



7/2013e

IFA Report



Safe drive controls
with frequency converters



Authors: Ralf Apfeld, Helmut Zilligen, Burkhard Köhler
Institut für Arbeitsschutz der Deutschen Gesetzlichen Unfallversicherung (IFA)
Alte Heerstr. 111
53757 Sankt Augustin
Germany
Phone: 0049 2241 23102
Fax: 0049 2241 2312234
Internet: www.dguv.de/ifa
Email: ifa@dguv.de

Database of publications: www.dguv.de/publikationen

Published by: Deutsche Gesetzliche Unfallversicherung e. V. (DGUV)
Mittelstr. 51
10117 Berlin
Germany
Phone: 0049 30 288763800
Fax: 0049 30 288763808
Internet: www.dguv.de
Email: info@dguv.de

– September 2014 –

Graphics and layout: Deutsche Gesetzliche Unfallversicherung e. V. (DGUV)

ISBN: 978-3-86423-131-5

ISSN: 2190-7994

Abstract

Safe drive controls with frequency converters

Machine drives with speed control are state of the art. As on drives without speed control, variable speed of movement of a machine part frequently gives rise to a hazard against which the users of the machine must be protected. The simplest means of preventing movements during manual intervention in danger zones is the (safe) disconnection of the energy driving the relevant motors. This is however often not possible, for example when intervention is required whilst the machine is running for the purpose of clearing faults, setup, during test operation, etc. Such cases require the machine to be operated with protective equipment disabled. In order to assure the user's safety despite this, the hazardous movements are performed in such cases at safely limited speeds and/or torques, and frequently in inching mode and/or only when an enabling switch is actuated. Safety functions for drive controls have been defined for implementation of the machine functions required for this purpose. Examples are STO (safe torque off), SLS (safely-limited speed) and

SS1 (safe stop 1). This report is intended for parties using drive control equipment who wish to use safety functions at a certain Performance Level to EN ISO 13849-1 in consideration of the application and risks. The basic safety functions of drive controls and the requirements relating to their use are presented. The principles of operation of frequency converters and DC-DC converters are described, and the concept of integrated safety functions explained. Examples of applied circuits are shown by which the various machine safety functions can be implemented. The corresponding SISTEMA files for quantification of these safety functions are available for download free of charge. The examples include both standard frequency converters and frequency converters with integral safety functions.

This report supplements BGIA Report 2/2008e, "Functional safety of machine controls", and requires a basic understanding of Categories and Performance Levels.

Kurzfassung

Sichere Antriebssteuerungen mit Frequenzumrichtern

Drehzahlgeregelte Antriebe sind an Maschinen Stand der Technik. Genau wie bei unregulierten Antrieben löst die drehzahlveränderliche Bewegung eines Maschinenteils häufig eine Gefährdung aus, vor der die Bedienpersonen geschützt werden müssen. Die einfachste Lösung zur Vermeidung von Bewegungen bei manuellen Eingriffen in Gefahrstellen ist das (sichere) Abschalten der Antriebsenergie der jeweiligen Motoren. Dies ist jedoch häufig nicht möglich, z. B. wenn zur Störungsbehebung, zum Einrichten, im Probetrieb usw. Eingriffe bei laufender Maschine notwendig sind. In diesen Fällen ist der Maschinenbetrieb bei aufgehobener Schutzwirkung von Schutzeinrichtungen erforderlich. Um trotzdem die Sicherheit der Beschäftigten zu gewährleisten, werden die gefahrbringenden Bewegungen dann bei sicher begrenzten Geschwindigkeiten, Drehzahlen, Drehmomenten und häufig im Tippbetrieb und/oder nur während ein Zustimmungsschalter betätigt wird, ausgeführt. Zur Realisierung der hierfür notwendigen Maschinenfunktionen wurden Sicherheitsfunktionen für Antriebssteuerungen definiert, wie z. B. STO (Sicher abgeschaltetes Moment), SLS (Sicher begrenzte Geschwindigkeit) und SS1 (Sicherer Stopp 1).

Es wird der Einsatz von Antriebssteuergeräten behandelt, die abhängig von Applikation und Risiken, Sicherheitsfunktionen in einem bestimmten Performance Level nach DIN EN ISO 13849-1 umsetzen. Die grundlegenden Sicherheitsfunktionen von Antriebssteuerungen und die Anforderungen bei deren Anwendung werden vorgestellt. Die prinzipielle Funktionsweise von Frequenzumrichtern und Gleichstromstellern wird beschrieben und das Konzept der Integration von Sicherheitsfunktionen erläutert. In Beispielen werden Applikationsschaltungen gezeigt, mit denen unterschiedliche Sicherheitsfunktionen an Maschinen realisiert werden. Die jeweiligen SISTEMA-Dateien zur Quantifizierung dieser Sicherheitsfunktionen stehen zum kostenlosen Download bereit. In den Beispielen finden sowohl Standardfrequenzumrichter Anwendung als auch Frequenzumrichter mit integrierten Sicherheitsfunktionen.

Dieser Report versteht sich als Ergänzung zum BGIA-Report 2/2008 "Funktionale Sicherheit von Maschinensteuerungen" und setzt Grundkenntnisse über Kategorien und Performance Level voraus.

Résumé

Commandes d'entraînement sûres avec convertisseurs de fréquence

La plupart des machines modernes sont équipées d'entraînements dont la vitesse est régulée. Comme pour les entraînements dont la vitesse n'est pas régulée, le déplacement à vitesse variable d'un organe de machine crée souvent un danger, qui nécessite une protection des opérateurs. La solution la plus simple pour empêcher des déplacements d'organes de machine lors d'interventions manuelles dans des zones de danger est la coupure (sûre) de l'alimentation en énergie des moteurs de ces organes de machine. Cependant, ceci n'est fréquemment pas possible, par exemple lorsqu'il est nécessaire d'effectuer des interventions sur une machine en fonctionnement pour éliminer des défauts, procéder à des réglages ou des marches d'essai, etc. Dans ces cas, la machine doit fonctionner bien que des dispositifs de protection soient désactivés. Pour que la sécurité de l'opérateur soit malgré tout assurée, les déplacements pouvant présenter un danger pour celui-ci sont exécutés fréquemment en mode manuel à vue et / ou uniquement pendant qu'un bouton d'assentiment est actionné, à des vitesses et avec des couples limités de façon sûre. Pour la réalisation des fonctions machine nécessaires à cet effet, des fonctions de sécurité pour commandes d'entraînement, telles que STO (Suppression sûre du couple), SLS (Vitesse limitée de

façon sûre), SS1 (Arrêt sûr 1) par exemple, ont été définies. Ce compte rendu s'adresse aux utilisateurs de variateurs de vitesse qui, en fonction de l'application et des risques, désirent mettre en œuvre des fonctions de sécurité ayant un Performance Level déterminé (EN ISO13849-1). Les fonctions de sécurité de base de commandes d'entraînement et les exigences qui doivent être satisfaites lors de leur utilisation sont présentées. Les principes de fonctionnement des convertisseurs de fréquence et des hacheurs sont décrits, et le concept d'intégration de fonctions de sécurité est expliqué à l'aide d'exemples de montages permettant de réaliser diverses fonctions de sécurité à des machines. Les fichiers SISTEMA correspondants pour la quantification de ces fonctions de sécurité peuvent être téléchargés gratuitement. Les exemples comportent aussi bien des convertisseurs de fréquence standards que des convertisseurs de fréquence avec fonctions de sécurité intégrées.

Ce compte rendu complète le compte rendu BGIA 2/2008e "Functional safety of machine controls" (« Sécurité fonctionnelle de commandes de machines ») et requiert des connaissances de base sur les catégories et les Performance Level.

Resumen

Controles de los accionamientos seguros con los convertidores de frecuencia

Los accionamientos con regulación de revoluciones en máquinas forman parte de la tecnología más avanzada. Exactamente del mismo modo que en los accionamientos sin regulación, el movimiento variable de revoluciones de un componente de la máquina a menudo conlleva un riesgo del que los operarios de máquinas deben protegerse. La solución más sencilla para evitar los movimientos durante las intervenciones manuales en los puntos peligrosos es la desconexión (segura) de la energía de los accionamientos de los motores respectivos. No obstante, esto a menudo no es posible, p. ej. cuando se requiere que la máquina esté en marcha para subsanar a averías, hacer ajustes, realizar una prueba de funcionamiento u otras intervenciones. En dichos casos, se requiere anular el efecto protector de los dispositivos de protección durante el funcionamiento de la máquina. A pesar de ello, para garantizar la seguridad del usuario, los movimientos que implican un riesgo se ejecutan a velocidades, revoluciones, pares de torsión limitados de forma segura y a menudo durante el modo por impulsos o solamente mientras esté pulsado un conmutador de autorización. Para ejecutar las funciones de la máquina necesarias, se han definido funciones de seguridad para los controles de los accionamientos, como p. ej. STO (momento de desconexión segura), SLS (velocidad

limitada segura), SS1 (parada segura 1). Este informe va dirigido a los usuarios de los aparatos de control de los accionamientos que quieren emplear las funciones de seguridad que dependen de la aplicación y los riesgos en un nivel de prestaciones determinado conforme a DIN EN ISO13849-1. Se presentan las funciones de seguridad básicas de los controles de accionamiento y los requisitos para su empleo. Se describe el funcionamiento principal de los convertidores de frecuencia y los interruptores periódicos y se explica el concepto de la integración de las funciones de seguridad. En los ejemplos se muestran conmutaciones de aplicación con las que se pueden llevar a cabo diferentes funciones de seguridad en máquinas. Los archivos de SISTEMA respectivos para cuantificar estas funciones de seguridad están disponibles para descargar gratuitamente. En los ejemplos se emplean tanto convertidores de frecuencia estándares, como también convertidores de frecuencia con funciones de seguridad integradas.

Este informe es una ampliación del informe 2/2008 de BGIA “Functional safety of machine controls” (“Seguridad funcional de los controles de máquinas”) y presupone unos conocimientos básicos de categorías y niveles de prestaciones.

Contents

1	Introduction	9
2	Risk reduction	11
2.1	Actors in safety functions	11
2.2	Overlapping hazards	11
3	Drive control devices employed as safety-related parts of control systems	13
3.1	Description of the safety functions	14
3.1.1	Stop functions	14
3.1.1.1	Safe torque off (STO)	14
3.1.1.2	Safe stop 1 (SS1)	15
3.1.1.3	Safe stop 2 (SS2)	16
3.1.2	Other safety functions	16
3.1.2.1	Safe operating stop (SOS)	17
3.1.2.2	Safely-limited speed (SLS)	17
3.1.2.3	Safely-limited torque (SLT)	17
3.1.2.4	Safely-limited increment (SLI)	17
3.1.2.5	Safely-limited position (SLP)	18
3.1.2.6	Safely-limited acceleration (SLA)	18
3.1.2.7	Safe direction (SDI)	18
3.1.2.8	Safe motor temperature (SMT)	19
3.1.2.9	Safe brake control (SBC)	19
3.1.2.10	Safe cam (SCA)	19
3.1.2.11	Safe speed monitor (SSM)	20
4	Safety functions in the application	21
4.1	Operating mode selection	21
4.1.1	Safety functions executed simultaneously	21
4.1.2	Operating mode selection safety function	22
4.1.3	Inching control safety function	22
4.1.4	Enabling control safety function (enabling device)	22
4.1.5	Lower risk conditions	22
4.1.6	Influence upon the sensors of the machine	23
4.1.7	Use of a portable control terminal	23
4.2	Stopping in an emergency	23
4.3	Failure of the power supply	23
4.3.1	Power supply to the control electronics from the intermediate DC circuit	24
4.3.2	Power supply to the control electronics from the supply system	24
4.3.3	Consideration of power failure in safety functions in accordance with EN ISO 13849-1	24
5	Frequency converters without integral safety functions (PDS)	27
6	Frequency converters with integral safety functions (PDS(SR))	29
6.1	Pulse blocking	29
6.1.1	Fault detection	30
6.1.1.1	Fault detection of pulse blocking	30
6.1.1.2	Fault detection of the servo enable	31
6.2	Safe movement control	32
6.3	PL, PFH and SIL	33
6.4	Stopping and holding in position	33
6.4.1	Stopping of loads	33
6.4.2	Holding up loads against gravity (vertical axes)	34
6.4.3	Mechanical brakes as components within safety functions	34
6.5	Limitations of safety functions	35
7	Safety functions on DC drives	37

8 Drive control: integrated or external safety? 39

9 Position encoders in safety functions 41

10 Acceptance test 43

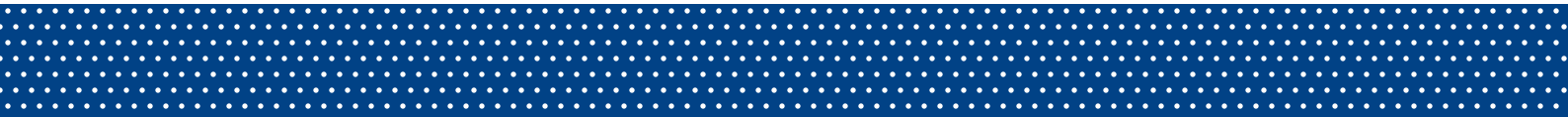
References 45

Annex A:
Acceptance test 49

Annex B:
Compendium of example circuits employing frequency converters 51

Annex C:
Expert committee information sheets 105

Annex D:
Index of abbreviations 117



1 Introduction

BIA Report 5/2003*) described the use of frequency converters in safety-related electrical circuits. Based upon safety functions and with reference to examples, the use of frequency converters was described both without and with integrated safety functions (power drive systems (PDS) and power drive systems safety related PDS(SR) respectively). The report was based upon the EN 954-1 [1] standard, listed under the Machinery Directive. Comprehensive revision of this standard, which is now available in the form of EN ISO 13849-1 [2] (Safety of machinery – Safety-related parts of control systems), and the publication of EN IEC 61800-5-2 [3] concerning the functional safety requirements of adjustable speed electrical power drive systems necessitated revision and adaptation of the report. The control of DC drives is also addressed.

Based upon the observations made in recent years during the testing and certification of products and consulting with manufacturers and with the Expert Committees of the German Social Accident Insurance Institutions, this report provides examples and explanations for support in the design of adjustable-speed power drive systems to EN ISO 13849-1 [2]. The report can thus be regarded as a supplement to BGIA Report 2/2008e concerning the functional safety of machine controls [4].

The examples described here presuppose, that the de-energized state of a drive control constitutes a safe state of the machine. Section 6.4, “Stopping and holding in position”, provides information for applications for which this is not necessarily the case.

The requirements concerning the functional safety of frequency converters are set out in the EN IEC 61800-5-2 product standard [3], which is based upon EN IEC 61508 [5]. Where necessary, the particular relationships to EN IEC 61508 [5] will therefore be addressed in this report. The safety functions are however always considered from the perspective of the machine manufacturer; reference is therefore always made to EN ISO 13849-1 [2].

The authors trust, that the present report will provide designers with substantial assistance in implementing safety functions with drive controls.

*) Sichere Antriebssteuerungen mit Frequenzumrichtern (BIA-Report 5/2003). Published by: Hauptverband der gewerblichen Berufsgenossenschaften (HVBG), Sankt Augustin 2003

2 Risk reduction

In accordance with EU Directive 2006/42/EC (Machinery Directive) [6], the manufacturer's obligations include performance of a risk assessment for the purpose of identifying all risks associated with his machine. The machine must be designed and constructed in consideration of the results of this analysis. Hazards should ideally be avoided at the design stage, or eliminated by design measures.

The machine must ensure by its design that when operated as intended and reasonably expected, it presents no hazards to persons. This applies to all operating modes; consequently, consideration must be given not only to automatic operation with safety guards closed, but also and in particular to all manual interventions that may be necessary.

The EN ISO 12100 standard [7] was developed in order to provide designers, manufacturers and other stakeholders with support in interpreting the essential safety requirements and in order to attain compliance with the European legislation governing the safety of machinery. This standard contains general design principles and provisions governing risk assessment and risk reduction. It serves as a general framework and guidance for the manufacturer of safe machines. EN ISO 12100 also provides useful guiding principles for cases where a relevant machine-specific type C standard does not exist.

For the purpose of risk reduction, the three-level hierarchy described in Section 6.1 of EN ISO 12100 applies:

- Level 1 – inherently safe design measures
- Level 2 – Safeguarding and/or complementary protective measures
- Level 3 – Information for use concerning the residual risk

The information for use must not be regarded as substitute for proper application of inherently safe design measures, safeguarding or complementary protective measures.

The second level of the hierarchy described above relates to safeguarding and complementary protective measures for the purpose of risk reduction. These include the safety functions addressed in this report. The requirements concerning the safety of the associated control systems are set out in EN ISO 13849. This standard comprises two parts [2; 8]:

Part 1 sets out safety requirements and provides a guide to the design and integration of safety-related parts of control systems (SRP/CS), including the development of software. Properties are specified for the SRP/CS that are required for implementation of the relevant safety functions. The standard is applicable to SRP/CS of all machine types, irrespective of the technology and form of energy employed (electrical, hydraulic, pneumatic, mechanical).

Part 2 sets out the validation procedure for the safety functions of control systems, including the procedures of analysis and testing. The validation procedure includes analysis of the behaviour of safety-related parts of the control system in case of a fault. For this purpose part 2 also provides lists of possible faults and – where applicable – design requirements for their exclusion for many components. The essential and well-tried safety principles are also listed.

The required Performance Levels (PL) for different safety functions may differ for one and the same hazardous zone of a machine. Accordingly, there is generally no uniform required PL_r for all safety functions at a hazardous zone.

The following two sections address two special cases relating to the use of safety functions for risk reduction.

2.1 Actors in safety functions

Safety functions have the purpose of reducing the risk presented by machinery. For evaluation of the safety functions, EN ISO 13849-1 [2] is applied. The scope of this standard begins at the sensor, i.e. the interface to the technical process, encompasses the logic, and ends with the power control element, such as the motor contactor or valve. The actual actor, such as the motor or hydraulic cylinder, lies outside the scope of the standard. This differentiation is logical, provided failure of an actor cannot give rise to a hazardous state. Should external forces upon take effect a machine however, as for example in the case of vertical axes, failure of an actor (such as a brake or motor) may cause the load to drop. This begs the question whether it is logical to place requirements in the form of a PL_r upon the control system for an actor without considering the actor itself. The method of EN ISO 13849-1 can also be applied here, though certain additional safety-related properties (such as mechanical strength) may however have to be considered. This situation has not yet been conclusively clarified. Together with the Expert Committee Woodworking and Metalworking of the German Social Accident Insurance (DGUV), the Institute for Occupational Safety and Health of the DGUV (IFA) has decided to consider the actor as a part of the safety function in such cases as well. This procedure has been published and thus presented for discussion in Expert Committee Information Sheet 050 (see Annex C, p. 105).

2.2 Overlapping hazards

Owing to the additional probabilistic analysis, the replacement of EN 954-1 [1] by EN ISO 13849-1 [2] also requires consideration of overlapping hazards. Overlapping hazards arise when a person operating at one location could be injured by multiple hazardous movements. Calculation of the probability of injury must consider not only one, but up to 20 hazardous movements, depending upon the machine. Since each of these movements

2 Risk reduction

is associated with a probability of failure, the probabilities of failure of a large number of components are summated, and the required Performance Level may no longer be reached. Together with the DGUVs Expert Committee Woodworking and Metal-

working, the IFA has described a strategy for a solution that is based upon analysis of discrete hazards presented by machine components. A paper [9] contains further information.

3 Drive control devices employed as safety-related parts of control systems

Drive control devices, such as frequency converters or DC-DC converters, have been used for many years to control the speed of electrical drives in machinery. These drives are generally associated with hazardous movements on the machines. Guards or electro-sensitive protective equipment prevent hazardous zones being accessed when the machine is in automatic mode. For setup and changeover tasks in the hazardous zone, measures are required in the first instance to prevent unexpected start-up. This can be achieved with relatively little effort by means of a mains contactor in the drive's mains circuit or a motor contactor between the drive control device and the motor. An alternative are drive control devices with integral safety functions featuring pulse blocking.

In some circumstances however, work must also be performed on an operating machine, without the protective effect of safeguards. This necessitates substitute safety measures which provide the operator with adequate protection even in such situations. An example is setup mode on a machine tool in which positions must be measured manually. The drive cannot be de-energized for this purpose, since this would result in a loss of the accurate position, which would not be acceptable owing to the required accuracy of the process. The closed-loop position

control must therefore remain active during the manual intervention. The Machinery Directive [6] permits this in principle (Annex I, Section 1.2.5), however additional requirements have to be placed upon the control system in this operating mode (see Section 4.1 of this report). In addition, the safety functions must be implemented in a Performance Level (PL) to EN ISO 13849-1 [2] that is commensurate with the risk.

Therefore other measures but guards and a disconnected motor are required in this case to assure a comparable level of safety for the machine operator. This is attained for example by application of the safety functions defined in EN 61800-5-2 [3] (Table 1).

These safety functions defined in the standard constitute a basis. The manufacturers of PDS(SR) offer a range of further safety functions beyond those listed. Selected basic functions are described in Section 3.1.

The safety functions described above are not a substitute for devices for disconnecting the electrical equipment from the mains system. Such devices are required in addition to enable working without the risk of electric shock or burns.

Table 1:
Safety functions described in EN 61800-5-2

Abbreviation	See Section	Designation	Function
STO	3.1.1.1	Safe torque off	No power capable of generating a rotary movement is applied to the motor; Stop Category 0 to EN 60204-1
SS1	3.1.1.2	Safe stop 1	Motor decelerates; monitoring of the braking ramp and STO once stationary, or STO after expiration of a delay time; Stop Category 1 to EN 60204-1
SS2	3.1.1.3	Safe stop 2	Motor decelerates; monitoring of the braking ramp and SOS once stationary, or SOS after expiration of a delay time; Stop Category 2 to EN 60204-1
SOS	3.1.2.1	Safe operating stop	Motor is stationary and withstands external forces.
SLA	3.1.2.6	Safely-limited acceleration	Exceeding of an acceleration limit value is prevented.
SAR	---	Safe acceleration range	The acceleration of the motor is maintained within specified limits.
SLS	3.1.2.2	Safely-limited speed	Exceeding of the speed limit value is prevented.
SSR	---	Safe speed range	The speed of the motor is maintained within specified limits.
SLT	3.1.2.3	Safely-limited torque	Exceeding of a torque/force limit value is prevented.
STR	---	Safe torque range	The torque of the motor is maintained within specified limits.
SLP	3.1.2.5	Safely-limited position	Exceeding of a position limit value is prevented.
SLI	3.1.2.4	Safely-limited increment	The motor is moved by a specified incremental movement and stops thereafter.
SDI	3.1.2.7	Safe direction	An unintended direction of motor movement is prevented.
SMT	3.1.2.8	Safe motor temperature	Exceeding of a motor temperature limit value is prevented.
SBC	3.1.2.9	Safe brake control	Safe actuation of an external brake
SCA	3.1.2.10	Safe cam	Whilst the motor is within specified position limits, a safe output signal is generated.
SSM	3.1.2.11	Safe speed monitor	Whilst the motor speed is below a specified value, a safe output signal is generated.

3.1 Description of the safety functions

In accordance with EN ISO 12100-1 [7], a safety function is any function of a machine the failure of which can result in an immediate increase of the risk. A safety function in this context is usually performed by the components of sensor, logic and output¹. The drive control devices addressed in this report cover the output aspect, which depending upon the implementation may also include the logic. Therefore they could be labelled as safety sub-functions. However, in safety technology, the usage of this term is not common.

The detection of faults is of major importance within safety technology. Regarding the use of PDS(SR) in particular, consideration must be given to the different kinds of responses in fault detection:

- Response to the exceedance of limit values

This is the response function that is triggered by the exceedance of limit values during intended use of the safety functions.

- Fault response function

This is the response function that is triggered by detection of a fault within the safety function.

The information for use of a PDS(SR) should contain this information.

It is expedient to divide the safety functions into stop functions and “other safety functions”.

The following descriptions of the safety functions contain example diagrams of time characteristics illustrating their behaviour. This behaviour may differ from one PDS(SR) to the next; differences may arise even where terms and abbreviations are identical. The operating manuals must therefore always be consulted for use of the devices.

3.1.1 Stop functions

The EN 60204-1 [10] standard on electrical equipment, which is also important for machinery, distinguishes between the following three categories of stop functions:

- Stop Category 0: stopping by immediate removal of power to the machine actuators (uncontrolled stop)

- Stop Category 1: a controlled stop with power available to the machine actuators to achieve the stop. Power is then removed from the actuators when the stop is achieved.
- Stop Category 2: a controlled stop with power left available to the machine actuators

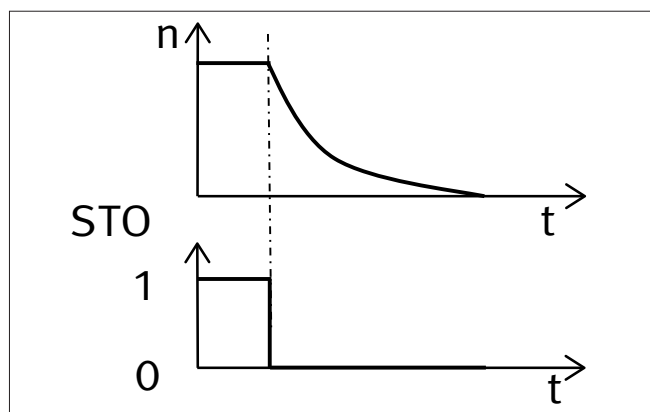
The stop functions defined in EN 61800-5-2 [3] give consideration to these stop categories, and are described in the sections below.

3.1.1.1 Safe torque off (STO)

“Power, that can cause rotation (or motion in the case of a linear motor), is not applied to the motor. The PDS(SR) will not provide energy to the motor which can generate torque (or force in the case of a linear motor).”[3].

Figure 1 shows the time characteristic of the input signal for activation of STO and the motor speed. The STO safety function corresponds to an uncontrolled stop to EN 60204-1, Stop Category 0. It may be employed when disconnection of the power is required in order to prevent unexpected start-up. The stop position is not monitored. Should the STO safety function be activated during operation, the motor coasts down unbraked.

Figure 1:
Example of the time characteristic of the STO (safe torque off) safety function



Where external forces are present (such as gravity on vertical axes), additional measures may be necessary for risk reduction, such as mechanical brakes (see also Section 6.4).

Electronic devices and contactors (insufficiently large contact gap) used for the implementation of safety functions do not provide adequate protection against electric shock; additional measures for galvanic isolation may be necessary.

Suitable measures for a safe torque off include (see Figure 2):

- contactor between electrical system and drive system (mains contactor)

¹ Section 5.5.2 of EN 61508-4:2011-02, Function safety of electrical/electronic/programmable electronic safety-related systems – Part 4: Definitions and abbreviations, defines in this context the “overall safety function”

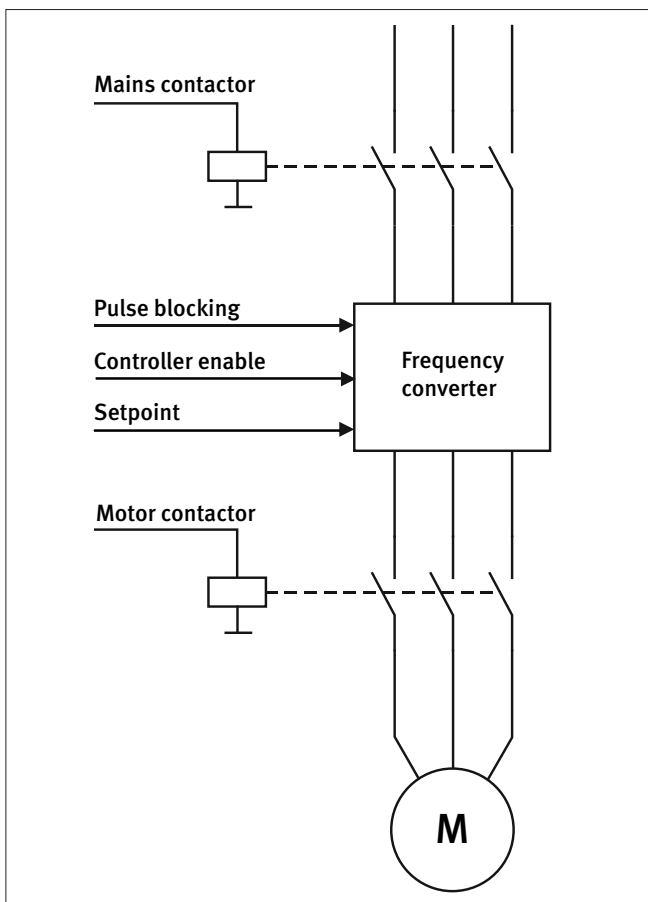
- contactor between power unit and drive motor (motor contactor)
- pulse blocking (blocking of the pulse triggering the power semiconductors within the frequency converter)
- servo enable
- reference value

Different PLs can be achieved, depending upon the combination of the above measures.

Application examples:

- Prevention of unexpected start-up of hazardous movements during setup, changeover and clearing of faults.
- When a safety guard is opened, STO is activated and the motor coasts to a halt.

Figure 2:
Alternative principles for achieving STO



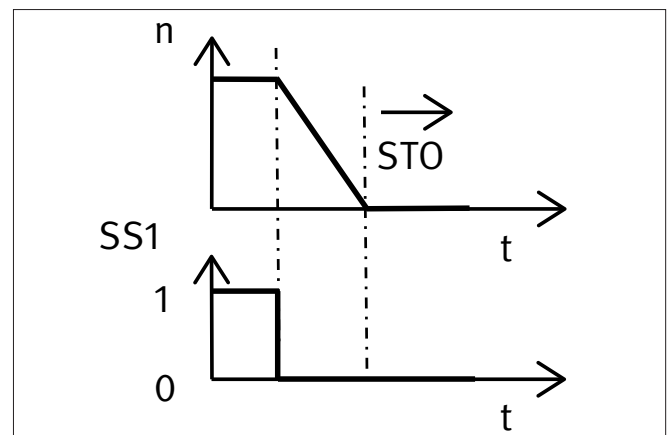
3.1.1.2 Safe stop 1 (SS1)

“The PDS(SR) either

- initiates and controls the motor deceleration rate within set limits to stop the motor and initiates the STO function, when the motor speed is below a specified limit²; or*
- initiates and monitors the motor deceleration rate within set limits to stop the motor and initiates the STO function when the motor speed is below a specified limit; or*
- initiates the motor deceleration and initiates the STO function after an application specific time delay.” [3].*

Figure 3 shows the time characteristic of the input signal for activation of SS1 and the motor speed. The SS1 safety function corresponds to a controlled stop in accordance with EN 60204-1, Stop Category 1. The “motor deceleration value” describes the degree to which the motor is braked.

Figure 3:
Example of the time characteristic of the SS1 safety function (Safe stop 1)



Should the safety function SS1 be implemented according to c), where the STO function is triggered following a time delay, attention must be paid to the following: the stop function of the drive control is not monitored during the delay. It may therefore fail unnoticed, and the motor could continue to run unbraked until the STO function is triggered; in a worst case scenario, the motor could even accelerate. The risk assessment for the machine must take this behaviour into account. If such behaviour is not acceptable owing to the anticipated hazard, an implementation of the SS1 function in this form is not suitable.

Conversely, if the SS1 safety function is implemented with monitoring of the braking ramp (motor deceleration variable) (b), a defective stop function can be detected very quickly.

Application examples:

- When a safety guard is opened, SS1 is triggered and the motor is stopped as quickly as possible. Unexpected start-up is then prevented, since STO is active.

² The authors are not currently aware of any product employing solution a).

- Should imbalances occur in a sugar centrifuge, the drive must be stopped as quickly as possible, since the drum, weighing in the order of tons, could otherwise uncontrollably break loose. Solution b) is therefore absolutely essential, since acceleration instead of braking owing to a defective drive control cannot be excluded. This situation is detected swiftly by monitoring of the braking ramp, and STO is triggered in response to the fault.

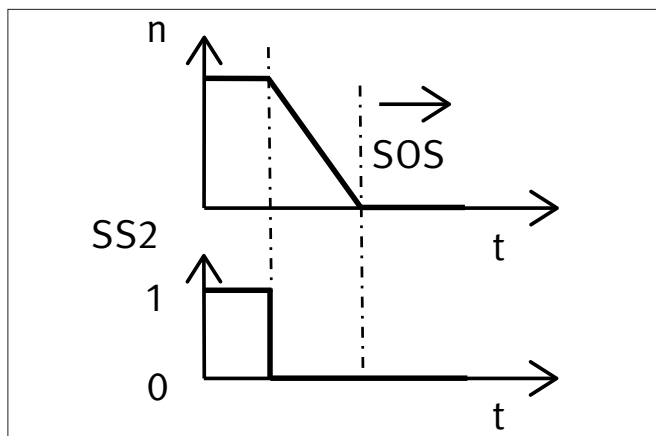
3.1.1.3 Safe stop 2 (SS2)

“The PDS(SR) either

- a) initiates and controls the motor deceleration rate within set limits to stop the motor and initiates the safe operating stop function when the motor speed is below a specified limit³; or
- b) initiates and monitors the motor deceleration rate within set limits to stop the motor and initiates the safe operating stop function when the motor speed is below a specified limit; or
- c) initiates the motor deceleration and initiates the safe operating stop function after an application specific time delay.”

Figure 4 shows the time characteristic of the input signal for activation of SS2 and the motor speed. The SS2 safety function corresponds to a controlled stop in accordance with EN 60204-1 [10], Stop Category 2.

Figure 4:
Example of the time characteristic of the SS2 safety function (Safe stop 2)



Should the SS2 safety function be implemented as described in c), where the SOS function is triggered following a delay, attention must be paid to the following: the stop function of the drive control is not monitored during the delay. It can therefore fail unnoticed, and the motor could continue to run unbraked until the SOS function is triggered; in a worst case scenario, it could even accelerate. The risk assessment for the machine must take this behaviour into account. If such behaviour is not acceptable owing to the anticipated hazard, an implementation of the SS2 function in this form is not suitable.

If the SS2 safety function is however implemented with monitoring of the braking ramp (motor deceleration value), a defective stop function can be detected very quickly.

Application examples:

- On a machine tool, a measurement on the workpiece must be performed during the working process without a position change occurring as a result of the motor control being de-energized. Opening of the safety guard causes triggering of SS2. The hazardous movement is stopped, and unexpected start-up is prevented by SOS.
- The load on a vertical axis is halted when a safety guard is opened, and held in position by the subsequent SOS. Depending upon the potential of operators being present within the hazardous zone, further measures may be required (see Information Sheet 005 of the Expert Committee Woodworking and Metalworking, Annex C, page 105).

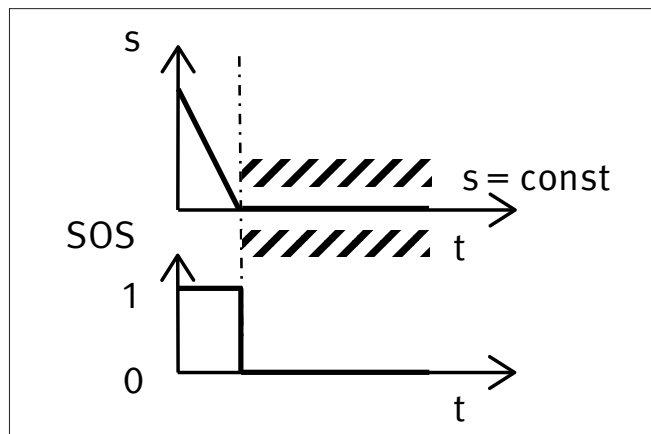
3.1.2 Other safety functions

3.1.2.1 Safe operating stop (SOS)

“The SOS function prevents the motor from deviating more than a defined amount from the stopped position. The PDS(SR) provides energy to the motor to enable it to resist external forces.”

Figure 5 shows the time characteristic of the input signal for activation of SOS and the motor position.

Figure 5:
Example of the time characteristic of the SOS safety function (Safe operating stop)



If the drive system must be stopped at a particular point in the manufacturing process without loss of position (for example the feed on a machine tool), all control functions must be retained when the machine is stationary. At the same time, unexpected start-up must be prevented. This is attained by safe monitoring of the stop whilst the motor remains under position control. Unexpected start-up is detected quickly. STO is activated to prevent a hazard to persons. Once SOS has been cleared, the drive movement can be resumed directly from the stop position.

³ The authors are not currently aware of any product employing solution a).

Application examples:

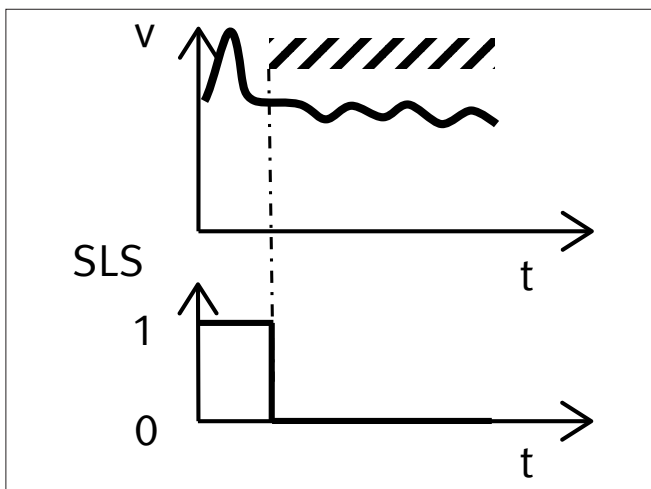
- setup mode on automatic lathes/machining centres,
- manual measurement during machining.

3.1.2.2 Safely-limited speed (SLS)

“The SLS function prevents the motor from exceeding the specified speed limit.”

Figure 6 shows the time characteristic of the input signal for activation of SLS and an axial speed.

Figure 6:
Example of the time characteristic of the SLS safety function (Safely-limited speed)



With this safety function, safe monitoring prevents the drive from exceeding a specified speed limit. Exceeding of the limit value is detected and the drive is stopped safely.

Application examples:

- setup mode on automatic lathes/machining centres,
- insertion of material on calender rollers.

Note:

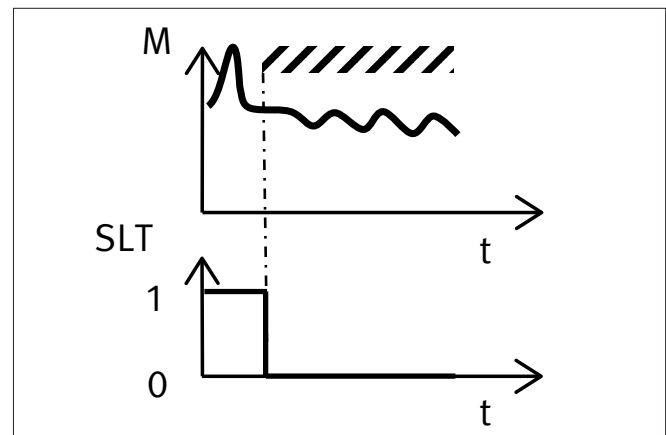
No generic speed limits are specified that can be regarded as being so safe that they do not present a hazard to operators. The speeds regarded as safe differ from one machine to the next. The IFA Manual on governing safety and health at the workplace, code 330216 [11], contains an overview of relevant stipulations in machine-specific standards (type C standards).

3.1.2.3 Safely-limited torque (SLT)

“The SLT function prevents the motor from exceeding the specified torque (or force, when a linear motor is used) limit.”

Figure 7 shows the time characteristic of the input signal for activation of SLT and the motor torque.

Figure 7:
Example of the time characteristic of the SLT safety function (Safely-limited torque)



SLT reduces the scale of harm caused by a hazardous movement. Guideline values for the effects of forces can be found in Chapter 6 of the 2013 list of limit values [12].

Application examples:

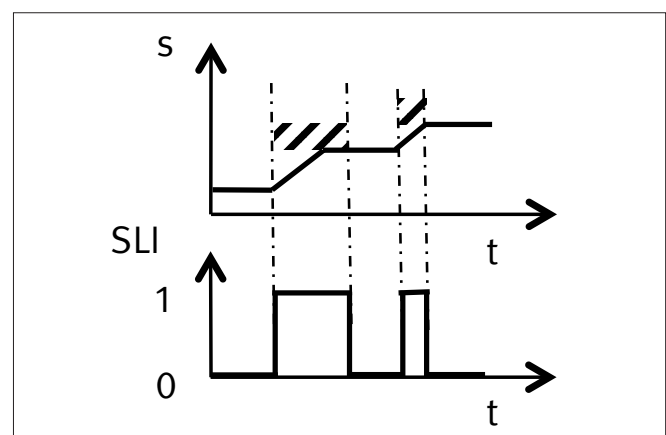
- limiting of forces at the closing edges of power operated doors,
- prevention of entrapment of operating personnel on coiling machines.

