IFA
Institut für Arbeitsschutz der
Deutschen Gesetzlichen Unfallversicherung

4/2018e

IFA Report

Safe drive controls with frequency inverters

Authors: Christian Werner, Helmut Zilligen, Burkhard Köhler, Ralf Apfeld
Institute for Occupational Safety and Health of the German Social Accident Insurance (IFA)

Published by: Deutsche Gesetzliche Unfallversicherung e. V. (DGUV)
Glinkastr. 40
10117 Berlin
Germany
Phone: ++49 (0)30 13001-0
Fax: ++49 (0)30 13001-9876
Internet: www.dguv.de
E-mail: info@dguv.de

– 3rd edition, August 2019 –

Database of publications: www.dguv.de/publikationen

ISBN (online): 978-3-86423-235-0
ISSN: 2190-7994

Abstract

Safe drive controls using frequency inverters

Machine drives using closed-loop speed control are state of the art. As on drives without closed-loop speed control, the movement of a machine part at varying speeds frequently gives rise to a hazard against which the machine operators 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. Scenarios such as these require the machine to be operated with protective equipment disabled. In order for the operators‘ safety to be assured nonetheless, Annex I, Section 1.2.5 of the Machinery Directive sets out the required measures. Safety sub-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 addresses the use of drive control equipment that implements safety sub-functions at a certain Performance Level according to ISO 13849-1 in consideration of the application and risks. The basic safety sub-functions of drive controls and the requirements relating to their use are presented. The principles of operation of frequency inverters and DC converters are described, and implementation of the safety sub-functions are explained. Examples are provided of application circuits 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 inverters and frequency inverters with integrated safety functions.

This report supplements IFA Report 2/2017, “Functional safety of machine controls”, and requires a basic understanding of Categories and Performance Levels according to ISO 13849-1.

Kurzfassung

Sichere Antriebssteuerungen mit Frequenzumrichtern

Drehzahlgeregelte Antriebe sind an Maschinen Stand der Technik. Genau wie bei ungeregelten 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 Störungsbeseitigung, zum Einrichten, im Probebetrieb usw. Eingriffe bei laufender Maschine erforderlich sind. In diesen Fällen ist der Maschinenbetrieb bei aufgehobener Schutzwirkung von Schutzeinrichtungen notwendig. Um trotzdem die Sicherheit der Beschäftigten zu gewährleisten, gibt die Maschinenrichtlinie in Anhang I Abschnitt 1.2.5 die erforderlichen Maßnahmen an. Zur Realisierung der hierfür notwendigen Maschinenfunktionen wurden Sicherheits-Teilfunktionen für Antriebssteuerungen definiert, wie z. B. STO (Sicher abgeschaltetes Moment), SLS (Sicher begrenzte Drehzahl) und SS1 (Sicherer Stopp 1).

Der vorliegende Report behandelt den Einsatz von Antriebssteuergeräten, die abhängig von Applikation und Risiken, Sicherheits-Teilfunktionen in einem bestimmten Performance Level nach DIN EN ISO 13849-1 umsetzen. Die grundlegenden Sicherheits-Teilfunktionen von Antriebssteuerungen und die Anforderungen bei deren Anwendung werden vorgestellt. Die prinzipielle Funktionsweise von Frequenzumrichtern und Gleichstromstellern wird beschrieben und die Umsetzung der Sicherheits-Teilfunktionen 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 IFA Report 2/2017 „Funktionale Sicherheit von Maschinensteuerungen“ und setzt Grundkenntnisse über Kategorien und Performance Level nach DIN EN ISO 13849-1 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. Or, il est fréquent que cela ne soit pas possible, par exemple lorsqu’il faut intervenir sur une machine en fonctionnement pour remédier à des défauts, procéder à des réglages, effectuer des marches d’essai, etc. Dans ces cas, il est nécessaire que la machine continue à fonctionner, bien que les dispositifs de protection soient désactivés. Pour que la sécurité de l’opérateur soit néanmoins garantie, la directive Machines indique, dans l’Annexe I, point 1.2.5, les mesures à prendre. Pour la réalisation des fonctions machine nécessaires à cet effet, des sous-fonctions de sécurité pour commandes d’entraînement ont été définies, telles que STO (Safe Torque Off = suppression sûre du couple), SLS (Safety Limited Speed = limitation sûre de la vitesse) et SS1 (Safe Stop 1 = stop sûr 1).

