangement matched to the operating task and good accessibility outside the hazardous area
- Ease of observation of the cutting process from the location of the THC
- Minimum dimensions and geometry of the actuators (ergonomic design in consideration of the requirements of EN 574)
- Easy operation with low forces, but with design measures for the prevention of unintended operation
- Robust design of the buttons, and suitable marking and colouring
- THC designed to prevent tampering and thus bypassing of the controlled location of the operator's hands

6.5.9 Requirements concerning the software, specifically SRESW

The following description is of a model implementation of safety-related firmware for the microcontroller K1. The software is embedded software (SRESW) for which the PL_r is e. Owing to the diversity-oriented approach of the logic control – the second channel takes the form of an ASIC – the requirements in accordance with the comment in Section 4.6.2 of the standard can be scaled down: *“When using diversity in specification, design and coding, for the two channels used in SRP/CS with category 3 or 4, PL_r e can be achieved with the above-mentioned measures for PL_r of c or d.”*

The development process for the firmware is based upon the V model in Figure 6.11, and is embedded in the manufacturer's certified quality management system. Based upon the specification for the safety-related control system as a whole, the specifications for the software safety requirements for the firmware (performance specification) are first written. This document describes the contribution made by the firmware to the safety functions of the machine, the required response times with regard to K1, responses to detected faults, interfaces to other subsystems, dependencies upon operating modes, etc. In addition, all fault-avoidance measures required under Section 6.3.2 of the standard for PL c or d are defined. The specification is then reviewed, for example by the safety project manager, and amendments made if appropriate. Once the specification has been approved, system design can commence.

Software architecture: an operating system is not assigned to the microcontroller; instead, a number of tasks are defined which, controlled by simple task management, are executed by timer interrupt at defined intervals. Some low-priority tasks are reserved for the standard functions of the paper-cutting guillotine, whilst the high-priority tasks are executed by the safety-related functions specified above. The determinacy of these task calls is necessary for the required high synchronicity of the two channels and the short response times. The cyclical self-tests for the control of random hardware failures are executed during task idle times.

The design of the software architecture and of the software modules and functions required for implementation of the software described above are summarized in a further document, the requirements specification for the system and module design. For fault avoidance over the entire life cycle, suitable modularization and in this case also a clear separation of the SRESW from the non-safety-related software are particularly important. Where necessary for the sake of clarity, the structure and flow of the software are shown by diagrams. Further requirements are laid down concerning the programming language to be used, in this case ANSI C with compiler-specific language extensions, and the development tools, e.g. compiler, version management, configuration management; all have been used successfully for many years. The programming guidelines and methods are also specified for tools-based static analysis for verification of coding. Planning of module and integration testing is also set out in this document. Following a further review, for example by the software development manager, the requirements specification is approved as a specification for coding. This review also verifies whether the requirements of the software specification are met.

Coding proper now begins, in compliance with the programming guidelines. Besides rules for better code legibility, the provisions of the programming guidelines specify such things as constraints upon the use of critical language constructs. Observance of the programming guidelines during coding is assured in-process by the use of suitable tools. For semantic verification (of the content) of the finished code against the requirements specification, the programmer conducts a walk-through with colleagues in which the program sequence and the data flow of critical signals are analysed at the same time.

The usual module tests are performed to check the functions and interfaces, firstly for correctness and secondly for compliance with the module design. This is followed by integration of the software and tests with the hardware of the microcontroller K1. K1 is then connected to the ASIC channel K2 in order to test synchronization, data exchange and fault detection of the two channels in combination. All tests are documented.

This integration test may reveal that the microcontroller's performance is not as good as previously assumed. Should this be the case, the software architecture, specifically the chronological planning of the tasks and the assignment of functions to them, must be modified. This would not result in changes to the specification of the software safety requirements; the system and module design, however, would have to be adapted and subjected once again to review in order to assure compliance with the specification. This is one example of how technical changes which become necessary during development may result in the V model being repeated in order for the modifications to be implemented in accordance with the QA requirements. The code for such modifications would be written and both the module and the integration tests would have to be repeated.

To cater for the event of the firmware having to be modified after the first production batch has already been delivered, suitable measures such as an impact analysis of the modifications and appropriate development activities in accordance with the V model should be defined within the organization of development itself.

6.5.10 SRP/CS in combination

Since the entire SRP/CS is structured from beginning to end in a single Category and no subsystems are combined, corresponding analysis in accordance with Section 6.4 is not required. It is obvious nevertheless that the various components and technologies must be compatible at their interfaces. Validation aspects regarding integration are addressed in Chapter 7.

6.5.11 Further details

Even in this detailed circuit example, many safety-related design aspects can only be touched upon. A bibliography is therefore provided here, as in the majority of the circuit examples which follow, of useful literature containing further explanations and referring to additional requirements.

More detailed references

- EN 1010-3: Safety of machinery – Safety requirements for the design and construction of printing and paper converting machines – Part 3: Cutting machines (07.02)
- IEC 61508-2:2005 (CD): Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 2: Requirements for electrical/electronic/programmable electronic safety-related systems (IEC 65A/468A/CD:2005)
- EN 574: Safety of machinery – Two-hand control devices – Functional aspects; principles for design (11.96)

Further details, in particular concerning verification and validation, follow in Chapter 7 in the continuation of this example of a paper-cutting guillotine.

7 Verification and validation

Verification and validation refer to quality assurance measures for the avoidance of faults during the design and implementation of safety-related parts of control systems (SRP/CS) which perform safety functions. Part 2 of EN ISO 13849 [7] in particular deals comprehensively with the subject.

Verification encompasses analyses and tests of SRP/CS and their sub-aspects which have the purpose of determining whether the results attained by a development phase satisfy the requirements for the phase concerned, i.e. whether for example the circuit layout corresponds to the circuit design.

Validation refers to demonstration, during or at the end of the development process, of whether the suitability is assured with regard to the actual intended purpose. In other words, the safety-related part of the machine control is examined with regard to whether it meets the specified safety requirements.

The process of assessment of a safety function in its implementation by an SRP/CS is therefore a combination of verification and validation steps which deal with both the SRP/CS as a whole, and specific aspects of it. The terms verification and validation are also described below as V&V activities.

7.1 Procedure

Figure 7.1 shows the relevant section of Figure 4.1 which deals with the activities of verification and validation.

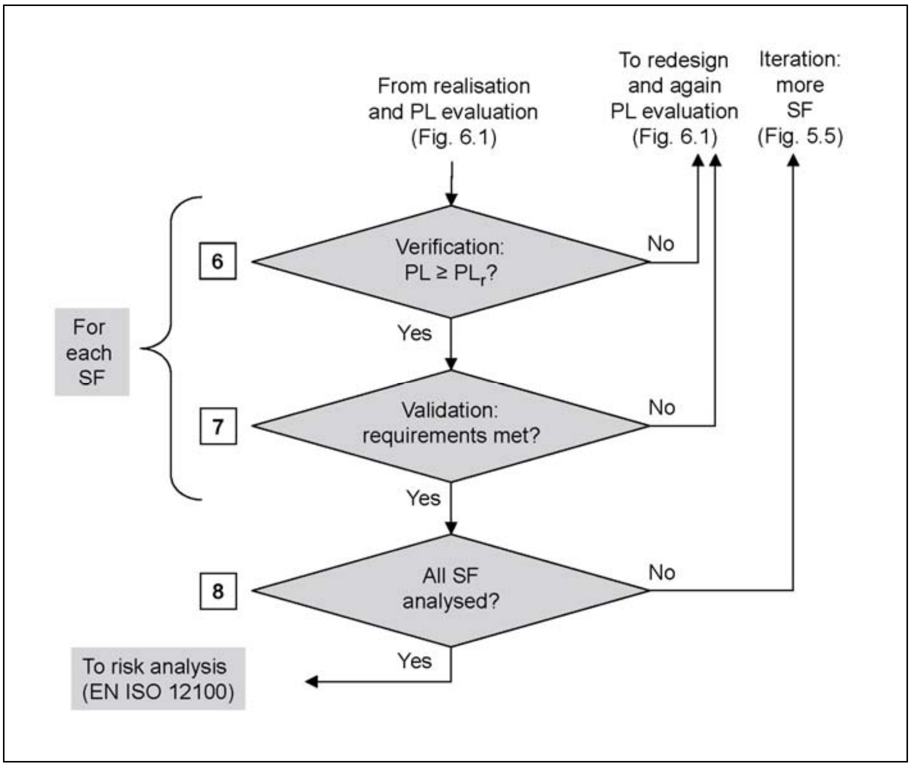
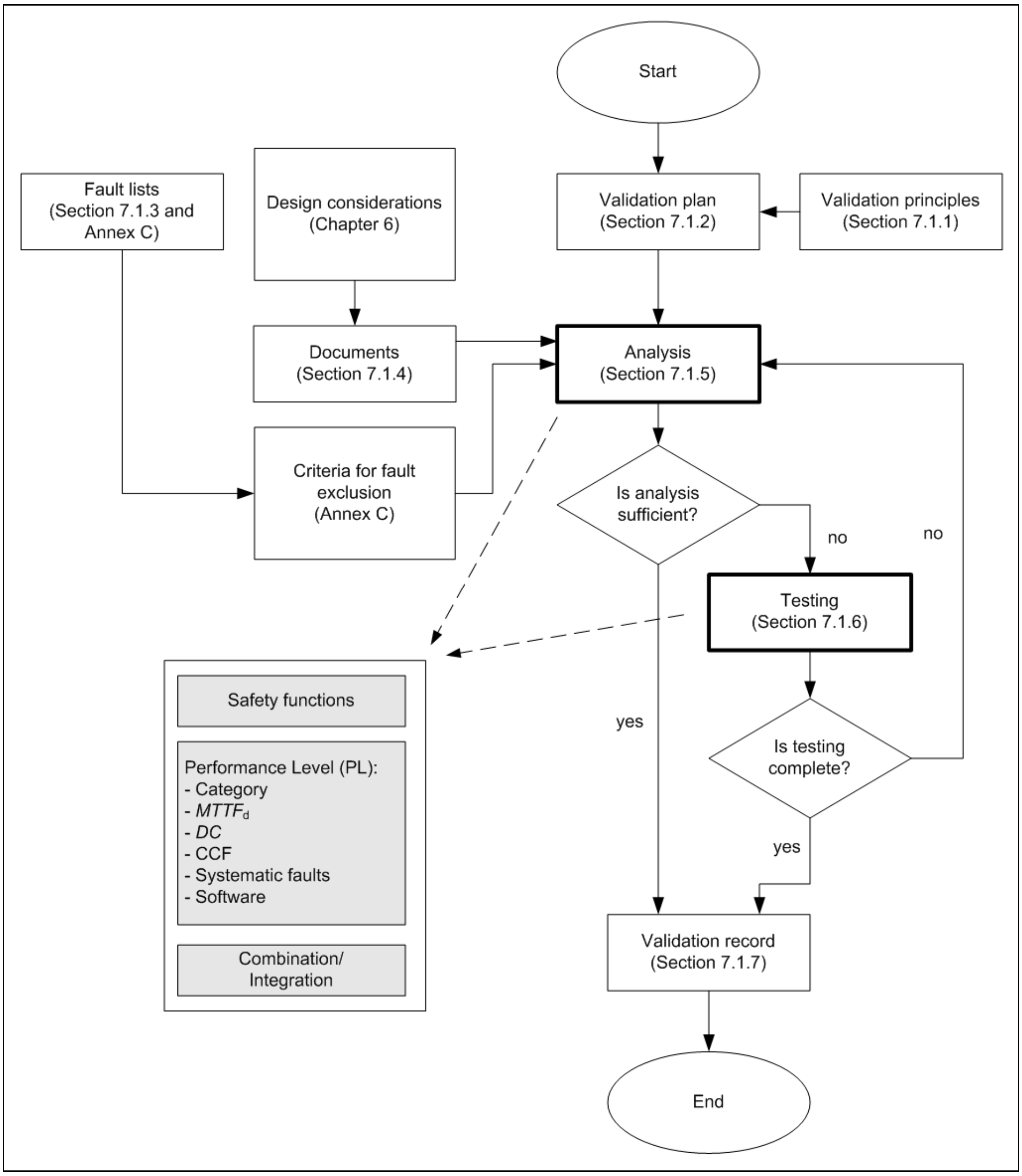

From realisation and PL evaluation (Fig. 6.1)
To redesign and again PL evaluation (Fig. 6.1)
Iteration: more SF (Fig. 5.5)
For each SF
6
Verification: PL ≥ PL$_r$?
No
Yes
7
Validation: requirements met?
No
Yes
8
All SF analysed?
No
Yes
To risk analysis (EN ISO 12100)

Figure 7.1: V&V activities; excerpt from Figure 4.1

An important first test step is performed at the top rhombus (Block 6): if the Performance Level (PL) of each implemented safety function does not correspond at least to the required Performance Level PL_r determined in accordance with Section 5, the design and implementation phase must be returned to. Conversely, if this requirement is met, the procedure continues with the second rhombus (Block 7).

The procedure shown in Figure 7.2 can be employed for planning of the steps required for this purpose. Figure 7.2 is taken from Part 2 of EN ISO 13849, published in 2003, and has been modified graphically here for clearer illustration of the V&V activities.

Figure 7.2:
Overview of the verification and validation procedure to EN ISO 13849-2


Start
Fault lists (Section 7.1.3 and Annex C)
Design considerations (Chapter 6)
Validation plan (Section 7.1.2)
Validation principles (Section 7.1.1)
Documents (Section 7.1.4)
Analysis (Section 7.1.5)
Criteria for fault exclusion (Annex C)
Is analysis sufficient?
no
no
Testing (Section 7.1.6)
Safety functions
Performance Level (PL):
- Category
- MTTF_d
- DC
- CCF
- Systematic faults
- Software
Combination/ Integration
yes
Is testing complete?
yes
Validation record (Section 7.1.7)
End

The most important aspects of the verification and validation procedure are explained briefly below.

7.1.1 Principles for verification and validation

Verification and validation are intended to assure conformity of the design of the SRP/CS with the Machinery Directive. Since EN ISO 13849-1 is listed as a safety standard for machine controls pursuant to the Machinery Directive, the V&V activities must show that each safety-related part and each of the safety functions which it implements satisfies the requirements of EN ISO 13849-1, if presumption of conformity is claimed. These activities should be begun as early as possible during development, in order for faults to be detected and eliminated in time. If possible, the tests should be performed by persons not involved in the process of designing the safety-related parts, i.e. who are independent of the design and development process. The parties concerned may be other persons, departments or bodies who/which are not subordinate to the design department within the organization's hierarchy. The level of independence should be commensurate with the risk, i.e. the required Performance Level PL_r.

Verification and validation can be performed by analysis alone or by a combination of analysis and testing.

7.1.2 Verification and validation plan

All planned activities must be set out in a binding manner in a verification and validation plan (V&V plan). The plan must contain the following information:

- Identification of the SRP/CS products to be tested
- Identification of the safety functions with their assignment to the SRP/CS involved
- Reference to documents with requirements/specifications (e.g. SRS/safety requirements specification)
- Test principles (standards) and internal company requirements (e.g. company standards, design rules and programming guidelines) to be applied
- Analyses and tests (methods) to be performed, including identification of the dedicated test specification document
- Fault lists to be employed
- Further reference documents (e.g. QM manual, QA procedures)
- Personnel responsible for the analyses and tests (testers, department or body)
- Specified apparatus and tools (may also be listed in the results documentation)
- Specified results documentation (test reports/records to be generated)
- Definition of criteria for the passing or failure of tests, including the measures which are to be taken in the event of failure of a test

- Formal aspects such as release notes, tester's signature, etc.
- New V&V activities required in the event of modifications to the product

7.1.3 Fault lists

The test procedure must address the failure mode behaviour of the SRP/CS. The principles for the consideration of faults can be found in the annexes of EN ISO 13849-2 (see also Annex C of this report). The fault lists are based upon many years' experience.

The fault lists and fault exclusions to be employed must be fully referenced. Depending upon the product and the technology used, the manufacturer should add his own fault lists and fault exclusions in the same way. This particularly applies to parts and assemblies which are not contained in the fault lists of EN ISO 13849-2. All fault exclusions must be supported by adequate reasoning.

7.1.4 Documents

As shown in Figure 7.2, detailed documentation is required for V&V activities. These documents have been generated in the course of development, and may differ according to the technology employed. The following content in summarized form should be adequately considered:

- Specification of all requirements upon the safety functions and of the requirements upon SRP/CS which are to execute them, performance criteria, listing of all implemented operating modes, comprehensive descriptions of functions, descriptions of processes
- Operating and environmental conditions of the standards to be applied, together with corresponding intensities (rating data), applicable for the intended applications
- Design description of the SRP/CS (with specifics of the mechanical, electrical, electronic, hydraulic and pneumatic components employed), wiring plans and descriptions of connections and interfaces, circuit diagrams, assembly diagrams, technical data and rating data for components; data sheets if applicable
- Analysis of all relevant faults, e.g. in the form of an FMEA (failure mode and effects analysis), with reference to the fault lists used
- Data for determining the PL (quantification documentation)
- Complete software documentation (see Section 6.3)
- Quality assurance rules followed for design and implementation, such as design rules for analogue and digital circuits, programming guidelines
- Test certificates of components, modules or SRP/CS which have already been tested

The documents must be complete, their content free of contradictions, logically structured, easily comprehensible and verifiable.

The following descriptions of the V&V activities contain detailed information concerning all documents.

7.1.5 Analysis

The SRP/CS and sub-aspects of it are evaluated in the first instance by analysis. The purpose of the analysis is to determine, by inspection of documents and if appropriate by the use of analysis tools, such as circuit simulators, tools for static and dynamic software analysis or FMEA tools, whether the specified requirements have been met. The aspects $MTTF_d$, *DC* and CCF are evaluated solely by analysis based upon the available documents.

7.1.6 Tests

Wherever evaluation by analysis alone is not adequate, tests must be performed in order to show that the requirements are met. Testing must be planned systematically and executed logically, generally against development stages which can actually be executed, such as prototypes, functional models or software/code. The tests must be performed on a configuration which is as close as possible to the intended operating configuration. The environmental conditions under which the tests are to be performed must be defined in advance. The tests may be performed either manually or automatically.

The measurement uncertainty at validation by testing must be reasonable. EN ISO 13849-2 provides information on the limits which are to be observed.

All analysis and test activities must be accompanied by a review of all documents relevant to the phase. Should the results of any tests be negative, procedures and measures are required by which the results can be dealt with appropriately in the development of the SRP/CS.

7.1.7 Documentation of the V&V activities

All analysis and test activities must be documented together with their results (pass or fail).

The following sections describe the steps for validation of the safety functions, both of the SRP/CS, and of sub-aspects such as the PL, Category, $MTTF_d$, *DC* and CCF.

If the requirements set out in the specification of the SRP/CS are not met in full, one must return to the adequate phase of the design and implementation process at this stage. Otherwise, the V&V activities in the third rhombus (Block 8) of Figure 7.1 must be concluded with evaluation of whether all safety functions have been analysed. If this is the case, evaluation of the SRP/CS to EN ISO 13849-1 is complete; if not, the test must be continued with the safety functions which are still open.

7.2 Validation of the safety functions

An important step is validation of the implemented safety function for its full compliance with the characteristics and performance criteria required by the specification. The following questions are intended to assist the tester in assessing whether the safety function has been properly implemented:

- Has the safety function been defined properly and completely?
- Has the correct safety function been implemented?
- Are the provisions for the safety function appropriate to the design?
- Have all necessary operating modes been considered?
- Have the operating characteristics of the machine been considered (including reasonably foreseeable misuse)?
- Have actions in response to emergencies been considered?
- Are all safety-related input signals processed properly and with correct logic to safety-oriented output signals?
- Have the results of the risk assessment for each specific hazard or hazardous situation been incorporated into the definitions of the safety function?

To permit an assessment of whether the functional requirements have been met, the following forms of sub-test should be performed:

- Function test (in redundant systems, for each channel)
- Extended function test of the behaviour of the SRP/CS in response to input signals, operator processes or inputs which are atypical, unexpected or outside the specification
- Black-box test
- Performance tests (functional aspects)

The V&V activities described in this chapter are focused upon SRP/CS which execute safety functions. However, complete testing of the safety function on the final machine includes a series of further aspects, such as the dimensioning of overruns and safety clearances.

7.3 Validation of the PL of the SRP/CS

This section describes the testing of individual SRP/CS. The procedure for testing a combination of several SRP/CS forming a safety function is explained in Section 7.5.

The PL must be estimated for the SRP/CS (quantification of the probability of failure). The following sections indicate the validation steps for the sub-aspects which are considered for calculation of the PL. These aspects include, on the one hand, quantifiable aspects such as the $MTTF_d$ values for discrete components, the *DC*, CCF and the Category, and on the other, qualitative aspects such as the fault-mode behaviour of the safety function, safety-related software, systematic failures, and functional behaviour under environmental conditions. Evaluation of the individual aspects is followed by a description of a procedure for checking the estimation of the PL.

7.3.1 Validation of the Category

The purpose of Category validation is that of confirming all requirements placed upon the Category implemented by the SRP/CS (see Section 6.2). Documents required for this purpose particularly include:

- Specifications of the SRP/CS
- Design descriptions
- Block diagrams/descriptions of the structure
- Circuit diagrams
- Fault lists

For ascertainment of whether the requirements have been met, the following forms of sub-test should be performed:

- Tests of the fault-mode behavior of the SRP/CS, with failure mode and effects testing and testing by fault injection
- Tests of the behaviour of the SRP/CS in the event of faulty input signal states and faulty operator processes/inputs, by means of extended functional testing

These sub-tests should be supplemented by the following analyses:

- Structure/signal path analysis
- Inspection of the observance of basic safety principles
- Inspection of the implementation of well-tried safety principles (Category 1 and higher)
- Inspection of the use of well-tried components (Category 1 only)
- Evaluation of individual faults to be considered which are added to fault lists and of permissible fault exclusions, including the adequacy of their reasoning

The annexes in Part 2 of the standard (see also Annex C of this report, page 301) provide detailed assistance with the last four of these analyses.

7.3.2 Validation of the $\mathrm{MTTF_d}$ values

The $\mathrm{MTTF_d}$ values employed for determining of the PL should be checked at least for plausibility. This typically includes evaluation of whether suitable sources have been stated for the origin of the values. Review of the precise reasoning given for the values is also advisable for the dominant components and otherwise by random selection for all other components. The data sources indicated in Section 6.2.12 and Annex D (see page 315) can for example be used for this purpose.

7.3.3 Validation of the DC values

Comprehensible reasoning must be provided for the diagnostic coverage (DC) assigned to the blocks on the basis of test measures. Once again, the information on the origin of the values is typically examined here, i.e. whether the values obtained are credible or questionable. As with the $\mathrm{MTTF_d}$ values, verification is advisable by random survey, or by review of the reasoning in the case of the dominant components. Annex E (page 333) contains instructions for estimation of the DC values.

The implemented design must be examined to verify whether the diagnostics measures described have actually been implemented. For this purpose, it is generally necessary for the diagnostics functions and modules to be identified in the development documentation, and for their effectiveness to be estimated. In addition, tests of the fault-mode behaviour of the SRP/CS (failure mode and effects testing/testing by fault injection) are to show that proper fault detection is assured by the diagnostics functions.

7.3.4 Validation of the measures against CCF

Annex F (see page 343) contains a possible points-based method for validation of the selected measures against common cause failure (CCF). Besides attainment of the total number of points, the method examines whether the selected measures are adequately described in the associated documentation. Analysis and/or testing must demonstrate that the measures have actually been implemented. The typical V&V activities employed for this purpose include static hardware analysis and function testing under environmental conditions (limit conditions).

7.3.5 Verification and validation of the measures against systematic failures

For verification of the measures for the avoidance of systematic failures, development documents should be inspected for ascertainment of whether the required design measures described in Section 6.1.2 have been implemented. Verification can typically be provided by:

- Failure mode and effects testing or testing by fault injection on the supply units (e.g. power supply, clock, pressure)
- Testing of the resistance to ambient influences, testing under specified environmental conditions
- Analysis of implementation of program sequence monitoring
- Inspection and testing of the properties decisive to the quality of data communications systems; where used, identification of certified components
- Inspections of development documents which confirm the application of basic and well-tried safety principles and if applicable further measures such as hardware diversity

7.3.6 Validation of the software

The verification measures performed in the course of design and coding of the software are described comprehensively in Section 6.3.

With the exception of the embedded solution in PL e described below, the simplified “V model” is to be used for the development of safety-related software (see Figure 6.11). The final development activity under this model is that of software validation. The requirements of the safety-related software specification upon the functional behaviour and the performance criteria (e.g. time-related specifications) must be examined for proper implementation. At this stage, validation no longer considers the internal workings of the software, but its external behaviour at the output of the complete software, integrated into the hardware, in response to changes at the inputs of the latter. The software is considered here as a “black box”, and is validated by the black-box test.

I/O tests must be performed on safety-related application software (SRASW) to ensure that the safety-related input and output signals are used properly. For PL d and e, an additional extended test-case implementation based upon limit value analyses is also recommended for validation purposes. In this case, fault cases are determined analytically beforehand and executed in the test, and the response to them observed in order for fault detection and control by the software to be tested.

Individual software functions in the form of safety function blocks which have already been certified or validated by quality assurance measures do not need to be tested again. Evidence must however be furnished that validation has already been performed. Where a number of such safety function blocks are combined for a specific project, however, the resulting total safety function must be validated.

For attainment of the PL by safety-related embedded software (SRESW), the required design measures for software implementation in accordance with Section 6.3 must be examined with regard to their proper implementation. In the particular case of SRESW which has been employed in SRP/CS with PL e and was not developed with diversity for the two channels, the requirements for SIL 3 set out in Section 7 of IEC 61508-3 [32] must be satisfied in full. This includes the V&V activities required in this section.

Should the safety-related software subsequently be modified, it must be revalidated on an appropriate scale.

7.3.7 Checking of the assessment of the PL

Checking of the proper assessment of the PL for each SRP/CS particularly entails comprehension of proper application of the assessment method employed, including proper calculation. For example, Section 6.2.11 and Annex D contain simplified methods for determining the $MTTF_d$; the average diagnostic coverage DC_{avg} can be verified by means of the formula in Annex E (see page 333).

If the simplified procedure for estimation of the PL has been applied, a check can be performed with reference to Figure 6.10 of whether the correct PL has been determined from the Category, $MTTF_d$, and DC_{avg} obtained beforehand.

7.4 Review of the information for use

The user must be provided with important information on safe use of the SRP/CS in the form of instruction handbooks, assembly instructions and rating plates. This entire documentation, described as the “information for use”, should be inspected to ascertain whether it includes all the content stated in Section 11 of the standard. This includes comprehensible descriptions of the:

- Intended use (scope of use and application)
- Information on the Performance Level and the Category, and dated reference to the standard
- Safety functions and standard functions
- Modes of operation
- Response times
- Muting (temporary disabling of the safety functions)
- Limits of operation (including environmental conditions)
- Interfaces
- Displays and alarms
- Safe assembly and commissioning; if relevant, safe parameterization and programming
- Maintenance (including preventive maintenance) measures including appropriate checklist(s)
- Maintenance and replacement intervals
- Accessibility and replacement of internal parts
- Tools and procedures for safe and easy troubleshooting

7.5 Validation of the combination and integration of SRP/CS

The individual SRP/CS must be tested separately prior to combination. In order for systematic faults to be avoided during the combination/integration of SRP/CS, the following V&V activities must be performed:

- Inspection of the design documents which together describe the safety function
- Comparison of the characteristic data for the interfaces between the SRP/CS (e.g. voltages, currents, pressures, information data)
- FMEA of combination/integration
- Function test/black-box test

- Extended functional test
- Checking of the simplified determining the overall PL from the PLs of the individual SRP/CS, as described in Section 6.4

7.6 Verification and validation with reference to the example of a paper-cutting guillotine with diverse redundancy in the logic control (Category 4 – PL e)

The general description of the verification and validation of safety functions is supplemented in this section by an explanation of the V&V activities with reference to the practical example of a paper-cutting guillotine already described in Sections 5.7 and 6.5.

7.6.1 Verification of the attained PL (see also Block 6 in Figure 7.1)

A risk analysis showed that for the desired safety function SF2, the required Performance Level is PL_r e. Following calculation of the probability of failure in consideration of all quantifiable aspects, this PL is attained. All requirements for the qualitative aspects, such as the behaviour of the safety function under fault conditions, safety-related software, systematic failures and the behaviour under environmental conditions, are also adequately met for PL e.

7.6.2 Validation of the safety-related requirements (refer also to Block 7 in Figure 7.1)

Fault lists

The PL is determined based upon the fault lists to EN ISO 13849-2 [7].

Documents

As already stated, analysis/testing is based upon circuit diagrams, parts lists, specification and functional description.

Documentation

All analysis and test results must be documented in writing.

Validation of the safety functions

For testing of the functional requirements upon the safety function, a functional test is performed, supplemented by an extended functional test, in order to test the behaviour of the safety function in response to rare or non-defined inputs. An example would be testing of the reaction of the SRP/CS when a second person enters the hazardous area through an ESPE (light curtain) just as a worker is operating the two-hand control. Performance tests of functional aspects are completed. These include testing of the time to be observed for synchronous actuation in accordance with EN 574 [37]. Only when the two actuators S1 and S2 are operated within an interval of ≤ 0.5 seconds may output signals be generated for actuation of the clamping bar and the knife. The tests and analyses stated above for the specified safety characteristics have been passed.

Validation of the PL of the SRP/CS

- Validation of the Category

With reference to the development documentation, tests of the fault-mode behaviour are performed on a prototype by the deliberate injection of faults. The SRP/CS must respond to the injected faults in the manner specified. An analysis is first performed, followed by testing, to ascertain the behaviour when, for example, individual contactor relays are no longer capable of executing switching commands; or of how the SRP/CS reacts when one of the two actuators S1 or S2 is actuated with a delay, or not at all. The safety function must be assured at all times when a single fault is injected into the SRP/CS. A single fault must be detected at or prior to the next performance of the safety function. Should the fault not be detected, an accumulation of undetected faults must not result in loss of the safety function.

Observance of the closed-circuit current principle as an example of basic safety principles can be demonstrated by the injection of interruptions and evaluation of the response to them. Should, for example, the supply voltage fail, the clamping bar and the knife are returned to their initial positions by spring force.

Plausibility tests may be cited in this context as an example of well-tried safety principles: mechanically linked contacts in the contactor relays K3 to K6 are read back by both channels. Tests are performed to demonstrate proper operation of readback.

- Validation of the $\mathrm{MTTF_d}$ values

The value of 150 years from Table C.1 of EN ISO 13849-1, substituted for the valves 1V3, 1V4, 2V2 and 2V1, is checked here by way of example for validation of the $\mathrm{MTTF_d}$ values (see Table D.2 of this report). The correct value has been selected, and it originates from a reliable source. The safety principles (e.g. fluid change) applicable for the assumption of an $MTTF_d$ of 150 years are observed, and are also communicated to the operator in the instruction handbook.

Design features

- The requirements of Category B, basic and well-tried safety principles, are observed. Owing to diversely redundant processing channels (microcontroller and ASIC), a single fault does not result in loss of the safety function, and systematic faults are largely prevented.
- The safety-oriented switching position is assumed from any position by removal of the control signal.
- All electrical signals, including those of the pressure sensors, are processed in a multi-channel control system.
- The actuators S1 and S2 of the two-hand control satisfy IEC 60947-5-1.
- K3 to K6 possess mechanically linked contact elements to IEC 60947-5-1, Annex L [38]. The associated break contacts for monitoring of the make contacts are monitored in the respective adjacent channel.
- All conductors carrying signals are laid either separately or with protection against mechanical damage.
- The software (SRESW) is programmed in accordance with the requirements for PL d (downgraded owing to diversity) and the instructions in Section 6.3.
- Fault-avoidance measures in development of the ASIC are performed in accordance with the ASIC development life cycle (V-model) of the IEC 61508-2:2005 (CD) [39] draft standard.

- Validation of the DC values

A *DC* of 90% is confirmed for K1 and K2, based upon self-diagnostics. This includes a cross-check of input signals and intermediate results (from the microcontroller and the ASIC), monitoring of the timing and logical behaviour of the program sequence, and detection of static failures and short-circuits. Further tests are a CPU test in the channel containing the microcontroller, in which all commands used are tested, and tests of adequate quality of the random-access memory (RAM) and read-only memory (ROM). Tests of comparable quality to those in the parallel channel are performed in the second channel (ASIC). The tests must demonstrate that the measures described have been adequately implemented.

K3, K4, K5 and K6 are assigned a *DC* of 99%. This is appropriate owing to the plausibility tests performed by readback of the mechanically linked contacts of the contactor relays. The plausibility tests which have already been checked during validation of the Category also serve at this point to demonstrate proper operation.

- Validation of the measures against CCF

The minimum requirements for measures against common cause failure are satisfied, with 65 points. Further measures are also effective in parts of the control system.

15 points are allowed for implementation of the measure “physical separation between the signal paths”. Correct implementation of the measures must be demonstrated by an analysis of development documentation such as circuit diagrams, and by tests on the hardware.

- Verification and validation of the measures against systematic failures

The observance of basic and well-tried safety principles is a highly effective measure against systematic failures. The activities for validation of the Category also include examination of whether both safety principles have been observed. The results of the analyses and tests performed there can thus also be used for that purpose in this phase.

Besides the tests, and parallel to development, an inspection is performed of the documentation describing the basic and well-tried safety principles which are applied and the measures for the control and avoidance of systematic failures according to Section 6.1.2 of this report and Annex G of the standard. The inspection supports assessment of whether the principles and measures have been adequately considered during the development process.

An example of the control of systematic failures is that the safety-related software monitors the program sequence in order to detect defective execution of the program. The effectiveness of process monitoring is tested by injected faults.

In order to demonstrate the capacity of the SRP/CS to withstand the specified environmental conditions, tests are performed under all anticipated and predictable adverse conditions for factors including temperature, humidity and electromagnetic disturbance. This is an example of a measure for the avoidance of systematic failures.

- Validation of the software

Verification of the software is described in detail in Section 6.3. At this point, the software is also validated, i.e. testing is performed of operation and also of the response times of the software following integration onto the hardware. Testing takes the form of functional tests and extended functional testing in which firstly, the safety-related input signals must be processed correctly to safety-related output signals, and secondly, test cases with injected faults are executed in order to validate the specified fault responses of the firmware of the microcontroller K1.

- Checking of the estimated PL

The simplified procedure to EN ISO 13849-1 was applied for estimation of the PL. Its correct application is confirmed. Calculation of the $MTTF_d$ in accordance with Section

6.2.11 and Annex D and of the average diagnostic coverage DC_{avg} in accordance with Annex E is checked, as is correct determining of the PL from the previously confirmed Category, $MTTF_d$, and DC_{avg} values by means of the bar chart shown in Figure 6.10.

- Review of the information for use

The information for use must pass review for the following points concerning the SRP/CS: description of the intended use; information on the PL and the Category (including dated reference to the standard); explanation of all operating modes; description of the protective devices and safety functions with response times, environmental conditions for operation and external interfaces; information and technical data on transport, safe erection, commissioning and maintenance.

- Validation of the combination and integration of SRP/CS

The safety function described is implemented by an SRP/CS. Since different technologies, electronic and hydraulic, are however combined within this SRP/CS, certain tests which are necessary when SRP/CS are combined should also be performed here, unless they have already been included in validation of the Category. These tests include comparison of the interface data between the technologies employed, and functional tests and extended functional tests.

7.6.3 Examination of whether all safety functions have been analyzed (see also Block 8 in Figure 7.1)

The V&V activities shown here for SF2 are conducted for all safety functions executed by the SRP/CS (SF1 to SF7). The additional effort is low, however, since many safety functions employ the same hardware. The analyses and tests must show that the safety functions have been implemented correctly. Once all safety functions have been considered, evaluation according to EN ISO 13849 Parts 1 and 2 is complete.

8 Circuit examples for SRP/CS

This report began by addressing the design of safe controls in general. Sections 5.7, 6.5 and 7.6 then illustrated, with reference to the example of a paper-cutting guillotine, how the methods for the design of safe control systems can be implemented. The methods for determining the PL are described step by step here and in EN ISO 13849-1; some of these steps, however, such as deriving the safety-related block diagram from the circuit diagram, require some practice. In addition, owing to the variety of possible safety functions and their implementation, they do not lend themselves to generic description. For this reason, this chapter now presents the evaluation of a number of circuit examples which implement the safety functions in various Categories and Performance Levels and by means of different technologies. In the circuit examples, the term control system generally covers only the safety-related parts of control systems. The examples are limited to essential aspects, and therefore serve only as suggestions for implementation. Importance was attached in their selection to a wide spectrum of technologies and possible applications. Readers of the 1997 report [40] on the Categories for safety-related control systems to EN 954-1 will recognize some of the examples, to which for example calculation of the probability of failure has been added. The examples are an interpretation of the Categories, and have been compiled by the authors based upon many years of experience with safety-related machine control systems and participation on national and European standardization committees, in order to provide designers with effective guidance for their own developments. Since the examples were created by different authors, some variation inevitably exists, for example in their presentation of details or in the reasoning behind certain numerical data. All calculations for the circuit examples were performed with the aid of Version 1.0 of the SISTEMA software application (Annex H), the version available at the time of drafting this report.

The descriptions in the examples are structured as follows:

- Safety function
- Functional description
- Design features
- Remarks
- Calculation of the probability of failure
- More detailed references

Under “Safety function”, the name of the safety function is stated together with the events which trigger it and the required safety responses.

The “Functional description” describes the essential safety-related functions, based upon a conceptual schematic diagram. The behaviour in the event of a fault is explained, and measures for fault detection are stated.

The “Design features” list the particular characteristics in the design of the example in question, such as the application of well-tried safety principles and the use of well-tried components.

The circuit diagrams are conceptual schematic diagrams which are limited solely to presentation of the safety function(s) with the relevant components required for the purpose. In the interests of clarity, certain other circuitry which would normally be required has been omitted, for example that for the assurance of electric shock protection, for control of overvoltage/undervoltage and overpressure or low pressure, for the detection of insulation faults, short-circuits and earth faults for example on external lines, or for assurance of the required resistance to electromagnetic disturbance. Circuit details which are not essential to definition of the safety-related block diagram have thus been deliberately omitted. Such details include protective circuitry in the electrical system, such as fuses and diodes, for example in the form of free-wheeling diodes. The diagrams also omit decoupling diodes in circuits in which sensor signals are read in for example redundantly into multiple logic components. This arrangement is intended to prevent an input becoming an output on redundant systems in the event of a fault, and thus influencing the second channel. These components are all essential in order for a control system to be implemented in accordance with a Category and a Performance Level. Further examples are listed in the technology-specific comments on fluid power technology. In accordance with the fault lists in EN ISO 13849-2, issues such as the influence of conductor short-circuits must of course also be considered in relation to the safety function concerned and the conditions of use. All components used must therefore be selected with consideration for their suitability according to their specification. Over dimensioning is one of the well-tried safety principles.

Only those design features, which are significant for the described safety function are considered. In most cases the safety function is “Safety-related stop function initiated by a safeguard”. Other safety functions such as “Prevention of unexpected start-up” or “Manual reset function” as well as “Start/restart function” are not covered in all circuit examples. If manually operated devices (e.g. push buttons) are used for the realisation of the latter mentioned safety functions, special attention should be drawn to the following: these safety functions – especially when used with electronic circuits – shall be realised by disengaging the actuator from its energized (on) position.

Where relevant to the example concerned, reference is made under “Remarks” to particular aspects concerning a possible application.

Under “Calculation of the probability of failure”, a description is found of calculation of the PL from the parameters Category, $MTTF_d$, DC_{avg} and CCF, based upon the safety-related block diagram derived from the conceptual schematic diagram. The Category is determined from the functional description and the design features.

The $\mathrm{MTTF_d}$ values employed in the calculations are marked as manufacturer's values (“[M]” for **M**anufacturer), typical values from databases (“[D]” for **D**atabase), or values from EN ISO 13849-1 (“[S]” for **S**tandard). According to the standard, priority should be given to manufacturers' data. For certain components, such as rotary signal encoders or frequency inverters, neither reliable manufacturers' data nor database values were available at the time of drafting of the report. Manufacturers were contacted directly in this case, or use was made of the parts count method for estimation of typical example values (marked “[E]” for **E**stimated). The $\mathrm{MTTF_d}$ values in this chapter should therefore be regarded more as estimates.

The presentation of the assumed measures for diagnostics (*DC*) and against common cause failure (CCF) is limited to general information. Specific values for these two criteria are dependent upon the implementation, the application and the manufacturer. It is therefore possible that different DC values are assumed for similar components in different examples. Here too, all assumptions regarding *DC* and CCF must be reviewed where actually implemented in practice; the assumed values are not binding and are intended for illustration only.

The focus in the description lies more upon the Categories in the form of the "resistance to faults" and upon the "mathematical" methods for determining the PL. Conversely, some sub-steps, such as fault exclusion, basic and well-tried safety principles or measures against systematic faults (including software) are mentioned only briefly. During implementation, appropriate attention must be paid to this aspect, since misjudgements or inadequate implementation of these measures could lead to a deterioration in the fault tolerance or probability of failure. As an aid to understanding of the circuit examples and for their practical implementation, the reader's attention is therefore drawn to Chapter 7 and Annex C, in which, for example, the basic and well-tried safety principles are described in detail.

Finally, reference is made to "More detailed references", where available.

For each form of technology, certain comments of a general nature are made in the following technology-specific sections in order to provide a better understanding of the examples and for implementation of the Categories. Some of the circuit examples represent "control systems involving multiple technologies". These "mixed" circuit examples are based upon the concept, enshrined in the standard, that a safety function is always implemented by "reception", "processing" and "switching", regardless of the technology employed.

8.1 General technology-related comments on the example control systems

8.1.1 Electromechanical controls

Electromechanical controls primarily employ electromechanical components in the form of switches or control devices (e.g. position switches, selector switches, pushbuttons) and switching devices (contactor relays, relays, contactors). These devices have defined switching positions. They do not generally change their switching state unless actuated externally or electrically. When selected properly and used as intended, they are largely immune to disturbance such as electrical or electromagnetic interference. In this respect they differ, in some cases considerably, from electronic equipment. Their durability and failure mode can be influenced by suitable selection, dimensioning and arrangement. The same applies to the conductors employed, when suitably routed within and outside the electrical compartments.

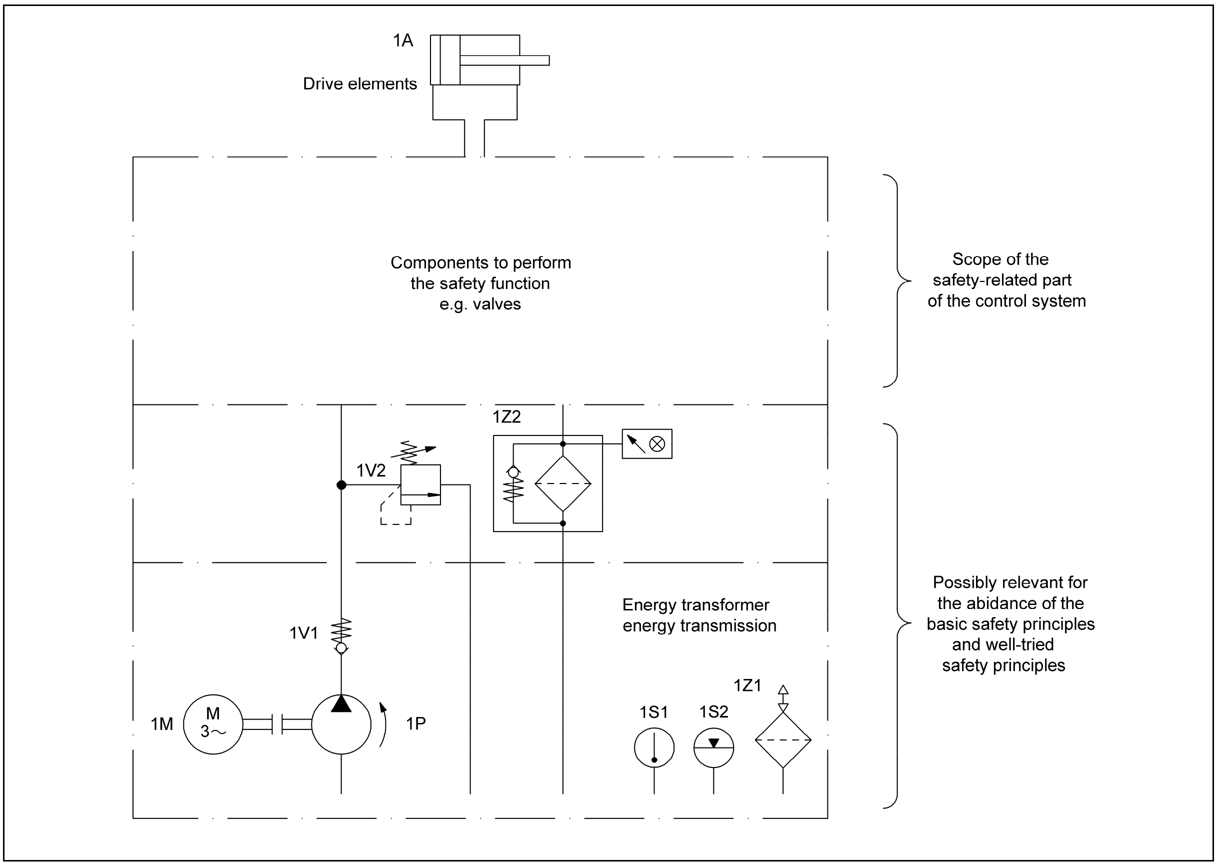
For the reasons stated above, the electromechanical components generally satisfy the "basic safety principles", and in many cases are to be regarded as "well-tried components" in a safety context. This holds true, however, only when the requirements of EN 60204-1 [20] for the electrical equipment of the machine/installation are observed. In some cases, fault exclusion is possible, for example on a control contactor with regard to pick-up in the absence of a control voltage, or non-opening of a break contact with direct opening action on a switch to IEC 60947-5-1 [38], Annex K.

8.1.2 Fluid power controls

On fluid power systems, the area of valves in particular should be considered a “safety-related part of the control system”, and specifically the valves which control hazardous movements or states. The fluid circuits shown constitute example arrangements only. The required safety functions can generally also be attained by alternative control logic employing appropriate valve types, or for that matter in some cases by additional mechanical solutions such as hold devices or brakes.

On **hydraulic systems** (see Figure 8.1), measures for pressure limitation in the system (1V2) and for filtration of the hydraulic fluid (1Z2) must also be considered in this context.

Figure 8.1:
Scope of EN ISO 13849 for hydraulic systems

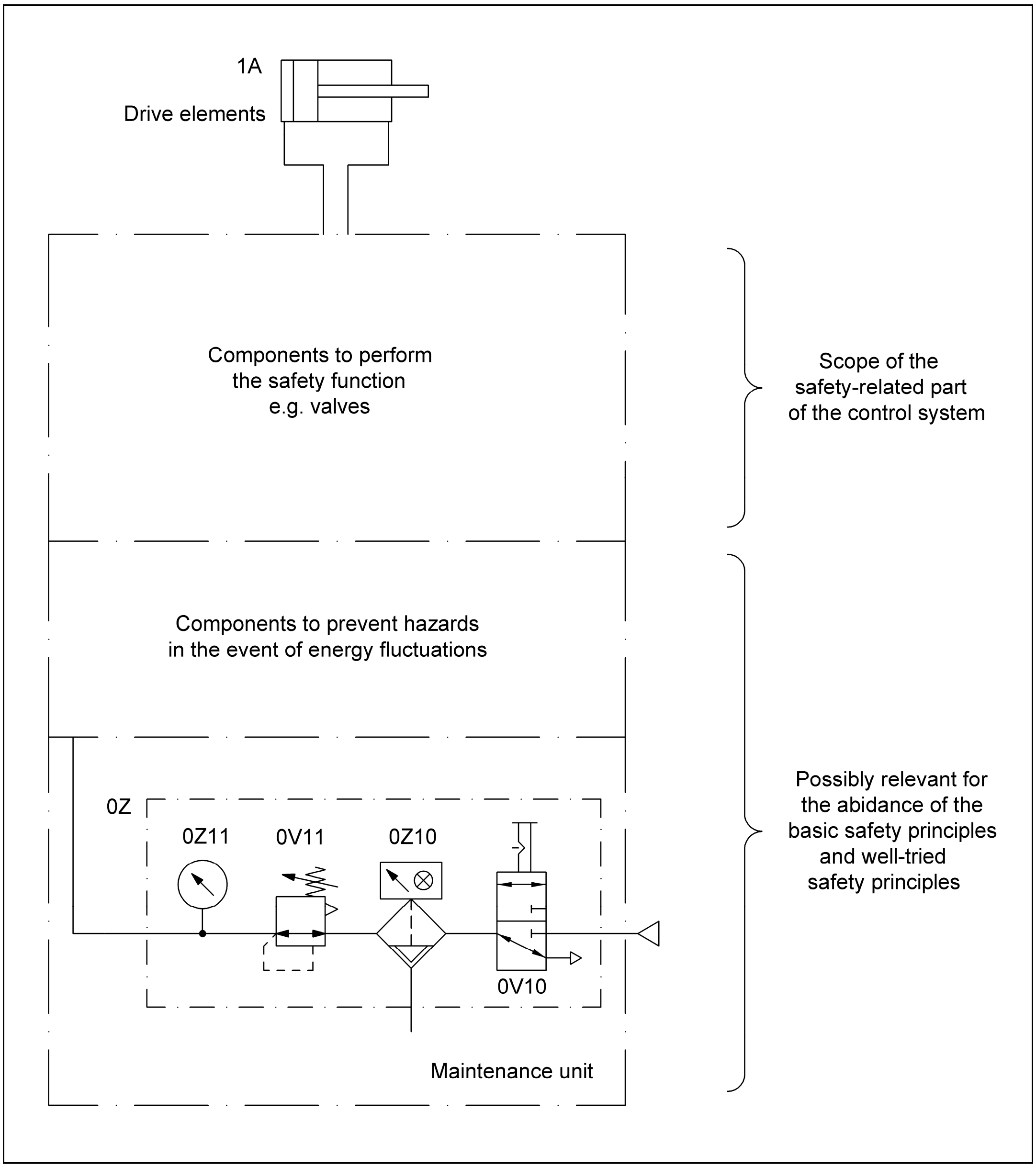


The components 1Z1, 1S1 and 1S2 shown in Figure 8.1 are present in the majority of hydraulic systems and are of great importance, particularly for the condition of the hydraulic fluid and consequently for the valve functions. The reservoir-breather filter 1Z1 arranged on the fluid reservoir prevents the ingress of external dirt. The fluid level indicator 1S2 ensures that the fluid level remains within the specified limits. The temperature indicator 1S1 constitutes suitable measures for limitation of the operating temperature range and thus the operating viscosity range of the hydraulic fluid. If necessary, heating and/or cooling facilities must be provided in conjunction with closed-loop temperature control (refer also to Annex C in this context).

The drive elements and the components for energy conversion and transmission in fluid power systems generally lie outside the scope of the standard.

On **pneumatic systems** (Figure 8.2), the components for the prevention of hazards associated with energy conversions and the maintenance unit for conditioning of the compressed air must be considered from a safety perspective in conjunction with the valve area.

Figure 8.2:
Scope of EN ISO 13849 for pneumatic systems



In order for the possible energy conversions to be controlled with consideration for safety aspects, an exhaust valve is frequently used in conjunction with a pressure switch. In the circuit examples in this chapter, these components are marked 0V1 (exhaust valve) and 0S1 (pressure switch). The maintenance unit 0Z (see Figure 8.2) generally consists of a manual shut-off valve 0V10, a filter with water separator 0Z10 which is used to monitor the degree of pollution, and a pressure control valve 0V11 (with adequately dimensioned secondary exhaust). The pressure indicator 0Z11 satisfies the requirement for monitoring of the system parameters.

Besides the safety-related control part, the fluid power control circuits presented as examples in this chapter contain only the additional components required for an understanding of the fluid control system or which are directly related to the control technology. The requirements which must be met by fluid power control systems are described comprehensively in [41; 42], [43 to 47] are further relevant standards.

The majority of control system examples are electrohydraulic or electropneumatic controls. A range of safety requirements are met on these control systems by means of the electrical control part, for example the requirement for energy changes on electrohydraulic control systems to be controlled.

On the control examples described here, the required safety function is the stopping of a hazardous movement or the reversal of a direction of movement. Prevention of unexpected start-up is implicitly included. The required safety function may however also be a defined pressure level or a pressure release.

The structures of most fluid power control systems are executed in Categories 1, 3 or 4. Since Category B already requires observance of the relevant standards and of the basic safety principles, Category B and 1 fluid power control systems do not differ essentially in their control structure, but only in the higher safety-related reliability of the relevant valves. For this reason, this report does not present any Category B fluid power control systems.

8.1.3 Electronic and programmable electronic control systems

Electronic components are generally more sensitive to external environmental influences than electromechanical components. If no particular measures are taken, the use of electronic components at temperatures < 0 °C is subject to substantially greater constraints than those for electromechanical components. In addition, environmental influences exist which are virtually irrelevant to electromechanical circuit elements but which present crucial problems for electronic systems, namely any electromagnetic disturbances which are coupled into electronic systems in the form of conducted disturbances or electromagnetic fields. In some cases, greater effort is required in order for adequate resistance to disturbance to be attained for industrial use. Fault exclusion is virtually impossible on electronic components. In consequence, safety cannot in principle be guaranteed by the design of a particular component, but only by certain circuit concepts and by the application of appropriate measures for the control of faults.

According to the fault lists for electrical/electronic components to EN ISO 13849-2, the faults short-circuit, open circuit, change of a parameter or a value, and stuck-at faults are essentially assumed. These are without exception fault effects which are assumed to be permanent. Transient (sporadically occurring) faults such as soft-errors caused by charge reversal of a capacitor in a chip owing to high-energy particles such as alpha particles can generally be detected only with difficulty and controlled for the most part by structural measures.

The failure mode of electronic components is frequently difficult to evaluate; generally, no predominant failure type can be defined. This can be illustrated by an example. If a contactor is not actuated electrically, i.e. current does not flow through its coil, there is no reason for the contactor contacts to close. In other words, a de-energized relay or contactor does not switch on of its own accord in response to an internal fault. The situation is different for the majority of electronic components, such as transistors. Even if a transistor is blocked, i.e. in the absence of a sufficiently high base current, the possibility cannot nevertheless be excluded of its suddenly becoming conductive without external influence as a result of an internal fault; under certain circumstances, this may lead to a hazardous movement. This drawback, from a safety perspective, of electronic components must also be controlled by a suitable circuit concept. Where highly integrated modules are used, in particular, it may not even be possible to demonstrate that a device or equipment is completely free of faults at the beginning of its mission time, i.e. at commissioning. Even at component level, manufacturers are no longer able to demonstrate freedom from faults with 100% test coverage for complex integrated circuits. A similar situation exists for the software of programmable electronics.

In contrast to electromechanical circuits, purely electronic circuits often have the advantage that a change of states can be forced dynamically. This permits attainment of the required *DC* at appropriately short intervals and without alteration of the state of external signals (forced dynamics).

Decoupling measures are required between different channels in order to prevent common cause failures. These measures generally consist of galvanically isolated contacts, resistor or diode networks, filter circuits, optocouplers and transformers.

Systematic failures may lead to simultaneous failure of redundant processing channels if this is not prevented by timely consideration, in particular during the design and integration phase. By the use of principles such as closed-circuit current, diversity or over-dimensioning, electronic circuits can also be designed with sufficient robustness for systematic failures to be prevented sufficiently reliably. Measures which render the processing channels insensitive to the physical influences encountered for example in an industrial environment should not be ignored. Such influences include temperature, moisture, dust, vibration, shock, corrosive atmospheres, electromagnetic influences, voltage breakdown, overvoltage and undervoltage.

A Category 1 SRP/CS must be designed and manufactured with the use of well-tried components and well-tried safety principles. Since complex electronic components such as PLCs, microprocessors or ASICs are not deemed well-tried in the context of the standard, this report contains no corresponding examples of Category 1 electronics.

The circuit examples include a statement of the effectiveness, i.e. the related Performance Level, of the required measures for fault avoidance/fault control for programmable electronics. Refer to Section 6.3 for further details. Should ASICs be employed in a development, measures for fault avoidance are required in the development process. Such measures can be found for example in the draft standard IEC 61508-2:2008 (CDV) [39], which specifies a V-model for the development of an ASIC, based upon the V-model known from software design and development.

The following points are worthy of mention, since such issues arise in practice:

- Generally, two channels of an SRP/CS shall not be routed through the same integrated circuit. For optocouplers, for example, this requirement means that they must be housed in separate enclosures when they are used to process signals from different channels.

- The influence of operating systems etc. must also be considered where programmable electronics are employed. A standard PC and typical commercial operating system is not suitable for use in a safety-related control system. The required freedom of faults (or realistically, low incidence of faults) cannot generally be demonstrated with reasonable effort, or will not be attainable, with an operating system that was not designed for safety-related applications.

8.2 Circuit examples

Table 8.1 shows an overview of circuit examples 1 to 37. Table 8.2 contains an alphabetical list of the main abbreviations used in the circuit examples.

Table 8.1:
Overview of the circuit examples

Attained PL	**Implemented Category**	**Technology/example No.**		
		Pneumatics	**Hydraulics**	**Electrical**
b	B			1
c	1	2	3	4, 5, 6, 7, 8
c	2			9
c	3			10, 24
d	2	11	12	13
d	3	14	15, 16	15, 16, 17, 18, 19, 20, 21, 22, 23, 24
e	3	25, 26	27	29, 30
e	4	31	32, 33	28, 33, 34, 35, 36, 37

Table 8.2:
Overview of the abbreviations employed in the circuit examples

Abbreviation	Full form
[D]	B_{10d} or $MTTF_d$ values from databases (refer for example to Annex D, Section D2.6)
[E]	Estimated B_{10d} or $MTTF_d$ values
[M]	B_{10d} or $MTTF_d$ values based upon manufacturers' information
[S]	B_{10d} or $MTTF_d$ values based upon data listed in EN ISO 13849-1 (refer for example to Table D.2 of this report)
µC	Microcontroller
B_{10}	Nominal lifetime: the average number of switching operations/ switching cycles reached before 10% of the considered units fail
B_{10d}	Nominal lifetime (dangerous): the average number of switching operations/switching cycles reached before 10% of the considered units fail dangerously
CBC	Clutch/brake combination
CCF	Common cause failure
CPU	Microprocessor (central processing unit)
DC	Diagnostic coverage
DC_{avg}	Average diagnostic coverage
ESPE	Electro-sensitive protective equipment
FI	Frequency inverter
FIT	Number of failures in 10^9 component hours (failures in time)
FMEA	Failure mode and effects analysis
M	Motor
MPC	Multipurpose control
$MTTF_d$	Mean time to dangerous failure
n_{op}	Mean annual number of operations

Table 8.2: continued

Abbreviation	Full form
PFH	Average probability of a dangerous failure per hour
PL	Performance Level
PL_r	Required Performance Level
PLC	Programmable logic controller
RAM	Random-access memory
ROM	Read-only memory
SLS	Safely limited speed (see Table 5.2)
SRASW	Safety-related application software
SRESW	Safety-related embedded software
SRP/CS	Safety-related part of a control system
SS1	Safe stop 1 (see Table 5.2)
SS2	Safe stop 2 (see Table 5.2)
STO	Safe torque off (see Table 5.2)
$T_{10\mathrm{d}}$	Mean time reached before 10% of the components studied fail dangerously
THC	Two-hand control

8.2.1 Position monitoring of moveable guards by means of a proximity switch – Category B – PL b (Example 1)

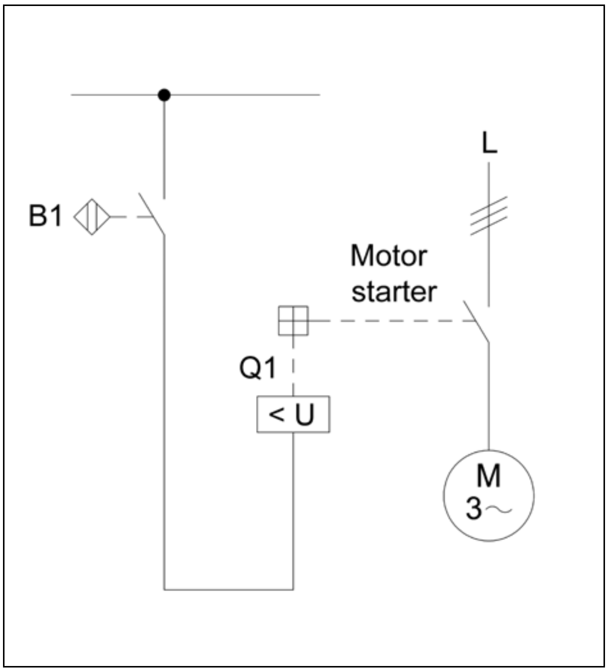


Figure 8.3:
Position monitoring of a moveable guard by means of a proximity switch

Safety function

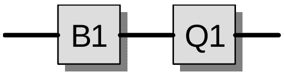
- Safety-related stop function, initiated by a protective device: actuation of the proximity switch when the moveable guard (safety guard) is opened initiates the safety function STO (safe torque off).

Functional description

- Opening of the moveable guard (e.g. safety guard) is detected by a proximity switch B1 which acts upon the undervoltage release of a motor starter Q1. The dropping out of Q1 interrupts or prevents hazardous movements or states.
- The safety function cannot be maintained with all component failures, and is dependent upon the reliability of the components.
- Removal of the protective device is detected.
- B1 contains no internal monitoring measures. No further measures for fault detection are implemented.

Design features

- Basic safety principles are observed and the requirements of Category B are met. Protective circuits (e.g. contact protection) as described in the initial paragraphs of Chapter 8 are implemented. The closed-circuit current principle of the undervoltage release is employed as the basic safety principle.



- A stable arrangement of the protective device (safety guard) provides assured actuation of the proximity switch.
- Depending upon the design of the proximity switch, safe operation can be bypassed in a reasonably foreseeable manner. Bypassing can be made more difficult, for example by particular conditions for installation, such as mounting in hidden position (see also EN 1088/A1, Annex J).
- The power supply to the entire machine is switched off (stop category 0 to EN 60204-1).

Calculation of the probability of failure

- $MTTF_d$: B1 is a conventional proximity switch on a safety guard with an $MTTF_d$ of 40 years [M]. For the undervoltage release of motor starter Q1, the B_{10} value approximates to the electrical lifetime of 10,000 switching operations [M]. If 50% of failures are assumed to be dangerous, the B_{10d} value is produced by doubling of the B_{10} value. At daily actuation of the proximity switch, an n_{op} of 365 cycles per year for Q1 produces an $MTTF_d$ of 548 years. For the combination of B1 and Q1, the $MTTF_d$ for the channel is 37 years. This value is capped to the arithmetical maximum value for Category B, i.e. 27 years (“medium”).
- DC_{avg} and measures against common cause failures are not relevant in Category B.
- The electromechanical control system corresponds to Category B with a medium $MTTF_d$ (27 years). This results in an average probability of dangerous failure of 4.23×10^{-6} per hour. This corresponds to PL b.

More detailed references

- EN 1088/A1: Safety of machinery – Interlocking devices associated with guards – Principles for design and selection (04.07)
- EN 60204-1: Safety of machinery – Electrical equipment of machines. Part 1: General requirements (06.06)

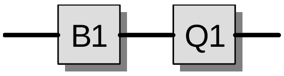
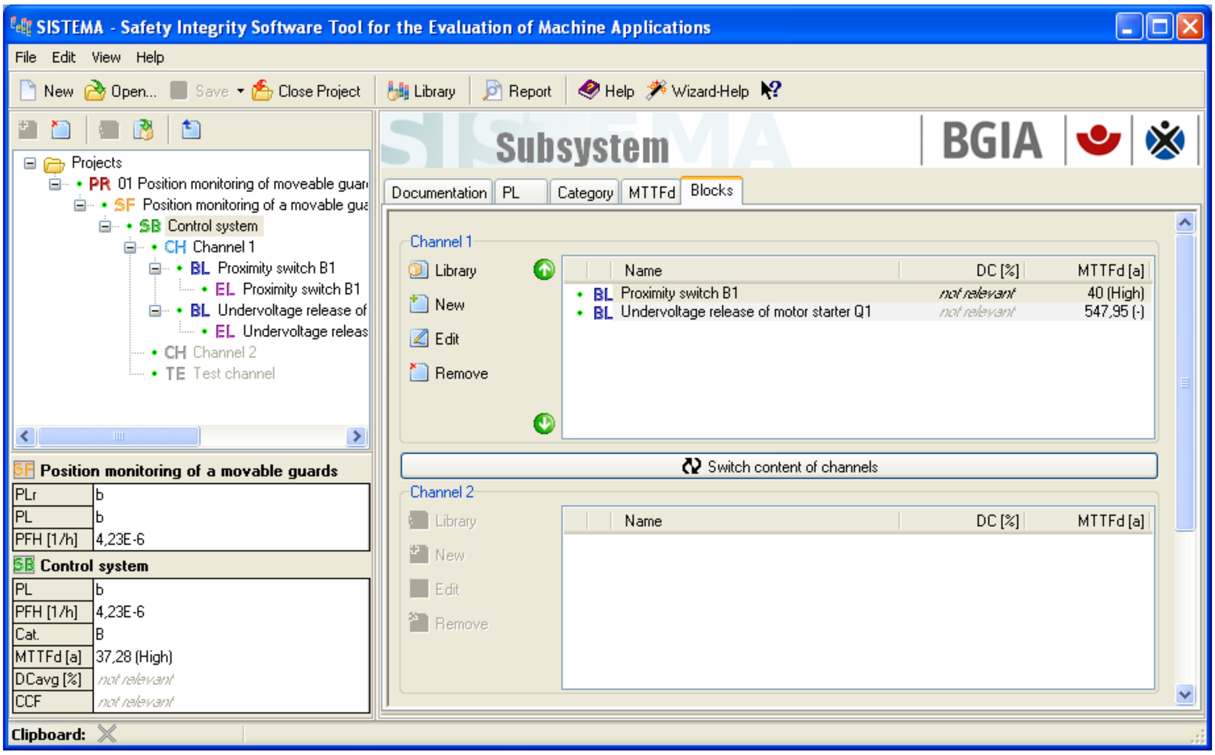


Figure 8.4:
Determining of the PL by means of SISTEMA


SISTEMA - Safety Integrity Software Tool for the Evaluation of Machine Applications
File Edit View Help
New Open... Save Close Project Library Report Help Wizard-Help
Subsystem
BGIA
Documentation PL Category MTTFd Blocks
Library
New
Edit
Remove
Switch content of channels
Clipboard:

- Projects
  - PR 01 Position monitoring of moveable guar
    - SF Position monitoring of a movable gua
      - SB Control system
        - CH Channel 1
          - BL Proximity switch B1
            - EL Proximity switch B1
          - BL Undervoltage release of
            - EL Undervoltage releas
        - CH Channel 2
        - TE Test channel

SF Position monitoring of a movable guards

PLr	b
PL	b
PFH [1/h]	4,23E-6

SB Control system

PL	b
PFH [1/h]	4,23E-6
Cat.	B
MTTFd [a]	37,28 (High)
DCavg [%]	*not relevant*
CCF	*not relevant*

Channel 1

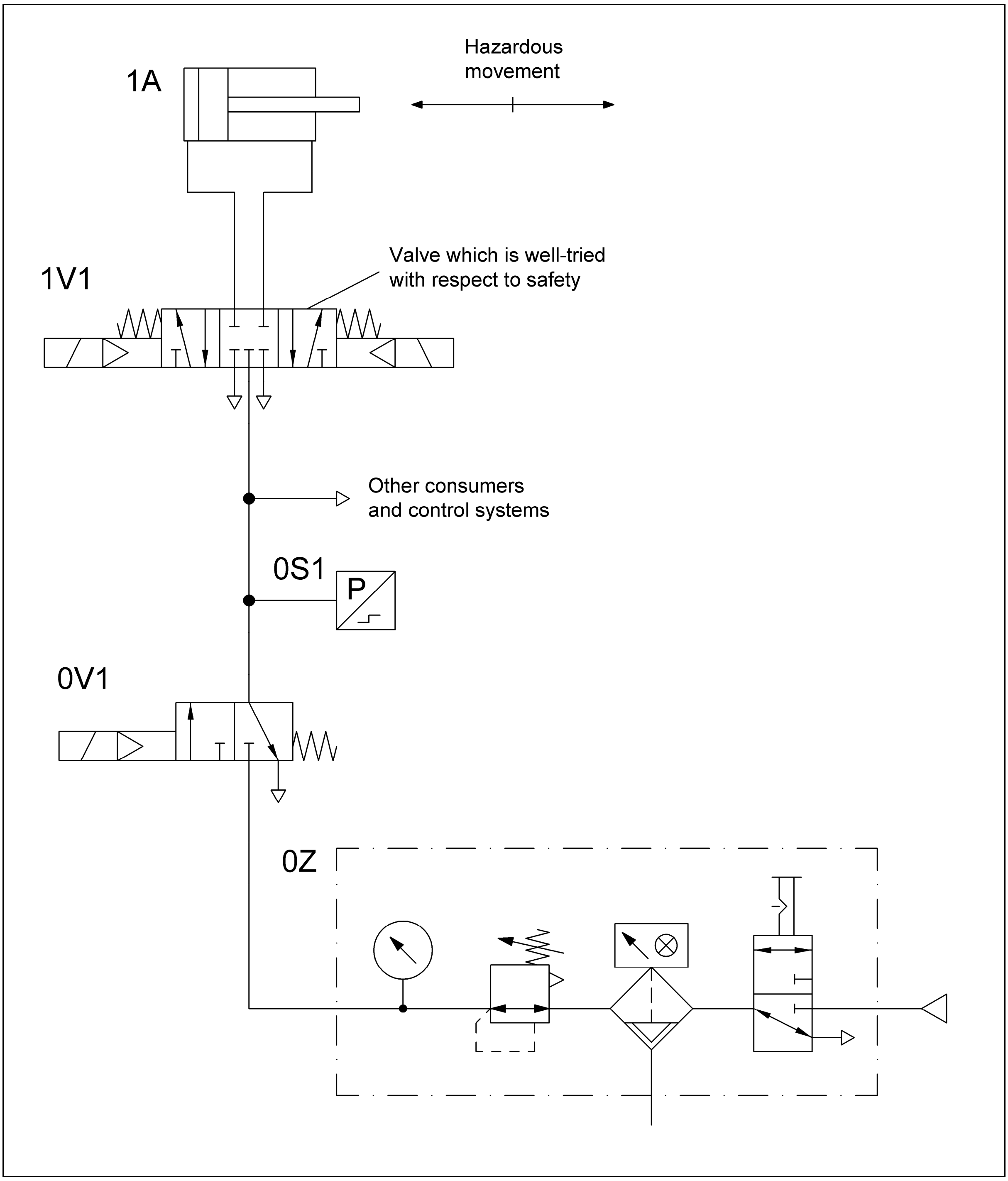
	Name	DC [%]	MTTFd [a]
BL	Proximity switch B1	*not relevant*	40 (High)
BL	Undervoltage release of motor starter Q1	*not relevant*	547,95 (-)

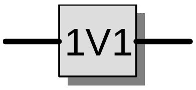
Channel 2

	Name	DC [%]	MTTFd [a]

8.2.2 Pneumatic valve (subsystem) – Category 1 – PL c (for PL b safety functions) (Example 2)

Figure 8.5:
Pneumatic valve for the control of hazardous movements





Safety functions

- Safety-related stop function: stopping of the hazardous movement and prevention of unexpected start-up from the rest position

- Only the pneumatic part of the control is shown here, in the form of a subsystem. Further safety-related control components (e.g. protective devices and electrical logic elements) must be added in the form of subsystems for completion of the safety function.

Functional description

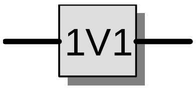
- Hazardous movements are controlled by a directional control valve 1V1 with well-tried safety functionality.
- Failure of the directional control valve may result in loss of the safety function. The failure is dependent upon the reliability of the directional control valve.
- No measures for fault detection are implemented.
- Should trapped compressed air pose a further hazard, additional measures are required.

Design features

- Basic and well-tried safety principles are observed and the requirements of Category B are met.
- 1V1 is a directional control valve with closed centre position, sufficient overlap, spring centering and fatigue-resistant springs.
- The safety-oriented switching position is attained by removal of the control signal.
- Where necessary, the manufacturer/user must confirm that the directional control valve is a component with well-tried safety functionality (of sufficiently high reliability).
- The safety function can also be attained by a logical arrangement of suitable valves.

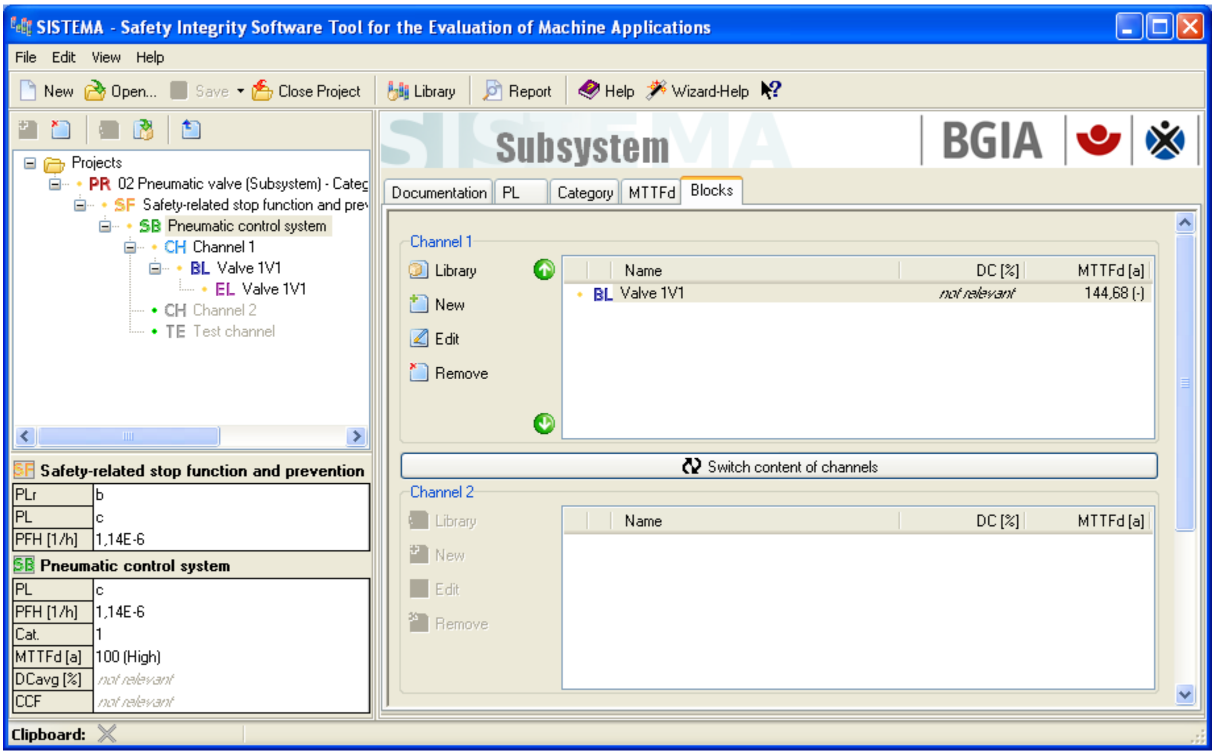
Calculation of the probability of failure

- $MTTF_d$: a B_{10d} value of 40,000,000 switching operations [E] is assumed for the directional control valve 1V1. At 240 working days, 16 working hours per day and a cycle time of 5 seconds, n_{op} is 2,764,800 cycles per year and the $MTTF_d$ is 145 years. This is also the MTTF_d value per channel, which is capped to 100 years (“high”).
- DC_{avg} and measures against common cause failures are not relevant in Category 1.



- The pneumatic control corresponds to Category 1 with a high *MTTF*$_d$ (100 years). This results in an average probability of dangerous failure of 1.14 × 10^{-6} per hour. This corresponds to PL c. The addition of further safety-related control parts as subsystems for completion of the safety function generally results in a lower PL.
- In consideration of the estimation erring on the safe side as described above, a T_{10d} value of 14 years operating time is produced for specified replacement of the wearing directional control valve 1V1.

Figure 8.6:
Determining of the PL by means of SISTEMA



Projects
PR 02 Pneumatic valve (Subsystem) - Categ
SF Safety-related stop function and prev
SB Pneumatic control system
CH Channel 1
BL Valve 1V1
EL Valve 1V1
CH Channel 2
TE Test channel

SF Safety-related stop function and prevention

PLr	b
PL	c
PFH [1/h]	1,14E-6

SB Pneumatic control system

PL	c
PFH [1/h]	1,14E-6
Cat.	1
MTTFd [a]	100 (High)
DCavg [%]	*not relevant*
CCF	*not relevant*

Channel 1

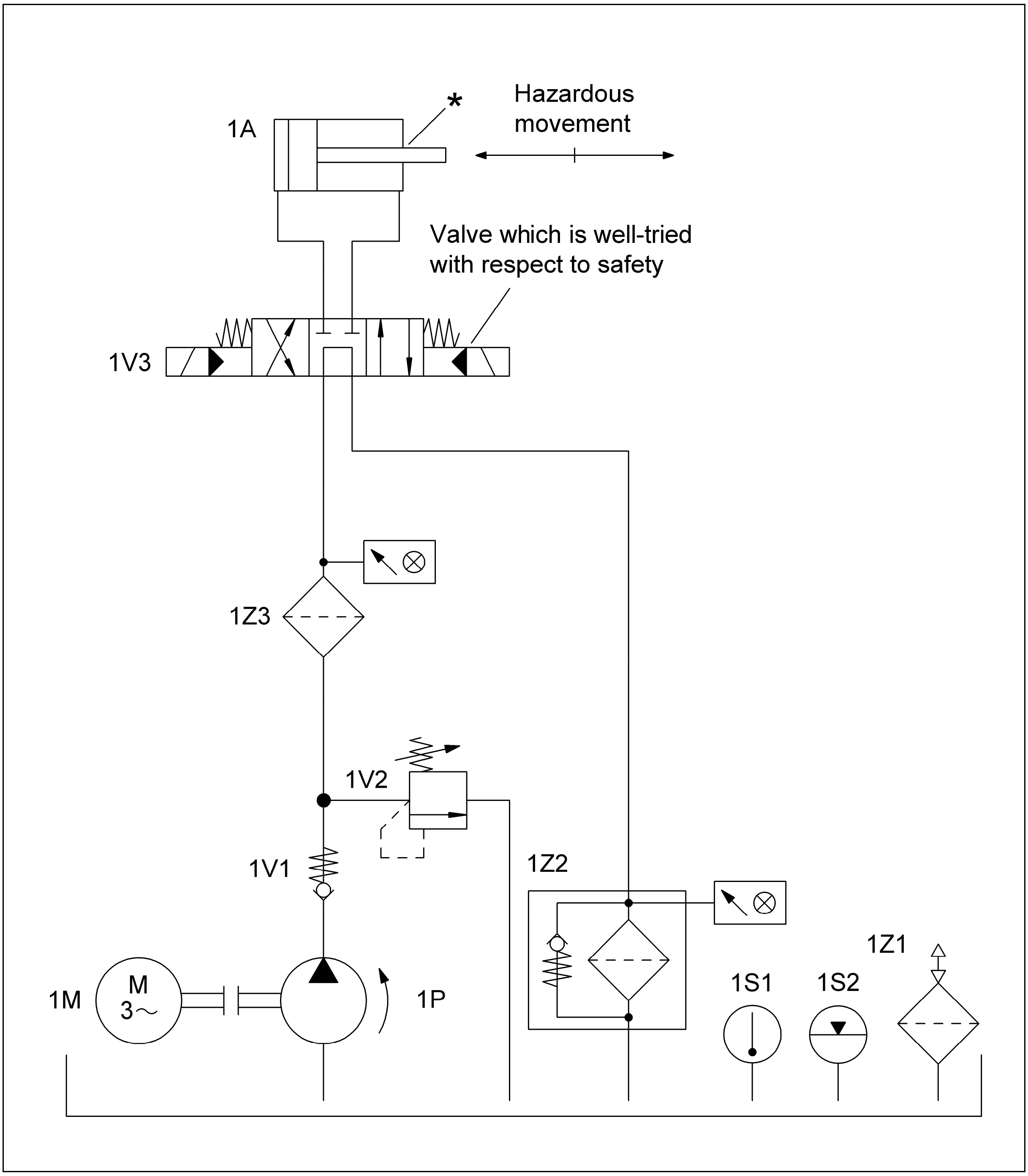
Name	DC [%]	MTTFd [a]
BL Valve 1V1	*not relevant*	144,68 (-)

Channel 2

Name	DC [%]	MTTFd [a]

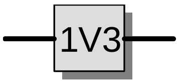
8.2.3 Hydraulic valve (subsystem) – Category 1 – PL c (for PL b safety functions) (Example 3)

Figure 8.7:
Hydraulic valve for the control of hazardous movements



Safety functions

- Safety-related stop function: stopping of the hazardous movement and prevention of unexpected start-up from the rest position



- Only the hydraulic part of the control is shown here in the form of a subsystem. Further safety-related control components (e.g. protective devices and electrical logic elements) must be added in the form of subsystems for completion of the safety function.

Functional description

- Hazardous movements are controlled by a directional control valve 1V3 with well-tried safety functionality.
- Failure of the directional control valve may result in loss of the safety function. The failure is dependent upon the reliability of the directional control valve.
- No measures for fault detection are implemented.

Design features

- Basic and well-tried safety principles are observed and the requirements of Category B are met.
- 1V3 is a directional control valve with closed centre position, sufficient overlap, spring centering and fatigue-resistant springs.
- The safety-oriented switching position is attained by removal of the control signal.
- Where necessary, the manufacturer/user must confirm that the directional control valve is a component with well-tried safety functionality.
- The following specific measures are implemented to increase the reliability of the directional control valve: a pressure filter 1Z3 upstream of the directional control valve and suitable measures on the cylinder to prevent dirt from being drawn in by the piston rod (e.g. effective wiper on the piston rod, see ∗ in Figure 8.6).

Calculation of the probability of failure

- $MTTF_d$: an $MTTF_d$ of 150 years is assumed for the directional control valve 1V3 [S]. This is also the $\mathrm{MTTF_d}$ value per channel, which is capped to 100 years (“high”).
- DC_{avg} and measures against common cause failures are not relevant in Category 1.
- The hydraulic control corresponds to Category 1 with a high $MTTF_d$ (100 years). This results in an average probability of dangerous failure of 1.14×10^{-6} per hour. This corresponds to PL c. The addition of further safety-related control parts as subsystems for completion of the safety function generally results in a lower PL.

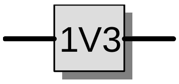
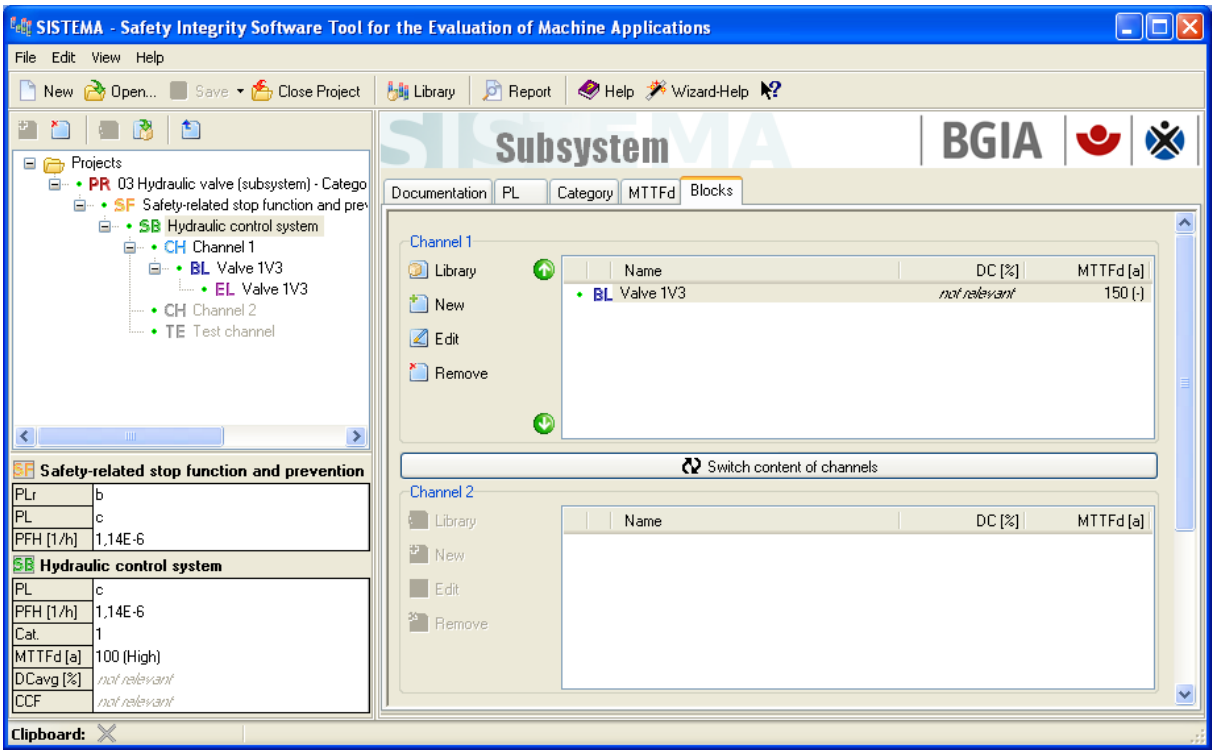


Figure 8.8:
Determining of the PL by means of SISTEMA


SISTEMA - Safety Integrity Software Tool for the Evaluation of Machine Applications
File Edit View Help
New Open... Save Close Project Library Report Help Wizard-Help
Subsystem
BGIA
Documentation PL Category MTTFd Blocks
Library
New
Edit
Remove
Switch content of channels
Clipboard:

- Projects
  - PR 03 Hydraulic valve (subsystem) - Catego
    - SF Safety-related stop function and pre
      - SB Hydraulic control system
        - CH Channel 1
          - BL Valve 1V3
            - EL Valve 1V3
        - CH Channel 2
        - TE Test channel

SF Safety-related stop function and prevention

PLr	b
PL	c
PFH [1/h]	1,14E-6

SB Hydraulic control system

PL	c
PFH [1/h]	1,14E-6
Cat.	1
MTTFd [a]	100 (High)
DCavg [%]	not relevant
CCF	not relevant

Channel 1

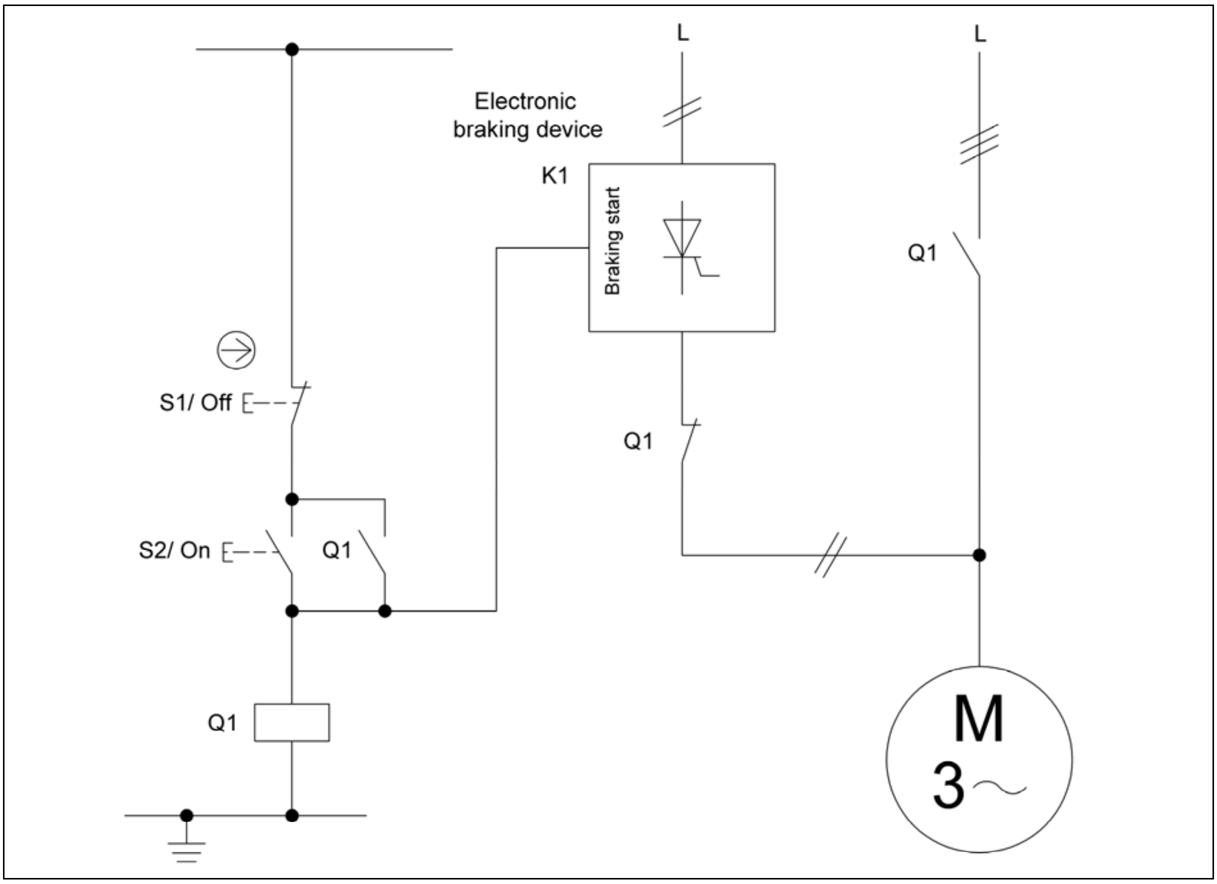
Name	DC [%]	MTTFd [a]
BL Valve 1V3	not relevant	150 (-)

Channel 2

Name	DC [%]	MTTFd [a]

8.2.4 Stopping of woodworking machines – Category 1 – PL c (Example 4)

Figure 8.9:
Combination of electromechanical control equipment and a simple electronic braking device for the stopping of woodworking machines

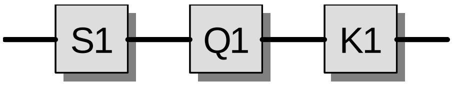


Safety function

- Actuation of the Off button leads to SS1 (safe stop 1), a controlled stopping of the motor within a maximum permissible time.