3.1.2.4 Safely-limited increment (SLI)

“The SLI function prevents the motor shaft from exceeding the specified limit of position increment.”

Figure 8 shows the time characteristic of the input signal for activation of SLI, and a shaft position.

Figure 8:
Example of the time characteristic of the SLI safety function (Safely-limited increment)



With this safety function, the drive may move by no more than a defined distance (increment) following a start command. Once the limit value has been reached, an STO or a safe operating

stop (SOS) must take effect. Exceeding of the limit values is detected, and the drive is stopped safely.

Application examples:

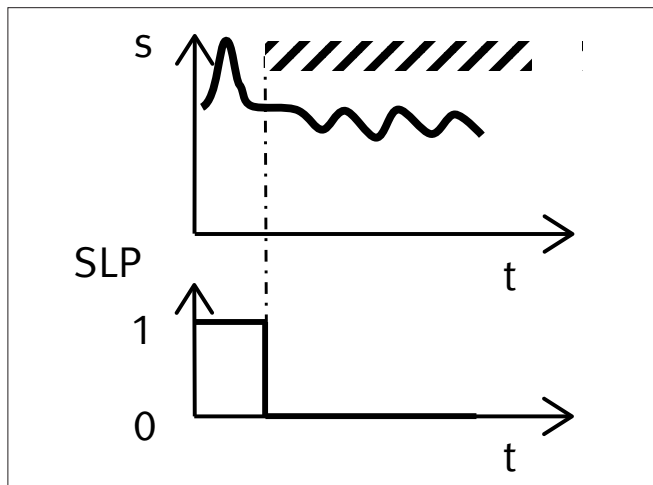
- setup mode on automatic lathes/machining centres,
- inching with limited travel on printing machines.

3.1.2.5 Safely-limited position (SLP)

“The SLP function prevents the motor shaft from exceeding the specified position limit(s).”

Figure 9 shows the time characteristic of the input signal for activation of SLP and the motor shaft position.

Figure 9:
Example of the time characteristic of the SLP safety function (Safely-limited position)



Safe limiting of the position ensures that the drive system enters an STO or SOS, when a specified absolute position limit value is reached. Regarding the limit value the overrun, arising for technical reasons, has to be taken into account. Below the limit value, unexpected movements of the drive must be anticipated. Exceeding of the limit value is detected, and the drive system is stopped safely.

Application examples:

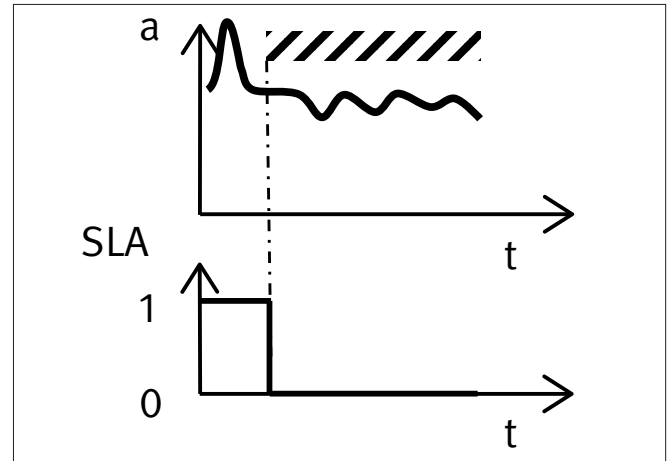
- area partitioning on a machine into manufacturing and feeding areas,
- limitation of a travel range (substitution for electromechanical limit switches),
- limitation of the range of robot arms.

3.1.2.6 Safely-limited acceleration (SLA)

“The SLA function prevents the motor from exceeding the specified acceleration limit.”

Figure 10 shows the time characteristic of the input signal for activation of SLA and the motor acceleration.

Figure 10:
Example of the time characteristic of the SLA safety function (Safely-limited acceleration)



Exceeding of the acceleration limit value is detected, and the drive is stopped safely. The acceleration limit value may be positive or negative; the same function can therefore also be used to limit the scale of braking.

The safety function keeps the motor acceleration or deceleration within defined limit values. Exceeding of the limit values is detected, and the drive system is stopped safely.

Application examples:

- During the transport of open vessels containing liquids, excessive acceleration or braking that would cause spillage is prevented.
- The acceleration of certain grinding wheels must be limited, since the inertia could otherwise cause the grinding wheels to burst.

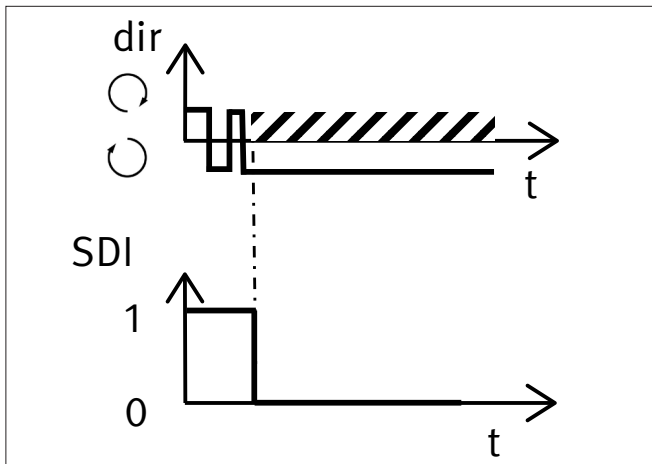
3.1.2.7 Safe direction (SDI)

“The SDI function prevents the motor shaft from moving in the unintended direction.”

Figure 11 shows the time characteristic of the input signal for activation of SDI and the direction of motor rotation.

Movement in the impermissible direction is detected and the drive is stopped safely.

Figure 11:
Example of the time characteristics of the SDI safety function
(Safe direction)



Application examples:

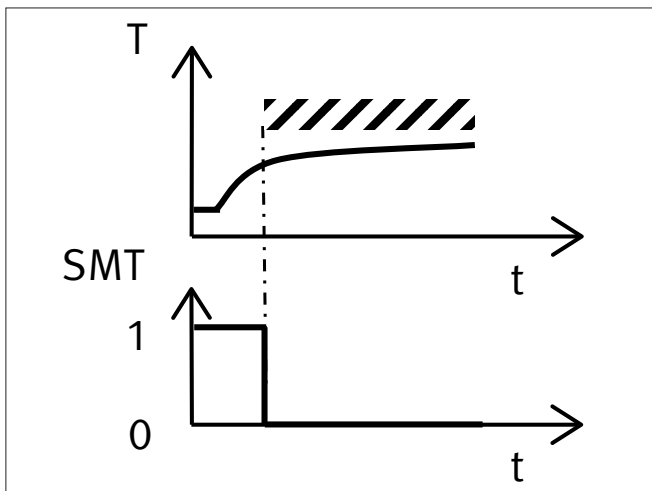
- Machine parts are prevented from moving towards the operator.
- A reversal in the direction of rotation of rollers is prevented, as this could otherwise give rise to entrapment points.

3.1.2.8 Safe motor temperature (SMT)

“The SMT function prevents the motor temperature(s) from exceeding a specified upper limit.”

Figure 12 shows the time characteristic of the input signal for activation of SMT and the motor temperature.

Figure 12:
Example of the time characteristic of the SMT safety function
(Safe motor temperature)



A temperature above the limit value is detected, and the drive is stopped safely.

Application examples:

- Impermissibly high motor temperatures are prevented for use in areas with potentially explosive atmosphere.
- Fire protection.

3.1.2.9 Safe brake control (SBC)

“The SBC function provides (a) safe output signal(s) to control (an) external brake(s).”

Additional mechanical brakes may also be required on motors that are driven by frequency converters. This is particularly the case when external forces act upon a motor, such as gravity, or tensile forces during the processing of material webs. The brakes can be actuated by the PDS(SR) by means of the SBC safety function. The moment of actuation is specific to the application, for example immediately after stopping of the motor, in response to a fault detection in the drive control, in the event of an emergency stop, etc.

Application examples:

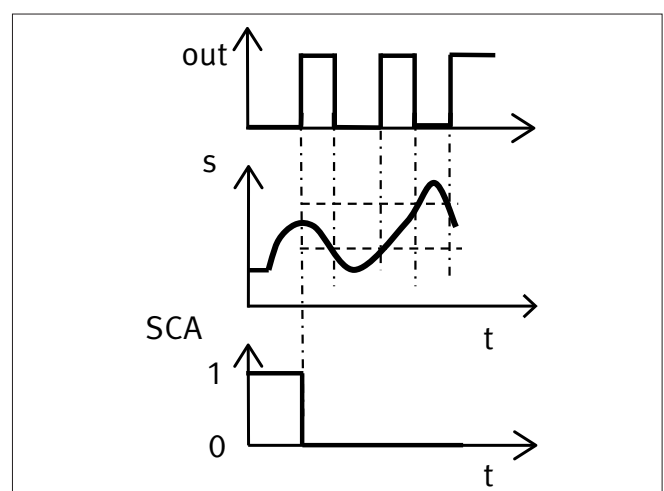
- actuation of an external brake on a vertical axis, simultaneous to activation of STO,
- actuation of an external brake on a vertical axis in the event of power failure.

3.1.2.10 Safe cam (SCA)

“The SCA function provides a safe output signal to indicate whether the motor shaft position is within a specified range.”

Figure 13 shows the time characteristic of the input signal for activation of SCA, the motor position, and the output signal.

Figure 13:
Example of the time characteristic of the SCA safety function
(Safe cam)



3 Drive control devices employed as safety-related parts of control systems

Parameters are used to specify a travel range of an axis. A safe output signal is generated whenever the axis is within this range. Departure from the range has no effects within the PDS(SR); only the output signal is set accordingly.

Application examples:

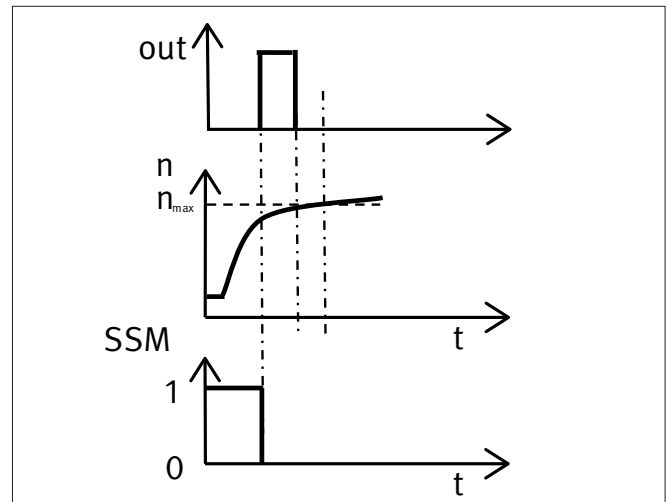
- disabling of guard locking on a safety guard is permitted only when the machine component is within a safe range. Unexpected start-up may also have to be prevented (STO),
- substitution of position sensors,
- position limitation of robot axes.

3.1.2.11 Safe speed monitor (SSM)

“The SSM function provides a safe output signal to indicate whether the motor speed is below a specified limit.”

Figure 14 shows the time characteristic of the input signal for activation of SSM, the motor speed, and the output signal.

Figure 14:
Example of the time characteristic of the SSM safety function (Safe speed monitor)



When the SSM function is activated, a safe output signal is generated as long as the current motor speed lies below the limit value n_{max} . Should the limit value be exceeded, only the output signal is reset; no further reactions occur within the PDS(SR).

Application example:

- Disabling of guard locking on a safety guard is permitted only when the drive speed is below a hazardous value.

4 Safety functions in the application

4.1 Operating mode selection

Operating mode selector switches are employed on machinery for changes to control or working processes. Where different protective measures are used, an operating mode selector switch, lockable in any position, is required. Each position of the selector switch must be clearly recognizable, and it must correspond only to a single control or operating mode (refer to the Machinery Directive [6] Annex I, Section 1.2.5). The control or operating mode selected must be prior to all other control or operating functions, with the exception of emergency stop.

The selector switch may be replaced by another selection device, for example an input unit with access code, that restricts the use of certain machine functions to certain categories of operators. It must be ensured however that the requirements of the electrical circuits employed for this purpose satisfy an equivalent safety level.

Where certain work requires the machine to be operated with the protective effects of the safeguards being suspended, for example in setup mode or during fault clearance, the following control specifications must be assigned to the relevant position of the selector switch:

- No other control or operating modes are possible. This means that all other operating/control modes must be disabled and prevented.
- Movements are possible only when control devices are activated (control devices with automatic reset, such as inching control, enabling control).
- The operation of hazardous functions is possible only under reduced risk conditions (such as limited speed, reduced power, step mode, limitation of the range of movement), while preventing hazards from linked sequences.
- Voluntary or involuntary action on the machine's sensors cannot give rise to any operation of hazardous functions.

These control provisions are supplemented by those of Section 9.2.4 of EN IEC 60204-1 [10]. Of note is the

- use of a portable control terminal with emergency-stop control device.

Selection of the operating mode or switching between operating modes must not result in machine movements starting automatically. Separate actuation of the start control must be required for this purpose. The start of movements must always require deliberate action.

If the control requirements mentioned above cannot be fulfilled simultaneously, the control or operating mode selector switch must activate other protective measures. These must be designed to ensure a safe working area.

A clear display of the selected operating mode must be provided, for example by marking of the positions of an operating mode selector switch, the use of signalling lamps, or an on-screen visualisation. If electrical signals are used, they must feature a test function.

The above control requirements concern safety functions, design requirements, and possibly further organizational measures. The operating mode selector switch therefore activates or deactivates the relevant safety functions according to the operating mode. Component faults in the operating mode selection device could therefore lead to required safety functions not being effective. Such faults increase the risk on a machine and must therefore be considered.

This raises the question whether the control aspect of operating mode selection is part of each safety function implemented on the machine, or whether operating mode selection can be regarded as a safety function in its own right. As with the procedure for overlapping hazards, in which discrete machine components are considered, operating mode selection is regarded as a safety function in its own right. This prevents that operating mode selection additionally raises the average probability of a dangerous failure per hour (PFH) in each individual safety function

4.1.1 Safety functions executed simultaneously

In some operating modes on machinery, the required risk reduction is attained by interaction between multiple measures, including by the simultaneous execution of multiple safety functions. This is particularly the case for operating modes in which a machine must be operated with an open safeguard, for example for the purposes of setup or fault clearance. In these cases, safety functions for limiting the speed (SLS) and for inching/enabling mode are frequently active simultaneously. In each case the PLs required for these safety functions are determined by a risk analysis. Here the risk presented by a hazardous movement of the same machine component might already be reduced by another safety function executed simultaneously. In this case a new risk analysis of the residual hazard leads to an additional safety function with a lower PL_r (see Annex A, Example 4 in BGIA Report 2/2008e [4]). The PL_r must not be reduced mutually by safety functions, since the overall risk reduction would turn out to be insufficient. This can be prevented by iterative application of the risk graph. In the above example, the PL_r for SF 2 (limited speed) was determined first. For inching mode in SF 3, it can then be assumed that the speed limitation of SF 2 makes the machine movements predictable for the machine operators and that he is able to avoid hazardous movements (risk parameter P1

instead of P2). Simultaneous execution of SF 2 therefore yields $PL_r = c$ rather than $PL_r = d$ for SF 3⁴.

4.1.2 Operating mode selection safety function

The provisions of the Machinery Directive governing operating mode selection require that working in an operating mode that has not been selected is prevented. This is generally achieved by means of safety technology by activating the safeguards required for the respective operating mode, and – if possible – prevention of unintended movements of individual machine parts. At the same time, other operating modes are blocked functionally via the machine control system (e.g. a standard PLC).

Common operating elements for the selection of operating modes are described below.

a) Cam-operated selector switches

Switches with positive actuation (direct opening action) are considered well-tries components when they satisfy EN 60947-5-1:2005 [13] (IEC 60947-5-1:1997), Annex K. They can therefore be classified in Category 1 to EN ISO 13849.

b) Cam-operated switches with further fault exclusions

If the following fault exclusions are possible – in accordance with Table D.8 of EN ISO 13849-2 [8] – on switches with positive actuation, the corresponding component faults need not be assumed

- short-circuit of adjacent contacts that are mutually isolated, and
- simultaneous short-circuit between the three terminals of changeover contacts

This may be demonstrated for example by a failure mode and effects analysis (FMEA). Categories higher than Category 1 are therefore possible (refer also in this context to Example 8 in Annex B, pages 70 ff).

c) Other electromechanical switches

For fault analysis an FMEA and possibly other measures must be taken.

d) Selection of the operating mode by means of electronic equipment (such as a keyboard or transponder)

For fault analysis an FMEA and possibly other measures must be taken.

4.1.3 Inching control safety function

Standard inching buttons with spring return are usually used as inching control devices. Observance of the closed-circuit current principle results in the movement being halted when the actuator of the control device is released. The design of the inching switch is not subject to any particular requirements, even though in the event of a fault (such as spring breakage) the contacts may fail to open when the inching button is released. Knowledge of the B_{10d} value of the pushbutton is necessary for quantification of the inching control safety function. The component manufacturer usually states this value. Alternatively, the data can be found in EN 13849-1. This enables the safety function for inching mode to be quantified.

Where machine-specific provisions have not been set out in type C standards, a risk analysis must be used to determine whether additional measures are necessary, such as enabling switches or emergency-stop by means of an emergency-stop control device.

4.1.4 Enabling control safety function (enabling device)

Enabling controls must be designed such that they permit hazardous machine functions only when their control devices (the enabling switches) are actuated in a particular stage (the “enabling function”). It must not be possible for hazardous movements to be initiated by the enabling control alone. The devices must be selected and located such that the possibility of being bypassed is reduced to a minimum.

Two-stage and three-stage enabling switches are available. Pressing a three-stage enabling switch through to the third stage (the “off” function) triggers a signal equivalent to that of an emergency stop. This enables the operator to bring the movement safely to a halt in a hazardous situation either by releasing the actuator or by pressing it fully down, for example by a convulsed movement.

The enabling control is a safety function, and the data required for calculation of the PFH are provided by the component manufacturer. It is recommended to use enabling equipment/enabling switches that satisfy the provisions of the test principles GS-ET-22 [14] of DGUV Test. Fault exclusions are permissible for these products up to an actuation number of 100,000 switching operations (see also BGIA Report 2/2008e [4], Table D.2).

Should two-stage control devices be used, an emergency-stop device must be fitted in addition in the proximity of the enabling switch.

4.1.5 Lower risks conditions

Should it be necessary for example that persons perform adjustment work (setup mode) in the hazardous zone, the risk of injury must be reduced to a minimum. For example, unexpected movements must be prevented (STO, SOS), or reduced (SLS, SLA) such that the operator is able to predict the current motion behaviour of machine components. This also means limiting the movement range of axes (SLP, SDI) and where possible, moving only one axis. Limitation of power (SLT) and step mode (SLI) may

⁴ Where a safety function is used in multiple operating modes, different risks may also give rise to different PL_r s. The safety function must be implemented in the highest PL_r .

also be necessary. In addition, hazards resulting from linked sequences must be excluded, so that no automatic (sub-)processes are performed on the machine.

If these requirements are satisfied by means of control technology, they are safety functions that must be designed in accordance with EN 13849-1 [2].

4.1.6 Influence upon the sensors of the machine

For automatic processes on machines, sensors are generally used, for example to detect the position of workpieces. Based upon these sensor signals, a PLC may then start the next production step. In other words, a movement is initiated. Work performed on the machine with opened safeguards may cause sensor signals to be triggered. In this situation, initiation of movement of a machine component could potentially endanger the machine operator. This must be prevented. For this reason, the Machinery Directive specifies for controls, that “any operation of hazardous functions by voluntary or involuntary action on the machine’s sensors” must be prevented. This is demonstrated effectively by analysis of the circuit diagram, or by tests on the machine by purposefully influencing of the sensors (for example by actuation or switching of position switches). Consideration must be given here where applicable in Categories 3 and 4 to the necessary single-fault tolerance and accumulations of undetected faults. The result of the analysis/test must be documented.

4.1.7 Use of a portable control terminal

“Use of a portable control terminal” as a specification for controls constitutes a requirement concerning the equipment of the machine. The information for use must make reference to the intended use.

The portable control terminal is usually equipped with an emergency-stop control device, inching switch and/or enabling switch.

4.2 Stopping in an emergency

In accordance with the provisions of the Machinery Directive 2006/42/EC, Annex I, all machinery (with certain exceptions) must be fitted with one or more emergency-stop devices to prevent an actual or impending hazard.

The emergency-stop function is triggered by a single human action by actuation of the emergency-stop control device. This must cause the hazardous process to be stopped as quickly as possible, without creating additional hazards.

The emergency-stop function must be available and operational at all times, regardless of the operating mode, in order to enable a machine or installation to be stopped as quickly as possible in an emergency. This also means that the emergency-stop equipment must not be disabled in any operating mode. It therefore overrides all other operating modes, operating states and safety functions. Note that the emergency-stop function constitutes a complementary protective measure that is employed in addition

to the best possible inherently safe design and other technical protective measures and safety functions. It must not be a substitute for these measures.

The control command that is triggered by actuation of the emergency-stop control device remains active until the control device has been reset. A corresponding control command can be activation of the STO safety function in the drives.

Manual resetting of the emergency-stop control device however must not trigger a re-start, and must only be possible at the location at which the emergency-stop command was issued. This ensures that it is possible to check from the location at which the device is reset whether the associated hazardous zone is “clear” again

Depending upon the result of the risk assessment, the emergency-stop function must be executed either in Stop Category 0 or in Stop Category 1 in accordance with EN 60204-1 [10]. Whether the appropriate measure is immediately interrupting the energy supply of the machine drives (STO) and allowing the motors to coast to a halt, or whether the hazardous process must be stopped as quickly as possible (SS1) must be assessed independently for each machine.

The decisive aspect in this assessment is the time between triggering the emergency-stop command – as with tripping of a protective device – and the drive coming to a halt. This time is termed overrun time. On a number of machines, such as presses or calender rollers, a limit value for the overrun time must be observed. For this reason, some type C standards place requirements upon the braking process.

Bringing a machine to a halt as quickly as possible in an emergency can be achieved by controlled stopping by the drive control system. The SS1 safety function is used for this purpose. This function can be implemented in a number of different forms (see Section 3.1.1.2). However, compared to the form involving activation of the STO function following a predefined delay, the SS1 function comprising a monitored braking ramp and subsequent activation of the STO function has the advantage that the response to faults during the stopping process is faster.

Machines on which the emergency stop is implemented must have suitable measures for electrical shock-hazard protection, such that an emergency off is not required. Consideration must also be given to the fact that the final de-energization following stopping does not simultaneously mean isolation from the energy supply. Pulse blocking in the frequency converter for example prevents rotary movement of the motor; high voltages may nevertheless still be present at the motor terminals. Even if mains or motor contactors are used, adequate isolation from the power supply is assured only when the contact gap of the contactors is sufficiently large. The emergency stop function is therefore completely unsuitable for isolation while working on the electrical equipment. The terminological distinction between emergency off and emergency stop was introduced in 2005 in EN 60204-1, but has yet to become universally adopted

4.3 Failure of the power supply

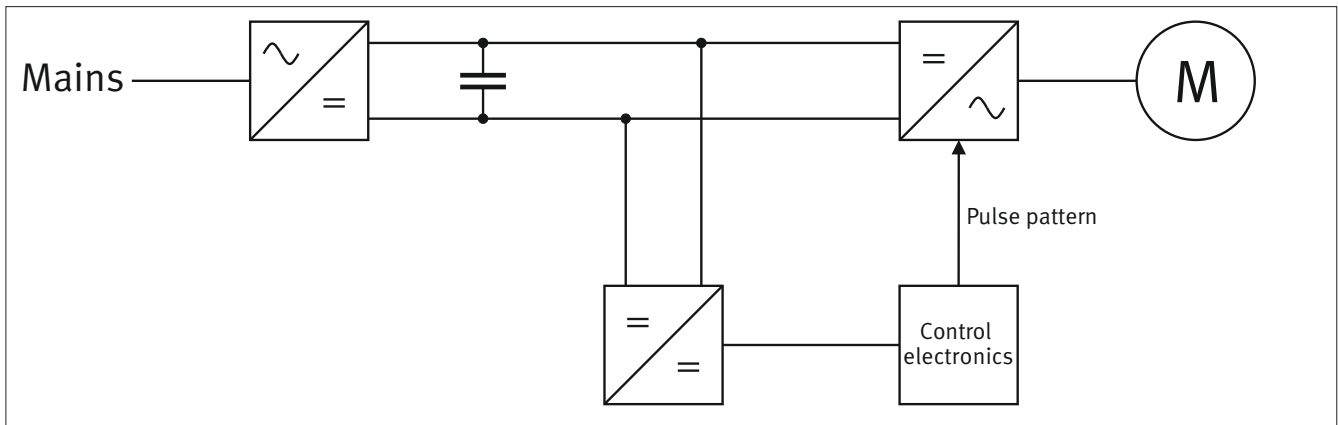
A failure of the power supply can occur at any time. This situation must be considered during engineering of a frequency converter for a machine control system, and does not constitute a fault condition (EN ISO 12100 Section 5.4b “Possible states of the machine: disturbance of its power supply”; EN ISO 13849-1, Section 5.2.8, “Fluctuations, loss and restoration of power sources”). The power failure must be considered in the risk analysis of a machine, and in particular the time characteristic of safety functions. Should fastest possible stopping (SS1 or SS2) be necessary but no longer achievable by means of the frequency converter, additional mechanical brakes can for example be employed. This is always the case for vertical axes as well.

The impact of a power failure upon a frequency converter and its ability to generate a torque in the motor or a force in a linear motor in this specific situation are dependent upon the converter’s internal design. The decisive factor is the source of the electrical energy to the frequency converter’s control electronics. A distinction must be drawn here between frequency converters in which the power for the control electronics is supplied from the intermediate DC circuit and those in which it is supplied from the mains system.

4.3.1 Power supply to the control electronics from the intermediate DC circuit

In this type, the control electronics are supplied with power from the intermediate DC circuit via a DC/DC converter (Figure 15).

Figure 15: Supply of power to the control electronics from the intermediate DC circuit



4.3.2 Power supply to the control electronics from the supply system

In this type, the control electronics receive their operational voltage from the mains supply via a power supply unit (Figure 16). Supply from a separate 24 V system is also common; such a system however also fails in the event of a power failure, unless an uninterruptible power supply (UPS) is employed.

Should the mains supply fail, the control electronic also loses its supply voltage and is not able to generate a pulse pattern for the power section of the frequency converter. The motor is no

longer able to generate torque, and neither controlled stopping nor the holding up of a suspended load is possible. The motor coasts to a halt; loads held by vertical axes drop. This behaviour is also exhibited by frequency converters with integrated SS1, SS2 and SOS safety functions. Where this situation gives rise to hazards on a machine, additional measures are required, such as the use of mechanical brakes. The brake can be actuated by the SBC safety function.

At the instant of the power failure, the intermediate DC circuit is at least partially charged. If the power electronics are supplied with power from this circuit, they are still able to generate the pulse pattern for driving the insulated-gate bipolar transistors (IGBTs) in the power section of the frequency converter. This enables torque to be generated in the motor. In many applications, the motor is to be halted as soon as possible in the event of power failure. Owing to the charged intermediate DC circuit, this is still possible for a certain duration, particularly since, depending upon their design, frequency converters may also be able to recover the kinetic energy from the motor during braking and feed it into the intermediate DC circuit. In many cases, this permits safe stopping. If this is required for the safety of an application, the time characteristic must be analysed. On vertical axes, a mechanical device must maintain the safe state at the end of the stopping process. This can be achieved by engagement of a mechanical brake that is actuated by the SBC safety function.

The feeding back of energy into the supply system may no longer be possible following a power failure. The kinetic energy generated during the braking process must therefore be consumed even where frequency converters possess energy recovery capability. This is achieved by braking resistors. Where this not the case, controlled stopping would no longer be fully possible owing to overloading of the intermediate DC circuit.

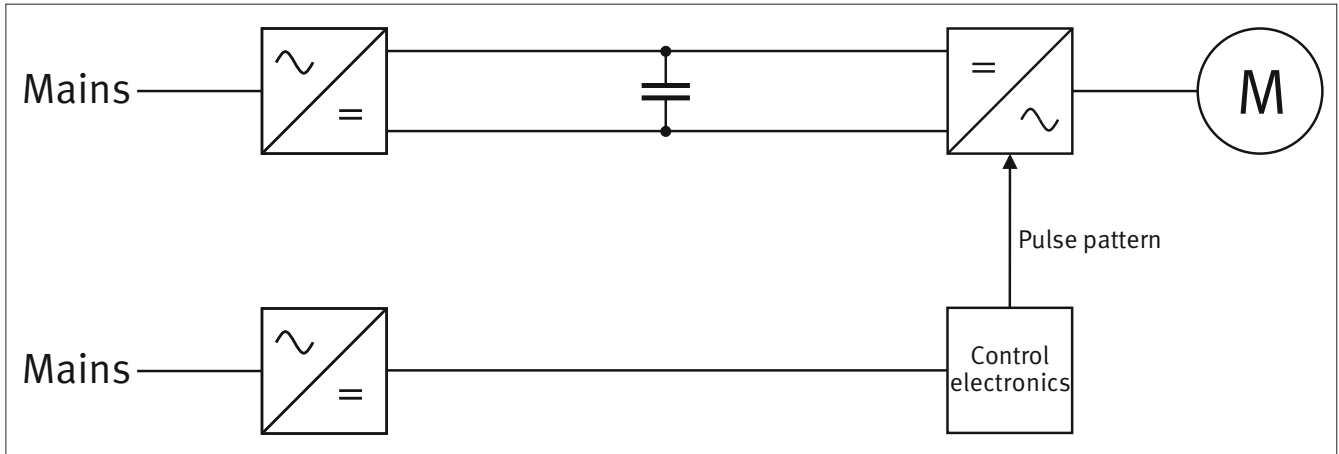
4.3.3 Consideration of power failure in safety functions in accordance with EN ISO 13849-1

In the specific case of vertical axes, different components may be used for the operating states of “supply voltage present” and “supply voltage not present” in order to maintain the safe state of the machine. This may result in different categories, PLs, and certainly different PFH values. For this case, the IFA suggests to provide different safety functions for the two states. Since it can be assumed that under normal circumstances, power

is available, this approach can yield a lower PL_r for the safety functions, that are required only in the event of power failure. Where the risk graph described in EN ISO 13849-1 [2] is applied, a power failure would result in a shorter presence in the hazardous zone, as a result of which the F-parameter of “duration of exposure” would probably always be rated as F1.

In 2012, the IFA submitted a proposal to this effect for the planned amendment to EN ISO 13849-1.

Figure 16:
Power supply to the control electronics from the supply system



5 Frequency converters without integral safety functions (PDS)

Whereas just a few decades ago the majority of variable-speed drives employed DC technology owing to its facility of control, this function is now primarily realized by three-phase drives employing frequency converters. The developments in the area of microprocessors and power electronics have contributed substantially to this change.

A frequency converter consists principally of a cascaded arrangement of a power rectifier, an intermediate DC circuit and a power inverter. The principle arrangement is shown in Figure 17.

The power rectifier is a bridge rectifier that generates a DC voltage from the AC voltage supplied by the three-phase mains supply. Bridge rectifiers are available both with and without closed-loop control.

The intermediate DC circuit is generally equipped with a DC link capacitor that smooths the DC voltage and also serves as an energy store. In some cases, inductances are also fitted in the DC circuits as energy storage devices.

The power inverter of the frequency converter uses power semiconductors (e.g. IGBTs) to generate a three-phase output voltage from the DC voltage of the intermediate circuit. The amplitude and frequency of this output voltage can be controlled over a wide range. The power semiconductors are driven by pulse-width modulation (PWM) in order to generate the rotating field. The pulse patterns required for this purpose are computed in a microprocessor or in a separate module (such as a field programmable gate array, FPGA).

Some types of frequency converter can be used not only to drive motors, but also for braking. In this case, the direction of the energy flow is reversed. Two types are commonly used for conversion of the kinetic energy:

- The kinetic energy is fed in the form of electrical energy through the intermediate circuit and a suitable power inverter back into the mains system.
- From the intermediate circuit, the kinetic energy is converted into thermal energy by means of a braking resistor.

On conventional frequency converters, safety functions can be implemented directly only to a limited extent. Generally, additional components are required. This can be illustrated by the example of the safe torque off (STO) safety function.

The STO safety function can, for example, be activated through the controller inhibit of the frequency converter. Deactivating the trigger signal at this input blocks the generation of pulse patterns. A rotary field can no longer be generated in the motor.

The signal is processed in a single channel involving the microprocessor; this permits a maximum Performance Level of PL b. In the majority of applications on machines, however, higher PLs are required that cannot be attained by means of a single channel. A second, independent channel is therefore required. For this purpose the use of a mains contactor may be appropriate (see Section 3.1.1.1).

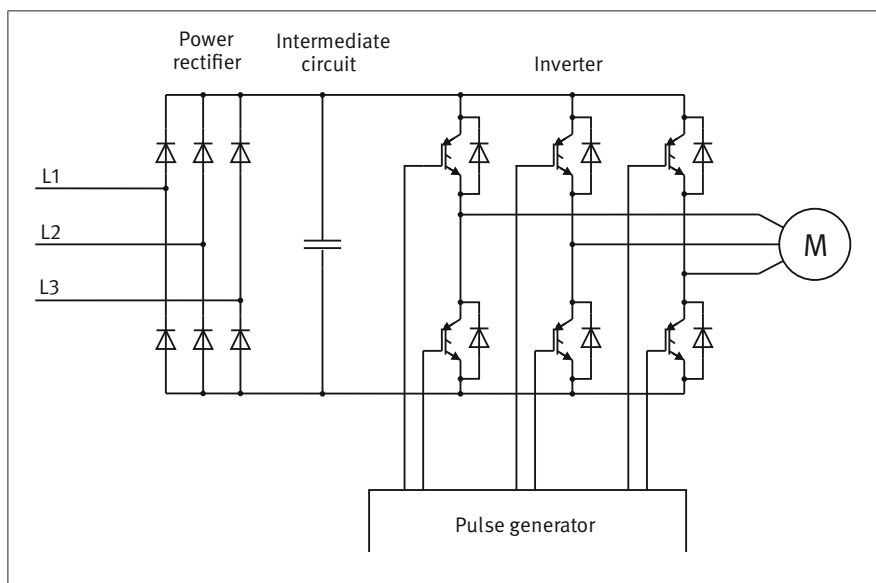


Figure 17:
Schematic diagram of a conventional frequency converter

6 Frequency converters with integral safety functions (PDS(SR))

Conventional frequency converters as described in Chapter 5 are designed in the first instance to satisfy the functional requirements and to cope with the operational stresses, such as vibration, temperature, electromagnetic interference or faults in the power supply. This is assured among other things by observation of the provisions of the EN 61800 series of standards.

Based upon these conventional products frequency converters have been developed, in which safety functions such as STO or safe movement control are already implemented. This brings with it a range of benefits, and simplifies the implementation of safe machine controls. In addition, certain applications are by definition not possible without integrated safety technology, owing to impermissibly long response times.

Implementation of specific safety functions in frequency converters imposes various requirements upon the complexity and design of the hardware. Some safety functions, such as STO, can be implemented in a frequency converter relatively easily. By contrast the SLS safety function for example requires a substantially more complex design. The description below distinguishes between pulse blocking and safe movement control for the implementation of safety functions.

6.1 Pulse blocking

A fault analysis is first to identify what faults or failures must be anticipated in frequency converters, and what effects these faults have upon their function. Suitable measures for implementation of an STO safety function are then presented.

The analysis is taken from a study conducted at the IFA (at that time still BIA). The study made the following observations, relevant to this assessment.

- Unintended power-up, loss of blocking capacity (short-circuit) or delayed de-energization of one or more power semiconductors in the inverter during operation (motor being driven) results in the intermediate circuit being short-circuited. Consequently fuses are tripped or further semiconductors destroyed. In all cases the fault inhibits operation. Should these faults occur during braking, failure of the regenerative braking facility must be expected.
- Loss of blocking capacity (short-circuit) of one or more power semiconductors in the rectifier bridge of the rectifier leads to short-circuiting of at least two phases of the three-phase mains supply. The result is the tripping of fuses or the

destruction of further power semiconductors. In all cases, the fault inhibits operation.

- The loss of conductivity (interruption) of one or more power semiconductors in the power inverter leads to the power available at the output being reduced. The generated torque drops or is lost completely, in both driving and braking modes.
- The loss of conductivity (interruption) of one or more power semiconductors in the rectifier bridge of the rectifier leads to a reduction of the power available at its output. The generated torque drops or is lost completely, in both driving and braking modes.
- The pulse patterns required for the generation of a rotary field are very complex. They can be generated only by means of complex electronic circuits. The random generation of a suitable pulse pattern, for example resulting from influence by electromagnetic interference or from component faults in the power section as described above, can therefore be ruled out.

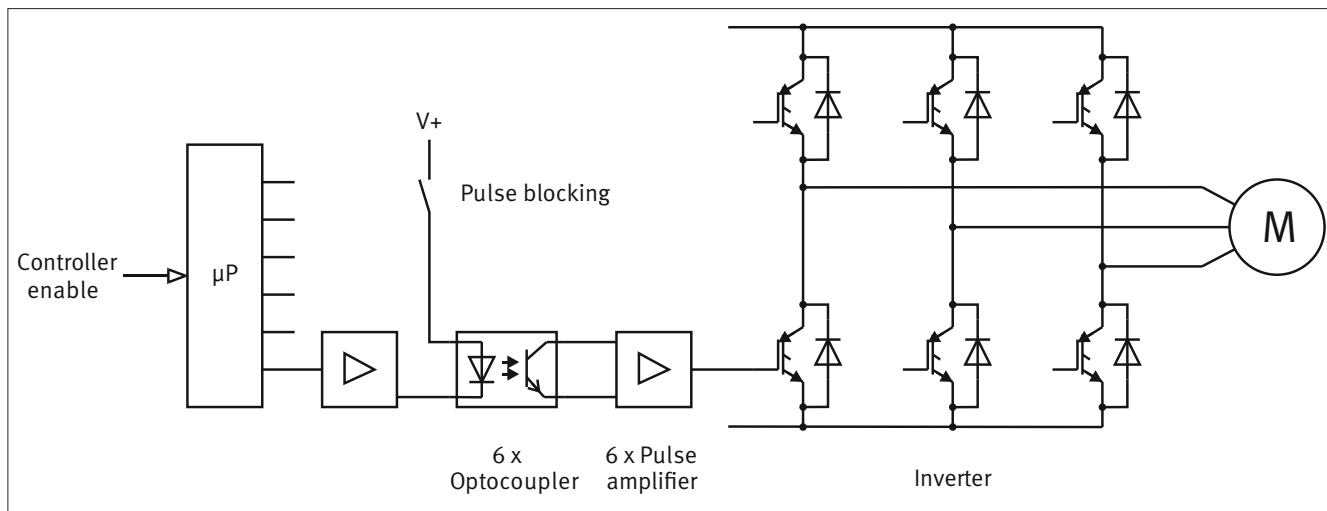
Component failures or influences upon the frequency converter inputs, that could give rise to any conceivable, unintended or incorrect triggering of the pulse pattern generation, must however be anticipated. Such phenomena could cause spontaneous and unexpected fault behaviour, such as unexpected start-up, acceleration, and termination of the braking process with the drive running on and up. Special measures adapted to the respective risk are required for the avoidance of hazardous situations.

If a suitable additional circuit safely prevents the power semiconductors of the inverter from being driven by pulse patterns, this constitutes one means of implementing the STO safety function. A rotary field can then no longer be generated in the inverter, and consequently a torque cannot be generated in the motor. The STO safety function can provide protection against unexpected start-up.

The transmission elements for the pulse patterns which provide galvanic isolation between the microprocessor and the inverter constitute a suitable location for such a circuit. The principle is the same, irrespective of whether transformers or optocouplers are used for this purpose.

If optocouplers are used, the transmission of pulse patterns is blocked by disconnection of the supply voltage to the optocouplers (Figure 18). As soon as voltage is no longer present on the anodes of the optocouplers, signals can no longer be transmitted, even if the microprocessor generates pulse patterns.

Figure 18:
Interruption of the supply voltage to the optocouplers



If this pulse blocking is combined with disabling of the servo enable, the triggering of the inverter with suitable trigger pulse patterns is prevented in two channels. In conjunction with suitable means of fault detection (see Section 6.1.1), Category 3 or 4 to EN ISO 13849-1 [2] can be achieved in this way.