Ce rapport traite de l’utilisation de dispositifs de commande d’entraînement qui, en fonction de l’application et des risques, met en œuvre des sous-fonctions de sécurité ayant un niveau de performance déterminé, conforme à la norme ISO 13849-1. Les sous-fonctions de sécurité de base des commandes d’entraînement et les exigences relatives à leur utilisation sont présentées. Les principes de fonctionnement des convertisseurs de fréquence et des convertisseurs DC-DC sont décrits et la mise en œuvre de la sous-fonction de sécurité est expliquée. Des exemples illustrent les circuits d’application grâce auxquels différentes fonctions de sécurité peuvent être réalisées sur les machines. Les fichiers SISTEMA permettant de quantifier ces différentes fonctions de sécurité peuvent être téléchargés gratuitement. Les exemples comportent aussi bien des convertisseurs de fréquence standard que des convertisseurs de fréquence avec fonctions de sécurité intégrées.

Le présent rapport complète le rapport IFA 2/2017 « Funktionale Sicherheit von Maschinensteuerungen » (Sécurité fonctionnelle des commandes de machines). Il requiert des connaissances de base sur les catégories et niveaux de performance selon la norme ISO 13849-1.

Resumen

Accionamientos seguros con convertidores de frecuencia

Los accionamientos con control de velocidad son un estándar técnico en maquinaria. Al igual que en los accionamientos no regulados, un movimiento de velocidad variable de un elemento en una maquinaria suele suponer un riesgo que requiere la consiguiente protección para los operarios. La solución más sencilla para evitar movimientos en las operaciones manuales en puntos de peligro es la desconexión (segura) de la energía de propulsión de los motores en cuestión. Pero con frecuencia no es posible hacerlo, por ejemplo, cuando es necesario realizar operaciones con la maquinaria en marcha para subsanar una avería, realizar ajustes o pruebas, etc. En esos casos, es necesario operar la maquinaria sin accionar los dispositivos de protección. Para aún así poder garantizar la seguridad de los empleados, se aplican las medidas necesarias según la directriz de maquinaria que figura en el anexo I, párrafo 1.2.5. Para implementar las funciones de la máquina necesarias para ello, se han definido funciones parciales de seguridad para los accionamientos como, por ejemplo, la STO (momento de desconexión segura), SLS (velocidad limitada segura) y SS1 (parada segura 1).

El presente informe trata sobre la utilización de accionamientos que, en función de su aplicación y los riesgos, implementan una función subsidiaria de seguridad en un nivel de rendimiento determinado según lo estipulado en la normativa ISO 13849-1. Las funciones subsidiarias de seguridad básicas de los accionamientos y los requisitos correspondientes para su aplicación se presentan en dicho informe. En él se describe el funcionamiento básico de los convertidores de frecuencia y los chopper CC, y se explica la aplicación de la función subsidiaria de seguridad. Se muestran ejemplos de conmutación de aplicaciones con los que se introducen diversas funciones de seguridad en las máquinas. Los archivos correspondientes de SISTEMA para cuantificar estas funciones de seguridad se pueden descargar gratuitamente. En los ejemplos se muestra la aplicación tanto de convertidores de frecuencia estándar como también de convertidores de frecuencia con funciones de seguridad integradas.

Este informe se entiende como complemento al IFA Report 2/2017 „Funktionale Sicherheit von Maschinensteuerungen“ (seguridad funcional de controles de maquinaria) y presupone conocimientos básicos sobre las categorías y el nivel de rendimiento según ISO 13849-1.

Table of contents

1 Introduction

The use of frequency inverters in safety-related electrical circuits has been described in two previous reports (BIA Report 5/2003 and IFA Report 7/2013e). Based upon the safety functions and with reference to examples, these described the use of frequency inverters both without and with integrated safety sub-functions ("power drive systems (PDS)" and "power drive systems safety related (PDS(SR))" respectively). The first report was based upon EN 954-1 [1], listed under the Machinery Directive. Comprehensive revision of this standard, which is now available in the form of ISO 13849-1 [2] (Safety of machinery – Safety-related parts of control systems), and the publication of IEC 61800-5-2 [3] concerning the functional safety requirements of adjustable speed electrical power drive systems, necessitated revision and adaptation of BIA Report 5/2003. The revised report was then published as IFA Report 7/2013e[1]. ISO 13849-1 [2] and EN 61800-5-2 [3] have been revised again since publication of the last edition of the report. The normative changes have been reflected in the present edition. As in IFA Report 7/2013e, the control of DC drives is also discussed.