Functional description

- Stopping of the motor is initiated by actuation of the Off button S1. The motor contactor Q1 drops out and the braking function is initiated. The motor is braked by a direct current generated in braking unit K1 by a thyristor employing phase-angle control and generating a braking torque in the motor winding.
- The run-down time must not exceed a maximum value (e.g. 10 seconds). The level of braking current required for this purpose can be set by means of a potentiometer on the braking unit.



- Upon expiration of the maximum braking time, the control signal to the thyristor ceases and the current path for the braking current is interrupted. The stopping process corresponds to a Category 1 stop in accordance with EN 60204-1.
- The safety function cannot be maintained with all component failures, and is dependent upon the reliability of the components.
- No measures for fault detection are implemented.

Design features

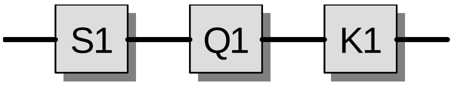
- Basic and well-tried safety principles are observed and the requirements of Category B are met. Protective circuits (e.g. contact protection) as described in the initial paragraphs of Chapter 8 are implemented. The de-energization principle (closed-circuit current) is employed as the basic safety principle. For protection against unexpected start-up following restoration of the power supply, the control system features latching-in at Q1.
- S1 is a pushbutton with positive mode of actuation to IEC 60947-5-1, Annex K (direct opening action). S1 is therefore regarded as a well-tried component.
- Contactor Q1 is a well-tried component provided the additional conditions in accordance with Table D.4 of EN ISO 13849-2 are observed.
- The braking unit K1 is designed exclusively from simple electronic components such as transistors, capacitors, diodes, resistors and thyristors, which are regarded as well-tried components. Fault-free performance of the safety-related braking function is characterized by the selection of the components. Internal measures for fault detection are not implemented. No complex electronic components (e.g. microprocessors) are employed that are not considered to be in accordance with EN ISO 13849-1, Section 6.2.4 as being equivalent to well-tried components.

Application

- On woodworking machines or similar machines on which unbraked stopping would result in an impermissibly long run-down of the hazardous tool movements. The control system must be designed such that at least PL b is attained (GS-HO-01 test principles for woodworking machines).

Calculation of the probability of failure

- S1 is a pushbutton with positive mode of actuation to IEC 60947-5-1, Annex K (direct opening action). If a pushbutton of this type is employed as a control device, fault exclusion is possible for failure of the electrical contact to open, including the mechanical components within the push-button.
- $MTTF_d$: a B_{10d} value of 2,000,000 switching operations [S] is assumed at nominal load for the contactor Q1. At 300 working days, 8 working hours and a cycle time of 2 minutes, n_{op} is 72,000 cycles per year and the $MTTF_d$ is



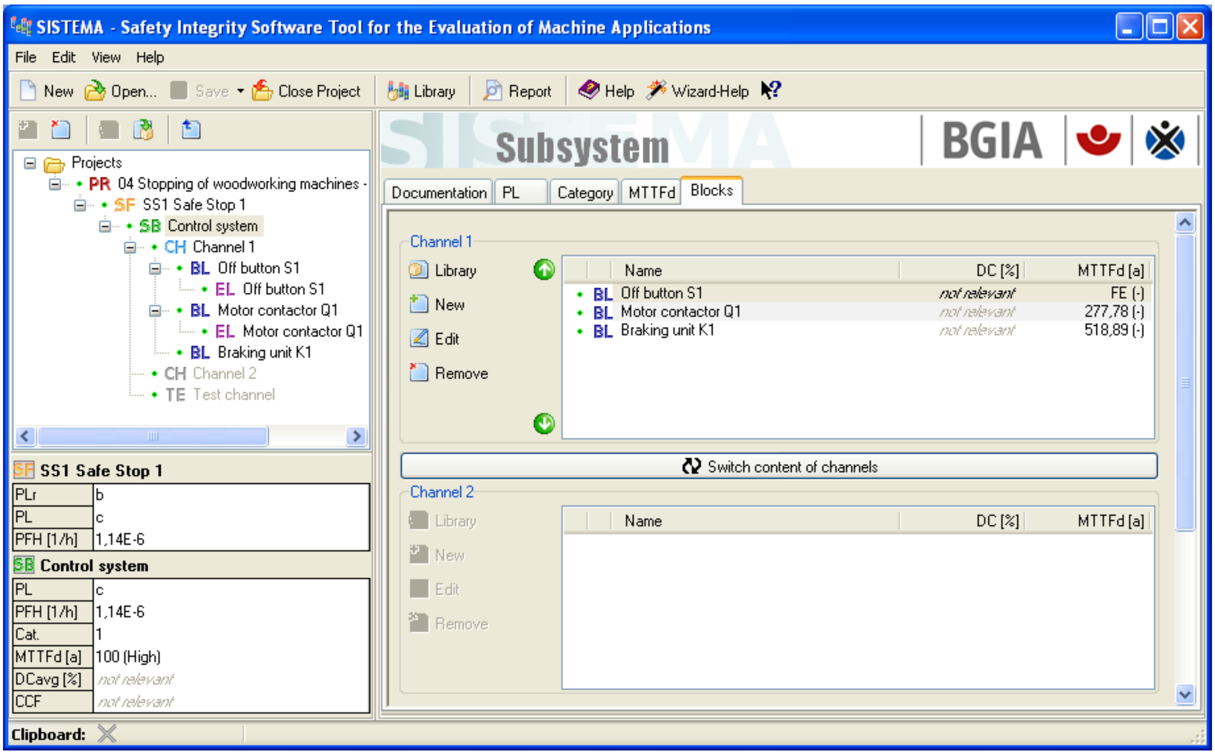
277 years. The $MTTF_d$ for the braking unit K1 was determined by means of the parts count method. The parts information from the parts list and the values from the SN 29500 database [36] produce an $MTTF_d$ of 518 years [D]. The combination of Q1 and K1 results in an $MTTF_d$ of 180 years for the channel, which is capped to 100 years ("high").

- DC_{avg} and measures against common cause failures are not relevant in Category 1.
- The electromechanical control system corresponds to Category 1 with a high $MTTF_d$ (100 years). This results in an average probability of dangerous failure of 1.14 × 10^{-6} per hour. This corresponds to PL c. The PL_r of b is therefore surpassed.

More detailed reference

- Grundsätze für die Prüfung und Zertifizierung von Holzbearbeitungsmaschinen GS-HO-01 (12/2007). www.dguv.de, Webcode d14898

Figure 8.10:
Determining of the PL by means of SISTEMA



Projects
- PR 04 Stopping of woodworking machines -
  - SF SS1 Safe Stop 1
    - SB Control system
      - CH Channel 1
        - BL Off button S1
          - EL Off button S1
        - BL Motor contactor Q1
          - EL Motor contactor Q1
        - BL Braking unit K1
      - CH Channel 2
      - TE Test channel

SF SS1 Safe Stop 1

PLr	b
PL	c
PFH [1/h]	1,14E-6

SB Control system

PL	c
PFH [1/h]	1,14E-6
Cat.	1
MTTFd [a]	100 (High)
DCavg [%]	not relevant
CCF	not relevant

Channel 1

	Name	DC [%]	MTTFd [a]
BL	Off button S1	not relevant	FE (-)
BL	Motor contactor Q1	not relevant	277,78 (-)
BL	Braking unit K1	not relevant	518,89 (-)

Channel 2

	Name	DC [%]	MTTFd [a]

8.2.5 Position monitoring of moveable guards – Category 1 – PL c (Example 5)

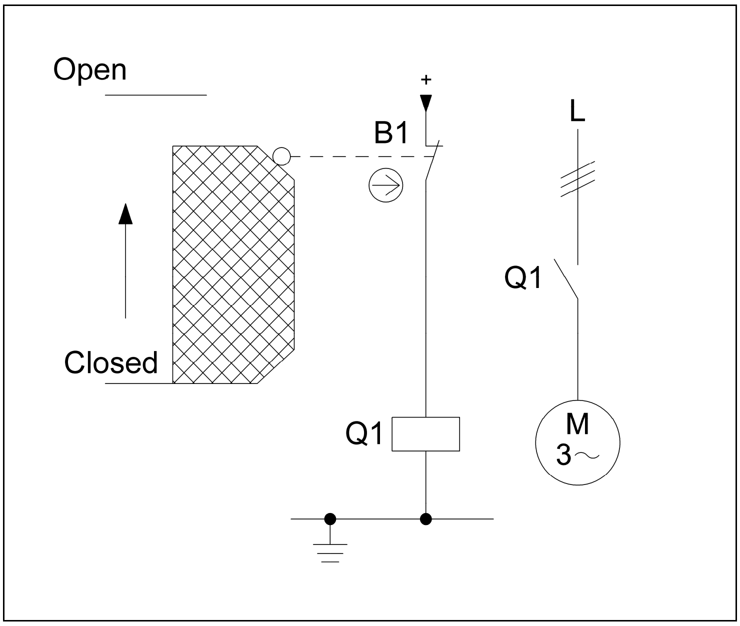


Figure 8.11:
Position monitoring of moveable guards for the prevention of hazardous movements (STO – safe torque off)

Safety function

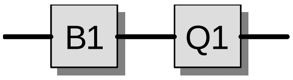
- Safety-related stop function, initiated by a protective device: opening of the moveable guard initiates the safety function STO – safe torque off.

Functional description

- Opening of the moveable guard (e.g. safety guard) is detected by a position switch B1 with direct opening action which actuates a contactor Q1. The dropping out of Q1 interrupts or prevents hazardous movements or states.
- The safety function cannot be maintained with all component failures, and is dependent upon the reliability of the components.
- No measures for fault detection are implemented.
- Removal of the protective device is not detected.

Design features

- Basic and well-tried safety principles are observed and the requirements of Category B are met. Protective circuits (e.g. contact protection) as described in the initial paragraphs of Chapter 8 are implemented. The closed-circuit current principle is employed as a basic safety principle. Earthing of the control circuit is regarded as a well-tried safety principle.



- Switch B1 is a position switch with direct opening action in accordance with IEC 60947-5-1, Annex K and is therefore regarded as a well-tried component. The break contact interrupts the circuit directly mechanically when the protective device is not in the safe position.
- Contactor Q1 is a well-tried component provided that the additional conditions in accordance with Table D.4 of EN ISO 13849-2 are observed.
- A position switch is employed for position monitoring. A stable arrangement of the protective device is assured for actuation of the position switch. The actuating elements of the position switch are protected against displacement. Only rigid mechanical parts (no spring elements between actuator and contact) are employed.
- The actuating stroke for the position switch complies with the manufacturer's specification.

Calculation of the probability of failure

- $MTTF_d$: fault exclusion for the direct opening electrical contact is possible for B1. A B_{10d} value of 1,000,000 cycles [M] is stated for the mechanical part of B1. At 365 working days, 16 working hours per day and a cycle time of 10 minutes, n_{op} is 35,045 cycles per year and the $MTTF_d$ is 285 years for these components. For contactor Q1, the B_{10} value corresponds under inductive load (AC 3) to an electrical lifetime of 1,300,000 switching cycles [M]. If 50% of failures are assumed to be dangerous, the B_{10d} value is produced by doubling of the B_{10} value. The above assumed value for n_{op} results in an $MTTF_d$ of 742 years for Q1. The combination of B1 and Q1 results in an $MTTF_d$ of 206 years for the channel. This value is capped to 100 years (“high”).
- DC_{avg} and measures against common cause failures are not relevant in Category 1.
- The electromechanical control system corresponds to Category 1 with a high $MTTF_d$ (100 years). This results in an average probability of dangerous failure of 1.14×10^{-6} per hour. This corresponds to PL c. The PL_r of b is therefore surpassed.

More detailed reference

- IEC 60947-5-1: Low-voltage switchgear and controlgear – Part 5-1: Control circuit devices and switching elements – Electromechanical control circuit devices (11.03)

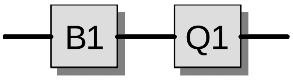
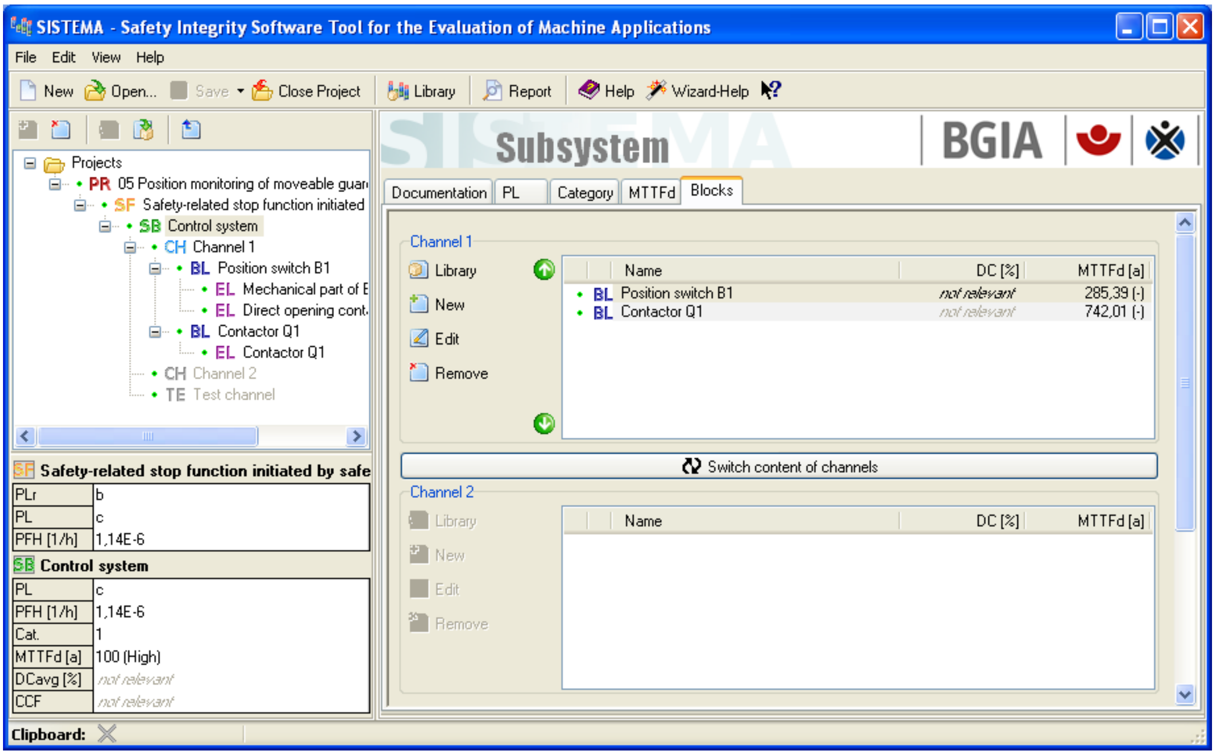


Figure 8.12:
Determining of the PL by means of SISTEMA


SISTEMA - Safety Integrity Software Tool for the Evaluation of Machine Applications
File Edit View Help
New Open... Save Close Project Library Report Help Wizard-Help
Subsystem
BGIA
Documentation PL Category MTTFd Blocks
Library
New
Edit
Remove
Switch content of channels
Clipboard:

- Projects
  - PR 05 Position monitoring of moveable guar
    - SF Safety-related stop function initiated
      - SB Control system
        - CH Channel 1
          - BL Position switch B1
            - EL Mechanical part of E
            - EL Direct opening cont
          - BL Contactor Q1
            - EL Contactor Q1
        - CH Channel 2
        - TE Test channel

SF Safety-related stop function initiated by safe

PLr	b
PL	c
PFH [1/h]	1,14E-6

SB Control system

PL	c
PFH [1/h]	1,14E-6
Cat.	1
MTTFd [a]	100 (High)
DCavg [%]	not relevant
CCF	not relevant

Channel 1

	Name	DC [%]	MTTFd [a]
BL	Position switch B1	not relevant	285,39 (-)
BL	Contactor Q1	not relevant	742,01 (-)

Channel 2

	Name	DC [%]	MTTFd [a]

8.2.6 Start/stop facility with emergency stop device – Category 1 – PL c (Example 6)

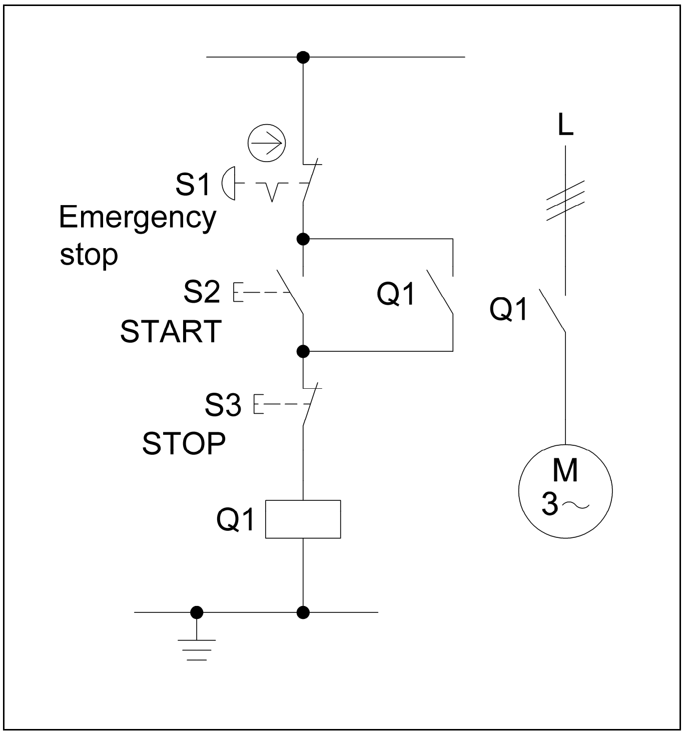


Figure 8.13:
Combined start/stop facility with emergency stop device

Safety function

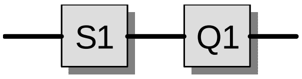
- Emergency stop function, STO – safe torque off by actuation of the emergency stop device

Functional description

- Hazardous movements or states are de-energized by interruption of the control voltage of contactor Q1 when the emergency stop device S1 is actuated.
- The safety function cannot be maintained with all component failures, and is dependent upon the reliability of the components.
- No measures for fault detection are implemented.

Design features

- Basic and well-tried safety principles are observed and the requirements of Category B are met. Protective circuits (e.g. contact protection) as described in the initial paragraphs of Chapter 8 are implemented. The closed-circuit current principle is employed as a basic safety principle. The control circuit is also earthed, as a well-tried safety principle.



- The emergency stop device S1 is a switch with direct mode of actuation in accordance with IEC 60947-5-1, Annex K, and is therefore a well-tried component in accordance with Table D.4 of EN ISO 13849-2.
- The signal is processed by a contactor (stop category 0 to EN 60204-1).
- Contactor Q1 is a well-tried component provided the additional conditions in accordance with Table D.4 of EN ISO 13849-2 are observed.

Remark

- The function for stopping in an emergency is a protective measure which complements the safety functions for the safeguarding of hazardous zones.

Calculation of the probability of failure

- $MTTF_d$: S1 is a standard emergency stop device to EN ISO 13850. Fault exclusion applies for the direct opening contact and the mechanical elements, provided the number of operations indicated in Table D.2 of this report is not exceeded. For contactor Q1, the B_{10} value corresponds under inductive load (AC 3) to an electrical lifetime of 1,300,000 switching operations [M]. If 50% of failures are assumed to be dangerous, the B_{10d} value is produced by doubling of the B_{10} value. If the start/stop facility is assumed to be actuated twice a day on 365 working days and the emergency stop device to be actuated three times a year, then at an n_{op} of 733 cycles per year, Q1 has an $MTTF_d$ of 35,470 years. This is also the $MTTF_d$ for the channel, which is capped to 100 years (“high”).
- DC_{avg} and measures against common cause failures are not relevant in Category 1.
- The electromechanical control system corresponds to Category 1 with a high $MTTF_d$ (100 years). This results in an average probability of dangerous failure of 1.14×10^{-6} per hour. This corresponds to PL c.

More detailed references

- EN ISO 13850: Safety of machinery – Emergency stop – Principles for design (11.06)
- EN 60204-1: Safety of machinery – Electrical equipment of machines. Part 1: General requirements (06.06)

8.2.7 Undervoltage tripping by means of an emergency stop device – Category 1 – PL c (Example 7)

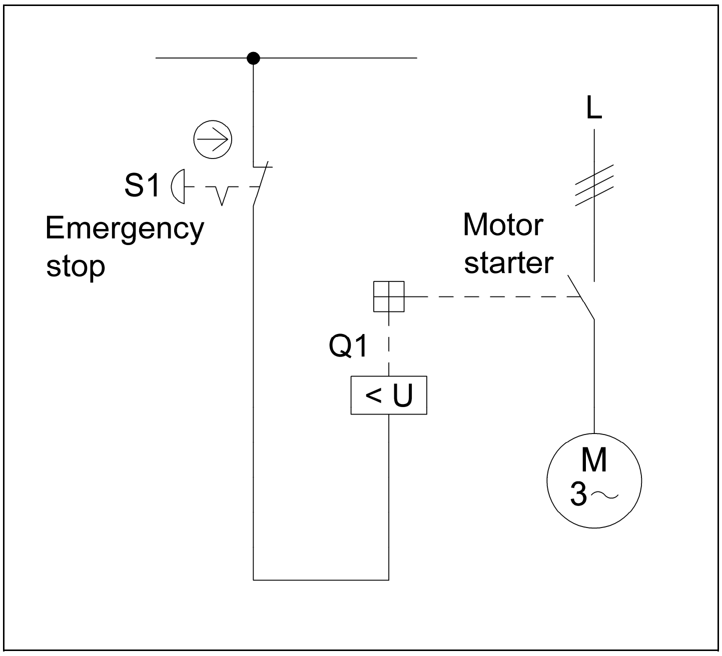


Figure 8.14:
Emergency stop device acting upon the undervoltage release of the supply disconnecting device (motor starter)

Safety function

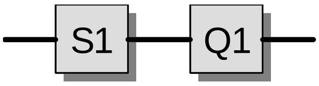
- Emergency stop function, STO (safe torque off) by actuation of the emergency stop device which acts upon the undervoltage release of a motor starter, where appropriate the supply disconnecting device.

Functional description

- Hazardous movements or states are interrupted by actuation of the emergency stop device S1 by undervoltage tripping of the supply disconnecting device, in this case in the form of a motor starter Q1.
- The safety function cannot be maintained with all component failures, and is dependent upon the reliability of the components.
- No measures for fault detection are implemented.

Design features

- Basic and well-tried safety principles are observed and the requirements of Category B are met. Protective circuits (e.g. contact protection) as described in the initial sections of Chapter 8 are implemented. The closed-circuit current principle of the undervoltage release is employed as the basic safety principle.
- The emergency stop device S1 is a switch with direct mode of actuation in accordance with IEC 60947-5-1, Annex K, and is therefore a well-tried component in accordance with Table D.4 of EN ISO13849-2.



- The motor starter Q1 is to be considered equivalent to a circuit-breaker in accordance with Table D.4 of EN ISO 13849-2. Q1 may therefore be regarded as a well-tried component.
- The power supply to the entire machine is switched off (stop category 0 to EN 60204-1).

Remark

- The emergency stop function is a protective measure which supplements the safety functions for the safeguarding of hazardous zones.

Calculation of the probability of failure

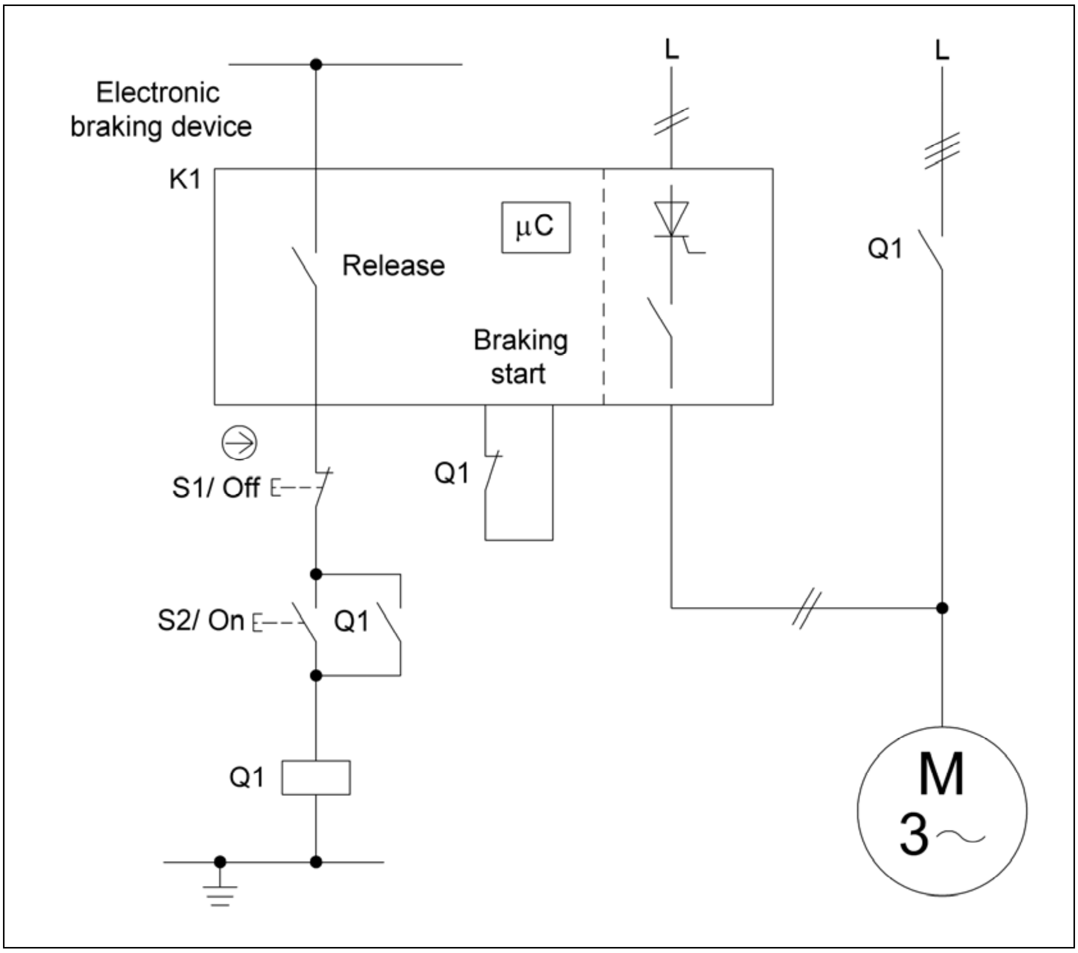
- $MTTF_d$: S1 is a standard emergency stop device to EN ISO 13850. Fault exclusion applies for the direct opening contact and the mechanical elements, provided the number of operations indicated in Table D.2 of this report is not exceeded. For the undervoltage release of the motor starter Q1, the B_{10} value approximates to the electrical lifetime of 10,000 switching operations [M]. If 50% of failures are assumed to be dangerous, the B_{10d} value is produced by doubling of the B_{10} value. At actuation of the emergency stop device three times a year and an n_{op} of 3 cycles per year, Q1 has an $MTTF_d$ of 66,666 years. This is also the $MTTF_d$ for the channel, which is capped to 100 years ("high").
- DC_{avg} and measures against common cause failures are not relevant in Category 1.
- The electromechanical control system corresponds to Category 1 with a high $MTTF_d$ (100 years). This results in an average probability of dangerous failure of 1.14×10^{-6} per hour. This corresponds to PL c.

More detailed references

- EN ISO 13850: Safety of machinery – Emergency stop – Principles for design (11.06)
- EN 60204-1: Safety of machinery – Electrical equipment of machines. Part 1: General requirements (06.06)

8.2.8 Stopping of woodworking machines – Category 1 – PL c (Example 8)

Figure 8.15:
Combination of electromechanical control equipment and a programmable electronic braking device for the stopping of woodworking machines

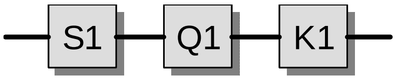


Safety function

- Actuation of the Off button leads to SS1 (safe stop 1), a controlled stopping of the motor within a maximum permissible time.

Functional description

- Stopping of the motor is initiated by actuation of the Off button S1. The motor contactor Q1 drops out and the braking function is initiated. The motor is braked by a direct current generated in braking unit K1 by thyristors employing phase-angle control, and which is connected to the motor winding by internal relays.
- The run-down time must not exceed a maximum value (e.g. 10 seconds). The desired run-down time and any other required parameters (e.g. braking current, threshold for zero-speed detection) can be set on the braking device.



- Once the motor is stationary or upon expiration of the maximum braking time, the braking device switches off the braking current and disconnects the motor again from the supply. The stopping process corresponds to a Category 1 stop in accordance with EN 60204-1.
- The safety function cannot be maintained with all component failures, and is dependent upon the reliability of the components.
- Fault-free performance of the braking function is monitored regularly by the braking device K1. Should a fault be detected, e.g. exceeding of the maximum permissible braking time, a release contact in the device prevents the motor from restarting. Measures for fault detection are not implemented in S1 or Q1.

Design features

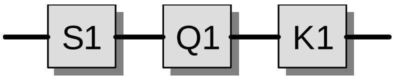
- Basic and well-tried safety principles are observed and the requirements of Category B are met. Protective circuits (e.g. contact protection) as described in the initial paragraphs of Chapter 8 are implemented. The de-energization principle (closed-circuit current) is employed as the basic safety principle. For protection against unexpected start-up following restoration of the power supply, the control system features latching-in at Q1.
- S1 is a pushbutton with direct mode of actuation to IEC 60947-5-1, Annex K (direct opening action). S1 is therefore regarded as a well-tried component.
- Contactor Q1 is a well-tried component provided the additional conditions in accordance with Table D.4 of EN ISO 13849-2 are observed.
- The braking device K1, which is controlled by a microcontroller, meets all requirements for Category 2 and PL c. The safety-related functions are tested at regular intervals. The program sequence timing of the microcontroller is monitored by a separate watchdog.

Application

- On woodworking machines or similar machines on which unbraked stopping would result in an impermissibly long run-down of the hazardous tool movements. The control system must be designed such that at least Performance Level b is attained (GS-HO-01 “Test principles for woodworking machines”).

Calculation of the probability of failure

- Since a standard module is employed for the electronic braking device K1, its probability of failure (5.28×10^{-7} per hour [M]) is added following calculation by SISTEMA. For the remaining part of the control system, the probability of failure is calculated below.
- S1 is a pushbutton with direct mode of actuation to IEC 60947-5-1, Annex K (direct opening action). If a pushbutton of this type is employed as a control device, fault exclusion is possible for failure of the electrical contact to open, including for the mechanical components within the push-button.

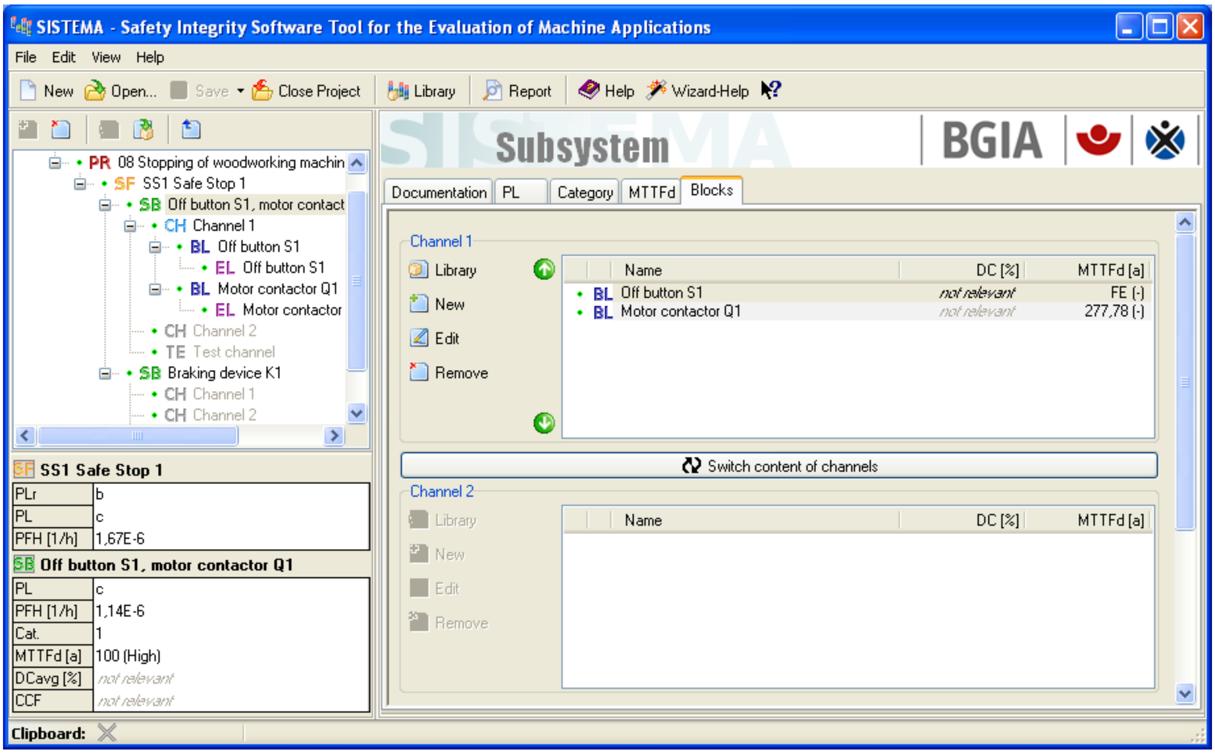


- *MTTF*$_d$: a B$_{10d}$ value of 2,000,000 switching operations [S] at nominal load is assumed for the contactor Q1. At 300 working days, 8 working hours and a cycle time of 2 minutes, n_{op} is 72,000 cycles per year and the *MTTF*$_d$ is 277 years. This is also the *MTTF*$_d$ for the channel, which is capped to 100 years ("high").
- *DC*$_{avg}$ and measures against common cause failures are not relevant in Category 1.
- The electromechanical control system, consisting of S1 and Q1, corresponds to Category 1 with a high *MTTF*$_d$ (100 years). This results in an average probability of dangerous failure of 1.14 × 10^{-6} per hour. Following addition of the subsystem K1, the average probability of dangerous failure is 1.67 × 10^{-6} per hour. This corresponds to PL c. The PL$_r$ of b is therefore surpassed.

More detailed reference

- Grundsätze für die Prüfung und Zertifizierung von Holzbearbeitungsmaschinen GS-HO-01 (12/2007). www.dguv.de, Webcode d14898

Figure 8.16:
Determining of the PL by means of SISTEMA



SISTEMA - Safety Integrity Software Tool for the Evaluation of Machine Applications

- PR 08 Stopping of woodworking machin
  - SF SS1 Safe Stop 1
    - SB Off button S1, motor contact
      - CH Channel 1
        - BL Off button S1
          - EL Off button S1
        - BL Motor contactor Q1
          - EL Motor contactor
      - CH Channel 2
      - TE Test channel
    - SB Braking device K1
      - CH Channel 1
      - CH Channel 2

SF SS1 Safe Stop 1

PLr	b
PL	c
PFH [1/h]	1,67E-6

SB Off button S1, motor contactor Q1

PL	c
PFH [1/h]	1,14E-6
Cat.	1
MTTFd [a]	100 (High)
DCavg [%]	not relevant
CCF	not relevant

Subsystem

Channel 1

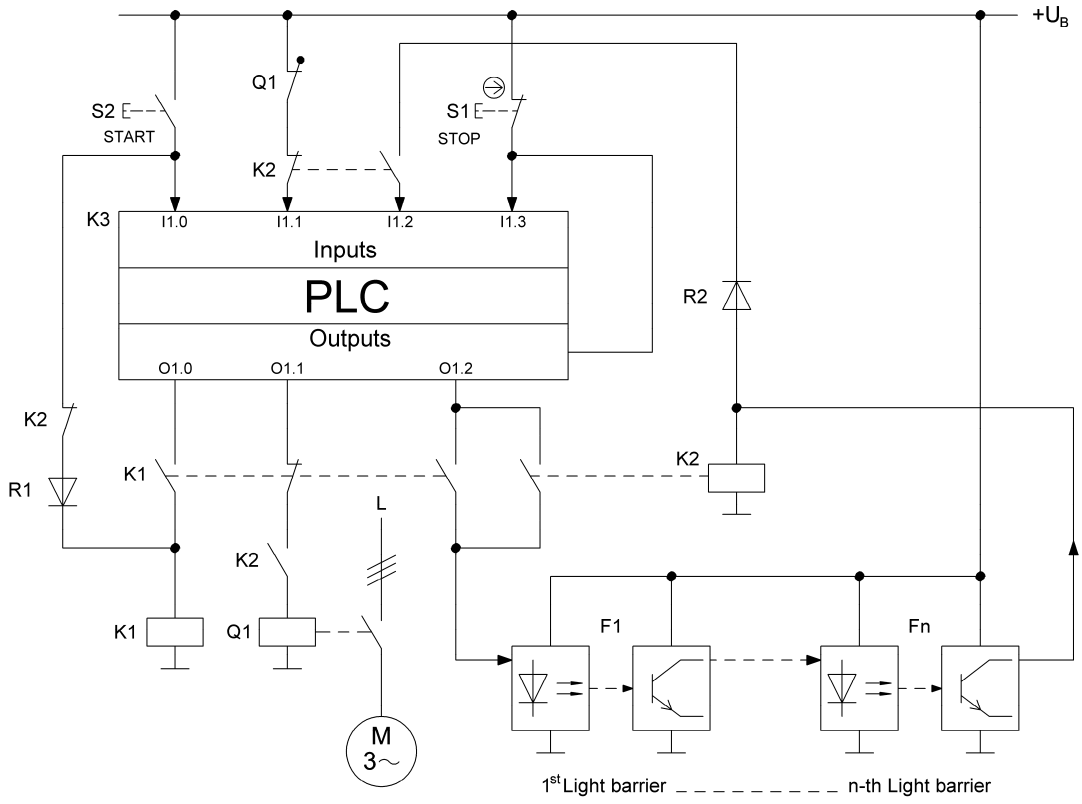
Name	DC [%]	MTTFd [a]
BL Off button S1	not relevant	FE (-)
BL Motor contactor Q1	not relevant	277,78 (-)

Channel 2

Name	DC [%]	MTTFd [a]

8.2.9 Tested light barriers – Category 2 – PL c with downstream Category 1 output signal switching device (Example 9)

Figure 8.17:
Testing of light barriers with a standard PLC

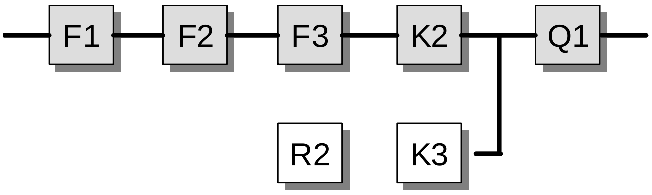


Safety function

- Safety-related stop function, initiated by a protective device: when the light beam is interrupted, a hazardous movement is halted (STO – safe torque off).

Functional description

- Interruption of the light beam of the *n* cascaded light barriers F1 to Fn triggers a de-energization command both by relays, by de-energization of the contactor relay K2, and via the PLC output (O1.1) of the test channel. The hazardous movement is then halted by means of the contactor Q1.
- The light barriers are tested before each start of the hazardous movement following pressing of the start button S2. For this purpose, PLC output O1.2 de-energizes the light barrier transmitter in response to a software command. The reaction of the receiver (K2 drops out again) is monitored on PLC inputs I1.1 and I1.2. Provided the behaviour is free of faults, K2 seals in via O1.2, and

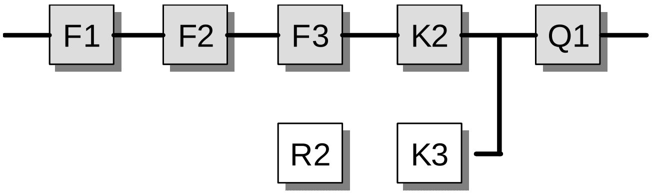


the hazardous movement can be initiated by the releasing of S2. K1 is de-energized via O1.0, and the main contactor Q1 actuated via O1.1.

- Should a fault in a light barrier or in K2 be detected by the test, the outputs O1.1 and O1.2 are deactivated, and an actuating signal is no longer applied to the main contactor Q1.
- In the event of global failure of the PLC (output O1.0 at low potential, outputs O1.1 and O1.2 at high potential), interruption of a light beam results in de-energization of K2, independently of the PLC. In order to ensure this independence, the light barrier outputs are decoupled from the PLC by the decoupling diode R2. Under unfavourable circumstances, the light barriers can be re-activated by K2 by actuation of the start button, and the main contactor Q1 thus actuated. In this case the test equipment (only) would have failed. Failure of the test equipment is detected owing to the probability of a functionally defective process under these circumstances.
- During the test, actuation of Q1 by K1 and O1.1 is blocked.

Design features

- Basic and well-tried safety principles are observed and the requirements of Category B are met. Protective circuits (e.g. contact protection) as described in the initial paragraphs of Chapter 8 are implemented.
- Special light barriers with adequate optical characteristics (aperture angle, extraneous light immunity, etc.) to IEC 61496-2 are employed.
- Several light barriers can be cascaded and monitored by only two PLC inputs and a relay or contactor relay.
- The contactor relays K1 and K2 possess mechanically linked contact elements in accordance with IEC 60947-5-1, Annex L. The contactor Q1 possesses a mirror contact in accordance with IEC 60947-4-1, Annex F.
- The standard components F1 to Fn and K3 are employed in accordance with the instructions in Section 6.3.10.
- The software (SRASW) is programmed in accordance with the requirements for PL b (downgraded owing to diversity) and the instructions in Section 6.3.
- The start button S2 must be located outside the hazardous area and at a point from which the hazardous area/danger point is visible.
- The number, arrangement and height of the light beams must comply with EN 999 and IEC 62046.



- Should an arrangement for the safeguarding of hazardous areas permit stepping behind the sensing field, further measures are required, such as a restart interlock. The start button S2 can be used for this purpose. To this end, the PLC K3 compares the duration for which the button is pressed with maximum and minimum values. Only if the conditions are met is a start command assumed to be valid.

Remarks

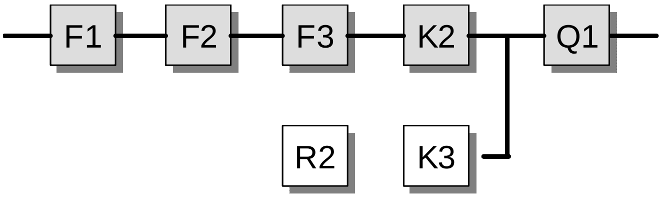
- The example is intended for use in applications with an infrequent demand upon the safety function. This enables the requirement of the designated architecture for Category 2 to be satisfied, i.e. “testing much more frequent than the demand upon the safety function” (cf. Annex G).
- Following triggering of a stop, the light barriers remain deactivated until the next start. This enables a hazardous area, for example, to be entered without this being “registered” by the circuit. The behaviour can be modified by corresponding adaptation of the circuit.

Calculation of the probability of failure

- For the sake of example, three light barriers F1 to F3 are considered for calculation of the probability of failure. Safeguarding of a second hazardous zone constitutes a further safety function for which calculation is performed separately.
- For calculation of the probability of failure, the overall system is divided into two subsystems, “light barriers” and “main contactor” (Q1).

For the “light barriers” subsystem:

- F1, F2, F3 and K2 constitute the functional path of the Category 2 circuit structure; the PLC K3 (including decoupling diode R2) constitutes the test equipment. S2 and K1 have the function of activating testing of the light barrier, and are not involved in the calculation of the probability of failure.
- $MTTF_d$: an $MTTF_d$ of 100 years [E] is assumed for each of F1 to F3. The B_{10d} value for K2 is 20,000,000 cycles [S]. At 240 working days, 16 working hours and a cycle time of 180 seconds, n_{op} is 76,800 cycles per year. Testing as described above doubles this value, to an n_{op} of 153,600 cycles per year with an $MTTF_d$ of 1,302 years for K2. These values yield an $MTTF_d$ of 32 years (“high”) for the functional channel. An $MTTF_d$ of 50 years [E] is assumed for K3. In comparison, the $\mathrm{MTTF_d}$ value of 228,311 years [S] for the decoupling diode R2 is irrelevant.



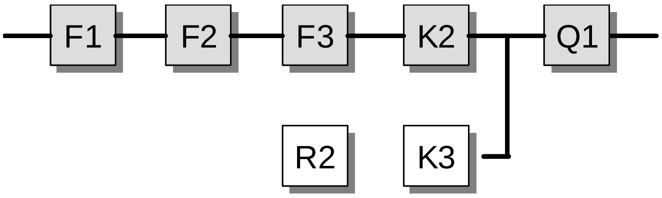
- DC_{avg}: the DC of 60% for F1 to F3 is attributable to the function test as described. The *DC* of 99% for K2 is derived from direct monitoring in K3 with the aid of mechanically linked contact elements. The averaging formula for DC_{avg} returns a result of 61.0% ("low").
- Adequate measures against common cause failure (85 points): separation (15), diversity (20), overvoltage protection etc. (15) and environmental conditions (25 + 10)
- The combination of the control elements in the "light barriers" subsystem corresponds to Category 2 with a high $MTTF_d$ per channel (32.5 years) and low DC_{avg} (61.0%). This results in an average probability of dangerous failure of 1.85 × 10^{-6} per hour.

The following assumptions are made for the "main contactor" subsystem:

- B_{10d} = 2,000,000 cycles [S] with a n_{op} of 76,800 cycles per year. This leads to an $MTTF_d$ of 260.4 years, which in accordance with the standard is capped to 100 years. The structure corresponds to Category 1; DC_{avg} and common cause failures are not therefore relevant. The resulting average probability of dangerous failure is 1.14 × 10^{-6} per hour.
- Addition of the average probability of dangerous failure of the two subsystems results in a value of 3.0 × 10^{-6} per hour. This corresponds to PL c.
- If it is anticipated that a demand will be made upon the safety function more frequently than assumed for the Category 2 designated architecture (the ratio is lower than 100 : 1, i.e. more frequently than once every 5 hours), this can be considered in accordance with Annex G down to a ratio of 25 : 1 with a penalty of 10%. In the case considered here with three light barriers, the "light barriers" subsystem still attains a probability of failure of 2.04 × 10^{-6} per hour. The overall average probability of dangerous failure of 3.18 × 10^{-6} per hour only attains PL b, however. For PL c to be attained, the number of light barriers would for example have to be reduced, or components with a higher $MTTF_d$ employed.

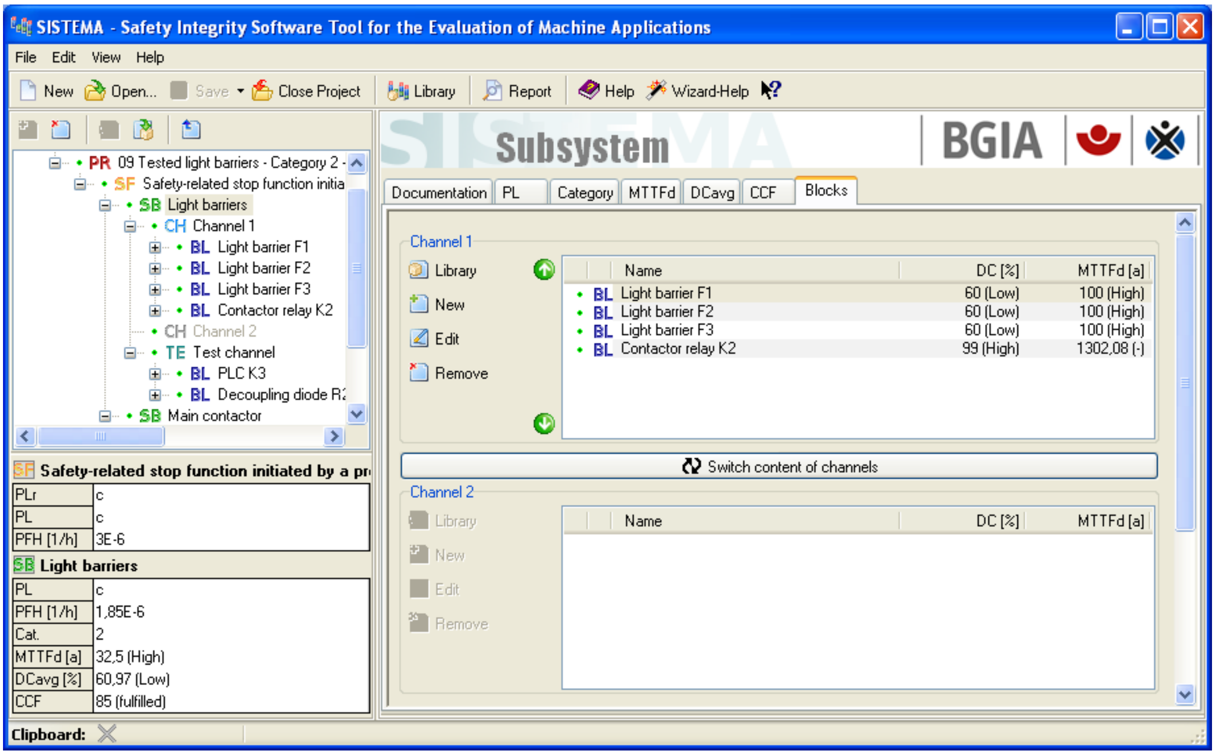
More detailed references

- *Grigulewitsch, W.; Reinert, D.*: Lichtschranken mit Testung. In: BGIA-Handbuch Sicherheit und Gesundheitsschutz am Arbeitsplatz. Kennzahl 330 228. 22th suppl. V/94. Ed.: BGIA – Institut für Arbeitsschutz der Deutschen Gesetzlichen Unfallversicherung, Sankt Augustin. Erich Schmidt, Berlin, 1985 – loose-leaf ed. www.bgia-handbuchdigital.de/330228
- EN 61496-1: Safety of machinery – Electro-sensitive protective equipment – Part 1: General requirements and tests (05.04)



- IEC 61496-2: Safety of machinery – Electro-sensitive protective equipment – Part 2: Particular requirements for equipment using active opto-electronic protective devices (AOPDs) (04.06)
- IEC 62046: Safety of machinery – Application of protective equipment to detect the presence of persons (draft standard IEC 44/501/CD:2005)
- EN 999: Safety of machinery – The positioning of protective equipment in respect of approach speeds of parts of the human body (10.98)

Figure 8.18:
Determining of the PL by means of SISTEMA



PR 09 Tested light barriers - Category 2 -
SF Safety-related stop function initia
SB Light barriers
CH Channel 1
BL Light barrier F1
BL Light barrier F2
BL Light barrier F3
BL Contactor relay K2
CH Channel 2
TE Test channel
BL PLC K3
BL Decoupling diode R2
SB Main contactor

SF Safety-related stop function initiated by a pr

PLr	c
PL	c
PFH [1/h]	3E-6

SB Light barriers

PL	c
PFH [1/h]	1,85E-6
Cat.	2
MTTFd [a]	32,5 (High)
DCavg [%]	60,97 (Low)
CCF	85 (fulfilled)

Channel 1

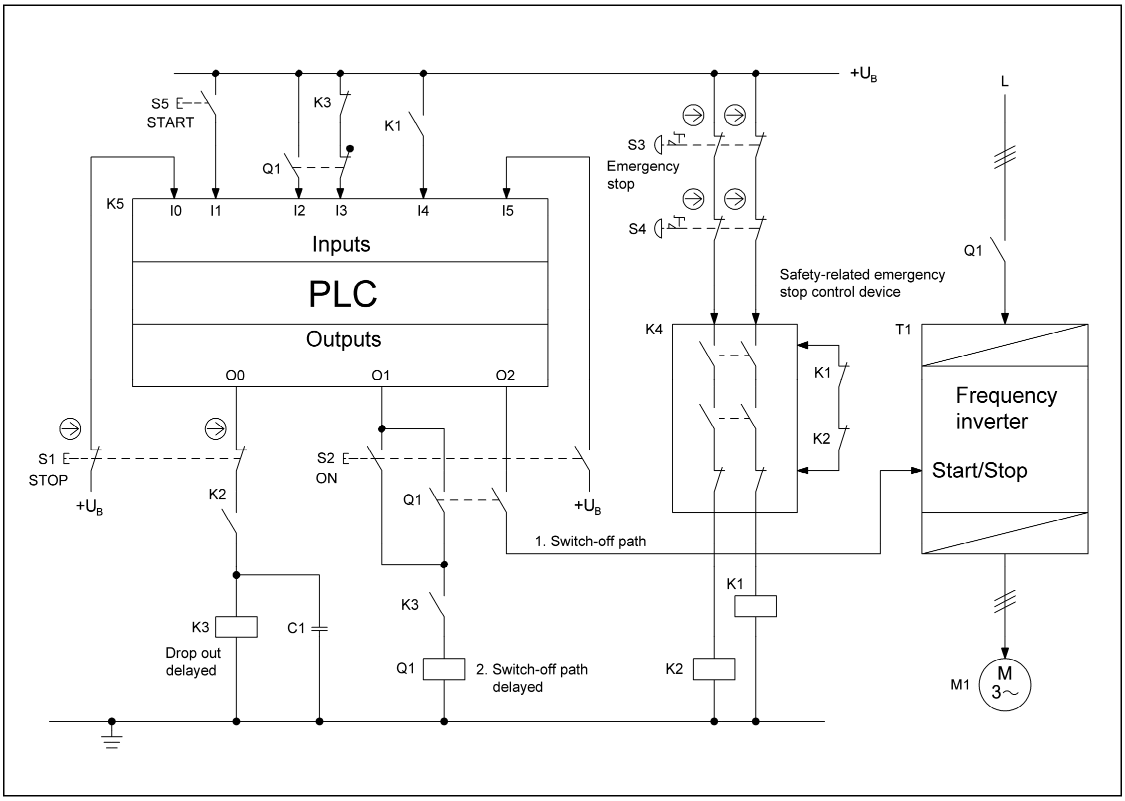
Name	DC [%]	MTTFd [a]
BL Light barrier F1	60 (Low)	100 (High)
BL Light barrier F2	60 (Low)	100 (High)
BL Light barrier F3	60 (Low)	100 (High)
BL Contactor relay K2	99 (High)	1302,08 (-)

Channel 2

Name	DC [%]	MTTFd [a]

8.2.10 Safe stopping of a PLC-driven drive with emergency stop – Category 3 – PL c (Example 10)

Figure 8.19:
Stopping of a PLC-driven frequency inverter drive following a stop or emergency stop command

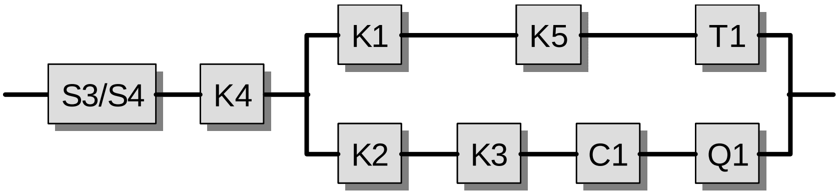


Safety function

- Safety-related stop function/emergency stop function: following a stop or emergency stop command, the drive is halted (SS1 – safe stop 1).

Functional description

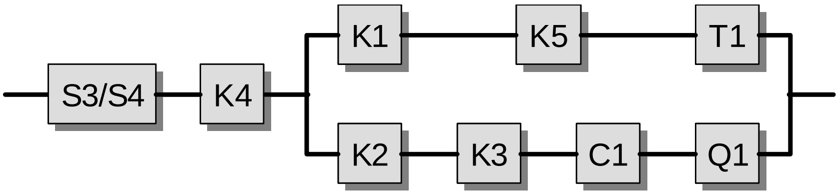
- The hazardous movement is interrupted redundantly if either the stop button S1 or one of the emergency stop devices S3 or S4 is actuated. The drive is halted in an emergency following actuation of S3/S4, resulting in deactivation of the safety-related emergency stop control device K4 and de-energization of the contactor relays K1 and K2. Opening of the make contact K1 on input I4 of the PLC K5 causes the starting signal on the frequency inverter (FI) T1 to be cancelled via the PLC output O2. Redundantly to the K1-K5-T1 chain, opening of the make contact K2 upstream of the contactor relay K3 (with drop-out delay) initiates a braking timer. Upon timeout of the braking timer the actuating signal for the mains contactor Q1 is interrupted. The timer setting is selected such that under unfavourable operating conditions, the machine movement is halted before the mains contactor Q1 has dropped out.



- Functional stopping of the drive following a stop command is caused by the opening of the two break contacts of the stop button S1. As with stopping in an emergency, the status is first queried by PLC K5, in this case via input I0, and the FI is shut down by resetting of the PLC output O2. Redundantly to this process, the contactor relay K3 is de-energized – with drop-out delay provided by the capacitor C1 – and following timeout of the set braking time, the activation signal to mains contactor Q1 is interrupted.
- In the event of failure of the PLC K5, the frequency inverter T1, the mains contactor Q1, the contactor relays K1/K2 or the contactor relay with drop-out delay K3, stopping of the drive is assured since two mutually independent de-energization paths are always present. Failure of the contactor relays K1 and K2 to drop out is detected, at the latest, following resetting of the actuated emergency stop device. This is achieved by monitoring of the mechanically linked break contacts within the safety-related emergency stop control device K4. Failure of the auxiliary contactor K3 to drop out is detected, at the latest, before renewed start-up of the machine movement through feedback of the mechanically linked break contact to the PLC input I3. Failure of the mains contactor Q1 to drop out is detected by the mirror contact read in on PLC input I3.

Design features

- Basic and well-tried safety principles are observed and the requirements of Category B are met. Protective circuits (e.g. contact protection) as described in the initial paragraphs of Chapter 8 are implemented.
- The contactor relays K1, K2 and K3 possess mechanically linked contact elements in accordance with IEC 60947-5-1, Annex L.
- The contacts of the pushbuttons S1, S3 and S4 are mechanically linked in accordance with IEC 60947-5-1, Annex K.
- The contactor Q1 possesses a mirror contact according to IEC 60947-4-1, Annex F.
- The standard components K5 and T1 are employed in accordance with the instructions in Section 6.3.10.
- The software (SRASW) is programmed in accordance with the requirements for PL b (downgraded owing to diversity) and the instructions in Section 6.3.
- The delayed initiation of the stopping by the second de-energization path alone in the event of a fault must not involve an unacceptably high residual risk.
- The safety-related control part of the safety-related emergency stop control device K4 satisfies all requirements for Category 3 and PL d.



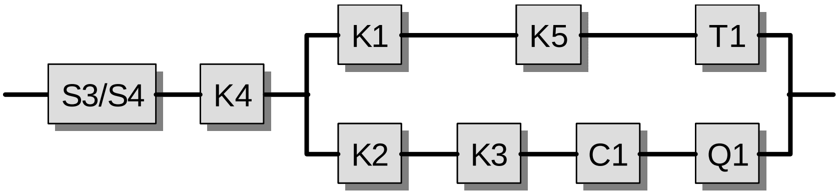
Calculation of the probability of failure

Only the probability of failure of the emergency stop function is calculated. For analysis of the safety-related stop function, S3/S4 and K4 must be replaced by S1, and K1 and K2 omitted.

- Fault exclusion is assumed for the emergency stop devices S3/S4, since the maximum number of 6,050 switching cycles within the mission time of the switching device as stated in Table D.2 is not exceeded. The safety-related emergency stop control device K4 is a tested safety component. Its probability of failure is 3.0 × 10^{-7} per hour [M], and is added at the end of the calculation. The value applies for a maximum number of 6,050 switching cycles within the mission time of the switching device.

The following applies for the probability of failure of the two-channel structure below:

- $MTTF_d$: the following $\mathrm{MTTF_d}$ values are estimated: 25 years for K5 and 50 years for T1 [E]. The capacitor C1 is included in the calculation with an $MTTF_d$ of 45,662 years [D]. At a $\mathrm{B_{10d}}$ value of 400,000 cycles [S] and a switching frequency of daily energization on 240 working days, the result is an $MTTF_d$ of 16,667 years for K1 and K2. At a $\mathrm{B_{10d}}$ value of 400,000 cycles [S] and at 240 working days, 16 working hours and a cycle time of 3 minutes, the result for n_{op} is 76,800 cycles per year and for the $MTTF_d$ 52 years in each case for K3 and Q1. These values produce a symmetrized $MTTF_d$ of the channel of 21 years ("medium").
- DC_{avg}: fault detection by the process in the event of failure in the actuation of the deceleration ramp leads to a *DC* of 30% for K5. For T1, the *DC* is 60%, likewise as a result of fault detection by the process. K1 and K2 yield a *DC* of 99% owing to the integral fault detection in K4, and K3 a *DC* of 99% owing to fault detection by K5. For C1, the *DC* is 60% owing to testing of the timing element with the FI de-energized. For Q1, the *DC* is thus 99% owing to direct monitoring in K5. The averaging formula for DC_{avg} produces a result of 63% ("low").
- Adequate measures against common cause failure (75 points): separation (15), diversity (20), FMEA (5) and environmental conditions (25 + 10)
- The two-channel combination of the control elements satisfies Category 3 with a medium $MTTF_d$ per channel (21 years) and low DC_{avg} (63%). This results in an average probability of dangerous failure of 1.04 × 10^{-6} per hour. This corresponds to PL c. The overall probability of failure is determined by addition of the probability of dangerous failure of K4, and is equal to 1.34 × 10^{-6} per hour. This then likewise corresponds to PL c.

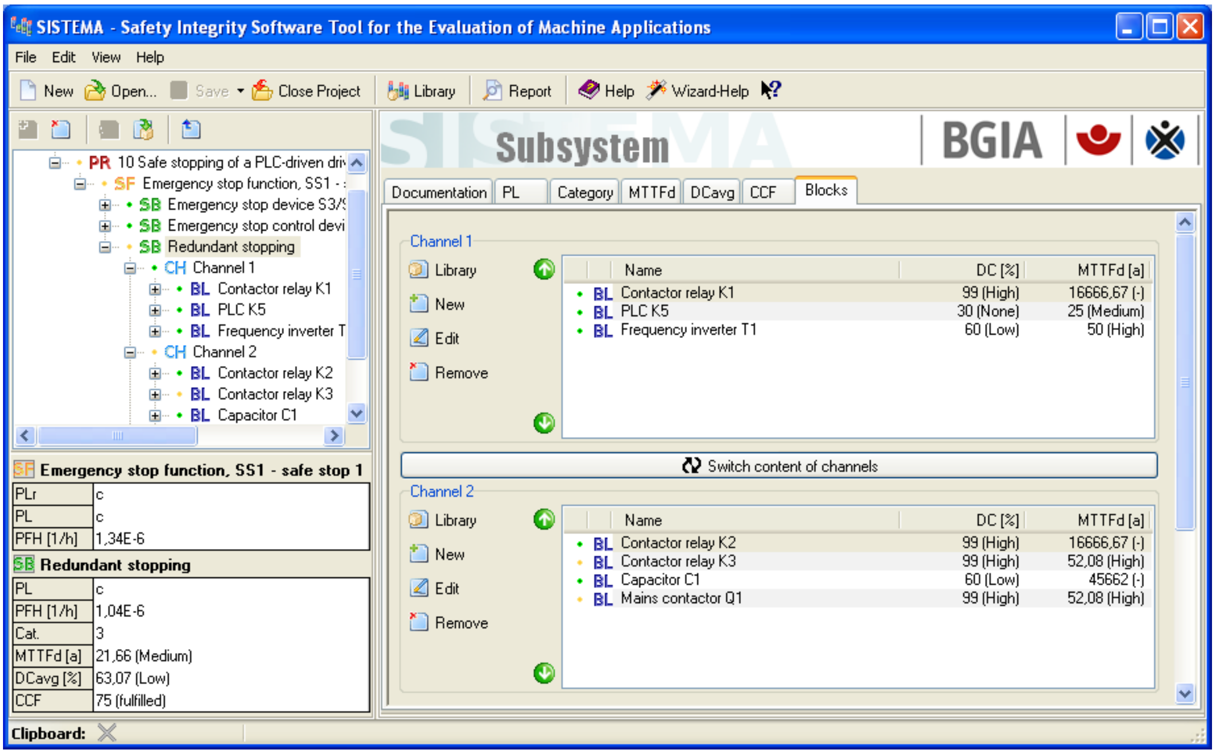


- The wearing elements K3 and Q1 should be replaced at intervals of approximately five years (T_{10d}).

More detailed references

- *Apfeld, R.; Zilligen, H.*: Sichere Antriebssteuerungen mit Frequenzumrichtern. BIA-Report 5/2003. Ed.: Hauptverband der gewerblichen Berufsgenossenschaften (HVBG), Sankt Augustin 2003.
  www.dguv.de/bgia, Webcode d6428
- IEC 61800-5-2: Adjustable speed electrical power drive systems – Part 5-2: Safety requirements – Functional (07.07)

Figure 8.20:
Determining of the PL by means of SISTEMA


SISTEMA - Safety Integrity Software Tool for the Evaluation of Machine Applications
File Edit View Help
New Open... Save Close Project Library Report Help Wizard-Help
Subsystem
BGIA
Documentation PL Category MTTFd DCavg CCF Blocks
Library
New
Edit
Remove
Switch content of channels
Clipboard:

- PR 10 Safe stopping of a PLC-driven dri
  - SF Emergency stop function, SS1 - :
    - SB Emergency stop device S3/S
    - SB Emergency stop control devi
    - SB Redundant stopping
      - CH Channel 1
        - BL Contactor relay K1
        - BL PLC K5
        - BL Frequency inverter T
      - CH Channel 2
        - BL Contactor relay K2
        - BL Contactor relay K3
        - BL Capacitor C1

SF Emergency stop function, SS1 - safe stop 1

PLr	c
PL	c
PFH [1/h]	1,34E-6

SB Redundant stopping

PL	c
PFH [1/h]	1,04E-6
Cat.	3
MTTFd [a]	21,66 (Medium)
DCavg [%]	63,07 (Low)
CCF	75 (fulfilled)

Channel 1

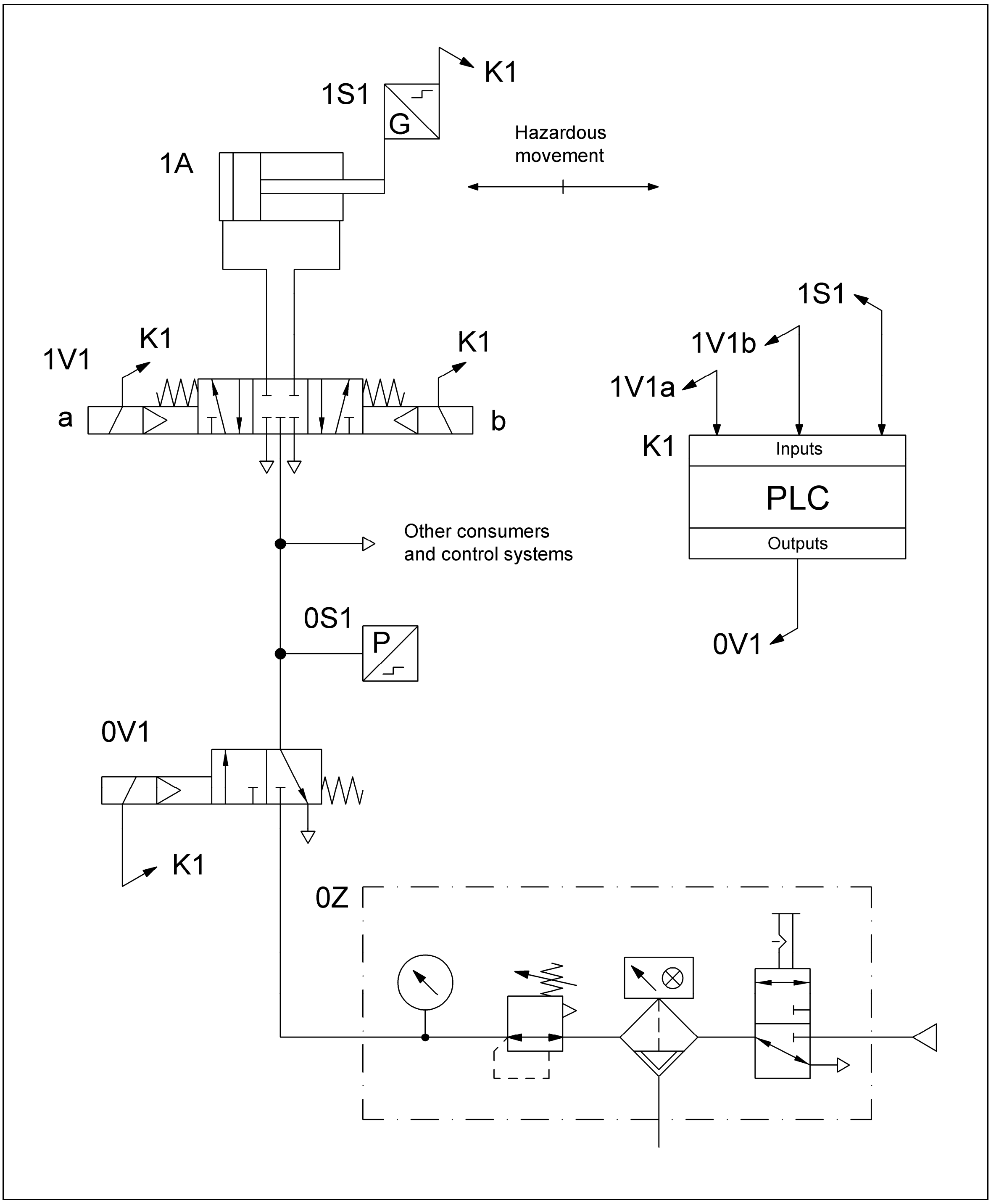
Name	DC [%]	MTTFd [a]
BL Contactor relay K1	99 (High)	16666,67 (-)
BL PLC K5	30 (None)	25 (Medium)
BL Frequency inverter T1	60 (Low)	50 (High)

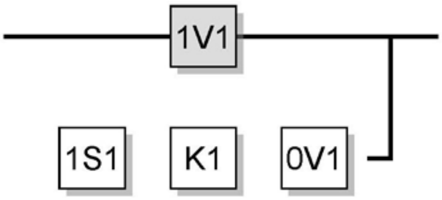
Channel 2

Name	DC [%]	MTTFd [a]
BL Contactor relay K2	99 (High)	16666,67 (-)
BL Contactor relay K3	99 (High)	52,08 (High)
BL Capacitor C1	60 (Low)	45662 (-)
BL Mains contactor Q1	99 (High)	52,08 (High)

8.2.11 Tested pneumatic valve (subsystem) – Category 2 – PL d (for PL c safety functions) (Example 11)

Figure 8.21:
Pneumatic valve with electronic testing for the control of hazardous movements





Safety functions

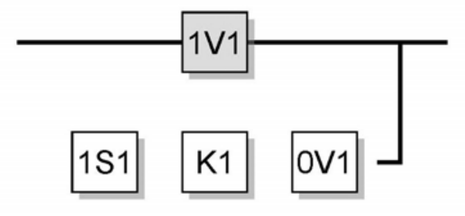
- Safety-related stop function: stopping of a hazardous movement and prevention of unexpected start-up from the rest position
- Only the pneumatic part of the control is shown here, in the form of a subsystem. Further safety-related control components (e.g. protective devices and electrical logic elements) must be added in the form of subsystems for completion of the safety function.

Functional description

- Hazardous movements are controlled by a directional control valve 1V1.
- Failure of the directional control valve 1V1 between function tests may result in loss of the safety function. The failure is dependent upon the reliability of the directional control valve.
- Testing of the safety function is implemented via the PLC K1 by means of a displacement sensor system 1S1. Testing takes place at suitable intervals and in response to a demand upon the safety function. Detection of the failure of 1V1 leads to the exhaust valve 0V1 being switched off.
- Hazardous movement interruption by the exhaust valve 0V1 generally results in a longer overrun. The distance from the hazardous area must be selected in consideration of the longer overrun.
- The test function must not be impaired by failure of the directional control valve. Failure of the test function must not lead to failure of the directional control valve.
- Should trapped compressed air pose a further hazard, additional measures are required.

Design features

- Basic and well-tried safety principles are observed and the requirements of Category B are met.
- 1V1 is a directional control valve with closed centre position, sufficient overlap and spring centering.
- The safety-oriented switching position is attained by removal of the control signal.
- Testing may for example take the form of checking of the time/distance characteristic (displacement sensor system 1S1) of the hazardous movements in

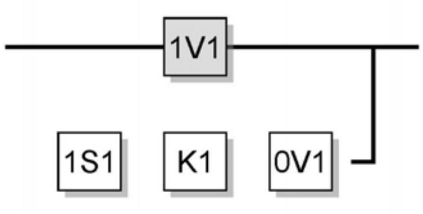


conjunction with the switching position of the directional control valve, with evaluation in a PLC (K1).

- In order to prevent a systematic failure, the higher-level de-energization function (acting upon exhaust valve 0V1 in this instance) is checked at suitable intervals, e.g. daily.
- It is implemented for use in applications with infrequent operator intervention in the hazardous area. This enables the requirement of the designated architecture for Category 2 to be satisfied, i.e. “testing much more frequent than the demand upon the safety function” (cf. Annex G).
- The standard component K1 is employed in accordance with the instructions in Section 6.3.10.
- The software (SRASW) is programmed in accordance with the requirements for PL b (downgraded owing to diversity) and the instructions in Section 6.3.

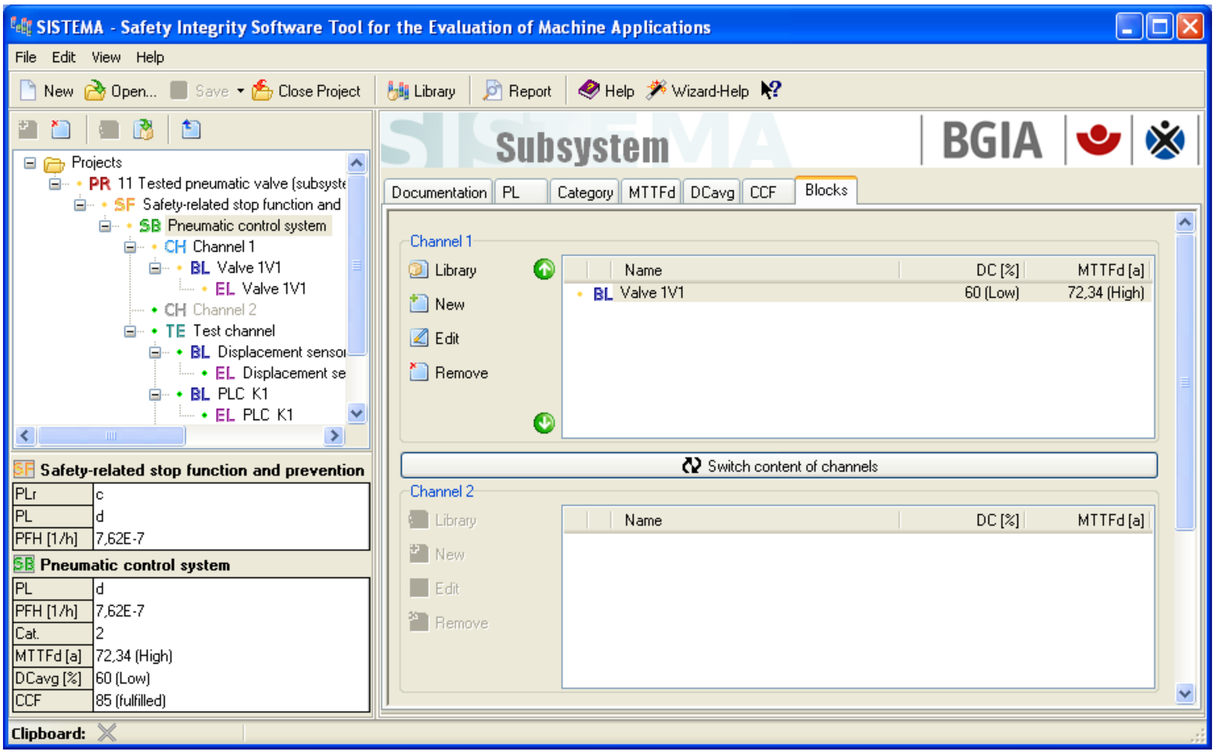
Calculation of the probability of failure

- $MTTF_d$ of the functional channel: a B_{10d} value of 20,000,000 switching operations [S] is assumed for the directional control valve 1V1. At 240 working days, 16 working hours per day and a cycle time of 5 seconds, n_{op} is 2,764,800 switching operations per year and the $MTTF_d$ is 72.3 years. This is also the $\mathrm{MTTF_d}$ value for the functional channel.
- $MTTF_d$ of the test channel: an $\mathrm{MTTF_d}$ value of 150 years [E] is assumed for the displacement sensor system 1S1. An $\mathrm{MTTF_d}$ value of 50 years [E] is assumed for the PLC K1. A B_{10d} value of 20,000,000 cycles [S] applies for the exhaust valve 0V1. At actuation once daily on 240 working days, the $\mathrm{MTTF_d}$ value for 0V1 is 833,333 years. The $MTTF_d$ of the test channel is thus 37.5 years.
- DC_{avg}: the DC of 60% for 1V1 is based upon the comparison of the distance/ time characteristic of the hazardous movement in conjunction with the switching status of the directional control valve. This is also the DC_{avg} (“low”).
- Adequate measures against common cause failure (85 points): separation (15), diversity (20), overvoltage protection etc. (15) and environmental conditions (25 + 10)
- The combination of the pneumatic control elements corresponds to Category 2 with a high $MTTF_d$ (72.3 years) and low DC_{avg} (60%). This results in an average probability of dangerous failure of 7.62×10^{-7} per hour. This corresponds to PL d. Following the addition of further safety-related control parts (subsystems) for completion of the safety function, PL c is generally attained for the complete safety function.



- The wearing element 1V1 should be replaced approximately every seven years (T_{10d}).

Figure 8.22:
Determining of the PL by means of SISTEMA


SISTEMA - Safety Integrity Software Tool for the Evaluation of Machine Applications
File Edit View Help
New Open... Save Close Project Library Report Help Wizard-Help
Subsystem
BGIA
Documentation PL Category MTTFd DCavg CCF Blocks
Library
New
Edit
Remove
Switch content of channels
Clipboard:

Projects
PR 11 Tested pneumatic valve (subsyste
SF Safety-related stop function and
SB Pneumatic control system
CH Channel 1
BL Valve 1V1
EL Valve 1V1
CH Channel 2
TE Test channel
BL Displacement sensor
EL Displacement se
BL PLC K1
EL PLC K1

SF Safety-related stop function and prevention

PLr	c
PL	d
PFH [1/h]	7,62E-7

SB Pneumatic control system

PL	d
PFH [1/h]	7,62E-7
Cat.	2
MTTFd [a]	72,34 (High)
DCavg [%]	60 (Low)
CCF	85 (fulfilled)

Channel 1

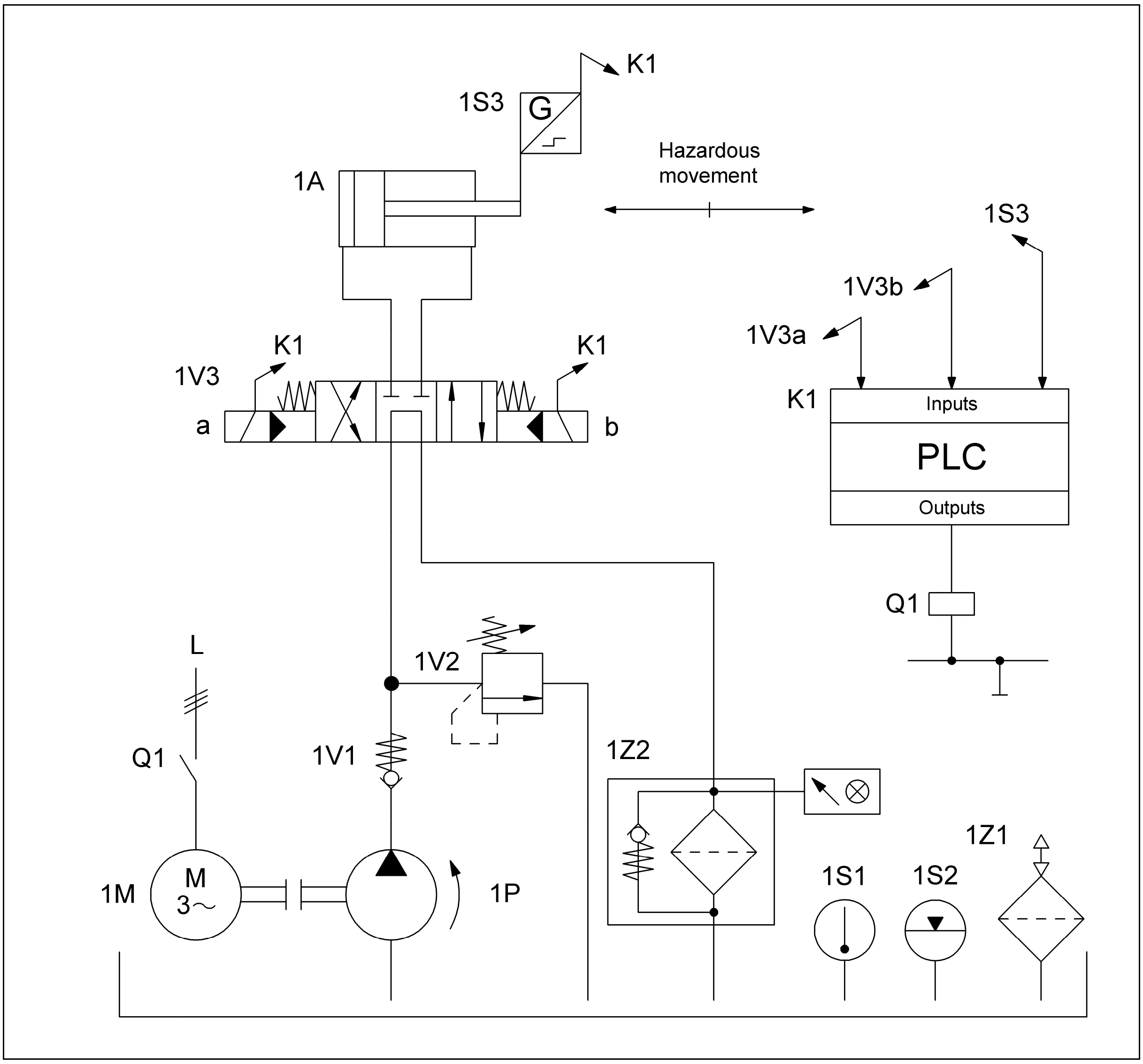
Name	DC [%]	MTTFd [a]
BL Valve 1V1	60 (Low)	72,34 (High)

Channel 2

Name	DC [%]	MTTFd [a]

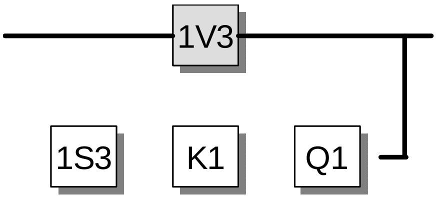
8.2.12 Tested hydraulic valve (subsystem) – Category 2 – PL d (for PL c safety functions) (Example 12)

Figure 8.23:
Hydraulic valve with electronic testing for the control of hazardous movements



Safety functions

- Safety-related stop function: stopping of a hazardous movement and prevention of unexpected start-up from the rest position
- Only the hydraulic part of the control is shown here, in the form of a subsystem. Further safety-related control components (e.g. protective devices and electrical logic elements) must be added in the form of subsystems for completion of the safety function.

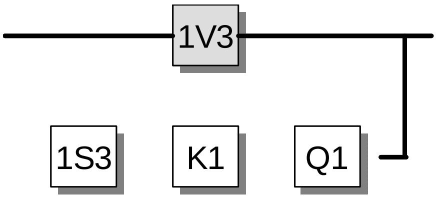


Functional description

- Hazardous movements are controlled by a directional control valve 1V3.
- Failure of the directional control valve 1V3 between function tests may result in loss of the safety function. The probability of failure is dependent upon the reliability of the directional control valve.
- Testing of the safety function is implemented via the PLC K1 by means of a displacement sensor system 1S3. Testing takes place at suitable intervals and in response to a demand upon the safety function. Detection of a failure of 1V3 leads to the hydraulic pump 1M/1P being switched off by the contactor Q1.
- Hazardous movement interruption by the hydraulic pump generally results in a longer overrun. The distance from the hazardous area must be selected in consideration of the longer overrun.
- The test function must not be impaired by failure of the directional control valve. Failure of the test function must not lead to failure of the directional control valve.

Design features

- Basic and well-tried safety principles are observed and the requirements of Category B are met.
- 1V3 is a directional control valve with closed centre position, sufficient overlap and spring centering.
- The safety-oriented switching position is attained by removal of the control signal.
- Testing may for example take the form of checking of the time/distance characteristic (displacement sensor system 1S3) of the hazardous movements in conjunction with the switching position of the directional control valve, with evaluation in a PLC (K1).
- In order to prevent systematic failure, the higher-level de-energization function (acting upon the hydraulic pump in this instance) is checked at suitable intervals, e.g. daily.
- It is implemented for use in applications with infrequent operator intervention in the hazardous area. This enables the requirement of the designated architecture for Category 2 to be satisfied, i.e. “testing much more frequent than the demand upon the safety function” (cf. Annex G).
- The standard component K1 is employed in accordance with the instructions in Section 6.3.10.



- The software (SRASW) is programmed in accordance with the requirements for PL b (downgraded owing to diversity) and the instructions in Section 6.3.