Notes:

Pulse blocking cannot prevent random component faults in the power circuit. Jerky motor movements amounting to a maximum of 180° per pole pair are therefore possible in the event of two certain faults occurring simultaneously in the power section. Start-up of the motor is however not possible. The actual application must be checked for whether jerking of the motor shaft is able to give rise to a hazardous machine movement.

Pulse blocking does not galvanically isolate the motor from the mains system; voltage may therefore still be present both on the frequency converter and on the motor terminals. For the purposes of maintenance and repair, a suitable switch with isolating function is therefore required in addition.

6.1.1 Fault detection

The two shutdown paths of pulse blocking and servo enable may fail in the event of a fault. Fault detection is however possible by means of suitable measures.

Depending upon the design of the frequency converter, fault detection is performed within the converter itself or must be achieved by means of external measures. In the case of internal fault detection, no additional circuitry is required for the frequency converter: fault detection and the safe response (generally the prevention of further movements) take place independently. Where this is not the case, this function must be performed by external components. This can be achieved for example by means of an available PLC, that performs control tasks in the machine, or by a safety switchgear device, such as a safety guard monitor, which generally also activates the safety function within the frequency converter. The manufacturer of the frequency converter sets out requirements for the application

concerned in the information for use. These requirements must be met in order to ensure the stated PL and PFH.

6.1.1.1 Fault detection of pulse blocking

The example below illustrates the operating principle of fault detection for pulse blocking. Figure 19 shows a circuit in which the trigger pulse pattern for driving the power semiconductors is transmitted by optocouplers. The pulse generator (such as a microprocessor) is not shown in the diagram.

When the safety guard is opened, the position switch B1 is actuated and its break contact interrupts the drive of relay K1. Dropping out of K1 disconnects the optocouplers from the supply voltage, and they can no longer transmit trigger pulse patterns. Actuation of the motor is no longer possible. Relay K1 features mechanically linked contacts (in accordance with EN 60947-5-1, Annex L). Break and make contacts are therefore mechanically linked, and cannot both be closed at the same time. The break contact's position is detected by the PLC and checked for plausibility against the position of the safety guard. For this purpose, a signal contact on position switch B1 must also be read by the PLC. A sticking of K1 when the safety guard is opened can be detected. The use of mechanically linked contacts, for example for monitoring functions, is one of the well-tried safety principles described in EN ISO 13849-2 [8].

Electronic components may be used in place of the relay, provided they possess feedback functionality.

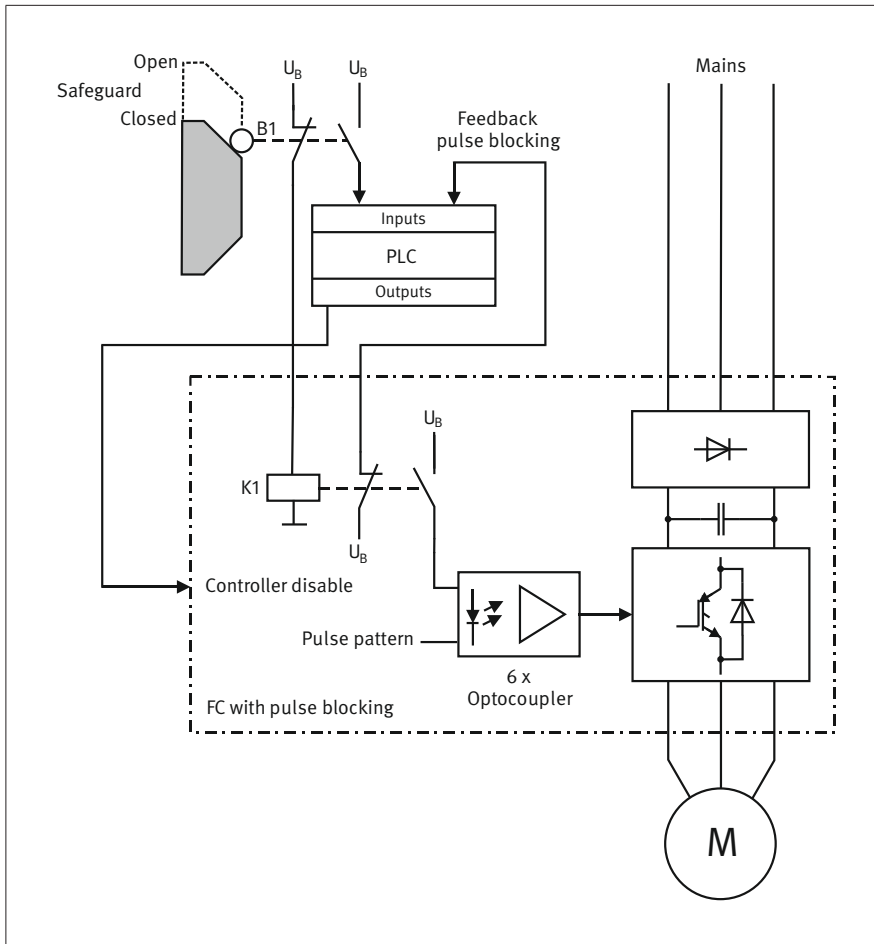


Figure 19:
Fault detection of pulse blocking

For the event of a fault the PLC must have a suitable shutdown path. This could for example take the form of cancellation of the servo enable, or of a primary mains contactor to prevent further motor operation.

Note (to manufacturers of frequency converters):

By reading back the mechanically linked contacts of K1 and the plausibility check in the PLC faults only in the relay itself and in the circuitry outside the frequency converter can be detected. But it cannot be determined whether supply voltage is actually still present at the optocouplers. Consequently, when such a trigger pulse block is implemented, it must be ensured that the optocouplers are not supplied incorrectly with voltage owing to a component fault or a short-circuit between adjacent conductor tracks/contact points on the PCB. Information on corresponding fault exclusions can be found in the tables in Annex D of EN ISO 13849-2 [8].

6.1.1.2 Fault detection of the servo enable⁵

The fault-mode behaviour of the servo enable must also be considered when it is used as a shutdown path. It must for example be anticipated that a random hardware fault in the frequency converter causes the servo enable signal to be read permanently as “1”, even though it has in fact been switched off. A fault of this type may remain undetected when for example the reference value of the speed is set to zero while the servo enable is blocked.

This fault can however be detected by means of a test. For this purpose, the PLC specifies an appropriate reference value for the frequency converter, whilst at the same time the servo enable is blocked (see Figure 20). Should a motor movement (detected by the rotary encoder) occur during this test, the “servo enable” shutdown path is defective. The PLC must possess a separate shutdown path for this case.

Note that the test itself must not give rise to a hazardous situation. Therefore, depending on the application, the right moment for such a test has to be considered carefully.

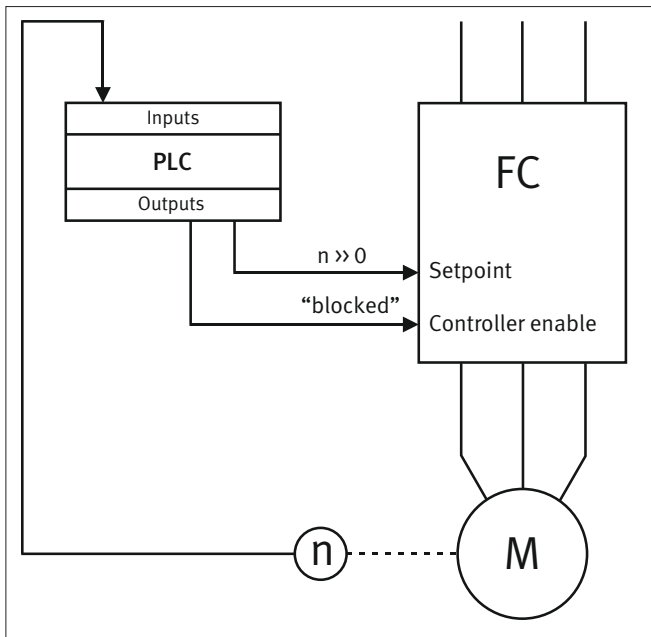
In order to detect faults in the rotary encoder, the PLC performs plausibility tests whilst the motor is in operation. In these tests,

⁵ The method described here for fault detection in the servo enable shutdown path can also be used with frequency converters without integral safety.

the specified reference value is compared cyclically with the actual encoder value. Only when the encoder operates correctly, the testing of the “servo enable” described above is reasonable.

Under certain circumstances, faults in the “servo enable” shutdown path can also be detected through the technical process. This is possible for example when the servo enable not only serves the purpose of activating the safety function, but is also used for operational starting and stopping of the motor. In this case a defective servo disable would then be detectable from the faulty operational behaviour of the machine, provided the speed reference value is not set to zero at the same time in this test.

Figure 20:
Fault detection of the servo enable



6.2 Safe movement control

With the exception of STO, all safety functions require complex calculations of speeds, positions, etc. and are therefore implemented with correspondingly complex microprocessor controls. The requirements placed upon these drive control systems generally give rise to two-channel processor structures that satisfy the requirements of Category 3 or Category 4 to EN ISO 13849-1 [2]. Figure 21 shows the concept of such a two-channel control.

The motor speed or axis positions are measured in Figure 21 by two independent encoders on the motor side⁶. The signals generated in the encoders are interpreted in microprocessor 1 and microprocessor 2. The speed, stationary status, final position, cams, etc. are therefore monitored in two channels. All inputs, for example those required for the selection of safety-related machine functions such as safe operating stop (SOS) or safely limited speed (SLS) are likewise implemented redundantly. The “pulse block” in Figure 21 executes the STO function by two channels and in accordance with the principle described in Section 6.1. In the event of a fault, processor 1 and processor 2 therefore each have an independent shutdown path.

In order for faults in the control and sensor systems to be detected, the two processors perform not only self-tests, but also other tests including cross-checking of data in which they compare their respective safety-related data. Inputs and outputs are also tested. Testing has an influence upon the probability of a dangerous failure per hour (PFH). Depending upon the diagnostic coverage (DC) of the tests and the frequency with which they are performed, the PFH for the safety function(s) is improved.

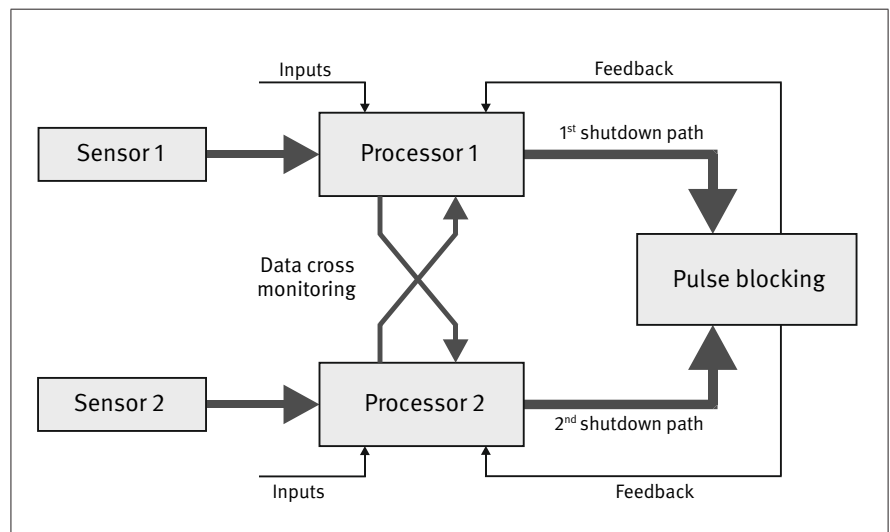


Figure 21:
Safe motion control

⁶ The number of encoders to be employed is dependent upon the safety function and the required PL/SIL. It may be possible to reduce this number by additional measures for the detection of encoder faults. Some manufacturers have implemented alternative methods as substitution for an encoder in the processor control (see Chapter 9).

The manufacturers state fault responses and fault response times in their instruction manuals; these must be suitable for the application concerned (see also Section 6.5).

6.3 PL, PFH and SIL

Frequency converters with integral safety functions (PDS(SR)) are safety components and logic units for safety functions in accordance with Annex IV of [6]. For their use information on their safety-related properties is required. The PDS(SR) is used to implement one or more safety functions for the purpose of risk reduction on the machine. The required scale of this risk reduction has been determined by the risk analysis at the hazard point concerned, and is expressed by the PL_r . In order to determine whether a PDS(SR) can be used, the PL (or SIL for use in accordance with IEC 62061 [15]) for the integrated safety functions must be known. The PFH resulting from the combination of all components involved is also calculated for the entire safety function on the machine. The user must therefore also know the PFH values for the integrated safety functions of the PDS(SR). The PFH may assume different values for different safety functions, since different components of the PDS(SR) are used. If several safety functions of a PDS(SR) are used at the same time, the individual PFH values can in principle be added together. For the most part however, the safety functions generally use identical hardware; the failure rate of many components must therefore be considered multiple times during this addition. The manufacturers of PDS(SR) therefore frequently also state PFH values for the combination of integrated safety functions.

MTTF_d and DC need not be stated for PDS(SR), since these values have already been considered during the determining of PL and PFH. The achieved Category also need not be stated for the application of the frequency converter. EN ISO 13849-1 however requires this information in the “Information for use” section, and certain type C standards contain requirements concerning the Category.

6.4 Stopping and holding position

6.4.1 Stopping of loads

Braking of a movement is a safety function and is to be evaluated in accordance with EN ISO 13849-1 when the risk assessment indicates that the coasting movement presents a hazard and for the purpose of risk reduction the movement needs to be brought rapidly to a halt by braking of the drive. This is the case for example with dangerous movements involving overrun that are not safeguarded by locked safety guards during the stopping process. The hazardous zone may become accessible on such machines before the movement has stopped.

Components for stopping

The following measures are commonly used for non-gravity-loaded axes driven by asynchronous motors:

- reverse-current braking,
- DC braking,
- dynamic braking.

Variable-speed drives are generally driven by frequency converters. These are typically suitable not only for driving the motors, but also for controlled stopping. The kinetic energy is either fed back into the mains supply or is converted into thermal energy in a braking resistor.

Stopping of movements can be achieved by means of mechanical brakes (service brake), or a load is held in position once already stopped (holding brake). The braking force is generally provided by springs. The brake is released electrically, pneumatically or hydraulically. With this concept, the braking action is also provided in the de-energized state (closed-circuit current principle).

Requirements concerning stopping

Risk assessment on the machine gives rise to certain requirements for the “stopping” safety function. In particular, the behaviour of the control system in the event of a fault and in the event of power failure must be considered in accordance with the required PL, as must the resulting additional hazards. In accordance with EN ISO 12100 Section 5.4 b) the following two operating states must be considered regarding the use of frequency converters for stopping:

- normal operation

The machine executes the function provided for controlled stopping. The frequency converter brakes the hazardous movement upon request and switches off the motor torque (SS1), or brakes the movement and subsequently maintains the position (SS2).

- malfunction

Failure of the power supply or failure of the frequency converter as a result of a fault. The load is braked by the frequency converter only with reduced braking torque, or not at all, or acceleration occurs as a result of a fault.

Extended overrun times may therefore arise during a malfunction. Since the power section of all known drive controls is of a single-channel architecture, a fault immediately results in a failure or reduced performance of the braking function. This applies both to conventional frequency converters and to frequency converters with an integral SS1 or SS2 safety function in which – following the incidence of a fault – the drive is de-energized (STO) and controlled stopping is therefore no longer possible (see Sections 3.1.1.2 and 3.1.1.3). It must be decided on a case-by-case basis whether the behaviour is acceptable. It is unacceptable for example for the braking of calender rollers. If

persons are working close to the entrapment point, the availability of the braking function is crucial.

Depending upon the PL required for safe stopping, other measures may be needed in addition to braking by the frequency converter, such as the use of a mechanical (linear or rotary) service brake, or braking by means of a DC voltage.

Note:

Some frequency converters/servo controllers are able to bring a movement to a controlled stop despite a power failure, by means of power supply from the intermediate circuit (see Section 4.3.1).

6.4.2 Holding up loads against gravity (vertical axes)

Gravity-loaded axes must be maintained in position both in operation and in event of power failure in cases in which persons are able to intervene in the hazardous zone. Holding brakes which prevent the load from descending inadvertently in the event of a power failure are generally a minimum requirement for this purpose. Examples are machines such as presses employing servo drives, with the hazardous zone safeguarded by a light curtain. On these machines, both controlled stopping by the drive control and the use of holding brakes are required.

In accordance with EN ISO 12100:2011-03 Section 5.4 b), the following two operating states must be considered for vertical axes:

Normal operation:

The machine executes the intended function:

- a) Following controlled stopping by the frequency converter, it also assumes the function of safe holding up against gravity (SS2).
- b) Following controlled stopping by the frequency converter (SS1), a holding brake is actuated (SBC) that maintains the load in position.

Malfunction:

Failure of the power supply or failure of the frequency converter as a result of a fault. The frequency converter is not able to maintain a load in a raised position.

In the event of a malfunction, the functions of stopping and holding up against gravity must be fulfilled by a mechanical brake (such as a spring-operated brake with emergency-stop capability, see [16]).

The special situation of vertical axes must also be considered during engineering of the measures for stopping in the event of an emergency (emergency stop). In accordance with EN 60204-1 [10], Section 9.2.5.4.2, the emergency-stop function must take the form of Stop Category 0 or Stop Category 1. In other words, the drive energy is always switched off, making mechanical brakes indispensable.

Requirements concerning holding up against gravity

Risk assessment on the machine gives rise to certain requirements for the safety function of “holding up against gravity”. Detailed information on determining the required PL and on suitable protective measures can be found in Expert Committee Information Sheet 005, Gravity-loaded axes (see Annex C, page 105). The comments in Section 4.3, Failure of the power supply, are also useful.

6.4.3 Mechanical brakes as components within safety functions

Where placed on the market separately, holding brakes provided by the manufacturer for safely holding up loads against gravity constitute safety components in accordance with Article 2 (c) of the Machinery Directive. The same applies to service brakes used to reduce the overrun times of hazardous movements. In these cases, the manufacturer of the brake issues a declaration of conformity and provides information in the instruction manual on the safe use of the brake. If standard components are used, it is the sole responsibility of the machinery manufacturer to implement the relevant safety functions correctly [17].

Requirements to be met by mechanical brakes in safety functions have as yet been formulated only for emergency brakes with holding brake function for linear movements. They are described in the GS-MF-28/02.2012 test principles [16] of DGUV Test.

Besides design requirements, tests are set out for demonstrating the mechanical service life. $1 \cdot 10^6$ switching cycles under static load and 2,000 switching cycles under dynamic load must be demonstrated under testing.

Note:

A spring-operated brake is frequently employed. The braking force is generated by several braking springs. It forces the friction lining against the brake disc. Sudden complete failure of the spring-operated brake is not generally assumed, owing to its design.

Besides suitable design of the brake, fault-detection measures are required in the application for Category 2 upwards in accordance with EN 13849-1 [2]. The serviceability of brakes can be determined by static and dynamic tests. The IFA recommends the following procedure:

a) Static test of the brake

The serviceability of the mechanical brake is determined by regular testing. For this purpose, 1.5 times the maximum load torque is applied to the brake by the drive motor. If the position of the load is held within the specified range, the brake is considered properly functional. Should the position leave the specified range, the brake must be checked in accordance with the instruction manual and, if necessary, be replaced.

b) Dynamic test of the brake

The dynamic brake test is performed at regular intervals under defined velocity and mass conditions. The interval between tests varies according to the operating and environmental conditions, but must not exceed one year.

Shortly before the braking process is initiated by the mechanical brake, the torque of the drive motor is switched off by the control system. The mechanical brake is engaged. The overrun travel and overrun time must be measured and compared with the permissible values. Should a permissible value be exceeded, further use of the machine must be prevented. If necessary, the mechanical brake must be replaced.

Note:

The dynamic test has the purpose of ensuring that the overrun during the braking process does not lengthen impermissibly in the course of the service life (for example owing to hardening of the brake linings). The overrun may increase slightly even if the static braking test is passed. This is partly due to differences in physical properties between dynamic braking and static holding. The test itself must not present a hazard. The overrun may increase between the dynamic tests; should the risk assessment show this not to be tolerable, additional measures are required.

6.5 Limitations of safety functions

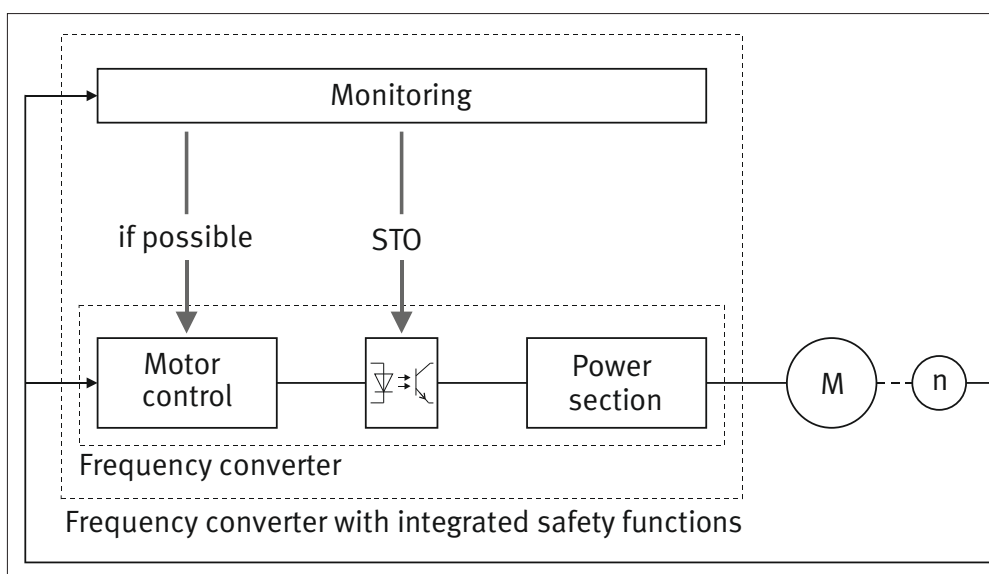
With the exception of STO, safety functions are generally purely monitoring functions. The motor is driven by single-channel control and without engineered safety (see frequency converter in Figure 22). An additional monitoring facility monitors the

motor movements and intervenes in the motor control when configured limit values are violated or when it is determined that the part of the control system executing the safety function itself has a fault.

It is normally assumed that the de-energized state of a machine is a safe state. No importance is therefore attached to the availability of a motor control. Accordingly, responses in the event of a fault are geared towards the stopping of movements. If for example a violation of the maximum permissible speed is detected (SLS safety function), stopping is initiated. Whether controlled stopping or merely coasting to a halt is possible depends upon the functions still available in the frequency converter. If the closed-loop motor control is still functioning properly and the power section does not exhibit a fault, the motor can be stopped as fast as possible. If however a fault is present in the closed-loop motor control of the frequency converter, the motor will no longer be able to generate the required braking torque. The cause of the fault is often not known; in the majority of cases, there is therefore no alternative but to activate the STO safety function and to allow the motor to coast to a halt. Definition of the safety functions required for a machine must consider the possibility of this behaviour, and additional measures must be taken if necessary. If for example lengthening of the time required for stopping in the event of failure of SS1 or SS2 is not tolerable, or loads held up against gravity could drop in the event of failure of SOS, a mechanical brake may be required.

This issue generally applies to all known frequency converters featuring integrated safety functions. As far as the authors are aware, a redundancy in the control and power sections in order to assure availability has not been implemented at this stage. Even if such redundancy were available, a solution would still have to be found for the power failure.

Figure 22:
Frequency converter + monitoring + pulse blocking = frequency converter with integrated safety functions



Many safety functions require parameters to be defined determining the behaviour of the safety function. Particular attention must be given here to the time characteristic. A fault must at first be detected before a suitable reaction can be triggered and the safe state can be provided.

Figure 23 shows by way of example the time characteristic for the SLP safety function. At time t_0 , the set maximum value for the position of an axis is exceeded. Monitoring detects the violation at t_1 and activates STO. The drive coasts down and comes to a halt at t_2 . For a duration $t_2 - t_0$, the axis is still moving and has entered the illegal range. In order to prevent this, consideration must be given to the time characteristic for execution of the safety function, and the limit value must be set correspondingly lower in order to prevent the permissible range from being left.

The STO safety function is not a monitoring function; it merely ensures that the functional drive of the motor is interrupted, with the result that a rotary field cannot be generated within the motor. This function also has its limitations, however. For example, STO cannot prevent the motor from jerking briefly when stationary in the event of a fault in the power section. The magnitude of the jerking movement is dependent upon the number of pole pairs of the motor, and where applicable upon the gear stage. STO prevents a rotary movement from occurring, however. Where STO is applied, it must be determined whether

jerking in the event of a fault can be tolerated. If not, a mechanical brake may have to be fitted in addition. This is the case, for instance, for a milling machine with a milling tool that must be clamped in place manually. Even minor movements of the motor may cause finger and hand injuries in this case.

All safety functions therefore have their own particular limitations of use and in some cases different reactions in the event of a fault. The manufacturer of the PDS(SR) provides corresponding information in the instruction manual. The following must be noted during engineering of a drive control with integral safety functions:

- What reaction occurs when a limit value is violated?
- What reaction occurs when a fault is detected in the part of the control system that executes the safety function?
- What reaction time must be considered before the safe state is reached?
- What hazard exists as a result in the application?
- Are additional measures required (such as a mechanical brake or a greater interval between the light curtain and the hazard point)?

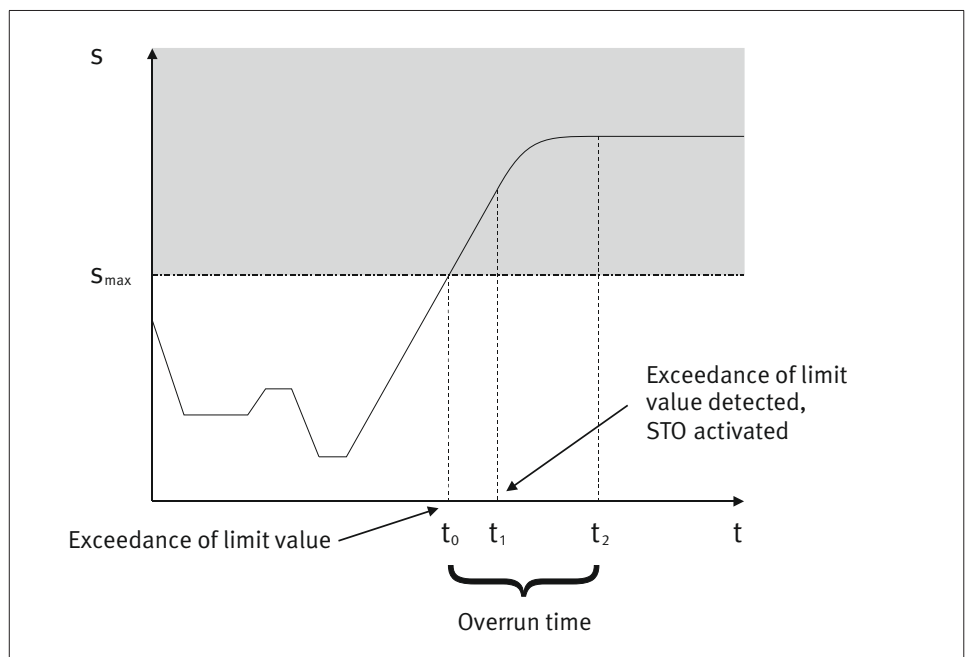


Figure 23: Distance/time chart of the SLP (safely limited position) safety function

7 Safety functions on DC drives

As already stated, only a few decades ago the majority of variable-speed drives employed DC technology, owing to the ease of control. Three-phase drives in conjunction with frequency converters or servo controllers are now primarily used for this purpose. For this reason, this report concentrates on the safety functions implemented in conjunction with drive controls for three-phase motors.

DC drives should not be completely ignored however, since they are still used in some areas, particularly in heavy industry (such as in rolling mills). The principle of speed control is explained briefly below with reference to the example of a DC motor with separate excitation.

The motor consists of a fixed part (the stator) and a rotating part (the rotor or armature). The magnetic field of the stator is generated in the field converter. The armature draws its energy from the armature converter (Figure 24).

The rotational speed of the motor can be adjusted up to its base speed by variation of the armature voltage. At a constant load, an increase in the armature voltage results in an increase in speed. In this example, the armature voltage is generated in the armature converter from the mains voltage by means of a three-phase thyristor bridge. The amplitude of the DC voltage is adjusted by means of a phase control, with its firing pulses being generated by the trigger pulse generator. To enable the drive to

be operated in both directions of rotation, two three-phase thyristor bridges are connected back-to-back. In order to increase the rotational speed of the machine beyond the base speed, the field current must be reduced in order to attenuate the exciting field. The circuit used for this purpose is located in the separate field converter.

In general safety functions are integrated into drive controls for DC motors in the same way as with three-phase motor drives. They differ substantially with regard to the STO function, however.

In order for the STO safety function to be implemented, generation of a torque in the motor must be prevented. This can be achieved by preventing the flow of current in the armature. This is possible, for instance, by using a mains contactor by means of which the supply of power to the motor armature is switched off. There are advantages to integrating the safety function into the drive control. Pulse blocking has already been described as a suitable measure for implementing the STO safety function within the drive controls of three-phase drives. By switching off the supply voltage for the transmission elements (such as optocouplers), the excitation of the power semiconductors is disabled. Figure 25 shows this concept with reference to the example of the armature converter. The use of contactors is not always advantageous (contact pitting, costs, etc.).

Figure 24: Principle arrangement of a drive control for DC motors with separate excitation

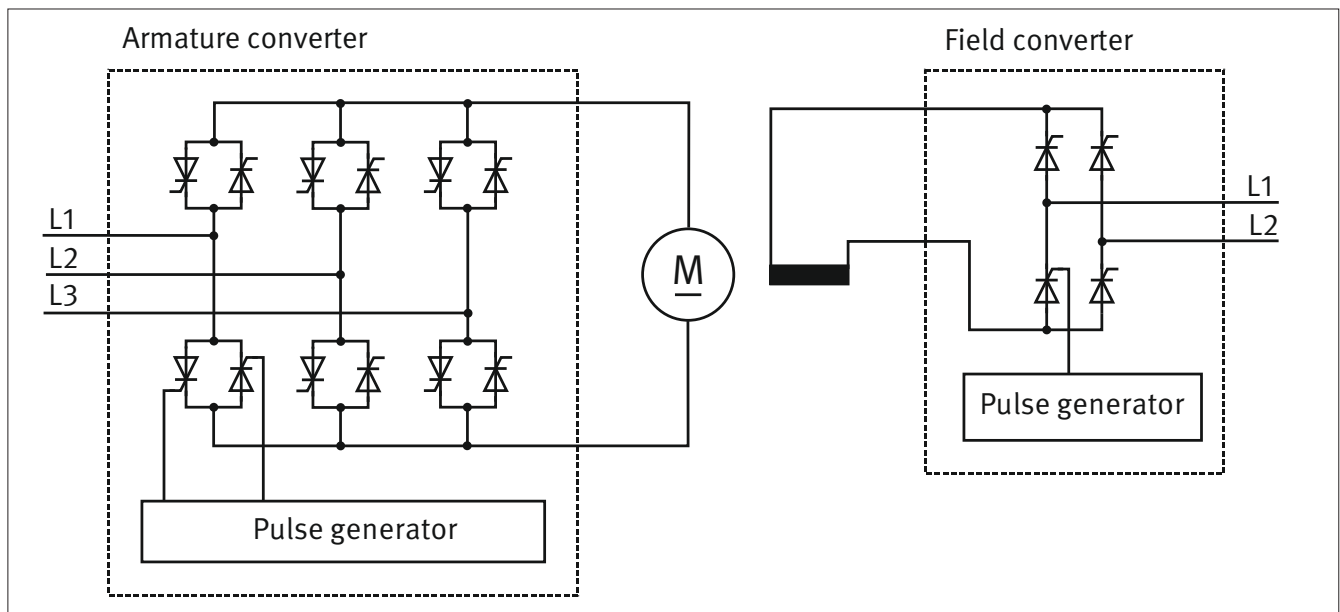
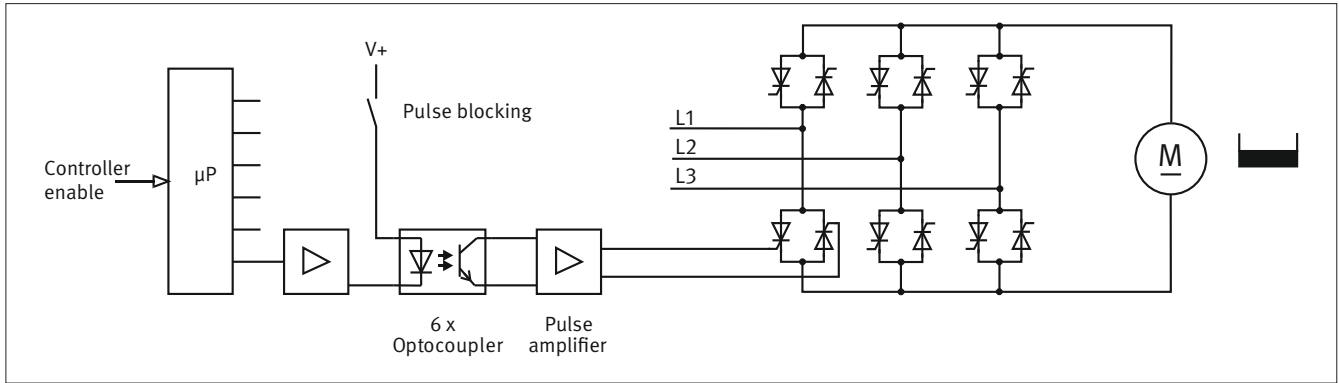


Figure 25:
Pulse blocking in the armature converter



In contrast to three-phase drives, that require complex pulse patterns for the generation of a rotary field, a DC motor requires only a DC current in order to generate a torque. This necessitates a different fault analysis with regard to the STO safety function, and constitutes the crucial difference between three-phase and DC drives. Whereas in the case of three-phase drives, it can be assumed that if the transmission of pulses is reliably blocked, a rotary field cannot be generated in the motor as a result of random component faults in the final stage and consequently no torque can be generated, the situation is different for a power converter used for DC motors. In this case, faults in the power thyristors may permit the flow of current despite pulse blocking (and possibly with the servo enable switched off) if, for example, a common-cause failure (CCF) causes two “suitable” thyristors to act as diodes. This fault gives rise to an armature

current by means of which the DC motor is able to generate a torque and cause the motor shaft to turn. The fault in the power thyristors assumed here could also occur in the power section for the three-phase motor; in this case however, it could only cause jerking of the motor shaft and not a rotary movement, since a rotary field cannot be generated.

In applications in which single-fault tolerance must be satisfied (Category 3 and Category 4), the measure of pulse blocking in the armature converter is not sufficient on its own. For these Categories, an additional shutdown path is required, even if pulse blocking is of two-channel or single-fault-tolerant design. This additional shutdown path could for example take the form of an additional mains contactor in the armature circuit, or additional pulse blocking in the field converter.

8 Drive control: integrated or external safety?

In principle, safety functions can be achieved with the use of purely functional drive controls by the addition of further external components. This report describes examples of this (see Annex B, pp. 51 ff.). However, an integrated solution employing a PDS(SR) offers additional benefits, as the performance of an external solution may also be unsatisfactory, depending upon the application. Figure 26 shows by way of example the two conceptual solutions for the safely limited speed (SLS) safety function. The motor speed is monitored for its compliance with a specific limit value. When this speed is exceeded, i.e. in the event of a fault, the safe torque off (STO) function is activated.

If for example motors with high acceleration and speeds are used, the shutdown times in the external monitoring path may be so high that a hazard cannot be avoided in time in the event of a fault. Integrated solutions have substantially shorter fault detection and response times, and could meet the requirements.

Even where external solutions are suitable for the tasks in hand, however, they may have substantial drawbacks. If for example unexpected start-up is prevented by a mains contactor, the intermediate circuit in the frequency converter must first be recharged before the motor can be moved again when it is

switched back on. This may lead to undesired delays. In addition, older frequency converters in particular may have very high inrush currents that may place a severe load upon the mains contactor. This may lead to premature wear of the contacts. If in addition an unsuitable circuit is used, a risk exists of this fault not being detected, and of hazards arising as a result.

A further benefit of the integrated solution is the lower hardware complexity. Fewer components are required, and the wiring work is reduced substantially. In addition, the mains contactor alone is a cost that should not be underestimated, particularly on drives with high power ratings.

Integrated solutions are also much simpler to engineer. Fewer interfaces need to be considered, and no measures are required for fault detection in the external components.

The frequency converter forms part of the overall safety function on the machine, and must be considered during quantification. A PDS(SR) is regarded as an encapsulated subsystem for which the manufacturer states all necessary data (PL and PFH). $MTTF_d$, DC, CCF and data for the converter software are not required. The integrated solution thus also simplifies calculation of the PFH for the safety function.

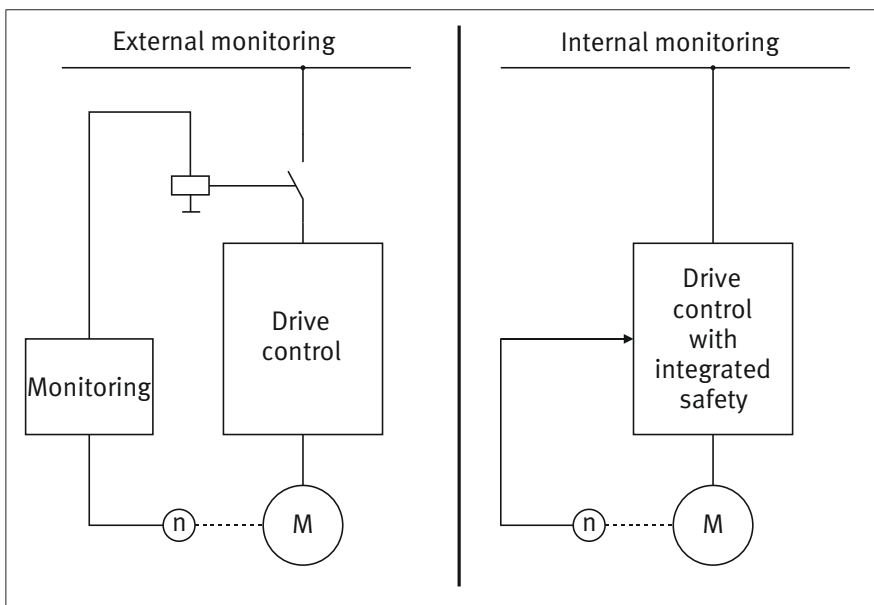
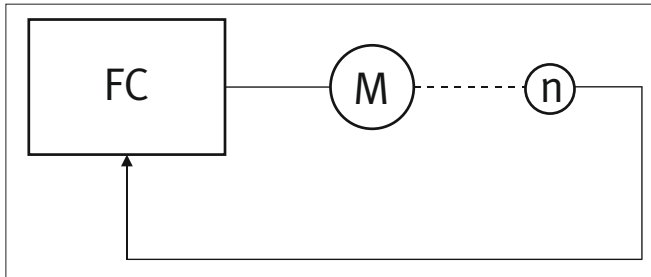


Figure 26: SLS with external monitoring and as an integrated solution

9 Position encoders in safety functions

For commutation and control of a motor, the frequency converter/servo controller requires the instantaneous position, which is normally provided by a rotary or linear encoder⁷. This can be used to create a closed control loop that is used for example for positioning tasks (see Figure 27).

Figure 27:
Closed control loop



Encoders can be divided broadly into incremental and absolute value encoders. Incremental encoders provide relative information on the rotary angle of an axis or the position of a linear movement. According to the requirements of the safety function to be implemented, a connected drive control can use this information to determine for example speed (safely limited speed, SLS) and/or acceleration (safely limited acceleration, SLA). In these cases, knowledge of the absolute position is not required.

However, if for example pinch points in a machine are to be safeguarded by means of safety functions, certain parts of the machine must remain within the permissible range of movement. This can be achieved by means of the SLP (safely limited position) safety function, which requires knowledge of the absolute position. Incremental encoders must first be reliably referenced when the mains supply is switched on. This is generally achieved by the machine travelling to a defined internal position that is fitted with an additional position sensor. Once the machine has travelled to the reference point, the absolute position can be computed in the drive control by addition or subtraction of increments.

The use of absolute value encoders is simpler. In this case, a digital position signal is available and referencing is not needed. A distinction is drawn between single-turn and multi-turn rotary encoders. On single-turn encoders, an unambiguous absolute position can be obtained only within a single rotation of the encoder shaft. Conversely, a multi-turn encoder also signals the number of turns that have been completed, thereby also providing an unambiguous absolute value after several turns.