This report is based upon observations made in recent years during the testing and certification of products and consulting with manufacturers and the Expert Committees of the German Social Accident Insurance Institutions. It provides examples and explanations for support in the design of adjustable speed power drive systems to ISO 13849-1 [2]. The present report can thus be regarded as a supplement to IFA Report 2/2017e, Functional safety of machine controls [4].

The examples provided in this report are conditional upon the de-energized state of a power drive control constituting a safe state of the machine. Section 5.4, "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 inverters are set out in IEC 61800-5-2 [3], which is based upon IEC 61508 [5]. Where necessary, the particular relationships to IEC 61508 [5] will therefore be addressed in this report. The safety functions are however always considered overall from the perspective of the machine manufacturer; reference is therefore always made to ISO 13849-1 [2].

The authors trust that the present report will provide designers with useful assistance in implementing safety functions involving power drive controls.

[1] Safe drive controls with frequency converters (IFA Report 7/2013e). Published by: Deutsche Gesetzliche Unfallversicherung (DGUV), Berlin, Germany 2013.

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 assessment. 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 as might reasonably be 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.

Standards including ISO 12100 [7] have been developed in order to provide designers, manufacturers and other stakeholders with support in interpreting the essential safety requirements, and in order for compliance to be attained with the European legislation governing the safety of machinery. ISO 12100 contains general design principles and provisions governing risk assessment and risk reduction. It serves as a general framework and provides guidance in the manufacture of safe machines. It also provides useful guiding principles for cases in which a relevant machine-specific (type C) standard does not exist.

For the purpose of risk reduction, “the three-step method” described in Subclause 6.1 of ISO 12100 [7] applies:

- Step 1 – inherently safe design measures
- Step 2 – safeguarding and/or complementary protective measures
- Step 3 – information for use concerning the residual risk

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

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

Part 1 sets out safety requirements and provides guidance on 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 controls, including the two procedures of analysis and testing. The validation procedure includes analysis of the behaviour of safety-related parts of the control system in the event of a fault. For this purpose, it includes lists of possible faults and – where applicable – design requirements for their exclusion for many components. The basic and well-tried safety principles are also listed.

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

Safety functions have the purpose of reducing the risk presented by machinery. ISO 13849-1 [2], the scope of which covers the safety-related part of the control system (SRP/CS), is used for evaluation of the safety functions. The SRP/CS 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 actuator proper, such as the motor or hydraulic cylinder, lies outside the scope of the standard. This demarcation is logical, provided failure of an actuator cannot give rise to a dangerous state. Should external forces act upon a machine however, as for example in the case of vertical axes, failure of an actuator (such as a brake or motor) may cause the load to drop, thereby presenting a hazard. In such cases, these actuators must also be included in the analysis of the safety function, and engineered for this purpose by means of additional safety measures. Such a measure could for example be a non-return valve on the hydraulic cylinder, or a supplementary mechanical brake.

The method of ISO 13849-1 [2] can also be applied to actuators; certain additional safety-related properties (such as mechanical strength) may however have to be considered. Expert Committee Information sheet 005 of the

Expert Committee Woodworking and Metalworking of the German Social Accident Insurance (Annex B, Page 111 ff.) describes typical hazard situations specific to "gravity-loaded axes", together with suitable risk-reduction strategies employing control measures.

2.2 Overlapping hazards

Overlapping hazards arise when a person present at a particular location could be injured by multiple hazardous movements. Calculation of the probability of injury must consider not only one but as many as 20 hazardous movements, depending upon the machine.

Since each of these movements is associated with a probability of failure, the probabilities of failure of a large number of components are added together, and the required Performance Level may no longer be reached.

Together with the DGUV Expert Committee Woodworking and Metalworking, the IFA has described a strategy for a solution that is based upon analysis of discrete hazards presented by machine components (Expert Committee Information Sheet 47). The regulatory content of this information sheet was included in the third revision of ISO 13849-1 [2]. The information sheet was consequently withdrawn. Section 5.3.2 of IFA Report 2/2017e describes an example for calculation of the PFH_D (probability of a dangerous failure per hour) in the case of overlapping hazards. The withdrawn Information Sheet 47 can be found in Annex J of IFA Report 2/2017e.