Calculation of the probability of failure

- *$MTTF_d$* of the functional channel: an *$MTTF_d$* of 150 years is assumed for the directional control valve 1V3 [S]. This is also the $\mathrm{MTTF_d}$ value for the functional channel, which is first capped to 100 years.
- *$MTTF_d$* of the test channel: an $\mathrm{MTTF_d}$ value of 150 years [E] is assumed for the displacement sensor system 1S3. An $\mathrm{MTTF_d}$ value of 50 years [E] is assumed for the PLC K1. A $\mathrm{B_{10d}}$ value of 2,000,000 cycles [S] applies for the contactor Q1. At actuation once daily on 240 days, the $\mathrm{MTTF_d}$ value for Q1 is 83,333 years. The *$MTTF_d$* of the test channel is thus 37.5 years. The *$MTTF_d$* of the functional channel must therefore be reduced to 75.0 years in accordance with the underlying analysis model.
- *DC_{avg}*: the *DC* of 60% for 1V3 is based upon the comparison of the distance/ time characteristic of the hazardous movement in conjunction with the switching status of the directional control valve. This is also the *DC_{avg}* ("low").
- Adequate measures against common cause failure (85 points): separation (15), diversity (20), overvoltage protection etc. (15) and environmental conditions (25 + 10)
- The combination of the control elements corresponds to Category 2 with a high *$MTTF_d$* (75.0 years) and low *DC_{avg}* (60%). This results in an average probability of dangerous failure of 7.31×10^{-7} per hour. This corresponds to PL d. Following the addition of further safety-related control parts (subsystems) for completion of the safety function, PL c is generally attained for the complete safety function.

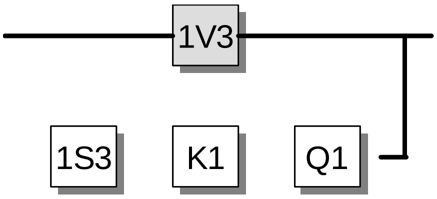
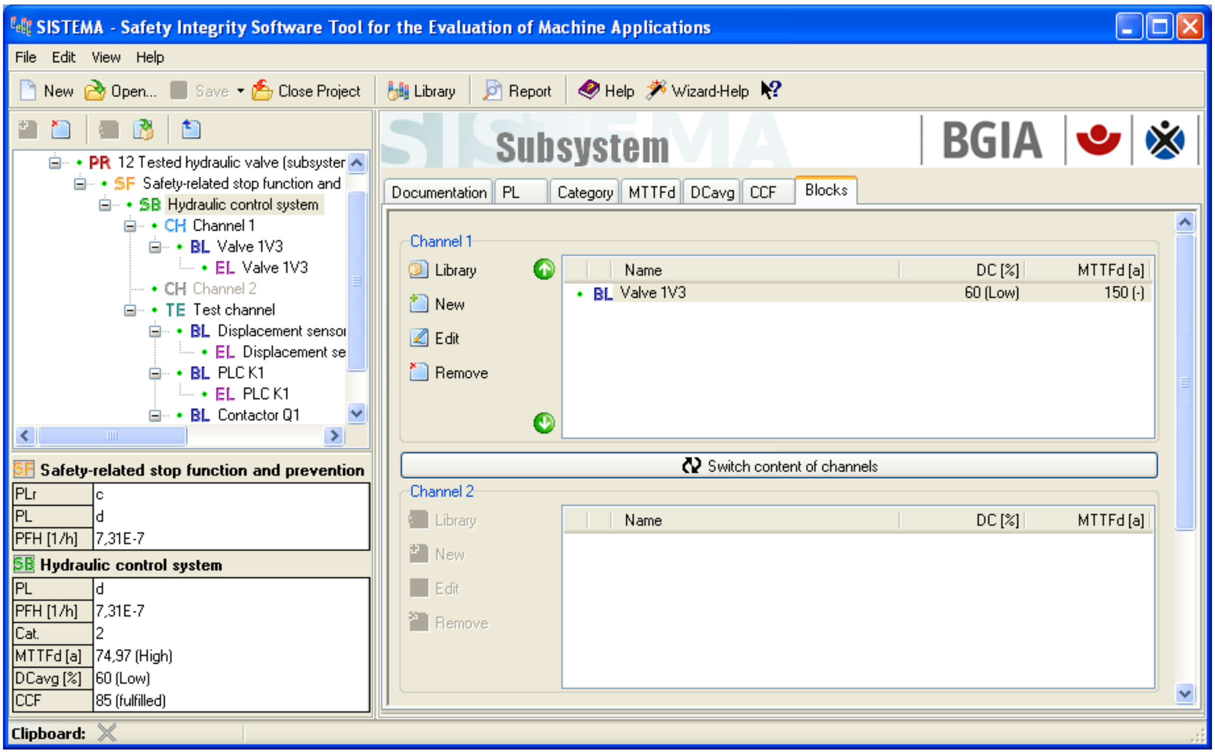


Figure 8.24:
Determining of the PL by means of SISTEMA


SISTEMA - Safety Integrity Software Tool for the Evaluation of Machine Applications
File Edit View Help
New Open... Save Close Project Library Report Help Wizard-Help
Subsystem
BGIA
Documentation PL Category MTTFd DCavg CCF Blocks
Library
New
Edit
Remove
Switch content of channels
Clipboard:

- PR 12 Tested hydraulic valve (subsyster
  - SF Safety-related stop function and
    - SB Hydraulic control system
      - CH Channel 1
        - BL Valve 1V3
          - EL Valve 1V3
      - CH Channel 2
      - TE Test channel
        - BL Displacement sensoı
          - EL Displacement se
        - BL PLC K1
          - EL PLC K1
        - BL Contactor Q1

SF Safety-related stop function and prevention

PLr	c
PL	d
PFH [1/h]	7,31E-7

SB Hydraulic control system

PL	d
PFH [1/h]	7,31E-7
Cat.	2
MTTFd [a]	74,97 (High)
DCavg [%]	60 (Low)
CCF	85 (fulfilled)

Channel 1

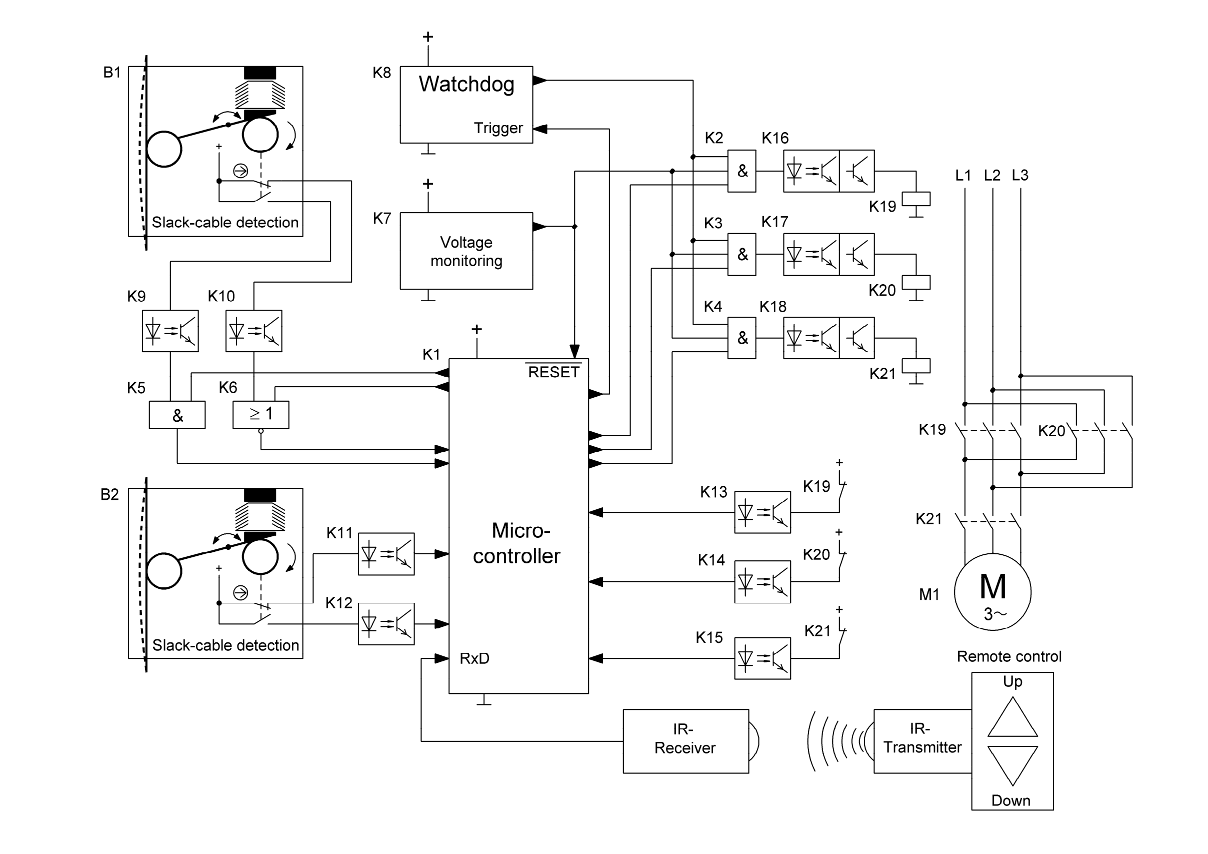
Name	DC [%]	MTTFd [a]
BL Valve 1V3	60 (Low)	150 (-)

Channel 2

Name	DC [%]	MTTFd [a]

8.2.13 No-load sensing system for a hoist – Category 2 – PL d (Example 13)

Figure 8.25:
Combined electromechanical and programmable electronic control system for the prevention of no-load states on hoists

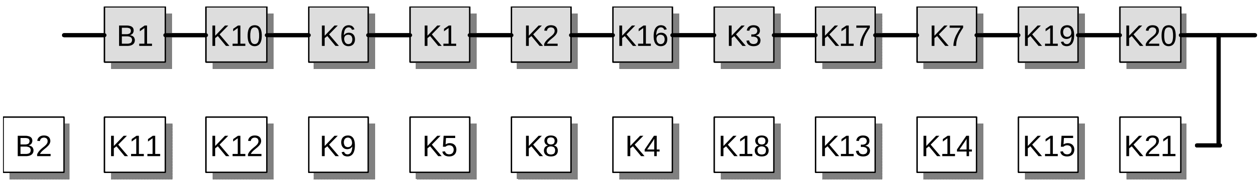


Safety function

- No-load/slack-cable detection: should a slack cable or suspension element be detected on a hoist, the downward movement is stopped (STO – safe torque off).

Functional description

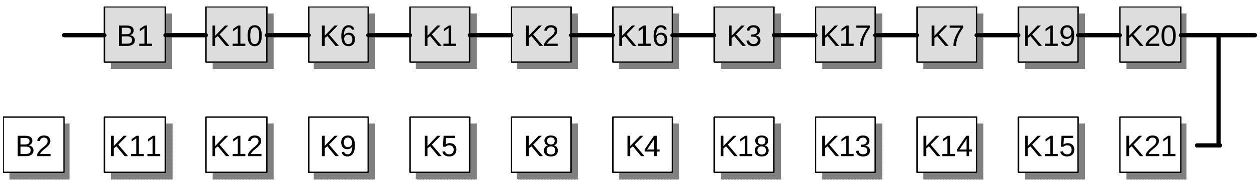
- Hoists driven by electric motors are widely used in studio and stage applications. During downward movement, the cable may become slack should the load stick or tilt or come to rest on other objects. In such cases, a risk exists for example of the obstruction suddenly giving way, the load slipping and consequently, danger arising for persons in the hazardous area.
- Upward and downward movements of the hoist can for example be controlled by means of an infrared remote control. This function is not evaluated here; it must, however, always be implemented with consideration for safety.



- In order for the hoist to be prevented from falling in the event of breakage of one suspension element, the load is borne by two suspension elements. A slack-cable switch B1/B2 with a break contact element/make contact element combination is fitted to each suspension element.
- The microcontroller K1 evaluates the switching states of the slack-cable switches B1 and B2. Via logic gates K2/K3 and optocoupled transistor amplifiers K16/K17, K1 also controls the contactor relays K19 and K20 for the upward and downward movements of the hoist.
- The switching states of the contacts of the slack-cable switches B1 and B2 are evaluated by the microcontroller K1 and tested for plausibility. For testing of the inputs used on the microcontroller, forced dynamics is employed on the signals from the slack-cable switch B1. This involves the microcontroller forcing a temporary signal change via the logic gates K5 and K6, in order to ascertain whether the inputs are still able to transmit the signal change. Forced dynamics of the signals of one slack-cable switch is sufficient.
- Self-tests of the integrated units such as ALU, RAM and ROM are performed in the microcontroller K1. The voltage monitor K7 detects faults in the supply voltage. Faults in the microcontroller are detected by temporal monitoring of the program sequence in the watchdog K8. The components K19 to K21 for control of the hoist's upward and downward movements are monitored by means of readback – decoupled by optocouplers K13 to K15 – in the microcontroller. Should a fault be detected, the hoist is shut off at a higher level by the component detecting the fault via the contactor relay K21, actuated by logic gate K4 and decoupled by optocoupler K18. If the watchdog K8 is not retriggered in time by the microcontroller K1, the movement of the hoist is stopped from K8 via all logic gates K2 to K4.

Design features

- Basic and well-tried safety principles are observed and the requirements of Category B are met. Protective circuits as described in the initial paragraphs of Chapter 8 are implemented.
- A slack cable is detected redundantly for both suspension elements via the two slack-cable switches B1 and B2. These switches contain position switches with direct opening action in accordance with IEC 60947-5-1, Annex K.
- A stable arrangement is assured for the operating mechanism of the slack-cable switches.
- K19 to K21 possess mechanically linked contact elements to IEC 60947-5-1, Annex L.



- The software (SRESW) for K1 is programmed in accordance with the requirements for PL d and the instructions in Section 6.3.

Remarks

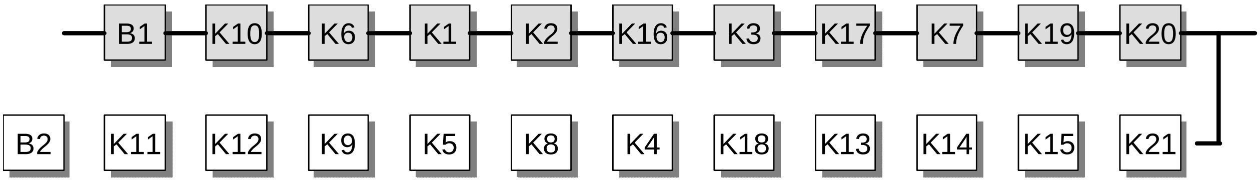
- The draft version of DIN 15560-46, Section 5.1.2 requires at least two suspension elements in order to prevent a hoist and its load from falling.
- Visual inspections and maintenance of the suspension elements must be performed at suitable intervals.
- Parts of the circuit structure as shown are not explicitly designed to prevent possible hazards resulting from unintended movement of the hoist (unexpected start-up).
- The circuit structure used attains PL d for the safety function under consideration here, as is demonstrated by the calculation of the probability of failure. Use of the risk graph to determine the required Performance Level PL_r with the parameters S2, F1 and P1 results in PL_r c in accordance with DIN 15560-46, Section B.1.1.3.3, provided the hoist is operated under observation and only by skilled personnel. Should this not be the case, PL_r d is required.

Calculation of the probability of failure

- Components are summarized in blocks in Figure 8.23 in the interests of clarity. K9 to K15 each contain one optocoupler and two resistances. K16 to K18 additionally each contain a transistor for driving the downstream contactor relays.
- For application of the simplified procedure for estimation of the achieved PL, the components in the circuit are assigned to the blocks of the designated architecture for Category 2 as follows:

I:	B1
L:	K10, K6, K1, K2, K16, K3, K17, K7
O:	K19, K20
TE:	B2, K11, K12, K, K5, K8, K13, K14, K15
OTE:	K21

- $MTTF_d$: the $MTTF_d$ values required for the calculation are obtained from EN ISO 13849-1 [S], and from SN 29500-2 and SN 29500-14 [D]. The following values are substituted for B1 and B2: B_{10d} = 100,000 cycles [E], n_{op} = 10 cycles per year. For the contactor relays K19 to K21: B_{10d} = 400,000 cycles [S], n_{op} = 10 cycles per day on 365 working days. An $MTTF_d$ of 1,141 years [D] is substituted for the microcontroller K1. The following $MTTF_d$ values are



substituted for the electronic components [D]: 4,566 years for the watchdog K8, 5,707 years for the optocouplers K9 to K18, 22,831 years for the logic gates K2 to K6, 38,051 years for the voltage monitor K7, 45,662 years for transistors and 228,310 years for resistors. Summation of the failure rates for all components of the functional channel (blocks I, L and O) produces an MTTF_d value of 288 years. This value is capped to 100 years ("High") in accordance with the requirements of the standard.

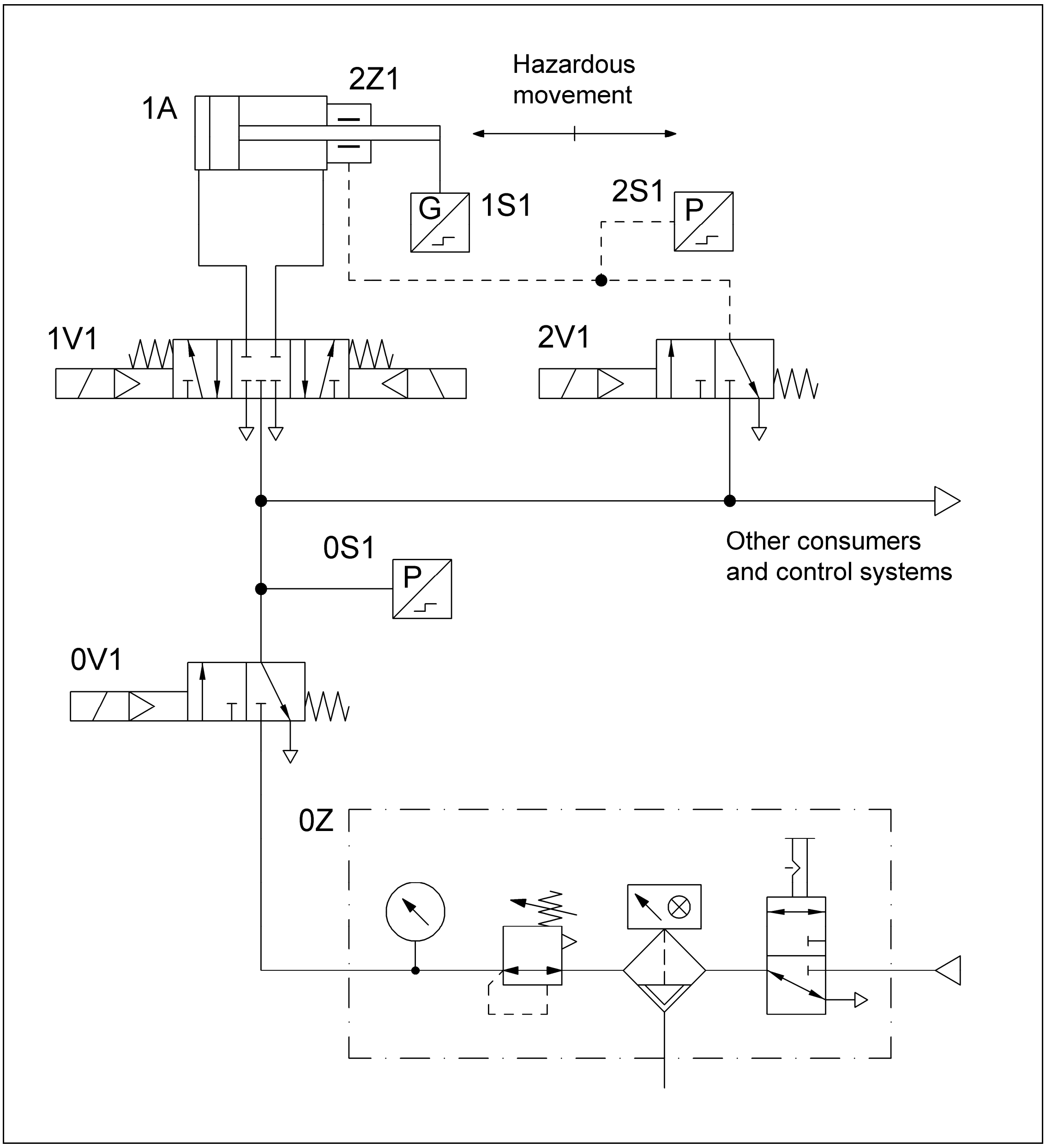
- The $MTTF_d$ of the test channel is produced by summation of the failure rates of all components of blocks TE and OTE. It is equal to 393 years and is thus greater than or equal to half of the $MTTF_d$ of the functional channel.
- DC_{avg}: the *DC* is 60% for B1, K10 and K6 owing to cross-checking of B1 and B2 in K1 with a low demand rate upon the safety function. The *DC* is 60% for K1 owing to temporal monitoring of the program sequence and self-tests of simple effectiveness. The *DC* is 99% for K2, K3, K16, K17, K19 and K20 owing to direct monitoring by means of mechanically linked contact elements. For K7, the *DC* is 0%. The averaging formula returns a result of 85% ("low") for DC_{avg}.
- Adequate measures against common cause failure (65 points): separation (15), overvoltage protection (15) and environmental conditions (25 + 10)
- The combination of the control elements corresponds to Category 2 with a high $MTTF_d$ per channel (100 years) and low DC_{avg} (85%). This results in an average probability of dangerous failure of 2.72×10^{-7} per hour. This corresponds to PL d.

More detailed references

- DIN 15560-46: Scheinwerfer für Film, Fernsehen, Bühne und Photographie – Teil 46: Bewegliche Leuchtenhänger; Sicherheitstechnische Anforderungen und Prüfung (Normentwurf) (06.07). Beuth, Berlin 2007
- Sicherheit bei Produktionen und Veranstaltungen – Leitfaden BGI 810. Ed.: Verwaltungs-Berufsgenossenschaft, Hamburg 2006 www.vbg.de/imperia/md/content/produkte/broschueren/bgi_810_.pdf

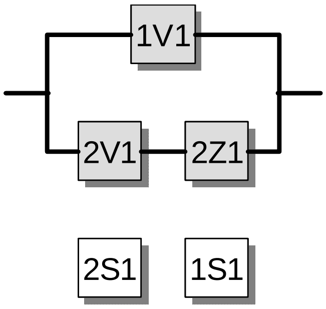
8.2.14 Pneumatic valve control (subsystem) – Category 3 – PL d (Example 14)

Figure 8.26:
Tested pneumatic valves for redundant control of hazardous movements



Safety functions

- Safety-related stop function: stopping of the hazardous movement and prevention of unexpected start-up from the rest position
- Only the pneumatic part of the control is shown here, in the form of a subsystem. Further safety-related control components (e.g. protective devices and electrical logic elements) must be added in the form of subsystems for completion of the safety function.

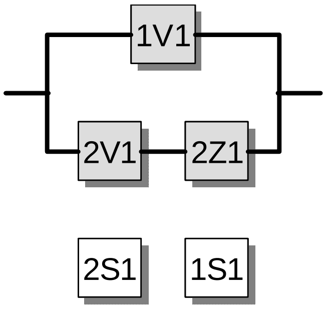


Functional description

- Hazardous movements are controlled/halted redundantly by a directional control valve 1V1 and a brake 2Z1 on the piston rod. The brake 2Z1 is actuated by a control valve 2V1.
- Failure of one of these valves or of the brake alone does not result in loss of the safety function.
- The directional control valve and the brake are actuated cyclically in the process.
- The functioning of the control valve 2V1 is monitored by means of a pressure switch 2S1. Certain faults on the unmonitored valve 1V1 and on the unmonitored brake 2Z1 are detected in the work process. In addition, the overrun (distance/time characteristic) during the braking process (dynamic) and/or at start-up of the machine (static) is monitored with the aid of a displacement sensor system 1S1 on the piston rod. An accumulation of undetected faults may lead to loss of the safety function.
- Testing of the safety function is implemented at suitable intervals, for example at least every eight working hours.
- The test function must not be impaired by failure of the brake. Failure of the test function must not lead to failure of the brake.
- Should trapped compressed air pose a further hazard, additional measures are required.

Design features

- Basic and well-tried safety principles are observed and the requirements of Category B are met.
- The directional control valve 1V1 features a closed centre position with sufficient overlap and spring-centering.
- The safety-oriented switching position is assumed from any position by removal of the control signal.
- The upstream electrical logic for example is employed for signal processing for the pressure monitor 2S1 and the displacement sensor system 1S1.



Calculation of the probability of failure

- *$MTTF_d$*: B_{10d} values of 40,000,000 cycles [E] are assumed for the directional control valves 1V1 and 2V1. At 240 working days, 16 working hours and a cycle time of 10 seconds, n_{op} is 1,382,400 cycles per year. The *$MTTF_d$* for 1V1 and 2V1 is thus 289 years. A B_{10d} value of 5,000,000 switching operations [M] is substituted for the mechanical brake on the piston rod 2Z1. This results in an *$MTTF_d$* of 36 years for the mechanical brake. Overall, the resulting symmetrized $MTTF_d$ value per channel is 71 years ("high").
- *DC_{avg}*: pressure monitoring of the control signal for the brake results in a *DC* of 99% for the valve 2V1. The *DC* for the valve 1V1 is 60% owing to fault detection through the process. A *DC* of 75% for 2Z1 is produced by start-up testing of the mechanical brake. Averaging thus results in a *DC_{avg}* of 75% ("low").
- Adequate measures against common cause failure (85 points): separation (15), diversity (20), overvoltage protection etc. (15) and environmental conditions (25 + 10)
- The combination of the pneumatic control elements corresponds to Category 3 with a high *$MTTF_d$* per channel (71 years) and low *DC_{avg}* (75%). This results in an average probability of dangerous failure of 1.21×10^{-7} per hour. This corresponds to PL d. Following the addition of further safety-related control components in the form of subsystems for completion of the safety function, the PL may under certain circumstances be lower.
- The wearing brake 2Z1 should be replaced at intervals of approximately three years (*T_{10d}*).

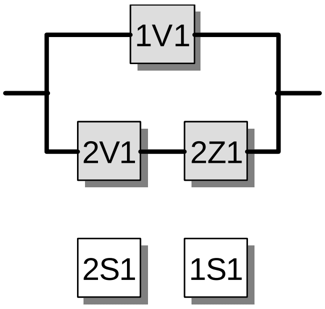
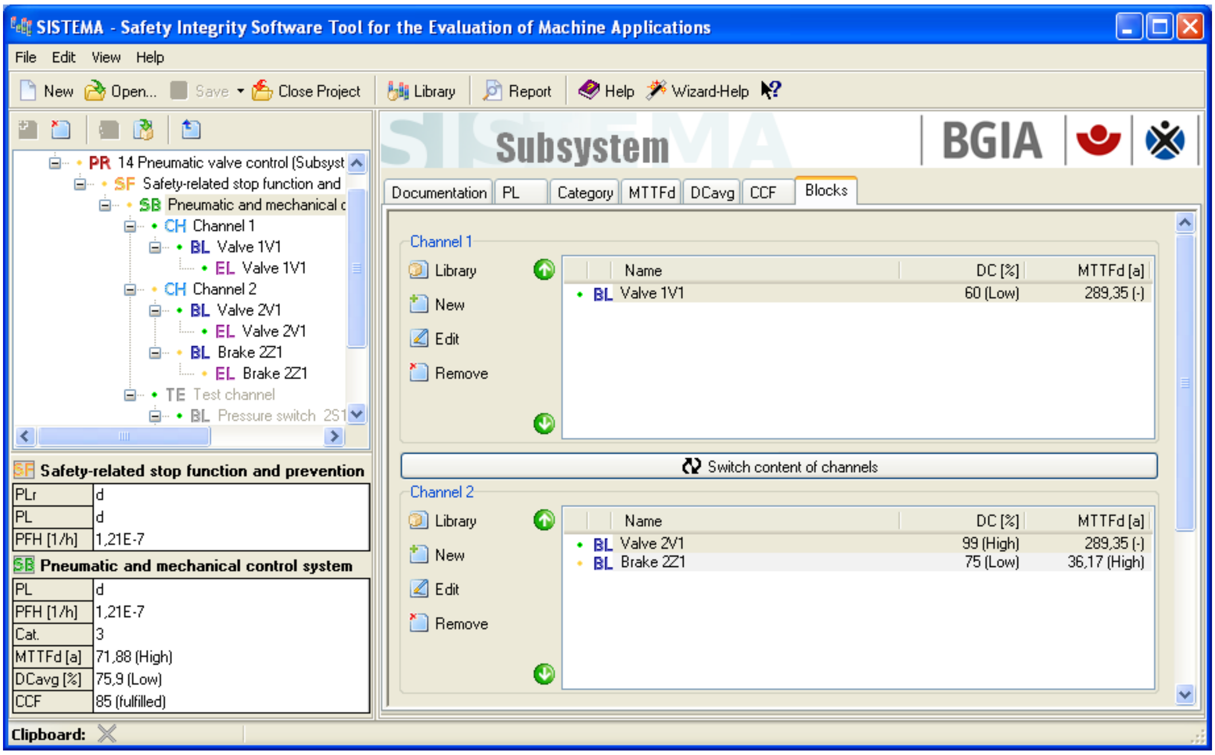


Figure 8.27:
Determining of the PL by means of SISTEMA


SISTEMA - Safety Integrity Software Tool for the Evaluation of Machine Applications
File Edit View Help
New Open... Save Close Project Library Report Help Wizard-Help
Subsystem
BGIA
Documentation PL Category MTTFd DCavg CCF Blocks
Library
New
Edit
Remove
Switch content of channels
Clipboard:

PR 14 Pneumatic valve control (Subsyst
SF Safety-related stop function and
SB Pneumatic and mechanical c
CH Channel 1
BL Valve 1V1
EL Valve 1V1
CH Channel 2
BL Valve 2V1
EL Valve 2V1
BL Brake 2Z1
EL Brake 2Z1
TE Test channel
BL Pressure switch 2S1

SF Safety-related stop function and prevention

PLr	d
PL	d
PFH [1/h]	1,21E-7

SB Pneumatic and mechanical control system

PL	d
PFH [1/h]	1,21E-7
Cat.	3
MTTFd [a]	71,88 (High)
DCavg [%]	75,9 (Low)
CCF	85 (fulfilled)

Channel 1

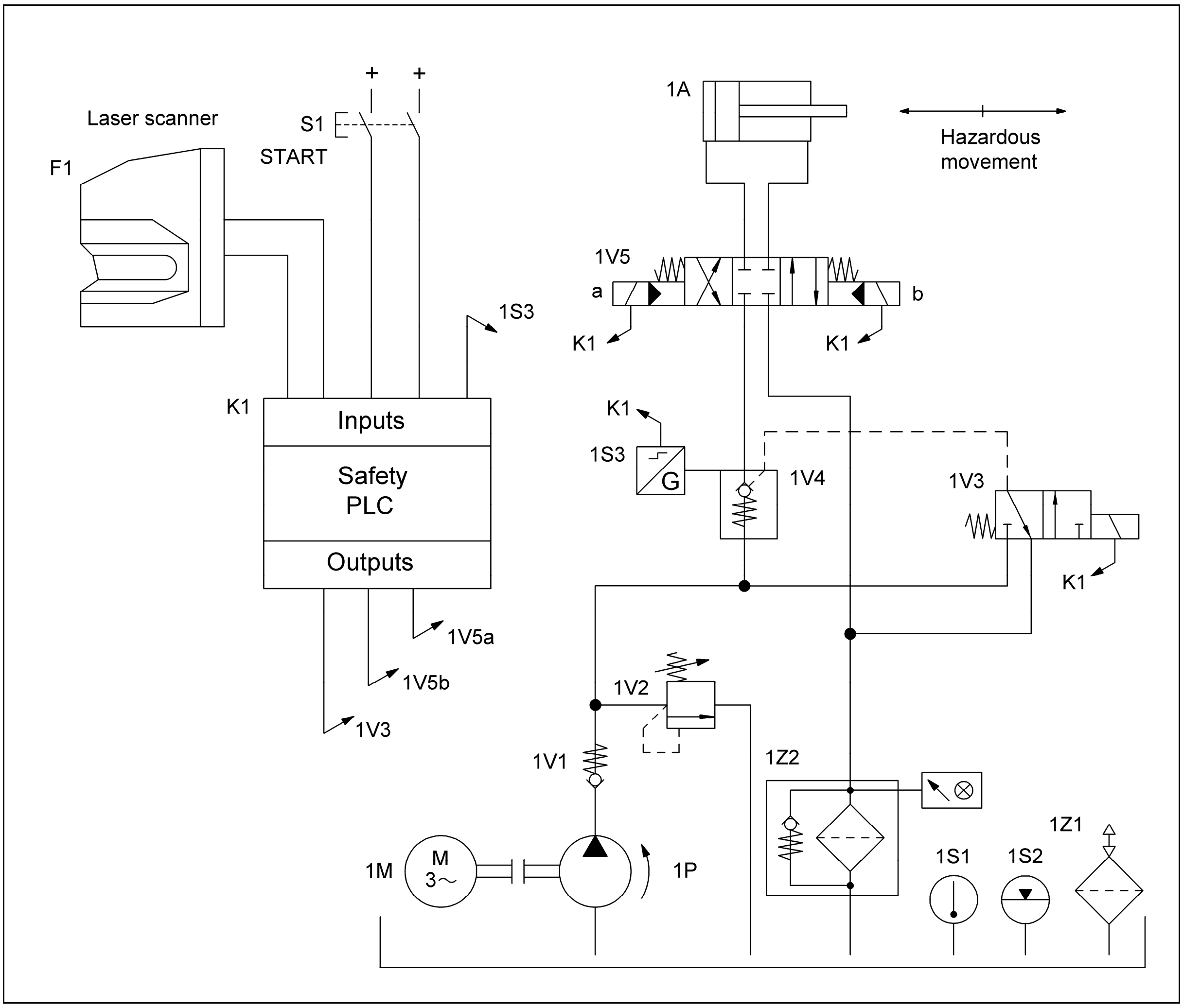
Name	DC [%]	MTTFd [a]
BL Valve 1V1	60 (Low)	289,35 (-)

Channel 2

Name	DC [%]	MTTFd [a]
BL Valve 2V1	99 (High)	289,35 (-)
BL Brake 2Z1	75 (Low)	36,17 (High)

8.2.15 Protective device and hydraulics controlled by PLC – Category 3 – PL d (Example 15)

Figure 8.28:
Detection zone monitoring by laser scanner with
electro-hydraulic deactivation of the hazardous movement

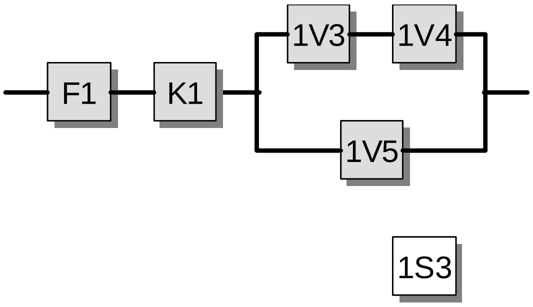


Safety function

- Safety-related stop function, initiated by a protective device: penetration of the laser scanner's detection zone results in stopping of the hazardous movement.

Functional description

- The laser scanner F1 monitors, with its detection zone, the area in which movement of the cylinder 1A may present a danger to the operator. The output signal of the laser scanner is read in on two channels by the safety PLC K1. Following any violation of the detection zone, the next movement must be enabled by actuation of a start button evaluated in K1 (restart interlock). With the aid of the hydraulic control part, K1 controls the movement of 1A.



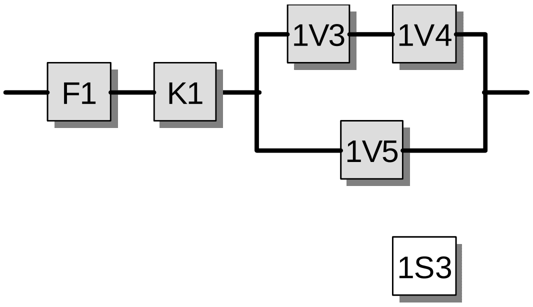
- The hydraulic control part comprises a two-channel arrangement. The first channel comprises directional control valve 1V3, which acts upon the pilot-operated non-return valve 1V4. In the closed position, 1V4 blocks movements by 1A. The second channel consists of the directional control valve 1V5, which in its closed centre position also prevents movement of 1A.
- 1V5 is actuated cyclically; 1V3 and 1V4 close only when the detection zone is violated.
- Direct position monitoring 1S3 is implemented on 1V4 and evaluated in K1 as a measure for fault detection. Faults in 1V5 can be detected via the process owing to the function. An accumulation of undetected faults in the hydraulic control part may lead to loss of the safety function.

Design features

- Basic and well-tried safety principles are observed and the requirements of Category B are met. Protective circuits (e.g. contact protection) as described in the initial paragraphs of Chapter 8 are implemented.
- Faults in the conductors to F1 and K1 must not be hazardous in their effects. For this purpose, faults are detected as they arise, and the safe state is initiated. Alternatively, fault exclusion to EN ISO 13849-2, Table D.4 must be possible for conductor short-circuits.
- The laser scanner F1 and safety PLC K1 are tested safety components for use in PL d which satisfy Category 3 and the relevant product standards.
- The directional control valve 1V5 features a closed centre position with sufficient overlap and spring-centering. 1V4 employs electrical position monitoring, since 1V4 is not switched cyclically.
- The software (SRASW) is programmed in accordance with the requirements for PL d and the instructions in Section 6.3.
- It is assumed that each output of the safety PLC is driven by both processing channels of the PLC. Should this not be the case, the outputs which drive 1V3 and 1V4 are driven by one channel of the PLC, and the output which drives 1V5 by the other.

Calculation of the probability of failure

- Since the laser scanner F1 and the safety PLC K1 are available for purchase as safety components, their probabilities of failure are added at the end of the



calculation (F1: 3.0 × 10^{-7} per hour [E], K1: 1.5 × 10^{-7} per hour [E]). For the hydraulic part of the control system, the probability of failure is calculated as shown below.

- *$MTTF_d$*: values of 150 years [S] are assumed for valves 1V3 to 1V5. Overall, this results in a symmetrized $MTTF_d$ value per channel of 88 years ("high").
- *DC_{avg}*: a *DC* of 99% for 1V4 is produced by direct monitoring in K1 with the aid of the position monitor 1S3. Owing to the close coupling of 1V3 and 1V4, this results in 1V3 being monitored indirectly at the same time with a *DC* of 99%. The *DC* of 60% for 1V5 is based upon fault detection in the process with cyclical actuation. Averaging thus results in a *DC_{avg}* of 86% ("low").
- Adequate measures against common cause failure (90 points): separation (15), diversity (20), FMEA (5), overvoltage protection etc. (15) and environmental conditions (25 + 10)
- The combination of the control elements in the hydraulic part corresponds to Category 3 with a high *$MTTF_d$* per channel (88 years) and low *DC_{avg}* (86%). This results in an average probability of dangerous failure of 6.2 × 10^{-8} per hour for the hydraulic system.
- Altogether, the average probability of dangerous failure is (3.0 + 1.5 + 0.62) × 10^{-7} = 5.12 × 10^{-7} per hour. This corresponds to PL d.

More detailed reference

- *Bömer, T.*: Hinweise zum praktischen Einsatz von Laserscannern. In: BGIA-Handbuch Sicherheit und Gesundheitsschutz am Arbeitsplatz. Kennzahl 310 243. 36th suppl. XII/99. Ed.: BGIA – Institut für Arbeitsschutz der Deutschen Gesetzlichen Unfallversicherung, Sankt Augustin. Erich Schmidt, Berlin 1985 – loose-leaf ed.
  www.bgia-handbuchdigital.de/310243

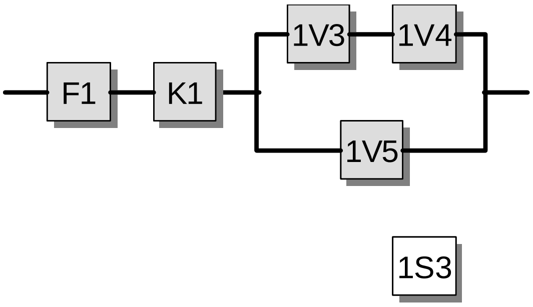
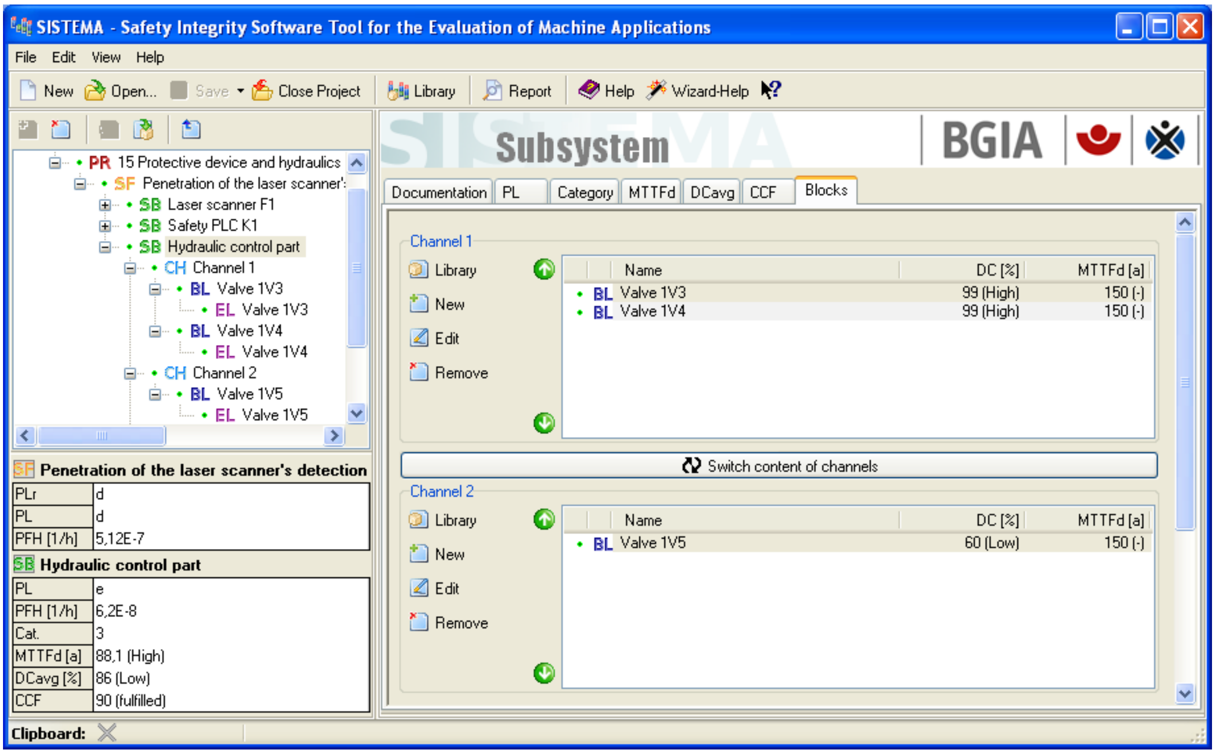


Figure 8.29:
Determining of the PL by means of SISTEMA


SISTEMA - Safety Integrity Software Tool for the Evaluation of Machine Applications
File Edit View Help
New Open... Save Close Project Library Report Help Wizard-Help
Subsystem
BGIA
Documentation PL Category MTTFd DCavg CCF Blocks
Library
New
Edit
Remove
Switch content of channels
Clipboard:

- PR 15 Protective device and hydraulics
  - SF Penetration of the laser scanner's
    - SB Laser scanner F1
    - SB Safety PLC K1
    - SB Hydraulic control part
      - CH Channel 1
        - BL Valve 1V3
          - EL Valve 1V3
        - BL Valve 1V4
          - EL Valve 1V4
      - CH Channel 2
        - BL Valve 1V5
          - EL Valve 1V5

SF Penetration of the laser scanner's detection

PLr	d
PL	d
PFH [1/h]	5,12E-7

SB Hydraulic control part

PL	e
PFH [1/h]	6,2E-8
Cat.	3
MTTFd [a]	88,1 (High)
DCavg [%]	86 (Low)
CCF	90 (fulfilled)

Channel 1

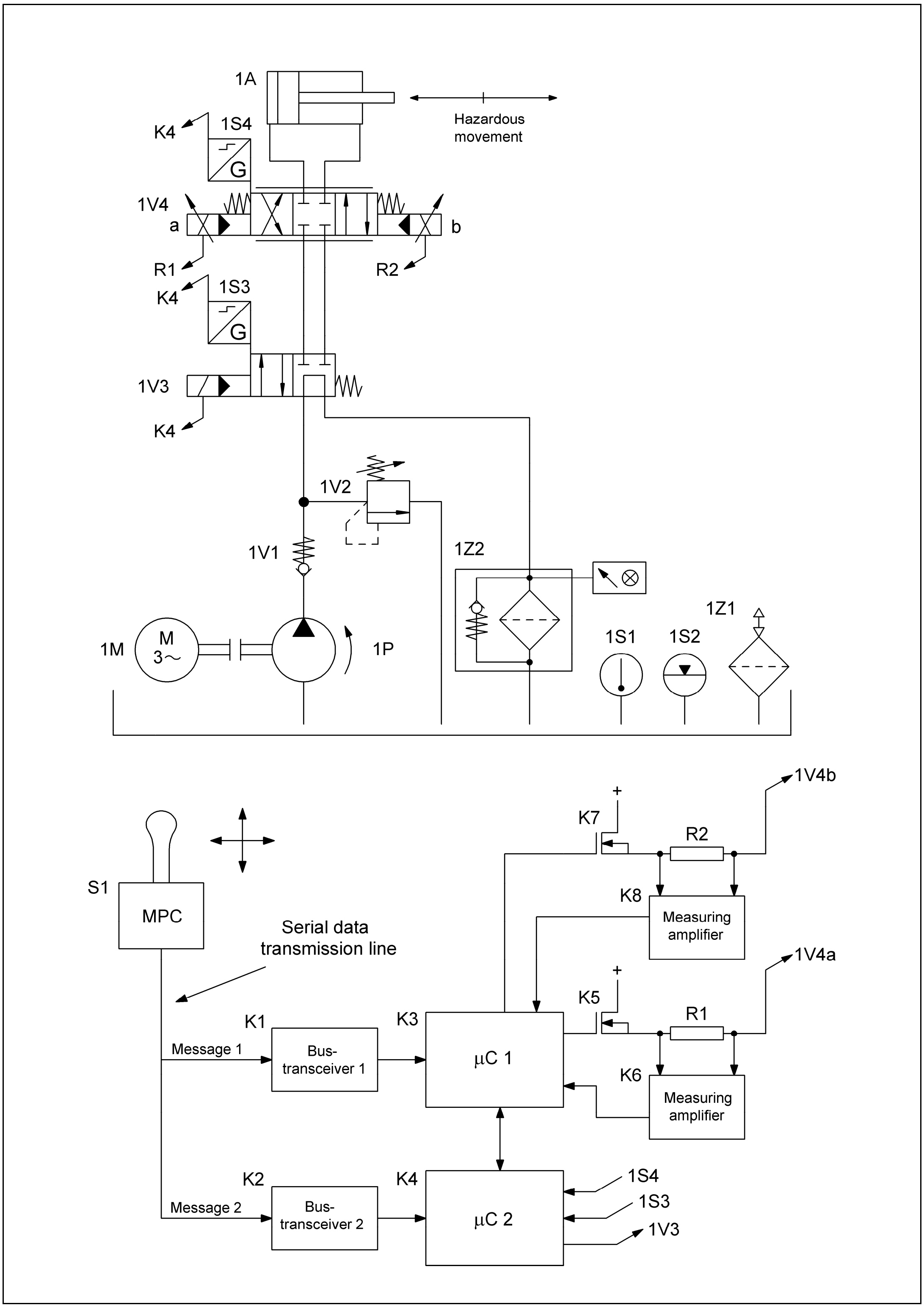
Name	DC [%]	MTTFd [a]
BL Valve 1V3	99 (High)	150 (-)
BL Valve 1V4	99 (High)	150 (-)

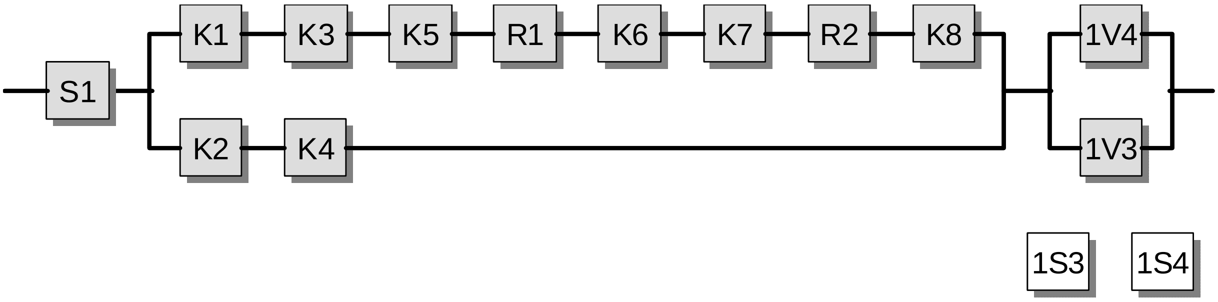
Channel 2

Name	DC [%]	MTTFd [a]
BL Valve 1V5	60 (Low)	150 (-)

8.2.16 Earth-moving machine control system with bus system – Category 3 – PL d (Example 16)

Figure 8.30:
Control of hazardous movements of an earth-moving machine





Safety function

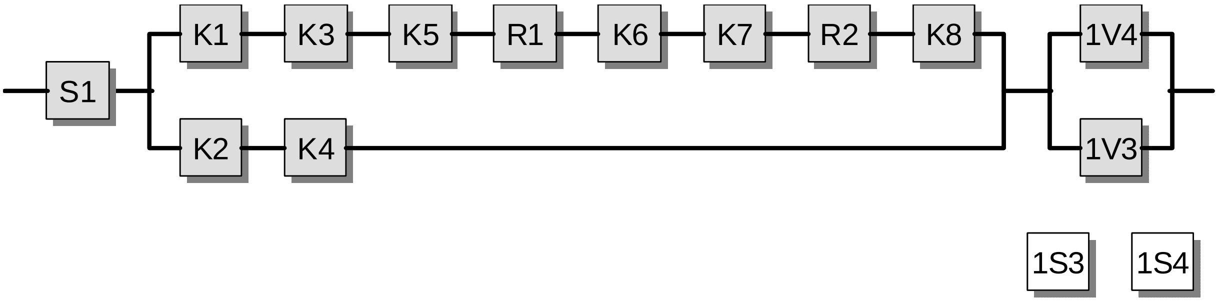
- Prevention of unexpected start-up: avoidance of unexpected movements of tools on earth-moving machines

Functional description

- The multi-purpose control (MPC) S1 converts the operator's manual movement of it into electronic messages. It sends these messages cyclically over a serial data communications line (bus system) to the logic control, which generates control signals for the hydraulics which then execute the working movements of the earth-moving machine desired by the user.
- The message 1 sent by the MPC S1 reaches the microcontroller K3 via the bus transceiver K1. From message 1 and in accordance with the algorithms stored in the software, K3 generates the analogue signals required for actuation of the proportional valve 1V4. The resistances R1/R2 and the measuring amplifiers K6/K8 have the function of controlling the output currents for the proportional valve. The microcontroller K4 receives a redundant message 2 from S1 over the bus transceiver K2. K4 checks the correct displacement of the proportional valve 1V4, as signalled by the position measuring system 1S4 integrated into 1V4, for plausibility against the desired position determined from message 2. Should faults be detected, K4 switches off the hydraulic pressure at a higher level by means of a directional control valve 1V3, and places the system in the safe state.

Design features

- Basic and well-tried safety principles are observed and the requirements of Category B are met. Protective circuits (e.g. contact protection) as described in the initial paragraphs of Chapter 8 are implemented.
- The MPC is a safety component suitable for use in PL d and satisfies the requirements for Category 3.
- The proportional valve 1V4 and the directional control valve 1V3 have a closed position/closed centre position, spring return/spring-centering, and sufficient overlap.
- The software (SRESW) for K3 and K4 is programmed in accordance with the requirements for PL d and the instructions in Section 6.3.



- Data transfer from the MPC to the logic control is safe in accordance with GS-ET-26 and IEC 61784-3. The data communications protocol employed contains redundant messages and measures for detection of the following transmission errors: repetition, loss, insertion, incorrect sequence, corruption and delay (see also Section 6.2.17). The residual error rate Λ is lower than 1 × 10^{-8} per hour and thus contributes, as specified in the principles for assessment, less than 1% towards the maximum permissible probability of failure of the safety function. This low percentage can be disregarded within the calculation of the overall probability of failure.

Remarks

- An emergency motion function of the earth-moving machine, which is not shown here, may be required; if so, it must be implemented at a higher level.

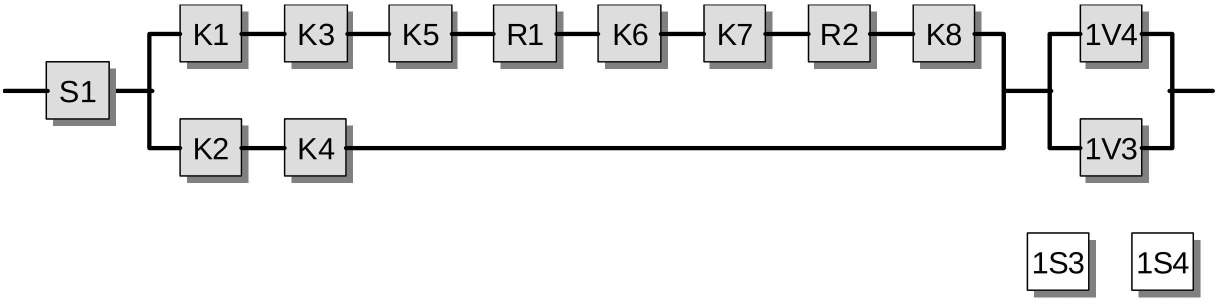
Calculation of the probability of failure

- The multi-purpose control S1 is a standard safety component. The associated probability of failure is added at the end of the calculation (PFH_{MPC} = 3.0 × 10^{-7} per hour [E]). For the remaining part of the control system, the probability of failure is calculated below.

- $MTTF_{\mathrm{d}}$ of the logic control: an $MTTF_{\mathrm{d}}$ of 11,415 years [D] is assumed for the bus transceivers K1 and K2. In accordance with SN 29500-2, an $MTTF_{\mathrm{d}}$ of 878 years [D] is considered for the microcontrollers K3 and K4, including peripherals. The following values are substituted for the remaining components [D]: 45,662 years for the switching transistors K5 and K7, 228,310 years for the resistances R1 and R2, and 1,141 years for the measuring amplifiers K6 and K8. The $\mathrm{MTTF}_{\mathrm{d}}$ values of the channels are thus 329 years and 815 years. Following capping to 100 years, the resulting symmetrized $\mathrm{MTTF}_{\mathrm{d}}$ value is 100 years.

- DC_{avg} of the logic control: the *DC* is 99% for K1 and K2 owing to cross-checking of the messages in the microcontrollers K3 and K4; the *DC* is 60% for K3 and K4 owing to cross-checking and self-tests of simple effectiveness achieved by software; and the *DC* is 90% for the remaining components owing to fault detection in K4 by means of the position measuring system 1S4. The averaging formula for DC_{avg} produces a result of 74% (“low”).

- Adequate measures against common cause failure (65 points): separation (15), overvoltage protection (15) and environmental conditions (25 + 10)



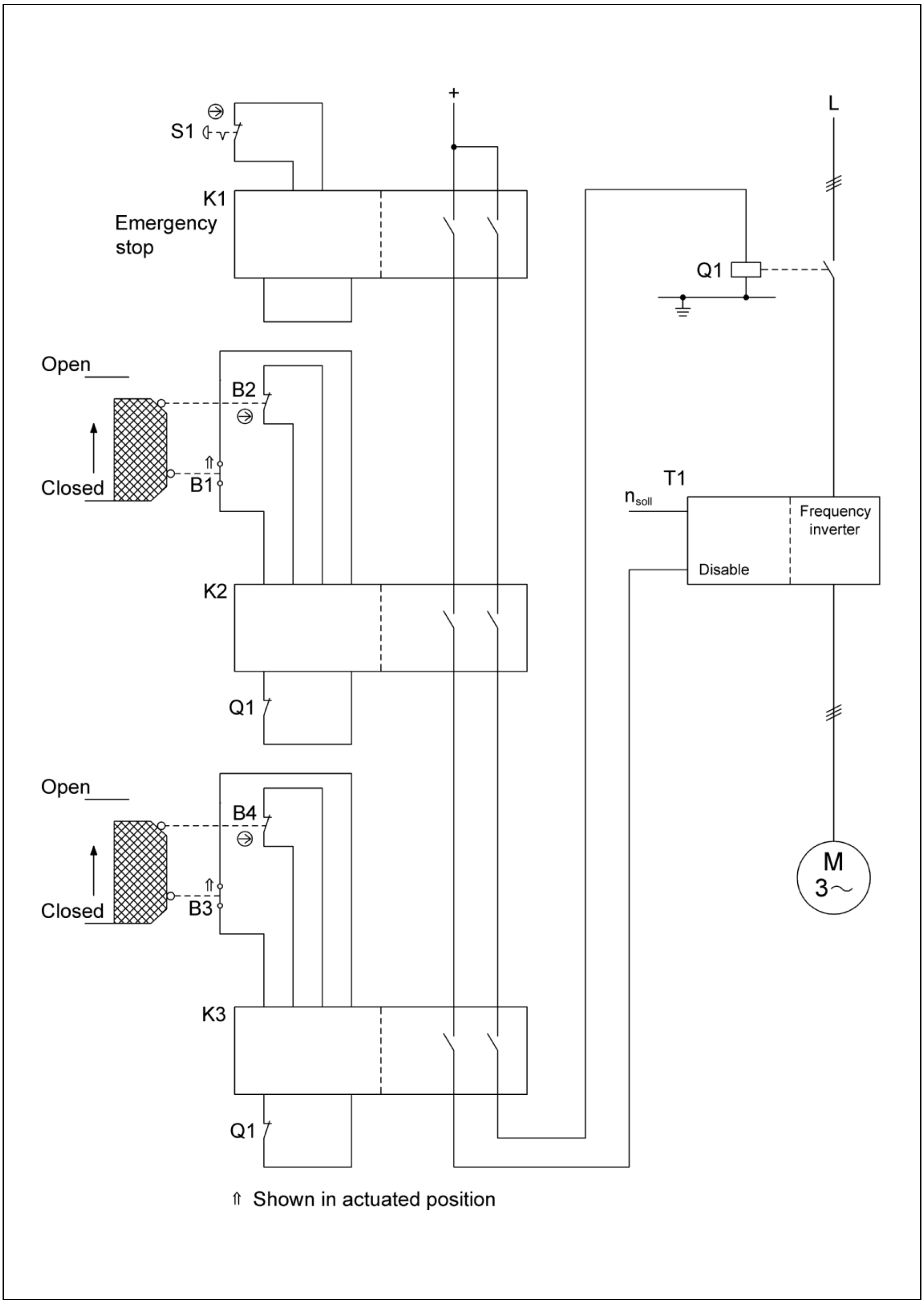
- The logic control corresponds to Category 3 with a high *MTTF*$_d$ per channel (100 years) and low *DC*$_{avg}$ (74%). This results in an average probability of dangerous failure of 7.36 × 10^{-8} per hour.
- *MTTF*$_d$ of the hydraulic part of the control system: an *MTTF*$_d$ of 150 years [S] is substituted for the proportional valve 1V4 and the directional control valve 1V3. Following capping, this results in a symmetrized MTTF$_d$ value of 100 years.
- *DC*$_{avg}$ of the hydraulic part of the control system: the DC for 1V4 and 1V3 is 99% owing to direct monitoring of the position in K4 via 1S4/1S3. The averaging formula for *DC*$_{avg}$ produces a result of 99% (“high”).
- Adequate measures against common cause failure (70 points): separation (15), the use of well-tried components (5), overpressure protection (15) and environmental conditions (25 + 10)
- The hydraulic part of the control system corresponds to Category 4 with a high *MTTF*$_d$ per channel (100 years) and a high *DC*$_{avg}$ (99%). This results in an average probability of dangerous failure of 2.47 × 10^{-8} per hour.
- The average probability of dangerous failure of the safety function is produced by addition of the proportions for the MPC, the logic control and the hydraulic part. The total is 3.98 × 10^{-7} per hour. This corresponds to PL d.

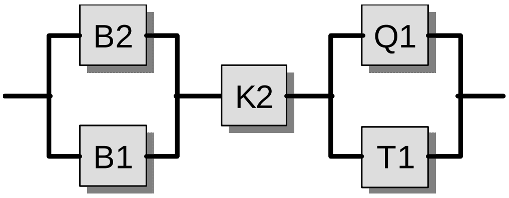
More detailed references

- ISO 15998: Earth-moving machinery – Machine control systems (MCS) using electronic components – Performance criteria and tests for functional safety (04.08)
- IEC 61784-3: Industrial communication networks – Profiles – Part 3: Functional safety fieldbuses – General rules and profile definitions (12.07)
- Prüfgrundsätze Bussysteme für die Übertragung sicherheitsrelevanter Nachrichten GS-ET-26. Ed.: Fachausschuss Elektrotechnik, Cologne 2002. www.dguv.de, Webcode d14884

8.2.17 Cascading of protective devices by means of safety modules – Category 3 – PL d (Example 17)

Figure 8.31:
Cascading of protective devices by means of safety modules (emergency stop function, STO)





Safety functions

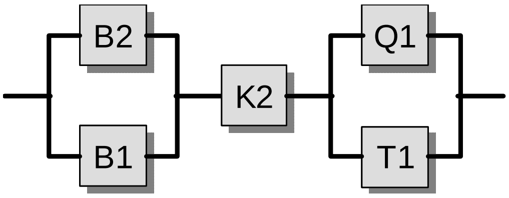
- Emergency stop function, STO – safe torque off by actuation of the emergency stop device
- Safety-related stop function, initiated by a protective device: opening of the moveable guard initiates the safety function STO – safe torque off.

Functional description

- Actuation of the emergency stop device S1 causes hazardous movements or states to be de-energized redundantly via the safety module K1, by interruption of the control voltage of the contactor Q1 and selection of the controller inhibit of the frequency inverter T1. A hazardous zone is also guarded by two moveable guards (e.g. one each for loading and unloading). Opening of the safety guard is detected by two position switches B1/B2 in a break contact/make contact combination, and evaluation by a central safety module K2. The latter can interrupt or prevent hazardous movements or states in the same way as K1. The second safety guard is monitored in the same way by the two position switches B3/B4 and a safety module K3, also acting upon Q1 and T1.
- The safety function is retained in the event of a component failure.
- The majority of component failures are detected and lead to operating inhibition. The two position switches on a safety guard are monitored for plausibility in the associated safety module. The safety module also employs internal diagnostics measures. Faults in the contactor Q1 are detected by means of mechanically linked contacts and their readback in K2 and K3. Additional readback in K1 is not necessary, since a demand for the emergency stop function is much less frequent. A part of the faults in T1 are detected by the process. A small number of faults are not detected by the controller.

Design features

- Basic and well-tried safety principles are observed and the requirements of Category B are met. Protective circuits (e.g. contact protection) as described in the initial paragraphs of Chapter 8 are implemented.
- A stable arrangement of the protective devices is assured for actuation of the position switches.
- The emergency stop device S1 corresponds to EN ISO 13850; B2 and B4 are position switches with direct opening contact to IEC 60947-5-1, Annex K.
- The supply conductors to the position switches B1 and B4 are laid separately or with protection.



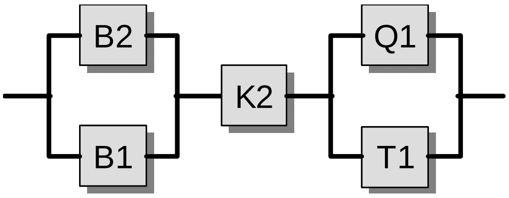
- The contactor Q1 possesses mechanically linked contact elements in accordance with IEC 60947-5-1, Annex L.
- The safety modules K1, K2 and K3 satisfy all the requirements for Category 4 and PL d.
- The frequency inverter T1 has no integral safety function.

Remark

- The emergency stop function is a complementary protective measure to EN ISO 12100-2:2004.

Calculation of the probability of failure

- The circuit arrangement can be divided into three safety functions, each of which is assigned to three subsystems. The safety-related block diagram shows the safety-related stop function with reference to an example for one protective device, since only one protective device is open at any one time. The same safety function and an identical calculation of the probability of failure apply to the second protective device. For the emergency stop function, the emergency stop device S1 and the safety module K1 take the place of the first two subsystems. The probability of failure of the standard safety modules K1, K2 and K3 is added at the end of the calculation (2.31 × 10^{-9} per hour [M], suitable for PL e). For the remaining subsystems, the probability of failure is calculated as follows.
- S1 is a standard emergency stop device to EN ISO 13850. Fault exclusion applies for the direct opening contact and the mechanical elements, provided the number of operations indicated in Table D.2 of this report is not exceeded. Three actuations per year is assumed for n_{op}. This value is ignored for the purpose of further calculation for both safety functions with regard to the overall circuitry of Q1 and the frequency inverter.
- $MTTF_d$: fault exclusion is possible for the electrical contact of the position switch B2 with direct opening action. For the electrical make contact of the position switch B1, the B_{10d} value is 1,000,000 switching operations [M]. A B_{10d} value of 1,000,000 cycles [M] is stated for the mechanical part of B2 and B1. At 365 working days, 16 working hours and a cycle time of 10 minutes, n_{op} is 35,040 cycles per year for these components, and the $MTTF_d$ is 285 years for B2 and 142 years for B1. For the contactor Q1, the B_{10} value corresponds under inductive load (AC 3) to an electrical life of 1,000,000 switching operations [M]. If 50% of failures are assumed to be dangerous, the B_{10d} value is produced by doubling of the B_{10} value. Since Q1 is involved in both safety-related stop functions,

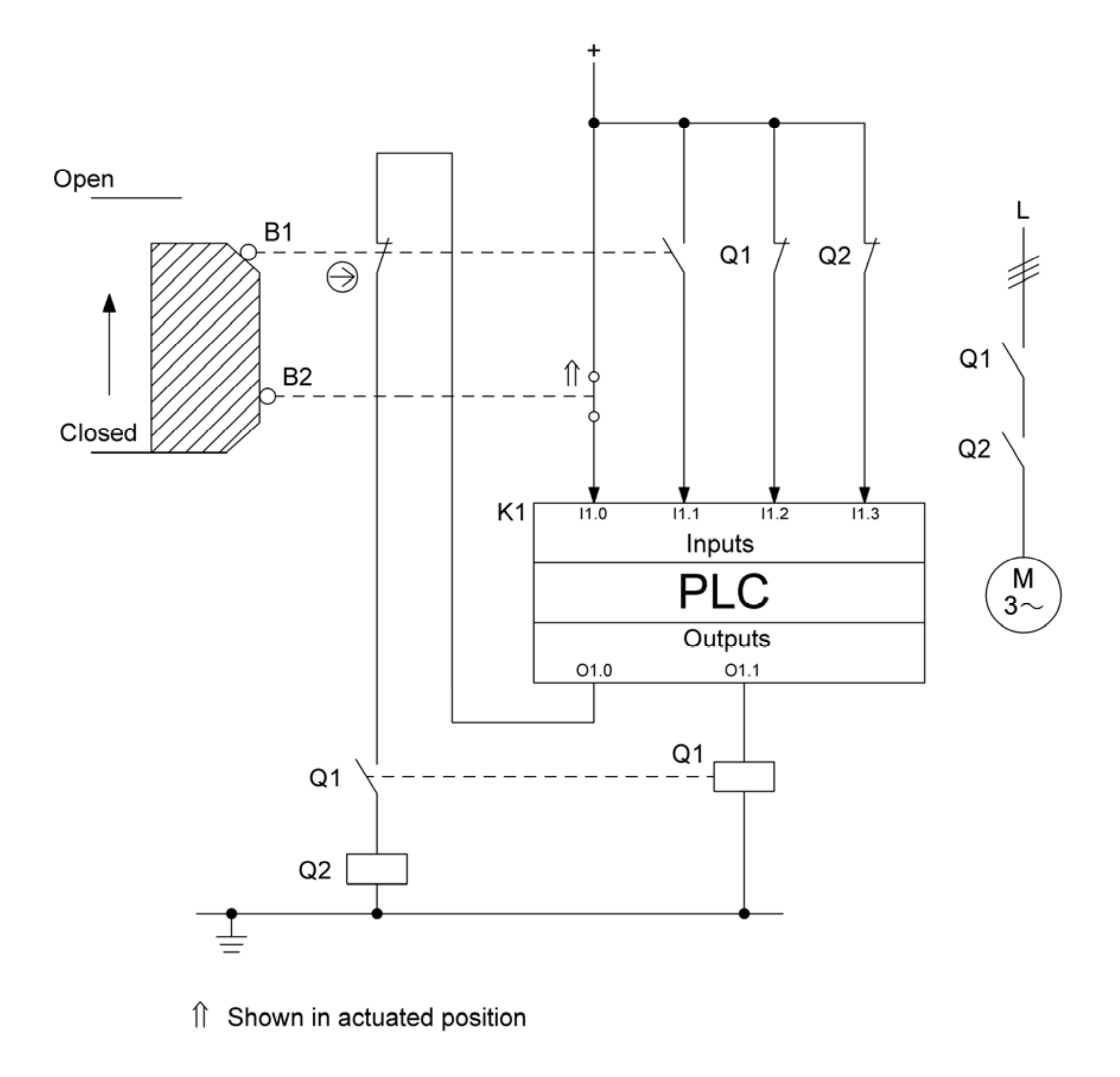


double the value assumed above for n_{op} results in an $MTTF_d$ of 285 years. The $MTTF_d$ for the frequency inverter T1 is 20 years [M]. Altogether, the symmetrized $\mathrm{MTTF_d}$ value per channel in the subsystem Q1/T1 is 68 years ("high").

- DC_{avg}: the *DC* of 99% for B1 and B2 is based upon plausibility monitoring of the break contact/make contact combination in K2. This corresponds to the DC_{avg} for the subsystem. The *DC* of 99% for the contactor Q1 is derived from readback of the contact position in the safety modules. Fault detection by the process yields a *DC* of 60% for the frequency inverter T1. Averaging thus results in a DC_{avg} of 62% ("low") for the subsystem Q1/T1.
- Adequate measures against common cause failure in subsystems B1/B2 and Q1/T2 (70 and 85 points respectively): separation (15), protection against overvoltage etc. (15) and environmental conditions (25 + 10), well-tried components in B2/B1 (5), diversity in Q1/T1 (20)
- The subsystem B1/B2 corresponds to Category 3 with a high $MTTF_d$ (100 years) and high DC_{avg} (99%). This results in an average probability of dangerous failure of 2.47×10^{-8} per hour. The subsystem Q1/T1 corresponds to Category 3 with a high $MTTF_d$ (68 years) and low DC_{avg} (62%). This results in an average probability of dangerous failure of 1.73×10^{-7} per hour.
- For the safety-related stop function, the resulting average probability of dangerous failure is 2.00×10^{-7} per hour. This corresponds to PL d.
- The resulting average probability of dangerous failure for the emergency stop function is 1.75×10^{-7} per hour. This corresponds to PL d.

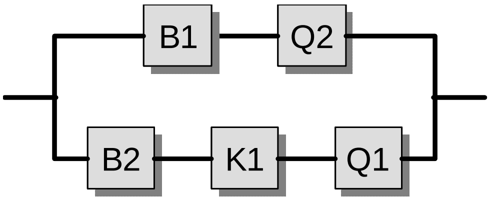
8.2.18 Position monitoring of a moveable guard – Category 3 – PL d (Example 18)

Figure 8.32:
Redundant position monitoring of a moveable guard employing diversity in its technical implementation (electromechanical and programmable electronic)



Safety function

- Safety-related stop function, initiated by a protective device: opening of the moveable guard (protective grating) initiates the safety function STO (safe torque off).

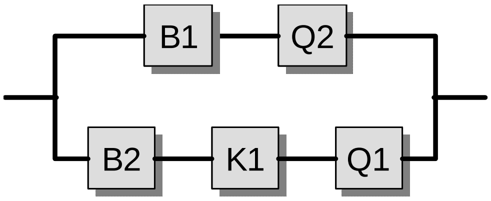


Functional description

- Opening of the moveable guard (e.g. safety guard) is detected by two position switches B1 and B2 in a break contact/make contact combination. The position switch B1 with direct opening contact actuates a contactor Q2 which interrupts/ prevents hazardous movements or states when it drops out. The position switch B2 with make contact is read in by a standard PLC K1, which can bring about the same de-energization response by actuation of a second contactor Q1.
- The safety function is retained in the event of a component failure.
- The switching position of B1 is also read into the PLC K1 by means of a make contact, and is compared for plausibility with the switching position of B2. The switching positions of the contactors Q1 and Q2 are likewise monitored in K1 by mechanically linked readback contacts. Component failures in B1, B2, Q1 and Q2 are detected by K1 and lead to operating inhibition owing to the dropping-out of Q1 and Q2. Faults in the PLC K1 are detected only by the function (fault detection by the process).

Design features

- Basic and well-tried safety principles are observed and the requirements of Category B are met. Protective circuits (e.g. contact protection) as described in the initial paragraphs of Chapter 8 are implemented.
- A stable arrangement of the protective device is assured for actuation of the position switch.
- B1 is a position switch with direct opening contact in accordance with IEC 60947-5-1, Annex K.
- The supply conductors to the position switches are laid separately or with protection.
- Faults in the start-up and actuation mechanism are detected by the use of two position switches differing in the principle of their actuation (break and make contacts).
- Q1 and Q2 possess mechanically linked contact elements to IEC 60947-5-1, Annex L.
- The PLC K1 satisfies the normative requirements described in Section 6.3.



Calculation of the probability of failure

- $MTTF_d$: fault exclusion is possible for the electrical contact of the position switch B1 with direct opening contact. For the electrical make contact of the position switch B2, the B_{10d} is 1,000,000 switching operations [M]. A B_{10d} value of 1,000,000 cycles [M] is stated for the mechanical part of B1 and B2. At 365 working days, 16 working hours per day and a cycle time of 1 hour, n_{op} is 5,840 cycles per year for these components, and the $MTTF_d$ is 1,712 years for B1 and 856 years for B2. For the contactors Q1 and Q2, the B_{10} value under inductive load (AC3) corresponds to an electrical life of 1,300,000 switching operations [M]. If 50% of failures are assumed to be dangerous, the B_{10d} value is produced by doubling of the B_{10} value. The above assumed value for n_{op} results in an $MTTF_d$ of 4,452 years for Q1 and Q2. An MTTF value of 15 years [M] is substituted for the PLC, resulting through doubling in an $MTTF_d$ value of 30 years. The combination of B1 and Q2 results in an $MTTF_d$ of 1,236 years for the first channel; B2, K1 and Q2 contribute to an $MTTF_d$ of 28 years in the second channel. Altogether, the $MTTF_d$ value symmetrized over both channels is 70 years per channel ("high").
- DC_{avg}: the *DC* of 99% for B1 and B2 is based upon plausibility monitoring of the two switching states in the PLC K1. The *DC* of 99% for the contactors Q1 and Q2 is derived from readback via mechanically linked contact elements, also in K1. Owing to the possibility of fault detection by the process, a *DC* of 60% is assumed for K1. Averaging thus results in a DC_{avg} of 62% ("low").
- Adequate measures against common cause failure (65 points): separation (15), overvoltage protection etc. (15) and environmental conditions (25 + 10)
- The combination of the control elements corresponds to Category 3 with a high $MTTF_d$ (70 years) and low DC_{avg} (62%). This results in an average probability of dangerous failure of 1.66×10^{-7} per hour. This corresponds to PL d.

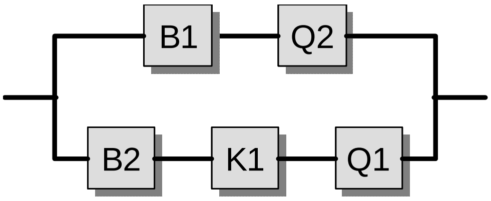
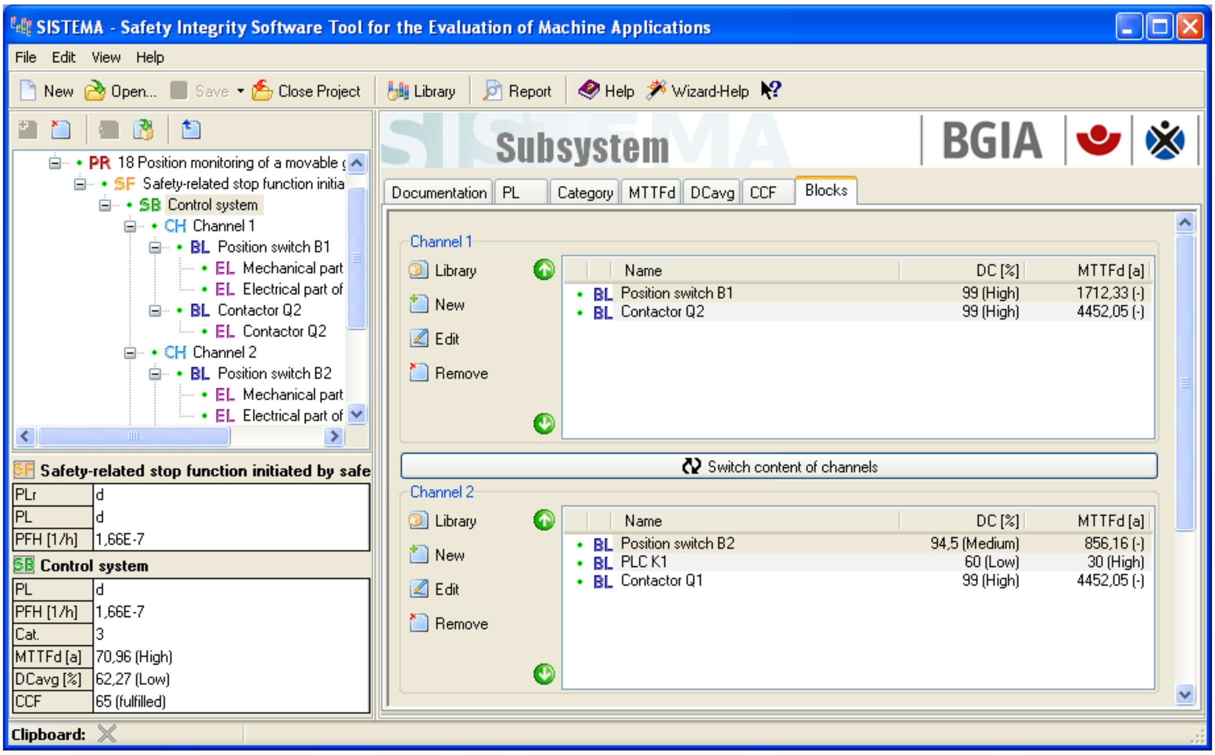


Figure 8.33:
Determining of the PL by means of SISTEMA


SISTEMA - Safety Integrity Software Tool for the Evaluation of Machine Applications
File Edit View Help
New Open... Save Close Project Library Report Help Wizard-Help
Subsystem
BGIA
Documentation PL Category MTTFd DCavg CCF Blocks
Library
New
Edit
Remove
Switch content of channels
Clipboard:

- PR 18 Position monitoring of a movable g
  - SF Safety-related stop function initia
    - SB Control system
      - CH Channel 1
        - BL Position switch B1
          - EL Mechanical part
          - EL Electrical part of
        - BL Contactor Q2
          - EL Contactor Q2
      - CH Channel 2
        - BL Position switch B2
          - EL Mechanical part
          - EL Electrical part of

SF Safety-related stop function initiated by safe

PLr	d
PL	d
PFH [1/h]	1,66E-7

SB Control system

PL	d
PFH [1/h]	1,66E-7
Cat.	3
MTTFd [a]	70,96 (High)
DCavg [%]	62,27 (Low)
CCF	65 (fulfilled)

Channel 1

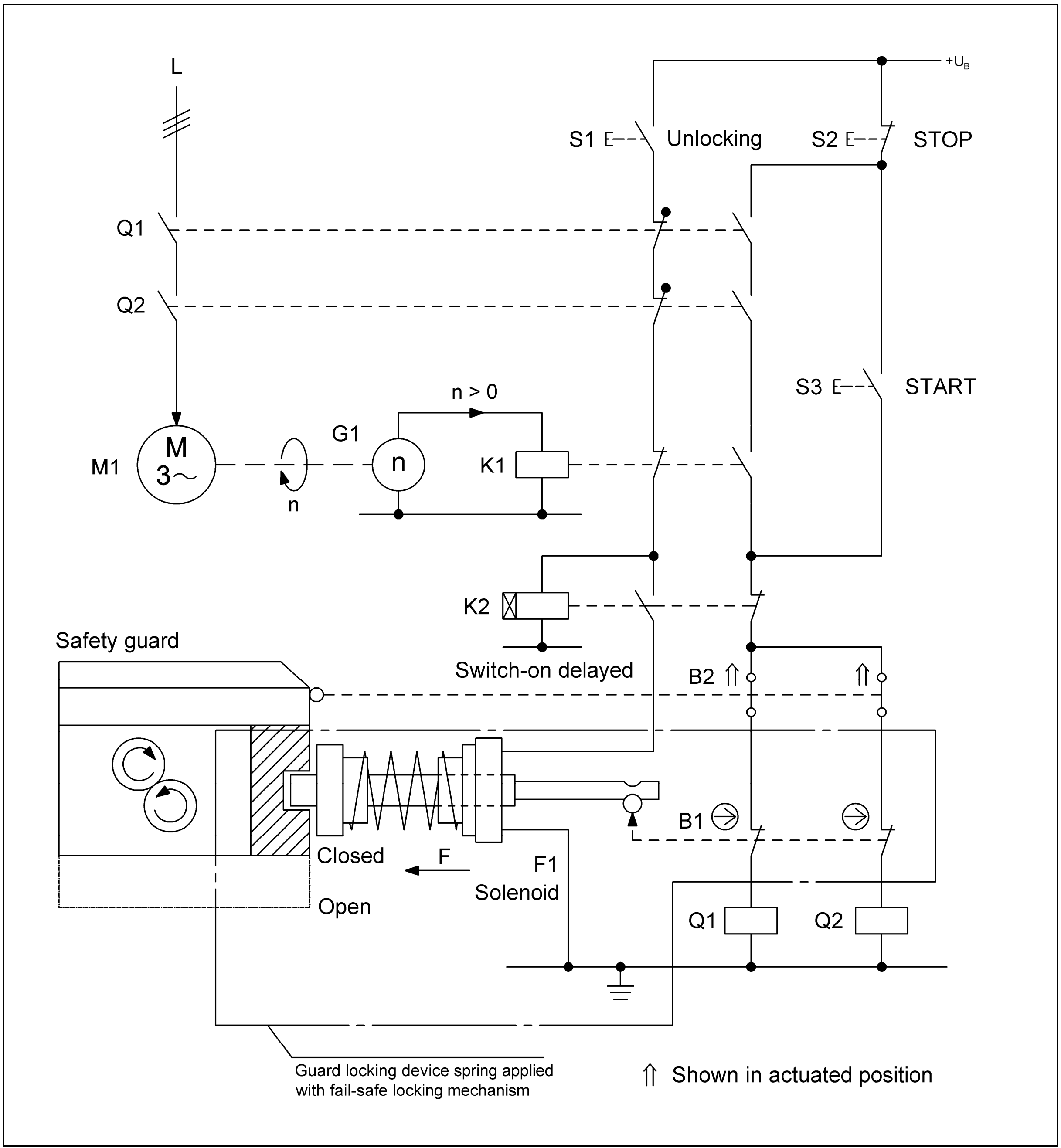
Name	DC [%]	MTTFd [a]
BL Position switch B1	99 (High)	1712,33 (-)
BL Contactor Q2	99 (High)	4452,05 (-)

Channel 2

Name	DC [%]	MTTFd [a]
BL Position switch B2	94,5 (Medium)	856,16 (-)
BL PLC K1	60 (Low)	30 (High)
BL Contactor Q1	99 (High)	4452,05 (-)

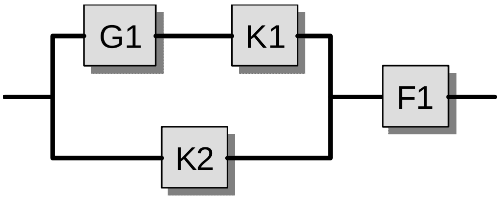
8.2.19 Interlocked guard with guard locking – Category 3 – PL d (Example 19)

Figure 8.34:
Guard locking on a safety guard employing relay technology – Category 3



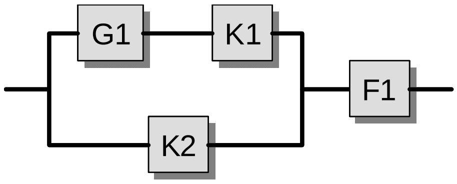
Safety functions

- No deactivation of guard locking at speeds greater than zero
- Prevention of unexpected start-up from rest whilst the safety guard is open



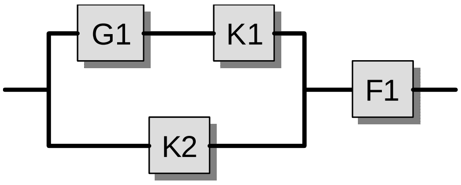
Functional description

- Access to hazardous movement is blocked by a safety guard with guard locking until the moving part has come to rest. The guard is closed by a positive-locking, spring-actuated safety bolt, which is withdrawn electromagnetically for opening of the guard. The position of the locking bolt is monitored by the integral position switch B1; the position of the safety guard is monitored in addition by the position switch B2, in order to increase the immunity to bypassing. The interlocked guard with integral spring-actuated guard locking also features a fail-safe locking mechanism.
- The hazardous movement can be initiated from the start button S3, only with the safety guard closed and with the locking bolt pushed in by spring force. In this position, position switch B1 is released, position switch B2 actuated. Under these conditions, the break contacts of B1 are closed, as are the make contacts of B2. Connection of these contacts in series enables the actuation of the motor contactors Q1 and Q2. The safety-related block diagram for the safety function “prevention of unexpected start-up from rest when the safety guard is open” (not shown here) therefore comprises two redundant channels, B1-Q1 and B2-Q2, where the simplification on the safe side is employed. Alternatively, B1-Q2 and B2-Q1 may be selected. Should these two models yield different values for the $MTTF_\mathrm{d}$ per channel, the higher $MTTF_\mathrm{d}$ can be used for calculation of the probability of failure.
- Opening of the safety guard during the hazardous movement is prevented with single-fault tolerance. This is achieved by inclusion of the following in the actuation circuit for the solenoid F1: one break contact (mirror contact) each of the contactors Q1 and Q2 and of the zero-speed relay K1, which acts upon the speed information from the tachometer G1 and the make contact of the contactor K2 with switch-on delay.
- Opening of the safety guard during coasting down of the motor following actuation of the stop button S2 and of the unlocking button S1 is prevented with single-fault tolerance. This is achieved by the break contact of the zero-speed relay K1 (based upon the speed information from G1) and the make contact of the contactor G1 with switch-on delay being included in the actuation circuit of the solenoid F1 (see safety-related block diagram).
- Once the motor has come to a halt (Q1, Q2 and K1 have dropped out), actuation of the unlocking button S1 causes the contactor K2 with switch-on delay to be actuated, the solenoid F1 to be activated, and thus the safety bolt to be withdrawn from the safety guard. Whilst the safety guard is open, the position switch B1 remains positively actuated and bypass-proof. Unexpected start-up from rest is also prevented by the position switch B2 (not actuated).