⁷ Frequency converters exist that deduce the necessary position information from internal signals and do not therefore require external encoders. They cannot be used to implement all safety functions, however.

The safety requirements imposed upon the encoders depend essentially upon the safety function to be implemented, and of course upon the PL_r determined for the application.

A wide range of encoders are available on the market. The interface between the encoder and the frequency converter or servo controller is particularly important for interaction between the two. The following are widely used:

- Incremental encoders with square-wave signals
- Incremental encoders with sin/cos signals
- Incremental and absolute encoders with bus interfaces

A large number of safe encoders are now available for safety applications. The manufacturers of these components state the PL or SIL up to which they can be used. Component faults leading to a dangerous failure of a safety function may also occur on safe encoders; measures for fault detection are therefore required. This is often not possible in the encoder itself, but must be achieved in the frequency converter or servo controller to which it is connected. The encoder manufacturers describe the measures required for attainment of the relevant PL/SIL in their instruction manuals. With sin/cos encoders, testing for $\sin^2 + \cos^2 = 1$ is often necessary. This detects many faults, albeit not all. The diagnostic coverage (DC) is generally 90 to 99%.

Encoder shaft breakage is critical. This is the loss of coupling between the encoder shaft and the motor shaft, or a mechanical defect in mounting of the encoder causing the entire encoder to rotate with the motor shaft. Depending upon the safety function, this may cause an undetected hazardous fault. This leads to limitations, particularly in the use of gravity-loaded vertical axes. A solution is the use of encoders that have been mechanically overdesigned by the manufacturer, thereby enabling encoder shaft breakage to be excluded (see [3], Table D.16).

Note:

Implementation of PL e/SIL 3 with the use of fault exclusion is not generally approved (see ISO/TR 23849 [18], Section 7.2.2.3). The mechanical encoder components under consideration here are however overdesigned by such a high factor that the fault exclusions are also permissible in PL e/SIL 3.

Where safe encoders are not used in an application, the implementation of safety functions is possible in principle even with non-safety-grade encoders. Some manufacturers of PDS(SR)s enable such encoders to be used by means of a suitable fault detection facility in the safe controller (refer to the instruction manual of the PDS(SR)). In all other cases however, responsibility lies with the machine manufacturer to demonstrate that the required PL/SIL has been met [17]. For this purpose, an FMEA must be conducted of the possible failure types and their effects upon the safety function for all components involved in signal generation and processing. The information and knowledge required for this purpose are not generally available to the user

of the encoder; the support of the encoder manufacturer is therefore required in this case.

Besides testing for $\sin^2 + \cos^2 = 1$, a further means of encoder fault detection exists: the encoder can be integrated into the frequency converter/motor control loop. Faulty encoder signals generally lead to an incorrect value being delivered for the motor position. Consequently a correct commutation of the motor is not possible. This leads to an operating fault and thus to a detection of the fault via the technical process (DC of at least 60%).

Processing of signals from safe sin/cos encoders

If encoders are employed in conjunction with safe frequency converters, speed monitors or zero-speed relays, the processing of signals is not an issue for the user. In these cases, the instructions for the use of these components describe the proper connection of the encoder and evaluation unit and – where applicable – the configuration of parameters. Signals are interpreted in the evaluation units according to the PL/SIL stated. If dedicated circuits are developed, however, the following must be considered.

Sin/cos encoders are used to increase the resolution by determining position values between the sin/cos zero crossings (coarse position) by means of an arctan calculation (fine position). In

general however, this increased resolution is not required for the implementation of safety functions. If for example a machine component is to be prevented from passing a particular position in order for finger protection to be achieved at a potential pinch point, resolution within the region of one millimetre is likely to be adequate for the position monitoring of the axis concerned. This resolution can generally be achieved by interpretation of the sine or cosine channel alone. Considered in this way, a safe encoder with one sine and one cosine output signal is regarded as a two-channel system. Should a higher resolution be necessary in a particular application (such as on a rotary table with a diameter of 4 m, or when gearing is used), as a result of which the fine resolution is required for the safety function, the sin/cos pair must be treated as a single channel. Depending upon the required PL, a second channel may then have to be added, for example by the use of a second encoder.

Should signal interpretation in Category 3 or Category 4 be implemented, for which the coarse position resolution is sufficient, the sine and cosine channels must be processed separately. This must be considered throughout. Merging the sine and cosine channels would result in a single-channel arrangement. This would for example be the case when, for the purpose of speed measurement, only the sum of the zero crossings of the sine and cosine signals are interpreted – even in a two-channel arrangement – rather than sine and cosine signals being processed separately.

10 Acceptance test

The system behaviour of each drive control is adapted to the application in question by means of configurable parameters. For this purpose, maximum permissible speed values for example or the time characteristic during stopping of a drive are defined. The settings must be reviewed, irrespective of whether safety functions are implemented by means of controls with integral safety or by the use of external monitoring equipment. The objective is to demonstrate correct system behaviour (time, travel, procedure, etc.), and thereby to detect any errors in engineering or inputs. Transmission errors, for example in the connection between the non-safe PC and the safe parameter memory, are not assumed at the time of the acceptance test. Specific requirements are set out in EN ISO 13849-1, Section 4.6.4 for the parameter configuration procedure. The purpose of the acceptance test is therefore to identify parameters for which unsuitable values have been selected but that have been set without faults in the safe control system. The following are possible sources of faults:

- Unsuitable limit values for speed, braking, delay times, position
- Parameters have in principle been selected correctly, but are unsuitable for certain machine states
- Input errors during parameter configuration
- Priority conflicts with other safety functions
- Different requirements for parameter configuration, depending upon the operating mode

Annex A (see page 49) contains an excerpt from [19] with minor modifications by the authors, providing information on the procedure for commissioning, the modification of parameters, and series production machines.

For the use of frequency converters with integral safety functions, the manufacturers provide forms in the instruction manual.

Performance of the acceptance test presents a good opportunity to examine the behaviour in the event of a power failure and occurrence of a fault within the safety function. Both are generally associated with a loss of motor torque, but must not give rise to a hazardous state.

References

- [1] EN 954-1: Safety of machinery – Safety-related parts of control systems – Part 1: General principles for design (3/1997). Beuth, Berlin 1997
- [2] EN ISO 13849-1: Safety of machinery – Safety-related parts of control systems – Part 1: General principles for design (07/07). Beuth, Berlin 2007
- [3] EN IEC 61800-5-2 (VDE 0160-150-2): Adjustable speed electrical power drive systems – Part 5-2: Safety requirements – Functional (4/2008). Beuth, Berlin 2008
- [4] Hauke, M.; Schaefer, M.; Apfeld, R.; Bömer, T.; Huelke, M.: Functional safety of machine controls – Application of EN ISO 13849. BGIA-Report 2/2008e. Published by: Deutsche Gesetzliche Unfallversicherung (DGUV), Sankt Augustin 2008
- [5] EN 61508: Functional safety of electrical/electronic/programmable electronic safety-related systems – Parts 0-7 (11/2002 to 10/2005). Beuth, Berlin 2002 to 2005
- [6] 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) 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. http://eur-lex.europa.eu/LexUriServ/site/en/oj/2006/L_157/L_15720060609en00240086.pdf and http://eur-lex.europa.eu/LexUriServ/site/en/oj/2007/L_076/L_07620070316en00350035.pdf
- [7] EN ISO 12100: Safety of machinery – General principles for design – Risk assessment and risk reduction. Beuth, Berlin 2010
- [8] EN ISO 13849-2: Safety of machinery – Safety-related parts of control systems – Part 2: Validation (2/2013). Beuth, Berlin 2013
- [9] Apfeld, R.; Schaefer, M.: Sicherheitsfunktionen nach DIN EN 13849 bei überlagerten Gefährdungen. Fachmesse und Kongress SPS/IPC DRIVES, 23. to 25. November 2010, Nuremberg – Lecture. Published by: Institut für Arbeitsschutz der Deutschen Gesetzlichen Unfallversicherung (IFA), Sankt Augustin 2011. <http://publikationen.dguv.de/dguv/pdf/10002/sicherheitsfunktionen.pdf>
- [10] EN 60204-1: Safety of machinery – Electrical equipment of machines – Part 1: General requirements (6/2007). Beuth, Berlin 2007
- [11] Apfeld, R.; Portmann, M.: Festlegen von Maximalgeschwindigkeiten für manuelle Eingriffe an laufender Maschine (Kennzahl 330 216). In: IFA-Handbuch Sicherheit und Gesundheitsschutz am Arbeitsplatz. 2. suppl. XII/2011. Published by: Deutsche Gesetzliche Unfallversicherung (DGUV), Berlin. Erich Schmidt, Berlin – loose-leaf ed. 2nd ed. 2003. www.ifa-handbuchdigital.de/330216
- [12] Grenzwerteliste 2013 – Sicherheit und Gesundheitsschutz am Arbeitsplatz. IFA Report 1/2013. Published by: Deutsche Gesetzliche Unfallversicherung (DGUV), Berlin 2013. www.dguv.de/ifa/grenzwerteliste
- [13] EN 60947-5-1: Low-voltage switchgear and controlgear – Part 5-1: Control circuit devices and switching elements – Electromechanical control circuit devices (2/2005). Beuth, Berlin 2005
- [14] Grundsätze für die Prüfung und Zertifizierung von Elektromechanischen Zustimmungsschaltern und Zustimmungseinrichtungen (GS-ET-22). Ed. 11/2009. Ed.: Fachausschuss Elektrotechnik, Prüf- und Zertifizierungsstelle im DGUV Test, Köln. www.bgetem.de, Webcode 12700341
- [15] IEC 62061: Safety of machinery – Functional safety of safety-related electrical, electronic and programmable electronic control systems (10/2005). Beuth, Berlin 2005
- [16] Prüfgrundsatz für Notfallbremsen mit Haltefunktion für lineare Bewegungen (GS-MF-28). Ed. 23/2013. Published by: Prüf- und Zertifizierungsstelle Maschinen und Fertigungsautomation im DGUV Test, Mainz 2012. www.dguv.de/dguv-test/de/produktsicherheit/pruefgrundlagen/pruefgrundsaeetze/10mf/index.jsp
- [17] Bömer, T.; Schaefer, M.: Unterschiede bei der Verwendung von fertigen Sicherheitsbauteilen und Standardbauteilen für die Realisierung von Sicherheitsfunktionen an Maschinen. Published by: Institut für Arbeitsschutz der Deutschen Gesetzlichen Unfallversicherung (IFA), Sankt Augustin 2011. <http://publikationen.dguv.de/dguv/pdf/10002/standardkomponenten.pdf>
- [18] ISO/TR 23849: Guidance on the application of ISO 13849-1 and IEC 62061 in the design of safety-related control systems for machinery (5/2010). Beuth, Berlin 2010
- [19] Sicherheitsgerichtete Funktionen elektrischer Antriebssysteme in Maschinen (6.98), Positionspapier DKE AK 226.03. Published by: Deutsche Elektrotechnische Kommission im DIN und VDE

Annex

Annex A:

Acceptance test*

1 Preliminary remarks

The following remarks were published in a DKE position paper in 1998. Most of the content has since been incorporated into international standards. The requirements regarding the acceptance test have however not been adopted in this detail (see [3], Section 7.1 f.), and are therefore reproduced here. The position paper is intended for manufacturers of drive controls with integrated safety functions. However, it also applies when safety functions are implemented by a suitable application of conventional components. In this case, the requirements concerning the acceptance test must be implemented analogously by the manufacturer of the machine control system.

2 Requirements concerning the complete acceptance test

The complete acceptance test must be performed at commissioning and whenever a completely saved data record of the safety-related parameters is modified.

The control system must issue a warning message prompting for performance of the complete acceptance test. Once the acceptance test has been passed, the warning message should be acknowledged by an action not normally used for operational acknowledgement (such as actuation of a dedicated button). The manufacturer of the drive must provide instructions for performance of a complete acceptance test, for example in the form of a checklist. The documentation must indicate that a complete acceptance test is to be performed by authorized personnel when the machine is commissioned and in the event of modifications to the software or hardware (including for example modification by the remote transmission of data). The documentation must also indicate that the modifications and passing of the complete acceptance test are to be documented in a suitable manner. The acceptance test must be performed by personnel authorized by the machine manufacturer.

3 Requirements concerning the partial acceptance test

The partial acceptance test must be performed in case that only some but not all of the saved safety-related parameter data has been modified. The control system must prompt for performance of the partial acceptance test with a suitable warning message. Once the acceptance test has been passed, the warning message should be acknowledged by an action not normally used for operational acknowledgement (such as actuation of a dedicated button). The manufacturer of the drive must provide instructions for performance of a partial acceptance test, for example in the form of a checklist. The documentation must indicate that, when safety-related data is partly modified, it needs to be checked at least by a partial acceptance test. The documentation must also indicate that the modifications and passing of the partial acceptance test are to be documented in a suitable manner. The acceptance test must be performed by personnel authorized by the machine manufacturer.

4 Acceptance test for series production machines

For series production machines, the acceptance test needs not to be repeated when a complete acceptance test has been performed on a model machine, and the safety-related parameter data is subsequently transferred to the series production machines in a manner that safeguards them against modification.

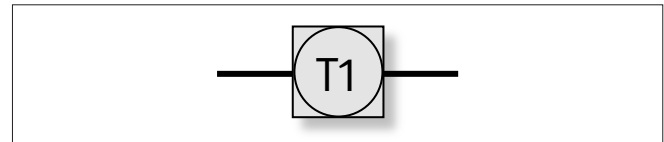
* Source: [19]

Annex B: Compendium of example circuits employing frequency converters

This compendium of example circuits has been compiled in order to illustrate the use of frequency converters in practice. The examples are the product of many years' experience in consulting and testing in the area of safety-related machine controls, but do not include manufacturer-specific proposals for implementation. For reasons of simplification some of the control equipment for implementation of the control specifications (operating mode selector switches, inching switches, etc.) is not shown.

The $MTTF_d$ values used in the calculations are marked as manufacturers' values (**(M)**), typical values from databases (**(D)**), values from EN ISO 13849-1 (**(S)**) and assumed values (**(A)**).

In addition to the symbols used in the presentation of the safety-related block diagrams in BGIA-Report 2/2008e, the encapsulated subsystem is also used in the following example circuits:



Safety components for which manufacturers state PL (or SIL) and PFH values are described as encapsulated subsystems. These data are sufficient for consideration in safety functions. The influence of the Category, fundamental and well-tried principles, $MTTF_d$, DC, CCF and the measures taken against systematic failure, including software, has already been considered. In the quantification with SISTEMA, only the PL and PFH need be entered (refer also to SISTEMA Cookbook Volume 1, Section 4.5).

Table B.1 can be used to select a specific example circuit in which a particular safety function has been implemented in a particular PL.

Table B.1:
Overview of the example circuits

Keyword	Circuit example with		
	PL c	PL d	PL e
Guard door monitoring, STO	1, 2	3, 6, 7, 8, 9, 10	12
Park position monitoring	1, 2		
SLS		4, 8, 9	
Enabling control	8	4, 9	
Emergency stop		5, 11	
SS1		5, 9, 10	
Guard locking		7, 11	
Operating mode selection		8, 9	
Manual reset		10	
Safe motion control		11	
Power-operated door		13	
Holding up vertical axis	14 (power failure)	14	
DC-drive, STO		15	

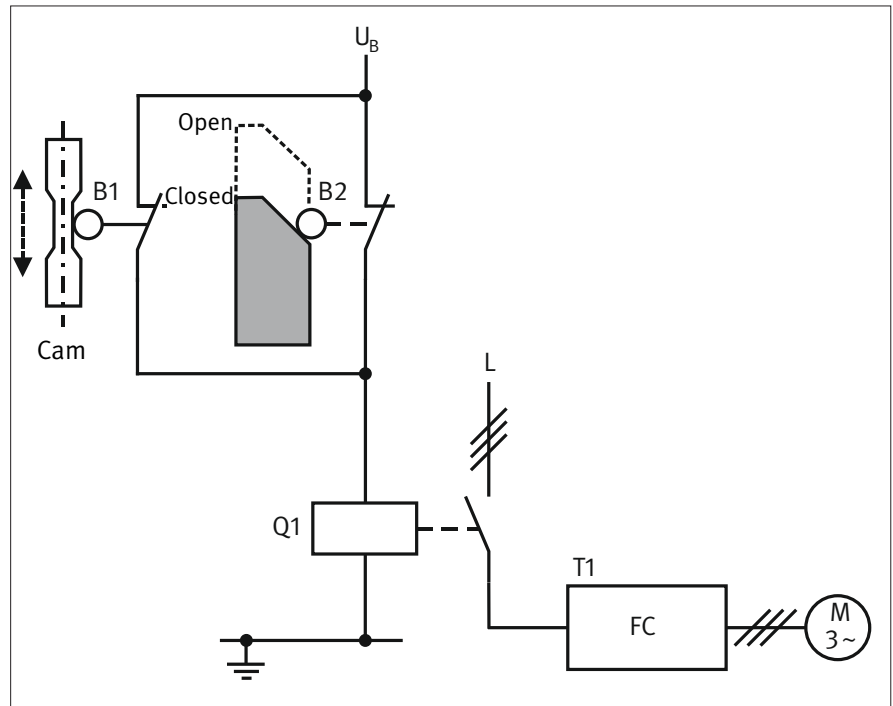
Example 1: Stopping when the safe park position of an axis is left when the safety guard is open – PL c


Figure B.1:
Combined position monitoring of a safety guard
and position monitoring of an axis with the aid
of a cam switch

Safety function

- SF1: Should the axis leave the safe park position whilst the safety guard is open, or should the safety guard be opened whilst the axis is in an unsafe position, the motor torque is switched off (STO).

Function description

- Before a manual intervention, the drive axis is moved to a safe park position in which the position switch B1 is not actuated. When closed, the break contact of B1 shunts the position switch B2, which monitors the position of the safety guard.
- Should the drive incorrectly start up, B1 is actuated and the shunt of B2 is removed. If the safety guard is open, dropping out of the mains contactor Q1 causes an uncontrolled stop (Stop Category 0 to EN 60204-1).
- An uncontrolled stop also occurs if the safety guard is opened whilst the axis is located outside the safe park position.

Design features

- Fundamental and well-tried safety principles and the requirements of Category B are observed. Protective circuits (such as contact fuse protection), as described in the first sections of Chapter 8 of BGIA Report 2/2008e, are provided. The present example includes, for example, the essential safety principles of the closed-circuit current principle and earthing of the control circuit. Well-tried safety principles include overdimensioning of the contacts of B1, B2 and Q1.
- Cross-circuits and short-circuits in electrical supply lines must be considered in accordance with EN ISO 13849-2, Table D.4.
- The actuating mechanism of the electromechanical position switches B1 and B2 must be designed and fitted as specified. The position switches are well-tried components to EN ISO 13849-2, Table D.3 with direct opening contacts in accordance with EN 60947-5-1, Annex K. The position switches and their actuating elements must be secured against displacement. Only rigid mechanical components (not spring elements) may be used.
- The contactor Q1 is a well-tried component and satisfies the requirements of EN 60947-4-1.

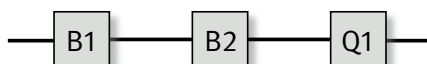


Figure B.2:
Safety-related block diagram for Example 1

- The frequency converter T1 is a standard commercial product without integrated safety functions. Should the power supply to the frequency converter be interrupted, the motor is not able to generate torque.

Comments:

- Where areas can be accessed from the rear, an additional acknowledgement facility must be provided that is actuated when the hazardous zone has been vacated and the safety guard closed. The hazardous zone must be visible from the acknowledgement point.
- A zero-speed relay satisfying at least PL c can be employed as an alternative to B1.
- Should B1 not be used, the frequency converter T1 is disconnected from the system directly when the safety guard is opened (safe torque off, STO).
- The time characteristic for stopping in the case of STO (coasting to a halt) must not give rise to hazards.

Calculation of the probability of failure

- For B1 and B2, fault exclusion is possible for the direct opening electrical contact. A B_{10d} value of 1,000,000 switching cycles [M] is stated for the mechanical part of B1/B2. At 365 working days, 16 working hours per day and a cycle time of 10 minutes, $n_{op} = 35,040$ cycles per year and $MTTF_d = 285$ years for these components.
- For the contactor Q1, the B_{10} value corresponds to 1,300,000 switching cycles [M] under inductive load (AC 3). With 50% of failures assumed to be dangerous, the B_{10d} value is attained by doubling of the B_{10} value. With the above assumed value for n_{op} , the result is an $MTTF_d$ of 742 years for Q1.
- DC_{avg} and measures against common-cause failure are not relevant in Category 1.
- For safety function SF 1 the evaluation is as follows: the control system satisfies Category 1 with a high $MTTF_d$ (100 years). The resulting average probability of dangerous failure is thus $PFH = 1.14 \cdot 10^{-6}$ per hour. This satisfies PL c.

Example 2: Stopping when the safe park position is left with the safety guard open – PL c

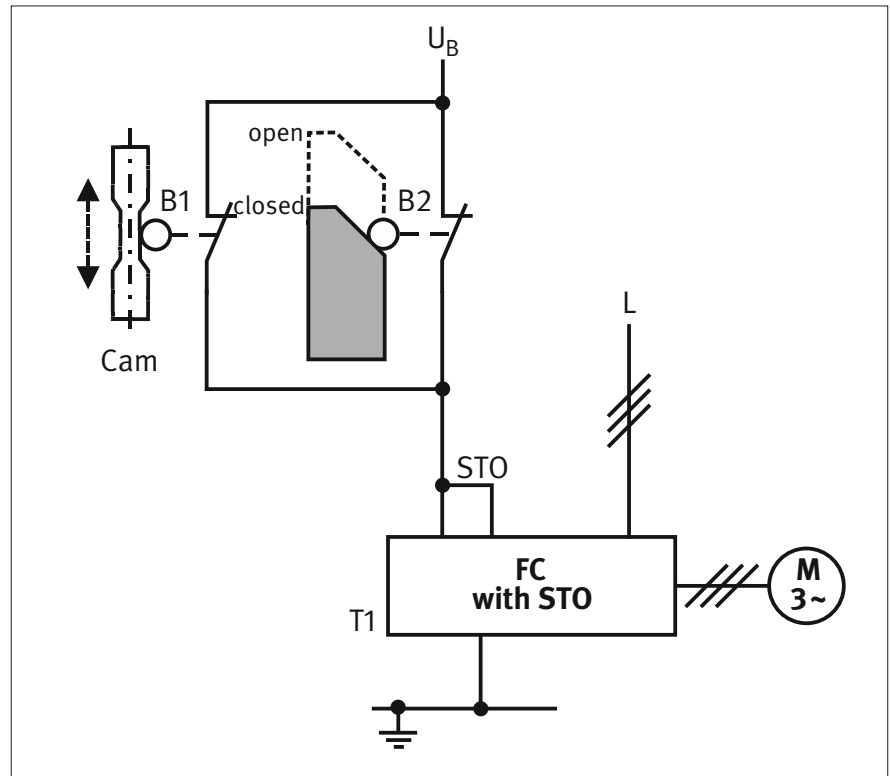


Figure B.3:
Combined position monitoring of a safety guard
and position monitoring of an axis with the aid
of a cam switch

Safety function

- SF1: Should the axis leave the safe park position whilst the safety guard is open, or should the safety guard be opened whilst the axis is in an unsafe position, the motor torque is switched off (STO).

Function description

- Before a manual intervention, the drive axis is moved to a safe park position in which the position switch B1 is not actuated. When closed, the break contact of B1 shunts the position switch B2, which monitors the position of the safety guard.
- Should the drive incorrectly start up, B1 is actuated and the shunt of B2 is removed. If the safety guard is open, activation of STO in the frequency converter T1 causes an uncontrolled stop (Stop Category 0 to EN 60204-1).
- An uncontrolled stop also occurs if the safety guard is opened whilst the axis is located outside the safe park position.

Design features

- Fundamental and well-tried safety principles and the requirements of Category B are observed. Protective circuits (such as contact fuse protection), as described in the first sections of Chapter 8 of BGIA Report 2/2008e, are provided. The present example includes, for example, the essential safety principles of the closed-circuit current principle and earthing of the control circuit. The well-tried safety principle includes overdimensioning of the contacts of B1 and B2.
- Cross-circuits and short-circuits in electrical supply lines must be considered in accordance with EN ISO 13849-2, Table D.4.
- The actuating mechanism of the electromechanical position switches B1 and B2 must be designed and fitted as specified. The position switches are well-tried components to EN ISO 13849-2, Table D.3 with direct opening contact in accordance with

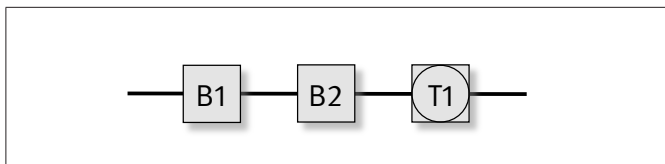


Figure B.4:
Safety-related block diagram for Example 2

EN 60947-5-1, Annex K. The position switches and their actuating elements must be secured against displacement. Only rigid mechanical components (not spring elements) may be used.

- The frequency converter T1 possesses the integral STO safety function.

Comments:

- Where areas can be accessed from the rear, an additional acknowledgement facility must be provided that is actuated when the hazardous zone has been vacated and the safety guard closed. The hazardous zone must be visible from the acknowledgement point.
- A zero-speed relay satisfying at least PL c can be employed as an alternative to B1.
- Should B1 not be used, the STO safety function is activated in the frequency converter T1 when the safety guard is opened.
- The time characteristic for stopping in the case of STO (coasting to a halt) must not give rise to hazards.

Calculation of the probability of failure

- For B1 and B2, fault exclusion is possible for the direct opening electrical contact. A B_{10d} value of 1,000,000 switching cycles [M] is stated for the mechanical part of B1/B2. At 365 working days, 16 working hours per day and a cycle time of 10 minutes, $n_{op} = 35,040$ cycles per year and $MTTF_d = 285$ years for these components.
- DC_{avg} and measures against common-cause failure are not relevant in Category 1.
- The manufacturer states Category 3, PL d and a PFH of $3.16 \cdot 10^{-7}$ per hour for the frequency converter T1.
- For safety function SF 1 the evaluation is as follows: the combination of the subsystems yields an average probability of dangerous failure of $PFH = 1.14 \cdot 10^{-6}$ per hour + $3.16 \cdot 10^{-7}$ per hour = $1.46 \cdot 10^{-6}$ per hour. This satisfies PL c.

Example 3: Opening of a movable guard leads to STO of the drive – PL d

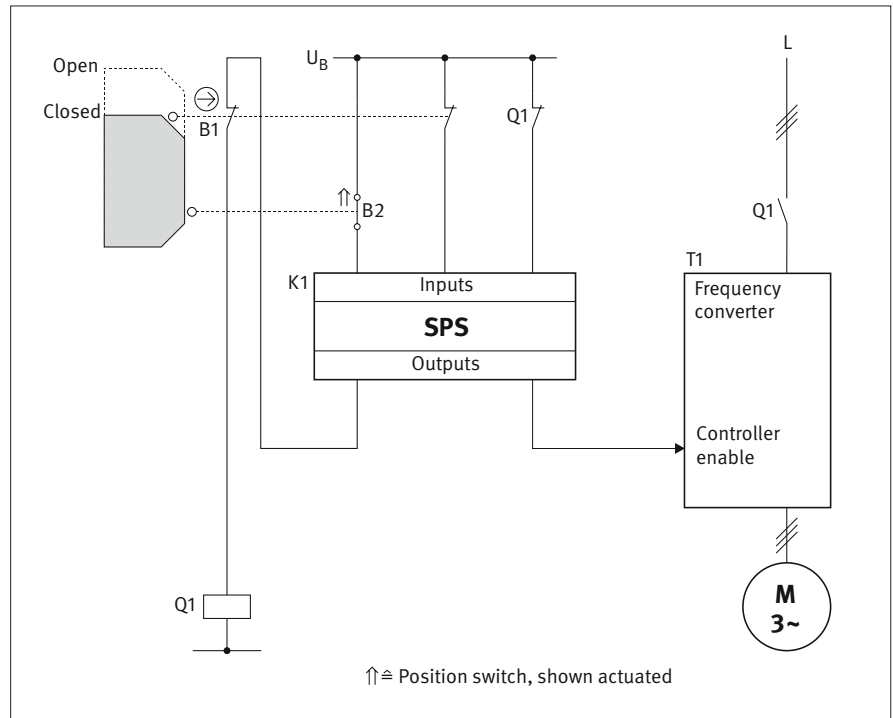


Figure B.5:
Schematic circuit diagram of position monitoring

Safety function

- SF1: Opening of the safeguard leads to STO of the frequency converter drive.

Function description

- When the safeguard is opened, B1 interrupts the control circuit of the mains contactor Q1, causing Q1 to drop out.
- The PLC K1 monitors the switching position of B2; when the contact is opened, K1 switches off the servo enable of the frequency converter T1.
- The PLC K1 also compares the signals of B1 and B2 and monitors the signalling contact of Q1. In the event of a fault, further operation is prevented by cancellation of the servo enable of the frequency converter T1.
- The servo enable in this example has no feedback signal that can be used for fault detection. Fault detection is possible by way of the technical process where motor movements are enabled solely via the servo enable and a fault becomes evident from a malfunction in machine behaviour. Alternatively, faults can be detected by an additional test cycle (refer in this context to Section 6.1.1.2, “Fault detection of the servo enable”).
- Faults in the PLC are also detected by way of the technical process.

Design features

- Fundamental and well-tried safety principles and the requirements of Category B are observed. Protective circuits (such as contact fuse protection, earthing of the control circuit), as described in the first sections of Chapter 8 of BGIA Report 2/2008e, are present.
- Cross-circuits and short-circuits in electrical supply lines must be considered in accordance with EN 13849-2, Table D.4. Faults are detected as they occur, and a safe state is brought about. Alternatively, the conductors must be laid such that fault exclusion is possible for cross-circuits and short-circuits.

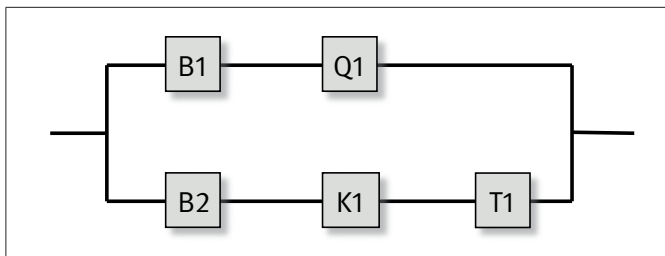


Figure B.6:
Safety-related blockdiagram for Example 3

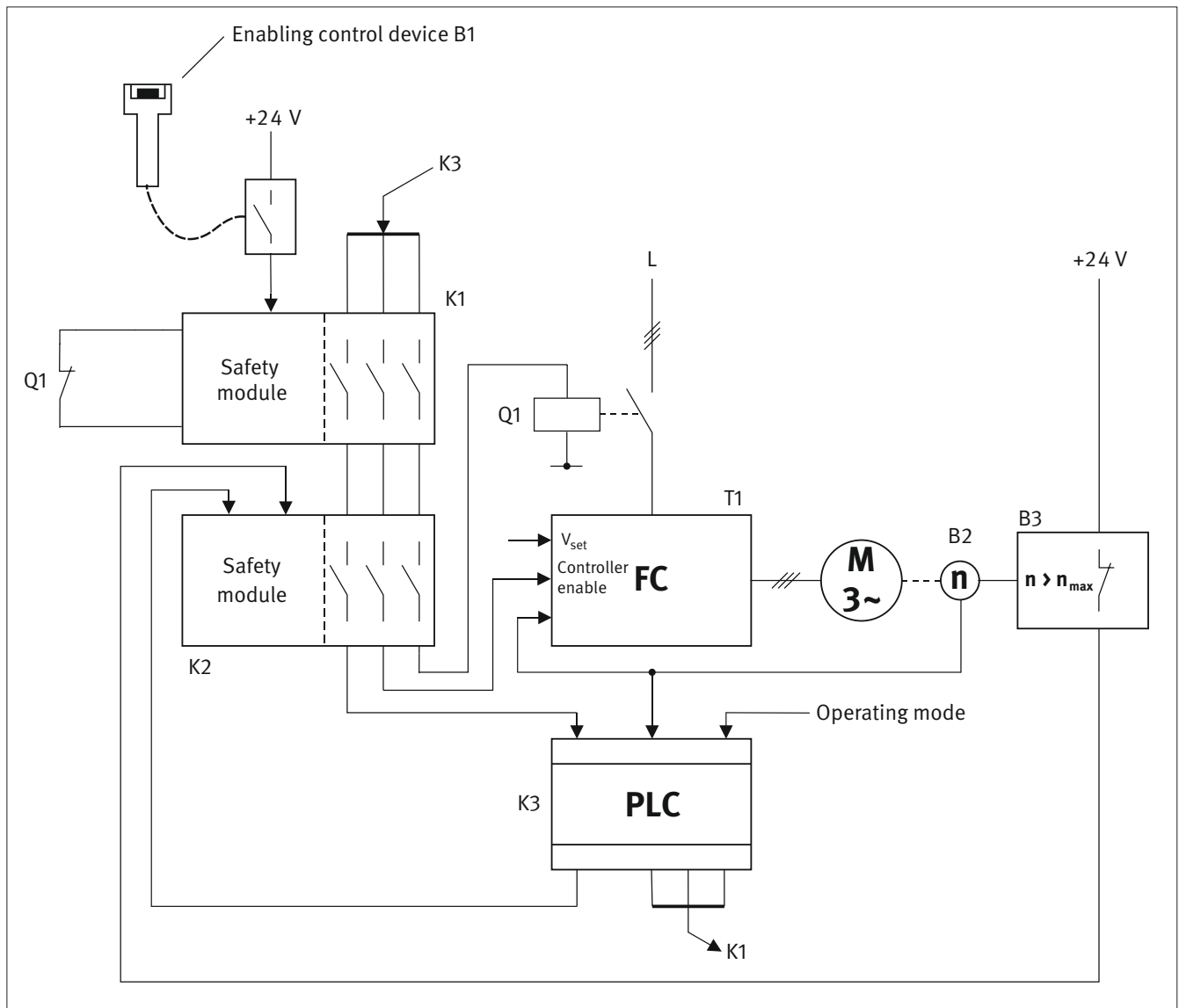
- The actuating mechanisms of the electromechanical position switches B1 and B2 must be designed and fitted as specified. Actuating elements and position switches must be secured against displacement. Only rigid mechanical components (not spring elements) may be used. The position switch B1 is a well-tried component to EN ISO 13849-2, Table D.3 with direct opening contact in accordance with EN 60947-5-1, Annex K.
- The mains contactor Q1 possesses a mirror contact in accordance with EN 60947-4-1, Annex F. Reading back of this auxiliary contact from Q1 provides information on the switching position of the main contacts of the contactor.
- The frequency converter T1 is a standard product without integrated safety functions.
- The standard components K1 (PLC) and T1 (frequency converter) are used in accordance with the information in Section 6.3.10 (requirements concerning SRESW) of BGIA Report 2/2008e.
- The application software (SRASW) is programmed in accordance with the requirements for PL b (downgraded owing to diversity) and the information in Section 6.3 of BGIA Report 2/2008e.

Calculation of the probability of failure

- For B1, fault exclusion is possible for the direct opening electrical contact.
- A B_{10d} value of 1,000,000 switching cycles [M] is stated for the electrical make contact of position switch B2. At 240 working days, 16 working hours per day and a cycle time of 30 minutes, the result is an n_{op} of 7,680 cycles per year and an $MTTF_d$ of 1,302 years.
- A B_{10d} value of 1,000,000 switching cycles [M] is stated for the mechanical part of position switches B1 and B2. An n_{op} of 7,680 cycles per year yields an $MTTF_d$ of 1,302 years.
- A B_{10d} value of 400,000 switching cycles [M] is stated for the mains contactor Q1. An n_{op} of 7,680 yields an $MTTF_d$ of 521 years.
- An $MTTF_d$ of 30 years [M] is stated both for the PLC K1 and for the frequency converter T1.
- DC = 99% for B1 and B2 is based upon the plausibility monitoring of the two switching states in the PLC K1.
- A DC value of 99% can be stated for the mains contactor Q1, since the mirror contact is constantly monitored directly in the PLC.
- A DC of 60% (fault detection by way of the technical process) is stated for the PLC K1 and for the servo enable in the frequency converter T1.
- Adequate measures against common-cause failure are taken (80 points): separation (15), different technologies (20), use of well-tried components (5), overvoltage protection etc. (15) and protection against environmental conditions (25).
- For safety function SF 1 the result is an average probability of dangerous failure of $1.78 \cdot 10^{-7}$ per hour. This satisfies PL d.

Example 4: Setup mode with limited speed and enabling control – PL d

Figure B.7:
Setup mode with limited speed and enabling control – cascading of safety modules



Safety functions

- SF 1: Safely limited speed (SLS) in setup mode; overspeed leads to STO of the drive.
- SF 2: STO is triggered when the enabling switch is released.

Function description

- This part of the control system implements the "safely limited speed" (SLS) safety function in the "setup" operating mode. Overspeed leads to uncontrolled stopping by means of STO.
- In this operating mode, drive movements are permitted by actuation of the enabling switch B1. They are prevented when B1 is not actuated or is fully depressed in switch position 3. The signals from the enabling switch B1 act upon the safety module K1.
- For the sake of clarity, selection of the operating mode is not shown.

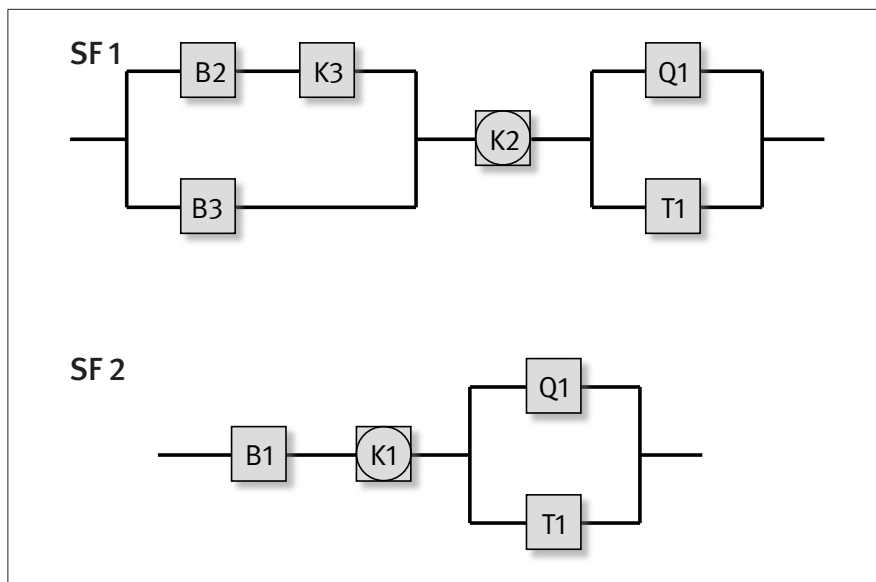


Figure B.8:
Safety-related block diagrams for Example 4

- Speed monitoring employs a two-channel arrangement. In one channel, the signal is processed by means of the rotary encoder B2 and the PLC K3. The second channel is implemented by means of the tachometric relay B3. The outputs of the two channels act upon the safety module K2.
- The safety-related signals from the enabling control and the speed monitor are cascaded through the safety modules K1 and K2. Opening of the enabling paths of a safety module leads to the drive being switched off by STO.
- The STO arrangement is two-channel in form, by blocking of the servo enable of the frequency converter T1 and interruption of the mains supply by means of the mains contactor Q1.
- Further protective equipment and control devices can be integrated by cascading of the safety modules in order to trigger the STO safety function.

Design features

- Fundamental and well-tried safety principles and the requirements of Category B are observed. Protective circuits (such as contact fuse protection, earthing), as described in the first sections of Chapter 8 of BGIA Report 2/2008e, are present.
- Cross-circuits and short-circuits in electrical supply lines must be considered in accordance with EN ISO 13849-2, Table D.4. Faults are detected as they occur, and a safe state is brought about. Alternatively, the conductors must be laid such that fault exclusion is possible for cross-circuits and short-circuits.
- The mains contactor Q1 possesses a mirror contact in accordance with EN 60947-4-1, Annex F. Reading back of this auxiliary contact provides information on the switching position of the main contacts of the contactor Q1.
- The frequency converter T1 and the PLC K3 are standard items of equipment without integrated safety functions. They are used in accordance with the information in Section 6.3.10 (requirements concerning SRESW) of BGIA Report 2/2008e.
- The application software (SRASW) is programmed in accordance with the requirements for PL b (downgraded owing to diversity) and the information in Section 6.3 of BGIA Report 2/2008e.
- The speed detection arrangement employs diversity. B2 is a sin/cos encoder connected to the PLC K3. B3 is a tachometric relay with integral switching contact. The rotary encoder and the tachometric relay must be fitted in such a way that a single fault (e.g. encoder shaft breakage) is not able to cause simultaneous failure of both components.
- The stopping time (overrun time) with STO following a violation of the speed limit value at maximum possible acceleration must not give rise to any hazard.