3 Power drive control devices as safety-related parts of control systems

Power drive control devices, such as frequency inverters, servo controllers or DC-DC converters, have been used for many years to control the speed of electrical drives on machinery. These power 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 relatively easily, for example by means of a mains contactor in the power drive‘s mains circuit or a motor contactor between the power drive control device and the motor. An alternative is power drive control devices with integrated safety sub-functions featuring pulse blocking.

In some circumstances however, work must also be performed on a machine whilst it is running, and thus with the protective action of safeguards disabled. This necessitates substitute safety measures which provide the operators 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 the precise position being lost; this would not be acceptable owing to the required accuracy of the process. The closed-loop position control of the power drive must therefore remain active during the manual intervention. The Machinery Directive [6] permits this in principle (Annex I, Section 1.2.5); additional requirements are however 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 ISO 13849-1 [2] that is commensurate with the risk.

Instead of guards and a motor that is isolated from the system, other measures are required in this case that assure a comparable level of safety for the machine operator. This is attained for example by application of the safety sub-functions defined in IEC 61800-5-2 [3] (Table 1, Page 12).

The safety sub-functions defined in IEC 61800-5-2 [3] can be regarded as a basis. The manufacturers of PDS(SR)s offer a range of further safety sub-functions beyond those listed in the standard. Selected basic functions are described in more detail in Section 3.1.

The safety sub-functions referred to above are not a substitute for devices for disconnecting the electrical equipment from the mains system. The latter are required in addition in order to enable work to be completed without risk of electric shock or burns.

Table 1:
Safety sub-functions in IEC 61800-5-2

Abbreviation	Subclause of the standard	Term	Function
STO	4.2.3.2	Safe torque off	No power capable of generating a rotary movement is applied the motor; stop category 0 to IEC 60204-1.
SS1	4.2.3.3	Safe stop 1	Motor decelerates; monitoring of the deceleration ramp and STO once stationary, or STO following expiration of a time delay; stop category 1 to IEC 60204-1.
SS2	4.2.3.4	Safe stop 2	Motor decelerates; monitoring of the deceleration ramp and SOS once stationary, or SOS following expiration of a time delay; stop category 2 to IEC 60204-1.
SOS	4.2.4.2	Safe operating stop	Motor is stationary and withstands external forces.
SLA	4.2.4.3	Safely-limited acceleration	Exceeding of an acceleration and/or deceleration limit value is prevented.
SAR	4.2.4.4	Safe acceleration range	The acceleration and/or deceleration of the motor is maintained within specified limits.
SLS	4.2.4.5	Safely-limited speed	Exceeding of a specified speed limit value is prevented.
SSR	4.2.4.6	Safe speed range	Monitoring of the motor speed within specified limit values.
SLT	4.2.4.7	Safely-limited torque	Exceeding of a torque/force limit value is prevented.
STR	4.2.4.8	Safe torque range	Monitoring of the torque or specified force of the motor within specified limit values.
SLP	4.2.4.9	Safely-limited position	Exceeding of a position limit value is prevented.
SLI	4.2.4.10	Safely-limited increment	The motor is moved by a specified incremental dimension, after which it stops.
SDI	4.2.4.11	Safe direction	The motor is prevented from moving more than a specified distance in the unintended direction.
SMT	4.2.4.12	Safe motor temperature	Exceeding of a motor temperature limit value is prevented.
SCA	4.2.4.13	Safe cam	Whilst the motor is within a specified position range, a safe output signal is generated.
SSM	4.2.4.14	Safe speed monitor	Whilst the motor speed is below a specified value, a safe output signal is generated.
SBC	4.2.5	Safe brake control	Safe actuation of an external brake.

3.1 Description of safety sub-functions

In accordance with ISO 12100-1 [7], a safety function is any function of a machine the failure of which can lead directly to an increase in the risk. A safety function in this context is usually implemented by the components of sensor (input devices), logic (processing unit) and actuator (output devices)[2]. The power drive control devices discussed in this report cover the aspect of the actuator, which depending upon the form of implementation may also include the logic. The safety functions of the PDS(SR) are thus only part of the complete safety function of an application and are therefore described as safety sub-functions.

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

- Response to the exceeding of limit values

  This is the response function that is triggered by the exceeding 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.

In both cases, consideration must be given to the possible safe states for the application. It must also be consi-

[2] Subclause 3.5.2 of IEC 61508-4:2010, Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 4: Definitions and abbreviations, defines the “overall safety function” in this context.

dered that parts of the PDS(SR) are no longer functional. The information for use of a PDS(SR) should provide information on this aspect.