Design features

- Basic and well-tried safety principles are observed and the requirements of Category B are met. Protective circuits (e.g. contact protection) as described in the initial paragraphs of Chapter 8 are implemented.
- The electrical lines are laid in the electrical compartment or take the form of separate multicore cables.
- The contactor relays K1 and K2 possess mechanically linked contact elements in accordance with IEC 60947-5-1, Annex L.
- The contactors Q1 and Q2 possess mirror contacts in accordance with IEC 60947-4-1, Annex F.
- A stable arrangement of the protective device is assured for actuation of the position switch.
- The position switch B1 features direct opening action in accordance with IEC 60947-5-1, Annex K.
- The interlocked guard implemented in the circuit (broken line in Figure 8.34) includes both the guard locking device with the spring-return release solenoid, and the position switch B1 required for position monitoring of the safety bolt and the safety guard. These are housed in an enclosure and therefore are not accessible from outside.
- The spring of the guard locking device is a well-tried spring to EN ISO 13849-2, Annex A.3. In addition, the spring is permanently fail-safe to EN 13906-1. The criteria set out in GS-ET-19, Section 5.5.1 are observed. The solenoid F1 does not pick up without voltage: with simultaneous fault exclusion for the fault assumption “breakage of the blocking device”, this therefore results in exclusion of dangerous faults for these elements altogether.
- The design arrangement of the fail-safe locking mechanism for the guard locking device assures that the safety bolt cannot assume the blocked position (guard locking position) whilst the safety guard is open.
- Not shown in Figure 8.34 are the additional functions integrated in a guard locking arrangement of “emergency unlock” and “escape” for deliberate manual opening of the protective device in the event of a hazard: these functions act positively upon the blocking device without tools and irrespective of the operating state; refer in this context to the test principles of GS-ET-19.
- The standard component G1 is employed in accordance with the instructions in Section 6.3.10.



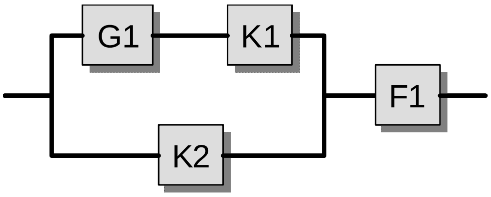
Calculation of the probability of failure

The probability of undesired disabling of the guard locking device/safety function “no disabling of guard locking at speeds greater than zero” (refer also to the safety-related block diagram) is first calculated.

- *MTTF*$_d$: for K1 and K2, the B_{10d} value is 400,000 cycles [S]. At 240 working days, 8 working hours and a cycle time of 10 minutes, n_{op} is 11,520 cycles per year and the *MTTF*$_d$ is 347 years for these components. For the electronic part of the switch-on delay in K2, an *MTTF*$_d$ of 1,000 years is assumed [E]. K2 thus has an overall *MTTF*$_d$ of 257 years. No manufacturer's figure is available for G1; an *MTTF*$_d$ of 30 years is assumed [E]. These values produce a symmetrized *MTTF*$_d$ per channel of 70 years.
- *DC*$_{avg}$: owing to the mechanical linking of the contacts, faulty states of K1 or K2 lead to sustained failure of the unlocking of the guard locking facility or of the motor energy. As a result, fault detection is provided by the process and a *DC* of 99% is assumed. A drift in the switching threshold of G1 can be detected by the process. A *DC* of 60% is therefore assumed. No fault detection is provided for failure of the switch-on delay of K2. This results in a *DC*$_{avg}$ of 64%.
- Adequate measures against common cause failure (70 points): separation (15), overvoltage protection etc. (15), use of well-tried components (5) and environmental conditions (25 + 10)
- Together with fault exclusion for the further elements of the guard locking device (see above), the combination of the control elements corresponds to Category 3 with a high *MTTF*$_d$ per channel (70 years) and low *DC*$_{avg}$ (64%). This results in an average probability of dangerous failure of 1.62×10^{-7} per hour. This corresponds to PL d.

Calculation of the probability for the safety function “prevention of unexpected start-up from rest whilst the safety guard is open” yields the following result.

- *MTTF*$_d$: for the position switch B1, a B_{10d} value of 20,000,000 cycles [S] is assumed owing to its direct opening action. At the assumed n_{op} value of 11,520 cycles per year indicated above, the associated MTTF$_d$ value is 17,361 years. A B_{10d} value of 100,000 cycles [E] is assumed for the position switch B2 (see also Table D.2); the associated MTTF$_d$ value is 86 years. For Q1 and Q2, the B_{10d} value is 400,000 cycles [S]. The same n_{op} produces an *MTTF*$_d$ of 347 years for each component. These values produce a symmetrized *MTTF*$_d$ per channel of 85 years.



- *DC*$_{avg}$: at the assumed high switching frequency, faulty states on all elements are detected with a *DC* in each case of 99%, e.g. by fault detection via the process. This leads to a *DC*$_{avg}$ also of 99%.
- Adequate measures against common cause failure (70 points): see above
- The combination of the control elements corresponds to Category 4 with a high *MTTF*$_d$ per channel (85 years) and high *DC*$_{avg}$ (99%). This results in an average probability of dangerous failure of 2.93 × 10^{-8} per hour. This corresponds to PL e. PL$_r$ d is thus surpassed, which with the required two-channel design of the hardware with few components, the use of B$_{10d}$ values in accordance with the standard, a *DC* of "high" and a "moderate" switching frequency will virtually always be the case.
- The wearing element B2 should be replaced approximately every eight years (T_{10d}).

More detailed references

- *Reudenbach, R.*: Maßnahmen gegen das Umgehen von Verriegelungseinrichtungen an Schutztüren. Die BG (2003) No. 7, pp. 275-281. www.diebg.info/download/reudenbach.pdf
- *Apfeld, R.; Huelke, M.; Lüken, K.; Schaefer, M.* et al.: Manipulation von Schutzeinrichtungen an Maschinen. HVBG-Report. Ed.: Hauptverband der gewerblichen Berufsgenossenschaften, Sankt Augustin 2006. www.dguv.de/bgia, Webcode d6303
- Grundsätze für die Prüfung und Zertifizierung von Verriegelungseinrichtungen mit elektromagnetischen Zuhaltungen GS-ET-19. Ed.: Fachausschuss Elektrotechnik, Cologne 2004. www.dguv.de, Webcode d14884
- Berufsgenossenschaftliche Information BGI 575: Merkblatt für die Auswahl und Anbringung elektromechanischer Verriegelungseinrichtungen für Sicherheitsfunktionen. Carl Heymanns, Cologne 2003
- EN 1088: Safety of machinery – Interlocking devices associated with guards – Principles for design and selection (12.95).
- EN 1088/A1: Safety of machinery – Interlocking devices associated with guards – Principles for design and selection (04.07)
- EN 13906-1: Cylindrical helical springs made from round wire and bar – Calculation and design – Part 1: Compression springs (04.02)

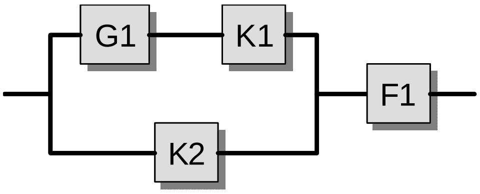
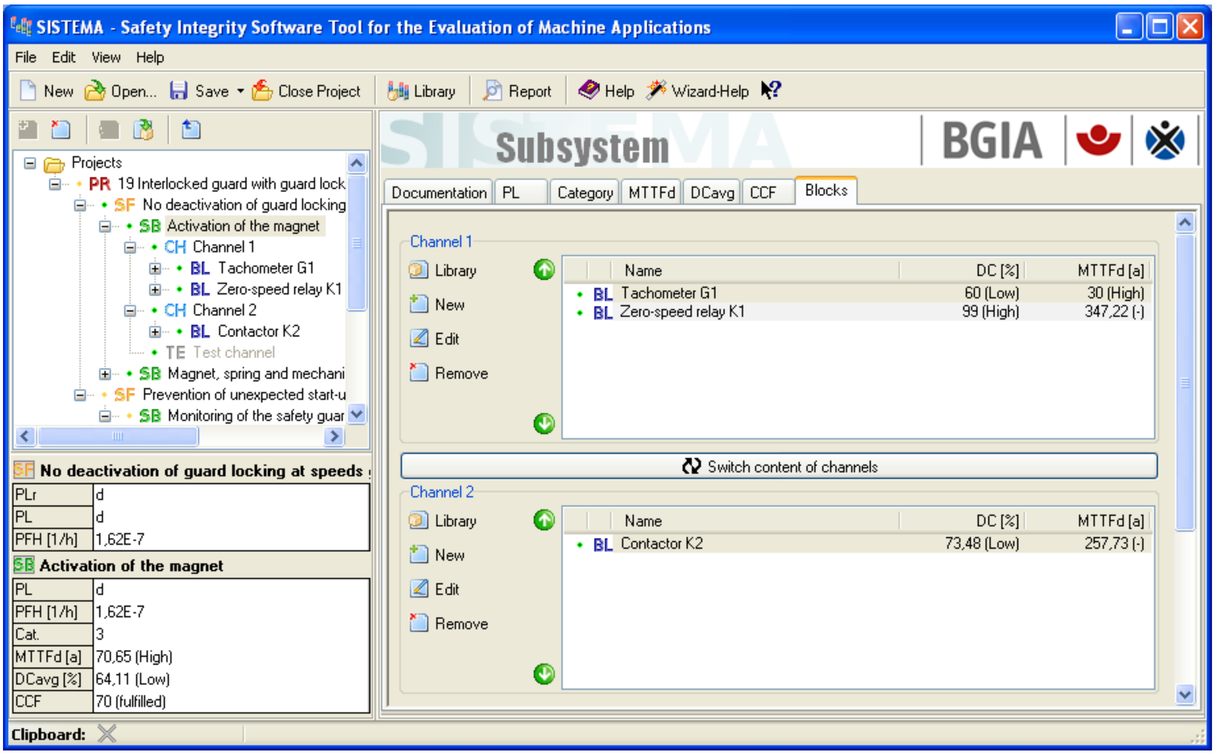


Figure 8.35:
Determining of the PL by means of SISTEMA


File Edit View Help
New Open... Save Close Project Library Report Help Wizard-Help
Subsystem
BGIA
Documentation PL Category MTTFd DCavg CCF Blocks
Library
New
Edit
Remove
Switch content of channels
Clipboard:

SISTEMA - Safety Integrity Software Tool for the Evaluation of Machine Applications

- Projects
  - PR 19 Interlocked guard with guard lock
    - SF No deactivation of guard locking
      - SB Activation of the magnet
        - CH Channel 1
          - BL Tachometer G1
          - BL Zero-speed relay K1
        - CH Channel 2
          - BL Contactor K2
        - TE Test channel
      - SB Magnet, spring and mechani
    - SF Prevention of unexpected start-u
      - SB Monitoring of the safety guar

SF No deactivation of guard locking at speeds

PLr	d
PL	d
PFH [1/h]	1,62E-7

SB Activation of the magnet

PL	d
PFH [1/h]	1,62E-7
Cat.	3
MTTFd [a]	70,65 (High)
DCavg [%]	64,11 (Low)
CCF	70 (fulfilled)

Channel 1

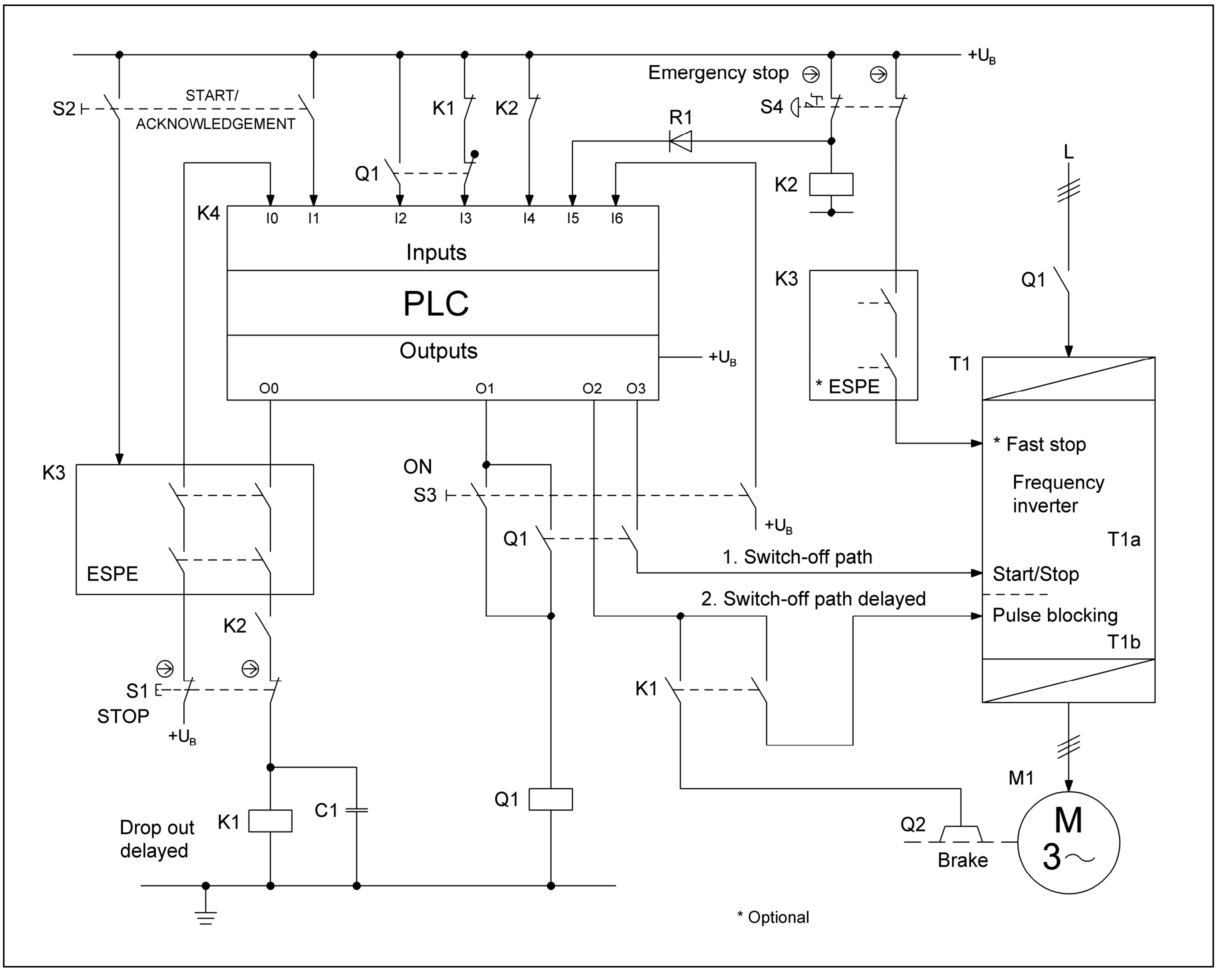
	Name	DC [%]	MTTFd [a]
BL	Tachometer G1	60 (Low)	30 (High)
BL	Zero-speed relay K1	99 (High)	347,22 (-)

Channel 2

	Name	DC [%]	MTTFd [a]
BL	Contactor K2	73,48 (Low)	257,73 (-)

8.2.20 Safe stopping of a PLC-driven drive – Category 3 – PL d (Example 20)

Figure 8.36:
Safe stopping of a PLC-driven frequency inverter drive following a stop or emergency stop command or following tripping of a protective device (in this case, an ESPE)

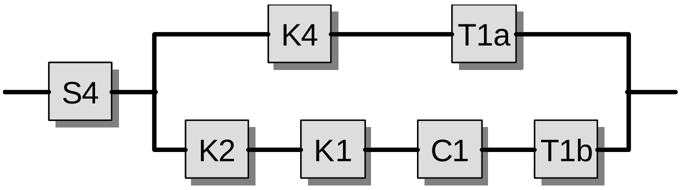


Safety function

- Safety-related stop function, initiated by a protective device: following a stop or emergency stop command or tripping of a protective device, the drive is halted (SS1 – safe stop 1).

Functional description

- The hazardous movement is interrupted redundantly if either the stop button S1 or the protective device K3 (shown in the circuit diagram as electro-sensitive protective equipment (ESPE)) is actuated. The drive is halted in an emergency following actuation of the emergency stop device S4. In all three cases, the first set braking time is implemented via the output O3 of the PLC K4 by deactivation of the “Start/Stop” input (T1a) on the frequency inverter (FI) T1. Redundantly to this arrangement, the second set braking time takes the form of deactivation of

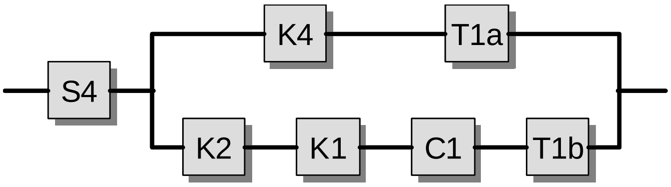


the “pulse blocking” input (T1b) on T1, which is achieved by de-energization of the contactor relay K1 (with the use of the capacitor C1 for drop-out delay), and application of the brake Q2. The first de-energization path is thus implemented directly by the PLC K4; conversely, the second de-energization path employs relay technology and delayed drop-out. The timer settings for O2 in the PLC program and for K1 are selected such that the machine movement is halted even under unfavourable operating conditions.

- Should a “fast stop” input with a particularly rapid speed reduction be available on the FI, the emergency stop device and ESPE may be connected to it if desired, as shown on the circuit diagram. This option is not considered further below.
- In the event of failure of the PLC K4, the frequency inverter inputs T1a/T1b, the contactor relay K1 with drop-out delay or the contactor relay K2, stopping of the drive is assured, since two mutually independent de-energization paths are always present. Failure of the auxiliary contactors K1 or K2 to drop out is detected, at the latest before renewed start-up of the machine movement, by the feedback of the mechanically linked break contacts to the PLC inputs I3 and I4.

Design features

- Basic and well-tried safety principles are observed and the requirements of Category B are met. Protective circuits (e.g. contact protection) as described in the initial paragraphs of Chapter 8 are implemented.
- Owing to the use of a frequency inverter with safe pulse blocking, the contactor Q1 is no longer absolutely essential for de-energization of the supply voltage. The frequency inverter must be suitable for ramping up and braking.
- The contactor relays K1 and K2 possess mechanically linked contact elements in accordance with IEC 60947-5-1, Annex L.
- The contacts of the pushbuttons S1 and S4 are mechanically linked in accordance with IEC 60947-5-1, Annex K.
- The standard components K4 and T1 are employed in accordance with the instructions in Section 6.3.10.
- The software (SRASW) is programmed in accordance with the requirements for PL c (downgraded owing to diversity) and the instructions in Section 6.3.
- If the brake Q2 is provided for functional reasons only, i.e. it is not involved in execution of the safety function, it is disregarded in the calculation of the probability of failure, as in this example. This procedure requires that coasting down of the drive in the event of a failure of T1a (see below), in which case



de-energization is effected by means of pulse blocking alone, is not associated with an unacceptably high residual risk. The involvement of a brake in execution of the safety function in conjunction with the use of an FI is described in the example of a revolving door control (Example 23).

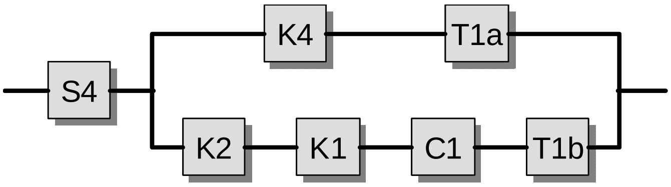
- The ESPE K3, for example in the form of a light curtain, satisfies the requirements for Type 4 to EN 61496-1 and IEC 61496-2, and for PL e.

Calculation of the probability of failure

- The probability of failure of safe stopping triggered by the emergency stop device S4 or by the ESPE, which is also shown on the safety-related block diagram, is calculated. The “fast stop” function of the FI and the facility for de-energization of the power supply to the FI via Q1 are not considered in the calculation of the probability of failure of the safety function.
- The frequency inverter T1 is broken down into the blocks T1a and T1b. The block T1a contains the functions Start and Stop and their implementation in the control system. The block T1b contains the pulse blocking, which is achieved by a low number of components.

Safe stop triggered by the emergency stop device S4:

- A fault exclusion is assumed for the emergency stop device, since the number of actuations stated in Table D.2 is not exceeded.
- $MTTF_d$: the following MTTF_d values are estimated: 50 years for K4, 100 years for T1a and 1,000 years for T1b [E]. At a B_{10d} value of 400,000 cycles [S] and at 240 working days, 8 working hours and a cycle time of 6 minutes, the n_{op} is 19,200 cycles per year and the $MTTF_d$ 208 years for K1. At a B_{10d} value of 400,000 cycles [S] and daily actuation on 240 working days, the $MTTF_d$ for K2 is 16,667 years. The capacitor C1 is included in the calculation with an $MTTF_d$ of 45,662 years [D]. These values produce a symmetrized $MTTF_d$ for each channel of 72 years (“high”).
- DC_{avg}: fault detection by the process results in a *DC* of 30% for K4, a *DC* of 90% for T1a and a *DC* of 60% for T1b. A *DC* of 99% for K1 and a *DC* of 60% for C1 are derived by testing of the timing element with the FI de-energized. The *DC* for K2 is 99% owing to plausibility testing in K4 with the switching status of S4. The averaging formula for DC_{avg} yields 56.9 % (within the tolerance for “low”).
- Adequate measures against common cause failure (85 points): separation (15), diversity (20), overvoltage protection etc. (15) and environmental conditions (25 + 10)



- The combination of the control elements corresponds to Category 3 with a high $MTTF_d$ per channel (72 years) and a low DC_{avg} (56.9%). This results in an average probability of dangerous failure of 1.76 × 10^{-7} per hour. This corresponds to PL d.

Safe stop triggered by the ESPE K3:

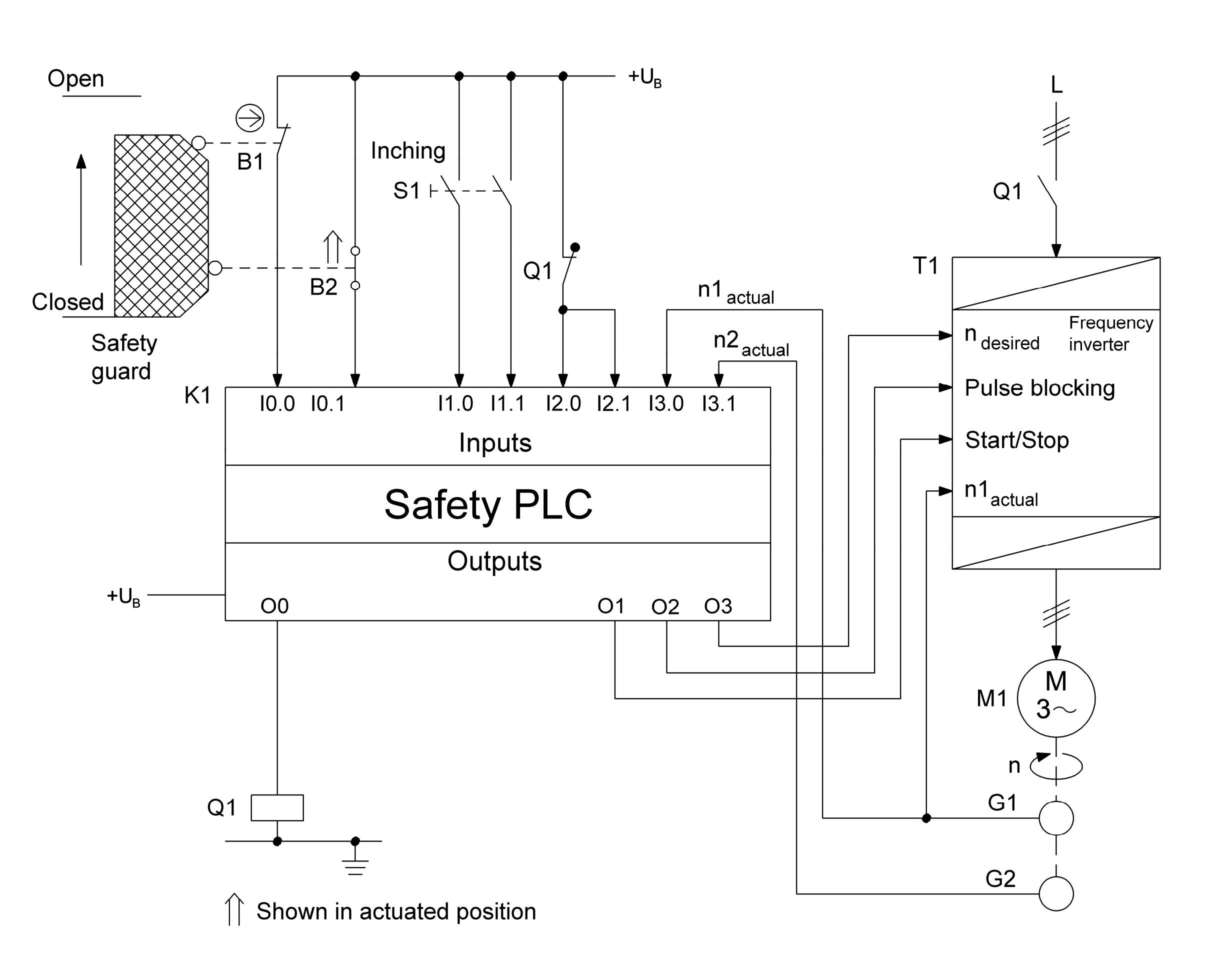
- The ESPE K3 is a standard safety component. Its probability of failure is 3.0 × 10^{-8} per hour [M], and is added at the end of the calculation.
- The probability of failure of the "PLC/electromechanical" two-channel structure is calculated using the same $\mathrm{MTTF_d}$ and DC values as those described above. The component K2 however is not involved in execution of this safety function. The results are: an $MTTF_d$ for one channel of 72 years ("high") and a DC_{avg} of 56.8% (within the tolerance for "low"). For Category 3, this results in an average probability of dangerous failure of 1.77 × 10^{-7} per hour. The overall probability of failure is determined by addition, producing a result of 2.07 × 10^{-7} per hour. This also corresponds to PL d.

More detailed references

- *Apfeld, R.; Zilligen, H.*: Sichere Antriebssteuerungen mit Frequenzumrichtern. BIA-Report 5/2003. Ed.: Hauptverband der gewerblichen Berufsgenossenschaften (HVBG), Sankt Augustin 2003. www.dguv.de/bgia, Webcode d6428
- EN 61496-1: Safety of machinery – Electro-sensitive protective equipment – Part 1: General requirements and tests (05.04)
- IEC 61496-2: Safety of machinery – Electro-sensitive protective equipment – Part 2: Particular requirements for equipment using active opto-electronic protective devices (AOPDs) (04.06)
- IEC 61800-5-2: Adjustable speed electrical power drive systems – Part 5-2: Safety requirements – Functional (07.07)

8.2.21 Safely limited speed for inching mode – Category 3 – PL d (Example 21)

Figure 8.37:
Inching mode with safely limited speed when the safety guard is open, with desired/actual value comparison and defined speed limit value within a safety PLC

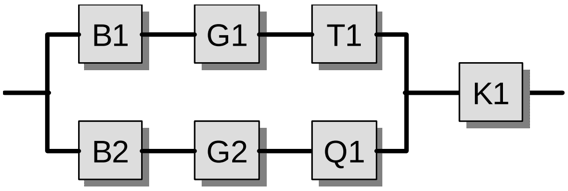


Safety function

- Safely limited speed (SLS): when the safety guard is open, exceeding of a permissible speed in inching mode is prevented.

Functional description

- A hazardous movement is safely prevented or interrupted when the safety guard is open. Opening of the safety guard is detected by two position switches B1 and B2 in a break contact/make contact combination. When the pushbutton S1 is actuated a safely limited speed is set on the frequency inverter T1 by means of the safety PLC K1. The two processing channels within the PLC each receive limit value settings independently of each other from their appli-

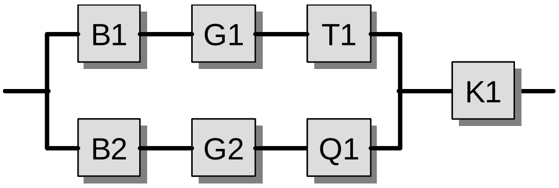


cation software. The actual rotational speed value of the inching speed on the inputs I3.0 and I3.1 of K1 is monitored by two separate tachogenerators G1 and G2. Each channel of the PLC performs the desired/actual speed comparison independently. Should the speed not be reduced successfully to the limited value by means of T1, K1 can initiate a halt by blocking of the start/stop signal and pulse blocking on the inverter. The power supply to T1 can also be interrupted by a mains contactor Q1.

- Safety-related data is exchanged through an internal interface in the safety PLC K1. Such data is employed for example for fault detection by a state comparison between the two processing channels. Should one processing channel fail, the remaining functioning processing channel reduces the speed of the inverter T1 and de-energizes the mains contactor Q1. A failure of the inverter which could for example lead to unexpected start-up, continued running or an increase in the speed is detected by separate monitoring of the speed by the tachogenerators G1 and G2 in both processing channels. Failure of the mains contactor Q1 to drop out is detected by the break contacts present in both processing channels (inputs I2.0 and I2.1 of K1), and leads both to blocking of the start/stop signal and to pulse blocking on the inverter by both processing channels.

Design features

- Basic and well-tried safety principles are observed and the requirements of Category B are met. Protective circuits (e.g. contact protection) as described in the initial paragraphs of Chapter 8 are implemented.
- A stable arrangement of the protective device is assured for actuation of the position switch.
- The position switch B1 features direct opening action in accordance with IEC 60947-5-1, Annex K. The position switch B2 also complies with IEC 60947-5-1.
- The contactor Q1 possesses a mirror contact according to IEC 60947-4-1, Annex F.
- The supply conductors to the position switches are laid either separately or with protection against mechanical damage.
- For the safety function “safely limited speed”, a fault exclusion is assumed for the fault condition of encoder shaft breakage (G1/G2). Details of the possibility of a fault exclusion can be found for example in IEC 61800-5-2, Table D.16.
- The standard components G1 and G2 (where relevant for the rotary signal encoders) and T1 are employed in accordance with the instructions in Section 6.3.10.



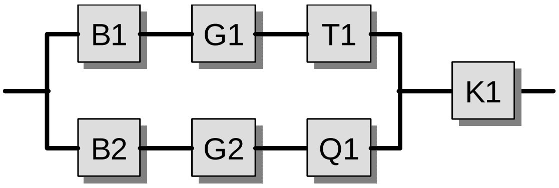
- The safety component K1 satisfies all requirements for Category 3 and PL d. The software (SRASW) is programmed in accordance with the requirements for PL d and the instructions in Section 6.3.
- It is assumed that each output of the safety PLC is actuated by both processing channels of the PLC (exception: O3).

Remarks

- According to EN 1010-1, the use of one position switch with direct opening action to IEC 60947-5-1, Annex K for each interlocked guard is sufficient on machines without routine operator intervention at danger points. Fault exclusion in this context is conditional upon the switch being installed in accordance with EN 60204-1.
- For full implementation of inching mode, the safety function “no unexpected start-up in inching mode” must also be considered.

Calculation of the probability of failure

- The SRP/CS is divided into the two subsystems sensor/actuator and PLC. For the PLC subsystem, a tested safety PLC suitable for PL d is employed. This PLC's probability of failure of 1.5×10^{-7} per hour [E] is added at the end of the calculation for the sensor/actuator subsystem. For production of the block diagram, refer also to Figure 6.14 and the corresponding comments in the associated text. The probability of failure for the sensor/actuator subsystem is calculated below.
- $MTTF_d$: at 240 working days, 8 working hours and a cycle time of one hour, n_{op} is 1,920 cycles per year. A B_{10d} value of 20,000,000 cycles [S] is assumed for the position switch B1 owing to its direct opening action; the associated $\mathrm{MTTF_d}$ value is 104,116 years. Owing to the defined control current (low load; the mechanical lifetime of the contacts is the determining factor), for the position switch B2 a B_{10d} value of 1,000,000 cycles [E] is assumed (see also Table D.2), and therefore an $MTTF_d$ of 5,208 years. The contactor Q1 with a B_{10d} value of 400,000 cycles switches operationally only once daily, corresponding to a n_{op} of 240 cycles per year and an $MTTF_d$ of 16,667 years. The following values are estimated: an $MTTF_d$ of 100 years for T1 and an $MTTF_d$ of 50 years for G1/G2 [E]. These values produce a symmetrized $MTTF_d$ for each channel of 41 years (“high”).
- DC_{avg}: for each of the components used, a DC of 99% is assumed. For the position switches and the tachogenerators, this value is based upon cross-checking of input signals in K1. For the inverter T1, fault detection is provided by the



process; the mains contactor Q1 is monitored directly by the PLC. These values produce a DC_{avg} of 99% (“high”).

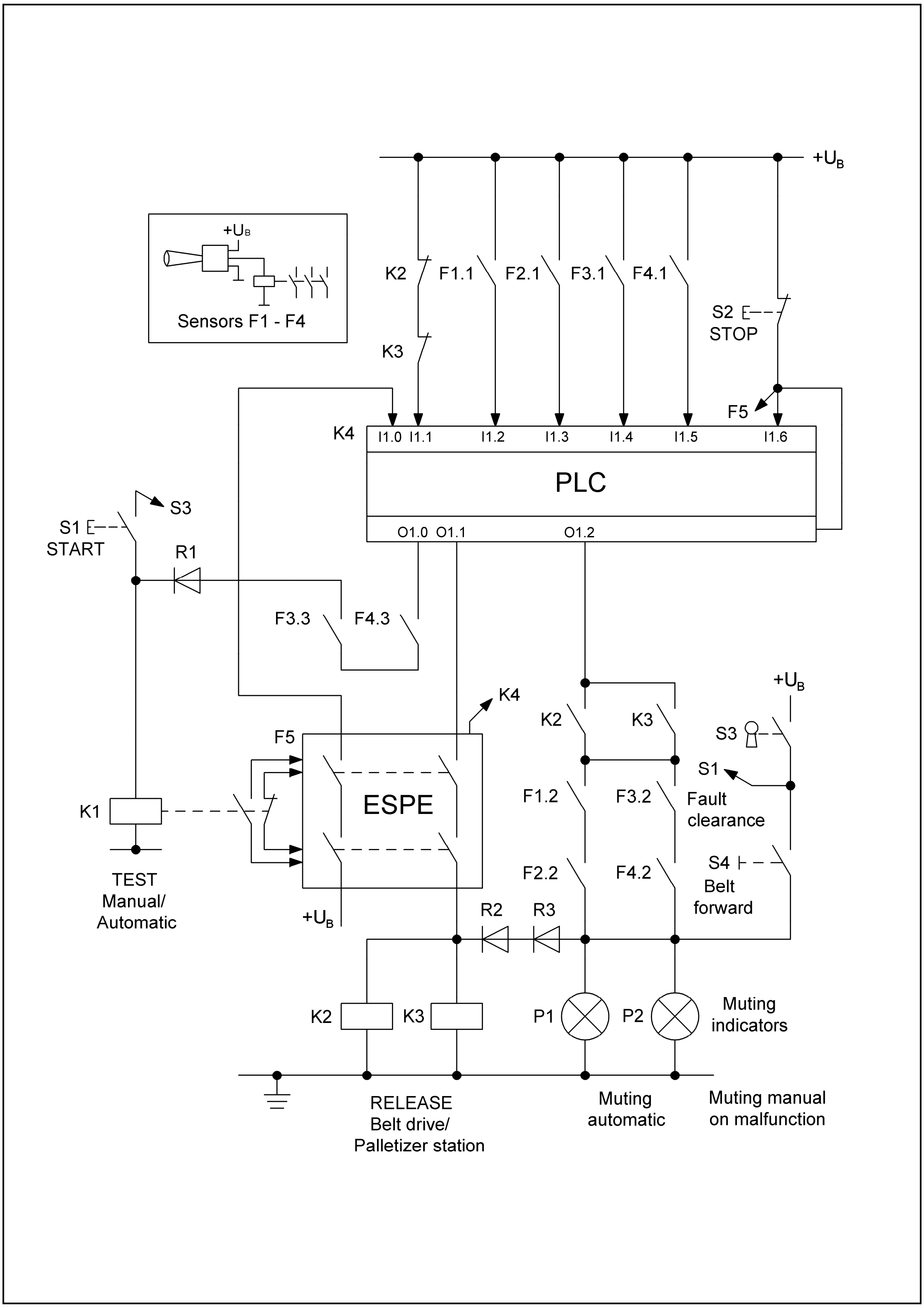
- Adequate measures against common cause failure (70 points): separation (15), FMEA (5), overvoltage protection etc. (15) and environmental conditions (25 + 10)
- The sensor/actuator subsystem corresponds to Category 3 with a high $MTTF_d$ per channel (41 years) and high DC_{avg} (99%). This results in an average probability of dangerous failure of 6.56×10^{-8} per hour. This corresponds to PL e. PL_r d is thus surpassed, which with the required two-channel design of the hardware with few components, the use of B_{10d} values in accordance with the standard, a *DC* of “high” and a “moderate” switching frequency will virtually always be the case.
- The overall probability of failure is determined by addition of the probability of dangerous failure of K1 (1.5×10^{-7} per hour) and is 2.16×10^{-7} per hour. This corresponds to PL d.

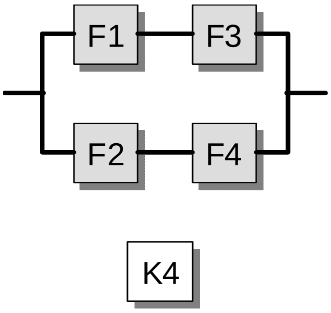
More detailed references

- *Grigulewitsch, W.; Reinert, D.*: Schaltungsbeispiele mit programmierbaren Steuerungen zur Umsetzung der Steuerungskategorie 3. In: BGIA-Handbuch Sicherheit und Gesundheitsschutz am Arbeitsplatz. Kennzahl 330 227. 27th suppl. I/95. Ed.: BGIA – Institut für Arbeitsschutz der Deutschen Gesetzlichen Unfallversicherung, Sankt Augustin. Erich Schmidt, Berlin 1985 – looseleaf ed. www.bgia-handbuchdigital.de/330227
- IEC 61800-5-2: Adjustable speed electrical power drive systems – Part 5-2: Safety requirements – Functional (07.07)
- EN 1010-1: Safety of machinery – Safety requirements for the design and construction of printing and paper converting machines – Part 1: Common requirements (12.04)

8.2.22 Muting of a protective device – Category 3 – PL d (Example 22)

Figure 8.38:
Muting of a protective device at the discharge point from a palletizing installation controlled by a PLC





Safety function

- Muting function: temporary muting of a protective device as a function of the process. Further safety functions, such as safeguarding of access to the palletizing installation or the start/restart interlock, are not dealt with in detail below.

Functional description

- Access to the discharge point from the palletizing installation is safeguarded by a triple-beam light barrier (ESPE) F5 of Type 4 to EN 61496. The light barrier embodies the additional functions of start interlock and restart interlock which are implemented by means of two antivalent inputs. Disabling of the start interlock of the light barrier is coupled to the start command for the belt drive, i.e. energization of the palletizing station, and is initiated by picking-up and subsequent dropping-out of contactor relay K1 in response to actuation and release of the start button S1. A condition for a valid start command is that contactor relays K2 and K3 have dropped out (queried via input I1.1) and that the start interlock has been cancelled (queried via input I1.0). Output O1.1 is set as a result.
- Four infrared light sensors F1 to F4 (for arrangement, refer also to Figure 8.38) are incorporated for control of the muting process. On inputs I1.2 to I1.5, the PLC monitors the actuation sequence of the four infrared light sensors via the sensors' contacts F1.1 to F4.1, in consideration of two programmed time settings. The muting function is implemented only in the output circuit of the PLC (output O1.2) independently of the output circuit of the light barrier F5. The muting contacts F1.2 and F2.2/F3.2 and F4.2, connected in series, are connected, via the diodes R2 and R3 respectively, by OR logic with the “enabling” function implemented by the contactor relays K2 and K3.
- R2 and R3 cause the muting function to be displayed correctly, and isolate the activated enabling output from the muting displays P1/P2 should the muting function not be active. Faults in R2 or R3 cannot lead to undesired muting (i.e. dangerous failure of the muting function).
- In the event of breakdown and subsequent restoration of the voltage, or with light barrier F5 interrupted and the muting function not active, the contactor relays K2 and K3 are de-energized. The absence under these conditions of latching-in prevents them from picking up again should the muting circuits be closed again. The installation can be restarted only by disabling of the restart interlock, i.e. by deliberate actuation and release of the start button S1.

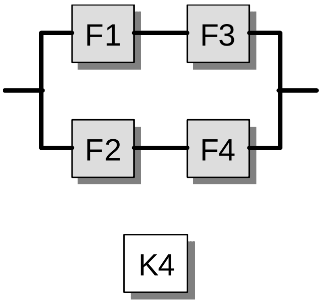
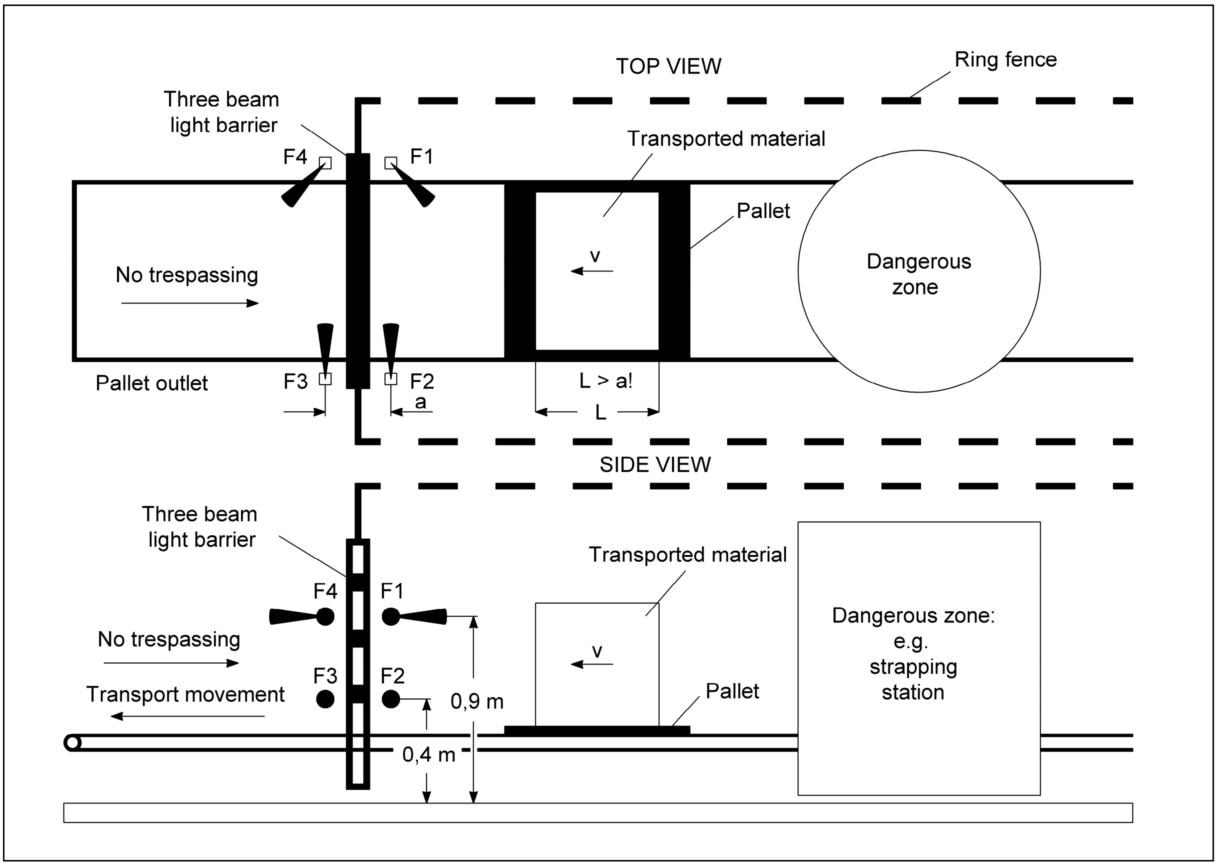
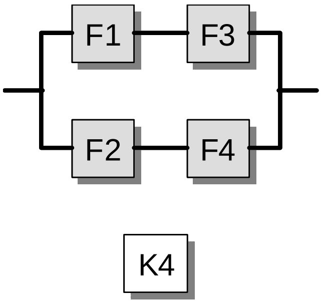


Figure 8.39:
Palletizing station with automatic control – principle of safeguarding of the pallet discharge point by means of a light barrier and arrangement of the muting sensors F1 to F4



- For intended starting/restarting, for example following a fault on the installation, the key switch S3 must be actuated. In the event of a fault condition, the operator can eject a pallet from the detection area of the light barrier and the muting sensors by means of the dead-man's button S4.

  For smooth progress of the pallets through the discharge opening, two time settings in the PLC program must be matched to the velocity of the transport movement:



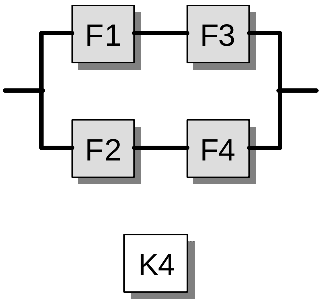
- The time setting T1 determines the maximum period within which – following activation of the sensor F1 – the sensor F2 must be activated and the muting function thus initiated by the transported product.

- Time setting T2 begins with renewed clearing of sensor F2. T2 must be selected such that when the detection zone of the light barriers becomes clear again, K1 is energized and de-energized again before sensor F3 is deactivated by the transported product and the muting function thereby terminated.

- Failure of the contactors K2 and K3 to drop out is detected at the latest before the belt drive/the palletizing installation start up again, owing to the feedback of the mechanically linked break contacts to the PLC input I1.1. Failure of K1 is detected at the next discharge of a pallet.
- Unintended start-up of the belt drive/palletizing installation in the event of the loss and subsequent restoration of power or a failure of the standard PLC is prevented by the function of the start-up and restart interlocks. The PLC can disable the restart interlock only immediately after the pallet has passed the light barrier, i.e. whilst sensors F3 and F4 are still activated.
- The failure of individual muting sensors is either detected directly by the PLC program (owing to monitoring for proper completion of activation and deactivation), or becomes evident by operating inhibition during transport of the pallet.
- Failure of the dead-man's button S4, which is used only for the clearing of faults (manual muting), is detected directly by the user.

Design features

- Basic and well-tried safety principles are observed and the requirements of Category B are met. Protective circuits (e.g. contact protection) as described in the initial paragraphs of Chapter 8 are implemented.
- Contactor relays K1 to K3 possess mechanically linked contact elements in accordance with IEC 60947-5-1, Annex L.
- The supply conductors to light barrier F5 and to the dead man's button S4 are laid such that short-circuits between individual conductors (including to the supply voltage) can be excluded.
- The control components S1 to S4 are located at a point outside the hazardous area and with a view of it.



- The muting state is displayed by two lights clearly visible to the operator at the access point to the hazardous area.
- The standard components F1 to F4 are employed, where applicable, in accordance with the instructions in Section 6.3.10.

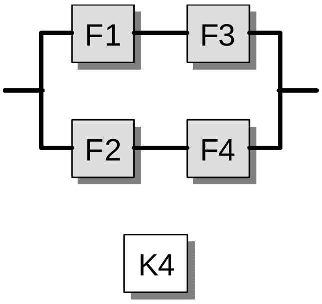
Remarks

- Example implementation of automated material discharge with safeguarding of access points to palletization and depalletization processes, transfer stations, strapping or wrapping machines. The same principle can be used for access points for material infeed.
- In accordance with EN 415-4, it can be assumed that the undetected access of persons through feed or discharge openings is prevented sufficiently reliably when requirements including the following are met:
  - use of a two or three-beam light barrier in consideration of the necessary fitting height (with the access point open or an empty pallet present in it), or
  - with the protective function of the light barrier muted by the loaded pallet with clearances to the side of less than 0.2 m and with muting being activated by the pallet load only immediately prior to interruption of the light beams (without greater timing intervals and geometrical gaps).

Calculation of the probability of failure

In the calculation below, a *DC* of 0% is assumed for the output relays of the muting sensors F1 to F4, since the contacts employed for muting are not subject to automatic fault detection. For this reason, periodic manual inspection which can be achieved by simple means is specified.

- $MTTF_d$: an $MTTF_d$ of 100 years [E] is assumed for the sensor part of each of the muting sensors F1 to F4. A B_{10d} value of 2,000,000 cycles [S] applies for the output relays F1 to F4. At 300 working days, 16 working hours and a cycle time of 200 seconds, n_{op} is 86,400 cycles per year and the $MTTF_d$ is 231 years for these elements. The $MTTF_d$ of the channel is 35 years (“high”).
- DC_{avg}: a *DC* of 90% for the sensor part of the muting sensors F1 to F4 is attained by the PLC monitoring. The *DC* for the output relays is estimated erring on the safe side at 0%. The resulting DC_{avg} value is 63% (“low”).
- Adequate measures against common cause failure (65 points): separation (15), overvoltage protection etc. (15) and environmental conditions (25 + 10)



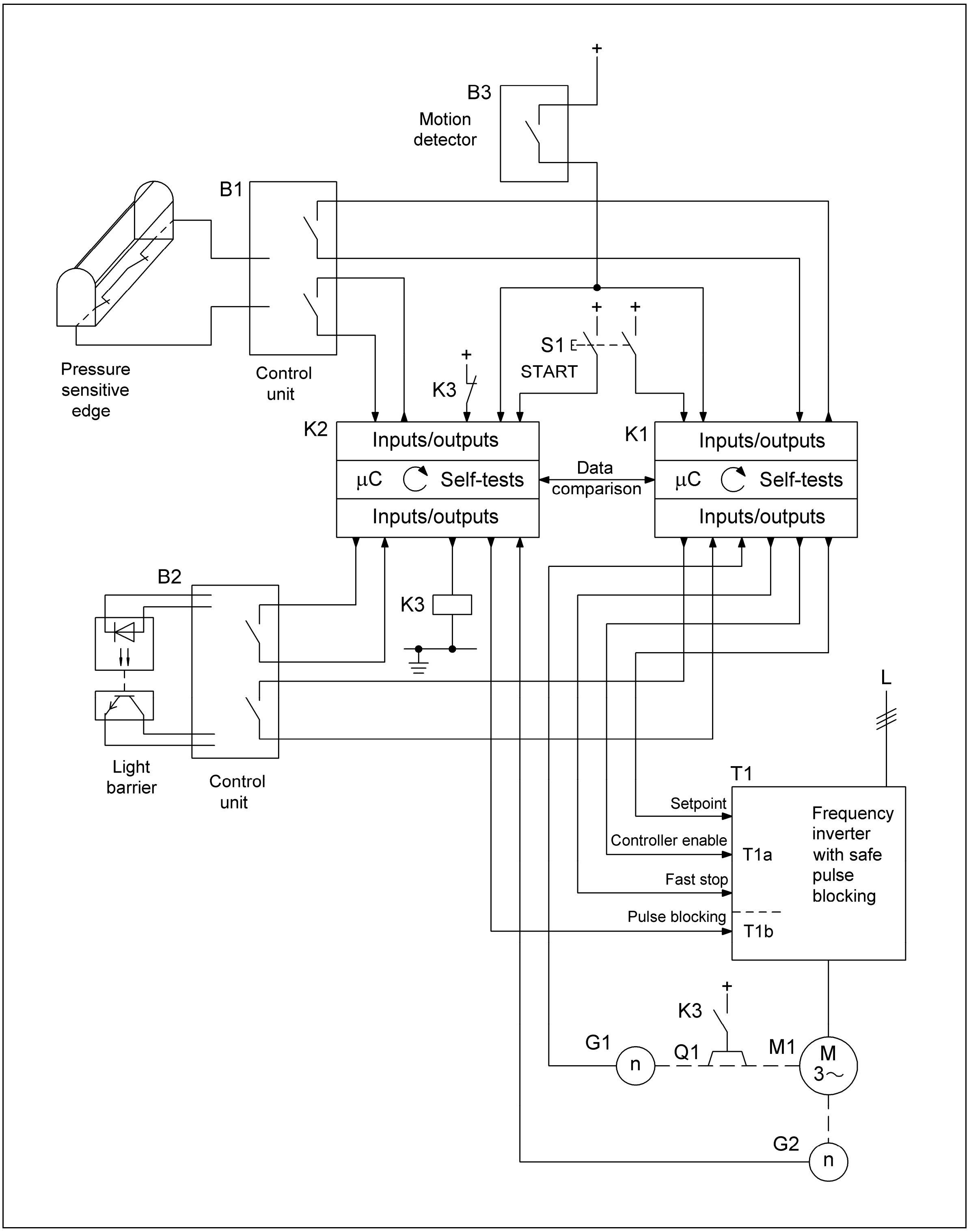
- The combination of the control elements corresponds to Category 3 with a high $MTTF_d$ per channel (35 years) and low DC_{avg} (63%). This results in an average probability of dangerous failure of 5.16×10^{-7} per hour. This corresponds to PL d.

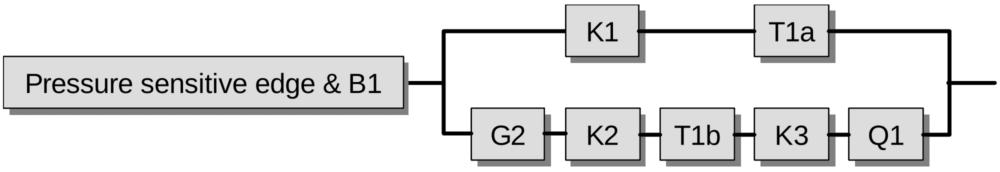
More detailed references

- *Grigulewitsch, W.*: Speicherprogrammierbare Steuerung (SPS) zum zeitlich begrenzten, prozessabhängigen Aufheben einer Sicherheitsfunktion – Schaltungsbeispiel. In: BGIA-Handbuch Sicherheit und Gesundheitsschutz am Arbeitsplatz. Kennzahl 330 231. 36th suppl. XII/99. Ed.: BGIA – Institut für Arbeitsschutz der Deutschen Gesetzlichen Unfallversicherung, Sankt Augustin. Erich Schmidt, Berlin 1985 – loose-leaf ed. www.bgia-handbuchdigital.de/330231
- *Kreutzkampf, F.; Hertel, W.*: Zeitbegrenztes Aufheben von Sicherheitsfunktionen. In: BGIA-Handbuch Sicherheit und Gesundheitsschutz am Arbeitsplatz. Kennzahl 330 214. 19th suppl. X/92. Ed.: BGIA – Institut für Arbeitsschutz der Deutschen Gesetzlichen Unfallversicherung, Sankt Augustin. Erich Schmidt, Berlin 1985 – loose-leaf ed. www.bgia-handbuchdigital.de/330214
- EN 415-4: Safety of packaging machines – Part 4: Palletisers and depalletisers (03.97) and amendment AC (12.02)
- EN 61496-1: Safety of machinery – Electro-sensitive protective equipment – Part 1: General requirements and tests (05.04)
- IEC 61496-2: Safety of machinery – Electro-sensitive protective equipment – Part 2: Particular requirements for equipment using active opto-electronic protective devices (AOPDs) (04.06)
- IEC 62046: Safety of machinery – Application of protective equipment to detect the presence of persons (draft standard IEC 44/501/CD:2005)
- EN 999: Safety of machinery – The positioning of protective equipment in respect of approach speeds of parts of the human body (10.98)

8.2.23 Revolving door control – Category 3 – PL d (Example 23)

Figure 8.40:
Revolving door control employing microcontrollers





Safety functions

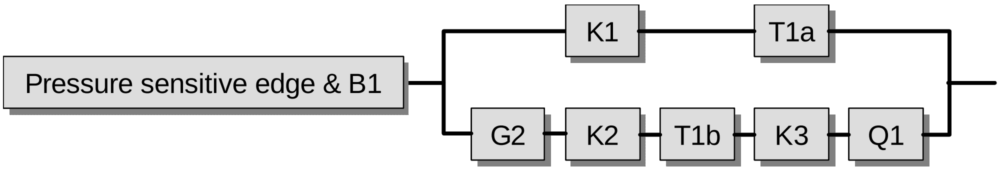
- Safety-related stop function: when the pressure sensitive edge is actuated, the revolving movement of the door is halted (SS1 – safe stop 1).
- Safely limited speed (SLS): when a person or object is detected by the light barrier, the speed of the revolving door is reduced and safely limited.

Functional description

- The revolving movement of the door is initiated only once the control system has been switched on by the pushbutton S1. In normal operation, the command for the revolving movement is issued by the motion detector B3 located on the door. The frequency inverter T1 is actuated jointly by the two microcontrollers K1 and K2. Each microcontroller (µC) contains a central processing unit (CPU) in the form of a microprocessor, and working memory (RAM) and read-only memory (ROM). K1 controls the functions of setpoint assignment, enabling of the controller, and fast stop. K2 actuates pulse blocking, and the holding brake Q1 can be released by means of the contactor relay K3. The rotary signal encoders G1 and G2 transmit the motor speed to K1 and K2 respectively.
- Faults in the pressure sensitive edge or light barrier are detected in the associated control units B1 and B2. The same applies to faults in B1 and B2 themselves, which are detected by internal monitoring. Faults in the components of the microcontrollers are detected by the performance of self-tests and by data comparison. Proper operation of the frequency inverter T1 is monitored by means of the rotary signal encoders G1 and G2 in K1 and K2 respectively. When detected, faults are controlled via K1 and/or K2, leading to the door's movement being halted by T1 and/or Q1. The wings of the door can be opened manually in order for trapped persons to be freed.
- Owing to redundant processing channels, a single fault does not result in loss of the safety function. The combination of undetected faults may lead to loss of the safety function.

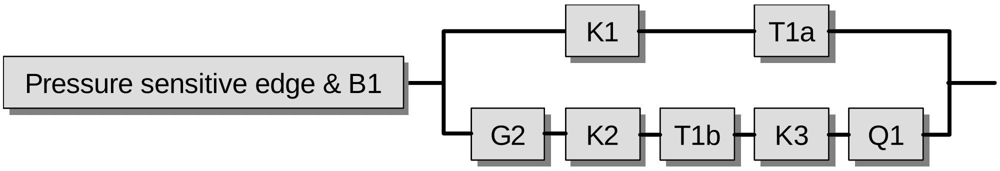
Design features

- Basic and well-tried safety principles are observed and the requirements of Category B are met. Protective circuits (e.g. contact protection) as described in the initial paragraphs of Chapter 8 are implemented.
- The pressure sensitive edge safeguards against crush, shear and entrapment points. It is connected to the control system via B1. The subsystem, comprising sensor and control unit, satisfies the requirements of EN 1760-2 in Category 3 and of EN ISO 13849-1 for PL d. Faults in the sensor of the pressure sensitive



edge or in the supply conductors must be excluded or be detected via the control unit (pressure sensitive edges operating on either the break-contact or make-contact principle may be employed). When a pressure sensitive edge is reset following actuation, the rotary movement begins again with a time delay. The pressure sensitive edge possesses an adequate deformation path and an adequate range of action.

- The light barrier has the function of leading, non-contact safeguarding of hazardous zones. Together with B2, it satisfies at least the requirements for Type 2 to EN 61496-1 and IEC 61496-2, and to EN ISO 13849-1 for PL d. The revolving speed, which is safely reduced following detection of a person or an object by the light barrier, is increased again to the normal speed following a present timeout. The supply conductors to the transmitter and receiver are laid separately or with protection.
- During the first start-up of the door's revolving movement, start-up tests are performed. The tests include, for example, tests of the microcontroller blocks (microprocessor, random-access and read-only memory), input and output tests, and checking of driving of the motor by the frequency inverter (including testing of controller enabling, the fast-stop functionality and pulse blocking). A brake test is also performed, in which the frequency inverter is required to act against the operating holding brake.
- During comparison of data between the two controllers, desired values and intermediate results are exchanged, with inclusion of the cyclical self-tests.
- Since the frequency inverter employs safe pulse blocking, a contactor is no longer required for de-energization of the supply voltage. The frequency inverter is suitable for driving and braking.
- K3 possesses mechanically linked contact elements to IEC 60947-5-1, Annex L. The switching position of the break contact is monitored by the microcontroller K2 for the purpose of fault detection.
- It is assumed in the example that closed-loop control provided by the frequency inverter T1 is sufficient for braking of the revolving door. Once the drive has come to a halt, pulse blocking is activated and controller enabling cancelled in order to prevent unexpected start-up. The braking time and braking distance are monitored by the controller. The brake Q1 is required in the event of a fault so that, should T1 for example no longer be able to execute the specified function, no danger may arise owing to an undesired movement. Q1 operates on the closed-circuit current principle.
- The software (SRESW) in K1 and K2 is programmed in accordance with the requirements for PL d as per Section 6.3.



- The standard components G1 and G2 (where relevant for the rotary signal encoders) and T1 are employed in accordance with the instructions in Section 6.3.10.
- For the safety function “safely limited speed”, a fault exclusion is assumed for the fault condition of encoder shaft breakage (G1/G2). For details of the possibility of a fault exclusion, refer for example to IEC 61800-5-2, Table D.16.

Remarks

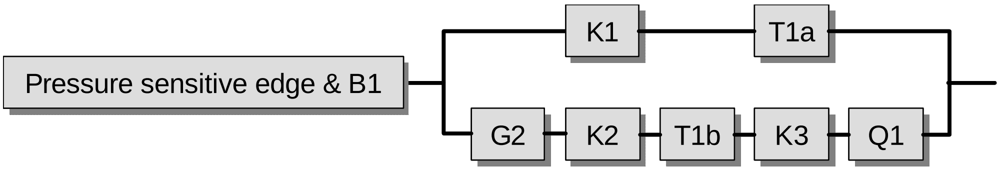
- The circuit example can be employed for implementation of the safety functions “safety-related stop function” and “safely limited speed” in a control system for three-wing and four-wing revolving doors with break-out function (the wings can be folded manually in an emergency) for use in public and commercial buildings.
- Regular manual inspection of the pressure sensitive edge is required. Firstly, the functionality must be checked; secondly, the pressure sensitive edge must be inspected visually in order for any damage to be detected in good time.

Calculation of the probability of failure

- For calculation of the probability of failure, the frequency inverter T1 is broken down into the blocks T1a and T1b. The block T1a contains the functions set-point assignment, enabling of the controller and fast stop, and their implementation in the control system. The block T1b contains the safe pulse blocking function, which is achieved by a small number of components.

The detailed calculation of the probability of failure is performed for the “safety-related stop function (SS1)”, which is also shown in the block diagram:

- Since the pressure sensitive edge with the associated control unit B1 is available commercially as a safety component, its probability of failure is added at the end of the calculation (3.00×10^{-7} per hour [E]).
- $MTTF_d$: the safety-related components of K1 and K2 and their peripherals are considered, following application of the parts count method, by a value of 878 years [E]. A value of 75 years [E] is substituted in the formula for G2. Values of 100 years [E] for T1a and of 1,000 years [E] for T1b are substituted in the formula. A B_{10d} value of 400,000 cycles [S] is substituted for K3. At one operation per day, n_{op} is 365 cycles per year, and the $MTTF_d$ is 10,959 years. Q1 is considered with an $MTTF_d$ of 50 years [E]. The holding brake Q1 is required only in the event of a fault, and is not subject to operational wear. Overall, the symmetrized $\mathrm{MTTF_d}$ value per channel is 64.3 years (“high”).



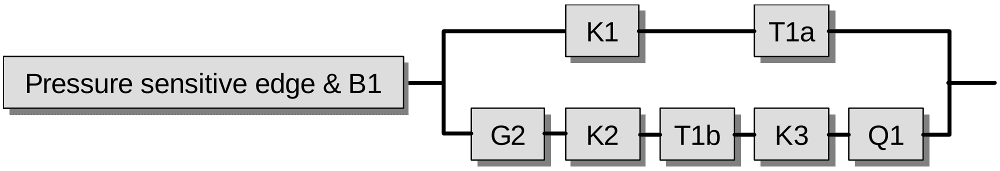
- *DC*$_{avg}$: owing to the selection of suitable test measures, the *DC* value for K1 and K2 is 60%. Internal self-tests are performed on the microcontroller components. A *DC* of 90% is substituted for the block T1a, since fault detection occurs via the process. G2 is rated with a *DC* of 90%; here too, fault detection is provided by the process and by the comparison with G1 via K1 and K2. K3 is rated with a *DC* of 99% owing to direct monitoring of readback of a mechanically linked contact. Owing to performance of the static start-up test, a *DC* of 60% is substituted for T1b and a *DC* of 30% for Q1. Averaging thus produces a *DC*$_{avg}$ of 62% ("low").
- Adequate measures against common cause failure (70 points): separation (15), FMEA (5), overvoltage protection etc. (15) and environmental conditions (25 + 10)
- The combination of the control elements corresponds to Category 3 with a high *MTTF*$_d$ (64.3 years) and low *DC*$_{avg}$ (62%). For the combination of the components K1 and T1a in the first channel and G2, K2, T1b, K3 and Q1 in the second channel, the average probability of dangerous failure is 1.94 × 10^{-7} per hour. Together with the sensor unit consisting of pressure sensitive edge and control unit B1, the overall average probability of dangerous failure of the control for this safety function is 4.94 × 10^{-7} per hour. This corresponds to PL d.

Calculation of the probability of failure for the safety function "safely limited speed (SLS)":

- G1 must also be considered in the first channel for this calculation. An *MTTF*$_d$ of 75 years [E] is substituted for this purpose. The *DC* of 99% is derived from fault detection via the process and the comparison with G2 via K2 and K1. Adequate measures against common cause failure were selected in the same way as for the first example analysis. With an *MTTF*$_d$ of 34.9 years and a *DC*$_{avg}$ of 70%, the average probability of dangerous failure is 4.46 × 10^{-7} per hour. Following addition of the sensor unit, in this case consisting of the light barrier and control unit B2 with a value of 2.00 × 10^{-7} per hour [E], the overall average probability of dangerous failure of the control system for this safety function is 6.46 × 10^{-7} per hour. This also corresponds to PL d.

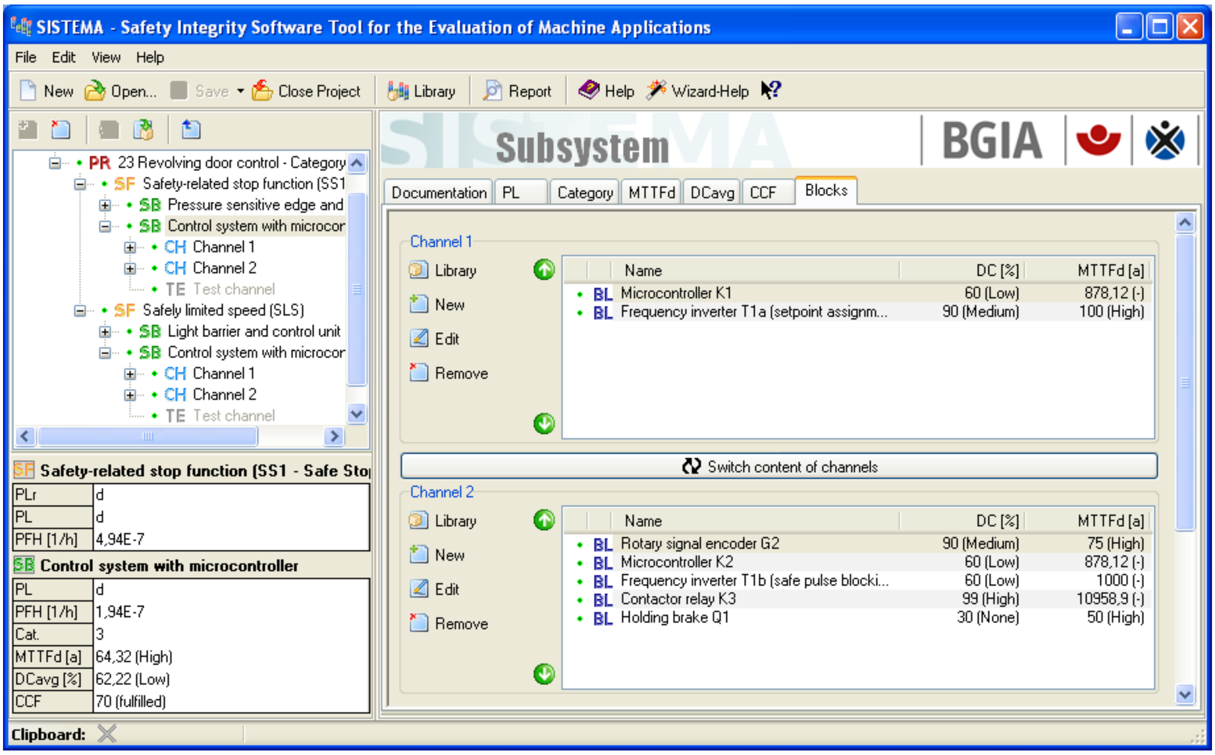
More detailed references

- EN 1760-2: Safety of machinery – Pressure sensitive protective devices – Part 2: General principles for the design and testing of pressure sensitive edges and pressure sensitive bars (03.01)
- DIN 18650-1: Schlösser und Baubeschläge – Automatische Türsysteme (12.05). Beuth, Berlin 2005



- IEC 60947-5-1: Low-voltage switchgear and controlgear – Part 5-1: Control circuit devices and switching elements – Electromechanical control circuit devices (11.03)
- EN 61496-1: Safety of machinery – Electro-sensitive protective equipment – Part 1: General requirements and tests (05.04)
- IEC 61496-2: Safety of machinery – Electro-sensitive protective equipment – Part 2: Particular requirements for equipment using active opto-electronic protective devices (AOPDs) (04.06)
- IEC 61800-5-2: Adjustable speed electrical power drive systems – Part 5-2: Safety requirements – Functional (07.07)

Figure 8.41:
Determining of the PL by means of SISTEMA


SISTEMA - Safety Integrity Software Tool for the Evaluation of Machine Applications
File Edit View Help
New Open... Save Close Project Library Report Help Wizard-Help
Subsystem
BGIA
Documentation PL Category MTTFd DCavg CCF Blocks
Library
New
Edit
Remove
Switch content of channels
Clipboard:

PR 23 Revolving door control - Category
- SF Safety-related stop function (SS1
  - SB Pressure sensitive edge and
  - SB Control system with microcor
    - CH Channel 1
    - CH Channel 2
    - TE Test channel
- SF Safely limited speed (SLS)
  - SB Light barrier and control unit
  - SB Control system with microcor
    - CH Channel 1
    - CH Channel 2
    - TE Test channel

SF Safety-related stop function (SS1 - Safe Sto

PLr	d
PL	d
PFH [1/h]	4,94E-7

SB Control system with microcontroller

PL	d
PFH [1/h]	1,94E-7
Cat.	3
MTTFd [a]	64,32 (High)
DCavg [%]	62,22 (Low)
CCF	70 (fulfilled)

Channel 1

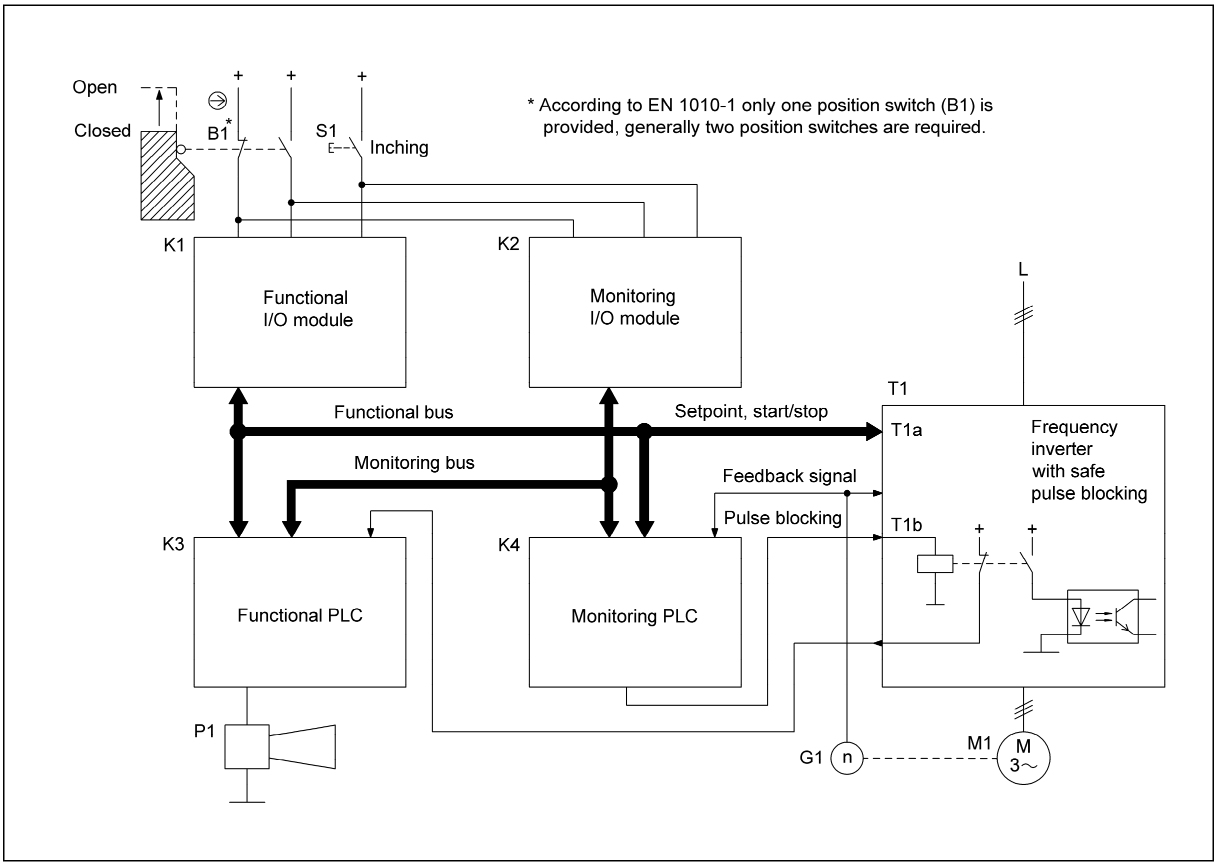
	Name	DC [%]	MTTFd [a]
BL	Microcontroller K1	60 (Low)	878,12 (-)
BL	Frequency inverter T1a (setpoint assignm...	90 (Medium)	100 (High)

Channel 2

	Name	DC [%]	MTTFd [a]
BL	Rotary signal encoder G2	90 (Medium)	75 (High)
BL	Microcontroller K2	60 (Low)	878,12 (-)
BL	Frequency inverter T1b (safe pulse blocki...	60 (Low)	1000 (-)
BL	Contactor relay K3	99 (High)	10958,9 (-)
BL	Holding brake Q1	30 (None)	50 (High)

8.2.24 Inching mode with safely limited speed on a printing machine – Category 3 – PL d (Example 24)

Figure 8.42:
Inching mode with safely limited speed on a printing machine with two-channel microprocessor control

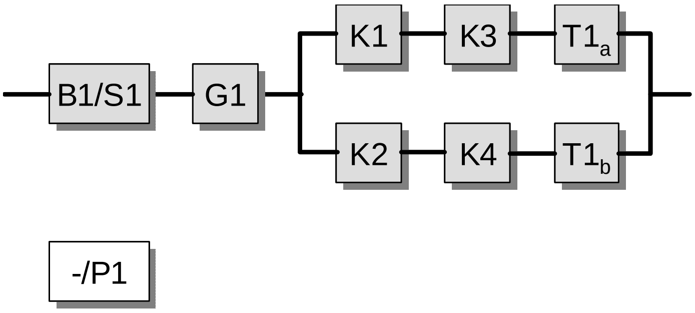


Safety functions

- Safety-related stop function, initiated by a protective device: the drive is to stop when the safety guard is opened (SS1 – safe stop 1).
- Safely limited speed (SLS): when the safety guard is open, machine movements may occur only at limited speed.
- Inching mode: when the safety guard is open, movements are possible only whilst an inching button is pressed.

Functional description

- The remote I/O module K1 registers the states of the position switch with personnel safety function B1 and of the inching button S1, and makes this information available on the functional bus. The information is evaluated by the functional PLC K3 and results in the frequency inverter T1 being actuated (functional actuation T1a) via the functional bus. The I/O module K2 and the monitoring PLC K4, which communicate over a dedicated monitoring bus,

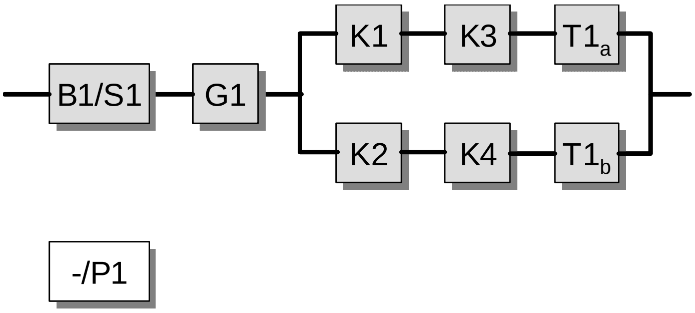


operate redundantly to K1 and K3. K4 can bring about an uncontrolled stopping (coasting down) by addressing the safe pulse blocking of T1 (safety shutdown T1b).

- With B1 open, only inching mode using S1 with safely limited speed is permitted.
- In accordance with EN 1010-1, a single position switch B1 is sufficient. The majority of faults in S1 are detected and controlled by an acoustic start-up warning involving P1 and forced dynamics: when S1 is pressed for the first time, an acoustic warning (P1) is output; only when S1 is released and pressed again does the drive start up again, with delay.
- Faults in K1 and K2 are detected by a status comparison in K4. K4 also monitors K3 by monitoring the input and output information. In addition, the faults in K3 are partly revealed by faults in the process. Self-tests (e.g. program sequence monitoring by an internal watchdog) are performed in K4; in addition, K3 uses K4 for regular addressing of the pulse blocking and monitors feedback from the latter via the mechanically linked break contact of the pulse blocking relay of T1.
- Together with the sin/cos encoder G1, the frequency inverter T1 forms a closed-loop control system in which faults (printing errors, paper tearing) are detected by the production process, which is highly synchronous. For monitoring or the safely limited speed, G1 is also read back into K4 and monitored for plausibility of the sin/cos information ($\sin^2 + \cos^2 = 1$) and for compliance with the setpoint for T1.

Design features

- Basic and well-tried safety principles are observed and the requirements of Category B are met. Protective circuits (e.g. contact protection) as described in the initial paragraphs of Chapter 8 are implemented.
- The break contact of B1 satisfies IEC 60947-5-1, Annex K. Measures are implemented for prevention of displacement and reasonably foreseeable misuse (see EN 1088 with Annex A1). A stable arrangement of the protective device is assured for actuation of the position switch.
- Despite the warning at start-up and forced dynamics, S1 may hang during inching operation. An additional requirement is therefore that an emergency stop device be installed within the operator's reach.



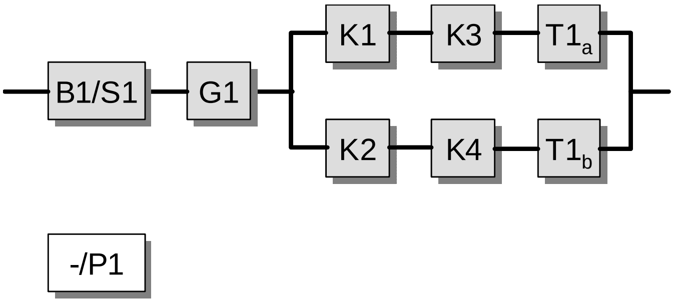
- The conditions for fault exclusion for conductor short-circuits to EN ISO 13849-2, Table D.4 must be observed for the connecting lines to S1. Faults in the connecting lines to B1 are detected by non-equivalence monitoring of the break and make contact in K1 and K2.
- The programmable components K1 to K4 satisfy the normative requirements in accordance with Section 6.3.
- G1 supplies redundant position information (e.g. sin/cos encoder) and is integrated into the closed-loop control circuit (acquisition of the commutation).
- T1 possesses safe pulse blocking (T1b), successful addressing of which is read back by a mechanically linked break contact.
- The standard components G1 and T1 are employed in accordance with the instructions in Section 6.3.10.
- The bus systems (functional bus, monitoring bus) are employed in accordance with the instructions in Section 6.2.17.

Remarks

- Application for example for the safeguarding of entrapment points on rotary printing machines. For non-cyclical operator intervention in the hazardous area, i.e. less frequently than one intervention per hour, EN 1010-1 requires only one position switch for monitoring of the guard position. The fault-tolerance criterion for Category 3 generally requires the use of two position switches (e.g. one break contact, one make contact) for similar machine control systems.
- For inching mode subject to the condition that safely limited speed is already guaranteed, the possibility of avoiding the hazard can be assumed under certain conditions.

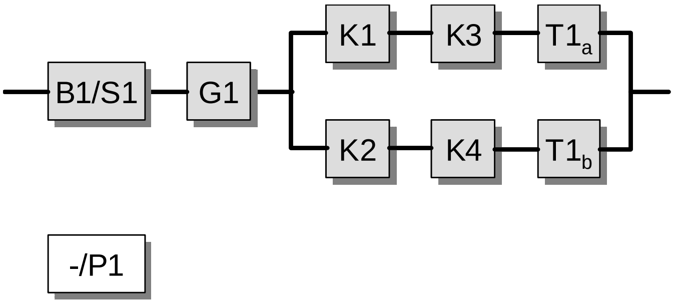
Calculation of the probability of failure

- The sensor level B1, S1 and G1 lies outside the redundant logic and actuator level and is therefore considered separately.
- Fault exclusion for the direct opening electrical contact is possible for B1. A B_{10d} value of 20,000,000 cycles [S] is assumed for the mechanical part of B1. At 10 operations per week, n_{op} is 520 cycles per year and the $MTTF_d$ is 384,615 years. This corresponds mathematically to an average probability of dangerous failure of 2.97 × 10^{-10} per hour. In order for consideration to be given



to the particular aspects of EN 1010-1, this value is downgraded to the upper marker value of 1.00 × 10^{-7} per hour for PL d, instead of the $MTTF_d$ for one channel being capped to 100 years as usual.

- S1 has a B_{10d} value of 100,000 cycles [M]. At 10 operations per week, n_{op} is 520 cycles per year and the $MTTF_d$ is 1,923 years. Owing to forced dynamics and the start-up warning, a *DC* of at least 60% is assumed (hanging following repeated inching is not detected, however). By incorporation into a Category 2 structure, S1 thus attains an average probability of dangerous failure of 5.28 × 10^{-7} per hour.
- Owing to evaluation of the sin/cos signals and its use in the closed-loop control circuit (for commutation), G1 is integrated in accordance with Category 3. At an $MTTF_d$ per channel of 30 years [E] and a *DC* of 90% owing to plausibility testing and fault detection in the process, the average probability of dangerous failure is 2.65 × 10^{-7} per hour.
- $MTTF_d$: 100 years [E] is allowed for K1 and K2, 50 years [E] for K4, and 30 years [E] for K3. In addition, 30 years [E] is substituted for T1a and 1,000 years [E] for T1b. Overall, this produces a symmetrized MTTF_d value per channel of 24 years (“medium”).
- DC_{avg}: the *DC* of 99% for K1 and K2 is produced by direct comparison of the supplied status information in K4. The *DC* of 99% for K3 is based upon parallel processing of all safety-related information in K4 and upon the direct comparison in K4 with the intermediate results and output signals formed by K3. The self-tests implemented in K4 together with partial monitoring by the reading back of pulse blocking by K3 result in a *DC* of 60% for K4. The *DC* of 99% for T1a is based upon comparison in K4 between the setpoint and actual value of the shaft position. For T1b, assumption of a fault exclusion for the internal optocoupler owing to readback of addressing of pulse blocking results in a *DC* of 60%. Averaging then produces a DC_{avg} of 91% (“medium”).
- Adequate measures against common cause failure (70 points): separation (15), FMEA (5), overvoltage protection etc. (15) and environmental conditions (25 + 10)
- The combination of K1 to K4 and T1 corresponds to Category 3 with a medium $MTTF_d$ per channel (24 years) and a medium DC_{avg} (91%). This results in an average probability of dangerous failure of 3.33 × 10^{-7} per hour. The values for B1 and of G1 must be added to this figure for the safety-related stop function



and the safely limited speed. (1.00 + 2.65 + 3.33) × 10^{-7} per hour = 6.98 × 10^{-7} per hour thus results in a PL of d. The values for S1 and G1 must be added for inching mode: a value of (5.28 + 2.65 + 3.33) × 10^{-7} per hour = 1.13 × 10^{-6} per hour is thus produced. This corresponds to PL c.