- The enabling device B1 is of three-stage design. It possesses a make contact and a positive-opening contact (opening in switch position 3).

Note:

The enabling control and the safely limited speed in conjunction with the operating mode selector switch etc. are specified controls in accordance with the Machinery Directive, 2006/42/EC Annex 1, Section 1.2.5.

Calculation of the probability of failure

- The safety modules K1 and K2 satisfy the requirements for Category 3, PL d and SIL 2. The PFH of each safety module is $2.31 \cdot 10^{-9}$ per hour [M].
- An $MTTF_d$ of 132 years [M] is stated for the rotary encoder B2.
- The manufacturer states an $MTTF_d$ of 60 years [M] for the tachometric relay B3.
- The contactor Q1 has a B_{10d} value of $1 \cdot 10^6$ switching cycles [M]. At 250 working days, 16 working hours per day and a cycle time of 60 minutes, this yields an n_{op} of 4,000 cycles per year and an $MTTF_d$ of 2,500 years.
- An $MTTF_d$ of 30 years is assumed for the standard PLC K3 [A].
- The frequency converter T1 does not possess integral safety functions. Since no manufacturers' information is available on the $MTTF_d$, it is estimated conservatively at ten years for the purpose of calculation [S] (see EN ISO 13849-1, Section 4.5.2).
- The three-stage enabling switch B1 is manufactured in accordance with the IEC 60947-5-8 product standard, and its number of operating cycles is below 100,000. In accordance with BGIA Report 2/2008e, Table D.2, fault exclusion is permissible for a failure to open of the break contact (fully depressing to the third stage) and the make contact (transition from the second stage to the first stage in response to release) for a number of operating cycles $< 100,000$.
- The DC for the rotary encoder B2 is assumed to be 60%, since the encoder is also required for functional control of the machine and is therefore tested by way of the technical process.
- A DC of 99% can be stated for the contactor Q1, since the mirror contact is read back by the safety module K1 (direct monitoring).
- The tachometric relay B3 is tested once a year for proper operation during the regular test of the machine. Here too, a DC of 60% is assumed. In accordance with the Co-ordination of Notified Bodies, Machinery Directive 2006/42/EC + Amendment, Recommendation for use CNB/M/11.050_R_E [1], a test interval of no more than twelve months is specified for automatic or manual functional tests for the detection of faults for safety functions in Category 3, PL d.
- Owing to the fault detection by way of the technical process, the DC for the PLC K3 is set at 60%. The DC for the frequency converter T1 is estimated at 60%, since functional stopping of the motor occurs solely by cancellation of the servo enable and a fault is detected by way of the technical process.
- DC is not applied for the enabling switch, since no faults need be assumed owing to the fault exclusion.
- Adequate measures against common-cause failures are taken for the B2/B3/K3 subsystem (80 points): separation (15), different technologies (20), protection against overvoltage etc. (15), failure mode and effects analysis (5) and protection against environmental influences (25).
- Adequate measures against common-cause failures are taken for the Q1/T1 subsystem (90 points): separation (15), different technologies (20), protection against overvoltage etc. (15), failure mode and effects analysis (5) and protection against environmental influences (25 + 10).
- The evaluation for the safety function SF 1, "Safely limited speed (SLS) in setup mode; overspeed leads to STO of the drive", yields the following result: the subsystems of speed detection and interpretation (B2, B3, K3) and shutdown paths (Q1, T1) satisfy Category 3 and PL d. In combination with the encapsulated subsystem of the safety module K2, the result is an average probability of dangerous failure of $5.51 \cdot 10^{-7}$ per hour for SF 1. This satisfies PL d.

- The evaluation for the safety function SF 2, “STO is triggered when the enabling switch is released”, yields the following result: the combination of the enabling switch (B1), safety module (K1) and shutdown paths (Q1, T1) subsystems yields an average probability of dangerous failure of $1.89 \cdot 10^{-7}$ per hour. This satisfies PL d.

Reference:

- [1] Co-ordination of Notified Bodies, Machinery Directive 2006/42/EC + Amendment, Recommendation for use CNB/M/11.050_R_E. http://ec.europa.eu/enterprise/sectors/mechanical/files/machinery/vertical-rfu_en.pdf

Example 5: Stopping in an emergency – PL d

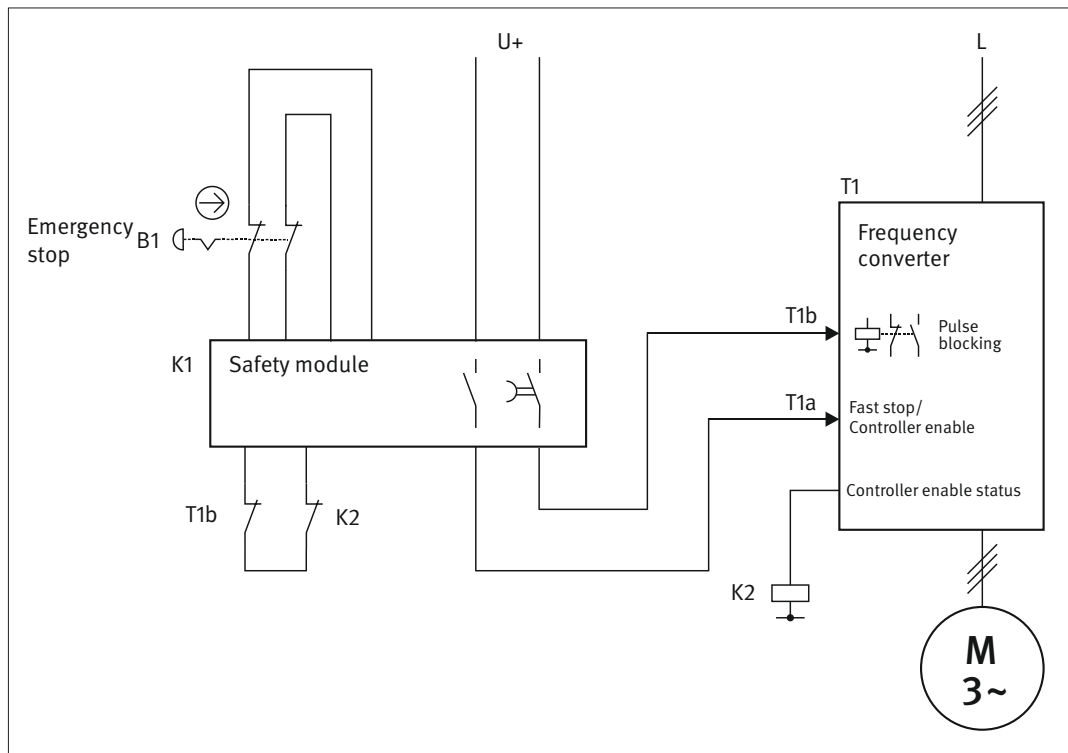


Figure B.9:
Schematic circuit
diagram of the drive
control

Safety function

- SF1: Fastest possible stopping in the event of an emergency-stop (SS1)

Function description

- Hazardous movements are stopped as fast as possible by actuation of the emergency-stop control device B1. The redundant contacts of B1 are interpreted in the safety module K1.
- The instantaneous switching contact of the safety module K1 activates the rapid-stop function in the frequency converter T1 with subsequent cancellation of the servo enable, as a result of which the drive is brought to a halt as quickly as possible. Following a time suitably configured for this application, the pulse block of the frequency converter T1 is activated via the delayed switch contact of K1, and the drive torque is de-activated. The delay in K1 is selected such that the frequency converter has just enough time to shut the drive down in a controlled manner.
- The emergency-stop control device B1 employs redundant contacts; these are monitored together with the wiring by K1. The two shutdown paths in the frequency converter T1 possess feedback signals that are integrated into the enabling circuit of K1 directly/via a coupling device K2. Faults in the frequency converter T1 are thus apparent before the drive is next started.

Design features

- Fundamental and well-tried safety principles and the requirements of Category B are observed. Protective circuits (such as contact fuse protection, earthing), as described in the first sections of Chapter 8 of BGIA Report 2/2008e, are present.
- Cross-circuits and short-circuits in electrical supply lines must be considered in accordance with EN ISO 13849-2, Table D.4. Faults are detected as they occur, and a safe state is brought about. Alternatively, the conductors must be laid such that fault exclusion is possible for cross-circuits and short-circuits.
- The emergency-stop control device B1 satisfies the requirements of EN ISO 13850 and is equipped with direct opening contacts in accordance with EN 60947-5-1, Annex K.

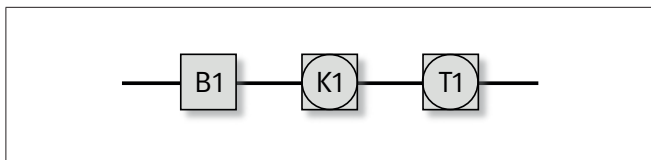


Figure B.10:
Safety-related block diagram for Example 5

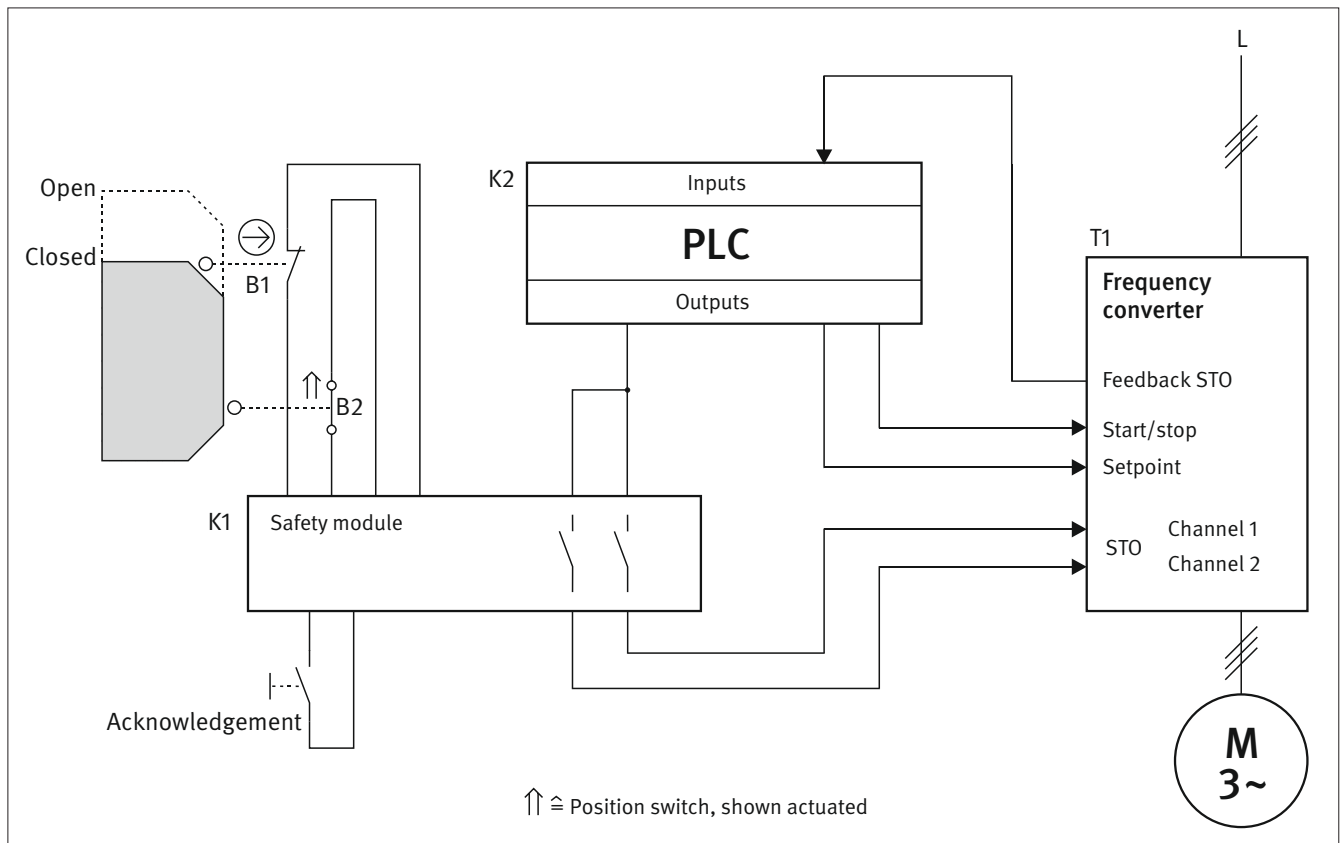
- The safety module K1 possesses instantaneous and delayed enabling paths and satisfies the requirements for Category 3 and PL d.
- T1 is a frequency converter with the integrated STO safety function. The safety function is achieved by a two-channel arrangement through the fast stop/servo enable (T1a) and pulse blocking (T1b) inputs. The SS1 safety function is implemented by combination with a suitable safety module. In this example, the fast-stop function is activated by cancellation of the servo enable.
- Both shutdown paths of T1 are monitored by K1. For the purposes of fault detection, the relay of the pulse block T1b possesses a mechanically linked break contact, and the status of the servo enable T1a is detected by means of the coupling element K2.
- Note that the fast-stop function of the frequency converter T1 is purely functional in its design, i.e. it is not engineered as a safety component. Should a fault in T1 occur and the emergency-stop control device be actuated at the same time, stopping as fast as possible may not take place at all, or braking may occur more slowly. In a worst-case scenario, it is even conceivable that the motor could accelerate and the acceleration not be terminated until pulse blocking is activated following expiration of the delay time in K1, leading to the motor coasting to a halt. The solution described in this example is widely used and can be regarded as the state of the art. Should the described fault behaviour not be acceptable despite the low probability of its occurrence (for example: SS1 in the event of imbalances in sugar centrifuges), a different solution must be engineered, for example involving monitoring of the braking ramp and the additional use of mechanical brakes.

Calculation of the probability of failure

- For the emergency-stop control device B1, fault exclusion for positive-opening contacts and the mechanism is possible in accordance with EN ISO 13849-2, Table D.8, and BGIA Report 2/2008e, Table D.2 up to 6,050 switching operations.
- The safety module K1 satisfies the requirements for Category 3, PL d and SIL 2. The PFH is $3.16 \cdot 10^{-7}$ per hour [M].
- T1 is a frequency converter with integrated STO safety function. It satisfies the requirements for Category 3, PL d and SIL 2. The PFH is $3.16 \cdot 10^{-7}$ per hour [M]. This data for T1 is valid only when the manufacturer's specification for fault recognition by external components is considered and is implemented in accordance with the instruction manual.
- For the safety function SF 1, "Fastest possible stopping in the event of an emergency-stop (SS1)" the result of evaluation is as follows: the combination of the B1, K1 and T1 subsystems yields an average probability of dangerous failure of $6.32 \cdot 10^{-7}$ per hour. This satisfies PL d.

Example 6: Safety-related stop function STO, triggered by a movable guard with position switches – PL d

Figure B.11:
STO of a frequency converter drive

**Safety function**

- SF1: Opening of the movable guard leads to STO of the frequency converter drive.

Function description

- The frequency converter drive is driven functionally by the PLC K2. It specifies the reference value for T1, switches the two STO inputs, and is able to start and stop the drive. The PLC is however not involved in the safety function.
- The hazard point is safeguarded by a movable guard. Opening of the safeguard is detected by the position switches B1 and B2 and evaluated in a safety module K1. The STO inputs are switched off in the frequency converter T1 via the enabling paths of K1, independently of the PLC. Generation of a rotary field is thus reliably prevented in the drive.
- Faults in the position switches B1 and B2 are detected by the plausibility comparison in the safety module K1. The frequency converter T1 is equipped internally with an STO monitoring function. This prevents the drive from restarting in the event of a fault. A corresponding fault signal is transmitted to the PLC K2.

Design features

- Fundamental and well-tried safety principles and the requirements of Category B are observed. Protective circuits (such as contact fuse protection, earthing of the control circuit), as described in the first sections of Chapter 8 of BGIA Report 2/2008e, are present.

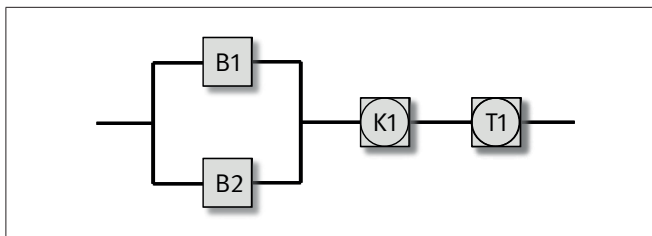


Figure B.12:
Safety-related blockdiagram for Example 6

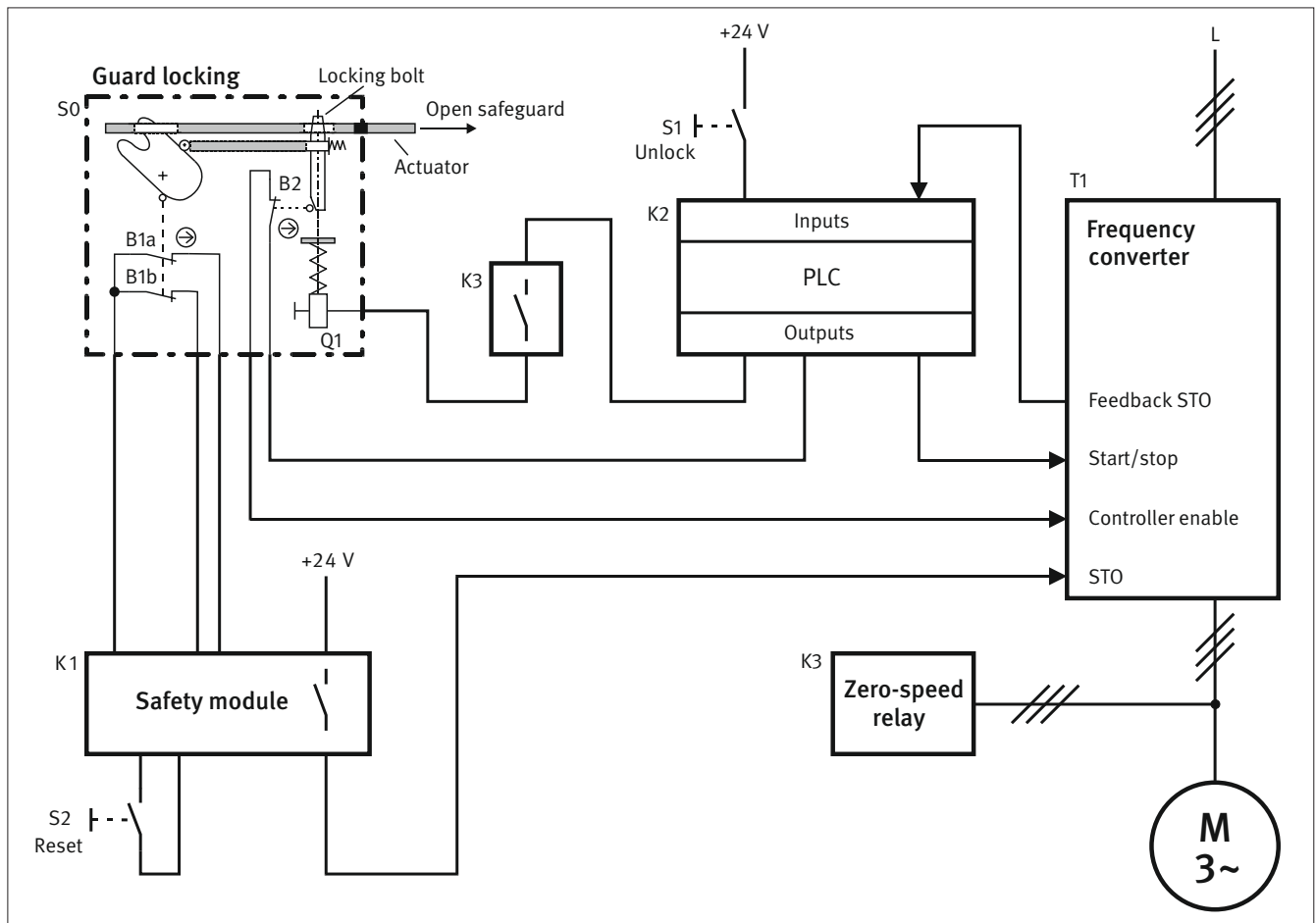
- Cross-circuits and short-circuits in electrical supply lines must be considered in accordance with EN ISO 13849-2, Table D.4. Faults are detected as they occur, and a safe state is brought about. Alternatively, the conductors must be laid such that fault exclusion is possible for cross-circuits and short-circuits.
- The actuating mechanisms of the electromechanical position switches B1 and B2 must be designed and fitted as specified. Actuating elements and position switches must be secured against displacement. Only rigid mechanical components (not spring elements) may be used. The position switch B1 is a well-tried component to EN ISO 13849-2, Table D.3 with direct opening contact in accordance with EN 60947-5-1, Annex K.
- The safety module satisfies the requirements of Category 4 and PL e.
- T1 is a frequency converter with integrated STO safety function. The requirements of Category 3 and PL d are met.

Calculation of the probability of failure

- Fault exclusion applies to the direct opening contact of B1.
- A B_{10d} value of 1,000,000 switching cycles [M] is stated for the electrical make contact of position switch B2. At 240 working days, 16 working hours per day and a cycle time of 60 minutes, the result is an n_{op} of 3,840 cycles per year and an $MTTF_d$ of 2,604 years.
- The same applies to the mechanical parts of the position switches B1 and B2. At a B_{10d} value of 1,000,000 cycles [M] and an n_{op} of 3,840 switching cycles per year, the $MTTF_d$ is 2,604 years for each switch.
- The safety module K1 satisfies the requirements for Category 4 and PL e. The PFH is $2.31 \cdot 10^{-9}$ per hour [M].
- The frequency converter with integral STO safety function satisfies the requirements of Category 3 and PL d. The PFH is $2.0 \cdot 10^{-7}$ per hour [M].
- The DC for the position switches B1 and B2 is 99%, owing to the plausibility check by the safety module K1.
- Adequate measures against common-cause failure are taken for the subsystem of the position switches B1/B2 (70 points): separation (15), use of well-tried components (5), protection against overvoltage etc. (15) and protection against environmental conditions (25 + 10).
- For the safety function the evaluation yields the following result: the B1/B2 subsystem satisfies Category 3 with a high $MTTF_d$ (100 years) and a high DC_{avg} (99%). This yields an average probability of dangerous failure of $2.47 \cdot 10^{-8}$ per hour.
- The combination of the switches B1/B2, safety module K1 and frequency converter T1 subsystems yields an average probability of dangerous failure of $PFH = 2.27 \cdot 10^{-7}$ per hour. This satisfies PL d.

Example 7: Safeguarding of a hazard point by a movable guard with guard locking – PL d

Figure B.13:
Safeguarding of a hazard point by a movable guard with guard locking

**Safety functions**

- SF1: Release of the guard locking only when the drive is stationary
- SF2: STO of the drive when the movable guard with guard locking is opened

Function description

- Access to a hazardous movement is prevented by means of a safety guard with guard locking S0 until the movement has ceased. The guard is held closed by a spring-actuated pin (the locking mechanism) of a solenoid that prevents the actuator being withdrawn from the switch head.
- Access to the hazardous zone is requested by actuation of the pushbutton S1. The standard PLC K2 then first initiates halting of the drive by T1. Once standstill has been reached, the zero-speed relay K3 enables the guard locking solenoids to be actuated by K2, and the guard locking thus to be opened.
- The position of the locking mechanism is monitored. The pin of the solenoid acts upon the position switch B2, which interrupts the servo enable of the frequency converter when actuated.
- Opening of the guard is detected by the two break contacts of the position switch B1 and interpreted in a safety module K1. The STO input in the frequency converter T1 is de-energized via the enabling path of K1, thereby preventing generation of a rotary field. This safety function implements protection against unexpected start-up of the motor.

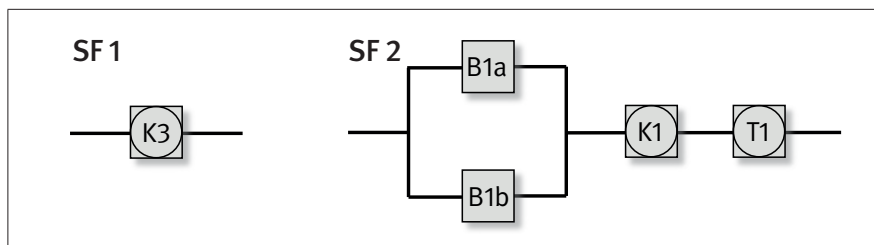


Figure B.14:
Safety-related block diagrams
for Example 7

- The hazardous movement can be restarted only when the guard is closed and guard locking actuated.
- Faults in the position switch B1 are detected by the plausibility comparison in the safety module K1.
- The STO safety function integrated within the frequency converter T1 is single-fault tolerant and does not require external monitoring. Feedback of the STO status to the PLC K2 is for functional purposes only.

Design features

- Fundamental and well-tried safety principles and the requirements of Category B are observed. Protective circuits (such as contact fuse protection, earthing of the control circuit), as described in the first sections of Chapter 8 of BGIA Report 2/2008e, are present.
- Cross-circuits and short-circuits in electrical supply lines must be considered in accordance with EN ISO 13849-2, Table D.4. Faults are detected as they occur, and a safe state is brought about. Alternatively, the conductors must be laid such that fault exclusion is possible for cross-circuits and short-circuits.
- S0 is a position switch with separate actuator (type 2) and integral guard locking. The break contacts B1a and B1b and the monitoring contact B2 for the locking mechanism are direct opening contacts that satisfy the requirements of EN 60947-5-1, Annex K.
- The guard locking device is regarded as a well-tried component and satisfies the requirements of EN 1088 for interlocks. The spring of the guard locking device is a well-tried spring to EN ISO 13849-2, Annex A3. The spring must also be permanently fail-safe to EN 13906-1. The criteria for guard locking employing spring force are set out in the GS-ET-19 test principles, Section 5.5.1. The facility of the guard locking device for prevention of inadvertent closure ensures by design that the locking pin is not able to assume the locked position when the safeguard is open. The locking pin is monitored by a direct opening contact B2. The spring of the guard locking device maintains the locking mechanism in the closed position in the event of a power failure (closed-circuit current principle). A single fault in the guard locking mechanism cannot lead to simultaneous failure of B1 and B2.
- The safety module K1 satisfies the requirements of Category 4 and PL e.
- T1 is a frequency converter with integrated STO safety function. The requirements of Category 3 and PL d are met. Single-channel actuation for STO is sufficient for this product.
- The zero-speed relay K3 satisfies the requirements of Category 3 and PL d.
- K2 is a standard commercial PLC that is not involved in the safety functions.

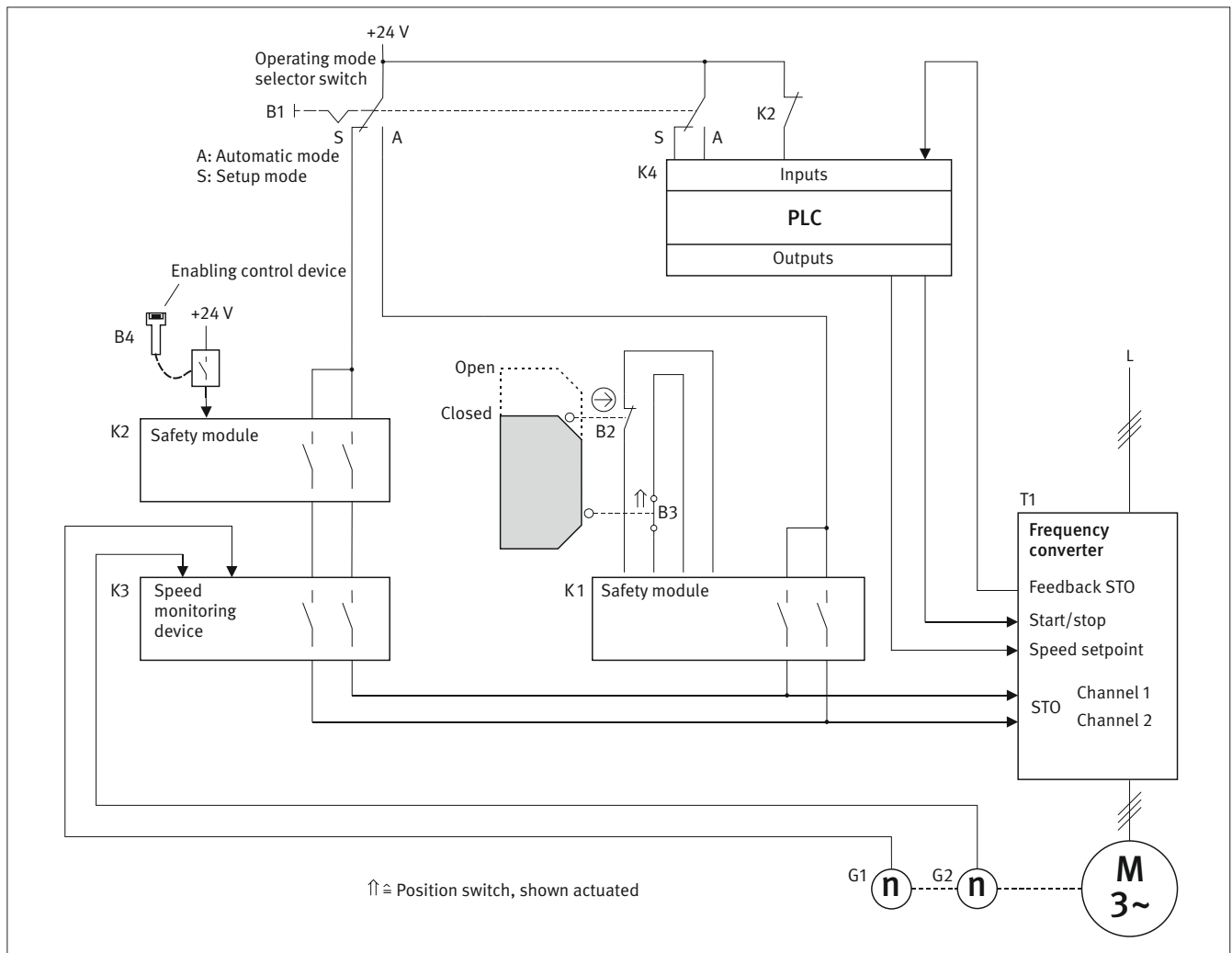
Calculation of the probability of failure

- Fault exclusion may be assumed for the direct opening electrical contacts B1a and B1b
- Fault exclusion can be assumed for the mechanical components of the guard locking device, including mechanical failure of the locking mechanism, when the following conditions are met:
 - use in accordance with the instruction manual, in particular the installation instructions and technical data (e.g. actuating radius, actuating velocity)
 - prevention of working loose
 - the static forces on the guard locking device are lower than the locking force stated on the data sheet

- no dynamic forces arise, since current does not flow through the unlocking solenoid until the safety guard is closed; refer in this context also to the latest edition of DGUV Information 203-003 (formerly BGI 575) and DGUV Information 203-010 (formerly BGI 670) concerning the selection and fitting of interlocking devices (in preparation)
 - the device is not used as a mechanical stop
 - the actuator is mounted such that it cannot be removed
 - regular maintenance
 - positive coupling following assembly
 - adequate mechanical strength of all mounting and functional elements
 - damage that could be caused by foreseeable external influences (such as penetration by dirt and dust, mechanical shock) is prevented by the form of mounting or need not be anticipated owing to the conditions of use.
- The safety module K1 satisfies the requirements for Category 4, PL e and SIL 3. The PFH is $2.98 \cdot 10^{-8}$ per hour [M].
 - T1 is a frequency converter with integral STO safety function. It satisfies the requirements of Category 3, PL d and SIL 2. The PFH is $2.0 \cdot 10^{-7}$ per hour [M].
 - The zero-speed relay K3 satisfies the requirements for Category 3, PL d and SIL 2. The PFH is $2.31 \cdot 10^{-7}$ per hour [M].
 - For the safety function SF 1, “Release of the guard locking only when the drive is stationary”, the evaluation yields the following result: for the speed detection subsystem (K3), the average probability of dangerous failure is $2.31 \cdot 10^{-7}$ per hour. This satisfies PL d.
 - For the safety function SF 2, “STO of the drive when the movable guard with guard locking is opened”, the evaluation yields the following result: the combination of the position switches B1a/B1b, safety module K1 and frequency converter T1 subsystems yields an average probability of dangerous failure of $PFH = 2.3 \cdot 10^{-7}$ per hour. This satisfies PL d.

Example 8: Drive control for automatic and setup mode with limited speed and enabling switch

Figure B.15:
Automatic and setup mode of a drive control



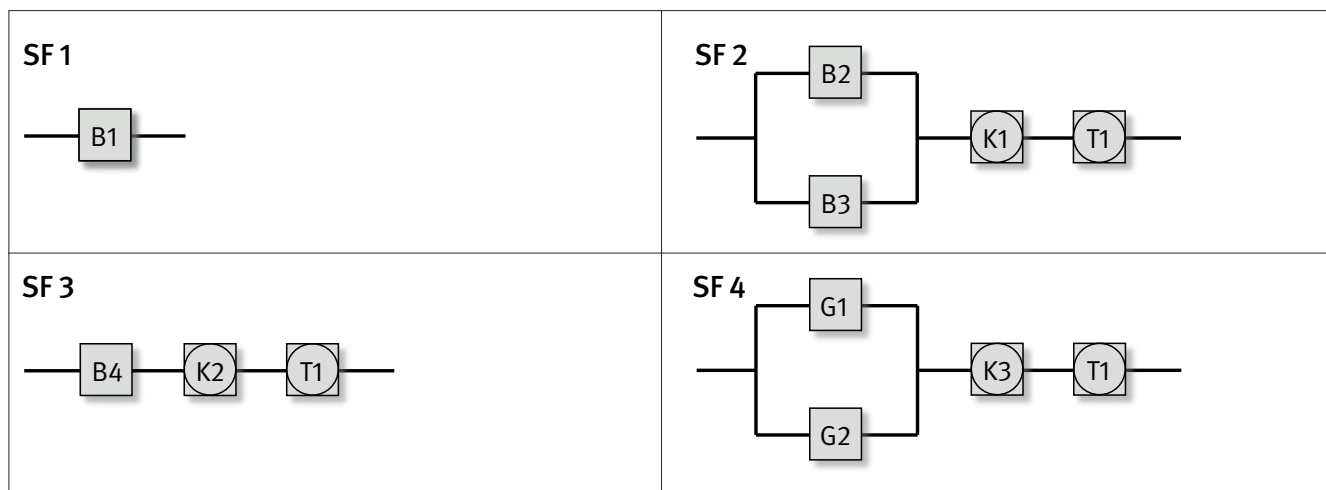
Safety functions

- SF 1: operating mode selection
- SF 2: automatic mode; opening of the movable guard brings the drive to a halt (STO)
- SF 3: setup mode; release of the enabling switch on the hand-held terminal brings the drive to a halt (STO)
- SF 4: setup mode; exceeding of the maximum permissible speed leads to the drive being brought to a halt (SLS)

Function description

- The operating mode selector switch B1 permits selection between automatic and setup modes. In automatic mode, the contacts of the position switches B2/B3 on the guard are closed, and the drive can be operated at any speed. Opening of the guard is detected via B2/B3 and the safety module K1, and leads to activation of the STO safety function in the frequency converter T1.
- Automatic control is blocked in setup mode. Operation whilst the guard is open is possible only at limited speed and by actuation of the enabling switch B4. The movement is initiated by a separate control device on a hand-held terminal (not shown).

Figure B.16:
Safety-related block diagrams for Example 8



- When the enabling switch B4 is released, the hazardous movement is brought to a halt via the safety module K2 by de-energization of the STO inputs of the frequency converter T1.
- The speed is monitored in setup mode by a monitoring device K3 (Category 3, PL d). For monitoring of the speed, two encoders or alternatively one encoder and the speed signal from the frequency converter are used. When the maximum speed set in the monitoring device is exceeded, the output relays drop out and the STO function of the frequency converter is activated.
- Faults in the position switches B2 and B3 are detected by the plausibility comparison in the safety module K1. The frequency converter T1 is equipped internally with an STO monitoring function. This prevents the drive from restarting in the event of a fault. A corresponding fault signal is transmitted to the PLC K4.
- Speed monitoring employs a two-channel arrangement. Faults in the encoder signals are detected by the plausibility comparison in the speed monitor K3.

Design features

- Fundamental and well-tried safety principles and the requirements of Category B are observed. Protective circuits (such as contact fuse protection, circuit earthing), as described in the first sections of Chapter 8 of BGIA Report 2/2008e, are present.
- Cross-circuits and short-circuits in electrical supply lines must be considered in accordance with EN ISO 13849-2, Table D.4. Faults are detected as they occur, and a safe state is brought about. Alternatively, the conductors must be laid such that fault exclusion is possible for cross-circuits and short-circuits.
- The operating mode selector switch B1 is a cam-operated selector switch with positive actuation. The design of the operating mode selector switch permits fault exclusions in accordance with EN ISO 13849-2, Table D.8.
- The actuating mechanisms of the electromechanical position switches B2 and B3 must be designed and fitted as specified. Actuating elements and position switches must be secured against displacement. Only rigid mechanical components (not spring elements) may be used. The position switch B2 is a well-tried component to EN ISO 13849-2 with direct opening contact in accordance with EN 60947-5-1, Annex K.
- The enabling control device B4 is a two-stage enabling switch with a single make contact. The enabling switch B4 satisfies the requirements of EN 60204-1, Section 10.9.
- The safety modules K1 and K2 satisfy the requirements of Category 4 and PL e.
- The speed monitor K3 satisfies the requirements of Category 3 and PL d.

- T1 is a frequency converter with integrated STO safety function. The requirements of Category 3 and PL d are met.
- K4 is a standard commercial programmable logic controller that is not involved in the safety functions.

Comments:

- The stopping time (overrun time) of the STO safety function triggered by a violation of the speed limit value at maximum possible acceleration must not give rise to any hazard. The same applies to overrun following opening of the safety guard.
- In the event of a fault in the enabling switch, spring-operated opening of the make contact when the switch is released may fail. The hand-held terminal must therefore feature a control device for stopping in the event of an emergency.
- The two rotary encoders must be fitted in such a way that simultaneous failure of both as a result of a single fault (e.g. encoder shaft breakage) is excluded.

Calculation of the probability of failure

- The operating mode selector switch B1 is a cam-operated selector switch with positive actuation (direct opening) in accordance with EN 60947-5-1, Annex K. Faults are excluded for the direct opening contacts

Faults are further excluded for short-circuiting of contacts that are mutually isolated.

In addition, faults are excluded for different positions of the two changeover contact levels.

Owing to the implemented control architecture and installation in a switching cabinet with a minimum ingress protection of IP 54, faults such as short-circuits between adjacent conductor paths, contact points and conductors can be excluded. The conditions for fault exclusion to EN ISO 13849-2, Section D.5 are met. Faults in the operating mode selection arrangement cannot lead to dangerous failure of a safety function. Any interruption in the path of the active operating mode leads to triggering of the safe state (STO), owing to consistent application of the closed-circuit current principle.

- Fault exclusion applies to the direct opening contact of B2.
- A B_{10d} value of 1,000,000 switching cycles [M] is stated for the electrical make contact of position switch B3. At 240 working days, 16 working hours per day and a cycle time of 60 minutes, the result is an n_{op} of 3,840 cycles per year and an $MTTF_d$ of 2,604 years.
- The same applies to the mechanical part of each position switch B2 and B3. At a B_{10d} value of 1,000,000 switching cycles [M] and an n_{op} of 3,840 cycles per year, the $MTTF_d$ is 2,604 years.
- The safety modules K1 and K2 satisfy the requirements for Category 4 and PL e. The PFH is $2.31 \cdot 10^{-9}$ per hour [M].
- The frequency converter with integral STO safety function satisfies the requirements of Category 3 and PL d. The PFH is $2.0 \cdot 10^{-7}$ per hour [M].
- The two-stage enabling switch B4 features a make contact. The manufacturer states a B_{10d} value of $1 \cdot 10^5$ switching cycles for both the mechanical and the electrical components. At $n = 3,840$ cycles per year, the $MTTF_d$ is 260 years in each case.
- The speed monitor K3 is a safety module that satisfies the requirements of Category 3 and PL d. The PFH is $2 \cdot 10^{-7}$ per hour [M].
- The rotary encoders G1 and G2 are flanged to the left and right-hand sides of the motor. The encoder manufacturer states an $MTTF_d$ of 40 years for each encoder with assumption of fault exclusion for shaft breakage.
- The DC for the position switches B2 and B3 is 99%, owing to the plausibility check by the safety module K1.
- The DC for the rotary encoders G1 and G2 is estimated at 99%, owing to the cross-check of the signals by the speed monitor K3.
- Adequate measures against common-cause failure are taken for the subsystem of the position switches B2/B3 (70 points): separation (15), use of well-tries components (5), protection against overvoltage etc. (15) and protection against environmental conditions (25 + 10).