It is expedient to divide the safety sub-functions into stop functions and monitoring functions.

The following descriptions of the safety sub-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 instruction manuals must therefore always be consulted for use of the devices.

3.1.1 Stop functions

The IEC 60204-1 standard governing electrical equipment [9], which is also important for machinery, distinguishes the following three categories of stop function:

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 and then removal of power when the stop is achieved.

Stop category 2:
A controlled stop with power remaining available to the machine actuators.

The stop functions defined in IEC 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)

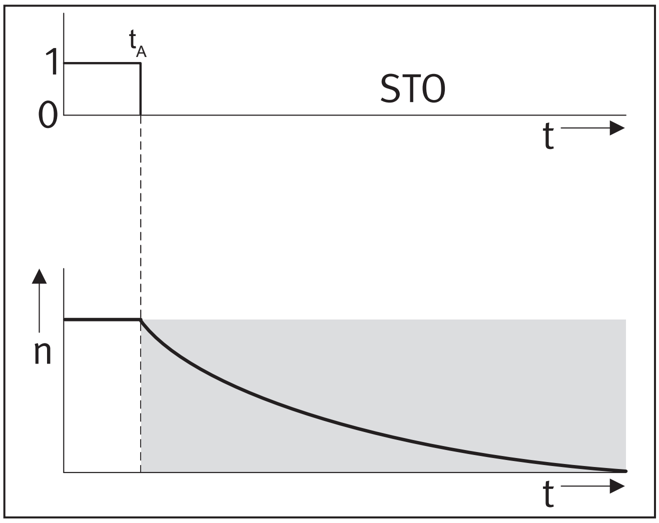
“This function prevents force-producing power from being provided to the motor.”

Figure 1 shows the time characteristic of the input signal for activation of STO, and of the motor speed.

The STO safety sub-function corresponds to an uncontrolled stop in accordance with IEC 60204-1 [9], stop category 0. It can be used where power removal is required to prevent an unexpected start-up. The standstill position is not monitored. Should the STO safety sub-function be activated during operation, the motor coasts down unbraked.

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 5.4).

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



Electronic devices and contactors which may be used to implement safety sub-functions are not suitable components for galvanic isolation; additional measures are required for adequate protection against electric shock (refer also to Section 5.7).

Suitable measures for safe torque off include
(see Figure 2, Page 14):

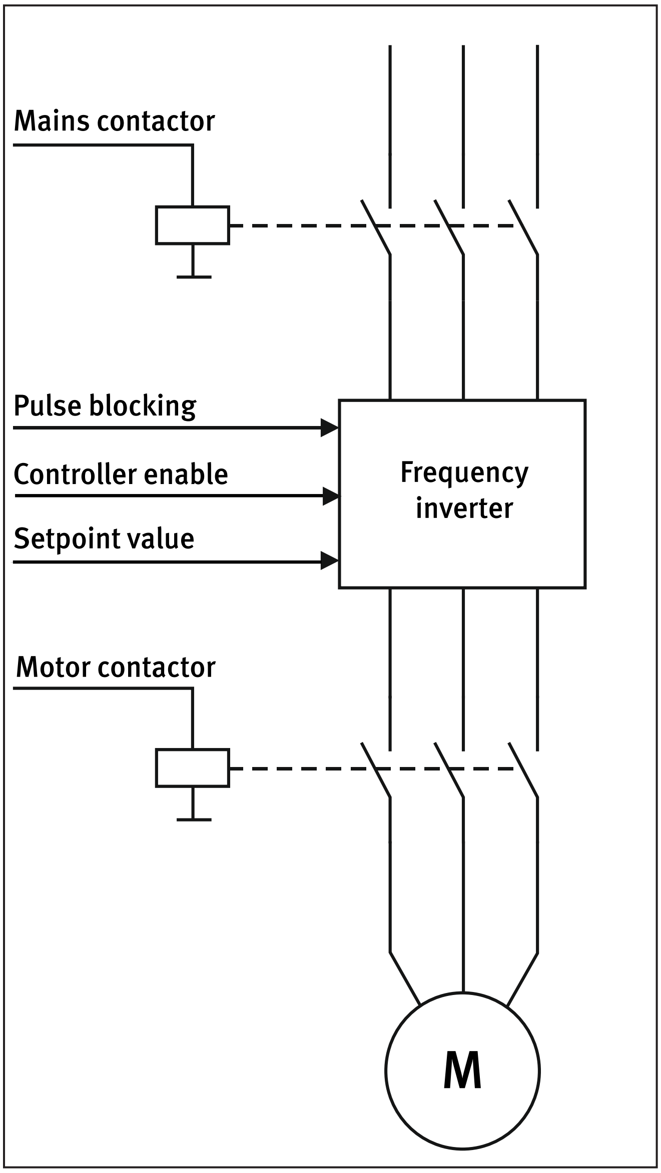
- Contactor between electrical system and power drive system (mains contactor),
- Contactor between power unit and power drive motor (motor contactor),
- Pulse blocking (blocking of the pulse triggering the power semiconductors within the frequency inverter),
- Controller enable,
- Setpoint value assignment.