More detailed references

- EN 1010-1: Safety of machinery – Safety requirements for the design and construction of printing and paper converting machines – Part 1: Common requirements (12.04)
- Safety in Construction and Design of Printing and Paper Converting Machines. Electrical Equipment and Control Systems. Ed.: Berufsgenossenschaft Druck und Papierverarbeitung, Wiesbaden, 2004.
  www.bgdp.de/pages/service/download/medien/220-2e.pdf
- *Apfeld, R.; Zilligen, H.*: Sichere Antriebssteuerungen mit Frequenzumrichtern. BIA Report 5/2003. Ed.: Hauptverband der gewerblichen Berufsgenossenschaften (HVBG), Sankt Augustin, 2003.
  www.dguv.de/bgia, Webcode d6428

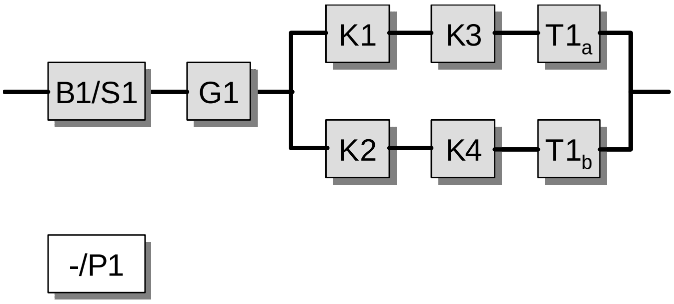
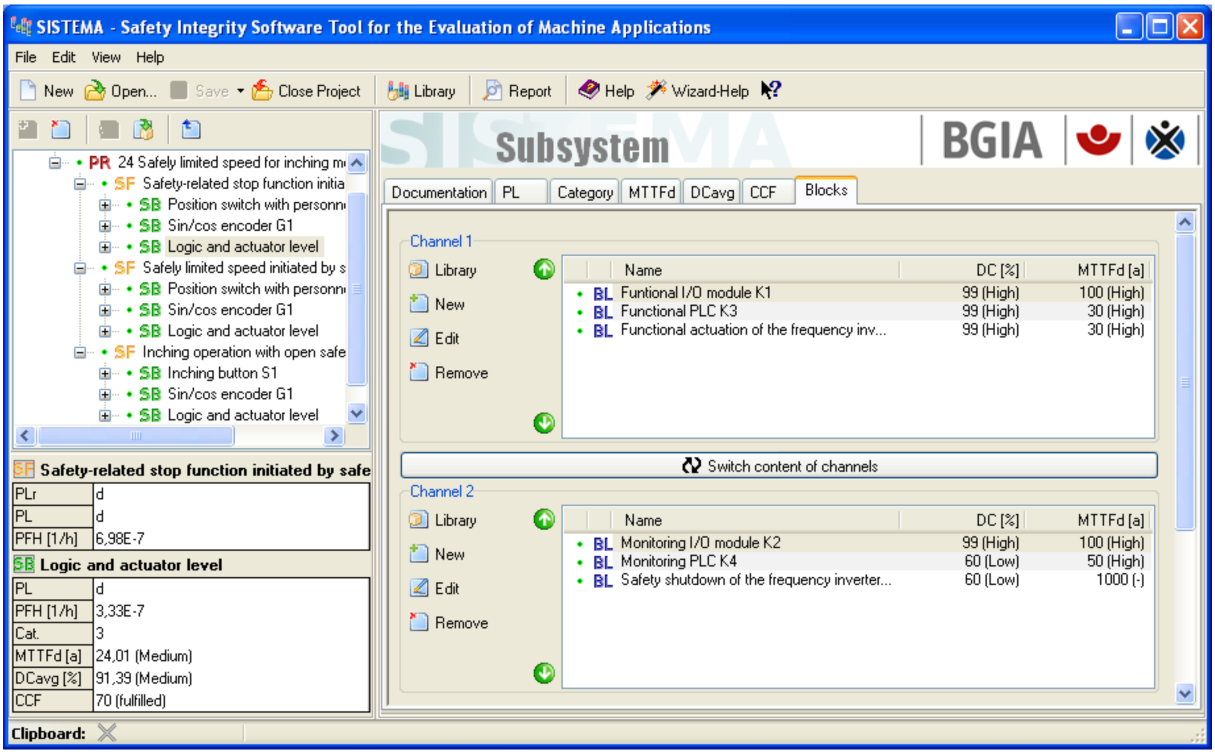


Figure 8.43:
Determining of the PL by means of SISTEMA


SISTEMA - Safety Integrity Software Tool for the Evaluation of Machine Applications
File Edit View Help
New Open... Save Close Project Library Report Help Wizard-Help
Subsystem
BGIA
Documentation PL Category MTTFd DCavg CCF Blocks
Library
New
Edit
Remove
Switch content of channels
Clipboard:

- PR 24 Safely limited speed for inching m
  - SF Safety-related stop function initia
    - SB Position switch with personn
    - SB Sin/cos encoder G1
    - SB Logic and actuator level
  - SF Safely limited speed initiated by s
    - SB Position switch with personn
    - SB Sin/cos encoder G1
    - SB Logic and actuator level
  - SF Inching operation with open safe
    - SB Inching button S1
    - SB Sin/cos encoder G1
    - SB Logic and actuator level

SF Safety-related stop function initiated by safe

PLr	d
PL	d
PFH [1/h]	6,98E-7

SB Logic and actuator level

PL	d
PFH [1/h]	3,33E-7
Cat.	3
MTTFd [a]	24,01 (Medium)
DCavg [%]	91,39 (Medium)
CCF	70 (fulfilled)

Channel 1

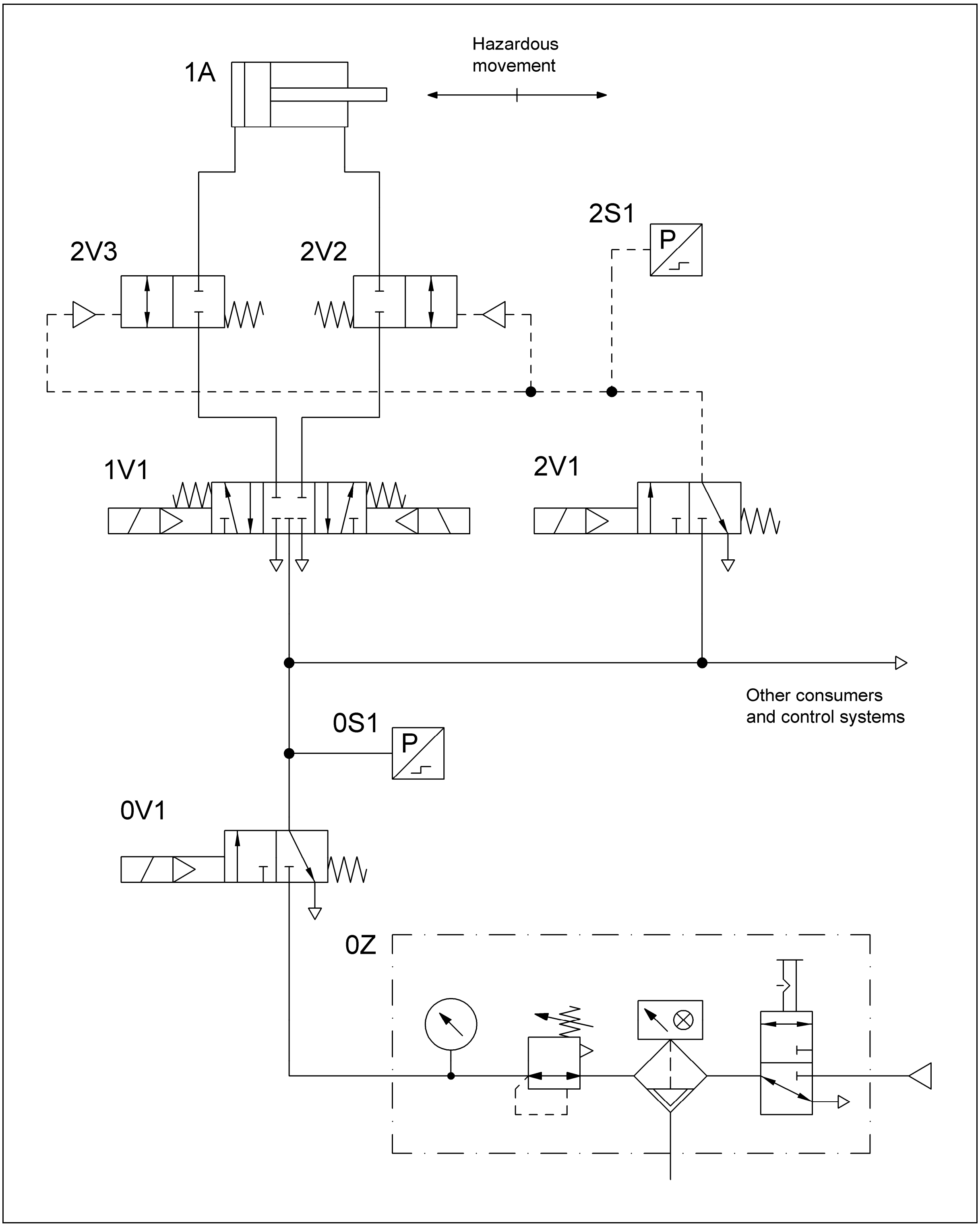
	Name	DC [%]	MTTFd [a]
BL	Funtional I/O module K1	99 (High)	100 (High)
BL	Functional PLC K3	99 (High)	30 (High)
BL	Functional actuation of the frequency inv...	99 (High)	30 (High)

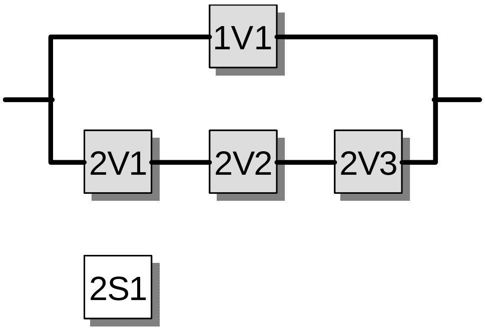
Channel 2

	Name	DC [%]	MTTFd [a]
BL	Monitoring I/O module K2	99 (High)	100 (High)
BL	Monitoring PLC K4	60 (Low)	50 (High)
BL	Safety shutdown of the frequency inverter...	60 (Low)	1000 (-)

8.2.25 Pneumatic valve control (subsystem) – Category 3 – PL e (for PL d safety functions) (Example 25)

Figure 8.44:
Tested pneumatic valves for redundant control of hazardous movements





Safety functions

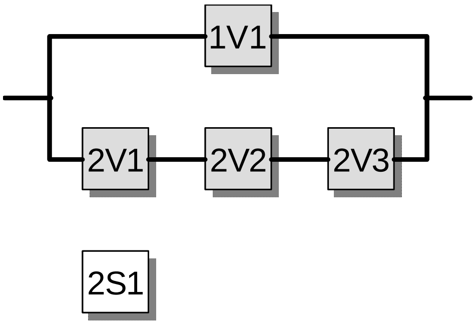
- Safety-related stop function: stopping of the hazardous movement and prevention of unexpected start-up from the rest position
- Only the pneumatic part of the control is shown here, in the form of a subsystem. Further safety-related control components (e.g. protective devices and electrical logic elements) must be added in the form of subsystems for completion of the safety function.

Functional description

- Hazardous movements are controlled redundantly by directional control valves. Movements can be halted either by the directional control valve 1V1 or by the directional control valves 2V2 and 2V3. The latter are driven by the control valve 2V1.
- Failure of one of these valves alone does not result in loss of the safety function.
- All directional control valves are actuated cyclically in the process.
- The functioning of the control valve 2V1 is monitored by means of a pressure switch 2S1. Certain faults on the unmonitored valves are recognized in the work process. The valves 2V2 and 2V3 should be equipped with position monitors, or – since this is not yet state of the art – their operation should be checked regularly. An accumulation of undetected faults may lead to loss of the safety function.
- Should trapped compressed air pose a further hazard, additional measures are required.

Design features

- Basic and well-tried safety principles are observed and the requirements of Category B are met.
- The directional control valve 1V1 features a closed centre position with sufficient overlap and spring-centering.
- The stop valves 2V2 and 2V3 are ideally screwed into the cylinder and driven by the valve 2V1 acting as a pilot valve.



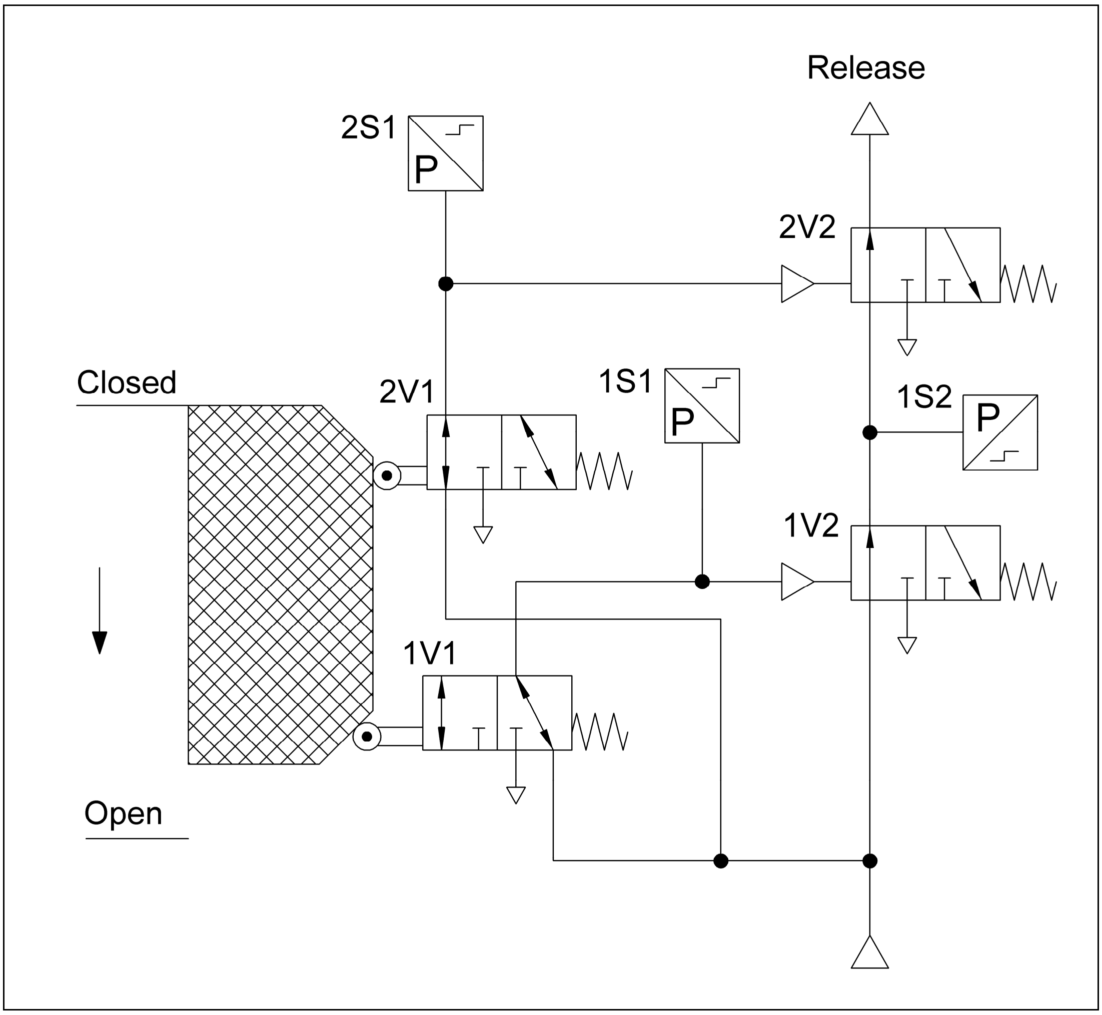
- The safety-oriented switching position is assumed from any position by removal of the control signal.
- A single-channel PLC for example is employed for processing of signals from the pressure monitor 2S1.

Calculation of the probability of failure

- *MTTF*$_d$: B$_{10d}$ values of 40,000,000 cycles [E] are assumed for the valves 1V1 and 2V1. B$_{10d}$ values of 60,000,000 cycles [E] are assumed for the valves 2V2 and 2V3. At 240 working days, 16 working hours and a cycle time of 10 seconds, n_{op} is 1,382,400 cycles per year. The *MTTF*$_d$ of 1V1 and 2V1 is thus 289 years, and that of 2V2 and 2V3 434 years. Capping of the two channels to 100 years results in a symmetrized MTTF$_d$ value per channel of 100 years (“high”).
- *DC*$_{avg}$: pressure monitoring of the control signal for the stop valves results in a *DC* of 99% for 2V1. Fault detection via the process results in a *DC* of 60% for 1V1, and regular checking of operation in a *DC* of 60% for 2V2/2V3. Averaging thus results in a *DC*$_{avg}$ of 71% (“low”).
- Adequate measures against common cause failure (85 points): separation (15), diversity (20), overvoltage protection etc. (15) and environmental conditions (25 + 10)
- The combination of the pneumatic control elements corresponds to Category 3 with a high *MTTF*$_d$ (100 years) and low *DC*$_{avg}$ (71%). This results in an average probability of dangerous failure of 7.86 × 10^{-8} per hour. This corresponds to PL e. The addition of further safety-related control parts as subsystems for completion of the safety function generally results in a lower PL.

8.2.26 Pneumatic valve control – Category 3 – PL e (Example 26)

Figure 8.45:
Redundant pneumatic control system for the interlocking of moveable guards

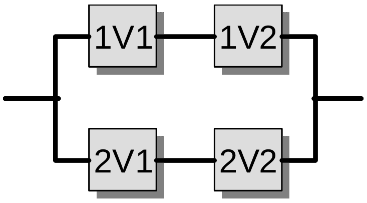


Safety function

- Safety-related stop function, initiated by a protective device: when the moveable guard is opened, the power is disconnected and the pneumatic control system depressurized.

Functional description

- The movable guard is interlocked by two “pneumatic position switches” (1V1 and 2V1). 1V1 and 2V1 issue control commands to the directional control valves 1V2 and 2V2 respectively.
- Pneumatic power is supplied only when the protective device is closed.
- Failure of a “pneumatic position switch” or directional control valve does not result in loss of the safety function.



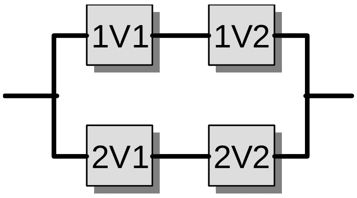
- Faults on valves 2V1 and 1V2 are detected by the pressure switches 1S1, 2S1 and 1S2. The relevant signals can be processed in a PLC. Should a fault be detected, the power can for example be disconnected. No fault detection is provided for the valve 2V2. This valve should be checked regularly for proper operation. An accumulation of undetected faults may lead to loss of the safety function.
- Should trapped compressed air pose a further hazard, additional measures are required.

Design features

- Basic and well-tried safety principles are observed and the requirements of Category B are met.
- 1V1 is a pneumatic position switch with positive actuation by the moveable guard in accordance with EN 1088.
- A stable arrangement of the protective device is assured for actuation of the position switch.
- The safety-oriented switch position of the directional control valves 1V2 and 2V2 is attained by removal of the control signals.

Calculation of the probability of failure

- $MTTF_d$: fault exclusion is assumed for the valve 1V1, since positive operation is assured by the moveable guard and the valve takes the form of a position switch with personnel safety function (based upon IEC 60947-5-1). $B10_d$ values of 20,000,000 cycles [S] are assumed for the valves 2V1, 1V2 and 2V2. At 240 working days, 16 working hours and a cycle time of 30 seconds, n_{op} is 460,800 cycles per year and the $MTTF_d$ is 434 years. Capping of the two channels to 100 years results in a symmetrized MTTF_d value per channel of 100 years (“high”).
- DC_{avg}: a *DC* of 99% is produced for the directional control valves 2V1 and 1V2 owing to fault detection by means of the pressure switches. A *DC* of 0% is assumed for the directional control valve 2V2 (estimation erring on the safe side). Averaging thus results in a DC_{avg} of 66% (“low”).
- Adequate measures against common cause failure (65 points): separation (15), overvoltage protection etc. (15) and environmental conditions (25 + 10)
- The combination of the pneumatic control elements corresponds to Category 3 with a high $MTTF_d$ (100 years) and low DC_{avg} (66%). This results in an average

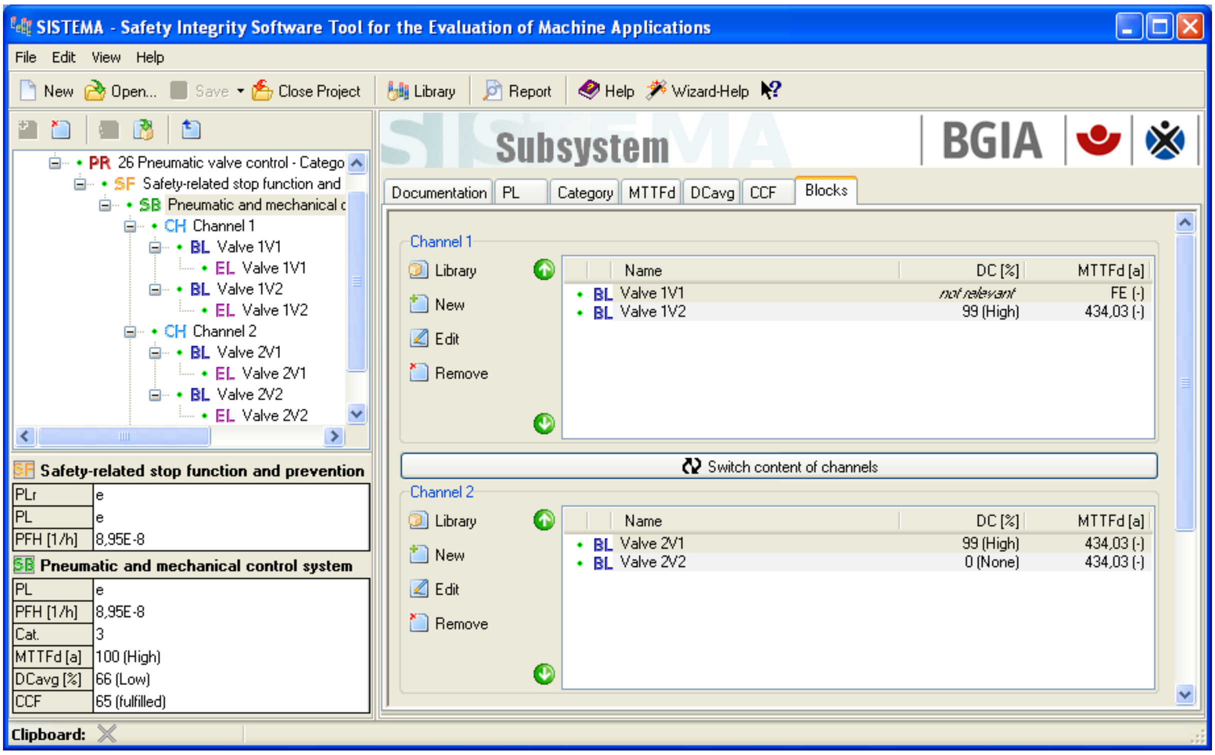


probability of dangerous failure of 8.95 × 10^{-8} per hour. This corresponds to PL e.

More detailed reference

- IEC 60947-5-1: Low-voltage switchgear and controlgear – Part 5-1: Control circuit devices and switching elements – Electromechanical control circuit devices (11.03)

Figure 8.46:
Determining of the PL by means of SISTEMA



PR 26 Pneumatic valve control - Catego
SF Safety-related stop function and
SB Pneumatic and mechanical c
CH Channel 1
BL Valve 1V1
EL Valve 1V1
BL Valve 1V2
EL Valve 1V2
CH Channel 2
BL Valve 2V1
EL Valve 2V1
BL Valve 2V2
EL Valve 2V2

SF Safety-related stop function and prevention

PLr	e
PL	e
PFH [1/h]	8,95E-8

SB Pneumatic and mechanical control system

PL	e
PFH [1/h]	8,95E-8
Cat.	3
MTTFd [a]	100 (High)
DCavg [%]	66 (Low)
CCF	65 (fulfilled)

Channel 1

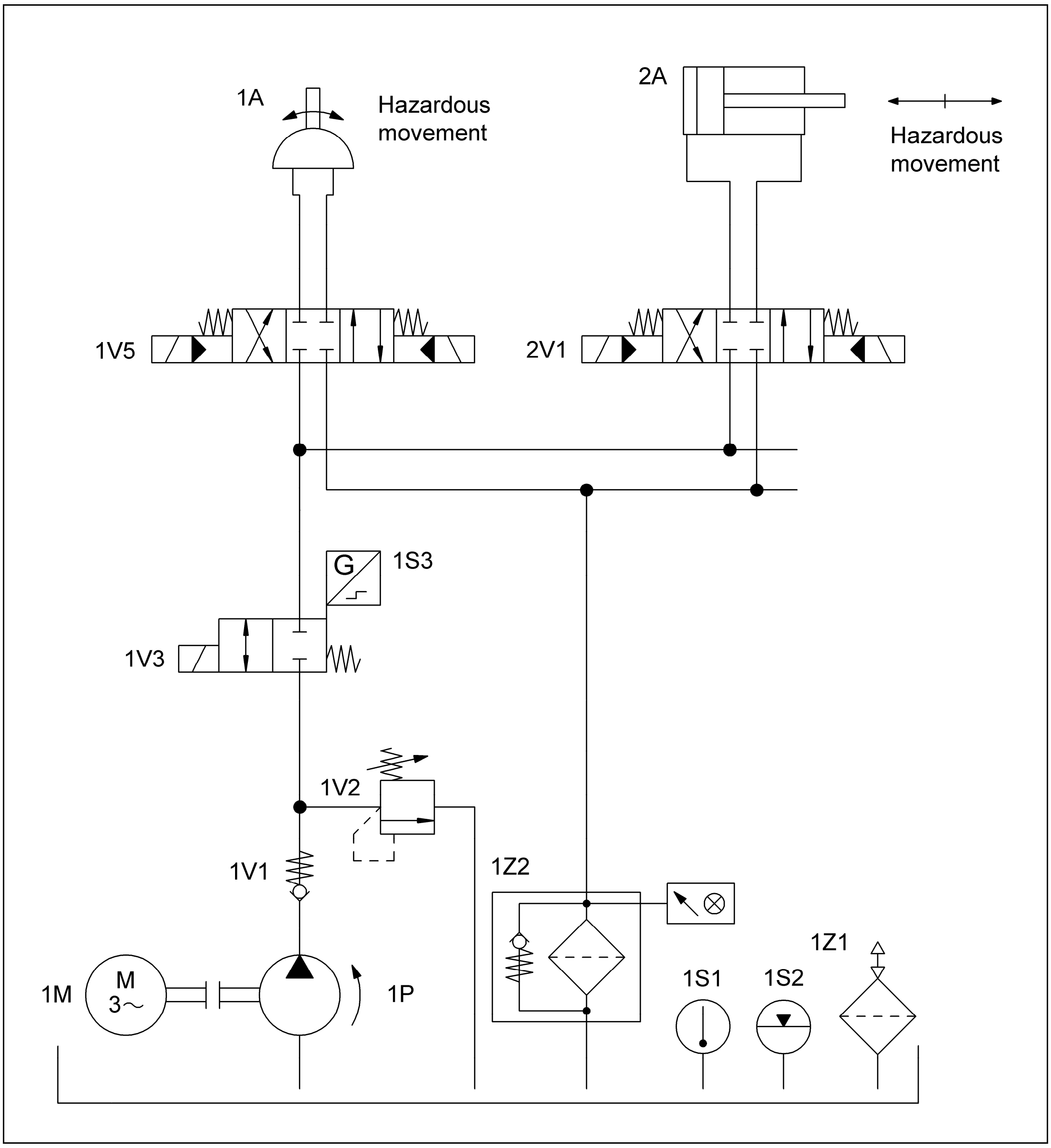
Name	DC [%]	MTTFd [a]
BL Valve 1V1	*not relevant*	FE (-)
BL Valve 1V2	99 (High)	434,03 (-)

Channel 2

Name	DC [%]	MTTFd [a]
BL Valve 2V1	99 (High)	434,03 (-)
BL Valve 2V2	0 (None)	434,03 (-)

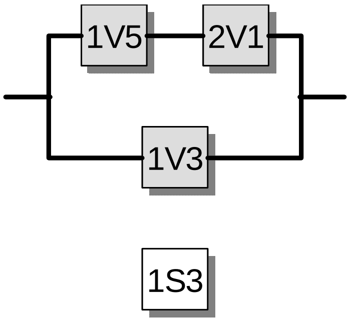
8.2.27 Hydraulic valve control (subsystem) – Category 3 – PL e (for PL d safety functions) (Example 27)

Figure 8.47:
Tested hydraulic valves for redundant control of hazardous movements



Safety functions

- Safety-related stop function: stopping of the hazardous movement and prevention of unexpected start-up from the rest position
- Only the hydraulic part of the control is shown here, in the form of a subsystem. Further safety-related control components (e.g. protective devices and electrical logic elements) must be added in the form of subsystems for completion of the safety function.



Functional description

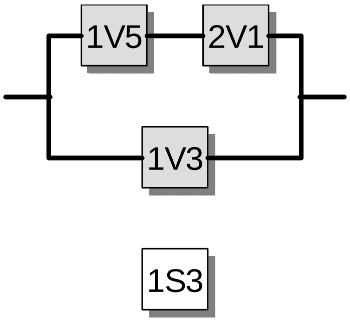
- Hazardous movements are executed in the same hazardous area by two actuators, 1A and 2A. The two movements can be stopped either by the two directional control valves 1V5 and 2V1, or at a higher level by directional control valve 1V3.
- Failure of one of these valves alone does not result in loss of the safety function.
- 1V5 and 2V1 are actuated cyclically in the process. 1V3 closes only in response to a demand upon the safety function, but at least once per shift.
- A technical measure for fault detection is implemented only on 1V3 (position monitoring by 1S3). Certain faults on the unmonitored valves are recognized in the work process. An accumulation of undetected faults may lead to loss of the safety function.

Design features

- Basic and well-tried safety principles are observed and the requirements of Category B are met.
- The directional control valves 1V5 and 2V1 possess a closed centre position with sufficient overlap and spring-centering. 1V3 features electrical position monitoring, since 1V3 is not switched cyclically.
- The safety-oriented switch position is attained in each case by removal of the control signal (electrical or hydraulic).
- A single-channel PLC may be used for signal processing of the electrical position monitoring.

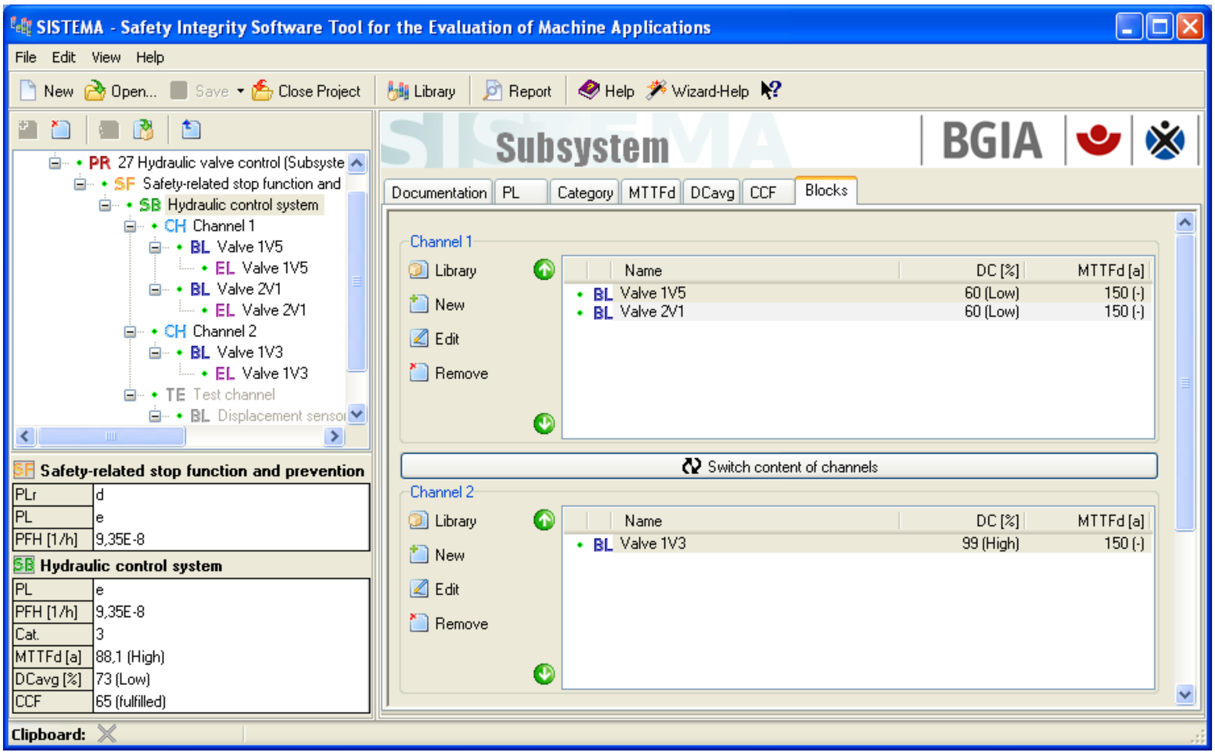
Calculation of the probability of failure

- $MTTF_d$: an $MTTF_d$ of 150 years [S] is assumed for the directional control valves 1V3, 1V5 and 2V1. Capping of the second channel (1V3) to 100 years produces a symmetrized MTTF_d value of 88 years (“high”).
- DC_{avg}: a *DC* of 99% for 1V3 is based upon the direct monitoring of the switching state by 1S3. The *DC* of 60% for the directional control valves 1V5 and 2V1 is based upon indirect monitoring by the process. Averaging thus produces a DC_{avg} of 73% (“low”).



- Adequate measures against common cause failure (65 points): separation (15), overvoltage protection etc. (15) and environmental conditions (25 + 10)
- The combination of the hydraulic control elements corresponds to Category 3 with a high $MTTF_d$ (88 years) and low DC_{avg} (73%). This results in an average probability of dangerous failure of 9.35 × 10^{-8} per hour. This corresponds to PL e. The addition of further safety-related control parts in the form of subsystems for completion of the safety function generally results in a lower PL.

Figure 8.48:
Determining of the PL by means of SISTEMA


SISTEMA - Safety Integrity Software Tool for the Evaluation of Machine Applications
File Edit View Help
New Open... Save Close Project Library Report Help Wizard-Help
Subsystem
BGIA
Documentation PL Category MTTFd DCavg CCF Blocks
Library
New
Edit
Remove
Switch content of channels
Clipboard:

PR 27 Hydraulic valve control (Subsyste
SF Safety-related stop function and
SB Hydraulic control system
CH Channel 1
BL Valve 1V5
EL Valve 1V5
BL Valve 2V1
EL Valve 2V1
CH Channel 2
BL Valve 1V3
EL Valve 1V3
TE Test channel
BL Displacement sensor

SF Safety-related stop function and prevention

PLr	d
PL	e
PFH [1/h]	9,35E-8

SB Hydraulic control system

PL	e
PFH [1/h]	9,35E-8
Cat.	3
MTTFd [a]	88,1 (High)
DCavg [%]	73 (Low)
CCF	65 (fulfilled)

Channel 1

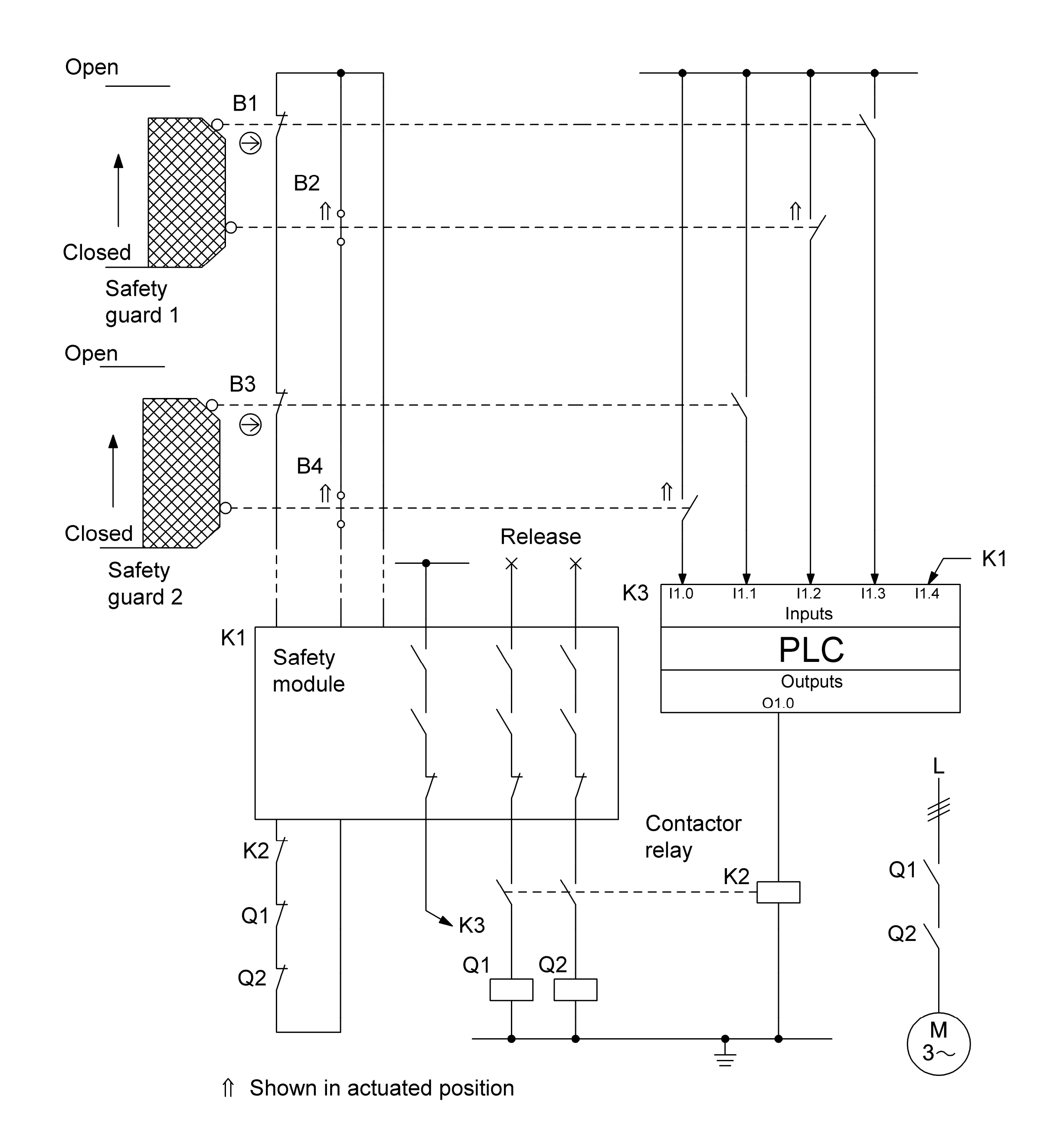
Name	DC [%]	MTTFd [a]
BL Valve 1V5	60 (Low)	150 (-)
BL Valve 2V1	60 (Low)	150 (-)

Channel 2

Name	DC [%]	MTTFd [a]
BL Valve 1V3	99 (High)	150 (-)

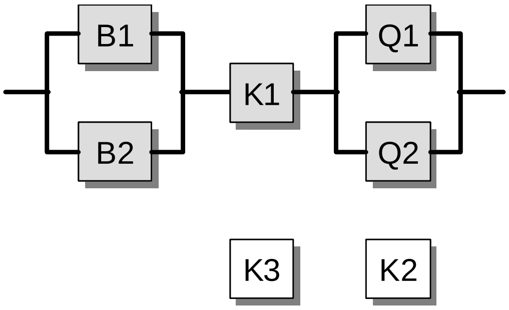
8.2.28 Position monitoring of moveable guards – Category 4 – PL e (Example 28)

Figure 8.49:
Position monitoring of moveable guards for the prevention of hazardous movements



Safety function

- Safety-related stop function, initiated by a protective device: opening of a moveable guard (safety guard) initiates the safety function STO (safe torque off).

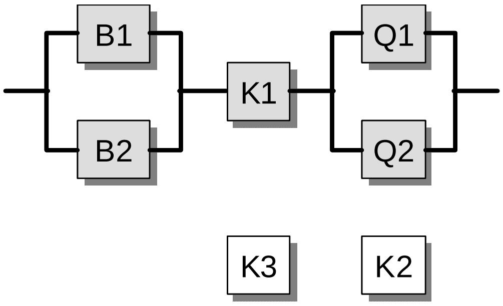


Functional description

- A hazardous zone is safeguarded by two moveable guards (safety guards). Opening of the two safety guards is detected by two position switches B1/B2 and B3/B4 comprising break contact/make contact combinations and evaluated by a central safety module K1. K1 actuates two contactors, Q1 and Q2, dropping out of which interrupts or prevents hazardous movements or states.
- For fault detection purposes, all position switch states are read by a second contact into a standard PLC K3, the chief purpose of which is functional control. In the event of a fault, K3 can de-energize the contactors Q1 and Q2 independently of K1 by means of a contactor relay K2. Faults in K2, Q1 and Q2 are detected by the safety module K1. A small number of faults are not detected (e.g. failure of the contacts in B2 and B4 to break).
- The safety function is retained in the event of a component failure. The majority of component failures are detected and lead to operating inhibition. An accumulation of undetected faults does not result in loss of the safety function.

Design features

- Basic and well-tried safety principles are observed and the requirements of Category B are met. Protective circuits (e.g. contact protection) as described in the initial paragraphs of Chapter 8 are implemented.
- A stable arrangement of the protective devices is assured for actuation of the position switches.
- B1 and B3 are position switches with direct opening contacts according to IEC 60947-5-1, Annex K.
- The supply conductors to the position switches are laid separately or with protection.
- Faults in the start-up and actuation mechanism are detected by the use of two position switches differing in the principle of their actuation (break and make contact combination).
- Several protective devices may be cascaded.
- The safety module K1 satisfies all requirements for Category 4 and PL e.
- The contactors K2, Q1 and Q2 possess mechanically linked contact elements to IEC 60947-5-1, Annex L.



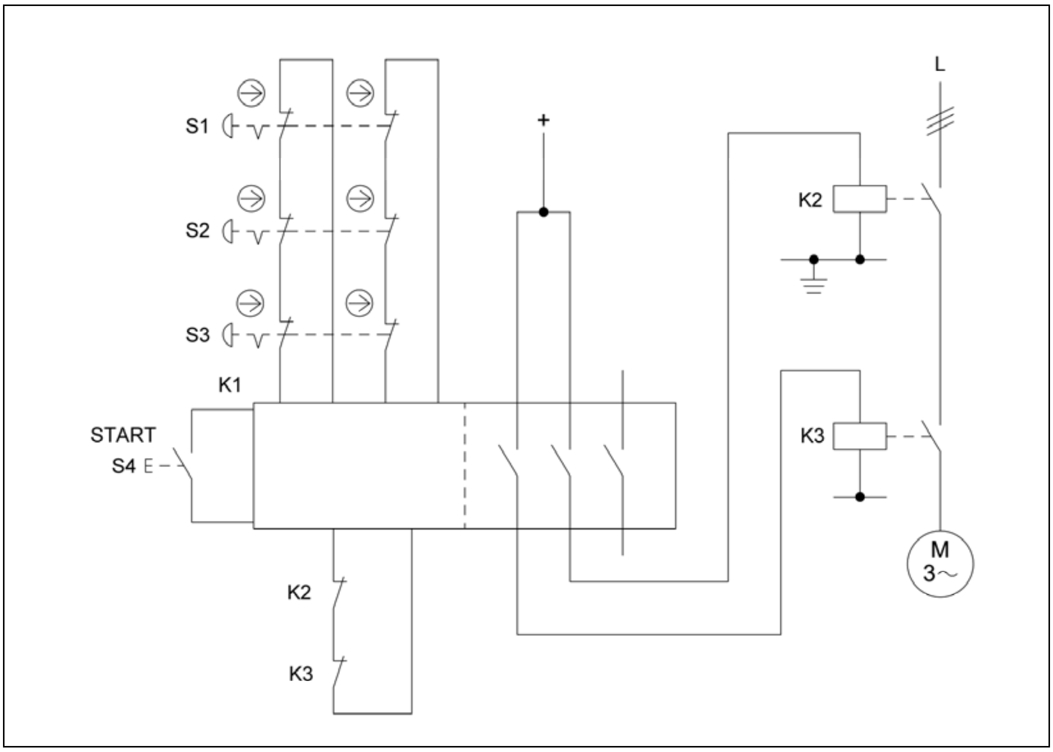
- The PLC K1 satisfies the normative requirements described in Section 6.3.

Calculation of the probability of failure

- The circuit arrangement can be divided into three subsystems as shown in the safety-related block diagram. The probability of failure of the safety module K1 is added at the end of the calculation (2.31 × 10^{-9} per hour [M], suitable for PL e). For the remaining subsystems, the probability of failure is calculated as follows. Since each safety guard forms part of a dedicated safety function, calculation is shown here by substitution for protective device 1.
- $MTTF_d$: fault exclusion is possible for the electrical contact of the position switch B1 with direct opening contact. For the electrical make contact of the position switch B2, the B_{10d} value is 1,000,000 switching operations [M]. A B_{10d} value of 1,000,000 cycles [M] is stated for the mechanical part of B1 and B2. At 365 working days, 16 working hours per day and a cycle time of 1 hour, n_{op} is 5,840 cycles per year for these components, and the $MTTF_d$ is 1,712 years for B1 and 856 years for B2. For the contactors Q1 and Q2, the B_{10} value corresponds under inductive load (AC 3) to an electrical lifetime of 1,000,000 switching operations [M]. If 50% of failures are assumed to be dangerous, the B_{10d} value is produced by doubling of the B_{10} value. The value assumed above for n_{op} results in an $MTTF_d$ of 3,424 years per channel for Q1 and Q2. Altogether, the symmetrized $\mathrm{MTTF_d}$ value per channel in the two subsystems is 100 years (“high”).
- DC_{avg}: the *DC* of 99% for B1 and B2 is based upon plausibility monitoring of the break/make contact combinations in the PLC K3. The *DC* of 99% for the contactors Q1 and Q2 is derived from monitoring at each energization of K1. The DC values stated correspond to the DC_{avg} of the subsystem concerned.
- Adequate measures against common cause failure in the subsystems B1/B2 and Q1/Q2 (70 points): separation (15), well-tried components (5), protection against overvoltage etc. (15) and environmental conditions (25 + 10)
- The subsystems B1/B2 and Q1/Q2 both correspond to Category 4 with a high $MTTF_d$ (100 years) and high DC_{avg} (99%). This results in an average probability of dangerous failure in each case of 2.47 × 10^{-8} per hour. Following addition of the subsystem K1, the average probability of dangerous failure is 5.16 × 10^{-8} per hour. This corresponds to PL e.

8.2.29 Cascading of emergency stop devices by means of a safety module – Category 3 – PL e (Example 29)

Figure 8.50:
Cascading of emergency stop devices by means of a safety module (emergency stop function, STO)

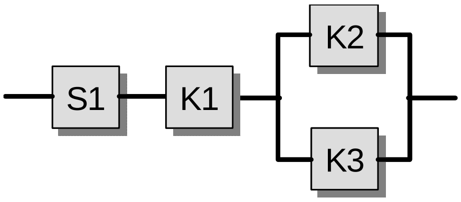


Safety function

- Emergency stop function, STO by actuation of an emergency stop device

Functional description

- Hazardous movements or states are interrupted or prevented by actuation of an emergency stop device. As shown by Example 3 in Section 5.3.2, each emergency stop device triggers a safety function of its own. S1 is considered below as being representative of all the devices. S1 is evaluated in a safety module K1, which actuates two redundant contactor relays K2 and K3.
- The signals from the emergency stop devices are read redundantly into the safety module K1 for fault detection. K1 also features internal test measures. The contactor relays K2 and K3 are also monitored in K1, by means of mechanically linked readback contacts. K2 and K3 are operated by switch S4 at each start-up command, approximately twice each month. An accumulation of more than two faults in the period between two successive actuations may lead to loss of the safety function.
- It is not assumed that more than one emergency stop device is pressed simultaneously.



Design features

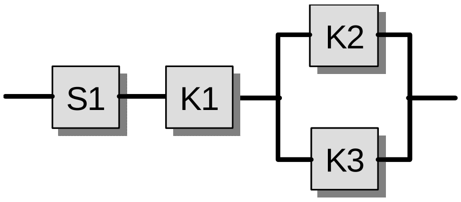
- Basic and well-tried safety principles are observed and the requirements of Category B are met. Protective circuits (e.g. contact protection) as described in the initial paragraphs of Chapter 8 are implemented.
- The emergency stop devices S1, S2 and S3 are switching devices with direct opening contacts in accordance with IEC 60947-5-1, Annex K.
- The supply conductors to the switching devices are laid separately or with protection.
- The safety module K1 satisfies all requirements for Category 4 and PL e.
- K2 and K3 possess mechanically linked contact elements to IEC 60947-5-1, Annex L.

Remark

- The emergency stop function is a complementary protective measure to EN ISO 12100-2:2004.

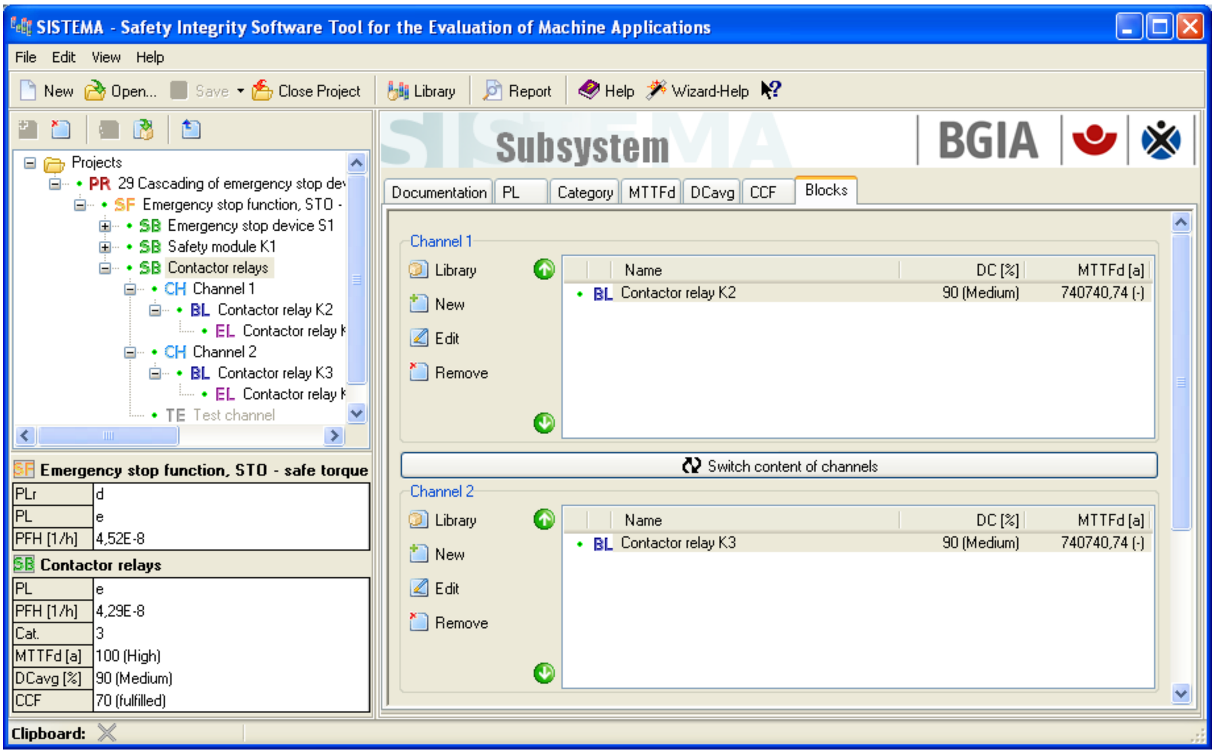
Calculation of the probability of failure:

- S1, S2 and S3 are standard emergency stop devices to EN ISO 13850. Fault exclusions apply for the direct opening contacts and for the mechanical elements, provided the number of operations stated in Table D.2 of this report is not exceeded.
- The probability of failure of the final safety module K1 is added at the end of the calculation (2.31 × 10^{-9} per hour [M], suitable for PL e). For the subsystem K2/K3, the probability of failure is calculated as follows.
- $MTTF_d$: for the contactor relays K2 and K3, the B_{10} value corresponds under inductive load (AC 3) to an electrical lifetime of 1,000,000 switching operations [M]. If 50% of failures are assumed to be dangerous, the B_{10d} value is produced by doubling of the B_{10} value. With three demands upon the emergency stop function and 24 start commands per year, n_{op} is 27 cycles per year and the $MTTF_d$ is 740,740 years. This is also the symmetrical $MTTF_d$ for the channel, which is capped to 100 years ("high").
- DC_{avg}: the *DC* of 90% for K2 and K3 is based upon testing by the safety module K1. This is also the DC_{avg} ("medium").
- Adequate measures against common cause failure (70 points): separation (15), well-tried components (5), overvoltage protection etc. (15) and environmental conditions (25 + 10)



- The subsystem K2/K3 corresponds to Category 3 with a high *MTTF*$_d$ (100 years) and medium *DC*$_{avg}$ (90%). This results in an average probability of dangerous failure of 4.29 × 10^{-8} per hour. Following addition of the subsystem K1, the average probability of dangerous failure is 4.52 × 10^{-8} per hour. This corresponds to PL e. The PL$_r$ of d is thus surpassed.

Figure 8.51:
Determining of the PL by means of SISTEMA


SISTEMA - Safety Integrity Software Tool for the Evaluation of Machine Applications
File Edit View Help
New Open... Save Close Project Library Report Help Wizard-Help
Subsystem
BGIA
Documentation PL Category MTTFd DCavg CCF Blocks
Library
New
Edit
Remove
Switch content of channels
Clipboard:

Projects
PR 29 Cascading of emergency stop dev
SF Emergency stop function, STO -
SB Emergency stop device S1
SB Safety module K1
SB Contactor relays
CH Channel 1
BL Contactor relay K2
EL Contactor relay K
CH Channel 2
BL Contactor relay K3
EL Contactor relay K
TE Test channel

SF Emergency stop function, STO - safe torque

PLr	d
PL	e
PFH [1/h]	4,52E-8

SB Contactor relays

PL	e
PFH [1/h]	4,29E-8
Cat.	3
MTTFd [a]	100 (High)
DCavg [%]	90 (Medium)
CCF	70 (fulfilled)

Channel 1

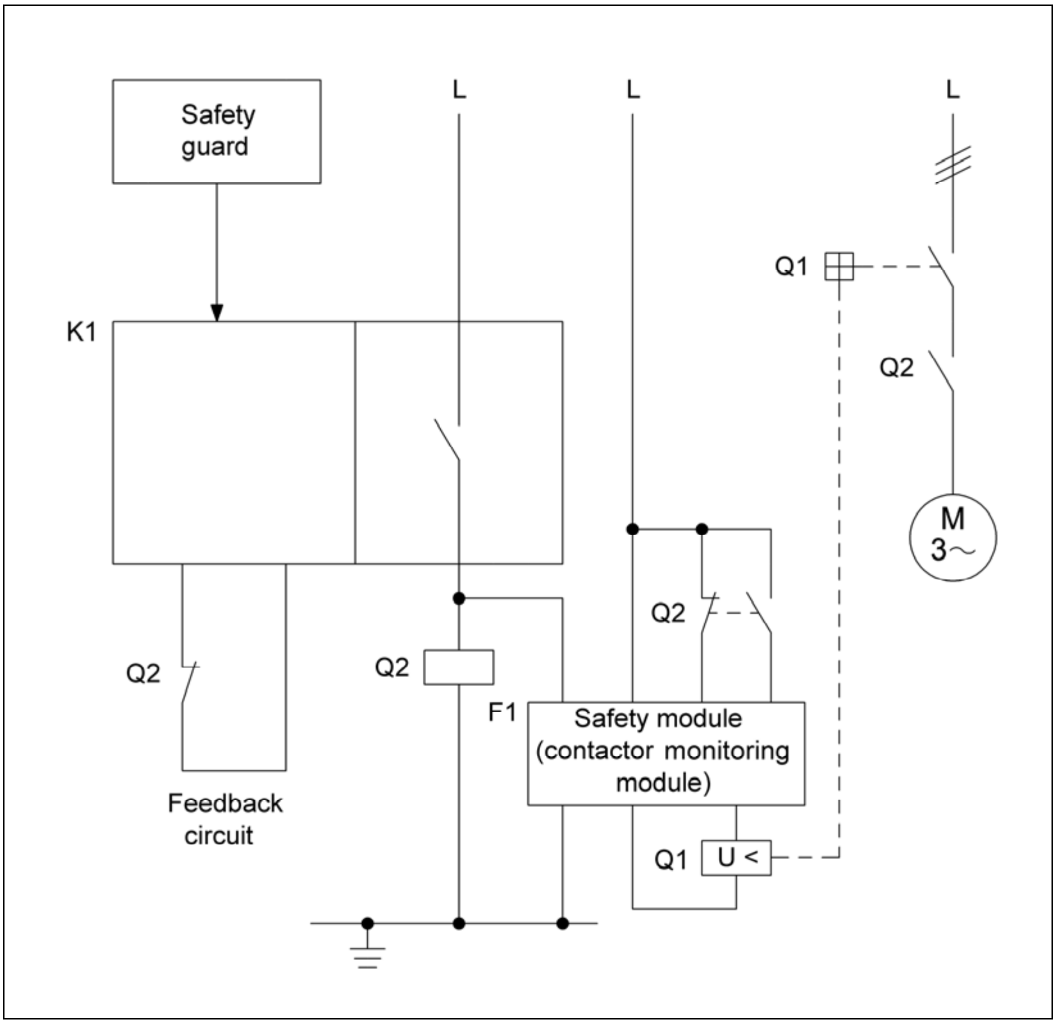
Name	DC [%]	MTTFd [a]
BL Contactor relay K2	90 (Medium)	740740,74 (-)

Channel 2

Name	DC [%]	MTTFd [a]
BL Contactor relay K3	90 (Medium)	740740,74 (-)

8.2.30 Contactor monitoring module – Category 3 – PL e (Example 30)

Figure 8.52:
Initiation of STO (safe torque off) by means of a safety module and contactor monitoring module

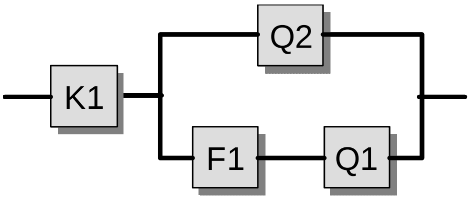


Safety function

- Safety-related stop function, initiated by a protective device: opening of the moveable guard initiates the safety function STO (safe torque off).

Functional description

- A hazardous zone is safeguarded by means of a protective device the opening of which is detected by a safety module K1. The latter actuates a contactor Q2 and a combination of a contactor monitoring module F1 and an undervoltage release Q1. The dropping-out of Q2 interrupts hazardous movements and prevents hazardous states. The contactor monitoring module F1 has the function of monitoring the main contacts of contactor Q2 for contact welding. Should Q2 fail to drop out, F1 trips the upstream circuit-breaker or motor starter Q1 via the



latter's undervoltage release. The circuit-breaker or motor starter then switches off the motor.

- The safety function is retained in the event of a component failure.
- An accumulation of faults between two successive actuations may lead to loss of the safety function.

Design features

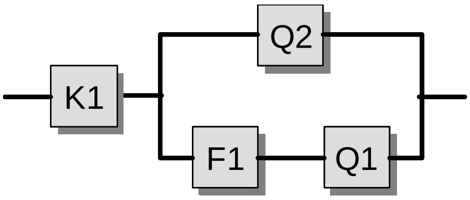
- Circuit-breaker Q1 is checked regularly by means of a test function which is to be implemented manually. The interval between the tests should not exceed one-hundredth of the $MTTF_d$ of Q1; the test could be performed for example during maintenance of the machine. The contactor Q2 is tested continually by the contactor monitoring module. Loss of the safety function between the tests, as is possible with Category 2, cannot occur. The single-fault tolerance is thus assured and the requirements of Category 3 are met.
- Basic and well-tried safety principles are observed and the requirements of Category B are met. Protective circuits (e.g. contact protection) as described in the initial paragraphs of Chapter 8 are implemented.
- For reasons of simplification, details of the protective device have been omitted from the presentation.
- The protective device acts upon a safety module K1 which satisfies all requirements for Category 3 or 4 and PL e.
- Contactor Q2 features mirror contacts to IEC 60947-4-1, Annex F, and is integrated into the feedback of safety module K1 for contactor fault detection.
- Fault consideration for Q2 (with mirror contacts) and for the internal relay of the contactor monitoring module F1 is as for mechanically linked contacts.

Remark

- Consideration must be given to the response time caused by contactor monitoring module F1 with regard to the dropping-out of Q1.

Calculation of the probability of failure

- The safety function permits division into two subsystems. The subsystem consisting of the protective device and safety module K1 is not considered in this example.
- $MTTF_d$: for the contactor monitoring module F1, the $MTTF_d$ is 125 years at a maximum n_{op} of 350,400 cycles per year [M]. Under inductive load (AC 3), the B_{10d} value for Q1 is 10,000 switching cycles, and the B_{10d} value for Q2

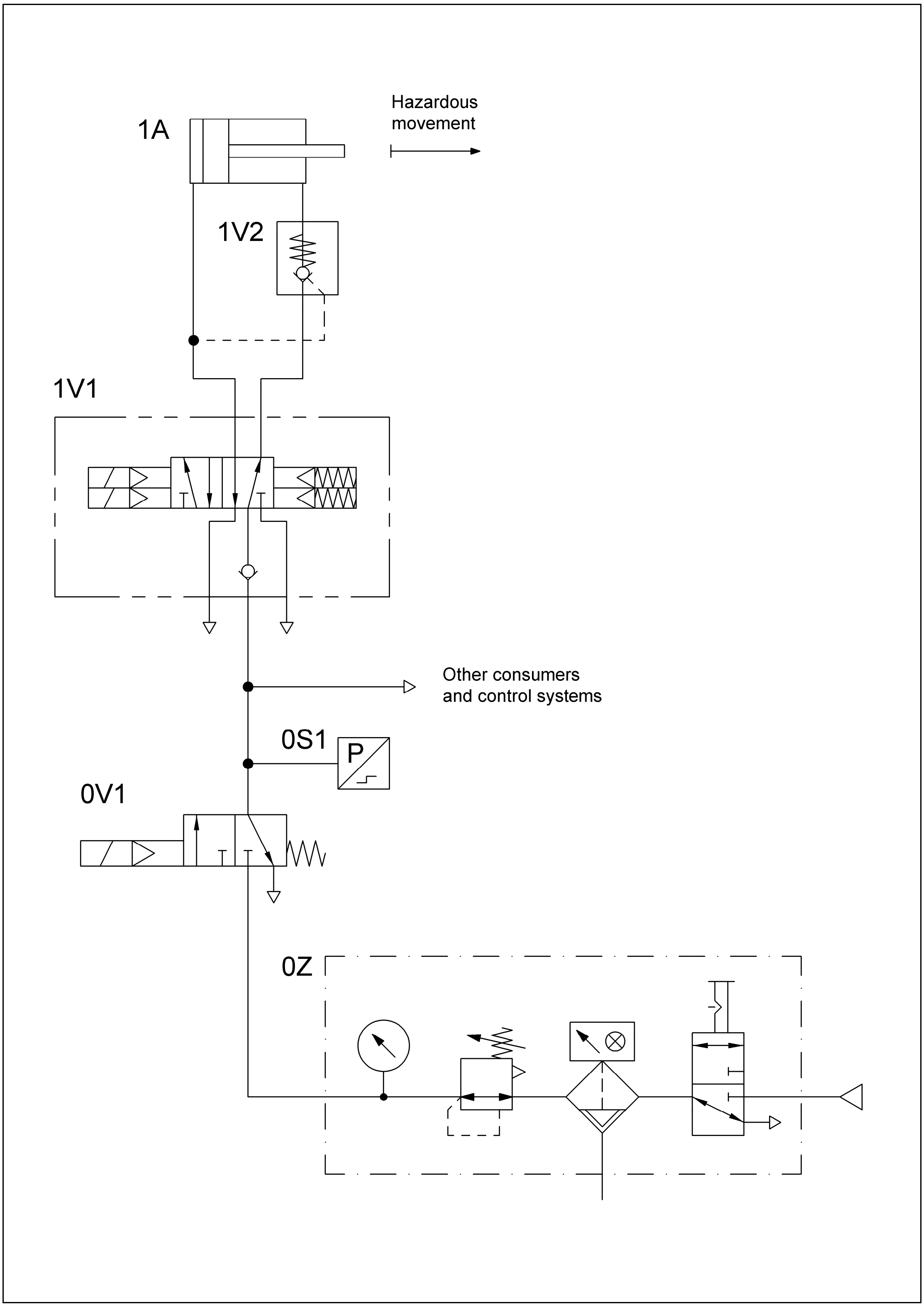


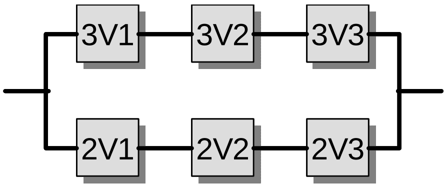
1,300,000 switching cycles. Assuming a once daily actuation on 365 working days, n_{op} is 365 cycles per year for Q1, and the $MTTF_d$ is 274 years. At 365 working days, 16 working hours per day and a cycle time of 1 minute, n_{op} is 350,400 cycles per year for Q2, and the $MTTF_d$ is 37 years. For the channel consisting of F1 and Q1, this results in an $MTTF_d$ of 85 years. Overall, the resulting symmetrized $\mathrm{MTTF_d}$ value per channel is 64 years ("high").

- DC_{avg}: the *DC* of 99% for Q2 is based upon testing by means of the contactor monitoring module F1. A *DC* of 99% for F1 is achieved by fault-detection measures within the contactor monitoring module. The circuit-breaker is tested by means of the manual test function which is to be implemented; this produces a *DC* of 90%. A *DC* of 99% is substituted for F1. Averaging thus yields a DC_{avg} of 98% ("medium").
- Adequate measures against common cause failure (65 points): separation (15), overvoltage protection etc. (15) and environmental conditions (25 + 10)
- The subsystem comprising Q1, Q2 and F1 corresponds to Category 3 with a high $MTTF_d$ (64 years) and medium DC_{avg} (98%). This results in an average probability of dangerous failure of 4.45×10^{-8} per hour. This corresponds to PL e. Following addition of the subsystem comprising protective device and safety module K1, the PL may under certain circumstances be lower.
- In consideration of estimation erring on the safe side as described above, a T_{10d} value of 3.7 years is produced for the wearing element Q2 when replaced as specified.

8.2.31 Pneumatic valve control (subsystem) – Category 4 – PL e (Example 31)

Figure 8.53:
Tested pneumatic valves for redundant control of hazardous movements





Safety functions

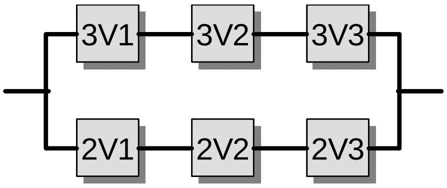
- Safety-related function: reversing of the hazardous movement and prevention of unexpected start-up from the rest position
- Only the pneumatic part of the control is shown here, in the form of a subsystem. Further safety-related control components (e.g. protective devices and electrical logic elements) must be added in the form of subsystems for completion of the safety function.

Functional description

- Hazardous movements are controlled by a valve combination 1V1 with self-monitoring, in conjunction with a pilot-operated non-return-valve 1V2 (relevant in the event of failure of the pneumatics and under external forces).
- A component failure within the valve combination does not result in loss of the safety function.
- The two pilot valves contained in the valve combination 1V1 are actuated separately. Should at least one of the control signals be removed, the movement is reversed.
- A single failure within the valve combination results in disablement in the safe state and is therefore detected in the working process; initiation of the next hazardous movement is prevented.
- The valve combination 1V1 can also be formed by several valves suitably linked and with suitable querying of the switching positions.
- Should trapped compressed air pose a further hazard, additional measures are required.

Design features

- Basic and well-tried safety principles are observed and the requirements of Category B are met.
- 1V1 is a self-monitoring valve combination with mechanically separate integrated pilot valves and pneumatic/mechanical fault detection with integrated non-return-valve in the P line.
- The safety-oriented switch position is attained by removal of the control signals.
- The pilot-operated non-return-valve 1V2 should ideally be screwed into the cylinder.
- Fault detection within the valve combination satisfies the corresponding requirements for the fault case.



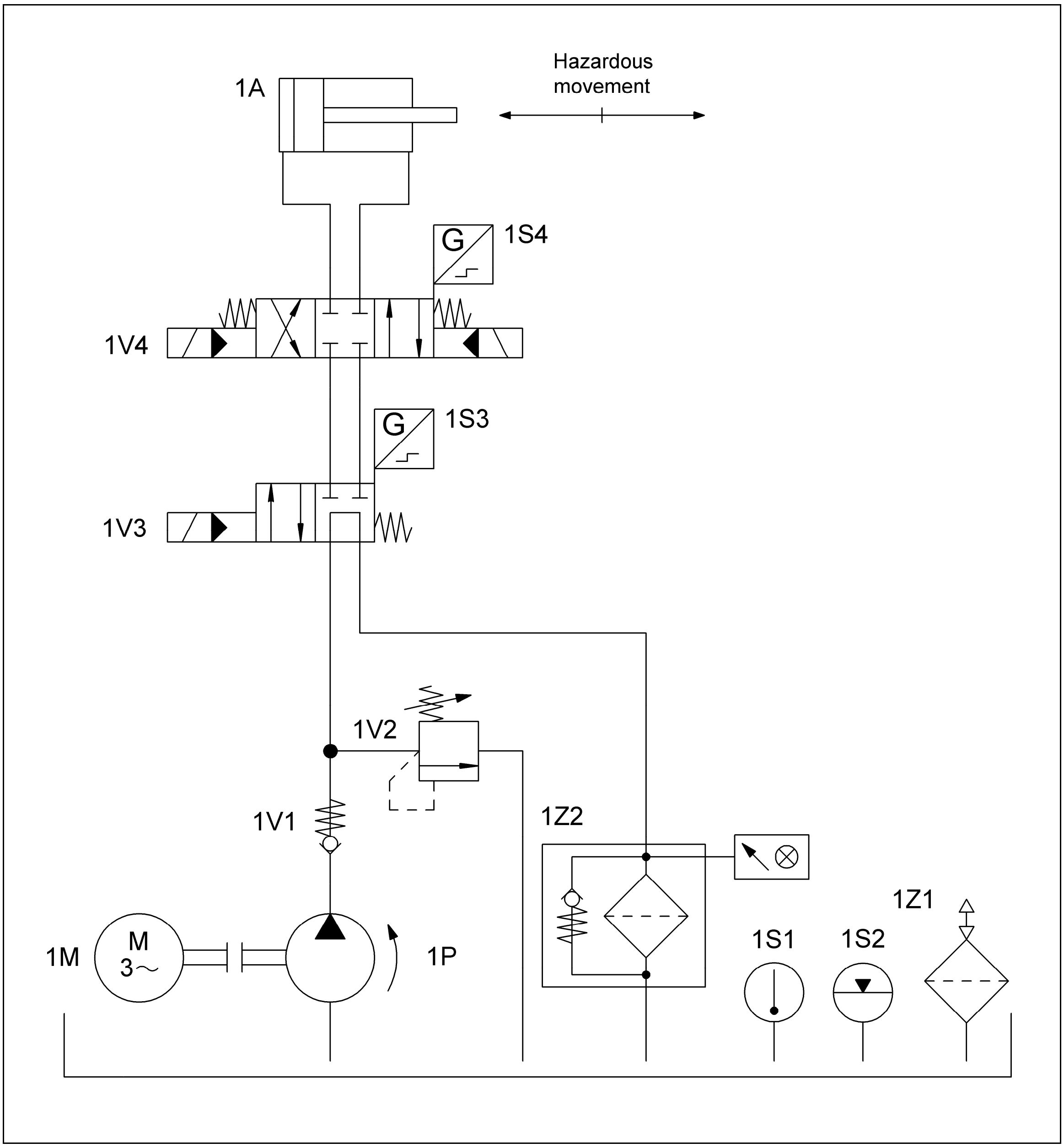
Calculation of the probability of failure

The valve combination 1V1 comprises two valve channels each with three interconnected valves. The valves are denoted on the block diagram as 2V1, 2V2 and 2V3 and 3V1, 3V2 and 3V3.

- $MTTF_d$: a B_{10d} value of 20,000,000 cycles [S] is assumed for each valve in the valve combination 1V1. At 240 working days, 16 working hours and a cycle time of 10 seconds, n_{op} is 1,382,400 cycles per year and the $MTTF_d$ is 144 years. This results in an MTTF_d value per channel of 48 years (“high”).
- DC_{avg}: a *DC* of 99% for 1V1 is produced by mechanical linking of the two valve channels with simultaneous internal cross-checking of the control pressure. The DC_{avg} is thus also 99% (“high”).
- Adequate measures against common cause failure (65 points): separation (15), overvoltage protection etc. (15) and environmental conditions (25 + 10)
- The combination of the pneumatic control elements corresponds to Category 4 with a high $MTTF_d$ (48 years) and a high DC_{avg} (99%). This results in an average probability of dangerous failure of 5.60×10^{-8} per hour. This corresponds to PL e. Following the addition of further safety-related control components in the form of subsystems for completion of the safety function, the PL may under certain circumstances be lower.
- Estimation erring on the safe side as described above results in a T_{10d} value of 14 years for the specified replacement of the valve combination 1V1, which is subject to wear.

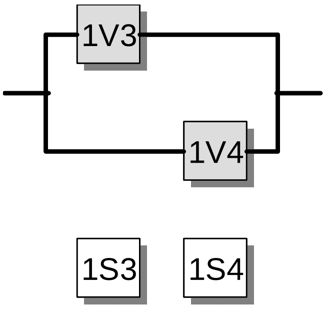
8.2.32 Hydraulic valve control (subsystem) – Category 4 – PL e (Example 32)

Figure 8.54:
Tested hydraulic valves for redundant control of hazardous movements



Safety functions

- Safety-related stop function: stopping of the hazardous movement and prevention of unexpected start-up from the rest position
- Only the hydraulic part of the control is shown here, in the form of a subsystem. Further safety-related control components (e.g. protective devices and electrical logic elements) must be added in the form of subsystems for completion of the safety function.



Functional description

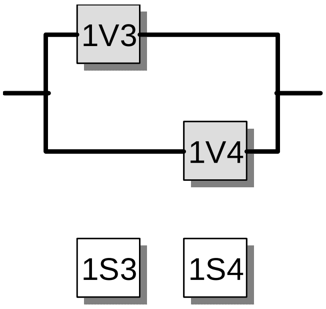
- Hazardous movements are controlled by two directional control valves (1V3 and 1V4).
- Failure of one of the two valves alone does not result in loss of the safety function.
- The two directional control valves are actuated cyclically.
- Both directional control valves are equipped with direct position monitors (1S3 and 1S4). Failure of either of the two directional control valves is detected; following a fault, initiation of the next hazardous movement is prevented.

Design features

- Basic and well-tried safety principles are observed and the requirements of Category B are met.
- Directional control valves 1V3 and 1V4 possess a closed centre position with sufficient overlap, spring-centering/return, and electrical position monitoring.
- The safety-oriented switching position is assumed from any position by removal of the control signal.
- Signal processing by the electrical position monitor satisfies the relevant requirements for the control of failures.

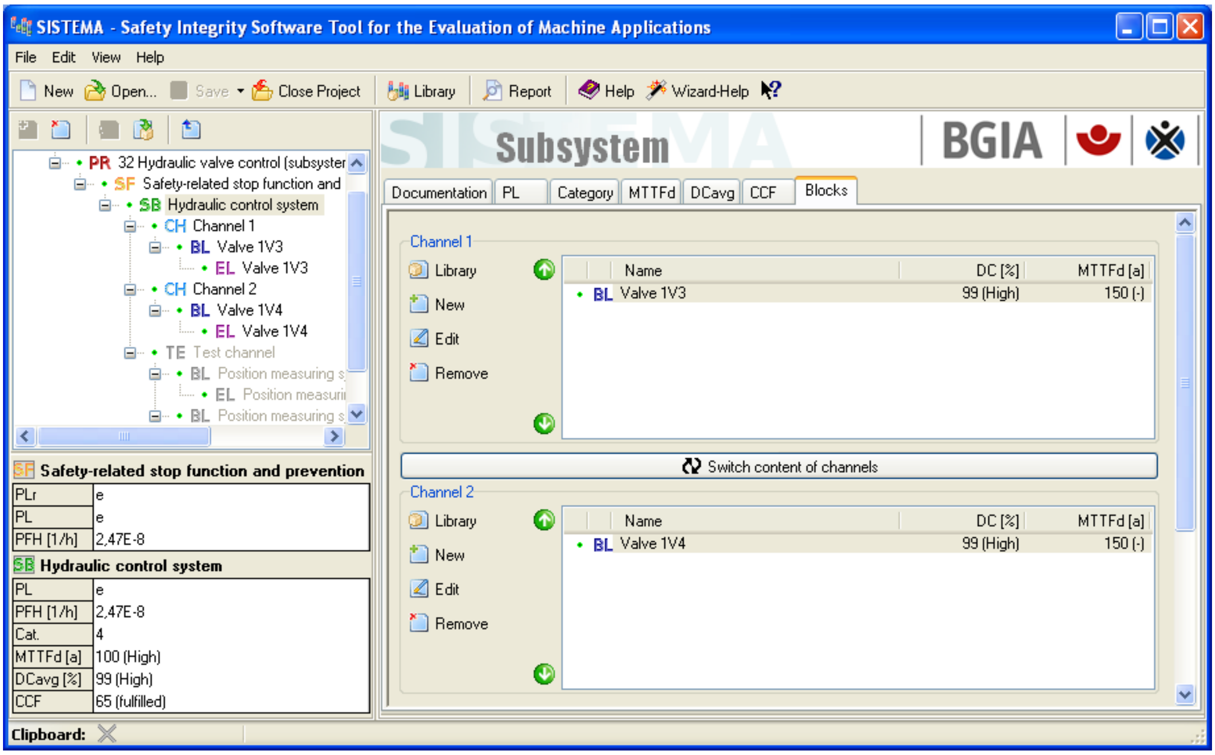
Calculation of the probability of failure

- $MTTF_d$: an $MTTF_d$ of 150 years is assumed for the directional control valves 1V3 and 1V4 [S]. This is also the $\mathrm{MTTF_d}$ value per channel, which is capped to 100 years (“high”).
- DC_{avg}: the *DC* of 99% for the directional control valves 1V3 and 1V4 is based upon direct monitoring of the switching states. Averaging thus also produces a DC_{avg} of 99% (“high”).
- Adequate measures against common cause failure (65 points): separation (15), overvoltage protection etc. (15) and environmental conditions (25 + 10)
- The combination of the hydraulic control elements corresponds to Category 4 with a high $MTTF_d$ (100 years) and high DC_{avg} (99%). This results in an average



probability of dangerous failure of 2.47 × 10^{-8} per hour. This corresponds to PL e. The addition of further safety-related control parts as subsystems for completion of the safety function generally results in a lower PL.

Figure 8.55:
Determining of the PL by means of SISTEMA


SISTEMA - Safety Integrity Software Tool for the Evaluation of Machine Applications
File Edit View Help
New Open... Save Close Project Library Report Help Wizard-Help
Subsystem
BGIA
Documentation PL Category MTTFd DCavg CCF Blocks
Library
New
Edit
Remove
Switch content of channels
Clipboard:

- PR 32 Hydraulic valve control (subsyster
  - SF Safety-related stop function and
    - SB Hydraulic control system
      - CH Channel 1
        - BL Valve 1V3
          - EL Valve 1V3
      - CH Channel 2
        - BL Valve 1V4
          - EL Valve 1V4
      - TE Test channel
        - BL Position measuring s
          - EL Position measurii
        - BL Position measuring s

SF Safety-related stop function and prevention

PLr	e
PL	e
PFH [1/h]	2,47E-8

SB Hydraulic control system

PL	e
PFH [1/h]	2,47E-8
Cat.	4
MTTFd [a]	100 (High)
DCavg [%]	99 (High)
CCF	65 (fulfilled)

Channel 1

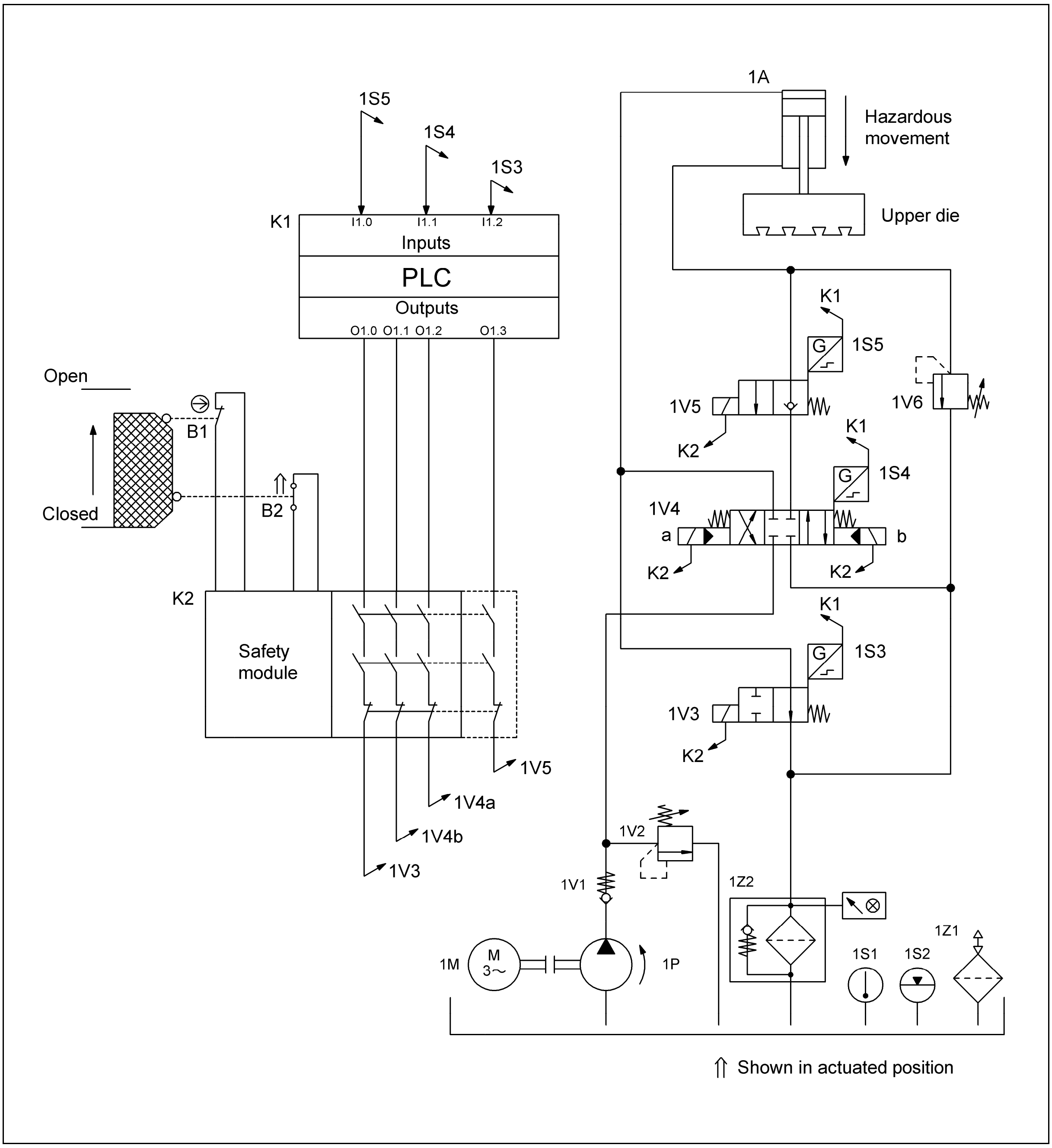
Name	DC [%]	MTTFd [a]
BL Valve 1V3	99 (High)	150 (-)

Channel 2

Name	DC [%]	MTTFd [a]
BL Valve 1V4	99 (High)	150 (-)

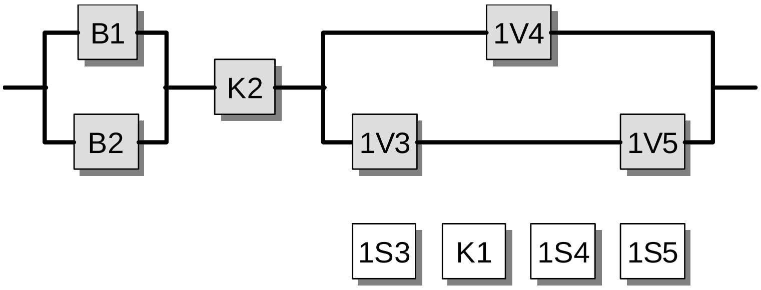
8.2.33 Electrohydraulic press control – Category 4 – PL e (Example 33)

Figure 8.56:
Press control, electrical monitoring of a moveable guard with hydraulic stopping of the hazardous movement



Safety function

- Safety-related stop function, initiated by a protective device: stopping of the hazardous movement

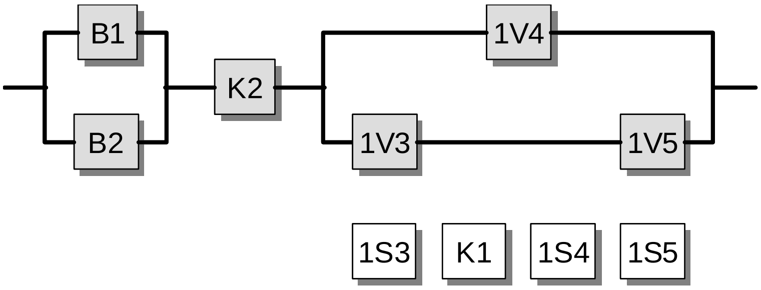


Functional description

- The hazardous area is safeguarded by means of a moveable guard, the position of which is detected by two position switches B1 and B2 in the form of a break contact/make contact combination. The signals are read into a standard safety module K2 which is looped into the enabling path for the electrical pilot control K1 (a conventional PLC) for the hydraulic actuators. Hazardous movements or states are controlled by three directional control valves (1V3, 1V4 and 1V5) on the actuator side.
- In response to a demand upon the safety function, all valves are de-energized by K2, and are placed by their return springs in the closed centre position (1V4) or closed position (1V3 and 1V5). The oil return from the lower piston side of the cylinder to the reservoir is interrupted by 1V4 and 1V5 at the same time. 1V5 is a poppet valve which is designed to shut off the volumetric flow without leakage. Valve 1V4, which also controls the direction of movement of the cylinder, is a piston-type directional control valve which also exhibits a certain degree of leakage in the closed centre position. Although 1V3 is only indirectly involved in the stop function, it can influence the safety function dangerously. Should 1V3 and 1V4 get stuck at the same time, there would be pressure on the upper side of the cylinder while the lower side is shut off by 1V5. Due to the pressure translation in the cylinder the pressure-relief valve 1V6 would open and the upper die descend.
- Failure of one of the valves does not result in loss of the safety function. All valves are actuated cyclically.
- Each valve is equipped with a position monitoring, 1S3, 1S4 and 1S5, for fault detection purposes. Failure of either of the valves is detected in the conventional PLC K1, which prevents initiation of the next hazardous movement following a fault.
- A single fault in one safety component does not result in loss of the safety function. In addition, single faults are detected at or prior to the next demand. An accumulation of undetected faults does not result in loss of the safety function.

Design features

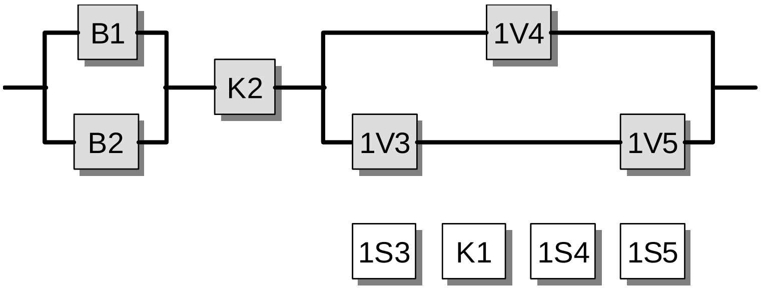
- Basic and well-tried safety principles and the requirements of Category B are observed. Protective circuits (e.g. contact protection) as described in the initial paragraphs of Chapter 8 are implemented.



- A stable arrangement of the protective device is assured for actuation of the position switch.
- Switch B1 is a position switch with a direct opening contact in accordance with IEC 60947-5-1, Annex K.
- The safety module K2 satisfies all requirements for Category 4 and PL e.
- The supply conductors to the position switches are laid separately or with protection.
- A standard PLC without safety functions is employed for K1.
- The valves 1V3, 1V4 and 1V5 possess a closed centre position and closed position respectively with sufficient overlap, spring-centering/return and position monitoring.
- The safety-oriented switching position is assumed from any position by removal of the control signal.
- The pressure-relief valve 1V6 to protect the cylinder 1A and the components below against “pressure intensifier effect” fulfils the requirements of EN 693:2001, cl. 5.2.4.4.

Calculation of the probability of failure

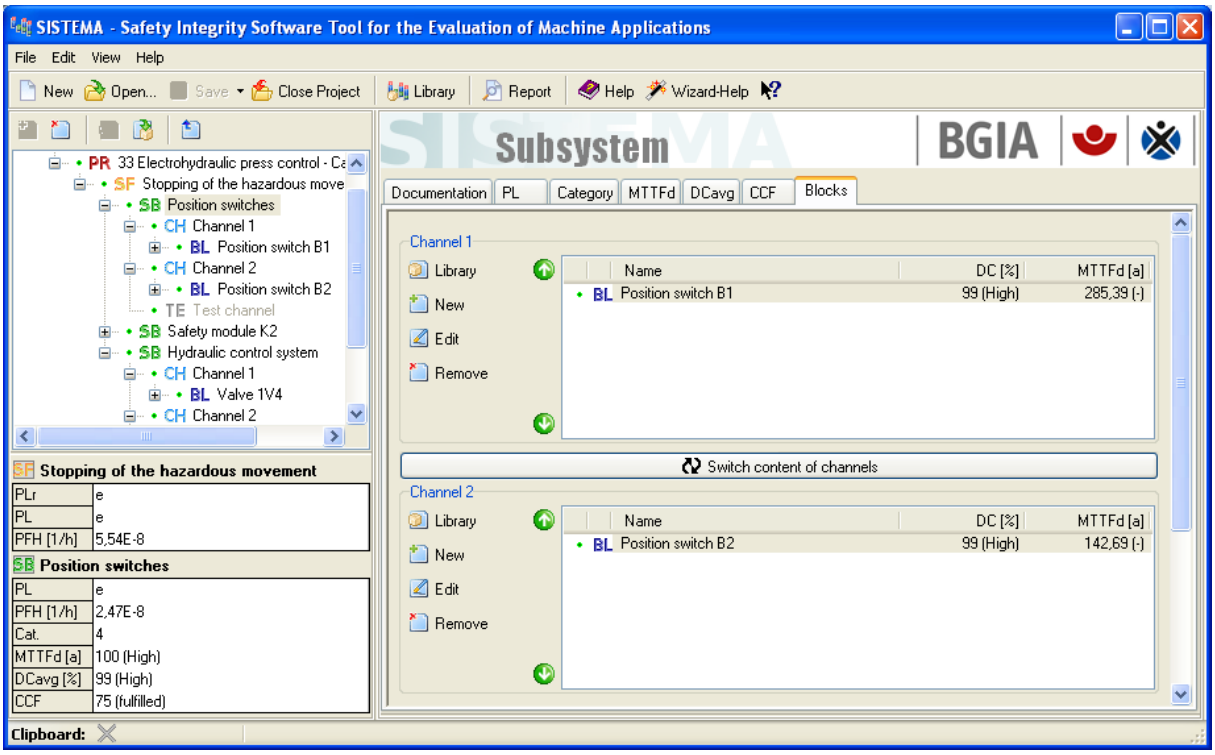
- K2 is considered as a subsystem with a probability of failure of 2.31 × 10^{-9} per hour [M]. The remainder of the control system is grouped separately by electromechanical and hydraulic components to form two Category 4 subsystems, the probability of failure of which is calculated below.
- $MTTF_d$: fault exclusion is possible for the electrical contact of the position switch B1 with direct opening action. For the electrical make contact of the position switch B2, the B_{10d} is 1,000,000 switching operations [M]. A B_{10d} value of 1,000,000 cycles [M] is stated for the mechanical part of B1 and B2. At 365 working days, 16 working hours per day and a cycle time of 10 minutes, n_{op} is 35,040 cycles per year for these components, and the $MTTF_d$ is 285 years for B1 and 142 years for B2. An $MTTF_d$ of 150 years [S] is assumed for each of the valves 1V3, 1V4 and 1V5. This results in $\mathrm{MTTF_d}$ values per channel of 100 or 88 years (“high”) for the two subsystems.
- DC_{avg}: the DC of 99% for B1 and B2 is based upon the plausibility monitoring of the two switching states in K2. The DC of 99% for the valves is based upon direct monitoring of the switching states by the PLC K1. This results in a DC_{avg} of 99% (“high”) for the two subsystems.