- Adequate measures against common-cause failure are taken for the subsystem of rotary encoders G1/G2 (65 points): separation (15), protection against overvoltage etc. (15) and protection against environmental conditions (25 + 10).
- The evaluation of the safety function SF 1, “Operating mode selection” ,yields the following result: the formulation of fault exclusion based upon the design characteristics enables the separation of automatic, setup and function control modes to be classified in PL d. The restriction to PL d is due to the fact that PL e must not be based solely upon fault exclusion (see EN ISO 13849-2, Table D.8).
- For the safety function SF 2, “Automatic mode; opening of the movable guard brings the drive to a halt (STO)”, the evaluation yields the following result: the B2/B3 subsystem satisfies Category 3 with a high $MTTF_d$ (100 years) and a high DC_{avg} (99%). This results in an average probability of dangerous failure of $2.47 \cdot 10^{-8}$ per hour.

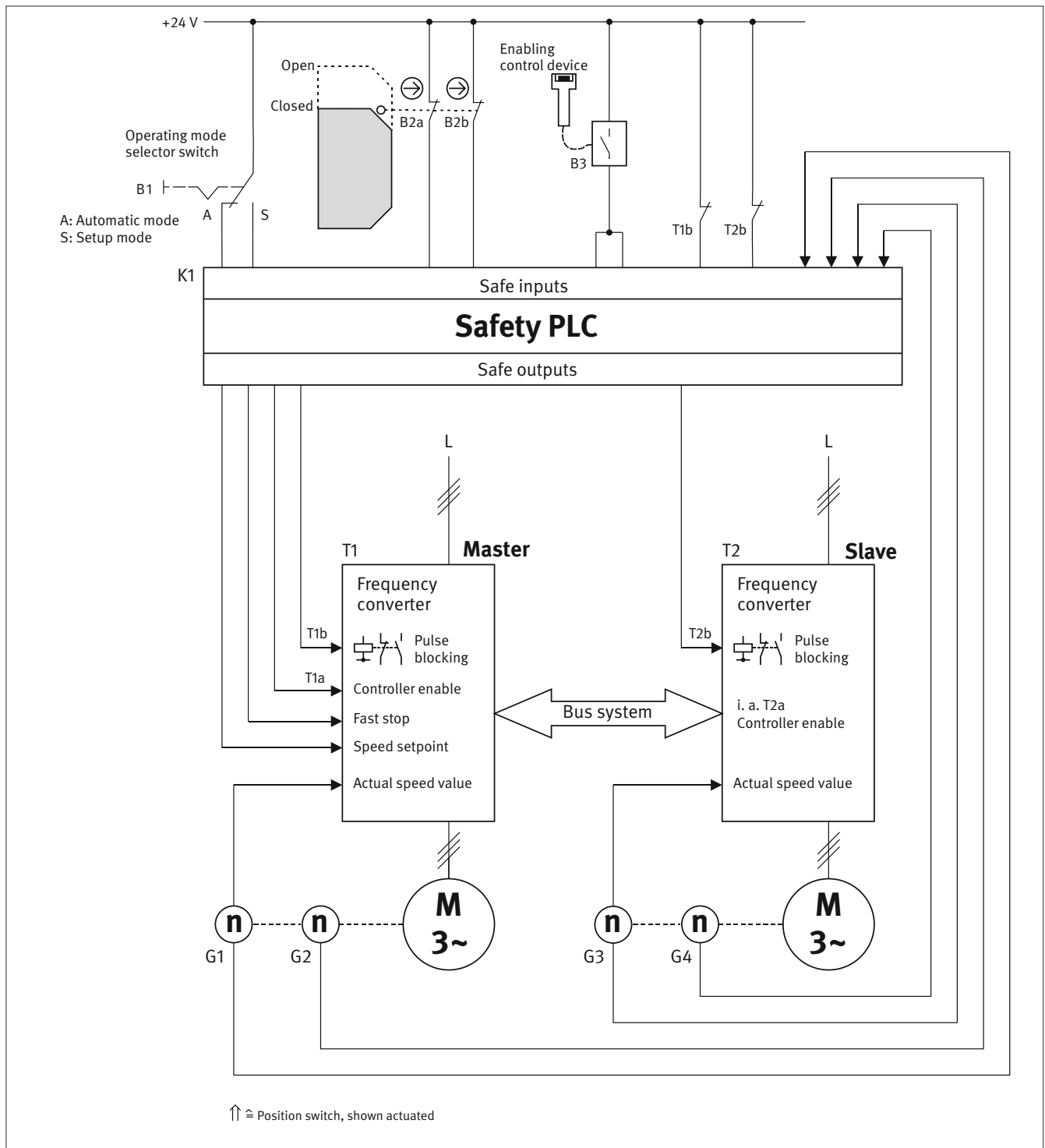
The combination of the position switches B1/B2, safety module K1 and frequency converter T1 subsystems yields an average probability of dangerous failure PFH of $2.27 \cdot 10^{-7}$ per hour. This satisfies PL d.

- For the safety function SF 3, “Setup mode; release of the enabling switch on the hand-held terminal brings the drive to a halt (STO)”, the evaluation yields the following result: the combination of the enabling switch B4, safety module K2 and frequency converter T1 subsystems yields an average probability of dangerous failure PFH of $1.34 \cdot 10^{-6}$ per hour. This satisfies PL c.
- For the safety function SF 4, “Setup mode; exceeding of the maximum permissible speed leads to the drive being brought to a halt (SLS)”, the evaluation yields the following result: the G1/G2 subsystem satisfies Category 3 with a high $MTTF_d$ (40 years) and a high DC_{avg} (99%). This results in an average probability of dangerous failure of $6.91 \cdot 10^{-8}$ per hour.

The combination of the respective subsystems of the rotary encoders G1/G2, speed monitor K3 and frequency converter T1 yields an average probability of dangerous failure PFH of $4.69 \cdot 10^{-7}$ per hour. This satisfies PL d.

Example 9: Drive control for automatic and setup mode with limited speed and enabling switch – PL d

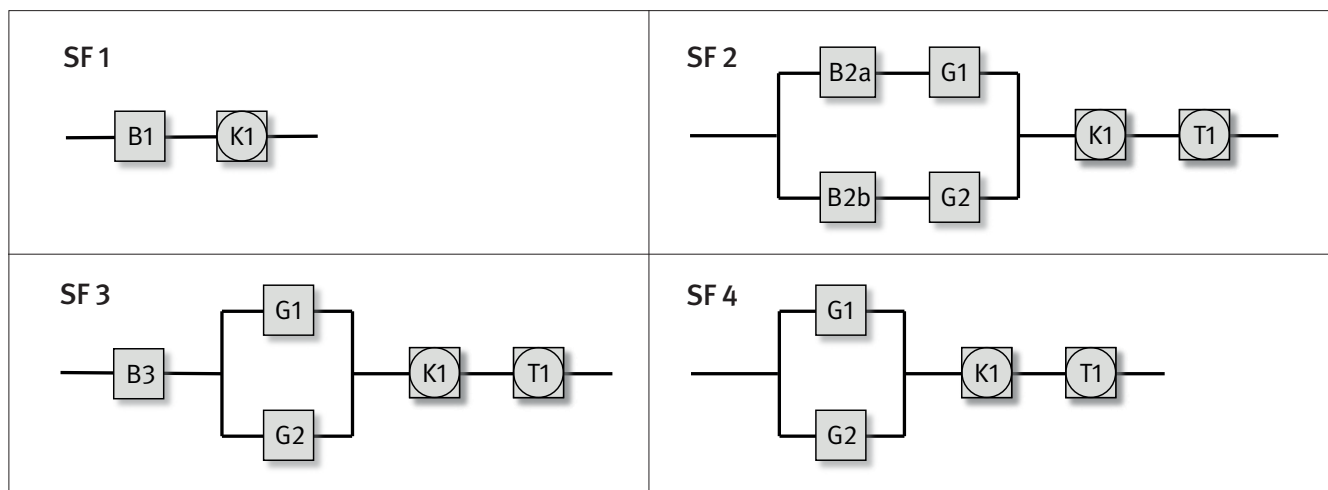
Figure B.17:
Schematic circuit diagram of the drive control



Safety functions

- SF 1: operating mode selection
- SF 2: automatic mode; SS1 following opening of a safeguard

Figure B.18:
Safety-related block diagrams for Example 9



- SF 3: setup mode; releasing or fully depressing the three-stage enabling switch brings the drive to a halt (SS1)
- SF 4: setup mode; safely limited speed – exceeding of the maximum permissible speed leads to the drive being brought to a halt (STO)

Note:

Hazards presented by individual machine components are considered during determining of the Performance Level for SF 2 and the following safety functions. A part of a machine is moved by a single drive. In this case this means that each drive that gives rise to a hazardous movement is considered separately. The calculation of the respective PL therefore need not consider both frequency converters, nor all rotary encoders. In this example, all safety functions in which the frequency converter T1 is involved are considered. During the analysis for T2 the signal processing for the servo enable must be considered additionally. Further information for the analysis of individual machine components can be found in Section 2.2 of this report (“Overlapping hazards”).

Function description

- The drive control implements synchronized movements with safely limited speed in setup mode. The frequency converters T1/T2 are operated as master and slave. The first frequency converter T1 (master) receives a reference value and drives the downstream frequency converter T2 (slave) over a data bus.
- The operating mode selector switch B1 permits selection between automatic and setup modes (SF 1). In automatic mode, the contacts of the position switch B2 on the safeguard are closed, and the drive can be operated at any speed. Opening of the safeguard in automatic mode (tripping of SF 2) is detected by the safety PLC K1, which consequently initiates a fast stop of the drive via the relevant input of the master frequency converter. The slave frequency converter T2 receives this command over the bus and follows the master. K1 monitors the braking ramp, de-activates the servo enable of the frequency converters T1a/T2a once the drive has stopped, and disables the trigger pulse block T1b/T2b. The SS1 safety function (corresponding to Stop Category 1 to EN 60204-1) is implemented by the addition of ramp monitoring in K1 to the frequency converters with STO.
- When the guard is open, only setup mode with limited speed is possible (SF 4). The enabling switch B3 must be actuated for this purpose (SF 3). The movement is initiated by a separate control device on a hand-held terminal (not shown).
- Following releasing or full depressing to the third stage of the enabling switch B3, the hazardous movement is brought to a halt via the safety PLC K1. This is achieved in the first instance by the fast stop function in the frequency converters T1 and T2. Stopping is monitored by K1. Following stopping, STO is activated in the frequency converters. This procedure implements SS1.

- The speed for each axis is monitored in setup mode (SF 4) by the safety PLC K1. Two encoders for each axis (G1/G2 and G3/G4) are used to detect the speed. Should the maximum permissible speed be exceeded, the hazardous movement is halted by activation of the STO safety function in the frequency converters T1/T2.
- Faults in the position switch B2, the pulse blocking relays of T1b/T2b and the rotary encoders G1 to G4 are detected by the safety PLC K1. The fast-stop ramp is also monitored and the stationary state recognized by K1 with the aid of the rotary encoders.
- Both shutdown paths of T1 and T2 are monitored. For the purposes of fault detection, the relays of the pulse blocks T1b/T2b each possess a mechanically linked break contact that is read in by K1. Faults in the servo enable are apparent in the form of disruptions to operation of the machine.

Design features

- Fundamental and well-tried safety principles and the requirements of Category B are observed. Protective circuits (such as contact fuse protection, circuit earthing), as described in the first sections of Chapter 8 of BGIA Report 2/2008e, are present.
- Cross-circuits and short-circuits in electrical supply lines must be considered in accordance with EN 13849-2, Table D.4. Faults are detected as they occur, and a safe state is brought about. Alternatively, the conductors must be laid such that fault exclusion is possible for cross-circuits and short-circuits.
- The operating mode selector switch B1 is a cam-operated selector switch with positive actuation. The design of the operating mode selector switch permits fault exclusions in accordance with EN ISO 13849-2, Table D.8.
- B2 is a position switch with separate actuator. The switch features two direct opening contacts that satisfy the requirements of EN 60947-5-1, Annex K. The actuating mechanism must be designed and fitted as specified.
- T1 and T2 are frequency converters with integrated STO safety function in accordance with Category 3 and PL d. STO is activated by disabling of pulse blocking and servo enable.
- The safety PLC satisfies the requirements of Category 4 and PL e.
- The software (SRASW) for the safety PLC K1 is programmed in accordance with the requirements for PL d and the instructions in Section 4.6.3 and where applicable 4.6.4 of EN ISO 13849-1.

Note:

- The two rotary encoders G1/G2 and G3/G4 must be fitted to the respective motor in such a way that simultaneous failure of both components as a result of a single fault (e.g. encoder shaft breakage) is excluded.

Calculation of the probability of failure

- Fault exclusion applies to the direct opening contact of B1 and to separation of the operating modes in this switch. Owing to the implemented control architecture and installation in a switching cabinet with a minimum ingress protection of IP 54, faults such as short-circuits between adjacent conductor paths, contact points and conductors can be excluded. The conditions for fault exclusion up to a maximum of PL d to EN ISO 13849-2, Table D.8 are met. Based upon an analysis, faults in the operating mode selection that could prevent the required safety functions being effective can be excluded.
- Fault exclusion may be assumed for not opening of the direct opening contacts of B2. Fault exclusion is justified for the mechanical components of the position switch owing to the environment and conditions of use. The position switch is for example mounted shrouded, thereby reducing the impact of environmental effects and at the same time preventing tampering.
- The safety PLC K1 satisfies the requirements of Category 4 and PL e. The PFH is $3.16 \cdot 10^{-8}$ per hour [M].
- T1 and T2 are frequency converters with integrated STO safety function. They satisfy the requirements for Category 3, SIL 2 and PL d. The PFH is $3.16 \cdot 10^{-7}$ per hour [M]. These data for T1 and T2 are valid only when the manufacturer's specifications for fault recognition by external components are implemented.
- The rotary encoders G1/G2 and G3/G4 are flanged to the left and right-hand sides of the motors. The encoder manufacturer states an $MTTF_d$ of 40 years for each encoder with assumption of fault exclusion for shaft breakage.

- The DC for the rotary encoders G1/G2 and G3/G4 is estimated at 99%, owing to the cross-check of the signals by the safety PLC K1.
- Adequate measures against common-cause failure are taken for the subsystem comprising the safety switch B2 and the rotary encoders G1/G2 (65 points): separation (15), protection against overvoltage etc. (15) and protection against environmental conditions (25 + 10).
- The evaluation of the safety function SF 1, “Operating mode selection”, yields the following result: the formulation of fault exclusion for B1 based upon the design characteristics enables the separation of setup and automatic modes to be classified in PL d. The restriction to PL d is due to the fact that the evaluation of the operating mode selector switch is based solely upon fault exclusions (see EN ISO 13849-2, Table D.8). The PFH value is determined solely by the contribution of K1, and is $3.16 \cdot 10^{-8}$ per hour.
- For the safety function SF 2, “Automatic mode; SS1 following opening of a safeguard”, the evaluation yields the following result: the B2/G1/G2 subsystem satisfies Category 3 with a high $MTTF_d$ (40 years) and a high DC_{avg} (99%). This results in an average probability of dangerous failure of $6.91 \cdot 10^{-8}$ per hour.

The combination of the respective subsystems of the position switch/rotary encoders B2/G1/G2, safety PLC K1 and frequency converter T1 yields an average probability of dangerous failure PFH of $4.17 \cdot 10^{-7}$ per hour. This satisfies PL d.

- For the safety function SF 3, “Setup mode; releasing or fully depressing the three-stage enabling switch brings the drive to a halt (SS1)”, the evaluation yields the following result: the G1/G2 subsystem satisfies Category 3 with a high $MTTF_d$ (40 years) and a high DC_{avg} (99%). This yields an average probability of dangerous failure of $6.91 \cdot 10^{-8}$ per hour.

The combination of the position switch B3, rotary encoders G1/G2, safety PLC K1 and frequency converter T1 subsystems yields an average probability of dangerous failure PFH of $4.17 \cdot 10^{-7}$ per hour. This satisfies PL d.

- For the safety function SF 4, “Setup mode; safely limited speed – exceeding of the maximum permissible speed leads to the drive being brought to a halt (STO)”, the evaluation yields the following result: the G1/G2 subsystem satisfies Category 3 with a high $MTTF_d$ (40 years) and a high DC_{avg} (99%). This results in an average probability of dangerous failure of $6.91 \cdot 10^{-8}$ per hour.

The combination of the respective subsystems of the encoders G1/G2, safety PLC K1 and frequency converter T1 yields an average probability of dangerous failure PFH of $4.17 \cdot 10^{-7}$ per hour. This satisfies PL d.

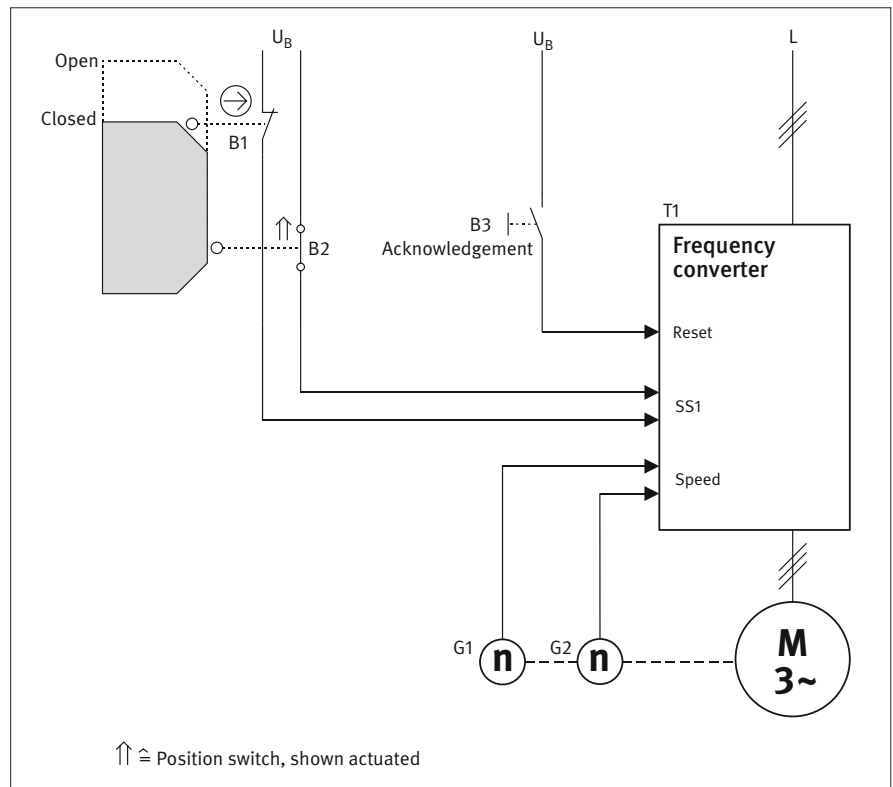
Example 10: Controlled stopping of a drive when the safeguard is opened, with acknowledgement function


Figure B.19:
Schematic circuit diagram of position
monitoring

Safety functions

- SF 1: Safe stopping when the safety guard is opened
- SF 2: Manual resetting by release of the actuated acknowledgement button B3 with the safeguard closed

Function description

- When the safeguard is opened, the “safe stopping” (SS1) input of the frequency converter T1 is interrupted in two channels via the position switches B1 and B2. The frequency converter T1 initiates stopping and monitors the deceleration ramp of the motor. When the drive has stopped, STO is activated.
- The rotary encoders G1 and G2 supply the relevant speed information required for monitoring of the deceleration ramp. Faults in the rotary encoders are detected by comparison of the two signals in the frequency converter T1.
- The frequency converter monitors the function of B1 in comparison with B2. In the event of a fault, continued operation is prevented.
- Access to the rear of the safeguard is possible; an acknowledgement function (manual reset) following vacation of the hazardous zone and closing of the safety guard is therefore provided in addition. The hazardous zone must be visible from the acknowledgement point.

Remarks

- In this example, the SS1 safety function is implemented by monitoring of the braking ramp.
- The control voltage U_B and the internal control voltage of the frequency converter T1 are generated from the intermediate circuit voltage of the frequency converter. The drive is brought to a controlled halt even in the event of a power failure.

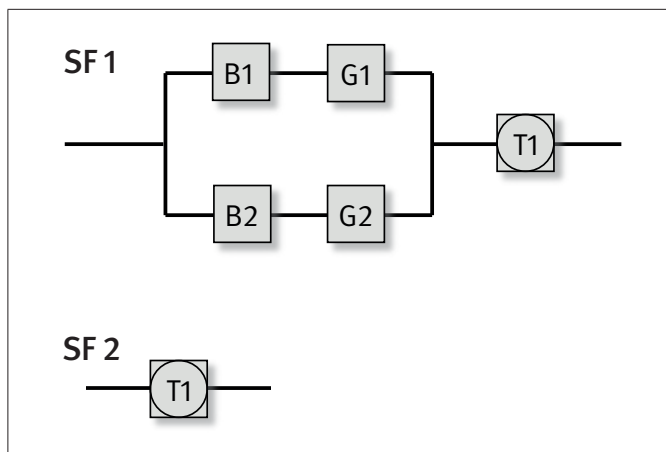


Figure B.20:
Safety-related block diagrams for Example 10

Design features

- Fundamental and well-tried safety principles and the requirements of Category B are observed. Protective circuits (such as contact fuse protection, circuit earthing), as described in the first sections of Chapter 8 of BGIA Report 2/2008e, are present.
- Cross-circuits and short-circuits in electrical supply lines must be considered in accordance with EN ISO 13849-2, Table D.4. Faults are detected as they occur, and a safe state is brought about. Alternatively, the conductors must be laid such that fault exclusion is possible for cross-circuits and short-circuits.
- The frequency converter T1 is equipped with the integral SS1 safety function with ramp monitoring in accordance with Category 3 and PL d.
- Actuating elements and position switches must be secured against displacement. Only rigid mechanical components (not spring elements) may be used.
- The position switch B1 is a positively opening position switch that satisfies the requirements of EN 60947-5-1, Annex K.
- Malfunctions in the actuating and operating mechanism of the protective equipment are detected by two counter-operated position switches B1 and B2 (make and break contact combination).
- The frequency converter T1 is equipped with an acknowledgement (manual reset) function.
- The requirements for the manual reset function in accordance with EN ISO 13849-1 Section 5.2.2 are met. These include the requirement for T1 to activate the reset function only when B3 has been released and for the reset alone not to lead to a restart of T1.
- The two rotary encoders must be fitted in such a way that simultaneous failure of both as a result of a single fault (e.g. encoder shaft breakage) is excluded.

Calculation of the probability of failure

- Fault exclusion applies to the direct opening contact of B1.
- A B_{10d} value of 1,000,000 switching cycles [M] is stated for the electrical make contact of the position switch B2. An n_{op} of 7,680 cycles per year yields an $MTTF_d$ of 1,302 years.
- The same applies to the mechanical part of each position switch B1 and B2. At a B_{10d} value of 1,000,000 switching cycles [M] and an n_{op} of 7,680 cycles per year, the $MTTF_d$ is 1,302 years.
- The frequency converter with integral SS1 safety function and acknowledgement function satisfies the requirements of Category 3 and PL d. The PFH is $2.0 \cdot 10^{-7}$ per hour [M].

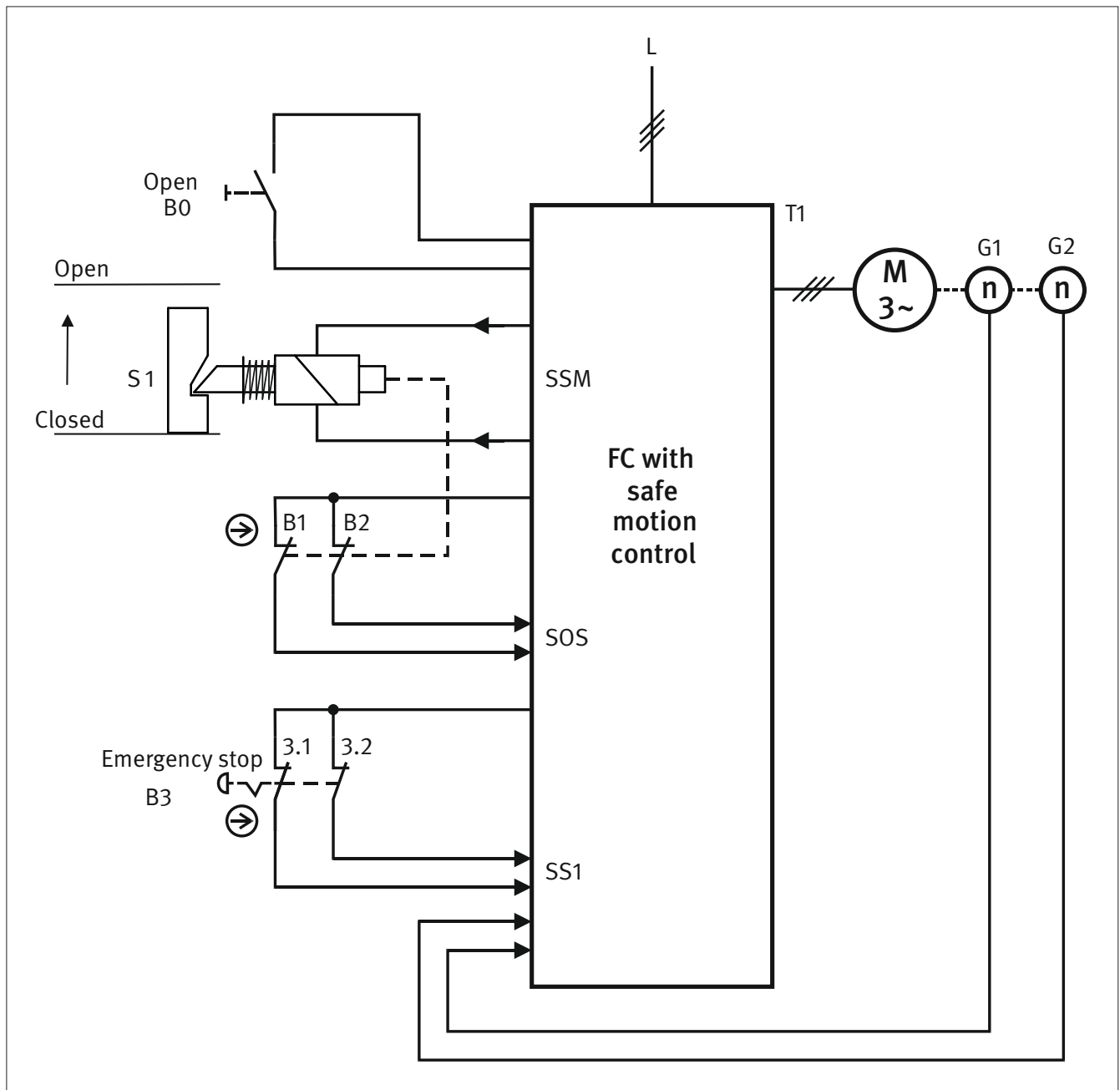
- Pushbutton B3 for the manual reset is a standard commercial pushbutton. Since a trailing signal edge caused by release of the pushbutton is required for signalling (see EN ISO 13849-1, Section 5.2.2), failure of the button does not lead to a dangerous fault. For this reason, B3 is not considered in the quantification.

Note: The DGUV Expert Committee Woodworking and Metalworking, Subcommittee Machinery, Systems, Automation and Design of Manufacturing Systems is currently preparing an information sheet on the subject of “Manual resetting” (www.dguv.de/medien/fb-holzundmetall/publikationen/infoblaetter/infobl_deutsch/067_rueckstellfunktion.pdf).

- The encoder manufacturer states an $MTTF_d$ of 40 years each for the rotary encoders G1 and G2 with assumption of fault exclusion for encoder shaft breakage.
- The DC for the position switches B1 and B2 is 99%, owing to the plausibility check by the frequency converter T1.
- The DC for the rotary encoders G1 and G2 is estimated at 99%, owing to the cross-check of the signals in the frequency converter T1.
- Adequate measures against common-cause failure are taken for the subsystem comprising the position switches B1/B2 and the rotary encoders G1/G2 (65 points): separation (15), protection against overvoltage etc. (15) and protection against environmental conditions (25 + 10).
- For the safety function SF 1, “Safe stopping when the safety guard is opened”, the evaluation yields the following result: the B1/B2/G1/G2 subsystem satisfies Category 3 with a high $MTTF_d$ (38 years) and a high DC_{avg} (99%). This results in an average probability of dangerous failure of $7.26 \cdot 10^{-8}$ per hour. The combination of the subsystems of the position switches/encoders (B1/B2/G1/G2) and the frequency converter T1 yields an average probability of dangerous failure PFH of $2.73 \cdot 10^{-7}$ per hour. This satisfies PL d.
- For the safety function SF 2, “Manual resetting by release of the actuated acknowledgement pushbutton B3 with the safeguard closed”, the resulting average probability of dangerous failure is $2.0 \cdot 10^{-7}$ per hour. This satisfies PL d.

Example 11: Drive control with frequency converter with integrated safe movement control – PL d

Figure B.21:
Position monitoring of a safeguard with guard locking device and emergency-stop


Safety functions

- SF1: Safe operating stop (SOS) when the guard locking device is unlocked
- SF2: Unlocking of the guard locking device at standstill by SSM
- SF3: Actuation of the emergency-stop control device leads to controlled stopping (SS1)

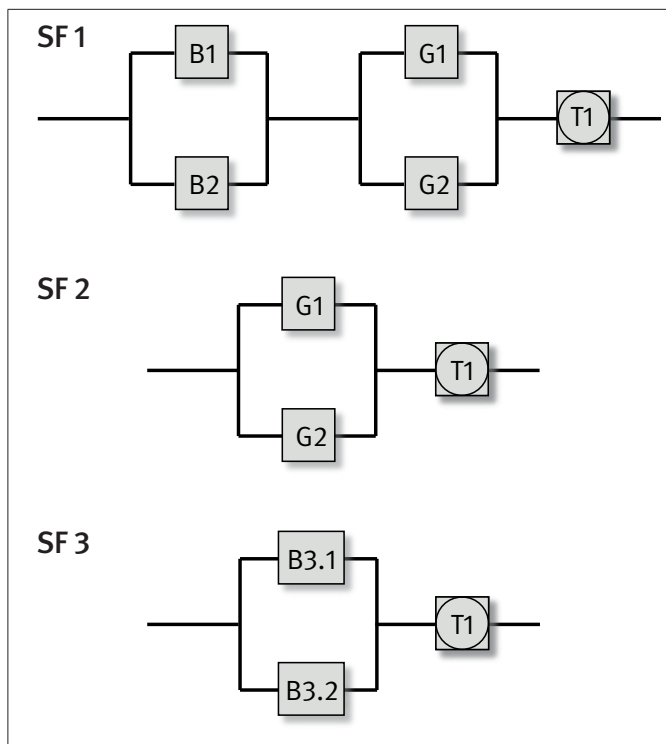


Figure B.22:
Safety-related block diagrams for Example 11

Function description

- Unlocking of the safeguard is requested by actuation of the inch button B0. This causes the frequency converter T1 to reduce the drive speed to zero. Opening of the safeguard is possible only with the drive stationary. At a motor speed of (almost) zero, the frequency converter generates a safe output signal for unlocking of the locking mechanism in the guard locking device S1 by means of the SSM (safe speed monitoring) safety function.
- Unlocking of the safeguard is detected by the two position switches B1 and B2. The safety function SOS (safe operating stop) is then activated in the frequency converter.
- When the emergency-stop control device B3 is actuated during a motor movement, the drive is brought to a controlled stop by SS1 (safe stop 1) as fast as possible.
- Where access can be gained to the rear of the safeguard, provision must be made for manual resetting of the safeguard at a point outside the hazardous zone.

Design features

- The frequency converter T1 possesses the integral safety functions SOS, SS1, SSM and STO (not used in this example).
- Note that with the SS1 function, the available braking torque may be reduced in the event of a fault in the frequency converter.
- The two rotary encoders must be fitted in such a way that simultaneous failure of both as a result of a single fault (e.g. encoder shaft breakage) is excluded.
- The speed is detected in this example by two encoders in a two-channel arrangement. Depending upon the frequency converter employed and the safety function to be implemented, the second encoder may not be necessary. In some cases, sensorless operation is also possible. The requirements set out in the user documentation provided by the frequency converter manufacturer must be observed in all cases.
- Cross-circuits and short-circuits in electrical supply lines must be considered in accordance with EN ISO 13849-2, Table D.4. Faults are detected as they occur, and a safe state is brought about. Alternatively, the conductors must be laid such that fault exclusion is possible for cross-circuits and short-circuits.

- The safeguard is a safety guard with a guard locking device S1. Access to the hazardous movement is prevented until the movement has come to a halt (SF 2). The safety guard is held closed by a locking mechanism in the form of a spring-operated pin of a solenoid: this prevents the actuator from being withdrawn from the switch head until the unlocking solenoid has been actuated. According to the manufacturer, the guard locking device is protected against inadvertent closure. Unexpected start-up of the motor when the safety guard is open is prevented by virtue of the fact that the device preventing inadvertent closure prevents the contacts B1 and B2 from closing unless the safety guard is closed and the locking mechanism of the guard locking device is in the locked position (SF 2).

Calculation of the probability of failure

- B1 and B2 are the direct opening contacts for monitoring the locking mechanism of the guard locking device. In conjunction with the function for preventing inadvertent closure of the guard locking device, this results in the closed position of the safety guard also being detected, since the locking mechanism can assume the locked position only when the safety guard is closed. Owing to the positive action of the contacts, fault exclusion is assumed for failure of the electrical contact to open.
- Fault exclusion can be assumed for the mechanical components of the guard locking device when the following conditions are met:
 - use in accordance with the instruction manual, in particular the installation instructions and technical data (e.g. actuating radius, actuating velocity)
 - prevention of working loose
 - the static forces on the guard locking device are lower than the locking force stated on the data sheet
 - no dynamic forces arise, since current flows through the unlocking solenoid only when the safety guard is closed; refer in this context also to the latest edition of DGUV Information 203/003 (formerly BGI 575) and DGUV Information 203-010 (formerly BGI 670) concerning the selection and fitting of interlocking devices (in preparation)
 - the device is not used as a mechanical stop
 - the actuator is mounted such that it cannot be removed
 - regular maintenance
 - positive coupling following assembly
 - adequate mechanical strength of all mounting and functional elements
 - damage that could be caused by foreseeable external influences (such as penetration by dirt and dust, mechanical shock) is prevented by the form of mounting or need not be anticipated owing to the conditions of use
- For the emergency-stop control device B3, fault exclusion for direct opening contacts and the mechanism is possible in accordance with EN ISO 13849-2:2013, Table D.8 and BGIA Report 2/2008e, Table D.2 up to 6,050 actuating cycles.
- The rotary encoders G1 and G2 are fitted to the same shaft. They are conventional encoders with pulse outputs. The signals are evaluated within the frequency converter. The manufacturer states an $MTTF_d$ of 50 years for the encoders. The rotary encoders must be fitted in such a way that simultaneous failure of both components caused by a single fault (e.g. encoder shaft breakage) is excluded.
- The frequency converter T1 with safe movement control possesses the following integral safety functions:
 - Safe torque off (STO)
 - Safe stop 1 (SS1)
 - Safe operating stop (SOS)
 - Safe speed monitoring (SSM)

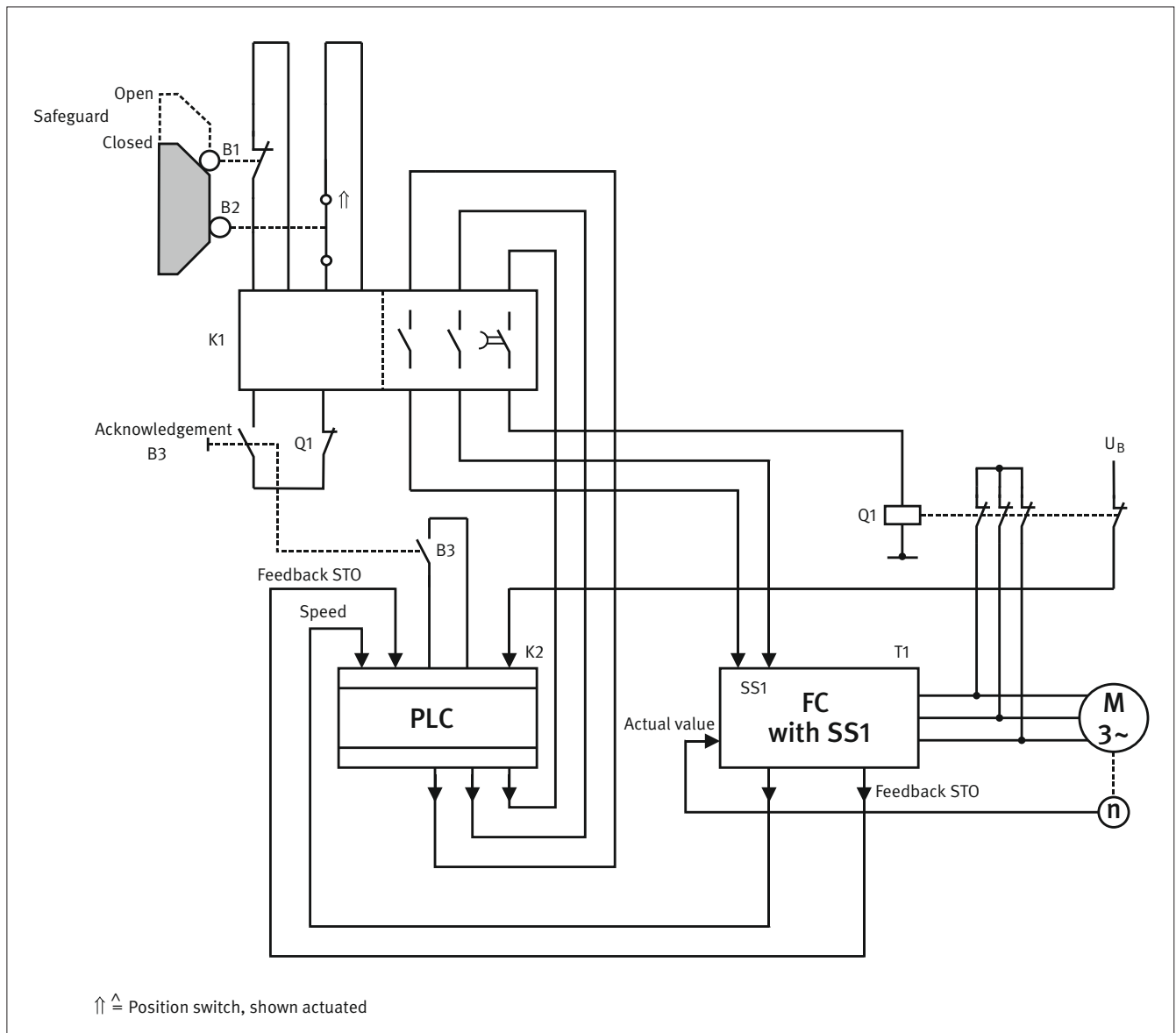
The manufacturer states a PFH of $5 \cdot 10^{-8}$ per hour [M] for the safety functions, individually and in combination.

- Owing to the plausibility test by the frequency converter T1, a DC of 90% is assumed for the rotary encoders G1 and G2.
- Adequate measures against common-cause failure are taken for the subsystem of G1/G2 (65 points): physical separation (15), protection against overvoltage etc. (15), protection against contamination and EMC and protection against environmental conditions (25 + 10).
- The subsystem of G1/G2 satisfies Category 3 with a high $MTTF_d$ (50 years) and medium DC (90%). This yields an average probability of dangerous failure of $1.22 \cdot 10^{-7}$ per hour in the PL d range.