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)*

In IEC 61800-5-2 [3] the following variants of SS1 are described.

"This function is specified as either

a) *Safe Stop 1 deceleration controlled*
SS1-d

initiates and controls the motor deceleration rate within selected limits to stop the motor and performs the STO function (see IEC 61800-5-2 [3], 4.2.3.2) when the motor speed is below a specified limit[3] *; or*

b) *Safe Stop 1 ramp monitored*
SS1-r

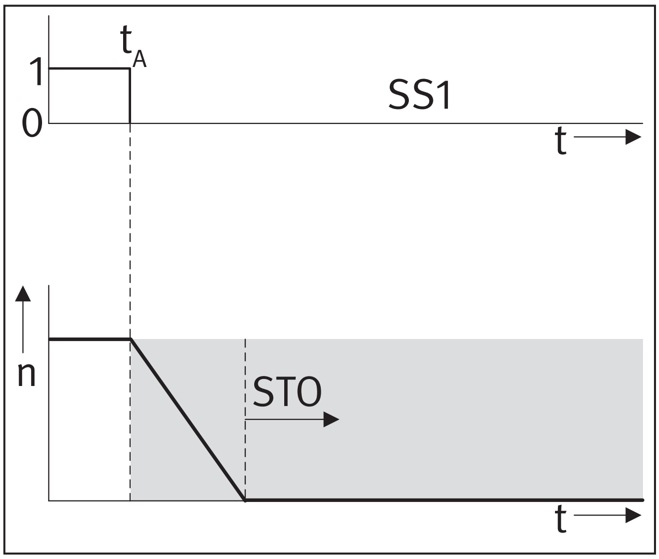
initiates and monitors the motor deceleration rate within selected limits to stop the motor and performs the STO function when the motor speed is below a specified limit, or"

c) *Safe stop 1 time controlled*
SS1-t

initiates the motor deceleration and performs the STO function after an application specific time delay."

Figure 3 shows the time characteristic of the input signal for activation of SS1, and of the motor speed. The SS1 safety sub-function corresponds to a controlled stop in accordance with IEC 60204-1 [9], stop category 1. The "motor deceleration rate" is a measure of motor braking.

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



Should the SS1-t safety sub-function be implemented, in which the STO function is triggered following a time delay, attention must be paid to the following: The stop function of the power 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, SS1-t is not suitable for implementation of the safety sub-function. Conversely, if the safety sub-function is implemented in the form of SS1-r, with monitoring of the deceleration ramp (motor deceleration rate), a defective stop function can be detected very quickly.

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

Application examples:

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

- 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 break loose, and control over it be lost. SS1-r is absolutely essential, since it cannot be ruled out that a defective drive control could cause acceleration instead of deceleration. This situation is detected swiftly by monitoring of the deceleration ramp, and STO is executed in response to the fault.

3.1.1.3 Safe stop 2 (SS2)

In IEC 61800-5-2 [3] Tthe following variants of SS2 are described.

“*This function is specified as either*

a) Safe stop 2 deceleration controlled
SS2-d

initiates and controls the motor deceleration rate within selected limits to stop the motor and performs the safe operating stop function (see IEC 61800-5-2 [3], 4.2.4.2) when the motor speed is below a specified limit[4] ; or