- Measures against common cause failures (75 points) for the two subsystems: separation (15), well-tried components (5), FMEA (5), protection against overvoltage etc. (15) and environmental conditions (25 + 10)

- The electromechanical and the hydraulic parts of the control system correspond to Category 4 with a high *MTTF*$_d$ per channel (100 or 88 years) and a high *DC*$_{avg}$ (99%). This results in an average probability of dangerous failure of 2.47 x 10^{-8} per hour and 2.84 x 10^{-8} per hour for each subsystem. Addition inclusive of K2 produces an average probability of dangerous failure for the complete safety function of 5.54 × 10^{-8} per hour. This corresponds to PL e.

Figure 8.57:
Determining of the PL by means of SISTEMA



PR 33 Electrohydraulic press control - Ca
SF Stopping of the hazardous move
SB Position switches
CH Channel 1
BL Position switch B1
CH Channel 2
BL Position switch B2
TE Test channel
SB Safety module K2
SB Hydraulic control system
CH Channel 1
BL Valve 1V4
CH Channel 2

SF Stopping of the hazardous movement

PLr	e
PL	e
PFH [1/h]	5,54E-8

SB Position switches

PL	e
PFH [1/h]	2,47E-8
Cat.	4
MTTFd [a]	100 (High)
DCavg [%]	99 (High)
CCF	75 (fulfilled)

Channel 1

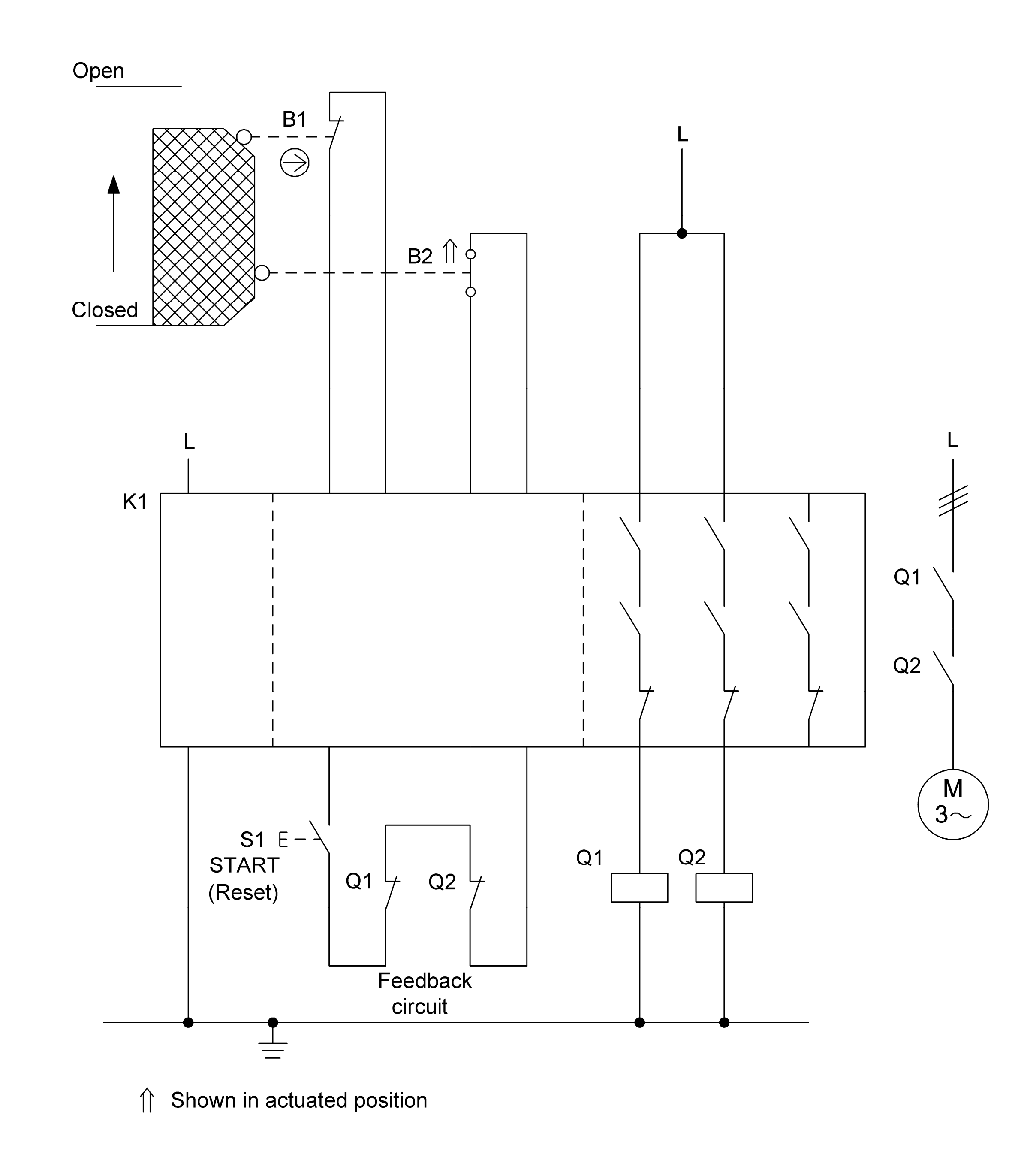
	Name	DC [%]	MTTFd [a]
BL	Position switch B1	99 (High)	285,39 (-)

Channel 2

	Name	DC [%]	MTTFd [a]
BL	Position switch B2	99 (High)	142,69 (-)

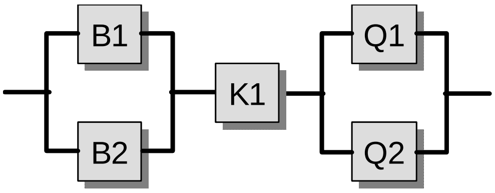
8.2.34 Position monitoring of moveable guards – Category 4 – PL e (Example 34)

Figure 8.58:
Position monitoring of moveable guards by means of a safety module



Safety function

- Safety-related stop function, initiated by a protective device: opening of the moveable guard (safety guard) initiates the safety function STO (safe torque off).



Functional description

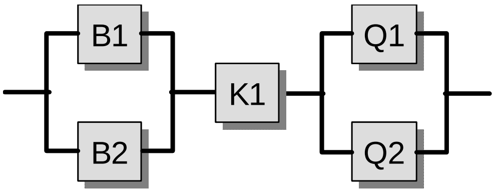
- A hazardous zone is safeguarded by a moveable guard (safety guard). Opening of the safety guard is detected by two position switches B1/B2, employing a break contact/make contact combination, and evaluation by a central safety module K1. K1 actuates two contactors, Q1 and Q2, dropping out of which interrupts or prevents hazardous movements or states.
- The position switches are monitored for plausibility in K1 for the purpose of fault detection. Faults in Q1 and Q2 are detected by a start-up test in K1. A start command is successful only if Q1 and Q2 had previously dropped out. Start-up testing by opening and closing of the protective device is not required.
- The safety function remains intact in the event of a component failure. Faults are detected during operation or at actuation (opening and closing) of the protective device by the dropping out of Q1 and Q2 and operating inhibition.
- An accumulation of more than two faults in the period between two successive actuations may lead to loss of the safety function.

Design features

- Basic and well-tried safety principles are observed and the requirements of Category B are met. Protective circuits (e.g. contact protection) as described in the initial paragraphs of Chapter 8 are implemented.
- A stable arrangement of the protective devices is assured for actuation of the position switches.
- Switch B1 is a position switch with direct opening contact in accordance with IEC 60947-5-1, Annex K.
- The supply conductors to position switches B1 and B2 are laid separately or with protection.
- The safety module K1 satisfies all requirements for Category 4 and PL e.
- The contactors Q1 and Q2 possess mechanically linked contact elements to IEC 60947-5-1, Annex L.

Remark

- Category 4 is observed only if multiple mechanical position switches for different protective devices are not connected in a series arrangement (i.e. no cascading), since faults in the switches cannot otherwise be detected.

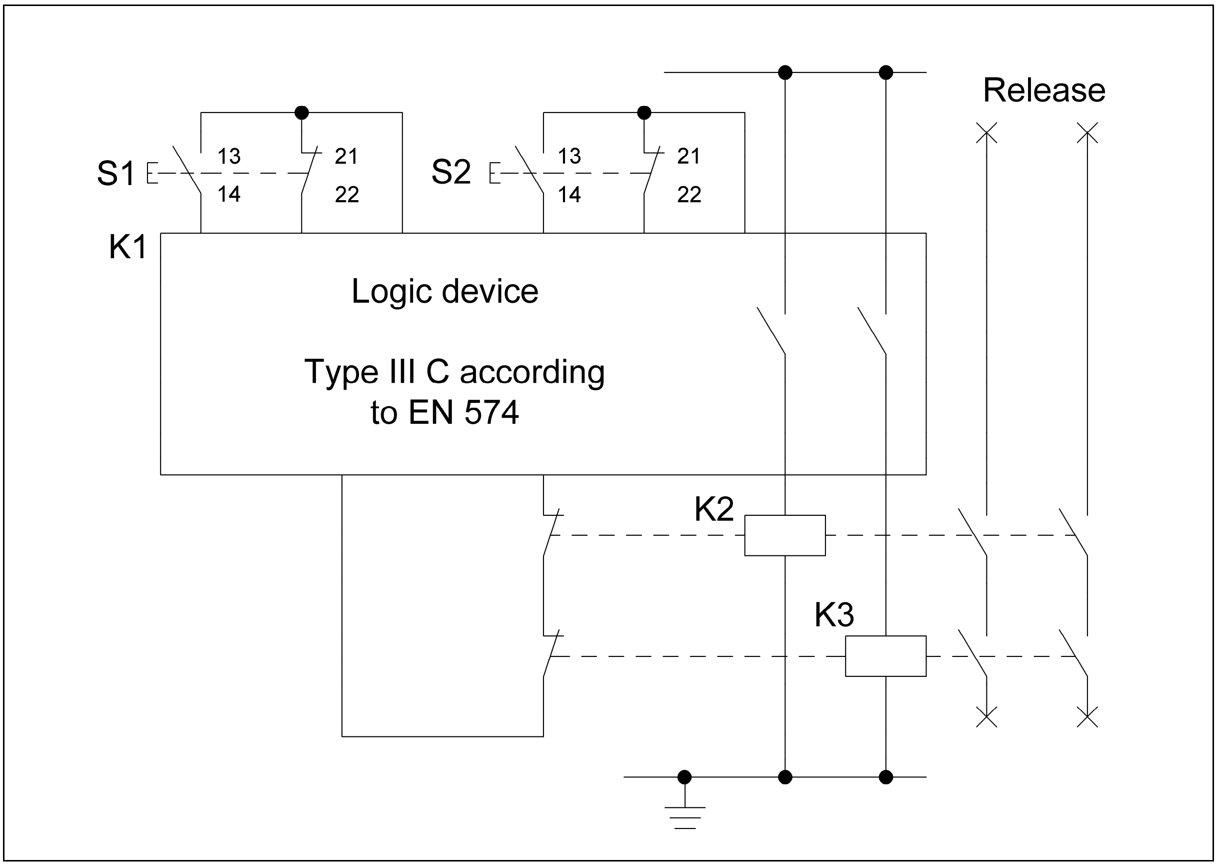


Calculation of the probability of failure

- The circuit arrangement can be divided into three subsystems as shown in the safety-related block diagram. The probability of failure of the standard safety module K1 is added at the end of the calculation (2.31 × 10^{-9} per hour [M], suitable for PL e). For the remaining subsystems, the probability of failure is calculated as follows.
- $MTTF_d$: fault exclusion is possible for the electrical contact of the position switch B1 with direct opening action. For the electrical make contact of the position switch B2, the B_{10d} value is 1,000,000 switching operations [M]. A B_{10d} value of 1,000,000 cycles [M] is stated for the mechanical part of B1 and B2. At 365 working days, 16 working hours per day and a cycle time of 1 hour, n_{op} is 5,840 cycles per year for these components, and the $MTTF_d$ is 1,712 years for B1 and 856 years for B2. For the contactors Q1 and Q2, the B_{10} value corresponds under inductive load (AC 3) to an electrical lifetime of 1,000,000 switching operations [M]. If 50% of failures are assumed to be dangerous, the B_{10d} value is produced by doubling of the B_{10} value. The value assumed above for n_{op} results in an $MTTF_d$ of 3,424 years per channel for Q1 and Q2. Altogether, the symmetrized $\mathrm{MTTF_d}$ value per channel in the two subsystems is 100 years ("high").
- DC_{avg}: the DC of 99% for B1 and B2 is based upon plausibility monitoring of the break/make contact combination in K1. The DC of 99% for contactors Q1 and Q2 is derived from regular monitoring by K1 during start-up. The DC values stated correspond to the DC_{avg} for each subsystem.
- Adequate measures against common cause failure in the subsystems B1/B2 and Q1/Q2 (70 points): separation (15), well-tried components (5), protection against overvoltage etc. (15) and environmental conditions (25 + 10)
- The subsystems B1/B2 and Q1/Q2 each correspond to Category 4 with a high $MTTF_d$ (100 years) and high DC_{avg} (99%). This results in an average probability of dangerous failure of 2.47 × 10^{-8} per hour. Following addition of the subsystem K1, the average probability of dangerous failure is 5.16 × 10^{-8} per hour. This corresponds to PL e.

8.2.35 Two-hand control – Category 4 – PL e (Example 35)

Figure 8.59:
Two-hand control, signal processing by a logic device with downstream contactor relays

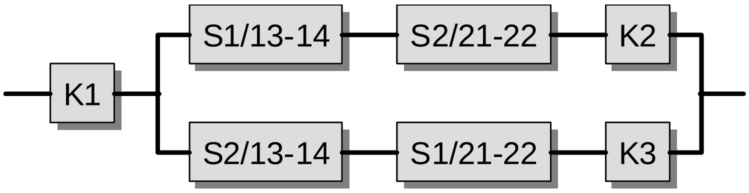


Safety function

- Controlled location of the operator's hands outside the hazardous area during a hazardous movement: when at least one of the two pushbuttons S1/S2 is released, enabling is cancelled and remains blocked until both pushbuttons are released and pressed again synchronously.

Functional description

- The logic device K1 monitors operation of the actuators (pushbuttons) S1 and S2. Only when both pushbuttons are operated synchronously (i.e. within a specified time) from the released state do the contactor relays K2 and K3 pick up and cause enabling. When at least one of the pushbuttons S1/S2 is released, K2/K3 cancel enabling.
- K2 and K3 have the function of contact multiplication/load adaptation. The actual prevention of the hazardous movement, for example by separation of the electrical or hydraulic energy, is dependent upon the application and is not shown here.



- Faults in the actuating mechanism are detected in S1/S2 to the greatest extent possible by the use of two contacts employing different principles (break and make contact combination). With regard to mechanical faults for this application, a fault exclusion is possible for failure of the break contact to open, provided the pushbuttons satisfy IEC 60947-5-1.
- Faults in S1/S2 and in K2/K3 (with break contacts in the feedback circuit) are detected in K1 and lead to sustained de-energization via K2 and K3. All individual faults are detected at or prior to the next demand upon the safety function.
- Frequent actuation of the electromechanical elements results in a sufficiently high test rate (forced dynamics).

Design features

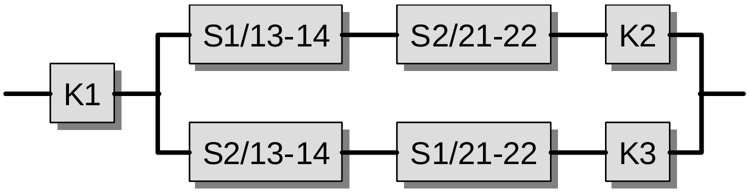
- Basic and well-tried safety principles are observed and the requirements of Category B are met. Protective circuits (e.g. contact protection) as described in Section 8.1 are implemented.
- The actuators S1 and S2 of the two-hand control satisfy IEC 60947-5-1.
- Faults in the conductors to S1 and S2 are detected in the logic device. If this were not possible, the conditions to EN ISO 13849-2, Table D.4 for a fault exclusion for conductor short-circuits would have to be observed. Owing to the low currents, pushbuttons with gold-plated contacts are recommended.
- Refer to EN 574 Section 8 with regard to fitting of the pushbuttons and to measures for the avoidance of accidental actuation and manipulation. The distance from the hazardous area must be sufficiently large.
- The logic device K1 corresponds to Type III C in accordance with EN 574, with self-monitoring and detection of internal faults. K1 is a tested safety component for use in Category 4 and PL e.
- K2 and K3 possess mechanically linked break contacts for readback.

Remark

- Application for example on mechanical presses (EN 692)

Calculation of the probability of failure

- K1 is treated as a subsystem with a probability of failure of 2.47 × 10^{-8} per hour [E]. The remaining part of the control system is grouped to form a Category 4 subsystem the probability of failure of which is calculated below.
- Since S1 and S2 must trigger de-energization independently of each other when released, they are connected logically in series. For this purpose, one



make contact 13-14 and one break contact 21-22 for each pushbutton were assigned to a control channel. The safety-related block diagram differs substantially in this respect from the functional circuit diagram. If the reliability data is available only for the pushbuttons as a whole (actuation mechanism and break and make contacts), the failure values for the pushbuttons may be employed as the failure values for the contacts (plus operating mechanism), constituting an estimation erring on the safe side.

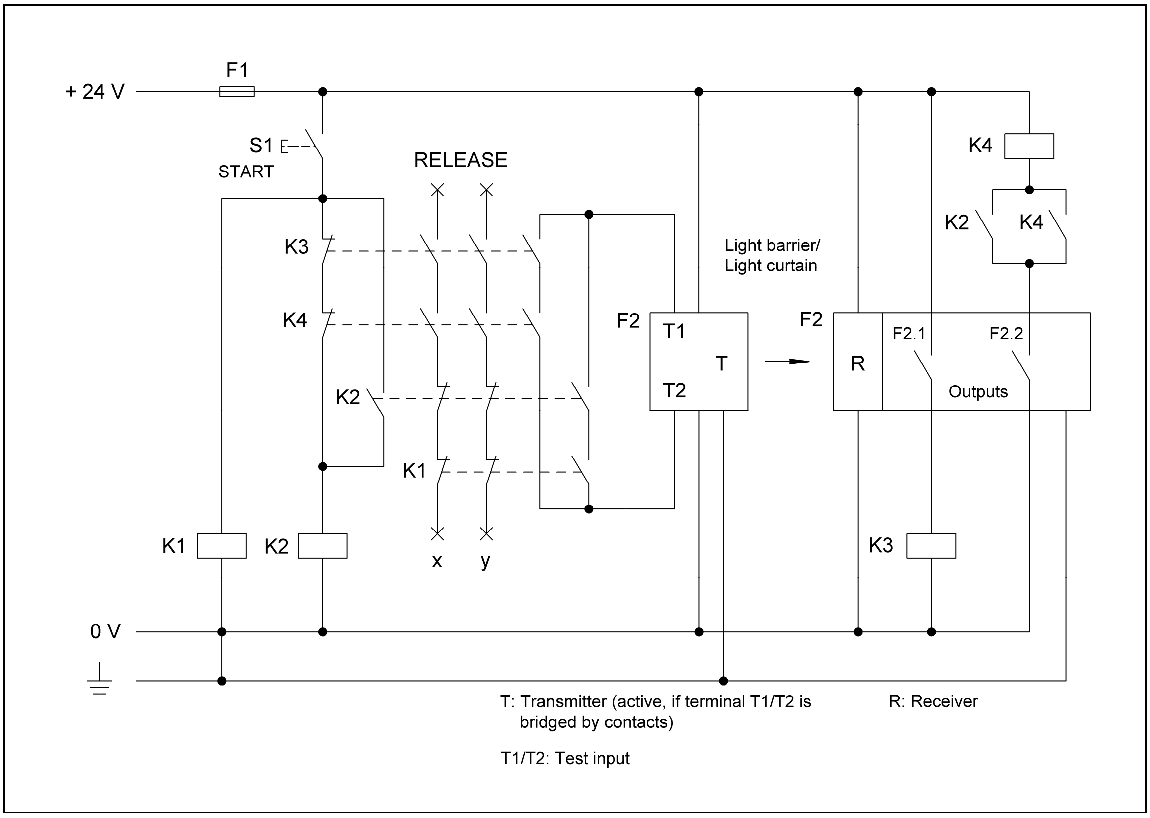
- *$MTTF_d$*: owing to the defined control current generated by K1 (small load, the mechanical lifetime of the contacts is the determining factor), B_{10d} values of 20,000,000 switching operations [M] are assumed in each case for S1 and S2. Since K2 and K3 also switch control currents, B_{10d} values of 20,000,000 cycles [S] apply to each of them. At 240 working days, 8 working hours and a cycle time of 20 seconds, n_{op} is 345,600 cycles per year for these components and the *$MTTF_d$* is 579 years. Should the requirements be higher (longer working hours or a shorter cycle time), higher B_{10d} values validated by the manufacturer may be required for K2/K3. Overall, the resulting MTTF_d value per channel is 193 years, capped to 100 years (“high”).
- *DC_{avg}*: a *DC* of 99% for S1 and S2 is produced by virtue of direct monitoring with the aid of the break and make contact combinations in K1. The *DC* of 99% for K2 and K3 is based upon readback of the mechanically linked break contacts in the feedback circuit of K1. The high frequency of actuation in the application constitutes effective testing. Averaging results in a *DC_{avg}* of 99% (“high”).
- Adequate measures against common cause failure (70 points): separation (15), FMEA (15), overvoltage protection etc. (15) and environmental conditions (25 + 10)
- The combination of the control elements corresponds to Category 4 with a high *$MTTF_d$* per channel (100 years) and high *DC_{avg}* (99%). For the combination of S1, S2, K2 and K3, the average probability of dangerous failure is calculated at 2.47×10^{-8} per hour. If a value of 2.47×10^{-8} per hour [E] for K1 is added, the result is an average probability of dangerous failure of 4.94×10^{-8} per hour. This corresponds to PL e. The probability of failure of downstream power components may have to be added for completion of the safety function.

More detailed references

- EN 574: Safety of machinery – Two-hand control devices – Functional aspects – principles for design (11.96)
- Recommendation for Use. Ed.: Vertical Group 11 (VG 11) in the Co-ordination of Notified Bodies. CNB/M/11.033/R/E Rev 05, p. 252, April 2006. http://europa.eu/comm/enterprise/mechan_equipment/machinery/vertical_rfu.pdf

8.2.36 Processing of signals from a light barrier – Category 4 – PL e (Example 36)

Figure 8.60:
Electromechanical input of safety-related signals into the machine control system with reference to the example of a light barrier or light curtain



T: Transmitter (active, if terminal T1/T2 is bridged by contacts)

R: Receiver

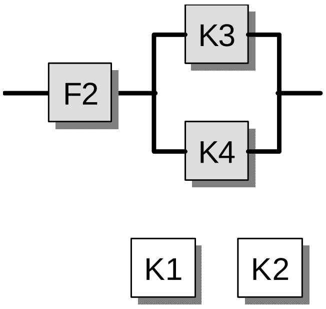
T1/T2: Test input

Safety function

- Safety-related stop function initiated by a protective device: sustained stopping of a hazardous movement in response to entry into a hazardous area or operator intervention at a hazardous zone, and start and restart interlock

Functional description

- Entry into a hazardous area or operator intervention at a hazardous zone is detected by the light barrier F2. The safety-related output signals from the light barrier (make contacts F2.1 and F2.2) de-energize the contactor relays K3 and K4, the coils of which are connected to the power supply in an offset arrangement. K3 and K4 then block the enabling signals x and y.
- For activation of the light barrier transmitter, actuation of the start button S1 first causes the test inputs T1 and T2 to be connected together by picking up of the contactor relays K1 and K2. K2 can pick up and latch in only once the contactor relays K3/K4 have dropped out. With the light path completed, K3 and K4 then pick up. K4 picks up and latches in only by means of the make contact of K2. With K3 and K4 picked up and the start button still depressed, the light barrier

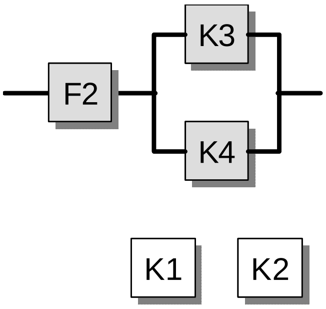


transmitter is activated and latched; the start button can therefore be released, and once K1 and K2 have dropped out, the enabling paths x and y are also closed. Following interruption of the light beam or in the event of breakdown and subsequent restoration of the voltage, the function of the start/restarting interlock prevents a valid enabling signal until K3 and K4 have picked up again following renewed pressing of the start button.

- One make contact each on K3 and K4 is integrated both into the two enabling paths and into the input circuit for activation of the light barrier transmitter (test inputs T1/T2). Connection of the test inputs generates an internal start-up test within the device, for example by blanking of the light beam for a short defined period. On the receiver side, this test is logically evaluated as valid only within a narrow time window. Provided the start-up test is passed, the light barrier outputs are enabled. Conversely, in the event of an outage or fault, or interruption of the light beam, they are blocked.
- Faults in other components in the circuit (contactor relays, output contacts of the light barrier, start button) which in combination could result in the loss of a safety function are detected during the start-up/restarting test following an interruption of the light beam, and prevent renewed enabling.

Design features

- Basic and well-tried safety principles are observed and the requirements of Category B are met. Protective circuits (e.g. contact protection) as described in the initial paragraphs of Chapter 8 are implemented.
- The contactor relays K1 to K4 possess mechanically linked contact elements in accordance with IEC 60947-5-1, Annex L. The relay operating voltage of the contactor relays K3 and K4 must be greater than half the value of the power supply, so that simultaneous pick-up of K3 and K4 in the event of a short-circuit in the cable (connection in series results in the voltage being divided between the contactor coils) does not present a hazard, even in combination with other faults.
- The output signals from the light barrier F2 are routed in a cable, together with the supply conductors, from the electrical compartment of the receiver to the electrical compartment of the machine control system. Owing to application of the closed-circuit current principle and the principle of offset coils (K3, K4) in the earthed control circuit, all open circuits, earth faults and circuit-to-circuit shorts are detected immediately when the light barrier is in the activated state (among other things, by tripping of the fuse F1). A short-circuit which causes a single



output to be bridged is detected at the latest at the next interruption of the light barrier when the start button is subsequently actuated. Common routing of the output signals within a single cable is therefore permissible.

- The light barrier satisfies the requirements for Type 4 in accordance with EN 61496-1 and IEC 61496-2, and PL e.

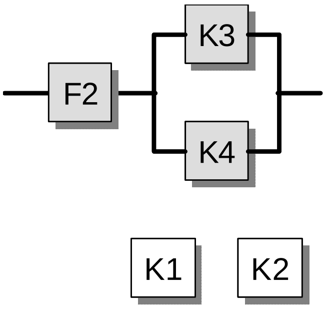
Remarks

- If the circuit is employed in applications in which the light barrier switches very infrequently, the possibility must be considered of the safety function being lost as a result of an accumulation of faults (two discrete undetected faults). Such loss may be countered by periodic testing.
- The manufacturer's information concerning the maximum switching frequency of the light barrier must be observed.

Calculation of the probability of failure

The probability of failure of the safety-related stop function, which is also shown on the safety-related block diagram, is calculated. If the contacts of the enabling paths x and y are processed further by the control system, the additional control components concerned, e.g. contactors, must be considered in the calculation of the probability of failure.

- The light barrier F2 is a standard safety component. The probability of failure of 3.0×10^{-8} per hour [E] is added at the end of the calculation.
- $MTTF_d$: owing to the unknown loads, the B_{10d} value for K3 and K4 is 400,000 cycles [S]. At 220 working days, 8 working hours per day and a cycle time of 120 seconds, n_{op} is 52,800 switching operations per year, and the $MTTF_d$ is thus 75 years. This is also the MTTF_d value of each channel (“high”).
- DC_{avg}: the *DC* of 99% for K3 to K4 is derived from incorporation of the mechanically linked break contacts into the actuation circuit of K2. This also corresponds to the DC_{avg} (“high”).
- Adequate measures against common cause failure (75 points): separation (15), well-tried components (5), FMEA (5), overvoltage protection etc. (15) and environmental conditions (25 + 10)
- The K3/K4 subsystem corresponds to Category 4 with a high $MTTF_d$ per channel (75 years) and high DC_{avg} (99%). This results in an average probability of dangerous failure of 3.37×10^{-8} per hour. The overall probability of failure is



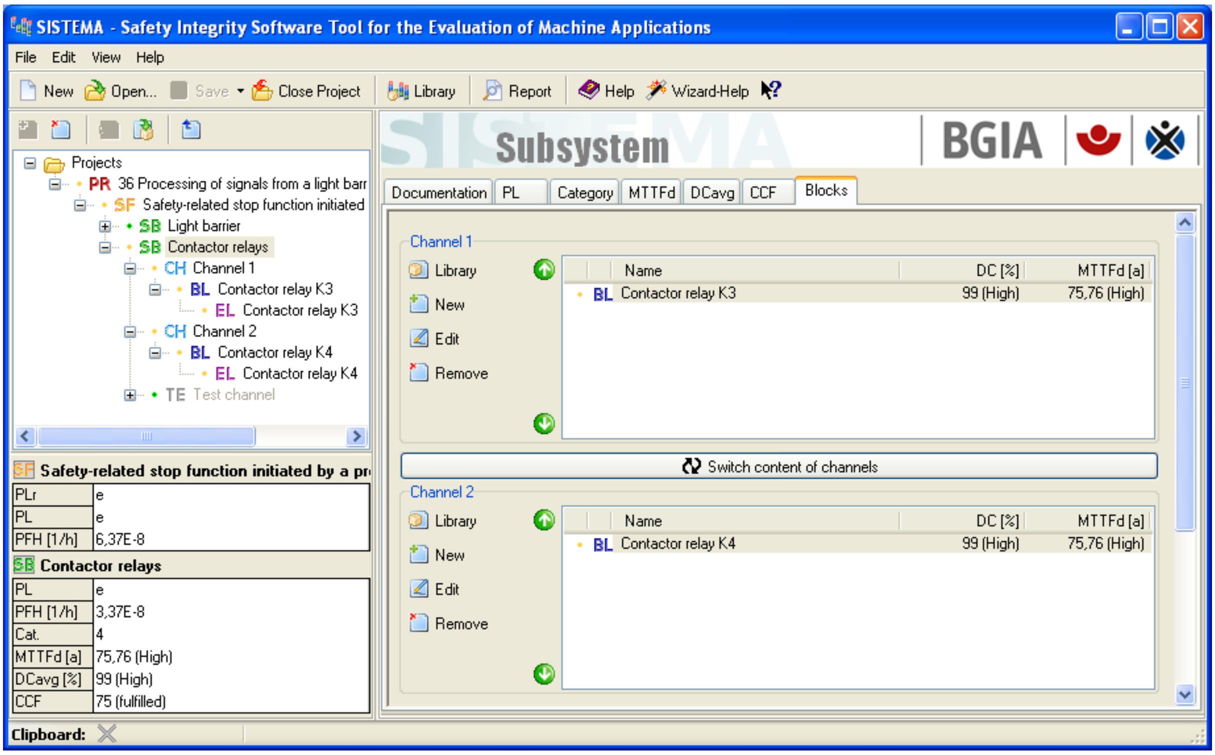
determined by addition of the probability of dangerous failure of F2 (3.0 × 10^{-8} per hour) and is equal to 6.37 × 10^{-8} per hour. This corresponds to PL e. The probability of failure of downstream power components may have to be added for completion of the safety function.

- The wearing elements K3 and K4 should be replaced at intervals of approximately seven years (T_{10d}).

More detailed reference

- EN 60204-1: Safety of machinery – Electrical equipment of machines – Part 1: General requirements (IEC 60204-1:2005, modified) (06.06). Section 9.4.3: “Protection against maloperation due to earth faults, voltage interruptions and loss of circuit continuity”

Figure 8.61:
Determining of the PL by means of SISTEMA


SISTEMA - Safety Integrity Software Tool for the Evaluation of Machine Applications
File Edit View Help
New Open... Save Close Project Library Report Help Wizard-Help
Subsystem
BGIA
Documentation PL Category MTTFd DCavg CCF Blocks
Projects
PR 36 Processing of signals from a light barr
SF Safety-related stop function initiated
SB Light barrier
SB Contactor relays
CH Channel 1
BL Contactor relay K3
EL Contactor relay K3
CH Channel 2
BL Contactor relay K4
EL Contactor relay K4
TE Test channel
Library
New
Edit
Remove
Switch content of channels
Clipboard:

SF Safety-related stop function initiated by a pr

PLr	e
PL	e
PFH [1/h]	6,37E-8

SB Contactor relays

PL	e
PFH [1/h]	3,37E-8
Cat.	4
MTTFd [a]	75,76 (High)
DCavg [%]	99 (High)
CCF	75 (fulfilled)

Channel 1

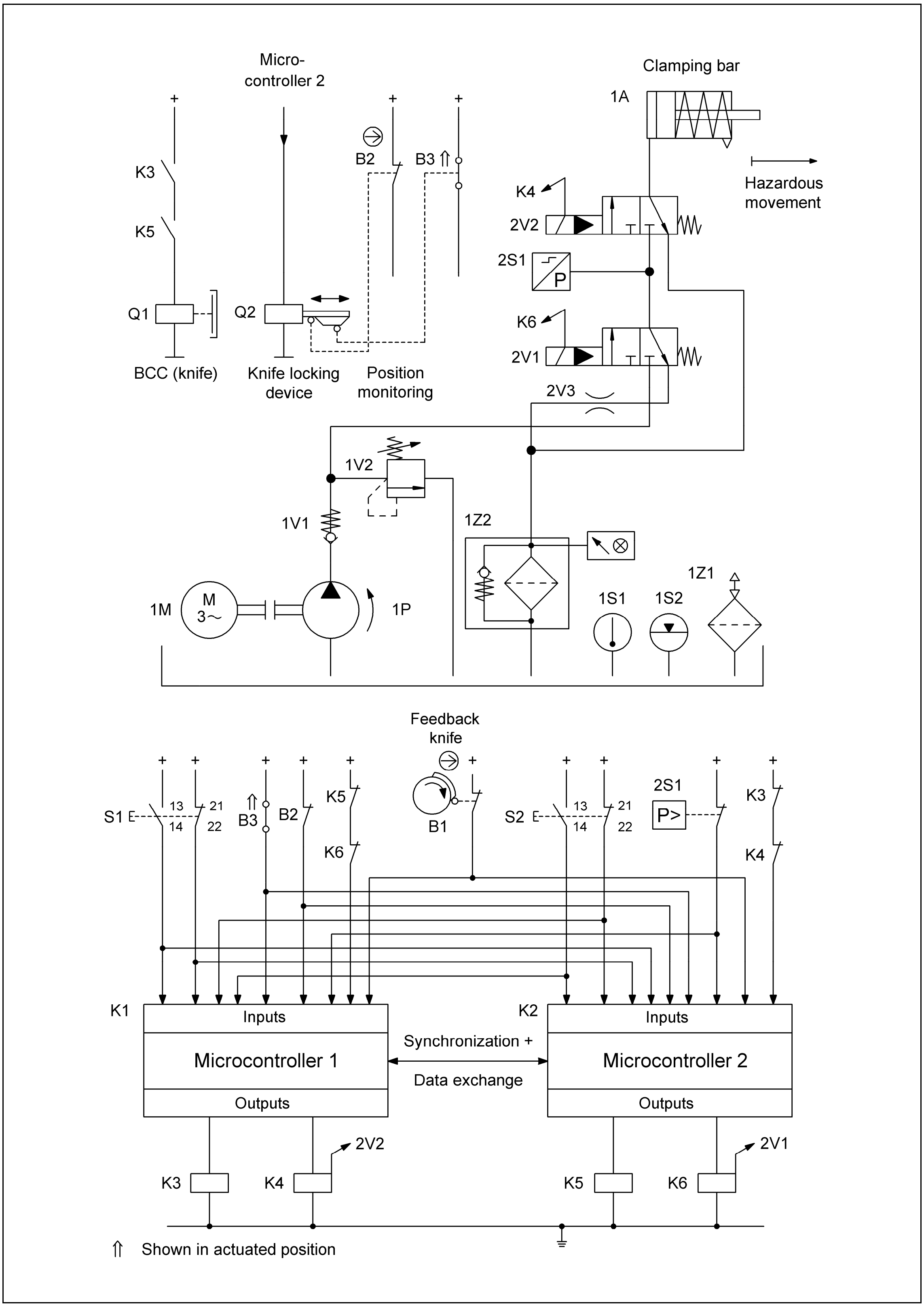
Name	DC [%]	MTTFd [a]
BL Contactor relay K3	99 (High)	75,76 (High)

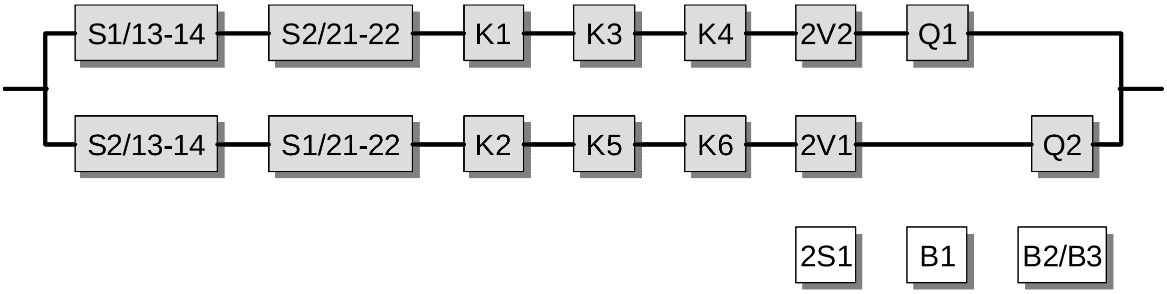
Channel 2

Name	DC [%]	MTTFd [a]
BL Contactor relay K4	99 (High)	75,76 (High)

8.2.37 Paper-cutting guillotine with programmable electronic logic control – Category 4 – PL e (Example 37)

Figure 8.62:
Actuation of an electric knife drive and a hydraulic clamping bar



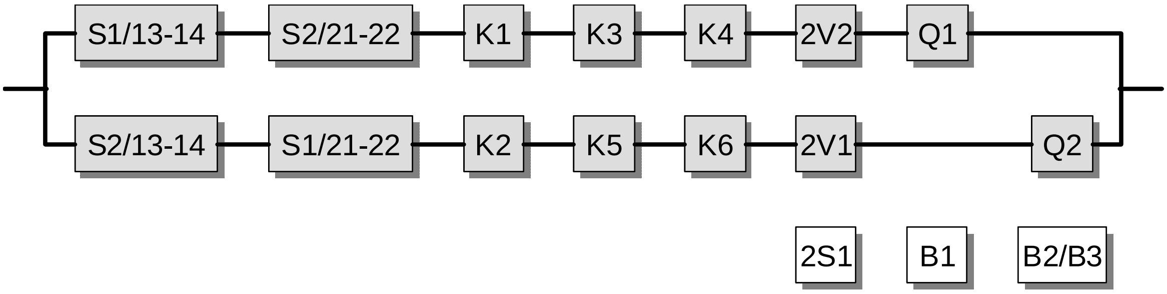


Safety function

- Controlled location of a single operator's hands outside the hazardous area during the press and cutting movement: when at least one of the two push-buttons S1/S2 is released, enabling is cancelled and remains blocked until both pushbuttons are released and pressed again synchronously.

Functional description

- Actuation of the two-hand control (THC) S1 and S2 initiates the hazardous movements (processing cycle) of the clamping bar (hydraulic) 1A and of the knife (electromechanical). If, during this cycle, either of the pushbuttons S1 or S2 is released or a signal change occurs in the peripheral system of the machine (e.g. light curtain, not shown on the circuit diagram) which is not expected by the control system, the cycle is halted and the machine remains in this safe state. Owing to their immediate physical proximity to each other, the knife and the clamping bar constitute a common hazardous zone. The hazard occurs cyclically. The knife is driven by an eccentric drive that receives its energy from a flywheel mass which is in constant motion. The drive is not shown explicitly. The clamping bar is driven linearly by a hydraulic arrangement with has a pump connected to the drive of the flywheel mass.
- When pushbuttons S1/S2 (THC) are pushed, the signal change is fed to the two microcontrollers K1 and K2. Provided these signals satisfy the requirements for simultaneity in accordance with the standard (EN 574, Type III C) and all peripheral signals satisfy the condition for a start, K1 and K2 set the outputs for a valid cut request. Each microcontroller monitors both hazardous movements through the contactor relays K3 to K6. The closing movement of the clamping bar 1A can be prevented by the two hydraulic valves 2V1 and 2V2. Actuation of the brake/clutch combination (BCC) Q1 can be prevented via K3 and K5. A suitably dimensioned mechanical knife locking device Q2 must also be enabled cyclically by K2. Should faults be detected in Q1, the knife cycle can therefore be prevented in the following cycle at the latest.
- Faults in the switches S1/S2 or in the contactor relays with mechanically linked positively operating readback contacts K3 to K6 are detected in the microcontrollers by cross-checking. The functioning of 2V1/2V2 is monitored by means of the pressure switch 2S1. Since the microcontrollers perform self-tests in addition in the background during operation, internal faults and faults in the peripherals can be detected here in time.



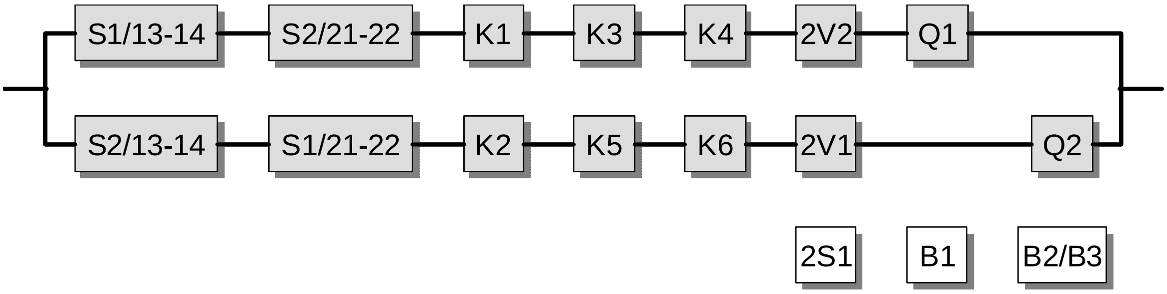
- All machine states are monitored and controlled by both microcontrollers. The cyclical nature of the cut operation causes all system states to be cycled through and compared with each other. Faults and deviations from defined intermediate states cause the machine to be halted at the latest upon completion of the cycle. This method is implied in the diagram by “feedback signal knife” B1 and “position monitoring” B2/B3 of “knife locking device” Q2.
- Brake wear is monitored with the aid of the position switch B1. B1 is actuated and a further cut prevented by the control system in response to the slightest increase in the overrun.

Design features

- Basic and well-tried safety principles are observed and the requirements of Category B are met. Protective circuits as described in the initial paragraphs of Chapter 8 are implemented.
- The actuators S1 and S2 of the two-hand control satisfy IEC 60947-5-1.
- B1 and B2 are position switches with direct opening action to IEC 60947-5-1, Annex K.
- K3 to K6 possess mechanically linked contact elements to IEC 60947-5-1, Annex L.
- The supply conductors to the position switches are laid either separately or with protection against mechanical damage.
- The software of the homogeneously redundant microprocessor structure satisfies the requirements of IEC 61508-3, Section 7 for SIL 3.
- A fault exclusion applies for the fault “complete failure of the brake/clutch combination”, i.e. failure to disengage when the cut enable is cancelled following initiation of a cut. The reasoning for this fault exclusion is based upon many years of experience and the design features of the brake/clutch combination with the possibility of early detection of brake wear.
- The components B1 and B2/B3 are required for implementation of the measures required in EN 1010-3 for stopping and overrun of the knife.

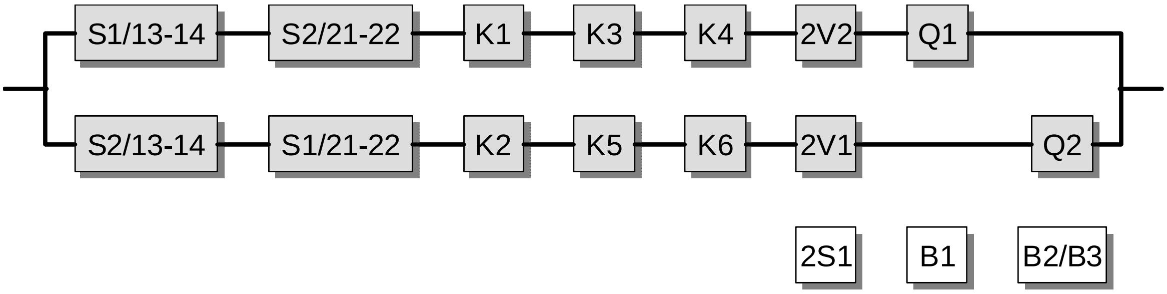
Calculation of the probability of failure

- The designated architecture for Category 4 for actuation of the knife drive and the clamping bar is implemented by two independent channels as described.



Since the channels are virtually identical in their arrangement and are calculated with the use of identical numerical data, symmetrization is not required. For the sake of simplification, only single-channel actuation of Q1 is assumed. The probability of failure is therefore slightly lower in practice than that calculated.

- Since S1 and S2 must trigger shut-off independently of each other when released, they are connected logically in series. For this purpose, one make contact 13-14 and one break contact 21-22 for each pushbutton were assigned to a control channel. The safety-related block diagram differs substantially in this respect from the functional circuit diagram. The B_{10d} value for each individual contact is employed, constituting an estimation erring on the safe side.
- $MTTF_d$: at 240 working days, 8 working hours and a cycle time of 60 seconds, n_{op} is 115,200 switching operations per year. Owing to the defined control current (low load; the mechanical lifetime of the contacts is the determining factor), B_{10d} values of 2,000,000 switching operations [M] are assumed for S1 and for S2, and therefore an $MTTF_d$ of 173 years. An $MTTF_d$ of 878 years [D] is stated for the microcontroller including peripherals, in accordance with SN 29500-2. At low load, a B_{10d} of 20,000,000 switching operations [S] and thus an $MTTF_d$ of 1,736 years applies for the contactor relays K3 to K6. The MTTF_d value of 607 years for the brake/clutch combination Q1 is calculated from the B_{10d} value of 7,000,000 cycles [E]. The same value is assumed for the knife locking device Q2 in the second channel. The values for the two directional control valves 2V1 and 2V2 are 150 years [S]. These values result in an $MTTF_d$ for one channel of 45.2 years (“high”).
- DC_{avg}: the *DC* of 99% for S1/S2 is based upon the cross-checking of input signals without dynamic test, with frequent signal changes. The *DC* of 90% for K1/K2 is derived from self-tests performed by software and the dynamic cross-checking of data with expectations regarding timing. The *DC* of 99% for K3 to K6 is derived from plausibility testing by means of mechanically linked contacts. For 2V1/2V2, the *DC* is 99% owing to indirect and direct electrical monitoring of the pressure with frequent signal changes. Wear in the clutch leads to a change in cutting behaviour. This behaviour is monitored by instruments. A *DC* of 99% is therefore assumed for Q1. Failure of Q2 is detected immediately owing to cyclical actuation and the monitoring elements B1 and B3. This is the reasoning for a *DC* of 99%. These values result in a DC_{avg} of 98.5% (within the tolerance of “high”).
- Adequate measures against common cause failure (65 points): separation (15), overvoltage protection etc. (15) and environmental conditions (25 + 10)

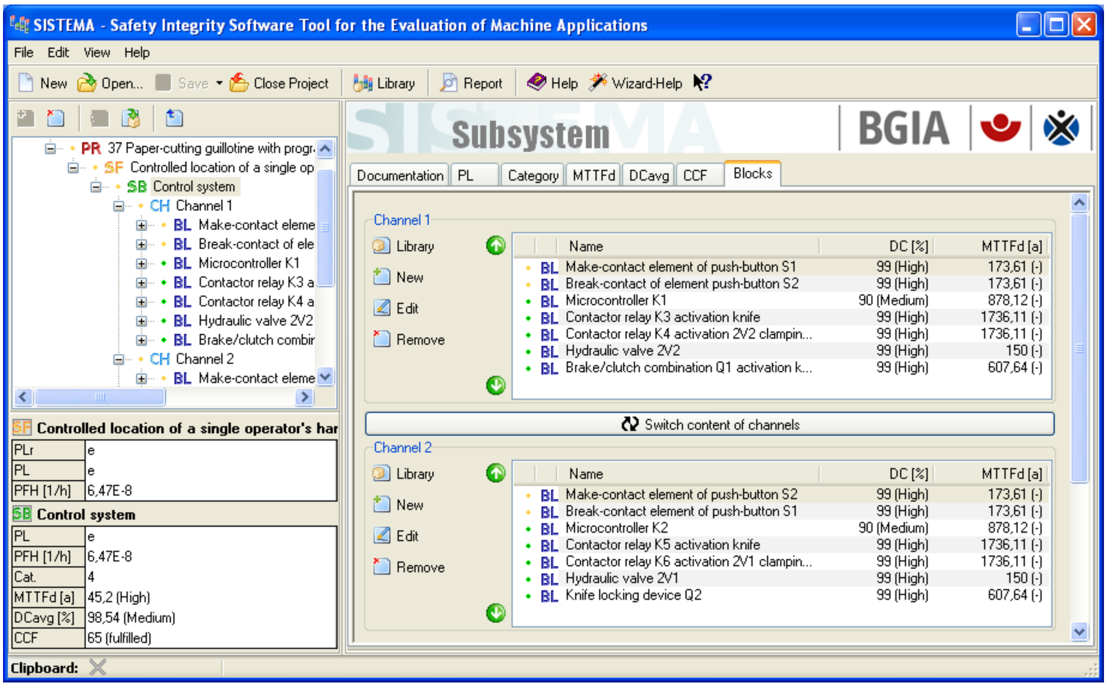


- For Category 4, the average probability of dangerous failure is 6.47 × 10^{-8} per hour. This corresponds to PL e.
- In consideration of the estimation erring on the safe side described above, a value of over 17 years (T_{10d}) is produced for the designated replacement of the wearing elements S1 and S2.

More detailed references

- EN 1010-3: Safety of machinery – Safety requirements for the design and construction of printing and paper converting machines – Part 3: Cutting machines (07.02)
- EN 574: Safety of machinery – Two-hand control devices – Functional aspects; principles for design (11.96)
- IEC 60947-5-1: Low-voltage switchgear and controlgear – Part 5-1: Control circuit devices and switching elements – Electromechanical control circuit devices (11.03)

Figure 8.63:
Determining of the PL by means of SISTEMA


SISTEMA - Safety Integrity Software Tool for the Evaluation of Machine Applications
File Edit View Help
New Open... Save Close Project Library Report Help Wizard-Help
Subsystem
BGIA
Documentation PL Category MTTFd DCavg CCF Blocks
Library
New
Edit
Remove
Switch content of channels
Clipboard:

PR 37 Paper-cutting guillotine with progr...
SF Controlled location of a single op...
SB Control system
CH Channel 1
BL Make-contact eleme...
BL Break-contact of ele...
BL Microcontroller K1
BL Contactor relay K3 a...
BL Contactor relay K4 a...
BL Hydraulic valve 2V2
BL Brake/clutch combir...
CH Channel 2
BL Make-contact eleme...

SF Controlled location of a single operator's har...

PLr	e
PL	e
PFH [1/h]	6,47E-8

SB Control system

PL	e
PFH [1/h]	6,47E-8
Cat.	4
MTTFd [a]	45,2 (High)
DCavg [%]	98,54 (Medium)
CCF	65 (fulfilled)

Channel 1

	Name	DC [%]	MTTFd [a]
BL	Make-contact element of push-button S1	99 (High)	173,61 (-)
BL	Break-contact of element push-button S2	99 (High)	173,61 (-)
BL	Microcontroller K1	90 (Medium)	878,12 (-)
BL	Contactor relay K3 activation knife	99 (High)	1736,11 (-)
BL	Contactor relay K4 activation 2V2 clampin...	99 (High)	1736,11 (-)
BL	Hydraulic valve 2V2	99 (High)	150 (-)
BL	Brake/clutch combination Q1 activation k...	99 (High)	607,64 (-)

Channel 2

	Name	DC [%]	MTTFd [a]
BL	Make-contact element of push-button S2	99 (High)	173,61 (-)
BL	Break-contact element of push-button S1	99 (High)	173,61 (-)
BL	Microcontroller K2	90 (Medium)	878,12 (-)
BL	Contactor relay K5 activation knife	99 (High)	1736,11 (-)
BL	Contactor relay K6 activation 2V1 clampin...	99 (High)	1736,11 (-)
BL	Hydraulic valve 2V1	99 (High)	150 (-)
BL	Knife locking device Q2	99 (High)	607,64 (-)

9 References

[1] Directive 98/37/EC of the European Parliament and of the Council of 22 June 1998 on the approximation of the laws of the Member States relating to machinery. OJ EC L 207 (1998), p. 1; amended by Directive 98/79/EC, OJ EC L 331 (1998), p. 1.
http://eur-lex.europa.eu

[2] EN ISO 12100-1: Safety of machinery – Basic concepts, general principles for design – Part 1: Basic terminology, methodology (11.03)

[3] EN ISO 12100-2: Safety of machinery – Basic concepts, general principles for design – Part 2: Technical principles (11.03)

[4] EN ISO 14121-1: Safety of machinery – Risk assessment – Part 1: Principles (09.07)

[5] ISO/TR 14121-2: Safety of machinery – Risk assessment – Part 2: Practical guidance and examples of methods (12.07)

[6] EN ISO 13849-1: Safety of machinery – Safety-related parts of control systems – Part 1: General principles for design (11.06)

[7] EN ISO 13849-2: Safety of machinery – Safety-related parts of control systems – Part 2: Validation (08.03)

[8] Directive 2006/42/EC of the European Parliament and of the Council of 17 May 2006 on machinery, and amending Directive 95/16/EC (recast). OJ EC L 157 (2006), p. 24; with corrigendum to Directive 2006/42/EC of the European Parliament and of the Council of 17 May 2006 on machinery, and amending Directive 95/16/EC of 9 June 2006. OJ EC L 76 (2007), p. 35
http://eur-lex.europa.eu

[9] *Ostermann, H.-J.; von Locquenghien, D.:* Wegweiser Maschinensicherheit. Bundesanzeiger Verlagsgesellschaft, Cologne 2007

[10] *Reudenbach, R.*: Sichere Maschinen in Europa – Part 1: Europäische und nationale Rechtsgrundlagen. 8th ed. Verlag Technik & Information, Bochum 2007

[11] EN 954-1: Safety of machinery – Safety-related parts of control systems – Part 1: General principles for design (12.96)

[12] IEC 61508: Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 0 to 7 (11.98 to 01.05)

[13] IEC 62061: Safety of machinery – Functional safety of safety-related electrical, electronic and programmable electronic control systems (01.05) and Corrigendum 1 (07.05) and Corrigendum 2 (04.08)

[14] *Bömer, T.*: Funktionale Sicherheit nach IEC 61508. In: BGIA-Handbuch Sicherheit und Gesundheitsschutz am Arbeitsplatz. Kennzahl 330 219. 47th suppl. XII/2005. Ed.: BGIA – Institut für Arbeitsschutz der Deutschen Gesetzlichen Unfallversicherung, Sankt Augustin. Erich Schmidt, Berlin 1985 – loose-leaf ed.
www.bgia-handbuchdigital.de/330219

[15] *Hauke, M.; Schaefer, M.*: Sicherheitsnorm mit neuem Konzept. O + P Ölhydraulik und Pneumatik 50 (2006) No. 3, pp. 142-147.
www.dguv.de/bgia, Webcode d4473

[16] *Schaefer, M.; Hauke, M.*: Performance Level Calculator – PLC. 2nd ed. Ed.: BGIA – Institut für Arbeitsschutz der Deutschen Gesetzlichen Unfallversicherung, Sankt Augustin; Zentralverband Elektrotechnik- und Elektronikindustrie (ZVEI) e.V. – Fachverband Automation, Frankfurt am Main, and Verband Deutscher Maschinen- und Anlagenbau e.V. – VDMA, Frankfurt am Main 2007.
www.dguv.de/bgia, Webcode e20892

[17] Summary list of titles and references of harmonised standards under Directive 98/37/EC on Machinery. Ed.: European Commission.
http://ec.europa.eu/enterprise/newapproach/standardization/harmstds/reflist/machines.html

[18] *Reinert, D.*: Risikobezogene Auswahl von Steuerungen. In: BGIA-Handbuch Sicherheit und Gesundheitsschutz am Arbeitsplatz. Kennzahl 320 100. 31th suppl. I/98. Ed.: BGIA – Institut für Arbeitsschutz der Deutschen Gesetzlichen Unfallversicherung, Sankt Augustin. Erich Schmidt, Berlin 1985 – loose-leaf ed.
www.bgia-handbuchdigital.de/320100

[19] IEC 61800-5-2: Adjustable speed electrical power drive systems – Part 5-2: Safety requirements – Functional (07.07)

[20] EN 60204-1: Safety of machinery – Electrical equipment of machines. Part 1: General requirements (IEC 60204-1:2005, modified) (06.06)

[21] Interpretationen zu Vorschriften: Wesentliche Veränderung von Maschinen. Ed.: Berufsgenossenschaft der chemischen Industrie (06/2005).
www.bgchemie.de/webcom/show_article.php/_c-781/_nr-2/i.html

[22] *Apfeld, R.; Huelke, M.; Lüken, K.; Schaefer, M.* et al.: Manipulation von Schutzeinrichtungen an Maschinen. HVBG-Report. Ed.: Hauptverband der gewerblichen Berufsgenossenschaften, Sankt Augustin 2006.
www.dguv.de/bgia, Webcode d6303

[23] Berufsgenossenschaftliche Information BGI 5048-1 und -2: Ergonomische Maschinengestaltung, Checkliste, Auswertungsbogen und Merkheft (10.2006). Carl Heymanns, Cologne 2006.
www.dguv.de/bgia, Webcode d3443

[24] VDI/VDE 3850 Part 1: User-friendly design of useware for machines (05/00). Part 2: User-friendly design of useware for machines – Interaction devices for displays screens (11/02). Part 3: User-friendly design of useware for machines – Design of dialogues for touchscreens (03/04). Beuth, Berlin

[25] *Birolini, A.*: Reliability Engineering: Theory and Practice. 5th ed. Springer, Berlin 2007

[26] IEC 61508-2: Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 2: Requirements for electrical/electronic/programmable electronic safety-related systems (05.00)

[27] IEC 61508-6: Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 6: Guidelines on the application of IEC 61508-2 and IEC 61508-3 (04.00)

[28] Prüfgrundsätze Bussysteme für die Übertragung sicherheitsrelevanter Nachrichten GS-ET-26. Ed.: Fachausschuss Elektrotechnik, Cologne 2002.
www.dguv.de, Webcode d14884

[29] IEC 61784-3: Industrial communication networks – Profiles – Part 3: Functional safety fieldbuses – General rules and profile definitions (12.07)

[30] *Reinert, D.; Schaefer, M.*: Sichere Bussysteme für die Automation. Hüthig, Heidelberg 2001

[31] *Huckle, T.:* Kleine BUGs, große GAUs. Lecture entitled "Softwarefehler und ihre Folgen". 2003.
www5.in.tum.de/~huckle/bugsn.pdf

[32] IEC 61508-3: Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 3: Software requirements (12.98) and Corrigendum 1 (04.99)

[33] IEC 61131-3: Programmable controllers – Part 3: Programming languages (01.03)

[34] *Schaefer, M.; Gnedina, A.; Bömer, T.; Büllesbach, K.-H.; Grigulewitsch, W.; Reuß, G.; Reinert, D.:* Programmierregeln für die Erstellung von Software für Steuerungen mit Sicherheitsaufgaben. Series of publications by the Bundesanstalt für Arbeitsschutz und Arbeitsmedizin, Dortmund, Fb 812. Wirtschaftsverlag NW, Bremerhaven 1998 (out of print; parts available at: www.dguv.de/bgia, Webcode d3250)

[35] MISRA Development Guidelines for Vehicle Based Software. Published by: The Motor Industry Software Reliability Association.
www.misra.org.uk

[36] SN 29500: Failure rates of components – Expected values. Ed.: Siemens AG, Center for Quality Engineering, Munich 1994 to 2005

[37] EN 574: Safety of machinery – Two-hand control devices – Functional aspects; principles for design (11.96)

[38] IEC 60947-5-1: Low-voltage switchgear and controlgear – Part 5-1: Control circuit devices and switching elements – Electromechanical control circuit devices (11.03)

[39] IEC 61508-2:2008 (CDV): Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 2: Requirements for electrical/electronic/programmable electronic safety-related systems (IEC 65A/523/CDV)

[40] *Kleinbreuer, W.; Kreutzkampf, F.; Meffert, K.; Reinert, D.*: Categories for Safety-related Control Systems in Accordance with EN 954-1. BIA-Report 6/97e. Ed.: Hauptverband der gewerblichen Berufsgenossenschaften (HVBG), Sankt Augustin 1997.
www.dguv.de/bgia, Webcode e21973

[41] EN 982: Safety of machinery – Safety requirements for fluid power systems and their components – Hydraulics (04.96)

[42] EN 983: Safety of machinery – Safety requirements for fluid power systems and their components – Pneumatics (04.96)

[43] EN 1037: Safety of machinery – Prevention of unexpected start-up (12.95)

[44] ISO 1219-1: Fluid power systems and components – Graphic symbols and circuit diagrams – Part 1: Graphic symbols for conventional use and data-processing applications (10.06)

[45] ISO 1219-2: Fluid power systems and components – Graphic symbols and circuit diagrams – Part 2: Circuit diagrams (12.95)

[46] ISO 8573-1: Compressed air – Part 1: Contaminants and purity classes (02.01)

[47] ISO 8573-1: Compressed air – Part 1: Contaminants and purity classes; Technical Corrigendum 1 (04.02)

Annex A: Examples of risk assessment

Example 1: Closing edge protection device

Figure A.1 shows the risk assessment for the safety function:

- SF1 Stopping the closing movement, reversal of movement

of a closing edge protection device[1]. The movement of power-operated windows, doors and gates (see Figure A.1) is generally associated with the formation of crushing and shearing zones. These hazardous zones generally exist only when the moving wing is approaching its final position. Injury to persons at such hazardous zones can be avoided, for example by the use of closing edge protection devices. Closing edge protection devices, such as pressure sensitive edges, are fitted to the closing edges of the moving wings. When an obstacle is detected, the closing movement is interrupted and a reverse movement initiated.

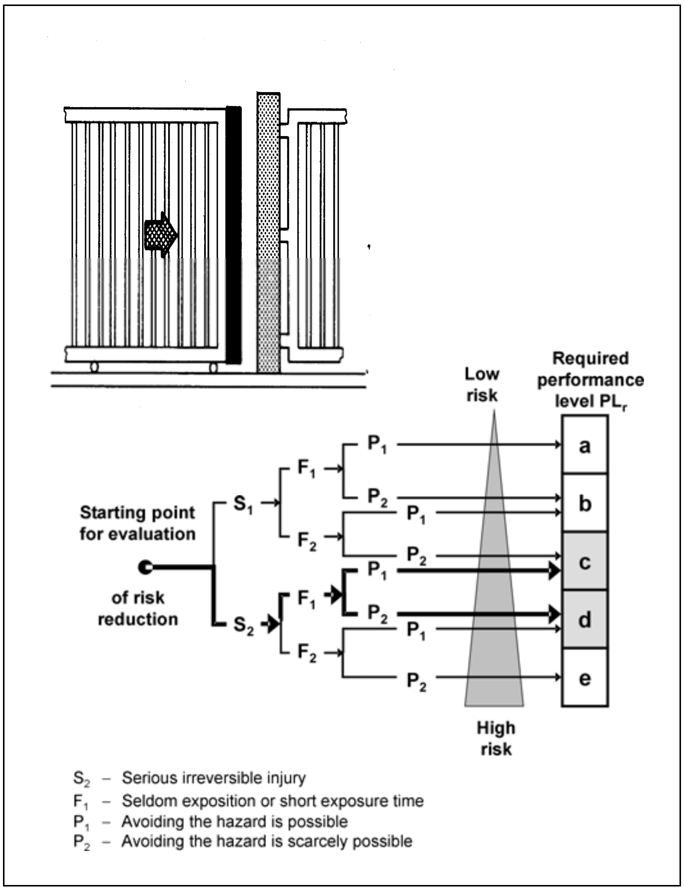

Low risk
Required performance level PL$_r$
Starting point for evaluation of risk reduction
S$_1$
S$_2$
F$_1$
F$_2$
P$_1$
P$_2$
a
b
c
d
e
High risk
S$_2$ – Serious irreversible injury
F$_1$ – Seldom exposition or short exposure time
P$_1$ – Avoiding the hazard is possible
P$_2$ – Avoiding the hazard is scarcely possible

Figure A.1:
Risk assessment for closing edge protection devices on power windows, doors and gates

[1] In the past, closing edge protection devices were governed by the Construction Products Directive. Since the pressure sensitive edges constitute safety components under the Machinery Directive, however, closing edge protection devices are also evaluated in accordance with this directive.

Crushing and shearing zones on power-operated windows, doors and gates may cause severe and, under some circumstances, fatal injury. A severity of injury of S2 must therefore be assumed. Persons are infrequently and only briefly present in the area of the crushing and shearing zones, which occur only temporarily (F1). Under normal circumstances, persons at risk are able to move out of the hazardous area formed by the moving wing (P1). The required Performance Level PL_r is therefore c. On fast-closing gates, this opportunity is limited (P2), resulting in a required Performance Level PL_r of d.

Example 2: Driverless truck

On driverless trucks, collision protection is assured by the safety function

- SF1 Stopping of the truck

Since a driverless truck may, under certain circumstances, be carrying a load weighing in the order of tons, severe irreversible injury is probable should a collision occur with the vehicle travelling at full speed (S2). The paths travelled by the vehicle are freely accessible to persons; the presence of the latter in the hazardous area must therefore be assumed to be relatively frequent (F2). Since such vehicles travel at a very low speed (generally 3 to 5 km/h), a pedestrian is generally able to take evasive action when such a vehicle approaches (P1). This therefore results in a required Performance Level PL_r of d for SF1 (see Figure A.2).

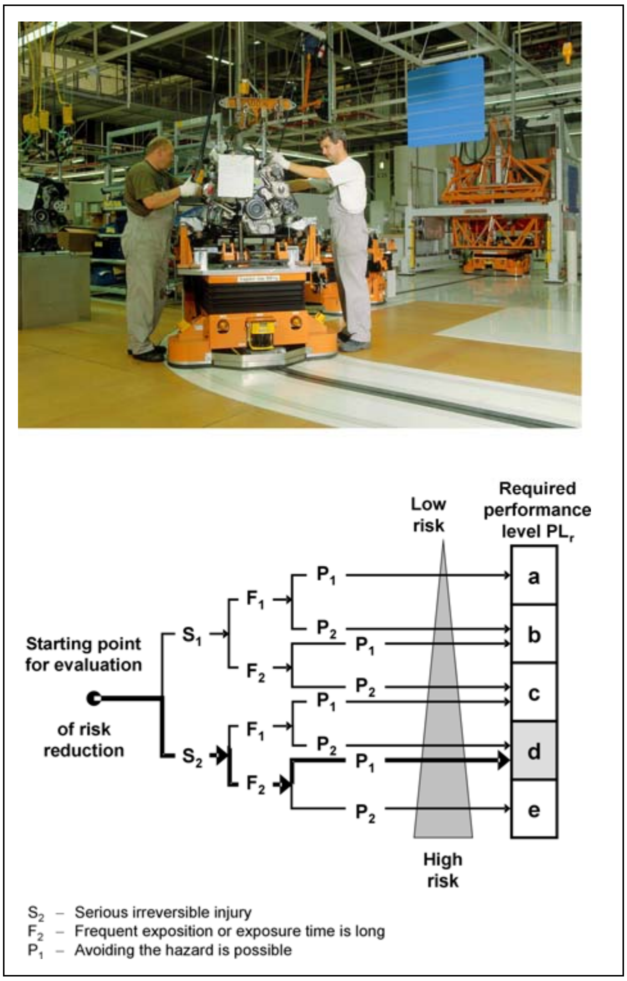

Required performance level PL_r
Low risk
High risk
Starting point for evaluation
of risk reduction
S1
S2
F1
F2
P1
P2
a
b
c
d
e
S2 – Serious irreversible injury
F2 – Frequent exposition or exposure time is long
P1 – Avoiding the hazard is possible

Figure A.2:
Risk assessment for collision protection on a driverless industrial truck

Example 3: Weaving machine

Weaving machines are employed for the fully automatic weaving of textiles. The essential hazard is that of crushing between the reed and the temple. In order to reconnect the ends of broken warp threads, the weaver must intervene at the hazardous zone with the machine stationary. Unexpected restarting is prevented by the safety function

- SF1 Safe torque off

Should the machine restart, the weaver's fingers may be crushed or broken (S2). The frequency and duration of exposure to danger can be described as low (F1). Should the weaver already have his hands in the hazardous area when the machine restarts unexpectedly, the movement is so fast as to make evasion virtually impossible (P2). The required Performance Level for SF1 is therefore a PL_r of d (see Figure A.3).

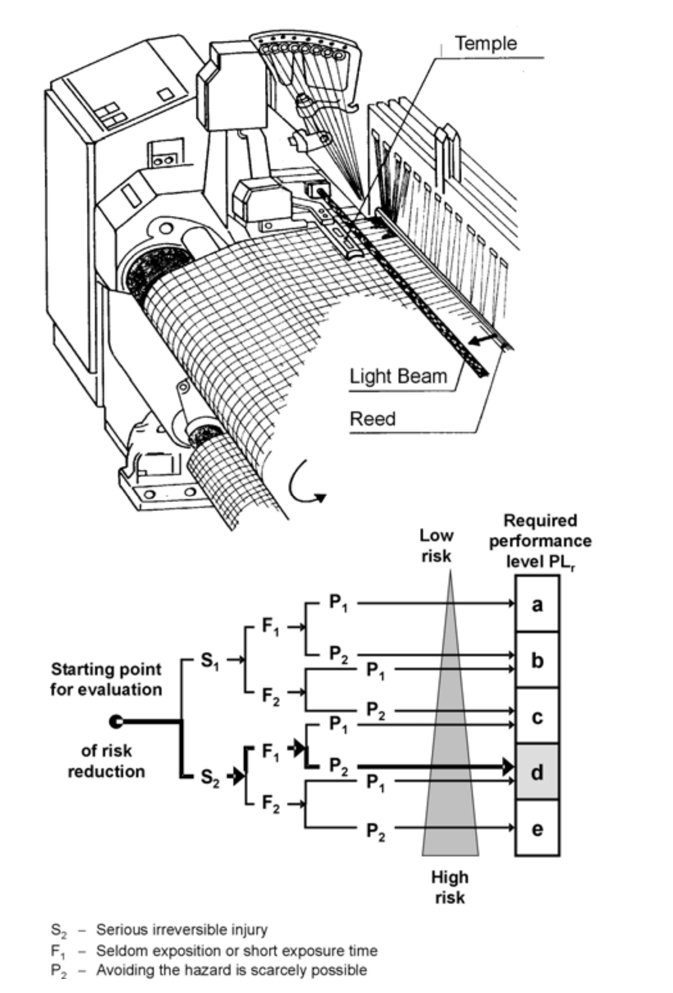

Temple
Light Beam
Reed
Low risk
Required performance level PL_r
Starting point for evaluation
of risk reduction
S_1
S_2
F_1
F_2
P_1
P_2
a
b
c
d
e
High risk
S_2 – Serious irreversible injury
F_1 – Seldom exposition or short exposure time
P_2 – Avoiding the hazard is scarcely possible

Figure A.3:
Risk assessment for a weaving machine

Example 4: Rotary printing machine

On a web-fed printing press, a paper web is fed through a number of cylinders. High operating speeds and rotational speeds of the cylinders are reached, particularly in newspaper printing. Essential hazards exist at the zones where it is possible to be drawn in by the counter-rotating cylinders. This example considers the hazardous zone on a printing machine on which maintenance work requires manual intervention at reduced machine speeds. The access to the hazardous zone is protected by a guard door (safeguarding). The following safety functions are designated:

- SF1 – Opening of the guard door during operation causes the cylinders to be braked to a halt.
- SF2 – When the guard door is open, any machine movements must be performed at limited speed.
- SF3 – When the guard door is open, movements are possible only whilst an inching button is pressed.

Entrapment between the cylinders causes severe injuries (S2). Since work in the hazardous area is necessary only during maintenance tasks, the frequency and duration of hazard exposure can be described as low (F1). At production speeds, no possibility exists of avoiding the hazardous movement (P2). This therefore results in a required Performance Level PL_r of d for the safety functions SF1 and SF2 (see Figure A.4).

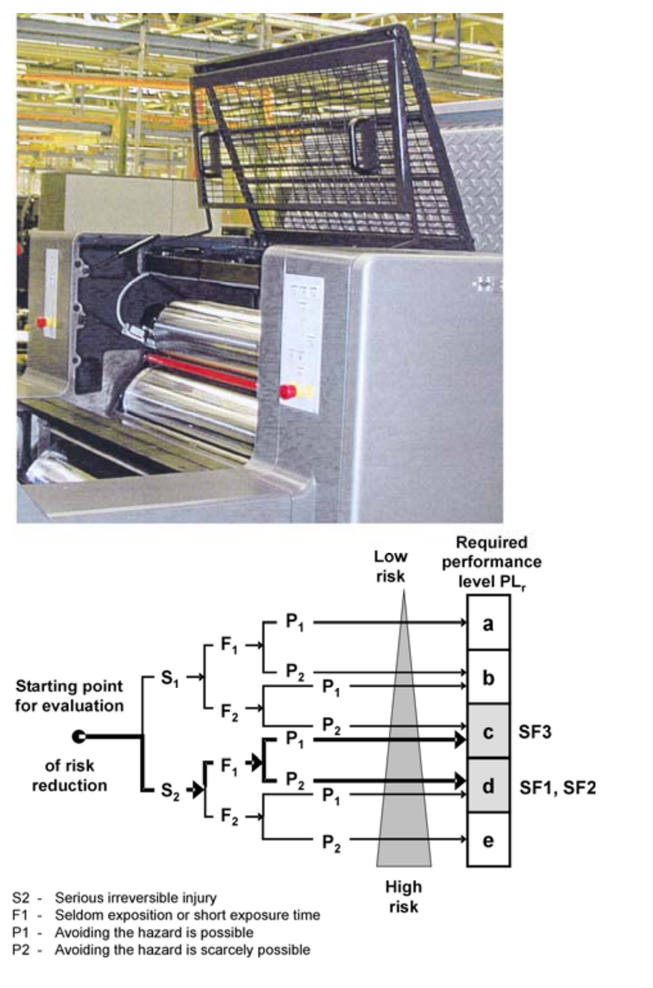

Low risk
Required performance level PL_r
Starting point for evaluation of risk reduction
S_1
S_2
F_1
F_2
F_1
F_2
P_1
P_2
P_1
P_2
P_1
P_2
P_1
P_2
a
b
c
d
e
SF3
SF1, SF2
High risk
S2 - Serious irreversible injury
F1 - Seldom exposition or short exposure time
P1 - Avoiding the hazard is possible
P2 - Avoiding the hazard is scarcely possible

Figure A.4:
Risk assessment on a rotary printing machine

The safety function SF3 can however be used only if the printing machine has first been halted (SF1) and the permissible rotational speed of the cylinders limited (SF2).

This results in the possible machine movements being predictable for the operator, who is thus able to evade hazardous movements (P1). A required Performance Level PL_r of c is therefore adequate for SF3 (see Figure A.4). Chapter 8, Example 24 (see page 230) describes how these safety functions can be implemented. Examples 1 to 3 have been taken from the BGIA-Handbuch [1] (BGIA Manual), which contains numerous other applications from the area of machine guarding.

Reference

[1] BGIA-Handbuch Sicherheit und Gesundheitsschutz am Arbeitsplatz. Ed.: BGIA – Institut für Arbeitsschutz der Deutschen Gesetzlichen Unfallversicherung, Sankt Augustin. Erich Schmidt, Berlin 1985 – loose-leaf ed. www.bgia-handbuchdigital.de

Annex B:
Safety-related block diagram and FMEA

For demonstration of the Category and Performance Level (PL) to EN ISO 13849-1, the structure of a safety-related system must be analysed with regard to the safety function to be implemented (possibly involving separate analysis of several functions). For the obligatory quantitative demonstration of the PL, system information must be suitably prepared to permit calculation of the quantitative value PFH (probability of a dangerous failure per hour), or direct calculation of the PL which is based upon it. Two important steps in this process are the safety-related block diagram and the failure mode and effects analysis (FMEA) which is performed for each function block.

B1 Purpose and generation of a safety-related block diagram

The result of the safety-oriented analysis of the system structure is presented conveniently in the form of a block diagram which can be described as a “safety-related block diagram”. The diagram is intended to show whether the safety function is executed in whole or part by a single-channel or multi-channel solution, and the available diagnostics by which internal component failures can be detected. Since – with regard to the relevant aspect here, i.e. quantification of the probabilities of failure – diagnostics represents a means of compensating for component failures, the term “failure detection” will be used in this Annex in place of the usual term “fault detection”.

In the field of machine safety, it is generally accepted that in the event of a control system failure, a substitute response should occur in place of the originally intended safety function. The substitute reaction brings about a safe state, such as operating inhibition with de-energized outputs (shut-down system). In accordance with EN ISO 13849-1, the Category and PL are intended to indicate only the safety quality, and not the probability of fault-free operation, i.e. the “availability”. For this reason, signal paths which bring about a safe state in the event of a fault are regarded as being fully equivalent to functional units which may execute complicated safety functions. A “simple safety signal path” in this context is however a “channel” in its own right only when it is continually engaged. If the safety path cannot become active until a failure in the main function path proper has been detected, its safety benefit is dependent upon the quality of the failure detection mechanism. This quality is described by the diagnostic coverage of the failure detection mechanism. In such cases, the safety path generally only provides test equipment and a shut-off path. Architectural features of this kind must be expressed correctly on the safety-related block diagram. The differentiated presentation of a true two-channel arrangement and a monitored single channel can be seen clearly from a comparison of Figures 10 and 11 in the standard.

Consideration must also be given as to whether components or partial circuits are present which, although they do not execute the safety function or the safety-related substitute function in the event of a fault, may be able to prevent other components from properly executing the safety or substitute function should certain component failures occur. Circuit components in this context include those providing necessary auxiliary functions such as the power supply or control functions which are not (intentionally) relevant to safety but which may have an impact upon safety-related parts. Where components and parts of circuits may be expected to impact negatively upon the safety function, its substitute function, or diagnostics functions in the event of failures, they must always be considered in a function block. For example, components for assurance of electromagnetic compatibility (EMC) must be examined with regard to whether their failure, for example short-circuiting of a capacitor, has negative effects upon safety-related circuits.

Parts of circuits with defined inputs and outputs may be regarded as a function block. In order to keep the number of required function blocks as low as possible, parts of circuits which are arranged functionally in series, i.e. circuits which execute different signal processing steps sequentially, can be grouped to form a function block. By the same token, blocks differing from this arrangement should be grouped only to the extent that redundancies such as separate shut-off paths and the mutual diagnostics of function blocks are still expressed. The circuit analysis must ultimately produce a block diagram in which all the structures which are of relevance to safety are reflected:

- Single or parallel signal paths ("channels") which are used to execute the safety function
- Signal paths which execute a safety-related substitute function in the event of a fault
- Circuits for the detection of failures (diagnostics)

Where auxiliary circuits which are required for execution of the safety function or for some other safety-related action (e.g. power supplies, oscillators) are able to influence one channel only, they should be grouped with the function block(s) of the channel concerned. Should these auxiliary circuits act upon several channels, they form a separate single-channel part (function block) on the safety-related block diagram. The same principle applies to circuits which are able to prevent execution of the safety function, another safety-related action or diagnostics owing to a certain failure type. Examples include circuits for selection of a safe operating mode, or certain components for the assurance of EMC.

The content of each function block must be determined unambiguously by circuit diagrams and parts lists. Owing to the way in which it is created and its particular function, the safety-related block diagram generally differs from block diagrams serving other purposes, such as those geared to the mechanical structure of assemblies.

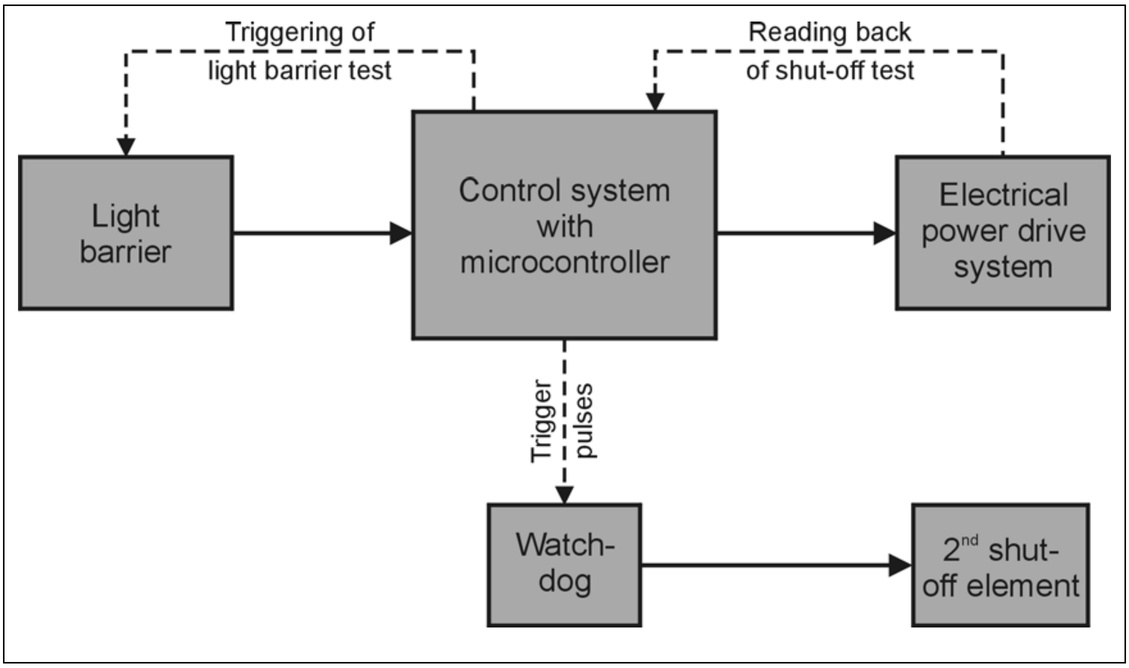
Figure B.1 shows, by way of example, the safety-related block diagram of a Category 2 single-channel machine control system featuring:

- A microcontroller
- A light barrier for the monitoring of hazardous zones
- A "watchdog" for the detection of certain controller malfunctions

- A closed-loop motor drive control (frequency inverter) driven by the controller
- A device for de-energization of the motor which can be actuated by the watchdog (pulse blocking)

The safety function entails de-energization of the motor as soon as, and for as long as, the light beam of the light barrier is interrupted ("safe torque off"). Besides the safety function, the microcontroller and the downstream drive control execute a number of other machine functions which, since they are not safety functions, are not considered here. Although in this example, the safety function is implemented entirely electrically, the principles described for the safety-related block diagram and the FMEA apply to all technologies.

Figure B.1:
Example safety-related block diagram of a Category 2 single-channel machine control system


Triggering of light barrier test
Reading back of shut-off test
Light barrier
Control system with microcontroller
Electrical power drive system
Trigger pulses
Watch-dog
2nd shut-off element

The safety-related block diagram contains only function blocks which are related to the "safe torque off" safety function, and not control or display devices for other machine functions. In the event of a fault, some components in these circuit parts may have negative repercussions for the safety function. Only in such cases shall these components be included in the function blocks which they could cause to fail.

The safety-related block diagram will often take the form of one of the "designated architectures" in accordance with EN ISO 13849-1, Section 6.2 (Sections 6.2.1 to 6.2.7 of this report), as in the example presented here. In such cases, the method described in Section 4.5.4 of the standard (supplemented by Annexes B, C, D, E, I and K) may be applied for quantitative calculation of the Performance Level. It is not advisable however to shoehorn a different structure into the form of one of these architectures. It may be possible to break an existing system structure down into parts each of which then corresponds to a designated architecture. Should such disassembly not be possible, a dedicated model must be produced for quantitative calculation of the safety-related reliability for the safety-related block diagram concerned. An introduction to suitable modelling techniques can be found for example in [1].