- For the safety function SF 1, “Safe operating stop (SOS) with the guard locking device is unlocked”, the evaluation yields the following result: the combination of the subsystems yields an average probability of dangerous failure of $1.72 \cdot 10^{-7}$ per hour. This satisfies PL d.
- For the safety function SF 2, “Unlocking of the guard locking device at standstill by SSM”, the evaluation yields the following result: the combination of the subsystems yields an average probability of dangerous failure of $1.72 \cdot 10^{-7}$ per hour. This satisfies PL d.
- For the safety function SF 3, “Actuation of the emergency-stop control device leads to controlled stopping (SS1)”, the evaluation is as follows: the combination of the subsystems yields an average probability of dangerous failure of $5 \cdot 10^{-8}$ per hour. This computes to PL e. However, since the frequency converter can be used only up to PL d, the result for SF 3 is PL d.

Example 12: Prevention of unexpected start-up with frequency converter and short-circuit contactor – PL e

Figure B.23:
Schematic circuit diagram of the drive control



Safety function

- SF 1: STO of the motor following opening of the safeguard and halting of the drive

Note:

Different components are employed for “halting” and “prevention of unexpected start-up”, since the additional short-circuit contactor Q1 is required only for the prevention of unexpected start-up. Q1 represents a third shutdown path by means of which a higher PL is attained. As already described, the safety functions are divided into two for calculation of the PFH. Only the prevention of unexpected start-up will be considered here, however.

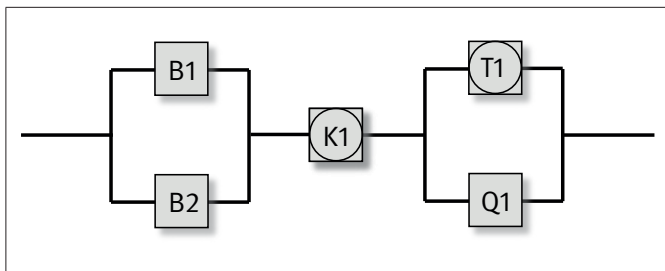


Figure B.24:
Safety-related blockdiagram for Example 12

Function description

- Opening of the safeguard is detected by the safety module K1 via B1 and B2. The instantaneous enabling paths of K1 drop out. SS1 of the frequency converter T1 is initiated and the drive stops. Q1 then drops out with a delay. The closing of the break contacts of Q1 causes the supply conductors to the motor to be short-circuited. The drive is in STO.
- Welding of the contacts of the contactor Q1 would always be evident when voltage is supplied to the motor via T1, by tripping of the output protective device. In addition, the contactor Q1 is monitored for “sticking” in the PLC K2.
- Failure of the supply voltage leads to controlled stopping of the motor and to delayed short-circuiting of the supply conductors from T1 to the motor. For this purpose, it is necessary for:
 - the control electronics of T1 to be supplied from the intermediate DC circuit;
 - K1 to have an uninterruptible power supply.

Design features

- Fundamental and well-tried safety principles and the requirements of Category B are observed. Protective circuits (such as contact fuse protection), as described in the first sections of Chapter 8 of BGIA Report 2/2008e, are provided. In the present example, the fundamental safety principles include the closed-circuit current principle and earthing of the control circuit. Well-tried safety principles include overdimensioning of the contacts of B1, B2 and Q1.
- Cross-circuits and short-circuits in electrical supply lines must be considered in accordance with EN ISO 13849-2, Table D.4. Faults are detected as they occur, and a safe state is brought about. Alternatively, the conductors must be laid such that fault exclusion is possible for cross-circuits and short-circuits.
- The frequency converter T1 possesses the integral STO and SS1 safety functions.
- The position switch B1 is a position switch with direct opening contacts to EN 60947-5-1, Annex K.
- Malfunctions in the actuating and operating mechanism of the protective equipment are detected by two counter-operated position switches B1 and B2 (make and break contact combination).
- Actuating elements and position switches must be secured against displacement. Only rigid mechanical components (not spring elements) may be used.
- Where hazardous zones can be accessed from the rear, an acknowledgement facility must be provided that is actuated when the hazardous zone has been vacated and the safety guard closed. The hazardous zone must be visible from the acknowledgement point.

Remarks

- The use of short-circuit contactors is controversial. The method is however used, for example on presses, for the assurance of the PL e in order to prevent unexpected start-up. It is used in particular to improve the PFH value in function controls that are complex owing to the process. The use of short-circuit contactors however requires trials to determine their behaviour when they are short-circuited. Should the SS1 fail, the contactor Q1 short-circuits the operational voltage of the motor, and damage to the contactor can be expected. Q1 therefore must then be replaced, and any other faults eliminated by repairs.

- The function of the control system presented here is only a part of it. Selection of the operating mode for example is not shown.

Calculation of the probability of failure

- Fault exclusion applies to the direct opening contact of B1.
- A B_{10d} value of 1,000,000 switching cycles [M] is stated for the electrical make contact of position switch B2. At 200 working days, 8 working hours per day and a cycle time of one minute, the result is an n_{op} of 96,000 cycles per year and an $MTTF_d$ of 104 years.
- The same applies to the mechanical part of each position switch B1 and B2. At a B_{10d} value of 1,000,000 switching cycles [M] and an n_{op} of 96,000 switching cycles per year, the $MTTF_d$ is 104 years.
- The safety module K1 is a standard commercial component for use in PL e and Category 4. The PFH is $1.8 \cdot 10^{-8}$ per hour [M].
- The contactor Q1 has a mechanical life of $2 \cdot 10^6$ switching cycles. Due to its low electrical load in this application the mechanical life is set as the B_{10d} value. At an n_{op} of 96,000 switching cycles per year, the $MTTF_d$ value computes to 416 years.
- The frequency converter T1 possesses the integral STO safety function with a check-back output. It is suitable for use in PL d and Category 3. The PFH value of the STO is $2 \cdot 10^{-7}$ per hour.

As shown in the safety-related block diagram (Figure B.24), T1 is an encapsulated subsystem with the addition of a channel comprising Q1. This structure does not correspond to any of the designated architectures of EN ISO 13849-1. The PFH for this sub-system is therefore calculated by the procedure described in SISTEMA Cookbook 4, Chapter 2:

The relationship $MTTF_d = 1/PFH$ yields an $MTTF_d$ of 570 years for T1. The internal DC of T1 cannot be used again, since it has already been used to reduce the PFH of T1. An additional DC by other components can however be considered.

- The additional fault detection relating to the STO safety function of the frequency converter T1 is external, being provided in the present case in the PLC K2 by comparison of Q1 and STO check-back. A DC of 99% is assumed for this fault detection.
- The DC for B1 and B2 is stated as 99%, owing to monitoring by the safety module K1.
- The DC of the contactor Q1 is assumed to be 99%. The contactor Q1 is monitored in the PLC K2 for “Sticking”.

Note:

Contact welding leads to a short-circuit when the motor supply voltage is applied. The output protection of the frequency converter T1 trips. A failure to safety occurs.

Execution of the safety function requires the break contacts of Q1 to close, thereby enabling current to flow in the event of a fault in T1 (deviation from the closed-circuit current principle).

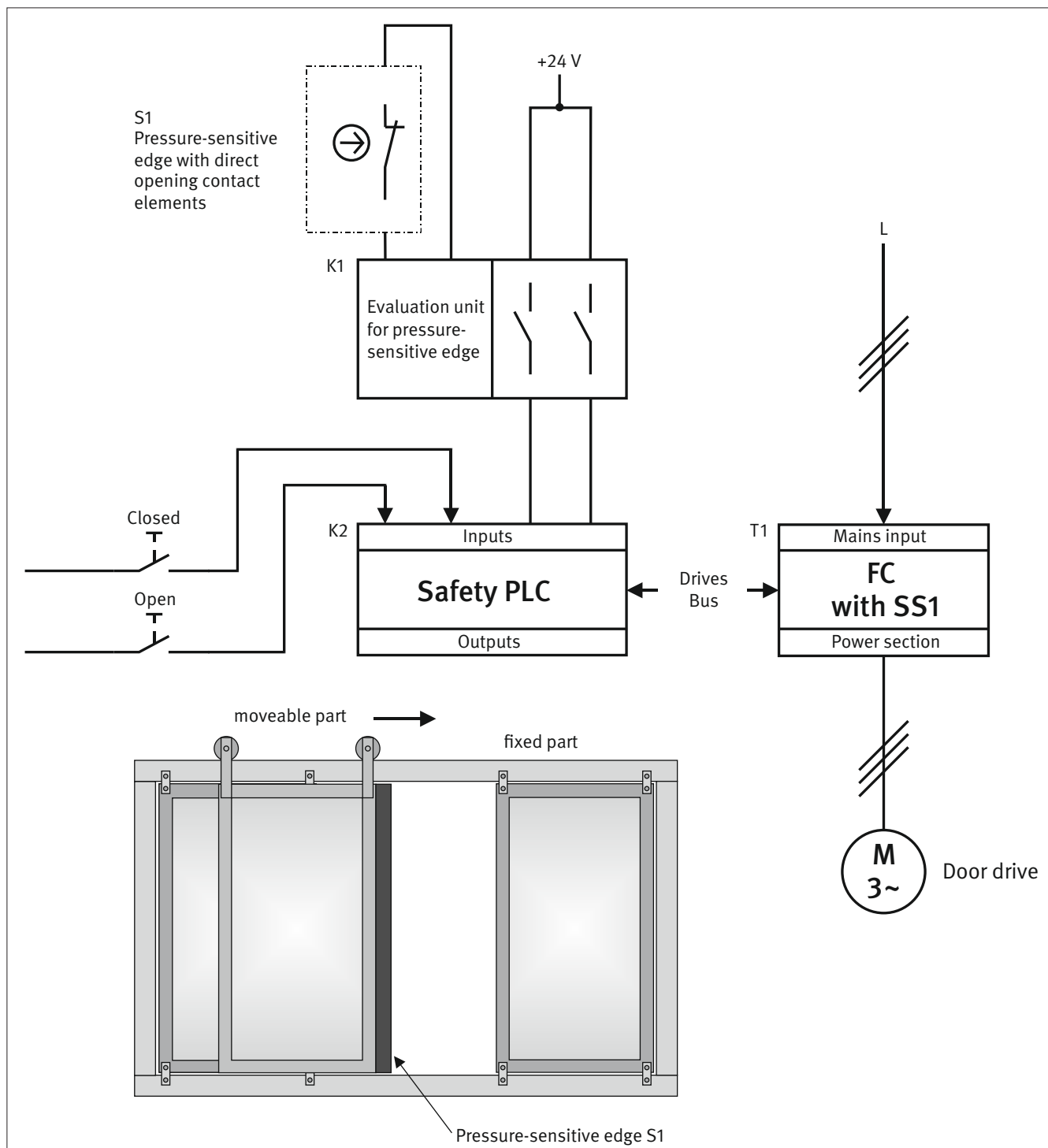
The manufacturer of Q1 states that the probability of failure of this capacity (security against malfunction) is $1 \cdot 10^{-8}$. This corresponds to one fault per 100 million switching cycles. Since this value is considerably lower than the mechanical life of the contact, it is not considered mathematically in this case.

- Adequate measures against common-cause failure are taken for the subsystem comprising B1 and B2 and for that comprising T1 and Q1 (75 points): separation (15), protection against overvoltage etc. (15), well-ried components (5), FMEA (5) and protection against environmental conditions (25 + 10).
- The subsystem B1/B2 satisfies Category 4 with a high $MTTF_d$ per channel (78.6 years) and a high DC (99%). This yields an average probability of dangerous failure of $3.23 \cdot 10^{-8}$ per hour.
- Owing to the limited service life of B1 and B2 in this application, a timely replacement after ten years is recommended.
- The subsystem T1/Q1 satisfies Category 4 with a high $MTTF_d$ per channel (100 years) and a high DC (99%). This yields an average probability of dangerous failure of $2.47 \cdot 10^{-8}$ per hour.

- For the safety function SF 1, “STO of the motor following opening of the guard and halting of the drive”, the evaluation yields the following result: the combination yields an average probability of dangerous failure of $7.5 \cdot 10^{-8}$ per hour. This satisfies PL e.

Example 13: Power-operated movable guard (safety guard) – PL d

Figure B.25:
Schematic circuit diagram of the drive control



Safety function

- SF 1: Limitation of the closing forces of a power-operated door by actuation of a pressure-sensitive edge

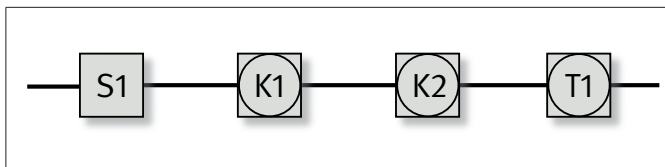


Figure B.26:
Safety-related block diagram for Example 13

Function description

- The safety guard (movable guard) must be opened for the charging and retrieval of workpieces and for tool changing. Powered opening of the safety guard can be initiated manually by the operator, or automatically, for example for charging or retrieval by robots. Opening and closing of the safety guard must not give rise to hazards, such as pinching of the operator by a closing movement. Provided the limit values for power guards are observed, it is assumed that no hazard exists (see notes).

If the limit values cannot be observed, the hazardous zone must be safeguarded by additional protective equipment.

In the present example, the safety guard is fitted with a pressure-sensitive edge S1 on the closing edge. When the safety guard is closed, the actuation of the pressure-sensitive edge brings the drive – by means of the evaluation unit K1, the safety PLC K2 and the frequency converter T1 – so rapidly to a halt that the permissible closing forces are not exceeded.

Notes: Limit values for power guards.

- The static force at the closing edge must not exceed 75 N and the kinetic energy of the guard must not exceed 4 Joules. If the guard is fitted with additional protective equipment that triggers automatic opening (reversal of movement) in response to contact with an obstruction, the static force and kinetic energy must not exceed 150 N and 10 Joules respectively (refer in this context to EN 953, Section 5.2.5.2). These requirements apply only under the condition that the closing edges are at least 8 mm in width and that no shear hazard exists.
- “*Shearing hazards occurring between secondary closing edges can be safeguarded by limitation of forces measured at the secondary closing edges to less than 150 N static and less than 400 N dynamic in addition to:*
 - either a distance of at least 25 mm between passing edges
 - or the passing edges shall be provided with round edges with radius of at least 2 mm for each edge and a combined radius (sum of the 2 radii) of at least 6 mm (e.g. at least 2 mm + 4 mm or 3 mm + 3 mm)”.

Source: Section 5.1.1.5.3 of:

EUROPEAN STANDARD

EN 12453

NORME EUROPÉENNE

EUROPÄISCHE NORM

November 2000

ICS 91.060.50

English version

Industrial, commercial and garage doors and gates - Safety in
use of power operated doors - Requirements

- Measurement of the forces is governed by EN 12445, and the dynamic behaviour by Annex A, Figure A.1 and Table A.1 of EN 12453 (Figure B.27 and Table B.2 in this report).

Where

F_d : maximum force, measured with an instrument to EN 12453 Section 5.1.1.5 during the dynamic duration T_d

F_s : maximum force, measured with an instrument to EN 12453 Section 5.1.1.5 after the dynamic duration T_d

T_d : duration for which the measured force exceeds 150 N

T_t : duration for which the measured force exceeds 25 N

- The values specified in Table B.2 are maximum values permitted for a duration of no more than 0.75 s ($T_d \leq 0.75$ s). The total time T_t must not exceed 5 s. A gap width of 4 mm must not be exceeded at the secondary closing edge between the movable guard and the enclosure.
- Should it not be possible for the above limit value requirements to be met, a remote-hold protective device for example must be provided for the operator.

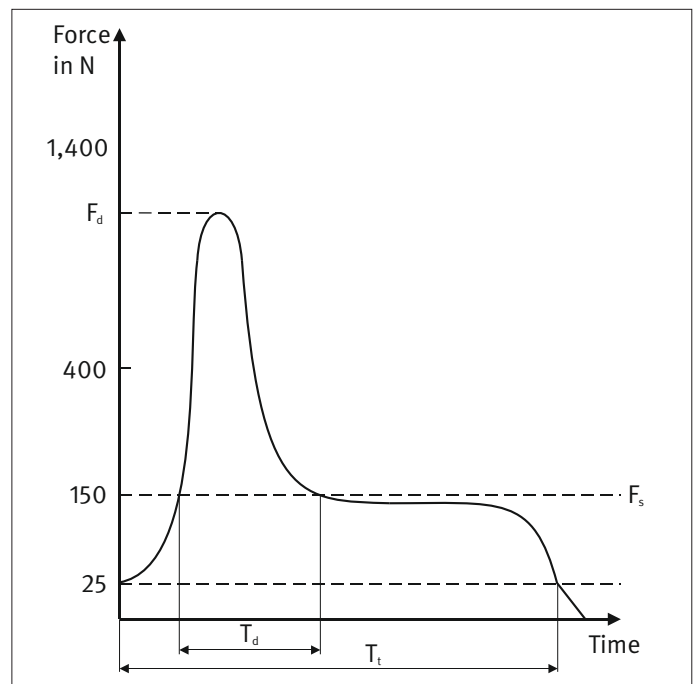


Figure B.27: Closing forces as a function of time, from EN 12453

Table B.2: Admissible dynamic forces

Admissible dynamic forces in N	Between closing edges and opposing closing edges		Between flat areas other than closing edges and counterclosing edges, $> 0.1 \text{ m}^2$ with no side $< 100 \text{ mm}$
	in opening gaps of 50 to 500 mm	in opening gaps of $> 500 \text{ mm}$	
horizontally moving door	400	1,400	1,400
door rotating around an axis perpendicular to the floor	400	1,400	1,400
vertically moving door	400	400	1,400
door rotating around an axis parallel to the floor – barriers	400	400	1,400

Design features

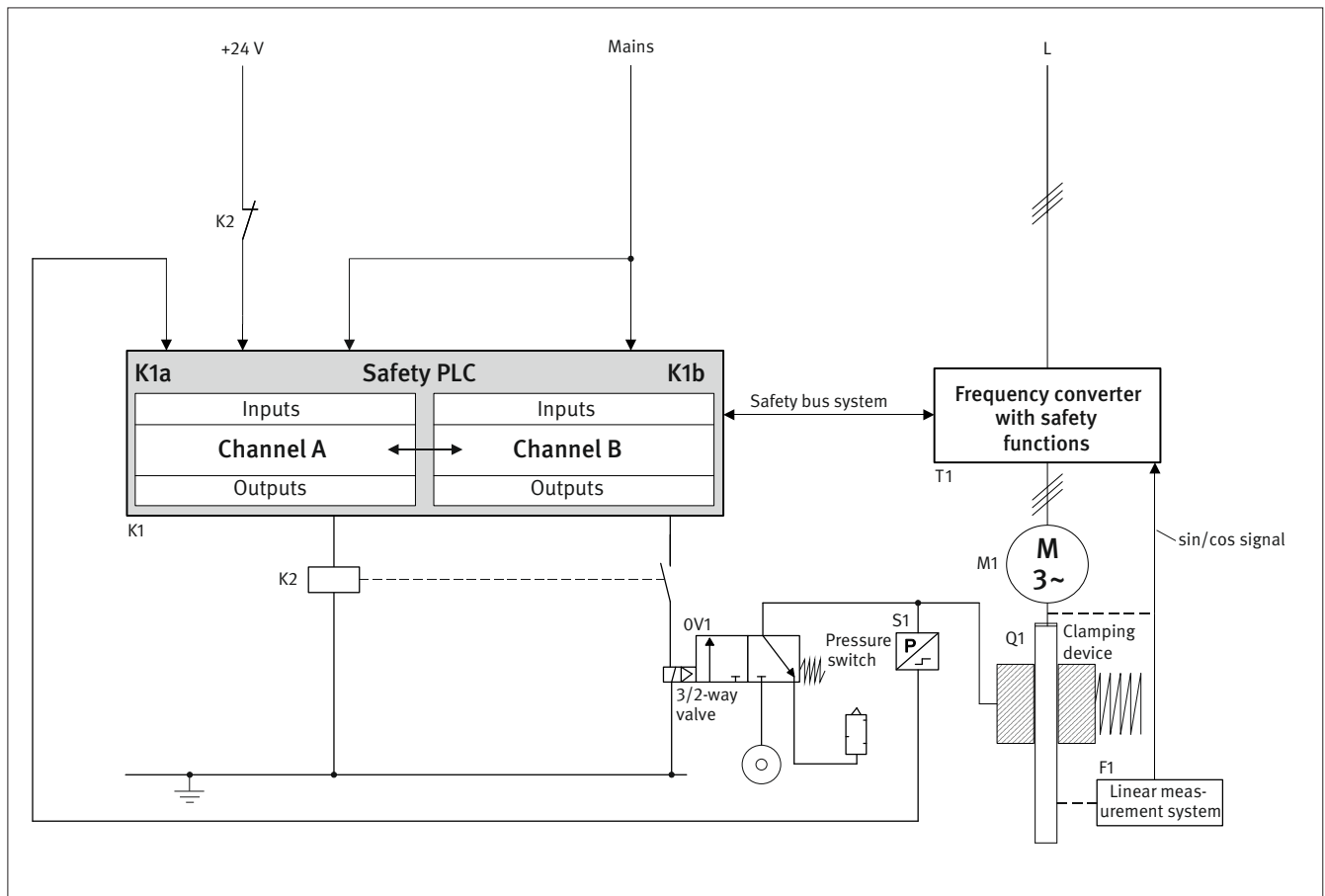
- Fundamental and well-tried safety principles and the requirements of Category B are observed. Protective circuits (such as contact fuse protection, circuit earthing), as described in the first sections of Chapter 8 of BGIA Report 2/2008e, are present.
- Faults in the electrical supply lines must not have dangerous consequences. Faults are detected as they occur, and a safe state is brought about. Cross-circuits and short-circuits must be considered in accordance with EN ISO 13849-2, Table D.4. Alternatively, the conductors must be laid such that fault exclusion is possible for cross-circuits and short-circuits.
- The pressure-sensitive edge S1 satisfies the requirements of EN 1760-2 and has the function of safeguarding pinch and shear points. The pressure-sensitive edge is connected to the control system through the evaluation unit K1. The evaluation unit K1 satisfies the requirements of EN ISO 13849-1 for Category 4, PL e. Faults in the supply lines to the pressure-sensitive edge are detected via the switching device K1, and the switching device de-energizes safely.
- The machine manufacturer must review the suitability of the pressure-sensitive edge for the application concerned (for example for an adequate deformation distance, consideration of the ambient influences and actuation range). The manufacturer of the pressure-sensitive edge confirms a fault exclusion for the specific application concerned for failure of the contacts of the pressure-sensitive edge to open when actuated.
- The drive control T1 features the SS1 safety function.
- The safety PLC K2 and the drive control T1 are safety components for use up to Category 4 and PL e (K2) and Category 3 and PL d (T1). Faults are detected when they occur and the safe state is triggered. The safety PLC K2 and the drive control T1 are connected over a safety bus system for use in PL d in accordance with BGIA Report 2/2008e, Section 6.2.17.
- The user software (SRASW) is programmed in K2 in accordance with the requirements for PL d and the information in Sections 4.6.3 and 4.6.4 of EN ISO 13849-1.

Calculation of the probability of failure

- The manufacturer confirms a fault exclusion for failure of the pressure-sensitive edge S1 to switch when actuated.
- The manufacturer states a PFH of $2 \cdot 10^{-8}$ per hour [M] for the evaluation unit K1.
- The safety PLC K2 has a PFH of $1.0 \cdot 10^{-8}$ per hour [M].
- The drive control T1 is included in the analysis with a PFH of $1.5 \cdot 10^{-8}$ per hour [M] and PL d.
- Since fault exclusion is permissible for S1, and K1, K2 and T1 are encapsulated subsystems, CCF need not be considered.
- For the safety function SF 1, “Limitation of the closing forces of a power-operated door by actuation of a pressure-sensitive edge”, the evaluation yields the following result: the combination of the subsystems yields an average probability of dangerous failure of $4.5 \cdot 10^{-8}$ per hour in the PL e range. Owing to the drive control T1 possessing PL d, the result is PL d for the entire safety function.

Example 14: Safe holding against gravity of a weighted vertical axis – PL c/PL d

Figure B.28:
Schematic circuit diagram of the drive control



Safety functions

- SF1: Safe holding up against gravity in setup and automatic mode (SOS)
- SF2: Safe holding up against gravity in the event of power failure

Function description

- The vertical axis subject to gravity loading is controlled by the safety PLC K1 in conjunction with the frequency converter T1. The safety PLC is a PLC K1a combined with an NC axis control K1b. K1 performs plausibility tests, for example regarding the control pressure of the clamping device Q1 and its actuation.
- The axis is braked in setup and automatic mode by SS1. During the subsequent safe holding up against gravity, the load of the vertical axis is held in position by the integral safety function SOS (safe operating stop: motor is at a halt and withstands external forces) of the frequency converter T1. The position of the load is detected in a two-channel architecture by the linear measurement system F1 and the frequency converter T1, transmitted over the safety bus to the safety PLC K1, and monitored. The safety PLC K1 comprises a PLC (channel A, K1a) and the NC axis control (channel B, K1b), which communicate with each other in a safe arrangement. Any incorrect deviation of the load from the specified position leads to T1 triggering an STO and the pneumatically released clamping device Q1 being engaged by K1 and K2. Following a delay, which is determined by the control chain (K1-K2-OV1-Q1), the axis is halted. The delay in engagement of the clamping device does not give rise to a hazard in this case (minor overrun travel).

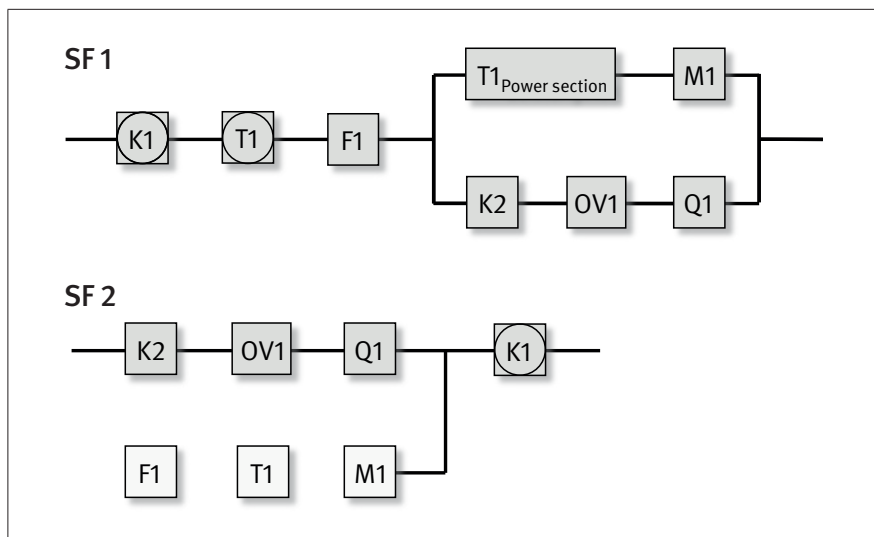


Figure B.29:
Safety-related block diagrams for Example 14

- SF 2, “Safe holding up against gravity in the event of power failure”, refers to the behaviour of the control system in consideration of interruption of the power supply in accordance with EN 12100, Section 6.2.11.5. The interruption of the power supply is detected in K1 (monitoring of the mains voltage). Since the control voltage for K1 possesses an adequate buffer time, the clamping device Q1 is engaged not by the “slow” drop in the output voltage of K1, but as quickly as possible by de-energization of the output signal. Following halting of M1, Q1 prevents dangerous falling of the suspended load on the vertical axis.

Note:

Buffering of the supply voltage for the safety PLC K1 is not required if failure of the supply voltage is detected by the frequency converter T1 and the clamping device is driven directly (for example by SSM). For this purpose however, the control voltage for T1 must be drawn from the intermediate DC circuit.

- Two cases must be distinguished for the system with regard to safe holding against gravity:

1. Setup and automatic mode:

In setup and automatic mode, the function of safe holding up against gravity is assured by the frequency converter T1 in the safety function SF 1 “Safe holding up against gravity in setup and automatic mode (SOS)”.

2. Power failure:

SF 2 is activated when a power failure is detected by the safety PLC K1. In the event of a power failure, the frequency converter T1 is not able to halt the vertical axis, since its control voltage is not generated from the intermediate circuit voltage (i.e. it is not buffered). The safety PLC is supplied from a buffered power supply and causes the spring-operated clamping device Q1 to engage.

In the event of power failure, the clamping device Q1 and actuation by K2 and OV1 constitute a Category 2 system in accordance with EN ISO 13849-1. Testing of the clamping device is required statically every eight hours and dynamically every six months. Testing at the specified intervals is adequate in the present application, since the clamping device engages only in the event of a power failure.

- Test of the clamping device Q1 including actuation by K2 and OV1:

1. static test

Proper operation of the clamping device Q1 including its actuation arrangement is tested daily (i.e. at intervals of eight hours). For the purposes of the test, the clamping device is subjected to 1.5 times the load torque by the linear motor M1. If the load is held within the specified position range, the clamping device is deemed to be properly functional. Should the position leave the

specified range, the clamping device must be checked in accordance with the instruction manual, or if necessary be replaced. The position is determined by means of the linear measurement system F1.

2. dynamic test

The dynamic test is performed at regular intervals under defined speed and mass conditions (the test interval is dependent upon the ambient conditions in the plant but must not exceed six months). Shortly before the braking process is triggered by the clamping device, the torque of the drive motor and the directional control valve are switched off.

The dynamic test of the clamping device Q1 measures the overrun travel. The measured value is compared with the permissible values. Should a measured value exceed the permissible value, the machine must not continue in use. The clamping device must be replaced if necessary.

Note:

The test has the purpose of ensuring that the overrun does not lengthen impermissibly in the course of the service life (for example owing to hardening of the brake linings, or a film of dirt).

- For the sake of clarity, selection of the operating mode is not shown.

Design features

- Fundamental and well-tried safety principles and the requirements of Category B to EN ISO 13849-1 are observed. Protective circuits (such as contact fuse protection, overdimensioning) are present.
- Cross-circuits and short-circuits in electrical supply lines must be considered in accordance with EN ISO 13849-2, Table D.4. Faults are detected as they occur, and a safe state is brought about. Alternatively, the conductors must be laid such that fault exclusion is possible for cross-circuits and short-circuits.
- The safety PLC K1 and the frequency converter with integrated safety functions T1 are safety components for use in PL d which satisfy Category 3 and the relevant product standards. The frequency converter features the safety functions SOS, SS1 and STO.
- The contactor relay K2 features mechanically linked contact elements to EN 60947-5-1, Annex L. The contact position is read back in the safety PLC K1 and checked for plausibility.
- The 3/2-way valve 0V1 features spring return. The fail-safe switching position is reached by removal of the control signal by means of contactor relay K2. Fundamental and well-tried safety principles of design, installation and operation (EN ISO 13849-2) are a precondition.
- The linear measurement system F1 supplies redundant position information (sin/cos) and is integrated into the position control loop. The measurement system is connected to the frequency converter T1. Fault exclusion is assumed for failure of the mechanical mounting of the linear measurement system's detection head and for the loss of the material measure (glass measuring rod). The manufacturer must demonstrate the fatigue strength for the fault exclusions (see also EN 61800-5-2, Table D.16). The manufacturer's respective information on maintenance must also be observed.
- The software (SRASW) for the safety PLC K1 and the frequency converter T1 is programmed in accordance with the requirements for PL d and the information in Section 4.6.3 and where applicable 4.6.4 of EN ISO 13849-1.
- The data bus between T1 and K1 is a safety bus system for use in PL d.
- The supply voltage (mains voltage) is monitored in two-channel architecture in the safety PLC K1.

Remarks

- This example relates to a vertical axis without counterbalancing and that is equipped with a clamping device. A condition is that the motor M1 is capable on its own of generating the torques required for movement of the axis. A pneumatically moveable counterbalance may for example be required when the clamping device is not capable on its own of holding the weight of the suspended axis. In such a case, the counterbalance must also be considered in the analysis.

- In addition, product-specific (type C) standards may describe particular requirements for stopping and holding in the raised position. These requirements take priority over type A and type B standards such as EN ISO 13849-1 (refer to the introductory section of EN ISO 13849-1).
- Comment on the clamping device Q1 in the event of failure of M1:
A failure of the motor is detected before a hazard is able to arise by descent of the suspended load. The clamping device must be rated such that the motor force and load together are always lower than the clamping force generated by the clamping device.

Calculation of the probability of failure

- K1 is a safety PLC. The PFH value is $8.97 \cdot 10^{-8}$ per hour [M]. Category 3 and PL d are confirmed by the manufacturer.
- The frequency converter T1 features the integrated safety functions SOS, SS1 and STO. The PFH value for the safety functions of the frequency converter is $2.31 \cdot 10^{-8}$ per hour [M]. For SF 1 however, the power section of the frequency converter must also be considered in the analysis, since the vertical axis must be actively held in the raised position in order to prevent it from dropping. The power section of T1 is included in calculation of the SF 1 in the form of an estimated $MTTF_d$ of 40 years [A].
- A B_{10d} value of 2×10^6 switching cycles [S] is stated for the contactor relay K2. With daily actuation and performance of the static test on six days and 50 weeks of the year, this yields a nop of 600 switching cycles per year. If 20 actuations are assumed as a result of power failure, the result is a nop of 620 switching cycles per year and an $MTTF_d$ of 32,258 years.
- M1 is a linear motor with insulation class F [3]. The insulation class temperature is 20 K below that specified. As a result, a life of 80,000 hours is assumed for the windings [1]. The daily duty is eight hours. This results in an $MTTF_d$ of 80,000 hours / (8 hours · 365 days) = 27.3 years. It is assumed that winding faults cause the motor M1 to fail dangerously. Consequently, $MTTF_d = MTTF$ is assumed.
- Table C1 of EN ISO 13849-1 states a B_{10d} of 20,000,000 [S] for the pneumatic valve 0V1. At 620 switching cycles per year, this results in an $MTTF_d$ of 322,580 years.
- The clamping device Q1 is a special linear brake (emergency brake with holding brake function for linear movements) with a rating of 200,000 switching cycles [M] for static loads. According to the manufacturer's information, the linear brake must be inspected at intervals of not greater than six months, and cleaned if necessary. Braking force checks (static tests) must be performed every eight hours at 1.5 times the anticipated loading. The manufacturer was consulted regarding the use for emergency-stop brake operations. The rating for emergency-stop (dynamic braking) is 2,000 switching cycles [M] and serves as the estimate for B_{10d} . With a frequency of actuation estimated on the safe side of 20 actuations per year, the $MTTF_d$ is 1,000 years. For SF 2, the clamping device is engineered in a Category 2 architecture. The tests are performed as described above.

Note:

In accordance with EN ISO 13849-1, Section 4.5.4, a demand rate of $\leq 1/100$ of the test rate is a criterion for Category 2, and the $MTTF_{dTE}$ must be greater than $0.5 \cdot MTTF_d$ of the function channel. The test rate (100 times more frequent than the demand for the safety function) is not met in SF 2. An additional 10% was therefore added for the Category 2 subsystem. This corresponds to a worst-case estimate, which is described in the BGIA Report (see BGIA Report 2/2008e, Section 6.2.14, p. 54, and Section 4 of SISTEMA Cookbook 4).

- The manufacturer states a failure rate of $1.5 \cdot 10^{-6}$ per hour [M] for the linear measurement system F1. A division of the faults into safe and dangerous failures is not known. In this case, an estimation is made erring on the safe side in that all possible faults are assumed to be dangerous. Owing to permanent monitoring by the frequency converter T1, the DC is set at 99%. With consideration of the DC of 99%, the resulting probability of dangerous failure is $1.5 \cdot 10^{-8}$ per hour.
- $MTTF_d$ values for the individual blocks are required for quantification of the Category 2 subsystem of SF 2. Since only PFH values are available for T1 and for F1, the assumption that $MTTF_d = 1/PFH$ is approximately valid (refer in this context to SISTEMA Cookbook 4, Section 2). This results in an $MTTF_d$ of 7,610 years for F1.
- For T1 (power section + control), the probability of failure is $MTTF = (1/40 + 1/4,942)^{-1}$ years = 39.6 years.
- A value of 99% can be stated for the DC of the contactor relay K2, since check-back to the safety PLC K1 is always provided.
- A value of 60% is assumed for the DC of the linear motor M1, since testing is performed by way of the process.

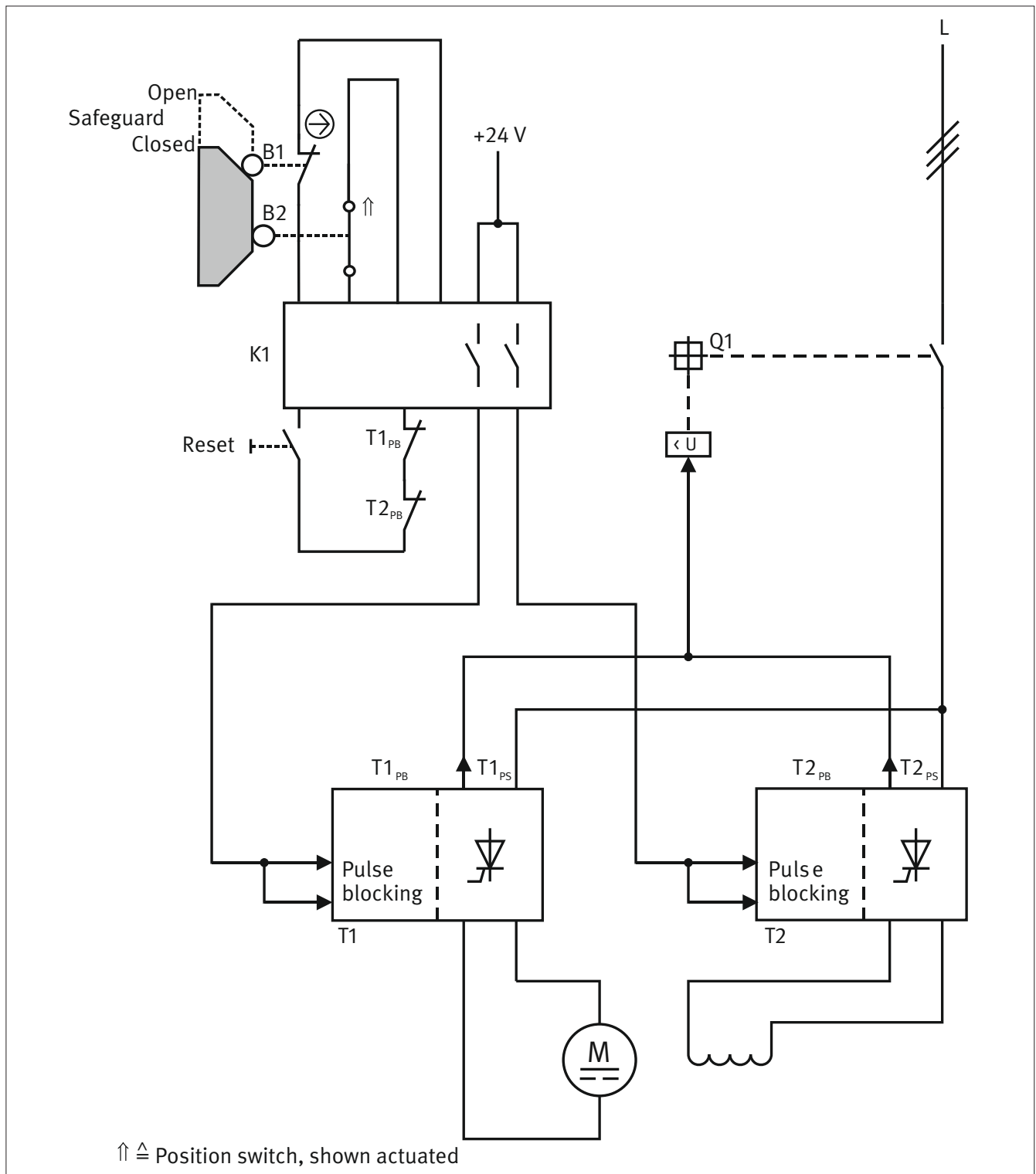
- The serviceability of the pneumatic valve 0V1 is tested by means of the pressure switch S1 (DC = 99%).
- A DC of 60% is assumed for the clamping device Q1.
- Adequate measures are provided against common-cause failure of the subsystem of the position control or de-energization of the SF 1 safety function, comprising T1_{power section}, M1/K2, 0V1, Q1 (65 points): separation (15), protection against overvoltage etc. (15) and protection against environmental conditions (25 + 10).
- For the safety function SF 1 “Safe holding up against gravity in setup and automatic mode (SOS)” the evaluation yields the following result: the combination of the subsystems yields an average probability of dangerous failure of $3.11 \cdot 10^{-7}$ per hour. This satisfies PL d.
- For the safety function SF 2 “Safe holding up against gravity in the event of power failure” the evaluation yields the following result: the combination of the blocks yields an average probability of dangerous failure of $2.14 \cdot 10^{-6}$ per hour. This satisfies PL c.