b) Safe stop 2 ramp monitored
SS2-r

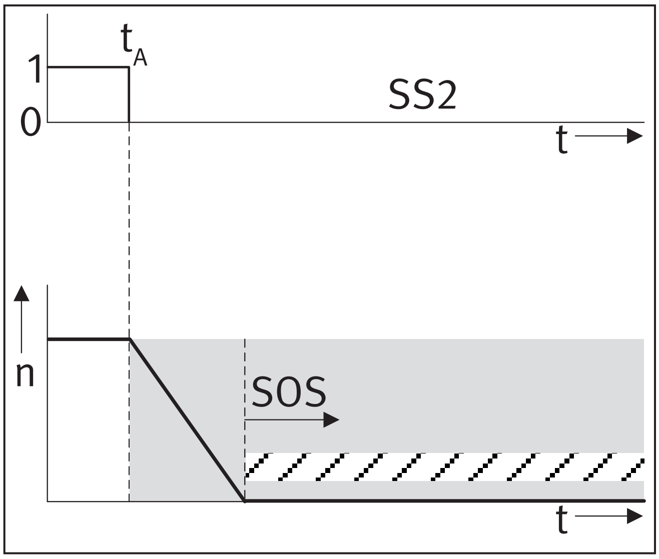
initiates and monitors the motor deceleration rate within selected limits to stop the motor and performs the safe operating stop function when the motor speed is below a specified limit; or

c) Safe stop 2 time controlled
SS2-t

initiates the motor deceleration and performs 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 of the motor speed. The SS2 safety sub-function corresponds to a controlled stop in accordance with IEC 60204-1 [9], stop category 2.

Figure 4:
Example time characteristics of the SS2 safety sub-function (Safe stop 2)



Should the SS2-t safety sub-function be implemented, in which the SOS function is triggered following a time delay, attention must be paid to the following: The stop function of the power drive control is not monitored during the delay. It may 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, SS2-t is not suitable for implementation of the safety sub-function.

Conversely, if the safety sub-function is implemented in the form of SS2-r, with monitoring of the deceleration ramp (motor deceleration rate), a defective stop function can be detected very quickly.

Application examples:

- On a machine tool, a measurement must be performed on the workpiece during the machining process; a position change must not however occur as a result of the motor control being de-energized. Opening of the safety guard causes triggering of SS2-r. The hazardous movement is halted, and unexpected start-up subsequently prevented by SOS.

- The load on a vertical axis is brought to a standstill when a safety guard is opened, and subsequently held in position by SOS. Depending upon whether operators may be present within the hazardous zone, further measures may be required (see Information Sheet 005 of the Expert Committee Woodworking and Metalworking, Annex B).

[4] The authors are not currently aware of any product employing solution a).

3.1.2 Monitoring functions

3.1.2.1 Safe operating stop (SOS)

"This 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." (Subclause 4.2.4.2 in [3]).

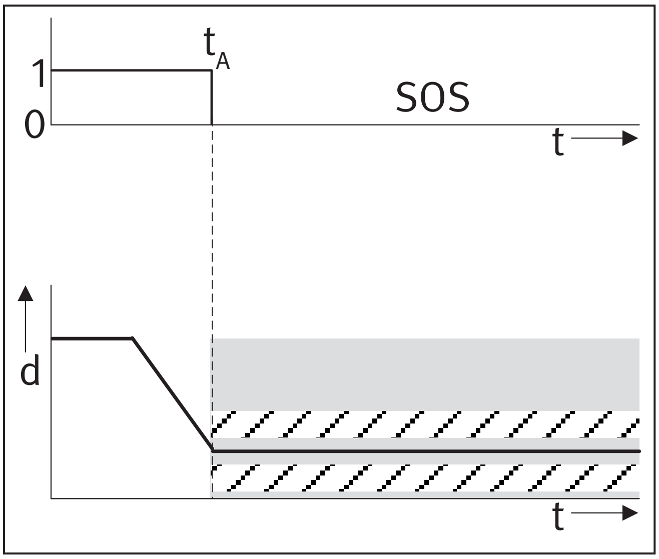
Figure 5 shows the time characteristic of the input signal for activation of SOS, and of the motor position.

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

Application examples:

- Setup mode on lathes/machining centres,
- Manual measurement during machining.

Figure 5:
Example time characteristic of the SOS safety sub-function (safe operating stop)



3.1.2.2 Safely-limited speed (SLS)

"This function prevents the motor from exceeding the specified speed limit." (Subclause 4.2.4.5 in [3]).