B2 Purpose and characteristic of an FMEA for quantification

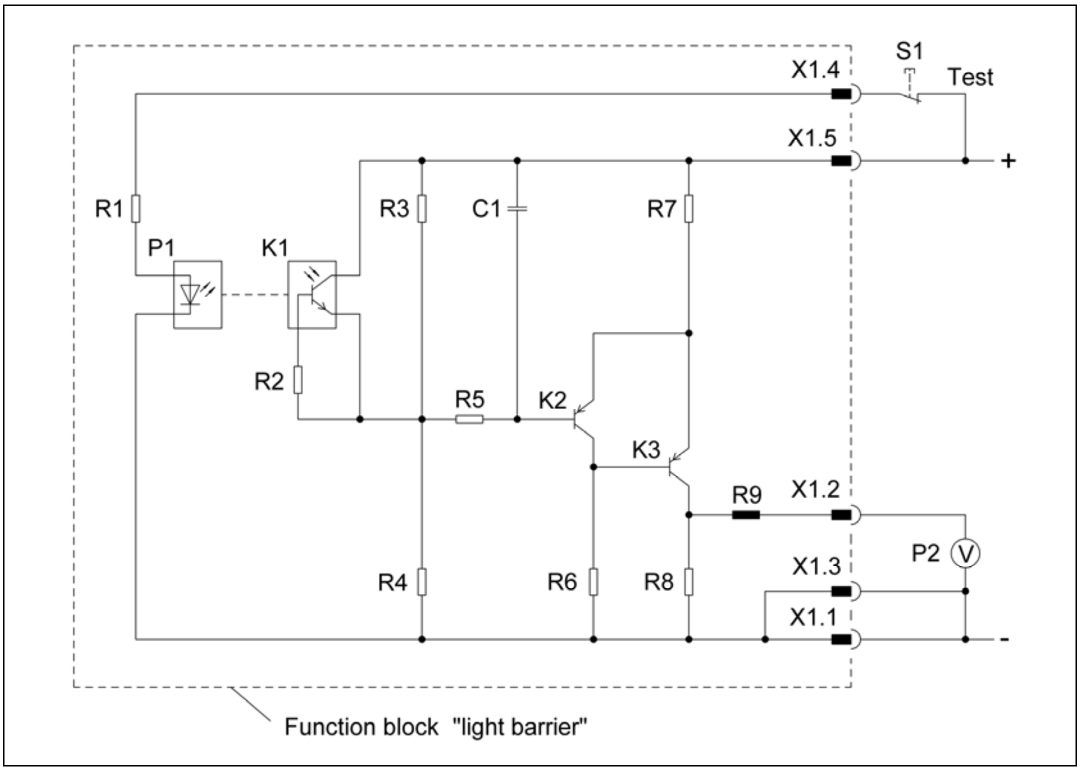
For quantitative demonstration of the PL, the average probability of a dangerous failure per hour (PFH) must be estimated. This can be achieved with the aid of the mathematical model (e.g. a Markov model) generated for the system under consideration. If the form of one of the "designated architectures" in accordance with Sections 6.2.3 to 6.2.7 can be identified formally from the safety-related block diagram, as in the example in Figure B.1, the method referred to above in this standard can be applied for quantitative calculation of the PL. In both cases, the dangerous (i.e. undesirable from a safety perspective) failure rate, specifically its reciprocal, the $MTTF_d$ (mean time to dangerous failure), and the *DC* (diagnostic coverage) must be known from the function blocks of the safety-related block diagram. For calculation of these values, a special variation of the FMEA is used which employs the component failure rates in the form of quantitative values. The special form of the FMEA used here differs in this respect from the majority of other FMEA types, which have different purposes, for example the early detection of problems and fault avoidance during development [2].

A particular feature of an FMEA for quantification purposes is its structure according to the function blocks of the safety-related block diagram. In principle, a separate FMEA is performed for each of these function blocks which produces results only for the function block concerned. The results for each function block are not combined until later, by inclusion together in the calculation of the PFH/PL via a system-specific mathematical model or the simplified quantification method in EN ISO 13849-1.

B2.1 Performance of an FMEA for quantification

The essential procedure employed for an FMEA for quantification is demonstrated below with reference to the "light barrier" function block from Figure B.2. For this purpose, the circuit has been deliberately kept simple. Only components framed by the dashed line belong to the function block. The elements S1 and P2 constitute a substitute circuit representation of the actual manner in which the function block is included within the system in accordance with Figure B.1. As long as the phototransistor K1 continues to receive light from the infrared LED P1, it maintains the transistor K2 blocked, as a result of which transistor K3 is conductive and a positive output voltage is present on terminal X1.2 which can be measured by the voltmeter P2. If the light beam is interrupted, K1 blocks, K2 becomes conductive and K3 switches off the output voltage. The test of the "light barrier" function block, which is performed by the microcontroller control system in Figure B.1 in accordance with the program, can be simulated by the pushbutton S1 and the voltmeter P2: the light source P1 is switched off temporarily, and the output voltage observed for whether it drops to 0 V as intended. The signal-processing elements of the "light barrier" function block (K1 to K3, R2 to R9, C1) are required to behave in the same way as in response to a "real" demand upon the safety function caused by interruption of the light beam. This test is described below as "Test 1".

Figure B.2:
Assumed circuit (simple example) of the “light barrier” function block from the safety-related block diagram from Figure B.1



B2.2 Dangerous failure mode of a function block

The first step entails identification of the dangerous failure mode of the function block. Generally, not only may individual elements fail, but an entire function block may also fail in various ways as a result. Modes of failure which are undesirable from a safety perspective are regarded as the “dangerous” failure mode. Some failures cause immediate and dangerous failure of the entire system, with the result that neither the original safety function, nor a safety-oriented substitute function can be executed. Other failures increase the probability of this happening in that fewer further failures are required in order to cause the system to fail dangerously. Should no redundancy exist for the function block suffering failure, i.e. no second channel capable of assuming its function, and should diagnostics fail to execute an action sufficiently rapidly which produces a safe state, the dangerous failure of the function block leads to dangerous failure of the system. However, even when, owing to the existence of redundancy or a rapid failure response by other circuit components, none of the possible failure modes of the function block under examination causes a dangerous system failure, its “dangerous” failure mode can and must be detected. The dangerous failure mode is that which leads to the function block no longer making its intended contribution to safe behaviour of the system. On occasions it may be necessary for several failure modes which are characterized by different but equally harmful block behaviour to be considered (e.g. continuous energization and oscillation on the output). The simplest solution is therefore to describe the dangerous failure mode in terms of the loss of the function block’s functionality required for safety. Diagnostics features are considered later and will be ignored at this stage. In the example under consideration here (light barrier, Figure B.2), the output voltage of the function block is to drop to zero for as long as the phototransistor K1 fails to receive light from the LED P1, since this constitutes the contribution of this function block to execution of the safety function: “safe torque off when the light beam is interrupted”. The dangerous failure mode of the function block can thus be described as “presence of an output voltage greater than zero during non-illumination of the phototransistor K1”.

B2.3 Component failure rates

Component failure rates may be obtained from a number of sources. Examples for electronic components are listed in [3 to 6]. These sources all contain generic data relevant to multiple manufacturers. Collections of failure rates also exist for mechanical, pneumatic and hydraulic components. For certain components which are not listed in the relevant indexes (such as special ASICs), the failure rate must be obtained from the manufacturer. Many common quantification techniques, including the simplified method in EN ISO 13849-1 Section 4.5.4, assume a constant failure rate over time. This represents an idealized view. With appropriate dimensioning and, if necessary, preventive replacement, components can be prevented from reaching the wear phase during which the failure rate rises sharply, before the end of the mission time T_M.

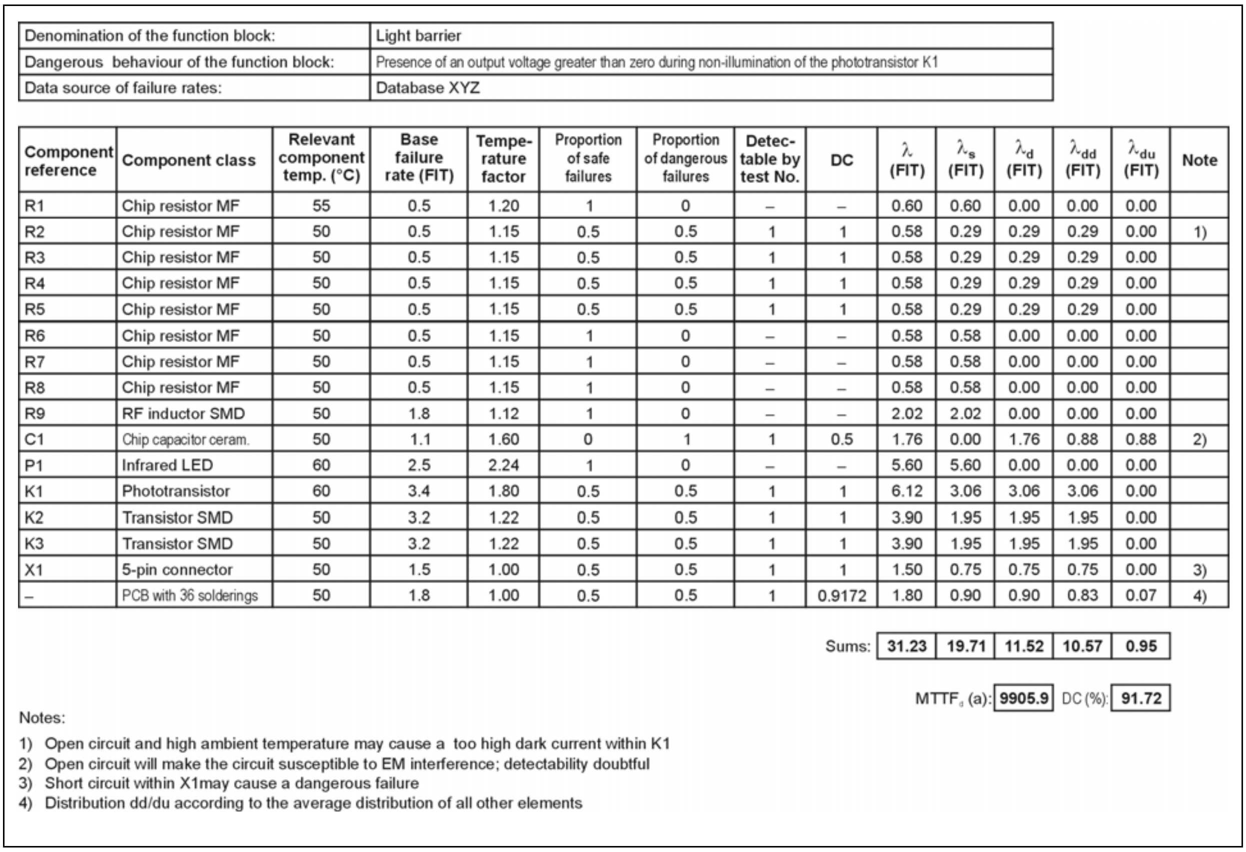
A quick source of generally conservative (pessimistic) estimations of failure rates can be found in EN ISO 13849-1, Annex C. In particular, a method is shown here by which failure rates for discrete, cyclically operating electromechanical, fluid power and mechanical components can be derived from the “B_{10}” values (see Table D.2 of this report).

Should a conservative estimate of the failure rate not be available, it must be ensured for each component that the value employed is valid under the conditions of use (temperature, current, voltage, power dissipation, etc.) for the application in question. The inherent heating effect must also be taken into account. Standard data sources, such as [3 to 6], provide measures by which the base failure rates applicable under defined reference conditions can be converted to values applicable under different conditions. Suitable conversion formulae (but not base failure rates) can be found in [7].

B2.4 Production of an FMEA on a function-block basis for quantification purposes

In the FMEA, the components of the function block are first assessed separately, and the complete assessment for the block is then derived from them. This is done for practical purposes in the form of a table which documents both the process and the results. The level of accuracy employed for performance of the FMEA may be varied; the accuracy employed is reflected in variation in the effort required for generation of the associated tables. One possible execution is shown by way of example in [8]. Binding rules do not exist. The variant shown in Figure B.3 represents a compromise between a high degree of accuracy and effort on one side and excessive simplification on the other, and takes the accuracy and availability of the data used into account. The figures used are assumed example values.

Figure B.3:
Intelligent form of execution of an FMEA table for the “light barrier” function block in Figure B.2



Denomination of the function block:	Light barrier
Dangerous behaviour of the function block:	Presence of an output voltage greater than zero during non-illumination of the phototransistor K1
Data source of failure rates:	Database XYZ

Component reference	Component class	Relevant component temp. (°C)	Base failure rate (FIT)	Temperature factor	Proportion of safe failures	Proportion of dangerous failures	Detectable by test No.	DC	λ (FIT)	λ_s (FIT)	λ_d (FIT)	λ_{dd} (FIT)	λ_{du} (FIT)	Note
R1	Chip resistor MF	55	0.5	1.20	1	0	–	–	0.60	0.60	0.00	0.00	0.00	
R2	Chip resistor MF	50	0.5	1.15	0.5	0.5	1	1	0.58	0.29	0.29	0.29	0.00	1)
R3	Chip resistor MF	50	0.5	1.15	0.5	0.5	1	1	0.58	0.29	0.29	0.29	0.00	
R4	Chip resistor MF	50	0.5	1.15	0.5	0.5	1	1	0.58	0.29	0.29	0.29	0.00	
R5	Chip resistor MF	50	0.5	1.15	0.5	0.5	1	1	0.58	0.29	0.29	0.29	0.00	
R6	Chip resistor MF	50	0.5	1.15	1	0	–	–	0.58	0.58	0.00	0.00	0.00	
R7	Chip resistor MF	50	0.5	1.15	1	0	–	–	0.58	0.58	0.00	0.00	0.00	
R8	Chip resistor MF	50	0.5	1.15	1	0	–	–	0.58	0.58	0.00	0.00	0.00	
R9	RF inductor SMD	50	1.8	1.12	1	0	–	–	2.02	2.02	0.00	0.00	0.00	
C1	Chip capacitor ceram.	50	1.1	1.60	0	1	1	0.5	1.76	0.00	1.76	0.88	0.88	2)
P1	Infrared LED	60	2.5	2.24	1	0	–	–	5.60	5.60	0.00	0.00	0.00	
K1	Phototransistor	60	3.4	1.80	0.5	0.5	1	1	6.12	3.06	3.06	3.06	0.00	
K2	Transistor SMD	50	3.2	1.22	0.5	0.5	1	1	3.90	1.95	1.95	1.95	0.00	
K3	Transistor SMD	50	3.2	1.22	0.5	0.5	1	1	3.90	1.95	1.95	1.95	0.00	
X1	5-pin connector	50	1.5	1.00	0.5	0.5	1	1	1.50	0.75	0.75	0.75	0.00	3)
–	PCB with 36 solderings	50	1.8	1.00	0.5	0.5	1	0.9172	1.80	0.90	0.90	0.83	0.07	4)
								Sums:	31.23	19.71	11.52	10.57	0.95	

$MTTF_d$ (a): 9905.9 DC (%): 91.72

Notes:

1) Open circuit and high ambient temperature may cause a too high dark current within K1
2) Open circuit will make the circuit susceptible to EM interference; detectability doubtful
3) Short circuit within X1may cause a dangerous failure
4) Distribution dd/du according to the average distribution of all other elements

The components of the function block are listed by row together with their failure rates. The usual unit for the failure rate is “FIT” (failures in time); 1 FIT = 10^{-9}/h. The only weighting factor indicated here for the base failure rate is the temperature factor. Other adjustment factors may justifiably be ignored when the components are on average electrically over-dimensioned, which is frequently the case. In such cases, their electrical load lies predominantly below the reference load upon which the base failure rate is based, with the result that the corresponding adjustment factors are < 1. Omission of these factors thus constitutes an estimation erring on the safe side and at the same time a saving in effort, since the precise electrical operating values for the components need not all be determined individually. As soon as it is known, however, that the load upon certain components lies above the reference load, the relevant adjustment factors must be considered. If the base failure rate of individual components predominates within the function block, which is often the case for example for processors and power semiconductors, precise examination and if applicable consideration of all necessary adjustment factors is necessary for the components concerned.

In the next stage, the total failure rate λ of each component is divided into the proportions λ_s ("safe" mode) and λ_d ("dangerous" mode). For this purpose, information such as the "dangerous failure mode" of the function block must be known (see above). A "purist" approach requires this to be performed in two steps. Firstly, the total failure rate is distributed between the various failure types (e.g. open circuit, short circuit, drift, change in function). In the second step, the proportions of each form of failure are assigned to λ_s or λ_d, according to whether the failure type concerned causes the function block to fail in its safe or unsafe mode. A continuation in function without change is regarded in this case as a safe-mode failure.

In practice, information on the distribution of the failure types of components is often contradictory, if available at all. The pragmatic solution followed in Figure B.3 is therefore appropriate, i.e. that of examining which of the following three cases applies to a component:

a) All failure types result in safe-mode failure of the function block, or have no impact upon its behaviour.

b) At least one failure type exists which causes the failure block to fail safely, and at least one failure type which causes it to fail dangerously.

c) All failure types cause the function block to fail in its dangerous mode.

In case a), the total failure rate λ is assigned to the safe mode failure rate λ_s (example: infrared LED P1). By the same token, in case c), the total failure rate λ is assigned to the dangerous mode failure rate λ_d (example: capacitor C1). In case b), the total failure rate λ is divided equally between λ_s and λ_d (example: transistor K2).

The simplified procedure shown in case b) is normally justified for components making only a small contribution to the total failure rate of the function block when it contains many such components. Individual components with an above average contribution to the total failure rate of the function block must be considered separately if appropriate. The failure rate may also be divided equally between λ_s and λ_d for complex integrated circuits such as processors. The same applies to soldering pads/printed circuit boards. Caution is required with discrete or low-integration components with a relatively high failure rate. Should for example a contactor or a power semiconductor contribute substantially to the total failure rate of the function block, failure should be assumed to be predominantly dangerous in cases of doubt. This is even more the case for elements of safety outputs which switch output currents.

For components intended to reinforce the circuit's resistance to disturbance influences (e.g. electromagnetic interference or excessive ambient temperature), it is advantageous to distinguish between two possible cases for assessment of the function block's behaviour. If the incidence of disturbance phenomena is merely "possible" and the function of the circuit measure is essentially to increase the availability of the device under (infrequent) unfavourable conditions, simultaneous presence of the "disturbance phenomenon" in the event of component failure need not be assumed during assessment of the function block behaviour. Conversely, should the intended operating mode of the device be associated with occasional to continuous presence of the disturbance or should this be anticipated in view of the typical operating conditions (e.g. installation within the range of known sources of electromagnetic interference or at a hot site), assessment of the component failure must allow a factor for the disturbance. The same applies to assessment of the scope provided by diagnostics measures for detection of failure of these components.

The next step in the method entails consideration for diagnostics. Only diagnostics relating to dangerous-mode failures (of the function block) are considered. Consideration for whether a test or, where applicable, several tests are capable of detecting these failures completely or in part need therefore be only given to components which exhibit a portion of dangerous-mode failures. The relevant effective test and the diagnostic coverage *DC* for the components, the latter indicating the detectable portion of dangerous mode failures, are entered in appropriate columns. Where the components concerned are discrete components, as in the example shown in Figure B.2, one of the two DC values “0” for “undetectable” or “1” for “detectable” can often be assigned to the dangerous failure of a single element. In the case of complex integrated components and of discrete components when its failure is capable of impairing the function of such a complex element, the component specific *DC* must be estimated in consideration of both the dangerous failure type and of the available test method. Support in this assessment is provided by Table E.2, in which DC values of 0% (“none”), 60% (“low”), 90% (“medium”) and 99% (“high”) are assigned for standard test methods. During assignment of a DC to a component, it must also be considered that an evaluation result of “detectable” is permissible only if the system is actually capable of performing the intended safety-oriented operation. Detection of a failure within a circuit, for example, is useless if it is rendered ineffective owing to a de-energization path that has already failed.

In the example shown, the components R1, R6 to R9 and P1 do not need to be considered with regard to the diagnostics aspect, since they are not capable of causing a dangerous-mode failure of the “light barrier” function block. The dangerous-mode failure portion of each of these components is 0. Dangerous-mode failure of elements R2 to R5, K1 to K3 and X1 is detected fully by “Test 1” (the only test in this example), i.e. when LED P1 is switched off for test purposes, the test detects an output voltage of > 0. The component-related DC value of “1” is therefore assigned to these elements. The situation is different for the capacitor C1, which has the function of suppressing frequent but not continuous electromagnetic interference (note: assumed for the purpose of this example). Drift failures (limited changes in capacitance) are not critical; a short-circuit, however, results in the output (terminal X1.2) being incapable of de-energization (dangerous failure mode of the function block). A short-circuit on C is detected by Test 1. In the event of an open circuit on C1, the electromagnetic interference is transported via K2 and K3 to the output of the function block. It is unclear how the downstream circuit will interpret this high-frequency alternating signal, and also whether the disturbance phenomenon is present during the test. In the worst case, the non-suppressed interference results in the output signal with superimposed disturbance not being interpreted by the downstream circuit as a demand upon the safety function, despite phototransistor K1 not being illuminated (= dangerous failure of the “light barrier” function block). Should the fault not be present at the time of the test, Test 1 is not able to detect the capacitor open circuit. Since no reliable information on the failure-type distribution is available for the capacitor, it is assumed (the non-critical drift failures being disregarded) that short circuits and open circuits each account for 50% of the failures. Both failure types lead to a dangerous failure of the function block; only short-circuiting of the capacitor, i.e. (an estimated) half of all dangerous capacitor failures, are however reliably detectable. The component-specific diagnostic coverage is thus estimated at 50% or 0.5.

The printed circuit board with the soldering pads can introduce short circuits and open circuits into the circuit at various points. The pragmatic approach, implemented in Figure B.3, for estimation of the DC value for soldering pads and printed circuit boards consists in assigning the average DC value to them which is produced for all other components of the function block from the formula $DC = \Sigma\lambda_{dd}/\Sigma\lambda_{d}$. The inclusion of the printed circuit board and soldering pads does not therefore have an influence upon the DC value which is calculated for the complete function block.

In each row of the table, i.e. for each component:

λ = temperature factor × base failure rate (if applicable with further correction factors, see above)

λ_s = proportion of safe failures × λ

λ_d = proportion of dangerous failures × λ

λ_{dd} = $DC \times \lambda_d$

λ_{du} = $(1 - DC) \times \lambda_d$

These λ values are summed by column in the table. The sum λ_d and the sums λ_d and λ_{dd} respectively yield the $MTTF_d$, i.e. the mean time to a dangerous failure of the function block, and the DC of the function block:

$$MTTF_d = 1/\lambda_d$$

$$DC = \lambda_{dd}/\lambda_d$$

The only input values required for determining the PL for one of the designated architectures in accordance with Sections 6.2.3 to 6.2.7 are the MTTF_d and DC values. The example shown yields an MTTF_d value of 9,905.9 years and a DC of 91.72%. If a different quantification method is employed, values from the FMEA table such as λ_{dd} and λ_{du} may also be used.

B3 Parts count method

Time and effort can be saved by use of a simpler method instead of an FMEA. If a detailed analysis of the circuit behaviour is not performed for the various failure types of the individual elements, the parts count method is an alternative (cf. Annex D of this report). This method was originally found in the MIL Handbook 217F (cf. [6]), and a variant of it is described in EN ISO 13849-1, Annex D.1. If at the same time a relatively conservative (high) failure rate is assumed, the failure rates require no adjustment to the actual operating conditions. In addition, a dangerous failure proportion of 50% – with regard to the function block – is frequently assumed for many elements. If the columns for weighting and proportioning of the failure rates, which are not required, are omitted from the FMEA table, the table is simplified. Compared to the FMEA results, the parts count method normally delivers poorer (lower) MTTF_d

values, since higher failure rates are generally input, and components are also considered which are capable of causing only safe-mode function-block failures. If the parts count principle is applied to the example described above (light barrier), and at the same time the failure rates from Figure B.3 are adjusted for temperature and a proportion of dangerous failures of 50% for all elements is assumed, the resulting MTTF_d value is 7,310.8 years. This value is approximately 26% poorer than the FMEA result. The inferior value is due in this example solely to the omission of a circuit analysis. If a DC value is required for the function block, the component-related *DC* for each element or, for example with reference to Annex E, the *DC* of the entire function block must be estimated, as with the FMEA.

The FMEA solution for quantification purposes presented in this annex of the Report with reference to an electronic circuit can be transferred to other technologies. It can therefore be applied in the same formal way for example for mechanical, hydraulic and pneumatic systems.

References

[1] *Goble, W.M.*: Control systems safety evaluation and reliability. 2^{nd} ed. Ed.: Instrumentation, Systems, and Automation Society (ISA), Research Triangle Park, North Carolina, 1998

[2] IEC 60812: Analysis techniques for system reliability – Procedure for failure mode and effects analysis (FMEA) (01.06)

[3] SN 29500: Failure rates of components – Expected values. Ed.: Siemens AG, Center for Quality Engineering, Munich 1994 to 2005

[4] IEC/TR 62380 (formerly UTE C 80-810): Reliability data handbook – Universal model for reliability prediction of electronics components, PCBs and equipment (08.04)

[5] Telcordia SR-332, Issue 2: Reliability Prediction Procedure for Electronic Equipment. Ed: Telcordia Technologies Inc., Piscataway, New Jersey

[6] 217Plus (successor to the “MIL-Handbook 217F”). Ed.: Reliability Information Analysis Center (RIAC), Utica, New York, 2006

[7] IEC 61709: Electronic components – Reliability – Reference conditions for failure rates and stress models for conversion (10.96)

[8] IEC 61508-6: Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 6: Guidelines on the application of IEC 61508-2 and IEC 61508-3, Annex C (04.00)

Annex C: Fault lists, fault exclusions and safety principles

C1 Fault lists

The faults and possible fault exclusions which are to be assumed for mechanical, pneumatic, hydraulic and electrical components during the validation of SRP/CS can be found in fault lists in EN ISO 13849-2 [1], Annexes A to D. Individual product standards such as EN 61496-1 [2], Annex B and IEC 60947-5-3 [3], Annex A also contain fault lists (in this case, for electrical components), the data of which deviates in part from those in EN ISO 13849-2.

Document 340 220 [4] explains the background and origins of the fault lists (reproduced at the end of this annex).

C2 Fault exclusions

Without the assumption of fault exclusions, some safe control systems would not be achievable at reasonable expense. Reasons for fault exclusion include, in particular, the physical impossibility of a certain type of fault or the technical improbability of a fault, and also good engineering practice (see also Section 7.3 of EN ISO 13849-1). Fault exclusions are also possible for new components. The precise reasoning for each fault exclusion must be stated in the technical documentation. EN ISO 13849-2 describes possible fault exclusions for certain discrete components, where considered permissible. The information in the following examples has been updated where required to bring it into line with standard practice. These aspects are being submitted as proposals for amendments in the current revision of the standard.

C2.1 Examples of fault exclusions on components

C2.1.1 Fluid power components

Similar fault exclusions are frequently formulated for pneumatic and hydraulic components. Fault exclusions specific to one form of fluid power also exist, however.

Example of common fault exclusions on fluid power components:

- Directional control valves

  The fault assumption “failure to switch or failure to switch completely” can be excluded under the following conditions:

  Positive mechanical operation of the moving parts, provided the actuating force is sufficiently high. On hydraulic directional control valves, a fault exclusion can be formulated for the failure of a special type of cartridge valve (refer to the remarks in EN ISO 13849-2, Table C.3) to open when it controls the main volumetric flow of the pressure medium in conjunction with at least one further valve.

C2.1.2 Electrical components

- Optocouplers

  EN ISO 13849-2, Table D.20 states that the fault assumption "short-circuit between any two input and output terminals" can be excluded under the following conditions: *"The base material used should be according to IEC 60249 and the creepage distances and clearances should be dimensioned at least to IEC 60664:1992 with at least pollution degree 2/installation category III."*

  Here, the requirements have clearly been assigned incorrectly during drafting of the standard. For this reason the BGIA, as a notified test body, applies the following two requirements in practice for formulation of a fault exclusion. These requirements have also been adopted in IEC 61800-5-2 [5]:

  - The optocoupler arrangement satisfies overvoltage category III in accordance with IEC 60664-1:1992, Table 1. If an SELV/PELV power supply is employed, pollution degree 2/overvoltage category II is sufficient.

  - Measures must be in place which ensure that an internal failure of the optocoupler cannot lead to a rise in the temperature of its insulating material.

- Printed circuit board/populated printed circuit board

  In accordance with the standard, the fault assumption "short-circuit between adjacent tracks/points of contact" can be excluded provided the following conditions are met:

  - A base material in accordance with IEC 60249 is employed for the printed circuit board.

  - Creepage distances and clearances are dimensioned in accordance with IEC 60664-1:1992 to pollution degree 2/overvoltage category III.

  - Also accepted in practice: provided the power supply satisfies the requirements for SELV/PELV, pollution degree 2 and overvoltage category II are sufficient for dimensioning of the creepage distances and clearances. The clearance must not be less than 0.1 mm, however.

  - The populated printed circuit board must be installed in an enclosure assuring ingress protection of at least IP 54, and the conductive side must feature a varnish or other form of protective coating which is resistant to ageing and which covers all tracks.

  - In practice, it is now also acceptable for a high-quality solder resist or similar to be employed for the ageing-resistant varnish/protective coating. Additional population of printed circuit boards in accordance with IEC 60664-3 may reduce the pollution degree forming the basis of the assumption, and thus also the required creepage distances and clearances.

- With regard to exclusion of the "short-circuit" fault, current practice necessitates that allowance be made for the possible formation of tin whiskers when lead-free soldering processes and components are used. Tin whiskers are conductive, may be several 100 µm in length, and can cause a short-circuit between tracks or points of contact. The risk of such whisker growth must therefore be evaluated. Should the risk be too high, fault exclusion is not permissible. The sources [6] and [7] may be useful for evaluation purposes.

- Conductors/cables

  The fault assumption of a "short-circuit between any two conductors" can be excluded under the following conditions. The conductors:

  - are laid permanently (fixed) and with protection against external damage (e.g. in the form of cable ducts, high-strength conduit); or
  - are laid in separate multicore cables; or are laid within an electrical compartment, provided that both the conductors and the compartment satisfy the relevant requirements, see EN 60204-1; or
  - are protected individually by earthing.

- Electromechanical position switches, hand switches

  The exclusion of the fault "failure of contacts to open" can be assumed under the following condition:

  - Contacts to IEC 60947-5-1: 2003, Annex K open of their own accord.

    Note: this fault exclusion applies only to the electrical part of the switch (the fault exclusion is from the fault list for the electrical system). The mechanical part of the switch – for example the separate actuator fitted to the safety guard for a Type 2 switch, the dog for a Type 1 switch, or the mechanical components within the switch – must be considered in addition. For this reason, Part 1 of EN ISO 13849, Table C.1 contains B_{10d} values despite this "electrical" fault exclusion.

C3 Basic safety principles

Basic safety principles are governed in Tables A.1, B.1, C.1 and D.1 (including D.2) of the informative annexes of EN ISO 13849-2.

C3.1 Applicable to all technologies

- Use of suitable materials and manufacturing processes

  Materials and processes for manufacture and treatment are selected with consideration for the use and stresses.

- Proper dimensioning and geometry of all components

  All components are selected in consideration of their compatibility with the anticipated operating conditions. Further criteria include switching capacity, switching frequency, electric strength, pressure level, dynamic pressure behaviour, volumetric flow, temperature and viscosity of the hydraulic fluid, type and condition of the hydraulic fluid or compressed air.

- All components are resistant to the environmental conditions and relevant external influences.

  The SRP/CS is designed such that it can perform its functions under the external influences which are usual for the application. Important criteria include mechanical influences, climatic influences, the degree of sealing of the enclosure, and the resistance to electromagnetic interference.

- Principle of de-energization (closed-circuit current principle)

  The safe state is attained by removal of the control signal (voltage, pressure), i.e. by de-energization. Important criteria include the safe state when the energy supply is interrupted, or effective spring resetting on valves in fluid power technology.

- Protection against unexpected start-up

  Unexpected start-up, caused for example by stored energy or upon restoration of the power supply, is avoided.

C3.2 Examples of basic safety principles in fluid power technology

- Pressure limitation

  The pressure within a system or in subsystems is generally prevented from rising beyond a specified level by one or more pressure-relief valve(s). Pressure-control valves with secondary ventilation are primarily employed for this purpose in pneumatics.

- Measures for the avoidance of impurities in the pressure medium

  The required purity grade of the pressure medium for the components used is attained by a suitable facility, generally a filter. In pneumatics, suitable dehumidification is also required.

C3.3 Examples of basic safety principles in electrical technology

- Proper connection of the protective earth conductor

  One side of the control circuit, one terminal of each electromagnetically actuated device or one terminal of other electrical devices is connected to a protective earth conductor. This side of the device is not therefore used for example for deactivation of a hazardous movement. A short-circuit to ground cannot therefore result in (undetected) failure of a de-energization path.

- Suppression of voltage spikes

  A facility for the suppression of voltage spikes (RC element, diode, varistor) is connected in parallel with the load (not in parallel with the contacts).

C3.4 Examples of basic safety principles in programmable systems/software

EN ISO 13849-2 does not describe basic safety principles for the use of programmable systems and software. The basic measures for SRESW and SRASW in accordance with Sections 4.6.2 and 4.6.3 of the standard may however be regarded as basic safety principles (refer also to Section 6.3). A further measure is the monitoring of the program sequence for detection of a defective sequence of commands/software modules which may occur despite all care taken during verification and validation. Program sequence monitoring is generally implemented by means of an external, cyclically retriggered watchdog which must be capable of placing the SRP/CS in a defined safe state in the event of a defective program sequence.

C4 Well-tried safety principles

Tables A.2, B.2, C.2 and D.3 in the informative annexes of EN ISO 13849-2 address well-tried safety principles. Well-tried safety principles are employed in order to minimize or exclude critical faults or failures and thus to reduce the probability of faults or failures which influence the safety function.

C4.1 General well-tried safety principles for all technologies

- Over-dimensioning/safety factor

  All equipment is subjected to loading below its rated values. The objective is to reduce the probability of failure.

- Positive actuation

  Reliable actuation by rigid mechanical parts with positive rather than sprung connections. The objective is to attain reliable transmission of commands, for example by the direct opening of a contact when a position switch is actuated, even should the contact be welded.

- Limiting of electrical and/or mechanical parameters

  Force, distance, time, and rotational and linear speeds are reduced to permissible values by electrical, mechanical or fluid power equipment. The objective is to reduce the risk by means of an improved hazard control.

C4.2 Examples of well-tried safety principles in fluid power technology

- Secure position

  The moving element of a component is held mechanically in a possible position (frictional restraint is not sufficient). Force must be generated in order for the position to be changed.

- The use of well-tried springs

  EN ISO 13849-2, Table A.2 contains detailed requirements for well-tried springs.

C4.3 Examples of well-tried safety principles in electrical technology

- Limiting of electrical parameters

  Limiting of voltage, current, energy or frequency, for the avoidance of an unsafe state

- Avoidance of undefined states

  Undefined states in the SRP/CS must be avoided. The SRP/CS must be designed such that its state can be predetermined during normal operation and under all anticipated operating conditions. This is to be achieved for example by the use of components with defined response behaviour (switching thresholds, hysteresis) and with a defined sequence of operations.

- Separation of non-safety and safety functions

  In order to prevent unanticipated influences upon safety functions, the functions concerned are implemented separately from non-safety functions.

C4.4 Examples of well-tried safety principles in programmable systems/software

EN ISO 13849-2 does not describe well-tried safety principles for the use of programmable systems and software. The additional measures for SRESW and SRASW in accordance with Sections 4.6.2 and 4.6.3 of the standard may however be regarded as well-tried safety principles (refer also to Section 6.3). A further well-tried safety principle is the use of self-tests for the detection of faults in complex components such as microcontrollers. Table E.1 of the standard for estimation of the level of diagnostic coverage lists self-tests of this kind, such as memory tests and CPU tests. Information on the implementation of such tests can also be found in the relevant BGIA Report [8]. Depending upon the application, “fault detection by the process” and “fault detection by comparison between channels” may be regarded as well-tried safety principles.

C5 Well-tried components

Well-tried components for mechanical and electrical systems are dealt with by Tables A.3 and D.4 of the informative annexes of EN ISO 13849-2. Well-tried components are used in order to minimize or exclude critical faults or failures and thus to reduce the probability of faults or failures which impact upon the safety function. In accordance with the provisions for Category 1, general criteria for a well-tried component are that it:

a) has been widely used in the past with success in similar applications; or

b) has been manufactured and verified with the application of principles which indicate its suitability and reliability for safety-related applications.

Complex electronic components (such as PLCs, microprocessors, ASICs) cannot be regarded as well-tried in the context of the standard. Classification as a well-tried component is dependent in part upon the application: a component may be considered well-tried in certain applications, whereas in other applications this must be excluded, for example owing to the environmental influences.

C5.1 Example of a well-tried component in mechanical technology

- Spring

  A spring is deemed to be a well-tried component when the provisions concerning well-tried safety principles for the application of well-tried springs in EN ISO 13849-2, Table A.2 are observed, and the technical provisions for spring steels to ISO 4960 [9] have also been considered.

C5.2 Examples of well-tried components in fluid power technology

EN ISO 13849-2 states no well-tried components for fluid power technology. The property of being well-tried is particularly dependent upon the application in question and upon observance of the requirements for well-tried components in Category 1 and the requirements of EN 982 [10] and EN 983 [11].

Examples of well-tried components in a safety context are:

- Directional control valves, stop valves and pressure valves

C5.3 Examples of well-tried components in electrical technology

- Fuse/miniature circuit-breaker

  Fuses and miniature circuit-breakers are facilities for overcurrent protection which interrupt an electrical circuit in the event of an excessively high current, caused for example by an insulation fault (principle of de-energization). Fuses and miniature circuit-breakers have for decades provided effective protection against overcurrents. Comprehensive provisions exist governing fuses and miniature circuit-breakers [12; 13]. Provided they are used as intended and are correctly rated, failure of fuses and miniature circuit-breakers can virtually be excluded.

- Emergency off device/emergency stop device

  Devices for emergency switching off and emergency stop in accordance with EN ISO 13850 [14] are employed for the initiation of action in an emergency. Both types of device feature auxiliary switches with direct opening action for interruption of the energy supply in accordance with Annex K of IEC 60947-5-1 [15]. A distinction is drawn between two types of auxiliary switch with direct opening action:

  - Type 1: with only one contact element, in the form of a direct opening contact

  - Type 2: with one or more break contacts and possibly with one or more make contacts and/or one or more changeover contacts. All break contacts, including the contact-breaking parts of the changeover contacts, must feature direct opening contact elements.

- Switches with positive mode of actuation (direct-opening)

  This particular type of switch is available commercially as a pushbutton, position switch, and selector switch with cam actuation, for example for the selection of operating modes. These switches have proved effective over many decades. They are based upon the well-tried safety principle of the positive mode of actuation by direct opening contacts. As a well-tried component, the switch must satisfy the requirements of IEC 60947-5-1, Annex K [15].

- Further non-complex and non-programmable components, owing to their failure modes being predictable. Examples are passive components, resistors, diodes, transistors, thyristors, operational amplifiers and voltage regulators.

References

[1] EN ISO 13849-2: Safety of machinery – Safety-related parts of control systems – Part 2: Validation (08.03)

[2] EN 61496-1: Safety of machinery – Electro-sensitive protective equipment – Part 1: General requirements and tests (05.04)

[3] IEC 60947-5-3: Low-voltage switchgear and controlgear – Part 5-3: Control circuit devices and switching elements – Requirements for proximity devices with defined behaviour under fault conditions (PDF) (03.99 + A1:01.05)

[4] *Bömer, T.; Grigulewitsch, W.; Kühlem, W.; Meffert, K.; Reuß, G.*: Fehlerlisten für sicherheitsbezogene Bauelemente – Bei der Prüfung unterstellte Fehlerarten. In: BGIA-Handbuch Sicherheit und Gesundheitsschutz am Arbeitsplatz.

Kennzahl 340 220. 48th suppl. V/06. Ed.: BGIA –Institut für Arbeitsschutz der Deutschen Gesetzlichen Unfallversicherung, Sankt Augustin. Erich Schmidt, Berlin, 1985 – loose-leaf ed.
www.bgia-handbuchdigital.de/340220

[5] IEC 61800-5-2: Adjustable speed electrical power drive systems – Part 5-2: Safety requirements – Functional (07.07).

[6] Test method for measuring whisker growth on tin and tin alloy surface finishes, JESD22A121A. Ed.: JEDEC Solid State Technology Association, Arlington, Virginia, USA, 2008.
www.jedec.org/download/search/22a121A.pdf

[7] Environmental acceptance requirements for tin whisker susceptibility of tin and tin alloy surface finishes, JESD201A. Ed.: JEDEC Solid State Technology Association, Arlington, Virginia, USA, 2008.
www.jedec.org/download/search/JESD201A.pdf

[8] *Mai, M.; Reuß, G.*: Self-tests for microprocessors incorporating safety functions or: “Quo vadis, fault?” BGIA Report 7/2006e. Ed.: BGIA – Institut für Arbeitsschutz der Deutschen Gesetzlichen Unfallversicherung, Sankt Augustin 2009.
www.dguv.de/bgia, Webcode e91093

[9] ISO 4960: Cold-reduced carbon steel strip with a mass fraction of carbon over 0.25% (12.07)

[10] EN 982: Safety of machinery – Safety requirements for fluid power systems and their components – Hydraulics (04.96)

[11] EN 983: Safety of machinery – Safety requirements for fluid power systems and their components – Pneumatics (04.96)

[12] IEC 60269-1: Low-voltage fuses – Part 1: General requirements (11.06).

[13] IEC 60127-1: Miniature fuses – Part 1: Definitions for miniature fuses and general requirements for miniature fuse-links (06.06)

[14] EN ISO 13850: Safety of machinery – Emergency stop – Principles for design (11.06)

[15] IEC 60947-5-1: Low-voltage switchgear and controlgear – Part 5-1: Control circuit devices and switching elements – Electromechanical control circuit devices (11.03)

Translation of:
Bömer, T.; Grigulewitsch, W.; Kühlem, W.; Meffert, K.; Reuß, G.: Fehlerlisten für sicherheitsbezogene Bauteile – Bei der Prüfung unterstellte Fehlerarten. In: BGIA-Handbuch Sicherheit und Gesundheitsschutz am Arbeitsplatz. Kennzahl 340 220. 48th suppl. V/06. Ed.: BGIA – Institut für Arbeitsschutz der Deutschen Gesetzlichen Unfallversicherung, Sankt Augustin. Erich Schmidt, Berlin 1985 – loose-leaf ed.
www.bgia-handbuchdigital.de/340220

Fault lists for safety-related components – Fault types assumed during testing –

1 Introduction

On technical equipment on which failure of a control or protective system could result in persons being injured, the fault-mode behaviour is subject to special safety requirements. Examples are familiar from the technical rules and standards of various sectors of engineering, such as machine and plant construction, traffic and transport technology, medical devices, and power generation and distribution. The Machinery Directive [1] also requires that control systems be designed and constructed in such a way that, in particular, logic faults do not lead to hazardous situations.

The potential effects of faults in safety-related control systems are shown by the safety information and worksheet 330 250 of this manual [2].

The safety requirements formulated in technical rules, accident prevention regulations and standards vary strongly according to the application concerned. They extend from, in the simplest case, organizational measures such as regular function tests performed deliberately by the user, through automatic test circuits, to control systems with watchdog functionality in which faults are detected automatically. The concept of fault consideration refers to the totality of considerations which are required to describe the safety-related behaviour of a facility in the event of a fault and to test it in a practical manner. One of the most important questions in the context of fault consideration is which faults must be assumed on components. Agreement is required on this issue in order for the developer to be provided with binding criteria for the design of his safety concept for the control system. At the same time, the agreement regarding faults is to ensure that tests of the same item by different test bodies and testers do not produce different results.

What faults, then, should be included in a fault list of this kind? Were all theoretically conceivable faults of a component to be assumed during the fault consideration, not only would the scope of testing be enormous; testing would in some cases not be possible at all. Assumed faults and fault exclusions have been specified in the past in many areas of application, for example in railway signalling. These fault lists were not readily transferable to general industrial applications, however, and their detailed provisions were in some cases contradictory. Yet the majority of standards and safety rules contained no provisions governing the specific faults to be assumed during the fault consideration.

2 Requirements for a fault list

In order to create a consistent basis upon which the safety aspects of control systems may be tested, the BGIA – Institute for Occupational Safety and Health produced a compilation of the fault types of electrical, hydraulic and pneumatic components assumed for test purposes, and published it in this manual in 1987 and 1990. These collections for the industrial machinery and plant sector have been revised several times over the years, and supplemented with information from the relevant literature and technical rules. The lists, which had been proved over many years in practical application prior to their publication, represent a compromise between different and in some cases contradictory requirements, which will be explained as follows:

High degree of fault coverage

The faults assumed for fault-mode testing should cover as many of the potential faults as possible. The higher the degree of fault coverage, the lower the risk of potentially hazardous fault types being overlooked.

Feasibility of performance

The more complex a component, the greater the variety of possible faults is. The draft general rules for safe signalling circuits and electronic devices, for example, describe 51 fault types for a transistor alone; the number of different possible faults is astronomically high even for simple integrated circuits. For the performance of fault-mode testing, the theoretically possible fault types must therefore be constrained. At the same time, it must be ensured that a high level of fault coverage is nevertheless attained in terms of the impact of faults. This is achieved for example by the assumption of a worst-case fault on a component or on an entire assembly. A worst-case fault means that the worst possible fault from a safety perspective is assumed at the outputs of the component or assembly.

Possibility of fault injection

Where possible, faults should be assumed which can also be injected into the original circuit to be tested. This is not always possible, as for example in the case of certain internal drift processes in semiconductor components or miniaturized electronic components. Depending upon the circuit principle, there may be no alternative in this case to determining the effects of such faults by analysis and simulation. In fluid-power systems, the cause of a fault frequently cannot be simulated realistically with justifiable effort. The contamination of the pressure medium by solid matter is an example. The effects of the cause of the fault, such as sticking of the moving part, can however generally be injected in the form of faults.

Reproducibility

The injected faults should, to the extent possible, be selected such that they deliver a reproducible test result.

Economic efficiency

The assumed faults should permit rational fault injection. Injection of the faults into the component or original circuit under consideration always involves a substantially greater investment in time than a theoretical fault consideration, however. For this reason, theoretical fault consideration should be preferred for components and circuits which can easily be assessed.

Non-manufacturer-specific faults

The types of injected fault should be largely independent of the manufacturer of the components. Fault exclusions can however generally be formulated only for particular designs, and are therefore in some cases indirectly specific to a certain manufacturer.

Realistic fault exclusions

Without the assumption of specific fault exclusions, safe control systems are not achievable. With the exception of a small number of cases for which physical reasons exist, any such fault exclusion represents a compromise between the safety requirements on the one hand, and what is technically and economically feasible on the other. Reasons for fault exclusions particularly include:

- The physical impossibility of a certain type of fault (for example: a strong increase in the capacitance of a capacitor, or an increase in the volumetric flow of a fixed-displacement pump in the absence of changes to the operating and drive parameters)

- Good engineering practice or experience independent of the application (for example: mechanical linking on relays or sudden breakage of a valve piston into a large number of pieces)

- Technical and economic aspects which are specific to the application and thus depend upon the specific risk of the application (for example: short-circuit on externally routed cables or switching of a valve in the absence of an actuating signal on applications involving a relatively low risk)

The first two reasons stated for a fault exclusion are the normal case. More far-reaching fault exclusions are nevertheless possible on some applications. These additional fault exclusions are based in particular upon the probability of incidence for the faults in question. The probability can be demonstrated by actual failure rates or by relevant plant experience.

3 Standardization of fault lists

The fault lists formerly listed in the safety information and worksheets 340 220 and 340 225 for electrical, hydraulic and pneumatic components have been adopted with minor adjustments in the European/international standard EN ISO 13849-2 [3]. For the validation of safety-related control components, Annexes A to D contain general fault lists for mechanical, pneumatic, hydraulic and electrical components. These lists now form the basis for testing to EN ISO 13849-1 [4].

Fault lists can also be found in some product standards for the machinery sector, for example in Annex B of EN 61496-1 [5] and in IEC 60947-5-3 [6] (for electrical components in these cases); these lists do not differ significantly from that for electrical components in [3]. Part 2, Table A.1 of IEC 61508 [7] contains a very short, general list of faults or failures which must be detected during operation or which must be analysed for determination of the safe failure fraction. This list is interesting with regard to the individual elements of a microprocessor system, e.g. main processor (CPU), clock and memory.

References

[1] Directive 98/37/EC of the European Parliament and of the Council of 22 June 1998 on the approximation of the laws of the Member States relating to machinery. OJ EC L 207 (1998), p. 1.

[2] *Börner, F.; Kreutzkampf, F.:* Unfälle und Störfälle, verursacht durch das Versagen von Steuerungen. In: BGIA-Handbuch Sicherheit und Gesundheitsschutz am Arbeitsplatz. Kennzahl 330 250. 22nd suppl. VI/94. Ed.: BGIA – Institut für Arbeitsschutz der Deutschen Gesetzlichen Unfallversicherung, Sankt Augustin. Erich Schmidt, Berlin 1985 – loose-leaf ed.

[3] EN ISO 13849-2: Safety of machinery – Safety-related parts of control systems – Part 2: Validation. (08.03)

[4] EN ISO 13849-1: Safety of machinery – Safety-related parts of control systems – Part 1: General principles for design (11.06)

[5] EN 61496-1: Safety of machinery – Electro-sensitive protective equipment – Part 1: General requirements and tests (05.04)

[6] IEC 60947-5-3: Low-voltage switchgear and controlgear – Part 5-3: Control circuit devices and switching elements – Requirements for proximity devices with defined behaviour under fault conditions (PDF) (03.99 + A1:01.05)

[7] IEC 61508-2: Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 2: Requirements for electrical/electronic/programmable electronic safety-related systems (05.00)

Annex D: Mean time to dangerous failure (*MTTF*$_d$)

D1 What does "*MTTF*$_d$" mean?

The mean time to dangerous failure *MTTF*$_d$ describes the reliability of the parts used in a control system, and is one of several parameters which are used to determine the Performance Level. The *MTTF*$_d$ is defined in EN ISO 13849-1 as the "expectation of the mean time to dangerous failure". This emphasizes several aspects:

- *MTTF*$_d$ is a statistical value, i.e. a value of empirical origin, one which in no way means "guaranteed lifetime", "failure-free time", or the like.
- *MTTF*$_d$ has the physical dimension of a period of time, and is generally stated in years.
- Only dangerous-mode failures are relevant, i.e. failures which impair execution of the safety function. Should the safety function be executed by several channels (redundancy), a "dangerous failure" occurs even if only one channel is affected.

D1.1 Bath-tub life curve and constant failure rate

Component reliability is commonly described in terms of failure rates, abbreviated λ (and by analogy λ_d for dangerous failures only), the usual unit being FIT (failures in time, i.e. number of failures in 10^9 component hours, 1 FIT = 10^{-9} per hour). This failure rate describes the rate, at a particular point in time, at which functional components fail. In other words, the number of failures per unit time is divided by the number of components which at the point in time concerned have not yet suffered failure. The failure mode of many types of components (particularly electronic components) as a function of time takes the form, to a greater or lesser degree, of a "bath-tub life curve" [1], see Figure D.1 (page 316).

A greater number of components generally fail at the beginning of the mission time. These early failures dominate only for a short period. Once the recommended mission time has been exceeded, the failures begin to rise again. In the mid-range of the usual mission time, a plateau of a constant failure rate is often observed, particularly for electronic components. Random failures are typical for this phase. Even components which are affected more strongly by wear than by random failures, such as electromechanical or pneumatic components, can often be described over their mission time by the assumption of a constant failure rate estimated erring on the safe side. Early failures are generally disregarded, since components exhibiting pronounced early failure patterns do not satisfy the availability requirements for a machine control system and are therefore not generally significant on the market. Suitable measures for the reduction of early failures are premature ageing (burn-in), selection, and optimization of the manufacturing process. In the interests of simplicity, constant failure rates within the mission time are therefore generally assumed in EN ISO 13849-1.

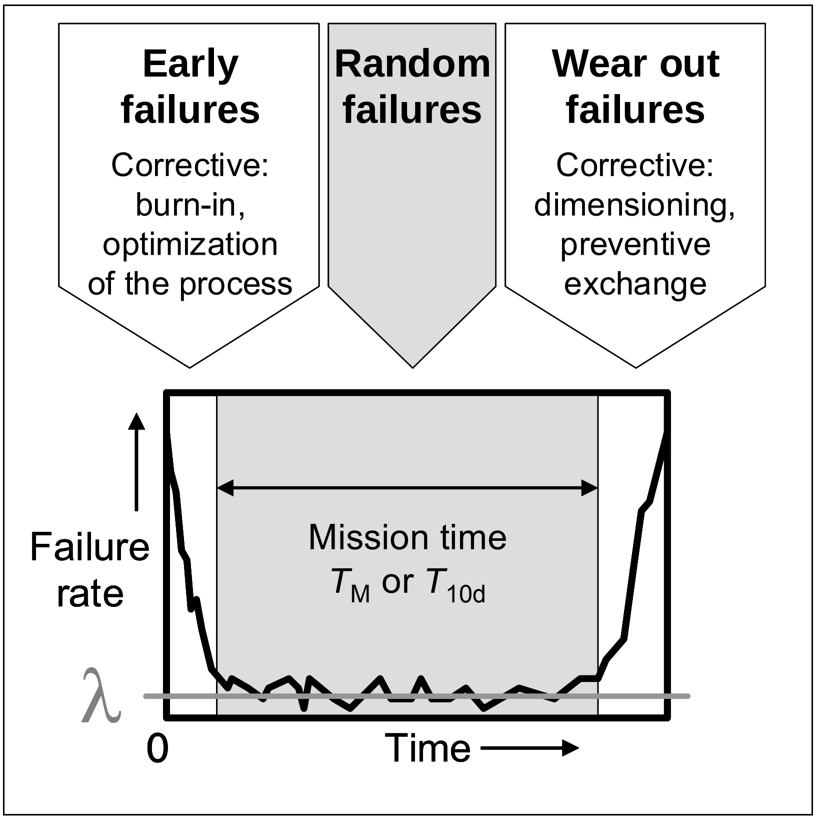


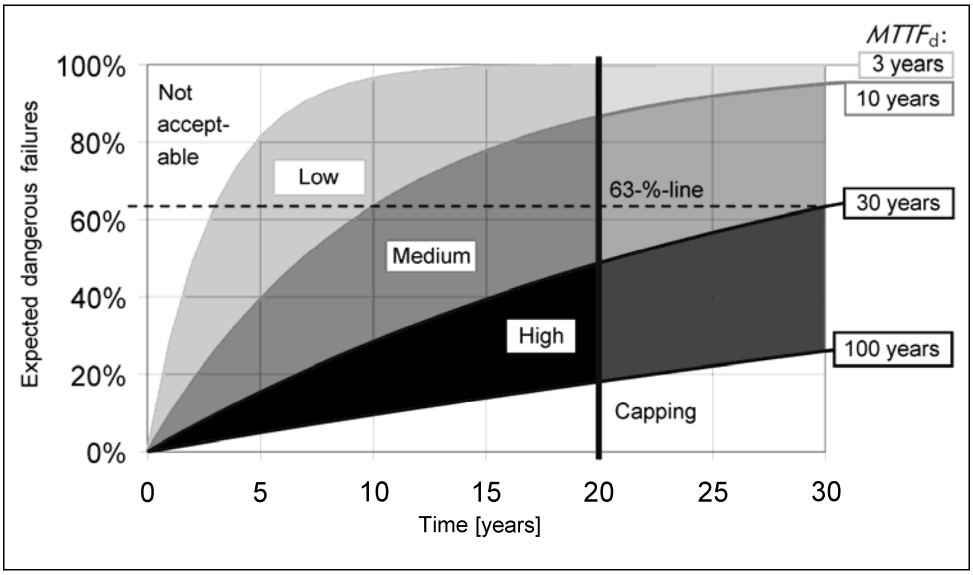
Figure D.1:
“Bath-tub life curve” of the failure rate

The advantage of this assumption is that subsequent mathematical analysis is considerably simplified as a result, and forms the basis for the Markov modelling of the designated architectures upon which the bar chart/the simplified method of EN ISO 13849-1 are based. A constant failure rate results mathematically in a reliability curve which falls exponentially over the mission time, and in an anticipated value for the time to failure ($MTTF_d$) which corresponds to the reciprocal of the failure rate, i.e.:

$$MTTF_d = \frac{1}{\lambda_d} \qquad (1)$$

At a constant failure rate, the $MTTF_d$ is therefore equivalent to statement of a failure rate, whilst being much more illustrative. Whereas the practical significance of an FIT value is not very illustrative, statement of an anticipated time in years conveys the quality of components more graphically. Figure D.2 shows the statistically anticipated development of the proportion of dangerous failures over the mission time for four different $\mathrm{MTTF_d}$ values. A further mathematical relationship can be observed here: at attainment of the $\mathrm{MTTF_d}$ mark on the time axis, a statistical average of approximately 63% of all initially intact components have failed dangerously (not 50%, since although more components fail prior to attainment of the $MTTF_d$, the remaining, intact components with residual operating times in some cases of several times the $MTTF_d$ are of greater statistical influence).

Figure D.2:
Illustration of the *MTTF*$_d$



The simplified quantification method to EN ISO 13849-1 assumes a usual mission time not exceeding 20 years for components in safety control systems in machine construction. Consequently, and with knowledge of the characteristic of the failure rate over time (Figure D.1), it becomes clear that a declared MTTF$_d$ value should be understood only as an illustrative indicator of the level of reliability within the mission time, and that it serves neither as a guarantee of a failure-free period before the *MTTF*$_d$ is reached, nor as a precise prediction of the point in time at which an individual component will fail. Once the wear phase is reached, the failure behaviour changes fundamentally and can no longer be described realistically by a constant failure rate.

D1.2 Division into classes and capping

The assumption of an *MTTF*$_d$ for each component of relevance to safety (where reasons are not given for a fault exclusion) is a condition for the following steps, by which the *MTTF*$_d$ of each channel is produced, first at block and then at channel level. At channel level, EN ISO 13849-1 proposes division into three typical MTTF$_d$ classes (Table D.1, see page 318). These classes are intended to cancel out minor differences between the calculated MTTF$_d$ values, which in any case become irrelevant within the statistical uncertainty. They also serve to retain the equivalence to the other parameters (five Categories, four DC levels), and to provide the necessary simplification for presentation in the bar chart.

Desired side effects of this classification are the rejection of MTTF$_d$ values from all channels < 3 years, and the capping of higher MTTF$_d$ values for each channel to a maximum of 100 years. Figure D.2 shows that with an *MTTF*$_d$ of three years, almost 30% dangerous failures can be expected after just one year, which would appear to be unacceptable for a safety control system. At the other end of the scale, a statistically validated reliability of > 100 years *MTTF*$_d$ appears highly dubious. Furthermore, a residual probability of a dangerous failure within the mission time remains at MTTF$_d$

values of any magnitude, and may occur for other reasons (e.g. maloperation). It would not therefore appear to be appropriate to validate higher Performance Levels by the use of highly reliable components alone. In the bar chart to EN ISO 13849-1, this conclusion is expressed by the fact that no further MTTF$_d$ range is shown above the "high" MTTF$_d$ class, even though this would be possible according to the calculated probability. Higher MTTF$_d$ values are not capped to the maximum value of 100 years until the channel level, i.e. substantially higher MTTF$_d$ rates may be substituted in the calculation for individual components.

Table D.1:
Division into classes of the *MTTF*$_d$ for channels which execute the safety function

Description of the *MTTF*$_d$ for each channel	**Range of the *MTTF*$_d$ for each channel**
Low	3 years ≤ *MTTF*$_d$ < 10 years
Medium	10 years ≤ *MTTF*$_d$ < 30 years
High	30 years ≤ *MTTF*$_d$ ≤ 100 years

D1.3 What is the origin of the data?

A possible problem for users of the standard, particularly at the time of publication of the revised EN ISO 13849-1, is the lack of MTTF$_d$ information for safety components [2; 3]. The standard proposes a hierarchy of data sources. The first of these are manufacturer's data, followed by typical values listed in the standard itself, and finally a very conservatively estimated substitutional value of ten years. Since this substitutional value relates to a component, and the lower limit of three years for the MTTF$_d$ value is rapidly reached where several components are employed in a channel, the MTTF$_d$ values listed in the standard itself are of particular importance, at least until manufacturers begin routinely declaring MTTF$_d$ values.

D2 Differences between technologies

By its nature, the failure mode of components varies strongly according to the technology employed, since the "bath-tub characteristic" and the relevance of wear factors may differ. A very high *MTTF*$_d$ may be assumed for mechanical and hydraulic components, which are optimized in their design and use for high reliability and low wear. Random failures (in the constant failure rate phase) and wear failures are insignificant for these components. Conversely, for the majority of electronic components, the failure behaviour over the typical mission time of comparatively "cheap" components is generally well-described by a constant failure rate, since the wear phase is reached only under exacerbated operating conditions. By contrast, the failure behaviour of electromechanical or pneumatic components is quite different in nature. In this case, the wear phase can easily be reached within the usual mission time. For this reason, the attainable number of successful switching cycles or switching operations is generally also stated as the parameter, rather than a lifetime in terms of a time or failure rate per unit time. Consideration must be given to all these technology-specific aspects during calculation of the MTTF$_d$ value. For this reason, EN ISO 13849-1 proposes differentiated procedures.

D2.1 *MTTF*$_d$ of mechanical control components

The approach employing a constant failure rate is, unfortunately, not well-suited to mechanical control components. At the same time, almost all safety functions involve mechanical control elements, at least in the sensor or actuator area, for example for the detection of movements or the stopping of hazardous movements. Although an *MTTF*$_d$ estimated erring on the safe side could often be stated for these components, fault exclusion is generally employed in this case. Provided the requirements for the fault exclusion are observed and documented, this is generally the most elegant means of considering the reliability of the mechanical components. These requirements include adequate resistance to the anticipated environmental influences, i.e. the validity of a fault exclusion may vary according to the selected application. Another requirement is that of adequate over-dimensioning, to ensure for example that the mechanical components are subject to stress only within the fatigue limit. If fault exclusion is not possible, the good engineering practice procedure described below may provide a means by which an MTTF$_d$ value can be estimated.

D2.2 BIA-Report 6/2004, "Untersuchung des Alterungsprozesses von hydraulischen Wegeventilen" (study of the ageing process on hydraulic valves)

On hydraulic systems, the area of valves warrants special consideration as a "safety-related part of the control system"; valves which control hazardous movements or states, in particular, are extremely important for calculation of the Performance Level. Experience has shown that the failure behaviour of hydraulic valves is characterized less by random failures than by failures due to wear. The causes of such failures are primarily systematic, such as excessive stress, unfavourable conditions of use, or lack of maintenance. In order for the lifetime of hydraulic valves to be estimated better, a degree thesis on the subject was commissioned by the BGIA and its results published in the form of BIA-Report 6/2004 "Untersuchung des Alterungsprozesses von hydraulischen Wegeventilen" [4] (study of the ageing process on hydraulic valves). Since valves which assume control tasks are generally piston-type directional control valves, the MTTF$_d$ values for "hydraulic components" were determined on valves of this type. The most important results of this study are presented briefly below.

Estimation of an MTTF$_d$ value is based first and foremost upon the failure rates for hydraulic piston-type directional control valves which were determined in a study conducted in the maintenance departments of two large-scale users of hydraulic equipment (referred to below as Users A and B). The failure rates were determined by the evaluation of computer data (quantities of re-ordered hydraulic piston-type directional control valves, repair reports) and involvement in maintenance work. In addition to the failure data for the valves, the operating conditions were also taken into account. The comparability of the MTTF$_d$ values determined for the different users of hydraulic systems is therefore assured. For validation and confirmation of these data, further failure data were collected by a survey of valve manufacturers.

In the case of User A, the failure rates for the directional control valves were recorded in the maintenance department of a transmission production plant. Data were available for all failures of directional control valves over a period of 38 months, during which 143 directional control valves failed. Approximately 8,050 directional control valves of various ages were in use on the machines, for the most part machine tools, in the transmission production plant. If a constant failure rate is assumed during this period, an *MTTF*$_d$ of 178 years can be calculated as the reciprocal of the failure rate from the data for User A. At this user's plant, the operating conditions specified by the manufacturers were observed for the most part on the hydraulic systems. Since the facility primarily comprised new production lines, condition-based maintenance was performed.

The failure data for the directional control valves at User B's facility were likewise recorded in the maintenance department of a transmission production plant. Approximately 25,000 directional control valves varying in age were in use in this case. Data were available for all directional control valves which had failed over a period of four years (2000 to 2003). In contrast to User A's situation, the failure data for each year were available. It was therefore possible to calculate an *MTTF*$_d$ for each individual year. The *MTTF*$_d$ rose, from 195 years in 2000 to 300 years in 2003. A significant relationship was observed between valve failures and operating/environmental conditions, since the maintenance measures and operating conditions in User B's facility were improved continually over the years. In addition, the operating conditions were superior to those in User A's plant owing to further measures, such as monitoring of the fluid temperature; larger fluid reservoirs, generally located outside the machine; finer return line filters; and flue gas discharge systems for reducing the impurities in the ambient atmosphere.

The study showed that, in conjunction with the type, quality, and level of contamination of the hydraulic fluid used and the design, material and type of the centring/ return spring, the cylindrical guides of the components in valves, e.g. spool valves, had a substantial influence upon the anticipated lifetime of hydraulic piston-type directional control valves. A clear relationship was also established between the quality of the operating conditions and the attained lifetime to failure over a defined period of observation.

D2.3 *MTTF*$_d$ of hydraulic control components

Based upon the results of the above study, an *MTTF*$_d$ of 150 years is proposed in EN ISO 13849-1 for hydraulic components, provided certain conditions are met. The valves studied were primarily of the piston type. Owing to the similarity in failure behaviour, however, the lifetime *MTTF*$_d$ determined for these valves serves as a good estimation for all safety-related hydraulic valves. This is however conditional upon observance during design and manufacture of the basic and well-tried safety principles described in EN ISO 13849-2 for hydraulic valves. The basic and well-tried safety principles for application, likewise described in EN ISO 13849-2, must also be stated by the valve manufacturer (in the manufacturer's data, operating conditions) and observed by the user.

Annex C.2, Table C.1 of EN ISO 13849-2 states the basic safety principles for hydraulic systems. The most important principles include the use of suitable materials and manufacturing procedures, and those of de-energization, pressure limitation, protection against unexpected start-up, and a suitable temperature range (for further details, see Annex C).

Annex C.3, Table C.2 of EN ISO 13849-2 lists well-tried safety principles for hydraulic systems. The most important principles comprise over-dimensioning/safety factors, speed limitation/reduction by means of a resistance for attainment of a defined volumetric flow, force limitation/reduction, an appropriate range for the operating conditions, monitoring of the condition of the pressure medium, the use of well-tried springs, and a sufficient overlap in piston-type valves (for further details, refer again to Annex C).

Even though EN ISO 13849-1 states an MTTF$_d$ value for hydraulic valves under these conditions, each valve manufacturer should, wherever possible, determine failure data for his own components and state an MTTF$_d$ value of his own.

D2.4 *MTTF*$_d$ of pneumatic and electromechanical control components

In fluid power, mechanical and electromechanical technology, the lifetime and reliability of the components are generally determined by the wear characteristics of the moving elements. In fluid power components such as valves, which generally consist of complex units with a large number of moving elements (such as pistons, plungers, springs in the pilot and main stages), the lifetime may also be strongly influenced by the operational environmental conditions. These include, in particular:

- The quality and condition of the pressure medium (compressed air)
- Compatibility of seals with the lubricants
- Temperature influences
- Environmental influences such as dusts, gases, fluids

It is essential that the requirements specified by the component manufacturer be observed, since the parameters for the failure behaviour of the component from which the control system Category is calculated are not otherwise valid.

If the following characteristics are satisfied, the MTTF$_d$ value for a single pneumatic, electromechanical or mechanical component can be estimated by means of the formulae shown further below:

- The manufacturer of the component confirms application of the basic safety principles to EN ISO 13849-2:2003, Tables B.1 or Table D.1 for the design of the component (confirmation on the data sheet for the component).
- The manufacturer of a component for use in a control system of Category 1, 2, 3 or 4 confirms that well-tried safety principles to EN ISO 13849-2:2003, Tables B.2 or D.2 have been applied in the design of the component (confirmation on the data sheet for the component).

- The manufacturer of the component specifies the suitable application and operating conditions for the user. The user must be informed of his responsibility to satisfy the basic safety principles to EN ISO 13849-2:2003, Tables B.1 or D.1 for implementation and operation of the component. For Category 1, 2, 3 or 4, the user must be informed of his responsibility to satisfy the well-tried safety principles to EN ISO 13849-2:2003, Tables B.2 or D.2 for implementation and operation of the component.

The actual measures behind the basic and well-tried safety principles are similar to those described above in greater detail for hydraulic components.

The MTTF$_d$ value is defined as the mean time to dangerous failure. In order for this time to be determined for a component, corresponding lifetime characteristics must be defined. Such characteristics may be the distances travelled by pneumatic cylinders, the frequency of actuation in the case of valves or electromechanical components, and stress reversal in the case of mechanical components. The reliability of pneumatic or electromechanical components is generally determined in the laboratory.

D2.4.1 Determining of the lifetime value B_{10d}

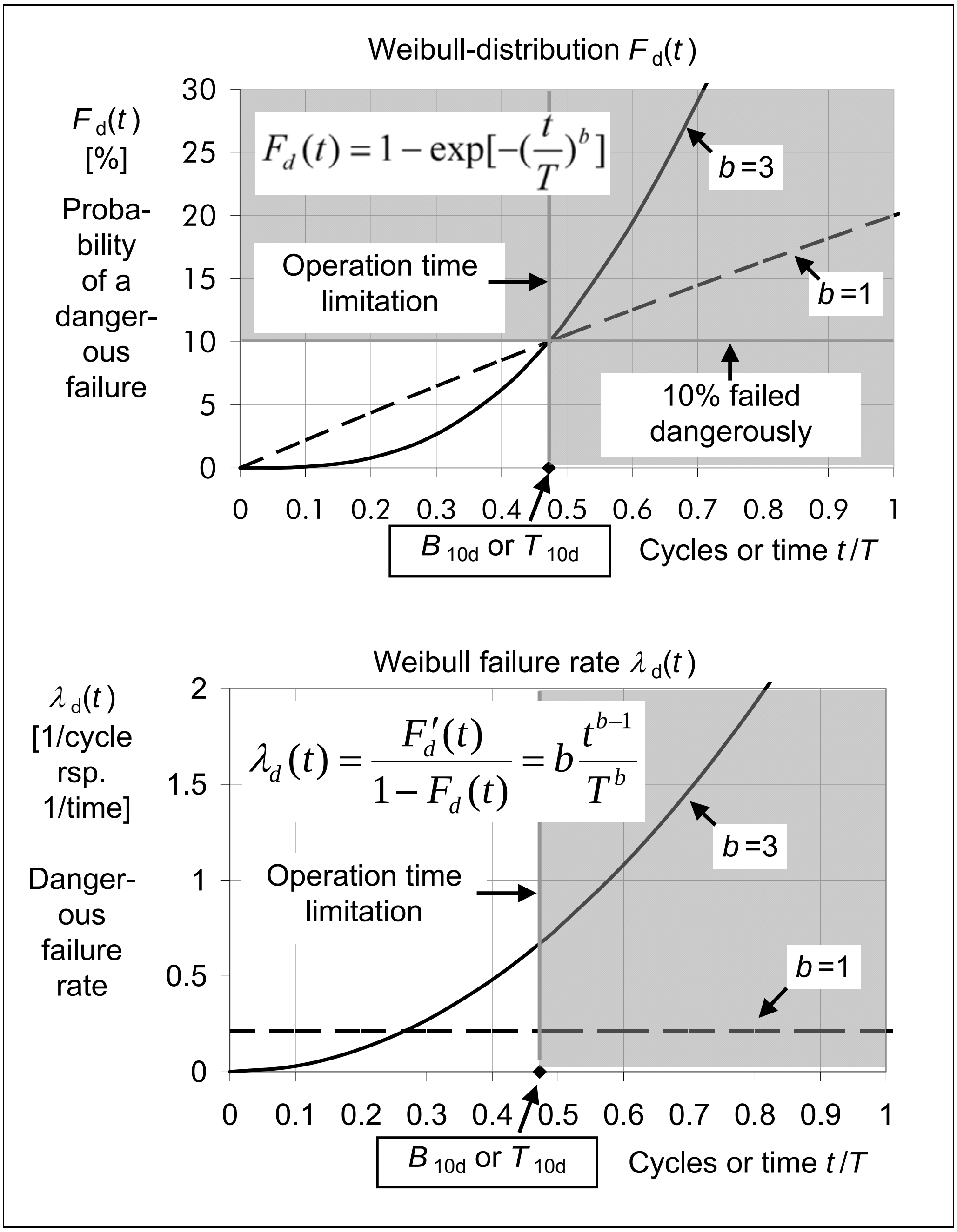
The frequency of failure can be determined from values obtained in the laboratory or possibly in field studies, for example by means of Weibull statistics [5]. The two-parameter Weibull distribution function shown in Figure D.3 is more flexible than the exponential distribution, which it includes as a special case (b = 1).

An increase in the failure rate following onset of the wear phase can be described well by b parameters > 1. The T parameter describes the characteristic lifetime at which 63.2% of the components studied have failed. The “linear regression XY” method can be used to determine the Weibull parameters. Should the data be incomplete, for example because intact components are to be considered, other methods may also be applied. Results in the form of data for the parameters *b* and *T* can be read off from the diagrams. In turn, the nominal lifetime B_{10}, at which 10% of the components studied have failed, can then be determined. The MTTF$_d$ value is determined by means of the nominal lifetime value B_{10}. A reliability analysis employing Weibull statistics can be conducted by means of commercial software.

The safety-related reliability values for fluid power and electromechanical components must be declared by the manufacturer of the components concerned. The reliability of pneumatic components can be determined with reference to the standard ISO 19973 “Pneumatic fluid power – Assessment of component reliability by testing”. This standard comprises four parts:

- Part 1: General procedures
- Part 2: Directional control valves
- Part 3: Cylinders with piston rod
- Part 4: Pressure regulators

Figure D.3:
Illustration of the conversion from B_{10d} to $MTTF_d$



Where the reliability of pneumatic valves is determined, the lifetime (B_{10} value or B value) is indicated in cycles before failure. The nominal lifetime B_{10} (in some literature references also t_{10}) is the average number of switching operations/switching cycles reached before 10% of the units studied fail. Since in the case of valves, the “availability” failure criterion also encompasses failures which are not relevant to safety (e.g. leakage above the defined threshold), it has been set out in the standard that the value determined for the nominal lifetime (B_{10}) multiplied by two may be considered equal to the B_{10d} (dangerous) value (nominal lifetime at which 10% of the components have suffered dangerous failure):

$$B_{10d} = 2 \text{ x } B_{10} \qquad (2)$$

The B_{10} value is generally determined in the laboratory. For this purpose, at least seven valves produced at different times are subjected to endurance testing. The maximum switching frequency for the endurance test is determined from the pressure build-up (attainment of 90% of the test pressure) and the pressure dissipation (attainment of 10% of the test pressure) in a connected volume which is defined according to the port cross-sections. At least five out of seven valves must fail for evaluation of the test results.

As an approximation, where testing is performed on a small number of test specimens, e.g. seven valves, the first failure determines the B_{10} value, i.e. the number of cycles attained by the time of the first failure corresponds approximately to the B_{10} value. Should the first failure be dangerous, the number of switching operations performed by this point approximates to the B_{10d} value.

Dangerous failures on pneumatic valves particularly include:

- Non-switching (sticking at an end or zero position) or incomplete switching (sticking at a random intermediate position)
- Change of switching times
- Spontaneous change of the initial switching position (without an input signal)

Analysis of the failures always refers to the entire unit, consisting for example of main valve and pilot valve.

D2.4.2 Conversion of *B*$_{10d}$ to *MTTF*$_d$

Since the $MTTF_d$ value is stated in years, the B_{10d} value, which is stated in terms of the number of cycles, must be converted accordingly. The following parameters are required for determining of the $MTTF_d$ value:

- h_{op} → Mean operating time in hours (h) per day
- d_{op} → Mean operating time in days per year
- t_{cycle} → Mean time between the beginning of two successive cycles of the component (e.g. switching of a valve) in seconds (s) per cycle

The mean number of annual operations n_{op} (in cycles per year) can be determined from these parameters:

$$n_{op} = \frac{d_{op} \text{ x } h_{op}}{t_{cycle}} \text{ x } 3{,}600 \, \frac{\text{s}}{\text{h}} \qquad (3)$$

Substitution of the n$_{op}$ value in formula (4) produces the *MTTF*$_d$ value for the component concerned, in years:

$$MTTF_d = \frac{B_{10d}}{0.1 \text{ x } n_{op}} \qquad (4)$$

The operating time of the component is limited here to the T$_{10d}$ value (the time at which 10% of the components under consideration fail dangerously). The T$_{10d}$ value can be determined as follows:

$$T_{10d} = \frac{B_{10d}}{n_{op}} \qquad (5)$$

This means that the components under consideration should be replaced before the T$_{10d}$ value is reached.

Conversion of the B$_{10d}$ value to an MTTF$_d$ value with the aid of n_{op} and limitation by T_{10d} is based upon an approximation. The actual failure behaviour, which strongly reflects the influence of wear effects and which is well-described by a Weibull function, is approximated by an exponential distribution with constant failure rate (the reciprocal of which represents the MTTF$_d$ value). This method is illustrated in Figure D.3. The unbroken line represents a Weibull distribution in which b = 3. By contrast, the dashed line shows an exponential distribution in which b = 1, which intersects the original Weibull distribution at the point ($t = B_{10d}$; F = 10%). If the relationship $MTTF_d = 1/\lambda_d$ for exponential distributions and the conversion of cycles to times by n_{op} are taken into account, this intersection condition yields the approximation formula for the conversion of B_{10d} to $MTTF_d$. This method exploits the fact that before the wear phase is reached the failure rate is very low, and that it rises significantly only after a certain point in time. This point in time is approximated by B_{10d} (in cycles) or T_{10d} (as a time in years). If the mission time is now limited to T_{10d}, the gently rising failure rate can be estimated erring on the safe side as a constant value in the region of T_{10d}. Figure D.3 shows the importance of limiting of the mission time to T_{10d} in this way: above this value, the proportion of dangerous failures which may actually be expected rises significantly over time when compared to the exponential approximation. The selected “substitution failure rate” $\lambda_d = 1/MTTF_d$ of the exponential approximation also corresponds approximately to the arithmetic mean of the failure rate which may actually be expected up to the point in time T_{10d}. Beyond T_{10d}, however, the onset of the wear phase is accompanied by strong deviations.

D2.5 Good engineering practice method

If no component reliability data is available from the manufacturer, the standard proposes the use of database values as the first alternative. It provides support in the form of “typical values” for mechanical, hydraulic and pneumatic components and for electromechanical safety components frequently used in practice. These values are listed in Table D.2 in the form of MTTF$_d$ values, B$_{10d}$ values or fault exclusions.

This B_{10d} value, obtained by the component manufacturer by testing, indicates the average number of cycles before 10% of the components fail dangerously. This value can be used to estimate the $MTTF_d$ value. Certain conditions must however be met when the values in Table D.2 are used:

- The manufacturer of the component confirms that basic safety principles to EN ISO 13849-2:2003 or the relevant standard (see Table D.2) were applied during design of the components (confirmation on the data sheet for the component).
- The manufacturer of a component which is to be used in a control system of Category 1, 2, 3 or 4 confirms that well-tried safety principles according to EN ISO 13849-2:2003 or the relevant standard (see Table D.2) were applied during the design of the component (confirmation on the data sheet for the component).
- The manufacturer of the component specifies the suitable application and operating conditions for the user and informs the latter of his responsibility to satisfy the basic safety principles to EN ISO 13849-2:2003 for implementation and operation of the component.
- The user satisfies the basic and/or well-tried safety principles according to EN ISO 13849-2:2003 for implementation and operation of the component.

Table D.2:
Typical reliability values which may be assumed to be reached
when good engineering practice is followed

	Basic and well-tried safety principles to EN ISO 13849-2:2003	**Other relevant standards**	**Typical values: *MTTF*$_d$ (years) *B*$_{10d}$ (cycles) or fault exclusion**
Mechanical components	Tables A.1 and A.2	—	$MTTF_d$ = 150
Hydraulic components	Tables C.1 and C.2	EN 982	$MTTF_d$ = 150
Pneumatic components	Tables B.1 and B.2	EN 983	B_{10d} = 20,000,000
Relays and contactor relays with negligible load	Tables D.1 and D.2	EN 50205 IEC 61810 IEC 60947	B_{10d} = 20,000,000
Relays and contactor relays with maximum load	Tables D.1 and D.2	EN 50205 IEC 61810 IEC 60947	B_{10d} = 400,000
Proximity switches with negligible load	Tables D.1 and D.2	IEC 60947 EN 1088	B_{10d} = 20,000,000
Proximity switches with maximum load	Tables D.1 and D.2	IEC 60947 EN 1088	B_{10d} = 400,000

Table D.2: continued

	Basic and well-tried safety principles to EN ISO 13849-2:2003	**Other relevant standards**	**Typical values: $MTTF_d$ (years) B_{10d} (cycles) or fault exclusion**
Contactors with negligible load	Tables D.1 and D.2	IEC 60947	B_{10d} = 20,000,000
Contactors with nominal load	Tables D.1 and D.2	IEC 60947	B_{10d} = 2,000,000
Position switches, independent of the load[a)]	Tables D.1 and D.2	IEC 60947 EN 1088	B_{10d} = 20,000,000
Position switches (with separate actuator, guard locking), independent of the load[a)]	Tables D.1 and D.2	IEC 60947 EN 1088	B_{10d} = 2,000,000
Position switches and push-buttons[b)] under resistive load and with over-dimensioning (≤ 10% of the maximum load) of the electrical contacts	Tables D.1 and D.2	IEC 60947 EN 1088	B_{10d} = 1,000,000
Position switches and push-buttons[b)] with over-dimensioning in accordance with Table D.2, EN ISO 13849-2:2003 of the electrical contacts	Tables D.1 and D.2	IEC 60947 EN 1088	B_{10d} = 100,000
Emergency stop devices used with low exposure to environmental influences, e.g. in laboratories[a)]	Tables D.1 and D.2	IEC 60947 ISO 13850	Fault exclusion up to 100,000 cycles, if confirmed by the manufacturer
Emergency stop devices used under normal exposure to environmental influences, e.g. on machines[a)]	Tables D.1 and D.2	IEC 60947 ISO 13850	Fault exclusion up to 6,050 cycles
Enabling switches (3-stage), independent of the load[a)]	Tables D.1 and D.2	IEC 60947	Fault exclusion up to 100,000 cycles

[a)] If fault exclusion is possible for direct opening action

[b)] For make contacts and for break contacts, if fault exclusion is not possible for direct opening action

Compliance with these requirements is to ensure that the application of basic and/or well-tried safety principles is assured from manufacture, through implementation, to routine operation of the component. The interface between the manufacturer and the user/operator of the machine is clearly defined: the manufacturer must provide binding confirmation that the safety principles have been observed during design, and must make all relevant information available on the conditions of use and operation.

For his part, the user/operator of the machine is responsible for observing all safety principles concerning implementation and operation of the component. Provided these conditions are met, the typical values cited in Table D.2 can be used for calculation of the *$MTTF_d$* or for assumption of a fault exclusion. The $\mathrm{MTTF_d}$ value of 150 years for hydraulic control components for which reasoning is provided above is extended here to mechanical components. This secondary value can be used when reasoning cannot be provided for a fault exclusion but when the use of basic/ well-tried safety principles is assured.

In addition, $\mathrm{B_{10d}}$ values for electromechanical components are stated which can be converted to an *$MTTF_d$* value in accordance with the procedure also described above involving the average number of actuations per year n_{op}. Emergency stop devices and enabling switches are a special case for which a fault exclusion may be assumed under certain conditions.

All values in the table relate to dangerous failures only, as expressed by the index “d”. It has generally been assumed here that only half of all failures are dangerous. For this reason, these values may well appear to be more optimistic than those indicated on manufacturers' data sheets, which relate to all fault types which could impair functionality in the sense of availability. On some electromechanical components, such as relays, contactor relays and contactors, the electrical load of the contacts is a major factor determining the $\mathrm{B_{10d}}$ value, as is frequently confirmed by observations in the field. Substantially better values are obtained at low electrical load (typically resistive load), described by EN ISO 13849-1 as up to 20% of the rated value. The mechanical rather than the electrical lifetime was assumed in this case. Depending upon the type (resistive or inductive) and magnitude of the load, B_{10d} intermediate values between the extremes stated here may be derived. For the position switches, guard-locking devices, emergency stop devices and pushbuttons, such as enabling switches, listed in the table, the safety principle of direct opening action is generally a requirement for the electrical part. A fault exclusion can therefore be assumed for the electrical part irrespective of the load, and the cited $\mathrm{B_{10d}}$ values are due primarily to failures in the operating mechanism. This approach is also the reason, for example, for the substantial differences between position switches with and without separate actuators or guard-locking devices. No fault exclusion may however be assumed for make contacts and break contacts without direct opening characteristic. This is reflected in substantially lower typical $\mathrm{B_{10d}}$ values. Since emergency stop devices and enabling switches must guarantee a minimum number of fault-free operations (see Table D.2), a fault exclusion may also be assumed for the mechanical elements up to this number of operations. Owing to the manual actuation, faults in the input mechanism or maladjustment need not be considered, in contrast to position switches. In the case of emergency stop devices, a distinction is drawn between low and normal loading. The minimum number of fault-free operations of 6,050 cycles which is to be demonstrated by type testing applies for normal exposure to environmental influences in this case. Some manufacturers confirm an additional 100,000 cycles for use with low environmental loading.

To enable fault exclusion to be applied for direct opening action for the electrical part of electromechanical safety components, the components concerned must satisfy not only the above conditions, but also those for “well-tried components”.

By their nature, these approaches constitute major simplifications of the actual, complex relationships. A very low load current in particular, combined with infrequent actuation, can for example lead to cold welding of electrical contacts. These effects should however be avoided by the required application of basic/well-tried safety principles. These principles include the suitability of both the mechanical and electrical component characteristics and their adaptation to the anticipated load.

D2.6 *MTTF*$_d$ of electronic control components

As already mentioned, declaration of the failure rates λ and λ_d, for example in the form of FIT values (failures in time, i.e. failures in 10^9 component hours), has long been normal practice for electronic components. It is therefore very likely that reliability information can be obtained from the manufacturer. These data may possibly have to be converted to MTTF$_d$ values, for example with the aid of the simplifying assumption that only 50% of all failures are dangerous. If manufacturers' data are not available, however, a number of known databases can be referred to. The following are cited by way of example in EN ISO 13849-1:

- Siemens Standard SN 29500, Failure rates of components, Siemens AG (updated at irregular intervals). www.pruefinstitut.de
- IEC/TR 62380, Reliability data handbook — Universal model for reliability prediction of electronics components, PCBs and equipment; identical to the RDF 2000/Reliability Data Handbook, UTE C 80-810, Union Technique de l’Electricité et de la Communication. www.ute-fr.com
- Reliability Prediction of Electronic Equipment, MIL-HDBK-217F, Department of Defense, Washington DC, 1982; now continued in the form of the 217Plus System Reliability Assessment Tool, Reliability Information Analysis Center, 6000 Flanagan Road, Suite 3, Utica, New York, 13502-1348 (theRIAC.org)
- Reliability Prediction Procedure for Electronic Equipment, Telcordia SR-332, Issue 01, May 2001 (telecom-info.telcordia.com), (Bellcore TR-332, Issue 06)
- EPRD, Electronic Parts Reliability Data (RAC-STD-6100), Reliability Information Analysis Center, 6000 Flanagan Road, Suite 3, Utica, New York, 13502-1348 (theRIAC.org)
- NPRD-95, Nonelectronic Parts Reliability Data (RAC-STD-6200), Reliability Information Analysis Center, 6000 Flanagan Road, Suite 3, Utica, New York, 13502-1348 (theRIAC.org)
- British Handbook for Reliability Data for Components used in Telecommunication Systems, British Telecom (HRD5, last issue)
- Chinese Military Standard, GJB/z 299B

In addition to these databases, a number of software tools are available on the market which provide computerized access to these or other databases. In the majority of databases, electronic components are catalogued by component type and other criteria (e.g. design, material, enclosure). Generally, base failure rates are stated in the first instance for reference conditions (e.g. for a component ambient temperature of 40 °C and nominal load) which can be corrected to the actual conditions of use, where these differ, by means of adjustment factors. EN ISO 13849-1 even lists values for certain typical electronic components which have been taken from the SN 29500 database and assigned a safety factor of 10. Since these values serve chiefly as examples, they will not be stated here. The safety factor of 10 in Annex C.5 of the standard is intended to cover the worst case when a very generic guideline value is required. Provided the data sources are applied correctly, an additional safety factor is not generally required. Adjustment to loads outside the reference conditions is not explicitly required by EN ISO 13849-1, and should be applied by approximate estimation in the interests of simplicity.