References

- [1] *Farschtschi, A.*: Elektromaschinen in Theorie und Praxis. 2nd ed. VDE, Berlin 2001
- [2] Expert Committee Information Sheet 005. Gravity-loaded axes – vertical axes. Issue 9/2012. Published by: Fachbereich Holz und Metall der Deutschen Gesetzlichen Unfallversicherung, Mainz.
www.dguv.de/medien/fb-holzundmetall/publikationen/infoblaetter/infobl_englisch/005_vertical-axes.pdf
- [3] EN 60085 (VDE 0301-1) 2008-08: Electrical insulation – Thermal evaluation and designation (IEC 60085:2007)
- [4] *Hauke, M.; Apfeld, R.*: The SISTEMA Cookbook 4. When the designated architectures don't match. Version 1.0. (EN). Published by: Deutsche Gesetzliche Unfallversicherung, Berlin 2012. www.dguv.de, Webcode: e109249

Example 15: STO safety-related stop function in DC drives, triggered by a movable guard – PL d

Figure B.30:
Schematic circuit diagram of the drive control



Safety function

- SF1: Opening of the movable guard leads to STO of the DC drive.

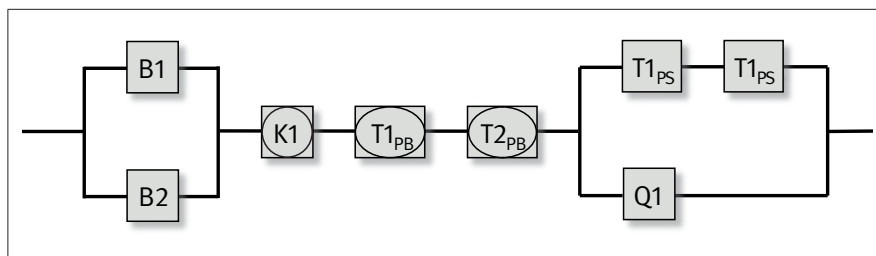


Figure B.31:
Safety-related block diagram for Example 15

Function description

- The hazard point is safeguarded by a movable guard. Opening of the guard is detected by the position switches B1 and B2 and evaluated in a safety module K1. The inputs of the trigger pulse block are each de-energized in the DC chopper converters for the armature current T1 and the excitation field T2 in a two-channel architecture via the enabling paths of K1. This prevents the generation of a torque in the DC motor.
- The function of the DC drive supplied with DC current is controlled by a PLC. The PLC itself is not involved in the safety function, and is not shown here. The schematic diagram (Figure B.30) is limited to the safety-related control, which takes priority over the functional control.
- The DC chopper converters (DC power converters) T1 and T2 each comprise a control section with redundant pulse block T1_{PB} and T2_{PB} and a single-channel power section T1_{PS} and T2_{PS}.
- Faults in the position switches B1 and B2 are detected by the safety module K1.
- Each DC chopper converter is equipped internally with a function for monitoring the pulse block (check-back contacts T1_{PB} and T2_{PB}). In the event of a fault, these functions prevent the drive from restarting, since they are integrated into the return circuit of K1.
- Faults in the power sections of T1 and T2 are detected, and in the event of a fault, a fault signal is output for T1PS/T2PS. These fault signals de-energize the circuit-breaker Q1 on the three-phase side by means of an undervoltage release. Q1 in turn disconnects the DC motor from the mains supply. Q1 is not de-energized with each request for the safety function, but only in the event of faults in the power sections of the DC chopper converters.

Note:

In contrast to three-phase motors, pulse blocking alone is not sufficient for STO on DC motors, since it does not reliably prevent a torque from being generated. Faults in the power thyristors may enable a current to flow that is sufficient to generate a torque, even with pulse blocking. This is the case for example when two relevant thyristors behave as diodes. Consequently, should a fault in the power section of the armature converter result in only the field converter being safely de-energized when the guard is opened, the extreme attenuation of the excitation field can cause the motor to turn when unwanted armature current is flowing. In order to prevent this, the circuit-breaker for the mains supply is de-energized in addition in the event of faults in the power section of a converter. Consequently, the power section of the DC chopper converter must also be included in the safety analysis of the STO.

- Faults in the circuit-breaker Q1 (including faults in the undervoltage release) are detected by manual tests conducted during the regular tests (at least annually).

Design features

- Fundamental and well-tried safety principles and the requirements of Category B are observed. Protective circuits (such as contact fuse protection, earthing of the control circuit), as described in the first sections of Chapter 8 of BGIA Report 2/2008e, are present.
- Cross-circuits and short-circuits in electrical supply lines must be considered in accordance with EN ISO 13849-2, Table D.4. Faults are detected as they occur, and a safe state is brought about. Alternatively, the conductors must be laid such that fault exclusion is possible for cross-circuits and short-circuits. In the example shown, the components K1, T1, T2 and Q1 are located in the same installation compartment. Fault exclusion for short-circuits between conductors is therefore permissible.

- The actuating mechanisms of the electromechanical position switches B1 and B2 must be designed and fitted as specified. Actuating elements and position switches must be secured against displacement. Only rigid mechanical components (not spring elements) may be used. The position switch B1 is a well-tried component to EN ISO 13849-2, Table D.3 with direct opening contacts in accordance with EN 60947-5-1, Annex K.
- The safety module K1 satisfies the requirements of Category 4 and PL e.
- The DC chopper controllers T1 and T2 are products with integrated pulse blocking. The requirements of Category 3 and PL d are satisfied for the pulse blocking. The power section of T1 and T2 must be considered separately.
- The circuit-breaker Q1 is a well-tried component in accordance with EN ISO 13849-2, Table D.3. Q1 (including the undervoltage release) and must be tested regularly by means of a manual test function that is to be implemented. Such a test can for example be performed during the regular test.

Calculation of the probability of failure

- Fault exclusion applies to the direct opening contact of B1.
- A B_{10d} value of 1,000,000 switching cycles [M] is stated for the electrical make contact of position switch B2. At 240 working days, 16 working hours per day and a cycle time of 60 minutes, the result is an n_{op} of 3,840 cycles per year and an $MTTF_d$ of 2,604 years.
- The same applies to the mechanical part of each position switch B1 and B2. At a B_{10d} value of 1,000,000 switching cycles [M] and an n_{op} of 3,840 cycles per year, the $MTTF_d$ is 2,604 years.
- The safety module K1 satisfies the requirements for Category 4 and PL e. The PFH is $2.31 \cdot 10^{-9}$ per hour [M].
- The control section of the DC chopper converters with pulse blocking $T1_{PB}$ and $T2_{PB}$ can be regarded as an encapsulated system. It satisfies the requirements for Category 3 and PL d. The PFH in each case is $3.16 \cdot 10^{-7}$ per hour [M].
- The power section of the DC chopper converters $T1_{PS}$ and $T2_{PS}$ is implemented in a single-channel architecture; the $MTTF_d$ for each DC chopper converter is 300 years [M].
- A B_{10d} of 5,000 switching cycles [M] is stated for the circuit-breaker Q1. An n_{op} of 100 cycles per year yields an $MTTF_d$ of 500 years.
- The DC for the position switches B1 and B2 is 99%, owing to the plausibility check by the safety module K1.
- The diagnostic functions for the power section in the DC chopper converters $T1_{PS}$ and $T2_{PS}$ are performed continually within the device with a DC of 99%. The circuit-breaker Q1 is de-energized as soon as a fault is detected in $T1_{PS}$ or $T2_{PS}$. The fault response time is so short that no hazard arises in this case. Loss of the safety function between the tests is not possible. Single-fault tolerance in this subsystem is thus assured, and the requirements of Category 3 in this respect are satisfied.
- Owing to the manual tests performed during regular testing, the DC for the circuit-breaker Q1 is 90%.
- Adequate measures against common-cause failure are taken for the subsystem of the position switches B1/B2 (70 points): separation (15), protection against overvoltage etc. (15), use of well-tried components (5) and protection against environmental conditions (25 + 10).
- Adequate measures against common-cause failure are taken for the subsystem of the DC chopper converters $T1_{PS}/T2_{PS}$ and circuit-breaker Q1 (85 points): separation (15), diversity (20), protection against overvoltage etc. (15) and protection against environmental conditions (25 + 10).
- The evaluation for the safety function is as follows:

The subsystem B1/B2 satisfies Category 3 with a high $MTTF_d$ per channel (100 years) and a high DC_{avg} (99%). This yields an average probability of dangerous failure of $2.47 \cdot 10^{-8}$ per hour. This satisfies PL e.

The subsystem of T1_{ps}/T2_{ps}/Q1 satisfies Category 3 with a high MTF_d per channel (100 years) and a medium DC_{avg} (97%). This yields an average probability of dangerous failure of $2.89 \cdot 10^{-8}$ per hour. This satisfies PL e.

For the safety function SF 1 the combination of the subsystems yields an average probability of dangerous failure of PFH = $6.88 \cdot 10^{-7}$ per hour. This satisfies PL d.

Annex C:

Expert committee information sheets

The following information sheets issued by the DGUV Expert Committee Woodworking and Metalworking can be downloaded from the DGUV website (see Table C.1).

Table C.1:
Overview of the expert committee information sheets in this annex

Number and title of the information sheet	Web URL
005 Gravity-loaded axes – vertical axes	www.dguv.de/medien/fb-holzundmetall/publikationen/infoblaetter/infobl_englisch/005_vertical-axes.pdf
050 Fluid engineering power elements – Hydraulic and pneumatic motors and cylinders	www.dguv.de/medien/fb-holzundmetall/publikationen/infoblaetter/infobl_englisch/050_fluid-power-elements.pdf

Gravity-loaded axes

Vertical axes

While it can be assumed that during horizontal movements in the automatic production no hazards to persons occur due to gravity in the de-energized state, for vertical movements, however, the risks of unintended gravity descent have to be considered in the risk assessment. These hazards particularly become obvious with linear robots (Fig. 1) for the handling of heavy parts, e. g. engines or gears but also with jointed-arm robots or inside machines, e.g. at vertical axes of machining or turning centers. If the existing brakes do not provide sufficient protection against unintended gravity descent, control measures can contribute to reduce the risk of hazard.



Figure 1: Vertical axes

Table of Contents

- 1 Motor brakes
- 2 Risk assessment and control measures
- 3 Self-acting (automatic) tests for upgrading existing (motor) brakes
- 4 Brakes with emergency stop features
- 5 Systems already placed on the market
- 6 Brakes as safety component
- 7 Summary and limits of application

1 Motor brakes

During the manufacturing process, vertical axes at a standstill are usually held solely by the brake which is installed in the drive motor. Mechanical wear or fouling by oil may cause the braking moment of the brakes to fall below its nominal value which may result in an unintended gravity descent or the fall down of the axis.

From the occupational safety point of view, the cases have to be considered in which persons have access to the danger zones and a full-time or a temporary stay under the axis, e.g. for feeding, setting, maintenance activities etc. is possible. If a failure of the holding brakes cannot be excluded in such situations, measures for a risk reduction shall be taken.

2 Risk assessment and control measures

According to Machinery Directive [1] Annex I, every machine manufacturer is obliged to prepare a risk assessment. A particular standard for assessing risks at vertical axes does not exist. DIN EN ISO 12100 [2] provides general information for carrying out the risk assessment at machines including the identification of hazards.

Annex B of DIN EN ISO 12100 provides a useful table indicating possible hazards which have to be considered with machines, including those due to gravity. Depending on the practical case of application and the risk to be reduced, different technical safety devices are suitable to prevent the unintended gravity descent of vertical axes (see table 3).

The examples indicated in table 1 are intended to be a guidance for the risk assessment for such systems. By presenting typical hazardous situations, adequate technical and organizational measures are proposed in order to prevent unintended gravity descent. Besides the measures shown in table 1, there exist of course the relevant EC directives and standards specifying further requirements for occupational safety for the machinery in question, the validity of which remains unaffected.

3 Self-acting (automatic) tests for upgrading existing (motor) brakes

According to the principles of the risk analysis, the summary in Table 1 considers the duration of stay, the severity of the possible injury and the probability of the occurrence of a hazardous situation. Therefore, redundant measures according to DIN EN ISO 13849-1 category 3 are proposed for highly exposed workplaces, which require a high duration of stay or frequent access [3]. Further explanations for implementing the measures according to category 3 are given in table 2.

For other activities in case of which e.g. a protective design prevents the access underneath the vertical axis or the probability of the occurrence of a hazardous situation and the duration of stay is less, a cyclic test of the single motor brake (brake test) can be a very effective measure. For this, a test moment is applied to the brake, e.g. motor brake. This test should be carried out according to the requirements of DIN EN ISO 13849-1, category 2 (see table 2). I.e. the test shall take place automatically during normal production, e.g. during a process-related stop, in case of a change of the mode of operation or similar. If this is not possible, the test shall be carried out prior to releasing access by a guard with guard locking at the latest.

Note:

According to DIN EN ISO 13849-1, the test rate for control systems of category 2 (checking) has to be estimated a 100 times more frequent than the demand upon the safety function. Due to the risks of vertical axes, i.e. particularly due to the accident history, such a high test rate is considered to be actually not required. Therefore, a calculation of the Performance Level according to the simplified procedures of DIN EN ISO 13849-1 is not possible and can be omitted in this particular case according to DIN EN ISO 13849-1, clause 6.2.2.

4 Brakes with emergency stop features

If the brakes should not only safely maintain the load in a raised position but should also be provided with emergency stop features (e. g. in case of protective stop actuation), it should be pointed out that the self-acting static brake tests do not provide sufficient proof with regard to inadequate or decreasing emergency stop features. This means that despite a successfully performed static brake test, a slightly extended overrun in case of emergency stop is possible since the physical characteristics of the brake have different dynamic and static effects. The risk assessment of the machine manufacturer must indicate in such cases if a slightly different overrun in the course of the operating life represents an unacceptable risk.

Note:

In order to refrain from providing emergency stop features to the brakes, a category 1 stop (guided stopping) should be preferred in case of a protective stop.

5 Systems already placed on the market

The above mentioned measures for the improvement of occupational safety at vertical axes are primarily suitable for application at systems which are intended to be put on to the market.

Machinery and systems (used systems) that are already on the market shall meet the requirements of the Betriebssicherheitsverordnung (Ordinance on Industrial Safety and Health) [4] and the accident prevention regulations of the institutions for statutory accident insurance and prevention (Unfallverhütungsvorschriften der Berufsgenossenschaften).

The technical safety measures which have to be specified correspondingly must not necessarily reach the same level as those specified for new machinery according to the Machinery Directive. The decisive factor is the state of the art at the time when the machine is put on the market for the first time and the development of the state of the art by the accident prevention regulations.

In particular, safety measures for risk reduction by control have mainly been established owing to recent findings. Measures by control cannot be easily retrofitted with the existing hard- and software. The employer is required to take measures according to § 4 of the BetrSichV (Ordinance on Industrial Safety and Health) in order to keep the hazard as low as possible. If the risks cannot be adequately reduced by technical safety measures, organizational measures have to be taken which contribute to the risk reduction (avoidance of presence underneath the axis, support etc.). Furthermore, employees have to be enabled by relevant instructions to assess hazards adequately. An essential element in this connection should also be the provision of periodic tests for detecting hazardous wear conditions. The kind, the scope, the test periods and the skill level of the testing personnel have to be specified by the user. The skilled person shall have sufficient knowledge and experience in the field of the work equipment to be tested and must be familiar with the relevant national occupational health and safety regulations, BG-rules and generally accepted rules of technique (e.g. regulations determined by the committee for rules for Operational Reliability, DIN standards, VDE regulations, technical regulations of other member countries of the European Union or other contracting states of the agreement about the European Economic Area) so that he is able to assess the safe state of the work equipment.

6 Brakes as safety component

Brakes for holding up vertical axes can be classified as safety component according to the Machinery Directive 2006/42/EC, article 2 no. c). The precondition is that the brakes are put on the market separately, i.e. independent of the machine or the drive motor. In this case, the conformity assessment procedures which apply to machines have to be used, amongst others, EC Declaration of conformity and EC mark.

These provisions do not apply to motor brakes since they are not separately put on the market due to the fact that they are built into the drive motor.

In this connection it should be pointed out to the fact that by means of tests and certifications according to test principle no. GS-MF-28 the proof of an operation-proven brake (category 1, Plc) can be certified [5].

7 Summary and limits of application

The measures mentioned in this division information sheet for occupational safety represent the results of detailed discussions in the woodworking and metalworking division (Fachbereich Holz und Metall) concerning an improved occupational safety for activities at or near vertical axes. They include practical technical control measures against unintended descent due to gravity. This information sheet is based on experience of manufacturers of industrial robots including linear robots and handling systems, of drive and control system manufacturers and the users of such systems, particularly in the automotive engineering and on experience of the woodworking and metalworking division. Furthermore, the results of the discussions have been considered at the Association of German Machine Tool Manufacturers (VDW).

This information sheet indicates typical hazardous situations in connection with vertical axes and provides suitable approaches for risk reduction by technical control measures. Other measures against unintended gravity descent which are not mentioned in this information sheet remain unaffected.

Subject of consideration are electro-motive driven vertical axes as well as inclined axes with motor-integrated brake or external brake which could descent in case of failure due to gravity. Relevant requirements stated in EC Directives and other rules of Technique remain unaffected. The developments of new technologies as well as equivalent solutions are not impeded by this information sheet. The applicability of the findings to machinery and systems with similar hazards is not excluded.

The measures may preferably be applied for systems which are put onto the market for the first time. Particularities at systems which are already placed on the market will be dealt with separately. The contents of this information sheet are intended to be included in the technical rules or have already been included.

The "Fachbereich Holz und Metall" (Woodworking and metalworking division) is composed of representatives of the German Social Accident Insurance Institution, federal authorities, social partners, manufacturers and users of machines. It is based on experience gathered by the FB Holz und Metall in the field of vertical axes and in particular in the field of gravity-loaded axes.

This division information sheet has been prepared by the metalworking and woodworking division, subdivision "machinery, systems, automation and design of manufacturing systems". This division information sheet replaces information sheet, draft 07/2011. Further information sheets published by the woodworking and metalworking division may be downloaded from the Internet [6].

Concerning the aims of the division information sheets, see division information sheet no. 001.

Bibliography:

- [1] Directive 2006/42/EC (Machinery directive) of the European Parliament, L157, 2006-06-09.
- [2] DIN EN ISO 12100 Safety of machinery - General principles for design - risk assessment and risk reduction March 2011.
- [3] DIN EN 13849-1 Safety of machinery - Safety-related parts of control systems - Part 1 - General principles for design, December 2008.
- [4] Verordnung über Sicherheit und Gesundheitsschutz bei der Bereitstellung von Arbeitsmitteln und deren Benutzung bei der Arbeit, über die Sicherheit beim Betrieb überwachungsbedürftiger Anlagen und über die Organisation des betrieblichen Arbeitsschutzes (Betriebssicherheitsverordnung – BetrSichV). BGBl. I S. 3777 - 27. September 2002, edition 2004
- [5] Prüfgrundsatz Nr. GS-MF-28 Notfallbremsen mit Haltebremsfunktion für lineare Bewegungen. Prüf- und Zertifizierungsstelle Maschinen und Fertigungsautomation im DGUV Test, Wilhelm-Theodor-Röhmed-Strasse 15, 55130 Mainz. (Inhaltlich gleichlautend vorhanden bei IFA).
- [6] Internet: www.dguv.de/fb-holzundmetall [Publikationen](#)

Picture credits:

The pictures mentioned in this division information sheet have been kindly provided by: FB Holz und Metall

Publisher:

Fachbereich Holz und Metall der DGUV
Sachgebiet Maschinen, Anlagen, Fertigungsautomation und -gestaltung
Postfach 37 80
55027 Mainz

Woodworking and Metalworking Division of DGUV
Subdivision machinery, plants, automation and design of manufacturing systems

Table 1: Typical hazardous situations and possible protective measures

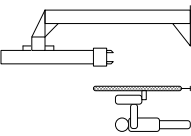
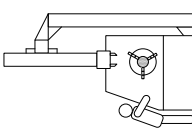
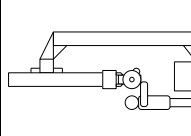
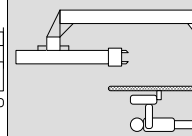
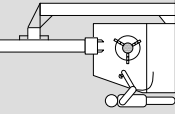
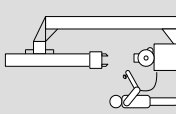
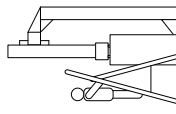
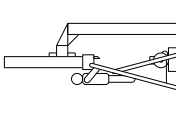
Mode of operation	Hazardous situation/ Intended use	Safety measures	
		Technical	Organizational
Automatic- Manual intervention A1	 <p>During manual intervention, the vertical axis is located in a safe position for the operator (access-protected area).</p>	<ul style="list-style-type: none"> - Guards have to be provided with guard lockings. - In case of access, unintended start of the vertical axis shall be safely prevented. 	<ul style="list-style-type: none"> - Warning sign mounted at the machine / system: „ Do not stay underneath the vertical axis!“ - Point out to hazards due to vertical axis and suspended load in the operating instructions.
A2	 <p>The vertical axis is located within the hazardous area. Staying under the vertical axis with the whole body is prevented by the machine / system design and not intended. A hazard exists for the upper limbs in case of a short duration of stay.</p>	<ul style="list-style-type: none"> - Cyclic test of the braking device by the machine control according to DIN EN ISO 13849-1, category 2 (see table 2). - Unexpected start of the vertical axis shall be safely prevented¹⁾. 	<ul style="list-style-type: none"> - Warning sign mounted at the machine / system: „ Do not stay underneath the vertical axis!“ - Point out to hazards due to vertical axis and suspended load in the operating instructions as well as to the need for skilled personnel. - Commissioning test to be carried out by the system manufacturer by means of a form with regard to the effectiveness of the brake test.
A3	 <p>The vertical axis is located within the hazardous area. Staying under the vertical axis cannot be prevented (e.g. intended feeding or assembling activities).</p>	<ul style="list-style-type: none"> - Redundant device for fall-down protection according to DIN EN ISO 13849-1, category 3, PLc (see table 2). - Unexpected start of the vertical axis shall be safely prevented¹⁾. 	<ul style="list-style-type: none"> - Warning sign mounted at the machine / system: „ Do not stay underneath the vertical axis!“ - Point out to hazards due to vertical axis and suspended load in the operating instructions as well as to the need for skilled personnel. - Limit stay under the vertical axis as far as possible.
Set-up or programming E1	 <p>The vertical axis is located in a safe position for the operator during set-up (access-protected area).</p>	<ul style="list-style-type: none"> - Guards have to be provided with guard lockings - In case of access, unintended start of the vertical axis shall be safely prevented). 	<ul style="list-style-type: none"> - Warning sign mounted at the machine / system: „ Do not stay underneath the vertical axis!“ - Point out to hazards due to vertical axis and suspended load in the operating instructions.

Table 1 (continued)

Mode of operation	Hazardous situation/ Intended use	Safety measures	
		Technical	Organizational
E2	<p>The vertical axis is operated in the set-up mode and is located within the hazardous area. Staying under the vertical axis with the whole body is prevented by the machine / system design and not intended. A hazard exists for the upper limbs for a short duration of stay.</p> 	<ul style="list-style-type: none"> - Measures for set-up operation according to relevant standard, e.g. DIN EN ISO 10218-1, DIN EN 12417 (lockable mode selection switch, reduced speed + enabling device/ safely reduced speed ...) - Cyclic test of braking device by the machine control system according to DIN EN ISO 13849-1, category 2 (see table 2). 	<ul style="list-style-type: none"> - Warning sign mounted at the machine / system: „Do not stay underneath the vertical axis!“ - Point out to hazards due to vertical axis and suspended load in the operating instructions as well as to the need for skilled personnel. - Commissioning test to be carried out by the system manufacturer by means of a form with regard to the effectiveness of the brake test.
E3	<p>The vertical axis is operated in the set-up mode and is located within the hazardous area. Staying under the vertical axis with the whole body cannot be prevented, however during a short duration of stay.</p> 	<ul style="list-style-type: none"> - Measures for set-up operation according to relevant standard, e.g. EN ISO 10218-1, DIN EN 12417 (lockable mode selection switch, reduced speed + enabling device/ safely reduced speed ...) - Cyclic test of braking device by the machine control system according to DIN EN ISO 13849-1, category 2 (see table 2). - If, in exceptional cases a high duration of stay can be expected in the hazardous area, and if staying under the vertical axis cannot be avoided, measures according to DIN EN ISO 13849-1, category 3 have to be provided (see table 2). 	<ul style="list-style-type: none"> - Warning sign mounted at the machine / system: „Do not stay underneath the vertical axis!“ - Point out to hazards due to vertical axis and suspended load in the operating instructions as well as to the need for skilled personnel. - Commissioning test to be carried out by the system manufacturer by means of a form with regard to the effectiveness of the brake test.
Maintenance, repair, cleaning	<p>Maintenance, cleaning and repair works are carried out at or next to the vertical axis. Safe support of the vertical axis and / or suspension with reasonable effort is feasible.</p> 	<ul style="list-style-type: none"> - Observe the regulations in force for maintenance/ repair/ cleaning, e.g. lockable mains switch. - Support or, as far as still possible, move to lowest end position 	<ul style="list-style-type: none"> - Warning sign mounted at the machine / system: „Do not stay underneath the vertical axis!“ - Point out to hazards due to vertical axis and suspended load in the operating instructions - Describe measures for safe support - Disconnect and lock mains switch
W2	<p>Maintenance, cleaning and repair works are carried out at or next to the vertical axis. Safe support and / or suspension of the vertical axis is not feasible with reasonable effort.</p> 	<ul style="list-style-type: none"> - Observe the regulations in force for maintenance/ repair/cleaning, e.g. lockable mains switch. - Device to be operated automatically or electromechanically resp. manually for safe arresting of the axis in the defined positions, e.g. arresting device. - Clear marking of the positions „interlocked/unlocked“. - Interrogation of positions by the control „interlocked/ unlocked“ and interlocking with drive control. 	<ul style="list-style-type: none"> - Warning sign mounted at the machine / system: „Do not stay underneath the vertical axis!“ - Point out to hazards due to vertical axis and suspended load in the operating instructions - Describe measures for the use of the devices for safe arresting (e.g. arresting device) - Disconnect and lock mains switch

¹⁾ Note: The control category and the Performance Level (PL) with regard to protection against unexpected start-up can usually be taken from the applicable product standards. In most cases, category 3, PLd applies.

Table 2: Examples of measures against unintended descent of gravity-loaded axes (vertical axes) according to DIN EN ISO 13849-1 category 2 and 3.

1 General requirements	
1.1	The mechanical parts of power transmission and the safety devices shall be at least designed to withstand the occurring static and dynamic stresses at double weight load.
1.2	If a brake fault is detected by control means according to DIN EN ISO 13849-1, category 2 or 3, the vertical axis shall immediately approach a safe position in case of protective devices or unlocked protective doors, as far as this is still possible. The indications given by the machine control shall request for brake repair. In case of guards with locked protective doors, a safe position shall not be approached until an unlock demand signal has been given.
1.3	One or several warning signs shall be visibly fixed at the machine pointing out to hazards due to vertical axes and suspended loads.
1.4	The operating instructions shall describe measures for fall-down protection. They shall point out to hazards due to vertical axes and suspended loads.
1.5	Measures against unauthorised access to safety relevant programme parts of the control system shall be provided, e.g. by one of the following measures: <ul style="list-style-type: none"> - write protection for relevant parts of the programme - password protection - modification protection by means of a key switch
1.6	In order to prevent unnecessary wear of the brakes, preference should be given to stop category 1 (controlled stopping) - if permitted by the risk assessment - according to EN 60204-1, for operational stop and for emergency stop, instead of stopping with mechanical brakes.
2 Measures according to DIN EN ISO 13849-1, category 2 (cyclic brake test)	
2.1	The brake test shall be carried out in a safe position for the operator, e.g. safe parking position, closed guard.
2.2	The brake test shall become effective automatically during normal operation of the vertical axis, however, after 8 hours or a shift at the latest. For systems to which access is safely prevented, (e.g. by means of protective doors with guard locking), the test may be effected immediately prior to access after unlock demand signal. Note: According to DIN EN ISO 13849-1, the test rate for control systems of category 2 (checking) has to be estimated a 100 times more frequent than the demand upon the safety function. Due to the risks of vertical axes, i.e. particularly due to the accident history, such a high test rate is considered to be actually not required. Therefore, a calculation of the Performance Level according to the simplified procedures of DIN EN ISO 13849-1 is not possible and can be omitted in this particular case according to DIN EN ISO 13849-1, clause 6.2.2.
2.3	By the brake test it shall be established, that at least the maximum static weight of the load of the axis occurring in the case of application is held safely. The level of the test moment has to be selected accordingly, i.e. 1,3-times the load torque. If several brakes are applied in a parallel manner, (e.g. two brakes) this is considered to be fulfilled if the braking devices are tested separately one after the other on the simple weight load.
2.4	In order to ensure its total effectiveness, the test moment shall be applied over a sufficient time period.
2.5	After repair of a defective brake, a brake test shall be forced by the control system and completed successfully prior to further operation.
2.6	As to the effectiveness of the brake test, an acceptance test at the commissioning of the machine shall be carried out and recorded. During this acceptance test, a failure condition of the brake device shall be simulated and the corresponding fault reaction shall be checked. For this acceptance test, the machinery manufacturer shall provide a form and prescribe the need for skilled personnel. The acceptance test shall be carried out with a reasonable effort.
3 Measures according to DIN EN ISO 13849-1, category 3 (redundant measures for fall-down protection):	
3.1	Devices for holding the vertical axis shall be of redundant design (see also table 3: Assignment of common braking devices to the individual modes of operation). If devices are applied which are not considered in table 3, they have to be classified logically according to table 1.
3.2	Measures for partial fault detection according to DIN EN ISO 13849-1 category 3 PLC shall be provided. Those measures include:
3.2.1	For electronic signal processing units: compilation of measures for detecting and controlling systematic and random faults.
3.2.2	Evaluation of signal states of sensors and actuators and signal processing units. Fault conditions shall result in a fail safe reaction
3.2.3	If a continuous state monitoring of parts of the control system is not feasible, forced dynamizations shall be provided. E.G.: since motor brakes in general do not dispose of reliable signal outputs with regard to the brake state „open/closed“, a forced dynamization according to 2 (cyclic brake test) may be provided as measure for fault detection for the motor brake, for the case that one channel of the dual channel holding system with motor brake is implemented.

Table 3: Assignment of common braking devices to the individual modes of operation

Design of braking device(s)	Suitable for mode of operation A1 During manual intervention, the vertical axis is located in a safe position for the operator within the hazardous area (in waiting position) or in an access-protected area.	Suitable for mode of operation A2 The vertical axis is located within the hazardous area. Staying under the vertical axis is prevented by the machine / system design. A hazard exists for the upper limbs.	Suitable for mode of operation A3 The vertical axis is located within the hazardous area. Staying under the vertical axis cannot be avoided.	Suitable for mode of operation E1 The set-up mode and is located during manual intervention in a safe position for the operator within the hazardous area or in an access-protected area. Staying under the vertical axis is not required for technical reasons.	Suitable for mode of operation E2 The vertical axis is operated in the set-up mode and is located within the hazardous area. Staying under the vertical axis is prevented by the machine / system design. A hazard exists for the upper limbs.	Suitable for mode of operation E3 The vertical axis is operated in the set-up mode and is located within the hazardous area. Staying under the vertical axis cannot be prevented.	Suitable for mode of operation W1 Maintenance, cleaning and repair works are carried out at the vertical axis. Safe support of the vertical axis is feasible.	Suitable for mode of operation W2 Maintenance, cleaning and repair works are carried out at the vertical axis. Safe support of the vertical axis is not feasible.
V0 Holding brake	✓	-	-	✓	✓	✓	-	-
V1 Holding brake with cyclic test	✓	✓	-	✓	✓	✓	-	-
V2 Holding brake with safety-related control and drives	✓	✓	✓*	✓	✓	✓	-	-
V3 Holding brake + second brake	✓	✓	✓	✓	✓	✓	-	-
V4 Safe brake	✓	✓	✓	✓	✓	✓	✓	✓
V5 Holding brake + mechanical counterweight	✓	✓	✓	✓	✓	✓	-	-
V6 Support or mechanical lock	-	-	-	-	-	-	✓	✓
V7 Holding brake + hydraulic/pneumatic counterweight	✓	✓	-	✓	✓	-	-	-
V8 Holding brake + hydraulic counterweight with brake valve	✓	✓	✓	✓	✓	✓	✓	✓
V9 Holding brake + safe clamping device	✓	✓	✓	✓	✓	✓	✓	✓
V10 Hydraulic/pneumatic axis + mechanical counterweight	✓	✓	✓	✓	✓	✓	-	-
V11 Hydraulic/pneumatic axis + hydraulic/pneumatic counterweight	✓	✓	-	✓	✓	-	-	-

* V2 only permitted in mode of operation A3 with additional protection in case of power failure.

Fluid engineering power elements

Hydraulic and pneumatic motors and cylinders

This Information Sheet contains guidance on the proper approach to fluid engineering power elements (e.g. motors, cylinders) in machinery. It is intended to provide information to designers and users of machines which fall within the scope of the European Machinery Directive [1].

The DIN EN ISO 13849-1 [2] defines design guidelines for safety-related parts of machine control systems. In accordance with the scope of the standard, the safety function begins at the point where the safety-relevant signals are generated and ends at the outputs of the power elements (valves).



Figure 1: Power element *cylinder* on a test machine

1 Power Elements

Fluid engineering power elements such as motors and cylinders are outside of the scope of DIN EN ISO 13849-1 and are thus not regarded as safety-related parts of a control system (SRP/CS).

If hazardous situations occur in the non-energized state (e.g. hazardous movement of the power element due to the effect of external forces), additional safety features must be added to the power elements, e.g. by using pilot operated check valves, brakes or holding devices. See section 2 and 3 for more information. Power elements (e.g. motors and cylinders) are not included in the determination of the Performance Level (PL) for a safety function.

Contents

- 1 Power Elements
- 2 External forces
- 3 Additional safety requirements of power elements
- 4 Fluctuation, loss and restoration of hydraulic or pneumatic energy
- 5 Summary and limits of applicability

A determination must be made for each application on a case-by-case basis whether additional hazards exist or can be excluded. The requirements which apply to specific equipment as defined in C-standards must also be taken into account.

NB:

Fluid engineering power elements such as motors and cylinders are outside of the scope of DIN EN ISO 13849-1 and are thus not regarded as safety-related parts of a control system (SRP/CS).

2 External Forces

If external forces act on the power elements, e.g. on gravity-loaded axes (rotary axes with eccentric load moments, vertical axes, etc.), additional components may have to be provided such as e.g. a mechanical brake.

The power elements must be included in the risk assessment. If there is good reason to exclude the possibility of failure (e.g. adequate dimensioning), there is no need for further measures.

Due to the inherent nature of the design, internal leakage must be considered on hydraulic motors.

NB:

The suitability of the hydraulic motor to keep loads from falling must be verified.

When evaluating potential failure modes, appropriate specific guidelines may be used such as BIA fault list 340225 for hydraulic and pneumatic components. The list can be found in BIA Report 6/97 [4].

3 Additional safety requirements of power elements

If a component such as a check valve, a load lowering valve, a load holding valve or line burst valve is used solely to provide protection on a gravity-loaded axis in case a line ruptures and if it is not directly involved in the execution a safety function as defined in DIN EN ISO 13849-1, only the control valve (direction valve with neutral position/ all ports are closed) for the power element and not the component must be included in the evaluation of the safety function. The same applies to the use of a holding device (clamp head) to statically keep the load up if a line ruptures.

If on the other hand, a brake on the piston rod provides controlled braking or blocking of hazardous motion of a power element (e.g. motor or cylinder), both the brake control valve and the brake itself must be included in the DIN EN ISO 13849-1 based evaluation of the control system. For example $BT0_d$ values are needed both for a brake and the brake control mechanism (e.g. valve).

4 Fluctuation, loss and restoration of hydraulic or pneumatic energy

Fluctuation, loss and restoration of energy must not result in hazardous motion of the power element (e.g. lowering of the load). This is required anyway by the Machine Directive and harmonized standards.

Note:

DIN EN ISO 13849-1 Section 5.2.8 requires that safety-related parts of the control system must continue to provide or induce output signals which enable other parts of the machine to remain in a safe state.

5 Summary and limits of applicability

This information sheet is based on experience and knowledge gathered by the FA MFS - expert committee "Mechanical engineering, manufacturing systems, steel construction". It is based on lessons learned from practical experience in the outfitting of machines and systems with hydraulic and pneumatic control systems.

The Hydraulic and Pneumatic Working Group at the statutory accident insurance and prevention institutions in Germany (BG) contributed to the preparation of this information sheet. It is intended to provide information for designers and users of machinery within the scope of the European Machinery Directive and to draw attention to the approach that should be taken with fluid engineering power elements (e.g. motors, cylinders).

The expert committee "Mechanical engineering, manufacturing systems, steel construction (FA MFS - Fachausschuss Maschinenbau, Fertigungssysteme, Stahlbau) is composed of representatives of the statutory accident insurance and prevention institutions in Germany (Berufsgenossenschaften), federal authorities, social partners, manufacturers and users.

The provisions according to individual national laws and ordinances remain unaffected by this information sheet. The requirements of legal provisions apply without reservation. In order to get detailed information, it is necessary to read the relevant wording of the provisions.

The present document is the translation of the German information sheet No. 050, edition of 03/2011. The translation into English was supported by Bosch Rexroth AG.

Other FA MFS information sheets are available for download on the Internet [5].

Bibliography:

- [1] Directive 2006/42/EC (Machinery Directive) Official Journal of the European Union No. L 157/24, 9.6.2006 with Corrigendum in Official Journal L76/35, 16.3.2007.
- [2] DIN EN ISO 13849-1 Safety of machinery – Safety-related parts of control systems – Part 1: General principles for design, 2008-12
- [3] DIN EN ISO 13849-2 Safety of machinery – Safety-related parts of control systems – Part 2: Validation, 2008-09
- [4] BIA Report 6/1997, free download at: <http://www.dguv.de/lifa/de/pub/rep/pdf/rep02/biar0697/rep697.pdf>
- [5] Internet: www.fa-mfs.bghm.de oder www.bghm.de Webcode: <97>

Picture credits:

Figure 1: This photo was kindly provided for publication in this Expert Committee Information Sheet by:
 Institut für Arbeitsschutz (IFA)
 der Deutschen Gesetzlichen Unfallversicherung (DGUV),
 53754 Sankt Augustin,
 Germany

Publisher:

Fachausschuss
 Maschinenbau, Fertigungssysteme, Stahlbau
 Postfach 37 80
 55027 Mainz
 Germany

Note: For objectives of the expert committee information sheet see expert committee information sheet No. 001.

Annex D:

Index of abbreviations

Table D.1 contains the abbreviations used in this report; Table 1 (see Page 13) contains the abbreviations and further information on the safety functions in EN 61800-5-2.

Table D.1:
Abbreviations used in this report

Abbreviation	Designation
[A]	Assumed B_{10d} or $MTTF_d$ values
[D]	B_{10d} or $MTTF_d$ values from databases
[M]	B_{10d} or $MTTF_d$ values based upon manufacturers' information
[S]	B_{10d} or $MTTF_d$ values based upon information listed in EN ISO 13849-1
B_{10d}	Nominal life: the average number of switching operations/cycles after which 10% of the units under analysis have failed
BIA	BG Institute for occupational safety (today: IFA)
CCF	Common cause failure
DC	Diagnostic coverage
DKE	German Commission for Electrical, Electronic and Information Technologies of DIN and VDE (Deutsche Kommission Elektrotechnik Elektronik Informationstechnik im DIN und VDE)
FGPA	Field programmable gate array
FMEA	Failure mode and effect analysis; Ausfalleffektanalyse
FC	Frequency converter
IFA	Institute for Occupational Safety and Health of the German Social Accident Insurance (Institut für Arbeitsschutz der Deutschen Gesetzlichen Unfallversicherung)
IGBT	Insulated-gate bipolar transistor
$MTTF_d$	Mean time to dangerous failure
NC	Numeric control
n_{op}	Mean annual number of operations
PDS	Power drive systems
PDS(SR)	Power drive systems safety related
PFH	Probability of a dangerous failure per hour
PL	Performance Level
PLC	Programmable logic controller
PL_r	Required Performance Level
PWM	Pulse-width modulation
SIL	Safety integrity level
SISTEMA	Safety of controls on machinery
SRASW	Safety-related application software
SRESW	Safety-related embedded software
SRP/CS	Safety related parts of control systems
UPS	Uninterruptible power supply