D3 Integration of components and equipment which have already been certified

In cases which are probably rare at present but which are likely to become more common in the future, manufacturers may state an *MTTF*$_d$ for their components on the data sheet itself. A similar case applies should a SIL to IEC 61508 or a PL to EN ISO 13849-1 already be stated in the manufacturer's information, in conjunction with an “average probability of a dangerous failure per hour” (or PFH value to IEC 61508). Should such components be employed in one channel of the SRP/CS only, the stated probability of failure per hour (*PFH*) may be considered as a substitute for the rate of dangerous failure. Internal component characteristics such as redundancy and self-diagnostics are already considered in this case:

$$MTTF_d = \frac{1}{\lambda_d} \approx \frac{1}{PFH} \quad \text{(“Black-box” components with } PFH \text{ in one channel)} \quad (6)$$

D4 Parts count method

Once the MTTF$_d$ values of all safety-related components are known, the *MTTF*$_d$ of each block must first be calculated. This step can be performed in great detail by an FMEA (failure mode and effects analysis, see Annex B); ideally, however, the different failure modes of each safety-related component and their effect upon the block must be analysed for this purpose. In consideration of the effort, this approach is therefore generally worthwhile only for components with a high failure rate, i.e. a low MTTF$_d$ value. A fast alternative which produces values which on average are not substantially worse is the parts count method stated in EN ISO 13849-1. Essentially, this method is a summation with three chief assumptions:

- Irrespective of the failure mode of a component and its effects upon the block, all failures are divided into two halves, safe and dangerous. This means that half of the failure rate λ of a component contributes to the dangerous failure rate λ_d of the associated block. If the proportion of dangerous failures, λ_d, within the failure rate as a whole has already been determined for the component, the same value λ_d is also allowed for the block.

- The dangerous failure rate λ_d of the block is then formed by summation of the λ_d contributions of all N safety-related components present in the block concerned (the contributions of identical components can easily be grouped):

$$\lambda_d = \frac{1}{2}\sum_{i=1}^{N}\lambda_i \quad \text{i.e.} \quad \lambda_d = \sum_{i=1}^{N}\lambda_{di} \tag{7}$$

Since, as described above, EN ISO 13849-1 assumes constant failure rates, failure rates λ_d can be converted to MTTF$_d$ values simply by formation of the reciprocal. Based upon this relationship, the MTTF$_d$ value of a block can easily be derived from the MTTF$_d$ values of the associated components. An example of application of the parts count method can be found in Chapter 6.

D5 Series arrangement of blocks in a channel and capping of the *MTTF*$_d$

If MTTF$_d$ values/failure rates λ_d are available for each block, the *MTTF*$_d$ for each channel can be calculated equally well by summation of the failure rates of all blocks involved in a channel (as in equation (7)). It is assumed in this case that the dangerous failure of any block in the chain of blocks constituting a channel is also to be treated as a dangerous failure of the channel. Since under certain circumstances however, downstream blocks are capable of detecting a dangerous failure of upstream blocks, this assumption constitutes an estimation erring on the safe side.

In this phase of determining the *MTTF*$_d$, the capping rule of EN ISO 13849-1 takes effect: each *MTTF*$_d$ of a channel which mathematically exceeds 100 years is routinely reduced to the maximum value of 100 years. The purpose of this rule is to prevent the component reliabilities from being overstated in comparison with the other dimensions relevant to the PL, such as the architecture, tests and common cause failures.

D6 Symmetrization of multiple channels

As soon as a control system involves two channels (as is generally the case for Categories 3 and 4), the question arises as to which of the MTTF$_d$ values for the different channels is to be used for determining the PL with the aid of the bar chart. For this issue, too, EN ISO 13849-1 has the answer in the form of a simple formula:

$$MTTF_d = \frac{2}{3}\left[MTTF_{dC1} + MTTF_{dC2} - \frac{1}{\dfrac{1}{MTTF_{dC1}} + \dfrac{1}{MTTF_{dC2}}} \right] \tag{8}$$

The average *MTTF*$_d$ per channel is thus produced from the MTTF$_d$ values of the two redundant channels C1 and C2 by means of an averaging formula (this formula can be derived mathematically by calculation of the MTTF$_d$ value for a two-channel system without diagnostics but with known MTTF$_d$ values of both channels – *MTTF*$_{dC1}$ and *MTTF*$_{dC2}$ [5]). This completes the successive summary of the MTTF$_d$ values of all components involved in the control system. The result is a value for the typical reliability of the components present in the control system, without consideration of the redundancy, diagnostics or CCF. Whereas *MTTF*$_d$ is already capped to 100 years for each channel involved, it is advantageous for the MTTF$_d$ values to be divided into one of the three classes, “Low”, “Medium” or “High”, only after symmetrization. The symmetrized value is substituted in the numerical calculation of the PL as a parameter in addition to the Category, the average diagnostic coverage and the measures against common cause failure. In addition, a minimum MTTF$_d$ value of three years (for Category B, 2 and 3) or 30 years (for Category 1 and 4) is required, depending upon the Categories which are to be attained.

References

[1] *Birolini, A.*: Reliability Engineering: Theory and Practice. 5th ed. Springer, Berlin 2007

[2] *Bork, T.; Schaefer, M.*: Aus Aktivität wird Vorsicht – Sinn und Unsinn der Quantifizierung. O + P Ölhydraulik und Pneumatik 51 (2007) No. 3, pp. 78-85. www.dguv.de/bgia, Webcode d4460

[3] *Schaefer, M.; Bork, T.*: Tangible and transparent use of reliability data for functional safety - The sense and nonsense of quantification. 5. International Conference Safety of Industrial Automated Systems, 12.-13. November 2007, Tokio/Japan - Lecture. Report, pp. 370-375. Ed.: Nippon Electric Control Equipment Industries Association (NECA), Tokio/Japan

[4] *Schuster, U.*: Untersuchung des Alterungsprozesses von hydraulischen Ventilen. BIA-Report 6/04. Ed.: Hauptverband der gewerblichen Berufsgenossenschaften (HVBG), Sankt Augustin 2004.
www.dguv.de/bgia, Webcode d6362

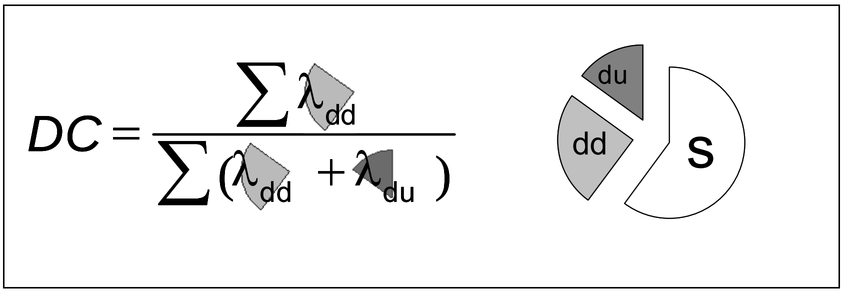
[5] *Weibull, W.*: A statistical distribution function of wide applicability. J. Appl. Mech. 18 (1951), pp. 292-297

[6] *Goble, W. M.*: Control systems safety evaluation and reliability. 2nd ed. Ed.: Instrumentation, Systems, and Automation Society (ISA), Research Triangle Park, North Carolina, 1998

Annex E: Determining of the diagnostic coverage *(DC)*

The diagnostic coverage *DC* is a measure of the effectiveness of a control system's self-test and monitoring measures. It may relate to individual components, blocks, or the entire control system (DC_{avg}). The precise definition of the *DC* is based upon the division of failures into three groups (see Figure E.1):

- Safe (s) failures: these failures automatically result in a safe state being assumed which does not give rise to any hazards (example: a contactor remaining open or a valve remaining closed, resulting in standstill of potentially hazardous movements).
- Dangerous detectable (dd) failures: these potentially dangerous failures are detected by test or monitoring measures and transferred to a safe state (example: failure of a contactor to open or of a valve to close, which is detected by a readback contact or position monitor, and handled safely).
- Dangerous undetectable (du) failures: these potentially dangerous failures are not detected (example: undetected failure of a contactor to open or of a valve to close, as a result of which a demand for a safe torque off does not result in stopping of a hazardous movement).



$$DC = \frac{\sum \lambda_{dd}}{\sum (\lambda_{dd} + \lambda_{du})}$$

Figure E.1: Illustration of the diagnostic coverage

On multi-channel systems, the term “dangerous failure” is used with regard to a single channel, although a dangerous system failure need not necessarily yet have occurred. The failures “dd” and “du” can be combined to form the group of dangerous failures (d). The safe failures may also be detectable or undetectable; the distinction is irrelevant, however, since the safe state is assumed in both cases.

The diagnostic coverage (*DC*) is determined by the proportion of detectable dangerous failures (dd) among all dangerous failures (d), and is generally stated as a percentage. For calculation of the *DC*, for example in conjunction with an FMEA (failure mode and effects analysis, see Annex B), the ratio is calculated of the totals of the failure rates λ_{dd} and λ_d of the unit under consideration. The *DC* is seen here to be a value relating to the tested unit (e.g. the block) and not to the facility performing the tests. For simplified calculation of the *DC*, EN ISO 13849-1 employs a different solution, proposing DC marker values for typical diagnostics measures the attainment of which may be assumed. In this way, a time-consuming FMEA is replaced by evaluation from tables of the implemented diagnostics measures. A similar procedure is frequently used by test bodies as standard and economic practice.

To calculate the PL it is necessary to evaluate the proportion of **un**detectable dangerous failures (i.e. 1 - *DC*). The higher the DC provided by the implemented test and monitoring means, the lower will be the probability of dangerous failure. EN ISO 13849-1 groups the DC into four levels as given in Table E.1 resulting, for simplicity, in four marker values: 0%, 60%, 90% and 99%.

***DC* (diagnostic coverage)**	
Description	**Range**
None	*DC* < 60%
Low	60% ≤ *DC* < 90%
Medium	90% ≤ *DC* < 99%
High	99% ≤ *DC*

Table E.1:
The four levels of diagnostic coverage according to the simplified approach of EN ISO 13849-1

A fundamental distinction must be drawn between the *DC* of an individual test for a certain component or block, and the average diagnostic coverage DC_{avg} for the entire control system under analysis. The formation of groups by means of the marker values is applied here both for qualification of the individual tests, and for definition of the DC_{avg}. Since the DC_{avg} is one of the input variables for the simplified bar-chart method for quantification of the probability of failure, the calculated DC_{avg} value is rounded down to one of the four marker values (0%, 60%, 90% and 99%) in accordance with Table E.1, i.e. placed in one of the four DC classes (None, Low, Medium and High). In the simplified approach, a DC_{avg} value of 80% is thus reduced to a value of 60% (in contrast to the procedure in the BGIA SISTEMA software utility, which employs intermediate DC_{avg} values in its default setting; see Annex H, page 355). The *DC* of individual tests will first be discussed below, followed by calculation of the DC_{avg}.

Table E.2 (see page 336 to 339) shows typical test and monitoring measures for components and blocks, and their DC evaluation to EN ISO 13849-1. Different measures are usual, depending upon the function (I, L, O, i.e. input, logic, output), Category and technology. Their evaluation may vary depending upon the design or upon external factors, for example according to the application in which the control system is operated. Depending upon the application, indirect monitoring by displacement transducers or position switches on the actuators rather than on the control system elements may for example not provide any indication of whether the safety function can still be executed independently by each of two redundant control channels. In general, no distinction is drawn in evaluation between automatic tests (e.g. program routines which are performed regularly) or deliberate tests (e.g. tests initiated manually by the operator at regular intervals). The unit conducting a test is also irrelevant, for example in the case of self-tests. It is important to note however that a test is only ever effective when the safe state is actually assumed following detection of a dangerous failure. If, for example, contact welding on a main contactor is detected, but no means exist for timely stopping of a hazardous movement, the detection is useless and must be rated with a *DC* of 0%.

The following requirement applies in addition to the test and monitoring measures stated in Table E.2: should a *DC* of "medium" or "high" be required for the logic, at least one measure with at least 60% must be selected in each case for variant memory, invariant memory and the processing unit. Measures other than those stated in Table E.2 may also be employed.

Further information on determining the DC for typical test measures can be found for example in Tables A.2 to A.15 of IEC 61508-2 [1]. These tables contain the marker values of 60%, 90% and 99% as the maximum *DC* to be attained by the relevant measure. With suitable unrestricted implementation of the measures stated, this maximum value can however generally be employed for estimation.

Once the *DC* for individual test measures has been determined, and prior to calculation of the DC_{avg}, the DC value per block must be determined. A test measure generally acts upon an entire block (e.g. cross-checking): the discrete value can then simply be adopted for the block. Further permutations are possible, however:

- If a block is monitored by a number of individual measures (see Figure E.2), the block DC is at least as good as the best individual *DC*. Should the measures mutually complement each other, a higher block DC may even be possible; this *DC*, however, must then be determined by analysis of the failures covered by each test, in a similar way to an FMEA.

Figure E.2:
Where several tests act upon the same block, their overlap may lead to a higher overall *DC* (left), or it may not (right). The hatched areas represent the proportion of the detected dangerous failures. The square overall area represents all dangerous failures (100%).

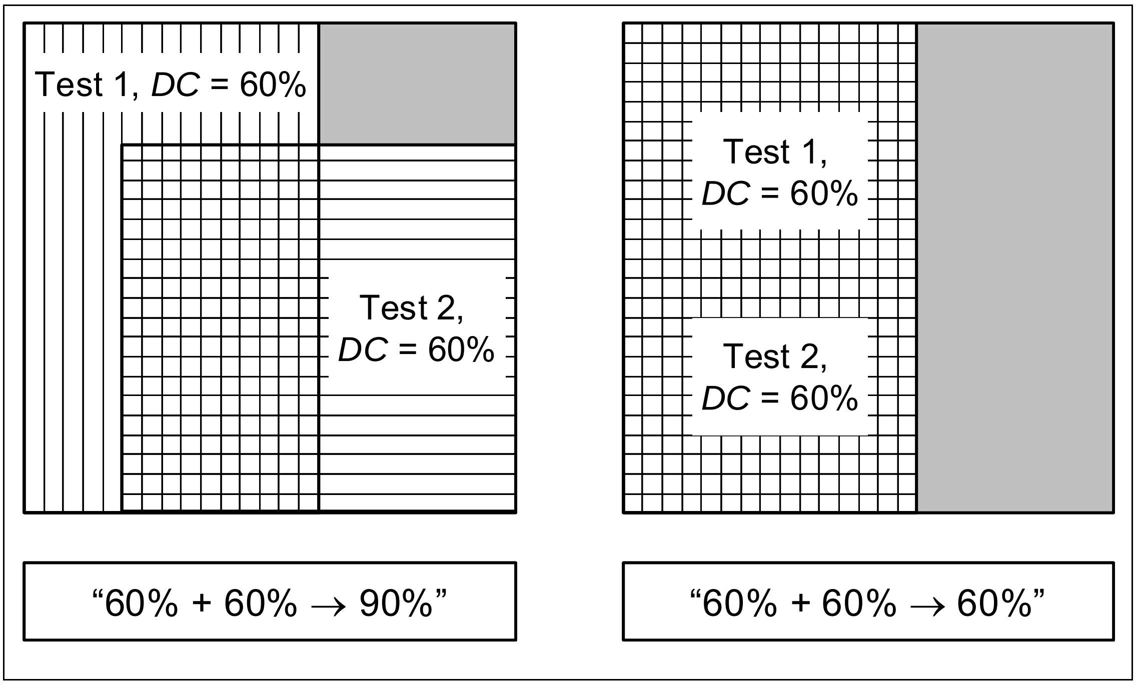


Table E.2:
DC marker values for typical tests and monitoring measures at component and block

Measure	**Primarily relevant for**			***DC* (%)**	**Description of measure**
	I	**L**	**O**		
Cyclic test stimulus by dynamic change	X			90	Periodic generation of a signal change with monitoring of the results
Plausibility check/readback/ (cross-)monitoring					
• Without dynamic test	X		X	0-99	The attained DC value depends on how often a signal change is done by the application.
• With dynamic test, without high quality fault detection	X		X	90	
• With dynamic test, with high quality fault detection	X		X	99	
Indirect monitoring	X	X	X	90-99	The attained DC value depends on the application.
Direct monitoring	X	X	X	99	
Fault detection by the process	X	X	X	0-99[1]	The attained DC value depends on the application; this measure alone is not sufficient for the required Performance Level e[2]
Monitoring some characteristics	X			60	
Program sequence monitoring					
• Simple temporal		X		60	Time monitoring
• Temporal and logical		X		90	
Start-up self-tests		X	(X)	90	To detect latent faults, DC depends on the testing technique

level, to EN ISO 13849-1

Typical realisation in different technologies				
Mechanics	Pneumatics	Hydraulics	Electrical systems	(Programmable) electronics
See description of measure				
Manual initiation of the test function				
	Position monitoring of the valving element, value of *DC* depends on concrete realisation		Comparison of inputs or outputs without detection of short circuits	
			Cross monitoring of inputs or outputs with detection of short circuits and static faults, e.g. using safety modules	Cross monitoring of signals and intermediate results with detection of short circuits and static faults and temporal and logical program sequence monitoring; dynamic cross monitoring of independently attained position or velocity information
Position measuring systems or limit switches at the actuators instead of the control elements	Position measuring systems or limit switches at the actuators instead of the control elements; monitoring of valves by pressure switches		Position measuring systems or limit switches at the actuators instead of the control elements	
Position monitoring directly at the control element	Position monitoring directly at the valving element over the whole stroke		Position monitoring by mechanically linked readback contacts (non-equivalent break contacts)	Signal monitoring by readback e.g. using optocouplers
Failure of the process control, becoming obvious through malfunction, damage of workpiece or parts of the machine, interrupts or delay of the functional process, without producing a hazard immediately				
Monitoring of response time, range of analogue signals			Monitoring of response time, range of analogue systems (e.g. electrical resistance, capacitance)	
Not relevant				Timer as watchdog, where trigger points are within the program of the logic
Not relevant				By the watchdog, where the test equipment does plausibility checks of the behaviour of the logic
			Detection of e.g. welded contacts by triggering and read-back	Detection of latent faults in program- and data memories, input/output ports, interfaces

Table E.2: continued

Measure	**Primarily relevant for**			***DC* (%)**	**Description of measure**
	I	**L**	**O**		
Checking the monitoring device		X		90	Checking the monitoring device reaction capability by the main channel at start-up or whenever the safety function is demanded or whenever an external signal demands it, through an input facility
Dynamic principle		X		99	All components of the logic are required to change the state ON-OFF-ON when the safety function is demanded
Test of memory and CPU					
• Invariable memory: signature of one word (8 bit)		X		90	
• Invariable memory: signature of double word (16 bit)		X		99	
• Variable memory: RAM-test by use of redundant date e.g. flags, markers, constants, timers and cross comparison of these data		X		60	
• Variable memory: check for readability and write ability of used data memory cells		X		60	
• Variable memory: RAM monitoring with modified Hamming code or RAM self-test (e.g. “galpat” or “Abraham”)		X		99	
• Processing unit: self-test by software		X		60-90	
• Processing unit: coded processing		X		90-99	
Redundant shut-off path					
• With no monitoring of the actuator			X	0	
• With monitoring of one of the actuators either by logic or by test equipment			X	90	
• With monitoring of the actuators by logic or test equipment			X	99	

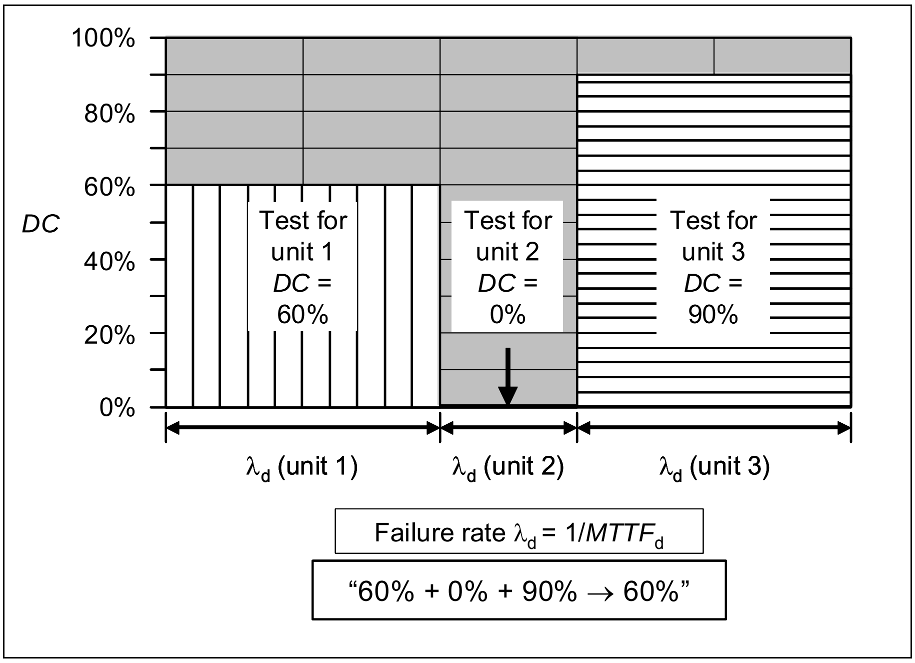
[1] For example to be determined by FMEA calculating the ratio of detected dangerous failures to all dangerous failures

[2] PL e normally requires two channels. Therefore as a minimum the complementary block of the redundant channel should implement a different DC measure, with a DC value at least as high as the assumed DC by the process

Typical realisation in different technologies				
Mechanics	Pneumatics	Hydraulics	Electrical systems	(Programmable) electronics
				Checking the watchdog reaction capability
	Interlocking circuits implemented by pneumatics		Interlocking circuits implemented by relays	
	not relevant			see description of measure
	not relevant			see description of measure
	not relevant			see description of measure
	not relevant			see description of measure
	not relevant			see description of measure
	not relevant			see description of measure
	not relevant			see description of measure

- A block consists of several units, each of which is tested by different measures, for example programmable electronics with separate tests for the memory and the processing unit (see Figure E.3). In this case, the block DC is at least as good as the poorest individual *DC* (if the latter is 0%, i.e. units exist which are not tested at all, the block DC would also be 0% in accordance with this rough estimate). A better and more precise value for the block DC can be attained by weighting the individual *DC* with the associated failure rate λ_d (= 1/$MTTF_d$). The weighted averaging formula corresponds here to Equation (1) for DC_{avg}. Depending upon the accuracy, such an analysis also ultimately leads to an FMEA, however.

Figure E.3:
Where the *DC* is averaged for several units of one block, weighting of the individual 60%, 0% and 90% DC with λ_d leads to a different value (60%) than for example the unweighted arithmetic mean (50%)



The average *DC* for the entire control system under consideration is termed DC_{avg} and is calculated from the DC values for all of its blocks. In contrast to the $MTTF_d$ per channel, no distinction is drawn between the control channels; rather, an overall value is determined directly. The averaging formula weights the individual *DC*s with the associated failure rate λ_d (= 1/$MTTF_d$) of each block. This ensures that blocks with a high failure rate, i.e. a low $MTTF_d$, are given greater consideration than blocks the dangerous failure of which is comparatively unlikely. The averaging formula is as follows:

$$DC_{avg} = \frac{\dfrac{DC_1}{MTTF_{d1}} + \dfrac{DC_2}{MTTF_{d2}} + \ldots + \dfrac{DC_N}{MTTF_{dN}}}{\dfrac{1}{MTTF_{d1}} + \dfrac{1}{MTTF_{d2}} + \ldots + \dfrac{1}{MTTF_{dN}}} \qquad (1)$$

The summation extends over all relevant blocks with the following provision:

- For blocks with no *DC*, a *DC* of 0% is substituted. These blocks thus contribute only to the denominator of the fraction.
- For blocks with fault exclusion for the dangerous failure mode (an imperceptibly low failure rate or infinitely high $MTTF_d$), the corresponding value is omitted from the numerator and the denominator.
- All blocks which execute safety functions in the various control channels are considered. Blocks which have the function of testing only are not considered. For Category 2 structures, this means that blocks in the monitoring channel ("TE" and "OTE") are not counted. In Category 3 and 4, the average value is formed directly over both channels; symmetrization is not performed separately per channel as it is for the $MTTF_d$.

For a detailed analysis of the influence of the tests upon the probability of failure of the overall system, further values must be considered in addition to the *DC*. Besides the test rate, these include the failure rate of the test equipment itself. In multi-channel systems, however, the frequency of a test has only minor consequences, since the relevant intervals are generally considerably smaller than the MTTF_d values of the channels. Consequently, several channels must fail before the impairment of a test becomes relevant to the system, which is very unlikely as long as the test cycles continue to be much smaller than the $MTTF_d$ of a channel. The situation is fundamentally different in Category 2 structures. In this case, the failure of the test equipment turns a single-channel-tested system into a single-channel-untested system which is no longer able to execute the safety function at the next failure. In addition to requirements for the *DC*, further conditions therefore apply to the simplified assessment of the probability of failure of Category 2 systems:

- All test rates should be at least 100 times greater than the demand rate upon the safety function. This is to ensure that a failure of a test can be detected before a demand upon the safety function fails to be met (see also Annex G, page 347).
- The $MTTF_d$ of the test equipment (TE) should be at least half as high as the $MTTF_d$ of the unit to be tested (L). This assumption ensures that the probability of failure of the test equipment is not unacceptably high.

Should it not be possible to map the functional channel to the blocks I, L and O (or to map the test channel to the blocks TE and OTE), the above condition can be interpreted such that the $MTTF_d$ of the entire test channel must be at least half as high as the $MTTF_d$ of the functional channel. Should this condition be violated (even after capping of the $MTTF_d$ of the functional channel to 100 years), it is of course permissible to calculate the probability of failure using an $MTTF_d$ of the functional channel which is mathematically reduced to double the $MTTF_d$ of the implemented test channel.

Reference

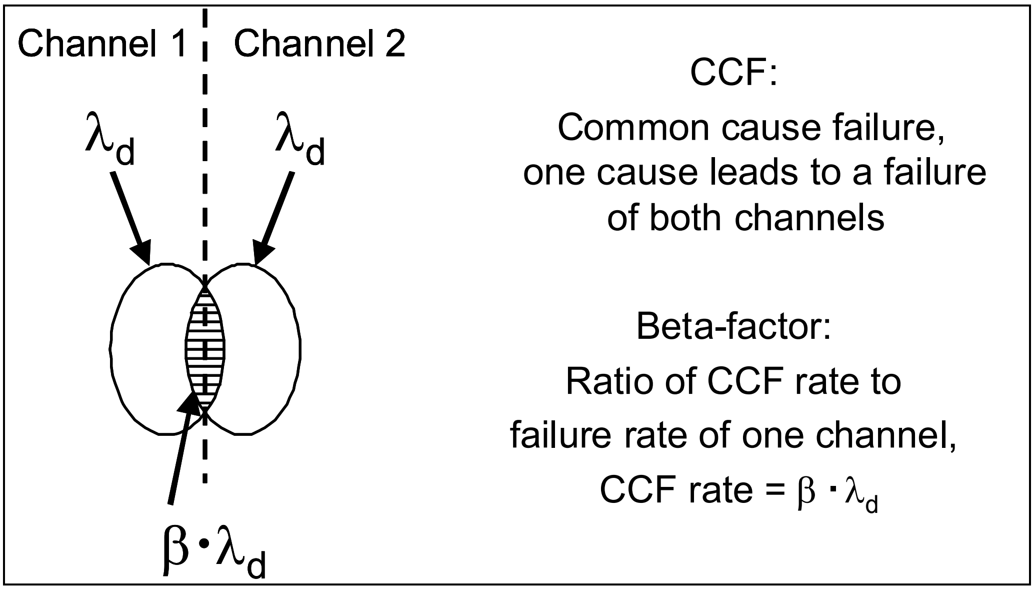
[1] IEC 61508-2: Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 2: Requirements for electrical/electronic/programmable electronic safety-related systems (05.00)

Annex F:
Common cause failure (CCF)

The term common cause failure (CCF) describes the fact that in a redundant system or a single-channel system with external test equipment, several channels may be disabled by one and the same cause. The desired single-fault tolerance of a redundant structure is thus negated. It is therefore important that this source of faults is eliminated as far as possible. The triggers of CCF may be physical in nature, such as over-temperature or strong electromagnetic interference, or systematic, e.g. defective circuit design or programming faults where identical software is employed for both channels.

A common strategy for quantification of a control system's susceptibility to CCF is the beta-factor model. This strategy assumes that a certain proportion of the dangerous failures in one channel share the same cause as dangerous failures in the second channel. This concept is illustrated in Figure F.1: the dangerous failure rates for the two channels (shown symbolically as elliptical areas) have a CCF overlap which is shown by the hatching. The proportionality factor between the CCF rate and the dangerous failure rate of the single channel λ_d is normally termed β (common cause factor or beta factor).

Figure F.1:
Illustration of common cause failure (CCF) by means of the beta-factor model



CCF:
Common cause failure,
one cause leads to a failure
of both channels

Beta-factor:
Ratio of CCF rate to
failure rate of one channel,
CCF rate = $\beta \cdot \lambda_d$

It is virtually impossible to calculate the beta factor precisely for a specific control system, particularly since this should be done at the beginning of the actual design process. IEC 61508-6 [1] employs a points system for this purpose by which β values between 0.5 and 10% can be determined. Points are assigned in a long list of measures sorted according to different causes; when certain rules are applied, the sum of these points results in an estimated β value. EN ISO 13849-1 takes up this method, both in simplified form and with adaptation to machine control system. Simplification is based upon technical measures which experts have considered particularly useful for the avoidance of CCF. This is, however, a compromise, which can be justified empirically, but not scientifically:

- The list of measures against CCF focuses upon the relevant solutions, primarily technical in nature, in machine control systems.
- A single target value with a maximum of 2% was selected instead of several possible β values. The target value can only be either attained or not attained. The simplified method to EN ISO 13849-1 for determining the Performance Level is based upon an assumed β factor of 2%.
- The mathematical rules for the points system were summarized in two steps: each measure can only be either satisfied completely (full number of points) or not satisfied (zero points); no allowance is made for proportional numbers of points for measures which are not completely satisfied. If measures (such as diversity, use of well-tried components) are satisfied completely only in individual SRP/CS in the form of subsystems, different packages of measures may act against CCF at subsystem level. The minimum number of 65 points must be reached for the Categories 2, 3 and 4 in order for the simplified method for determining the Performance Level to be used. A maximum of 100 points can be reached.

The following points must be observed during evaluation of the measures:

- The measures must be evaluated with particular consideration for their effectiveness against CCF. For example, the product standards already require insensitivity to environmental influences and electromagnetic interference. In addition, an evaluation must be performed of whether these influences have been effectively minimized as sources of common cause failures.
- The physical counter-measures differ according to the control technology employed: of the environmental influences, for example, electromagnetic interference is more relevant in the case of electrical control systems, whereas contamination of the fluid is more relevant in the case of fluid control systems. Counter-measures must therefore be evaluated with consideration for the technology employed.
- The tested structure of Category 2 systems constitutes a special case. In this case, CCF concerns failure of both the safety channel and the test channel. A common cause failure results in the structural benefit being negated. The evaluation of the measures must be adjusted accordingly to the particular aspects of the Category 2 structure.
- The full number of points may be credited for a measure against common cause failures which cannot occur owing to the inherent characteristics of the control system.

The measures against common cause failures and the associated numbers of points from EN ISO 13849-1 are as follows:

- Separation (15 points): physical separation of the signal paths, e.g. separate wiring/piping or adequate clearances and creepage distances on printed circuit boards

- Diversity (20 points): different technologies/designs or physical principles are employed in the two control channels. Examples include:
  - One channel employing programmable electronics, the other hard-wired
  - Form of initiation, e.g. pressure and temperature
  - Measurement of distance and pressure
  - Digital and analogue
  - Sourcing of components from different manufacturers
- Design/application/experience: protection against overvoltage, overpressure, overcurrent, etc. (15 points) and the use of well-tried components (5 points)
- Assessment/analysis (5 points): Were the results of a failure mode and effects analysis taken into account during development for the avoidance of common cause failures?
- Competence/training (5 points): Did designers/maintainers receive training which enabled them to identify the reasons for and effects of common cause failures?
- Environmental conditions concerning protection against CCF resulting from contamination and electromagnetic influences, in compliance with the appropriate standards (25 points):
  - Fluid systems: filtration of the pressure medium, prevention of the ingress of dirt, dehumidification of compressed air, for example in compliance with the manufacturer's requirements for purity of the pressure medium
  - Electrical systems: was the system checked for electromagnetic immunity to CCF, for example as set out in the relevant standards?

  On combined fluid power and electrical systems, both aspects must be considered.
- Environmental conditions with regard to other influences (10 points): Were all requirements for resistance to all relevant environmental conditions considered, such as temperature, shock, vibration, humidity (for example as set out in the relevant standards)?

Reference

[1] IEC 61508-6: Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 6: Guidelines on the application of IEC 61508-2 and IEC 61508-3 (04.00)

Annex G: What is the significance of the bar chart in Figure 5 of EN ISO 13849-1?

Unlike its predecessor, EN 954-1 [1], EN ISO 13849-1 makes provision for demonstration of a Performance Level (PL) in addition to examination of the Category. The numerical value of the Performance Level is determined, as shown in Table 6.1 of this report, from the average probability of a dangerous failure per hour, or *PFH*. This value must be determined from the system structure, the failure rates of the components, the level of diagnostic coverage provided by automatic testing, the mission time of the system, and in the case of relevant system structures, the sensitivity of the system to CCF (common cause failure).

Mathematical models are employed for this purpose which take account of the interaction of the stated factors and return the result in the form of the *PFH* (average value over the mission time). The user of the standard should in fact create a custom model for each system to be analysed. For certain common structural variants, the "designated architectures" of EN ISO 13849-1, Section 6.2, (cf. Sections 6.2.1 to 6.2.7 of this report), Markov models have been developed at the BGIA the numerical results of which are compiled in the form of a bar chart in Section 4.5.4, Figure 5 of the standard (Figures 6.10 and G.3 of this report). This dispenses with the need for development of a dedicated mathematical model and for complex calculations, provided the system essentially shares the form of one of the designated architectures, or can be broken down into subsystems which do so (cf. in this context Section 6.3 and Annex H of EN ISO 13849-1, or Section 6.4 of this report). A basic introduction to the Markov modelling technique can be found for example in [2].

For a comprehensible diagram to be obtained, certain restrictions and simplifications have been necessary. Firstly, the standard limits the number of designated architectures and therefore also the number of necessary models. Secondly, the large number of input parameters has been reduced by intelligent grouping. For this purpose, the values $MTTF_d$ and DC_{avg} have been introduced, each of which summarizes several input parameters.

The $MTTF_d$ used in the diagram represents a mean time to failure of each channel in its dangerous failure mode. The $\mathrm{MTTF_d}$ values of several function blocks are combined here to form a single channel $\mathrm{MTTF_d}$ (Chapter 6 and Annex D). All $\mathrm{MTTF_d}$ values are based upon the assumption of constant component failure rates λ_d, hence $MTTF_d = 1/\lambda_d$. In a two-channel structure with different $\mathrm{MTTF_d}$ values by channel, an averaged substitute $\mathrm{MTTF_d}$ value is employed. Conversely, the value DC_{avg} denotes the weighted average value of the diagnostic coverage for the entire system; this value is used for assignment to one of the four $\mathrm{DC_{avg}}$ levels (cf. Table 6.4).

The meaningfulness and permissibility of this summary within the required quantifycation accuracy have been demonstrated by comprehensive test calculations. The same applies to the relationship, permissible in Section 4.5.4 of the standard, between the $\mathrm{MTTF_d}$ values of the test and functional channels in the Category 2 architecture: the $MTTF_d$ of the test equipment must be at least half the $MTTF_d$ for the tested logic. Finally, a requirement is imposed for redundant structures that common cause failures be reduced to an appropriate level: the number of dangerous failures with a common cause must be below 2%. This must be demonstrated in each case by the user of the standard by means of a simple estimation method (Annex F).

The Markov models upon which the bar chart in EN ISO 13849-1 (and Figure G.3 of this report) are based take account of operation of the systems under underlying conditions which are realistic for the machinery sector. They assume that the systems:

- Are subject to at least to one demand upon the safety function per year
- Assume the safe "Operating inhibition" state in response to automatic detection of an internal fault, and are then generally switched off manually shortly afterwards (and at the latest after a few hours)
- Are repaired or replaced and returned to service following assumption of the "Operating inhibition" state or an accident or detected dangerous failure

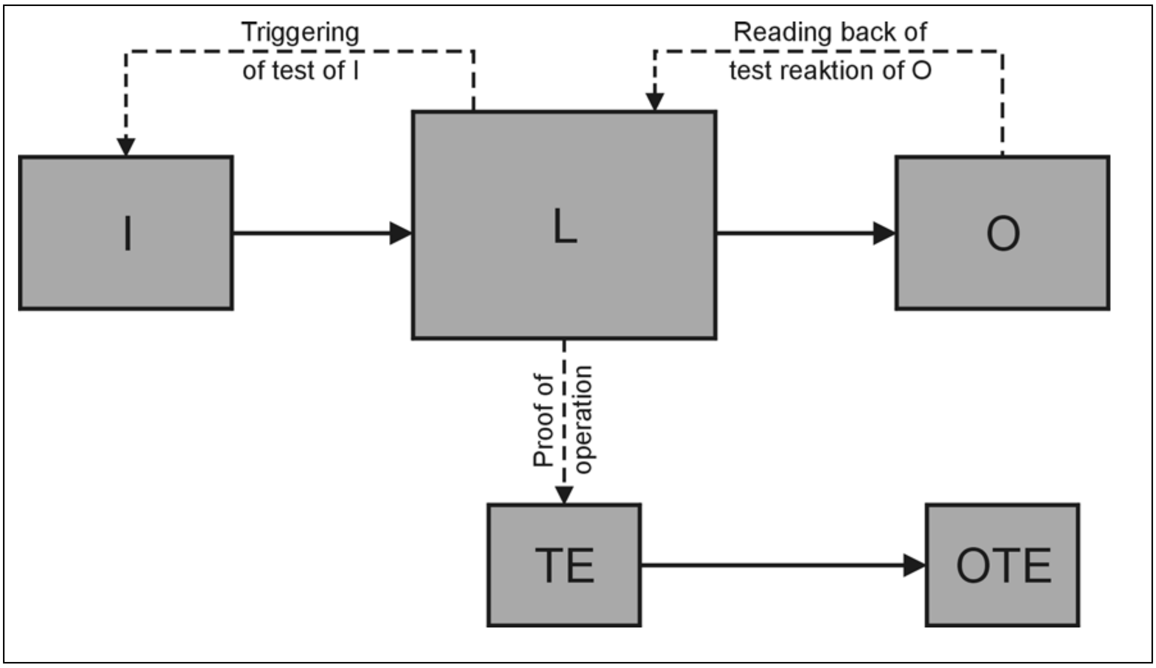
Under these underlying conditions, the quantitative target value for modelling, the *PFH*, represents the average number per hour of demands upon the safety function which are not met owing to failure. In the continuous mode of operation, it indicates the number of dangerous system failures per hour (exception: Category 2, the *PFH* of which has been calculated only for discrete-time demands). Since the *PFH* determined in this way considers only random failures, and not systematic failures and other negative effects, it must be regarded as a theoretical performance value which denotes the safety quality of a design but does not permit conclusions for example regarding the frequency of accidents. This *PFH* is the mathematical quantity indicated on the vertical axis of the bar chart (cf. Figure G.3 of this annex).

Despite consideration being given in principle to demands upon the safety function and to repair, the absolute values for the demand rate and the repair rate (the reciprocal of the mean time to repair) have only a negligible influence upon the *PFH* in this sense. Only for the designated architecture for Category 2 must provision be made for testing at a frequency substantially higher than that of the demand upon the safety function (cf. EN ISO 13849-1, Section 4.5.4; exception: the test interval and the time for the safe response are together shorter than the specified system response time). For this purpose, the standard proposes a test rate which is at least 100 times that of the demand rate. Even down to a ratio of 25 : 1, however, the *PFH* increases only by approximately 10%. For a similar reason, the PFH values determined from the diagram – with the limitation applicable to the Category 2 architecture – apply for any demand rates and any (mean) repair times. (For values lower than one demand per year, the bar chart provides an estimation erring on the safe side.)

The columns for Category B and 1 in Figure G.3 were calculated by means of a model which considers the demand upon the safety function and the repair. The PFH values for these categories can however be approximated very well by the simple relationship $PFH \approx \lambda_d = 1/MTTF_d$. This means simply that the *PFH* of the single-channel untested system (DC = 0) corresponds practically to its dangerous failure rate.

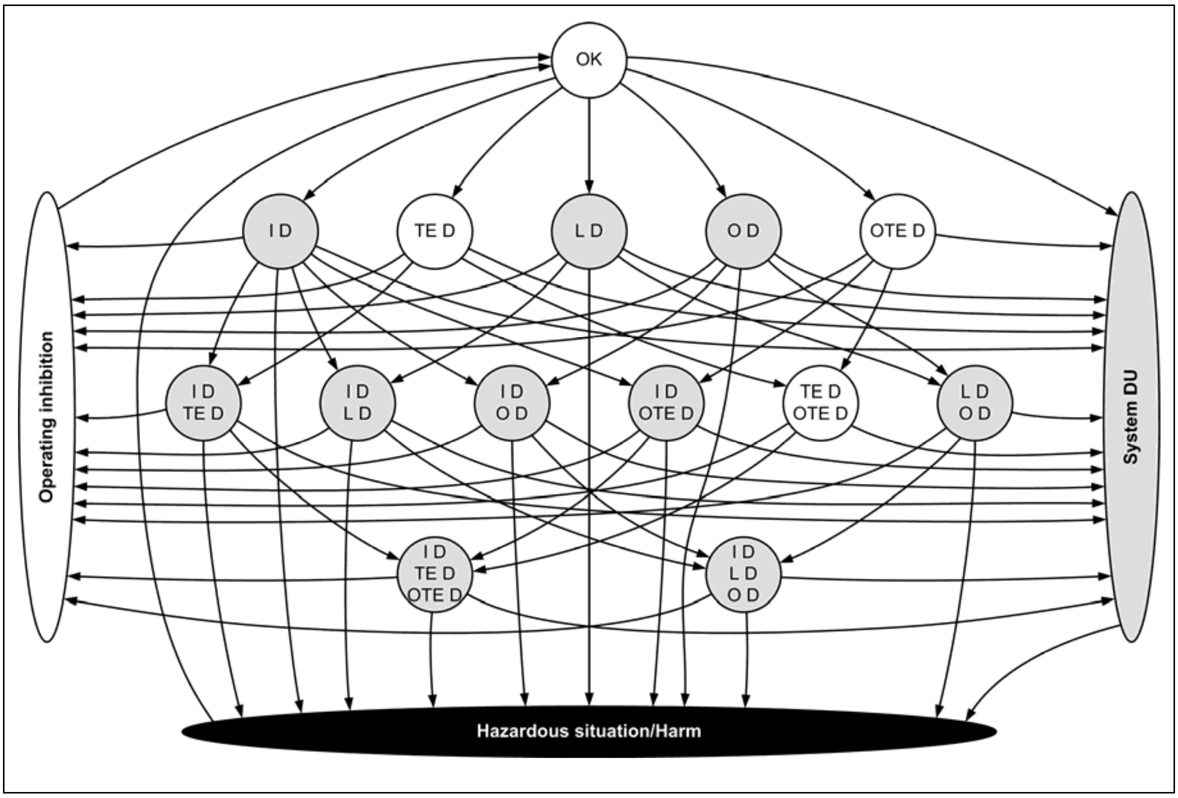
For other categories, however, a more complex method of calculation is required. The principle of the modelling method is explained below with reference to the example of the “designated architecture” for Category 2. This structure is shown again in Figure G.1. Five function blocks are present, of which the blocks I (input), L (logic) and O (output) execute the safety function proper in a logical series arrangement. Block L tests blocks I, O and itself in conjunction with the function block TE (test equipment). The function block OTE (output of TE) is capable of bringing about a safe state in the event of failure of the main I-L-O channel. The additional function blocks TE and OTE, which are not directly essential to the function, thus constitute a form of substitute channel for the fault case which – unlike a “true” second channel – can become active only in the event of faults being detected in the main channel.

Figure G.1:
Designated architecture for Category 2 to EN ISO 13849-1, Section 6.2.2



The state graph in Figure G.2 can be derived from the safety-related block diagram in Figure G.1. To this end, all 2^5 = 32 failure combinations of the five function blocks are first formed. The state without failure is the OK state shown above. It is followed by a series of states in which only one function block has failed, then by a series in which two blocks have failed, and so on. The failed function blocks are each denoted by a following “D” for the function state, indicating that the block concerned has failed dangerously (i.e. unfavourably in safety terms). Failures of function blocks cause consequential states to be reached, indicated here by arrows. States in which the system is no longer capable of executing the safety function are shown in grey. In cases where the failure can be detected and a safe response is therefore possible, a transition exists to the “Operating inhibition” state shown on the left hand side. Of the 32 failure combinations, those in which the system has failed dangerously and undetectably (to itself) are grouped together for simplification of the model. This collective state, denoted “System DU” (dangerous undetectable), is shown on the right. It can be attained from several states as a consequence of the failure of function blocks. The “Hazardous situation/Harm” state can be seen at the bottom of Figure G.2. This state is attained only when a demand is made upon the safety function from dangerous (shown in grey) previous states. Like the “Operating inhibition” state, this state is also transitioned to the OK state by repair. Further transition arrows, for example from “OK” to “System DU”, are the result of simultaneous, common cause failure (CCF) of several function blocks. It is assumed that 2% of the dangerous failures of either of the function blocks L and TE also come along with the other of the two blocks to fail dangerously for the same reason. The same is assumed for the function blocks O and OTE.

Figure G.2:
State graph of the Markov model for the Category 2 designated architecture for determining of the PFH



All arrows are assigned to transition rates the dimension of which is determined by the transition processes concerned (failures, tests, demands, repairs). Consideration of common cause failures (CCF) at different points also results in a change in the original transition rate. For the purpose of calculation of the bar chart, the unfavourable case is assumed in which the test equipment employed in the system is itself not tested. For this reason, a rate of zero is assigned to some transitions in Figure G.2. Systems which test their test equipment are therefore estimated erring on the safe side. For the purpose of simplified calculation by means of the Markov method, it is assumed that all transition processes are characterized by state residence periods which are distributed exponentially, even though this holds true, strictly speaking, only for the constant-rate random failures. Separate considerations justify this simplification.

It is assumed that at the beginning of the mission time, the probability of the system being in the OK state is 1 and the probability of all other possible system states is 0. During the assumed mission time of 20 years, all state probabilities gradually change: beginning at the OK state, they are redistributed along the transition arrows. The sum of the state probabilities remains constant, at one. This also results in a migration over time to the “Hazardous situation/Harm” state, the average time value of which over the 20-year mission time is represented by the PFH, i.e. the average probability of a dangerous failure of the system per hour.

This PFH value is entered on the vertical axis of the bar chart for the different “designated architectures” in accordance with Section 6.2 of the standard (cf. Sections 6.2.3 to 6.2.7 of this report); Categories 2 and 3 are subdivided further according to the average diagnostic coverage (DC_{avg}). The columns are created by variation of the $MTTF_{\mathrm{d}}$, i.e. the mean time to dangerous failure of the (or a) functional channel, for a combination of the architecture (or the associated Markov model) and the DC_{avg}. The Markov model for Figure G.2 could for example be used to calculate the two columns for the designated Category 2 architecture. (For mathematical reasons, an equivalent substitute model differing from this model was used in practice. This model is not presented here, since its relationship to the block diagram in Figure G.1 is less transparent. The substitute model delivers virtually identical results.) The other columns are based upon further Markov models which were also developed in accordance with the principles described above for the corresponding designated architectures.

According to Table 6.1, the PFH intervals were assigned to the Performance Levels a to e on the logarithmic PFH scale. This is shown in Figure G.3 (see page 354), in which an additional PFH scale has been added to Figure 5 of EN ISO 13849-1.

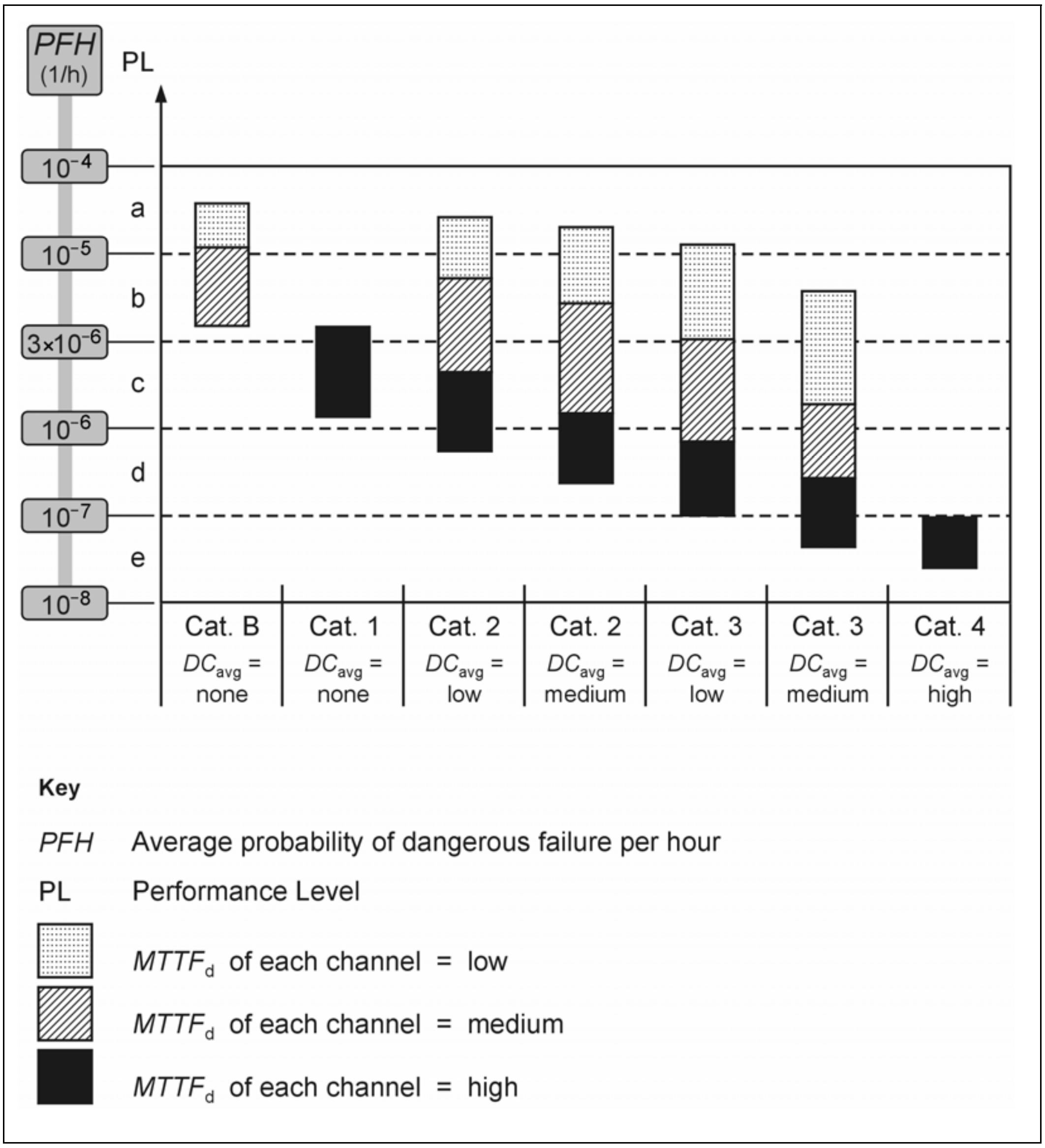
The PFH interval of 10^{-6} per hour to 10^{-5} per hour has a particular peculiarity. It is mapped to the two adjacent Performance Levels b and c. Division of the logarithmic scale in the middle places the boundary between Performance Levels b and c at the geometric mean of 10^{-6} per hour and 10^{-5} per hour, i.e. at $\sqrt{10} \times 10^{-6}/\mathrm{h} \approx 3 \times 10^{-6}$ per hour. Assignment of PFH intervals and Performance Levels corresponds essentially to Table 6.1 and to IEC 61508-5, Figure D.2; see [3; 4].

Annex K of the standard contains the numerical content of Figure G.3 in the form of Table K.1. Table K.1 can be used to determine the Performance Level more precisely than is possible by means of the figure; this is particularly useful when the PFH contributions of several cascaded subsystems require summation. Conversely, the bar chart provides, above all, a swift overview of the suitability of various technical solutions for the PL, and can therefore be used to make a preliminary selection. The information in Table K.1 of the standard is also contained in the “Performance Level Calculator” (PLC), a convenient disk card which can be used for determining of the PL and which can be obtained from the BGIA (among other sources) [5].

Occasionally, the DC_{avg} value determined for a system may lie only slightly below one of the thresholds “low” (60%), “medium” (90%) or “high” (99%). If the simplified quantification method in EN ISO 13849-1 is then applied, formal constraints require that the next-lower DC_{avg} level, i.e. “none”, “low” or “medium”, be used. This procedure provides an estimation of the system which errs on the safe side. Owing to the small number of graduations on the DC_{avg} scale, however, a minor change to the system which has the effect of causing the DC_{avg} value to drop just below one of the thresholds may result in a substantially poorer assessment of the system. This may occur even when components with high-quality testing (a high DC) in a channel are replaced by superior components (with a higher $MTTF_{\mathrm{d}}$) (cf. the DC_{avg} formula in

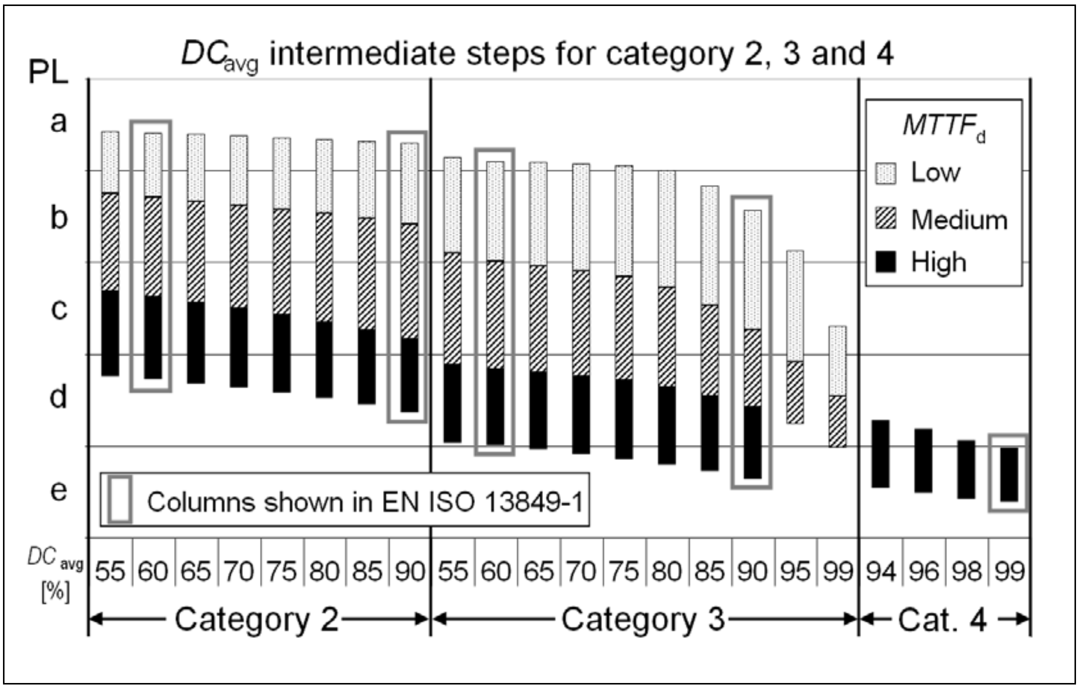
Section 6.2.14). The minor improvement in the channel $\mathrm{MTTF_d}$ is then over-compensated for by the formal reduction of the DC_{avg} to the next lower value, as a result of which the PFH value which is determined becomes poorer (i.e. greater). This effect, which appears paradoxical, is a consequence of the coarse division of the $\mathrm{DC_{avg}}$ scale, i.e. ultimately of the simplicity of Figure 5 (and Table K.1) of the standard; cf. Figure G.3 of this report.

Figure G.3:
PFH and Performance Level as a function of the Category, *DC* and $MTTF_{\mathrm{d}}$



The described effect can be prevented or improved by use of a graph with a finer scale for $\mathrm{DC_{avg}}$ values in place of Figure G.3 (Figure G.4). In consideration of the limited accuracy of $\mathrm{DC_{avg}}$ values (cf. EN ISO 13849-1, Table 6, Note 2), the minimum possible $\mathrm{DC_{avg}}$ values were also considered for all Categories. The BGIA “SISTEMA” software utility (see Annex H, page 355) can be used to determine the PFH. SISTEMA even interpolates between the columns shown in Figure G.4. Generally, a major downgrading of the DC_{avg} can be avoided, and PFH values often obtained which are both more precise and superior.

Figure G.4:
Performance Level with finer resolution of the DC_{avg} scale
(extended modification of Figure 5 from EN ISO 13849-1)



References

[1] EN 954-1: Safety of machinery – Safety-related parts of control systems – Part 1: General principles for design (12.96)

[2] *Goble, W. M.*: Control systems safety evaluation and reliability. 2nd ed. Ed.: Instrumentation, Systems, and Automation Society (ISA), Research Triangle Park, North Carolina, 1998

[3] IEC 61508-1: Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 1: General requirements (12.98 + Corrigendum 1 05.99)

[4] IEC 61508-5: Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 5: Examples of methods for the determination of safety integrity levels (11.98 + Corrigendum 1 04.99)

[5] *Schaefer, M.; Hauke, M.*: Performance Level Calculator – PLC. 2nd ed. Ed.: BGIA – Institut für Arbeitsschutz der Deutschen Gesetzlichen Unfallversicherung, Sankt Augustin; Zentralverband Elektrotechnik- und Elektronikindustrie (ZVEI) e.V. – Fachverband Automation, Frankfurt am Main, and Verband Deutscher Maschinen- und Anlagenbau e.V. – VDMA, Frankfurt am Main 2007. www.dguv.de/bgia, Webcode e20892

Annex H:
SISTEMA: the software tool for evaluation of SRP/CS

H1 What is SISTEMA capable of?

The SISTEMA software utility (Safety Integrity Software Tool for the Evaluation of Machine Applications) provides developers and testers of safety-related machine controls with comprehensive support in the evaluation of safety in the context of EN ISO 13849-1. The tool, which runs on Windows, enables users to model the structure of the safety-related control components based upon the “designated architectures”, and ultimately permits automated calculation of the reliability values at various levels of detail, including that of the attained Performance Level (PL).

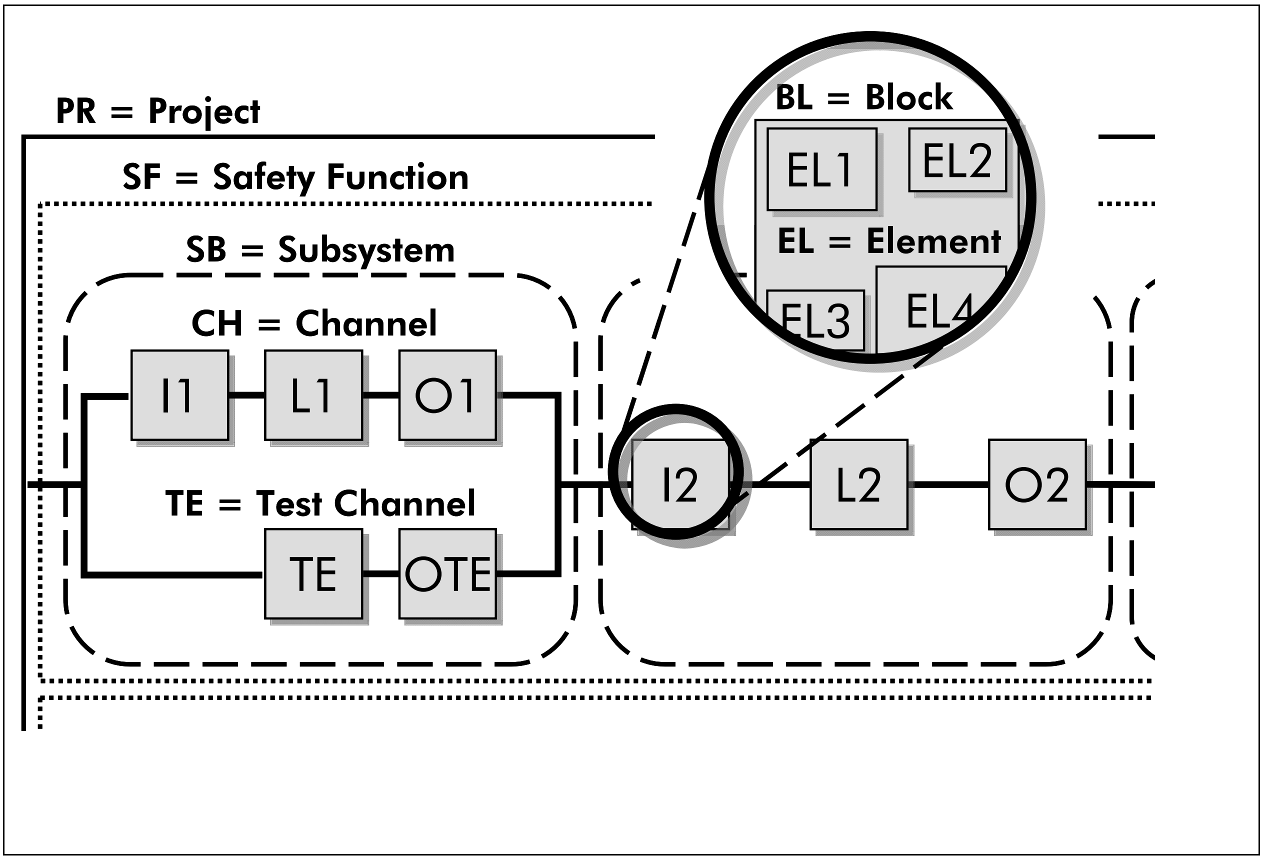
Relevant parameters such as the risk parameters for determining the required Performance Level (PL_r), the Category of the SRP/CS, measures against common cause failures (CCF) on multi-channel systems, the average component quality ($MTTF_d$) and the test quality (DC) of components and blocks are entered step by step in input dialogs. Once the required data have been entered into SISTEMA, the results are calculated and displayed instantly. A practical advantage for the user is that each parameter change is reflected immediately on the user interface with its impact upon the entire system. Users are spared time consuming consultation of tables and calculation of formulae (calculation of the $MTTF_d$ by means of the parts count method, symmetrization of the $MTTF_d$ for each channel, estimation of the DC_{avg}, calculation of the PFH and PL etc.), since these tasks are performed by the software. This enables the user to vary parameter values and to assess the effects of changes with little effort. The final results can be printed out in a summary document.

H2 How is SISTEMA used?

SISTEMA processes basic elements from a total of six hierarchy levels: The project (PR), the safety function (SF), the subsystem (SB), the channel (CH)/test channel (TE), the block (BL) and the element (EL). The relationship between them is shown briefly below (Figure H.1, page 356).

The user first opens a project, after which he can define the machine/hazardous zone which is to be analysed. All required safety functions are assigned to the project. The safety functions can be defined and documented by the user, and a PL_r assigned to them. The PL actually attained by the parameterized SRP/CS is determined automatically from the subsystems which – in a series arrangement – execute the safety function. Each subsystem is based upon a designated architecture from the standard, as a function of the selected Category. The architecture determines, among other things, whether the control system is of single-channel, single-channel-tested or redundant design, and whether a special test channel must be considered during evaluation. Each channel can in turn be subdivided into any desired number of blocks, for which the user enters either an $MTTF_d$ value and a DC value directly or, on the lowest hierarchy level, the values for the individual components of which the block is composed.

Figure H.1:
Hierarchy levels considered in SISTEMA



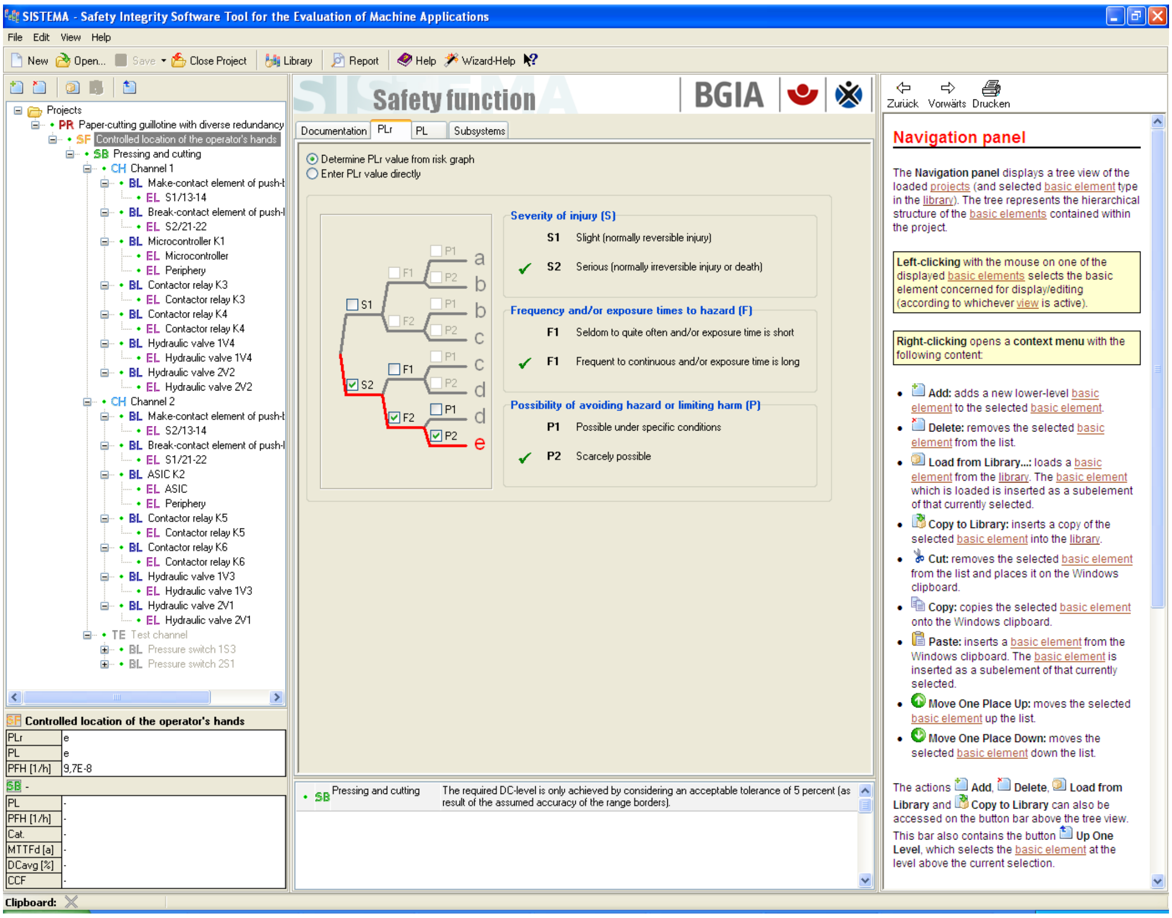
User friendly library functions complete SISTEMA's functionality. The libraries supplied contain certain standard elements in the form of elements, blocks and complete subsystems which can however be extended as desired by the user. Where additional library modules are available from manufacturers for their components they can be installed retrospectively as an option.

H3 The SISTEMA user interface

The SISTEMA user interface is divided into four areas (see Figure H.2). The greater part of the interface is occupied by the workspace in the centre. Depending upon which view is active the workspace contains an editable input dialog or a partial view of the overview document. The content of the active view is determined by the basic element selected from the hierarchy described above and is selected from a tree view on the left hand side.

Each branch in the tree view represents one basic element. Basic elements can be created, deleted, moved or copied in the tree view. The details of the selected basic element are entered in the input dialog in the editing view. Each input dialog is further sub-divided into different areas by tabs. The final tab in each input dialog contains a table summarizing all lower level branches and listing the main information. If, for example, the user has marked a block in the tree view, this table shows all elements contained within it, together with their $MTTF_d$ and DC values.

Figure H.2:
SISTEMA user interface



● Determine PLr value from risk graph
○ Enter PLr value directly

Severity of injury (S)

S1 Slight (normally reversible injury)
✓ S2 Serious (normally irreversible injury or death)

Frequency and/or exposure times to hazard (F)

F1 Seldom to quite often and/or exposure time is short
✓ F1 Frequent to continuous and/or exposure time is long

Possibility of avoiding hazard or limiting harm (P)

P1 Possible under specific conditions
✓ P2 Scarcely possible

SF Controlled location of the operator's hands

PLr	e
PL	e
PFH [1/h]	9,7E-8

SB -

PL	-
PFH [1/h]	-
Cat.	-
MTTFd [a]	-
DCavg [%]	-
CCF	-

•	SB	Pressing and cutting	The required DC-level is only achieved by considering an acceptable tolerance of 5 percent (as result of the assumed accuracy of the range borders).

Navigation panel

The **Navigation panel** displays a tree view of the loaded projects (and selected basic element type in the library). The tree represents the hierarchical structure of the basic elements contained within the project.

Left-clicking with the mouse on one of the displayed basic elements selects the basic element concerned for display/editing (according to whichever view is active).

Right-clicking opens a **context menu** with the following content:

- **Add:** adds a new lower-level basic element to the selected basic element.
- **Delete:** removes the selected basic element from the list.
- **Load from Library...:** loads a basic element from the library. The basic element which is loaded is inserted as a subelement of that currently selected.
- **Copy to Library:** inserts a copy of the selected basic element into the library.
- **Cut:** removes the selected basic element from the list and places it on the Windows clipboard.
- **Copy:** copies the selected basic element onto the Windows clipboard.
- **Paste:** inserts a basic element from the Windows clipboard. The basic element is inserted as a subelement of that currently selected.
- **Move One Place Up:** moves the selected basic element up the list.
- **Move One Place Down:** moves the selected basic element down the list.

The actions **Add**, **Delete**, **Load from Library** and **Copy to Library** can also be accessed on the button bar above the tree view. This bar also contains the button **Up One Level**, which selects the basic element at the level above the current selection.

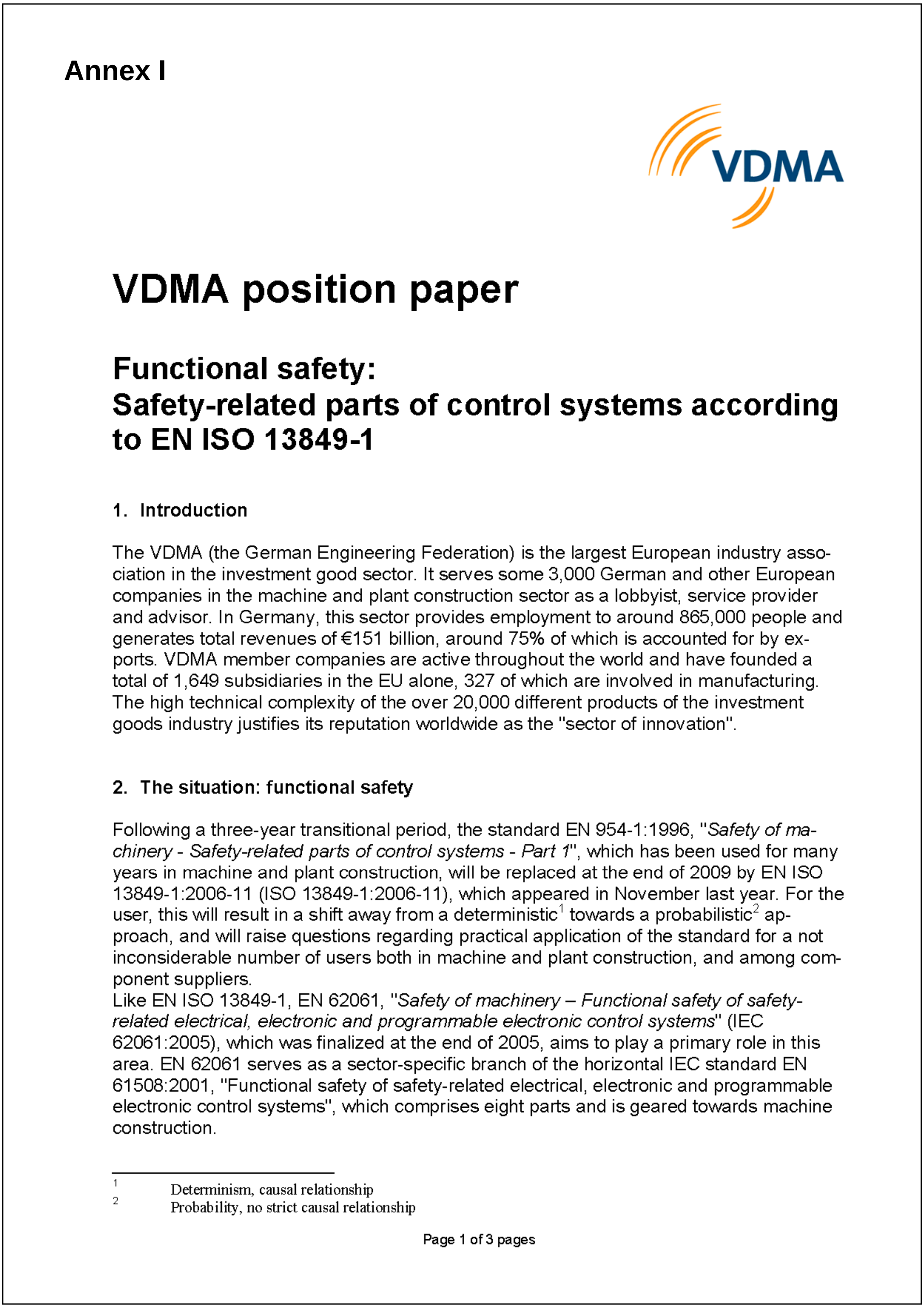
The tree view also shows status information for each basic element. The status information takes the form of a coloured dot adjacent to the branch. A red dot indicates that a condition of the standard is not satisfied, that a limit value is exceeded or that a required value cannot be calculated because of a general inconsistency. A warning is output in this case. A yellow dot indicates a non-critical message (e.g. a basic element has not yet been named). All other basic elements are marked with a green dot. The colour marking is also always inherited by the branches higher up in the hierarchy, red having the highest and green the lowest priority. All warnings and information concerning the active basic element are displayed in the message window below the workspace.

The area below the tree view shows the main context information for the selected basic element. This information comprises the PL, *PFH*, *MTTF*$_d$, *DC*$_{avg}$ and CCF of the higher level subsystem, and the PL$_r$, PL and *PFH* of the higher level safety function (this applies, of course, only to basic elements on lower hierarchy levels). The consequences of any changes to the displayed parameters are thus displayed immediately to the user.

In addition to its flexibility, the SISTEMA user interface is notable for its ease of use and intuitiveness. Context help on the right-hand side facilitates the learning process. The wizard supplied with the application offers further help: it supports new users step by step in the virtual modelling of their control systems, and assures rapid access.

H4 Where can SISTEMA be obtained from?

The SISTEMA software can be downloaded from the BGIA's website. SISTEMA is now available in German and English. Versions in other languages are to follow. Following registration, the tool will be available as freeware for use and distribution free of charge. Up-to-date information and the link for the download can be found at www.dguv.de/bgia, Webcode e34183.



Annex I

VDMA position paper

Functional safety: Safety-related parts of control systems according to EN ISO 13849-1

1. Introduction

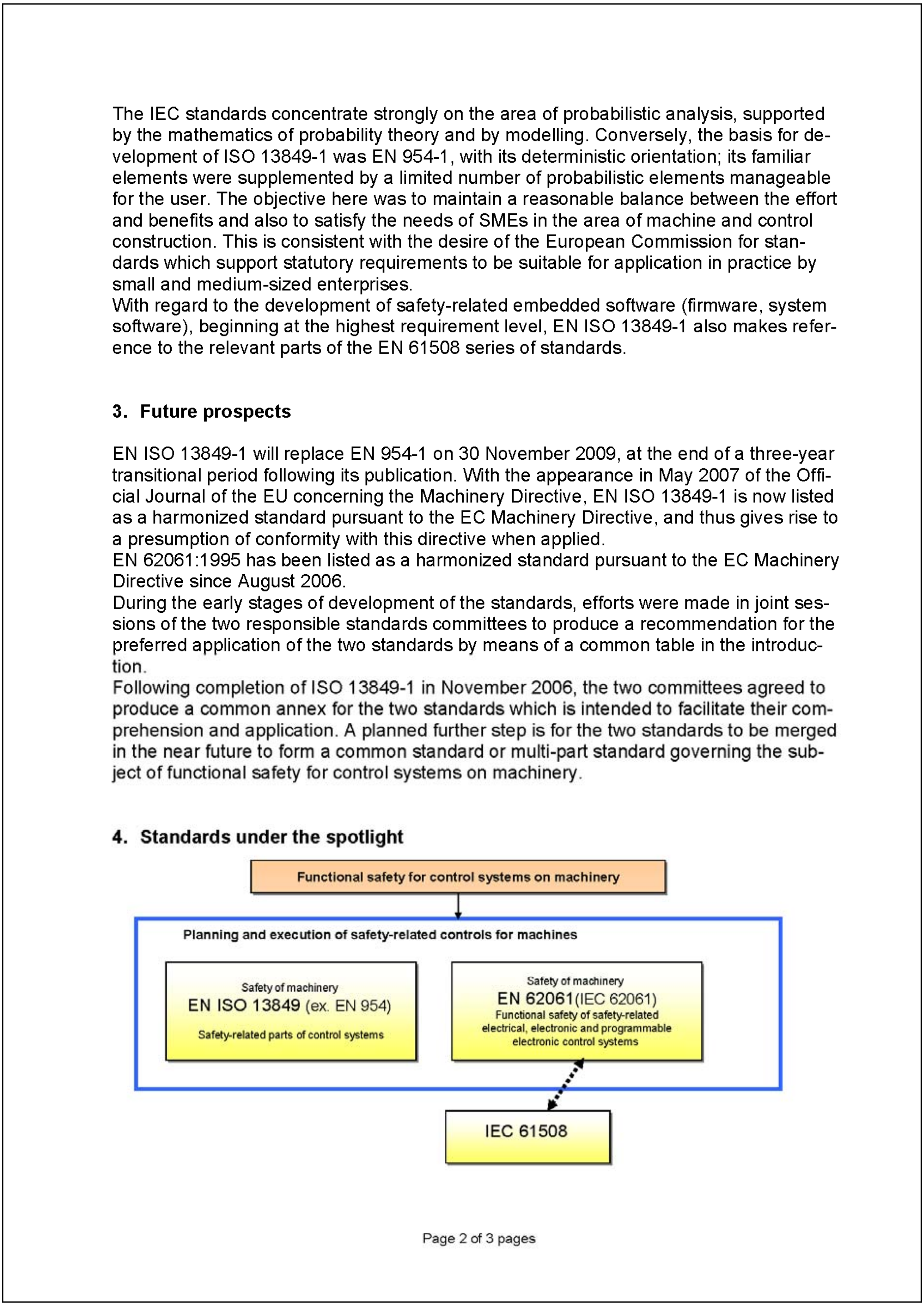
The VDMA (the German Engineering Federation) is the largest European industry association in the investment good sector. It serves some 3,000 German and other European companies in the machine and plant construction sector as a lobbyist, service provider and advisor. In Germany, this sector provides employment to around 865,000 people and generates total revenues of €151 billion, around 75% of which is accounted for by exports. VDMA member companies are active throughout the world and have founded a total of 1,649 subsidiaries in the EU alone, 327 of which are involved in manufacturing. The high technical complexity of the over 20,000 different products of the investment goods industry justifies its reputation worldwide as the "sector of innovation".

2. The situation: functional safety

Following a three-year transitional period, the standard EN 954-1:1996, "*Safety of machinery - Safety-related parts of control systems - Part 1*", which has been used for many years in machine and plant construction, will be replaced at the end of 2009 by EN ISO 13849-1:2006-11 (ISO 13849-1:2006-11), which appeared in November last year. For the user, this will result in a shift away from a deterministic[1] towards a probabilistic[2] approach, and will raise questions regarding practical application of the standard for a not inconsiderable number of users both in machine and plant construction, and among component suppliers.
Like EN ISO 13849-1, EN 62061, "*Safety of machinery – Functional safety of safety-related electrical, electronic and programmable electronic control systems*" (IEC 62061:2005), which was finalized at the end of 2005, aims to play a primary role in this area. EN 62061 serves as a sector-specific branch of the horizontal IEC standard EN 61508:2001, "Functional safety of safety-related electrical, electronic and programmable electronic control systems", which comprises eight parts and is geared towards machine construction.

[1] Determinism, causal relationship

[2] Probability, no strict causal relationship



The IEC standards concentrate strongly on the area of probabilistic analysis, supported by the mathematics of probability theory and by modelling. Conversely, the basis for development of ISO 13849-1 was EN 954-1, with its deterministic orientation; its familiar elements were supplemented by a limited number of probabilistic elements manageable for the user. The objective here was to maintain a reasonable balance between the effort and benefits and also to satisfy the needs of SMEs in the area of machine and control construction. This is consistent with the desire of the European Commission for standards which support statutory requirements to be suitable for application in practice by small and medium-sized enterprises.

With regard to the development of safety-related embedded software (firmware, system software), beginning at the highest requirement level, EN ISO 13849-1 also makes reference to the relevant parts of the EN 61508 series of standards.

3. Future prospects

EN ISO 13849-1 will replace EN 954-1 on 30 November 2009, at the end of a three-year transitional period following its publication. With the appearance in May 2007 of the Official Journal of the EU concerning the Machinery Directive, EN ISO 13849-1 is now listed as a harmonized standard pursuant to the EC Machinery Directive, and thus gives rise to a presumption of conformity with this directive when applied.

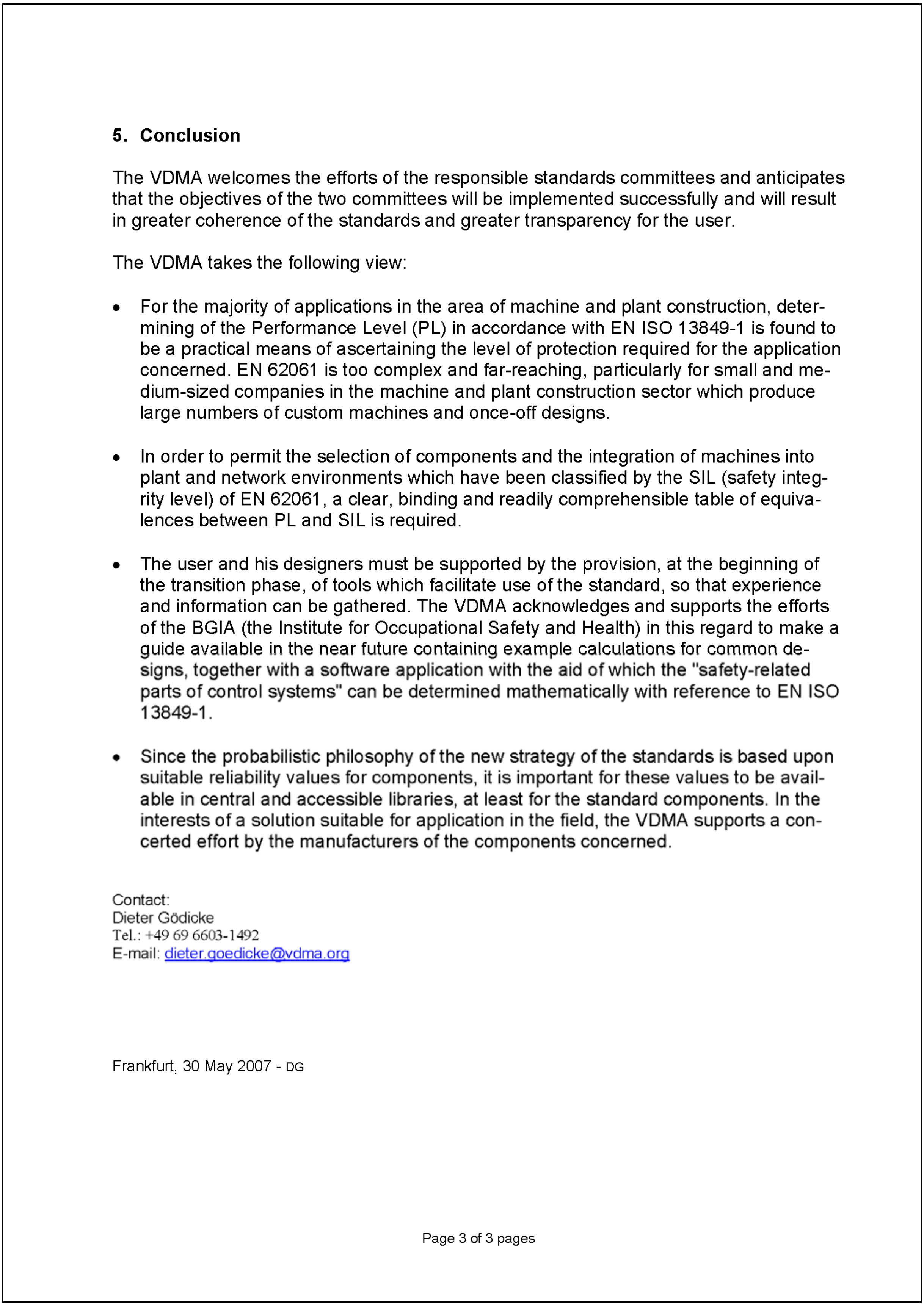
EN 62061:1995 has been listed as a harmonized standard pursuant to the EC Machinery Directive since August 2006.

During the early stages of development of the standards, efforts were made in joint sessions of the two responsible standards committees to produce a recommendation for the preferred application of the two standards by means of a common table in the introduction.

Following completion of ISO 13849-1 in November 2006, the two committees agreed to produce a common annex for the two standards which is intended to facilitate their comprehension and application. A planned further step is for the two standards to be merged in the near future to form a common standard or multi-part standard governing the subject of functional safety for control systems on machinery.

4. Standards under the spotlight

Functional safety for control systems on machinery
Planning and execution of safety-related controls for machines
Safety of machinery
EN ISO 13849 (ex. EN 954)
Safety-related parts of control systems
Safety of machinery
EN 62061 (IEC 62061)
Functional safety of safety-related electrical, electronic and programmable electronic control systems
IEC 61508



5. Conclusion

The VDMA welcomes the efforts of the responsible standards committees and anticipates that the objectives of the two committees will be implemented successfully and will result in greater coherence of the standards and greater transparency for the user.

The VDMA takes the following view:

- For the majority of applications in the area of machine and plant construction, determining of the Performance Level (PL) in accordance with EN ISO 13849-1 is found to be a practical means of ascertaining the level of protection required for the application concerned. EN 62061 is too complex and far-reaching, particularly for small and medium-sized companies in the machine and plant construction sector which produce large numbers of custom machines and once-off designs.

- In order to permit the selection of components and the integration of machines into plant and network environments which have been classified by the SIL (safety integrity level) of EN 62061, a clear, binding and readily comprehensible table of equivalences between PL and SIL is required.

- The user and his designers must be supported by the provision, at the beginning of the transition phase, of tools which facilitate use of the standard, so that experience and information can be gathered. The VDMA acknowledges and supports the efforts of the BGIA (the Institute for Occupational Safety and Health) in this regard to make a guide available in the near future containing example calculations for common designs, together with a software application with the aid of which the "safety-related parts of control systems" can be determined mathematically with reference to EN ISO 13849-1.

- Since the probabilistic philosophy of the new strategy of the standards is based upon suitable reliability values for components, it is important for these values to be available in central and accessible libraries, at least for the standard components. In the interests of a solution suitable for application in the field, the VDMA supports a concerted effort by the manufacturers of the components concerned.

Contact:
Dieter Gödicke
Tel.: +49 69 6603-1492
E-mail: dieter.goedicke@vdma.org

Frankfurt, 30 May 2007 - DG

Annex J: Index

Page

Page

Page