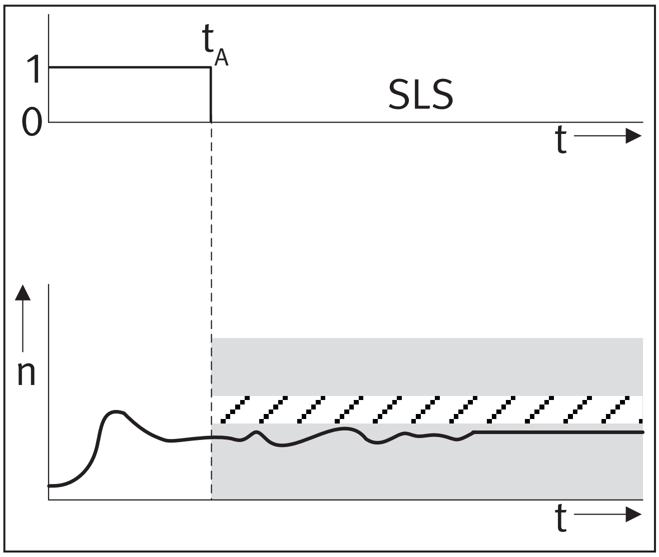
Figure 6 shows the time characteristic of the input signal for activation of SLS, and of the axial speed.

With this safety sub-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 lathes/machining centres
- Feeding in of material on calender rolls

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



Note:

No generic rotational 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 governing safety and health at the workplace, code 330216 [10], contains an overview of relevant provisions governing speeds in machine-specific standards (type C standards).

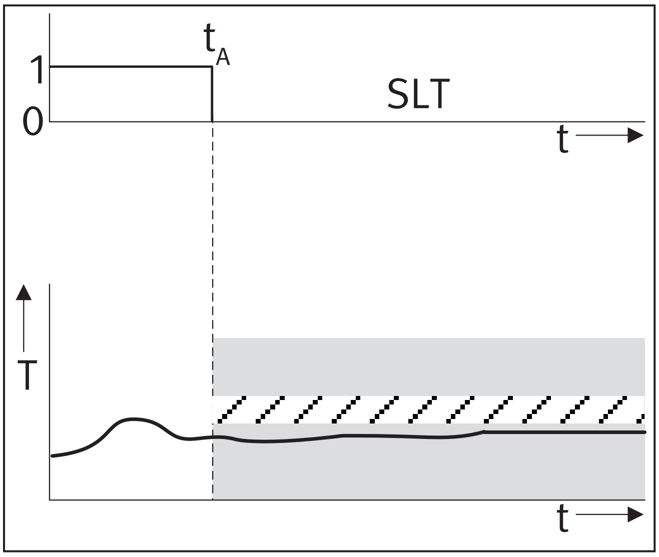
3.1.2.3 Safely-limited torque (SLT)

"This function prevents the motor from exceeding the specified torque (or force, when a linear motor is used)." (Subclause 4.2.4.7 in [3]).

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

SLT reduces the scale of harm caused by a hazardous movement. Guideline values for the effects of forces can

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



be found in the list of limit values in Chapter 6 of the IFA Report 3/2017[11].

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)

"This function prevents the motor shaft (or mover, when a linear motor is used) from exceeding the specified limit of position increment." (Subclause 4.2.4.10 in [3]).

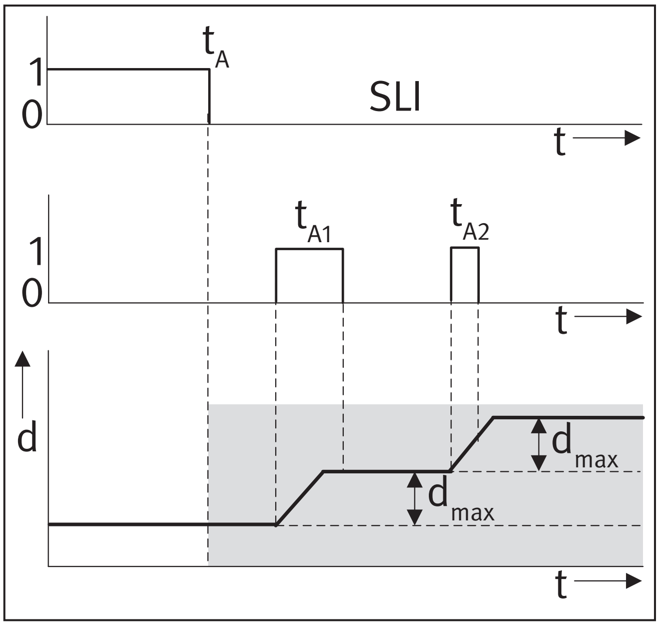
Figure 8 shows the time characteristics of the input signal for activation of SLI, the command for initiation of the movement, and the step performed.

With this safety sub-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 lathes/machining centres,
- Inching with limited travel on printing machines.

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

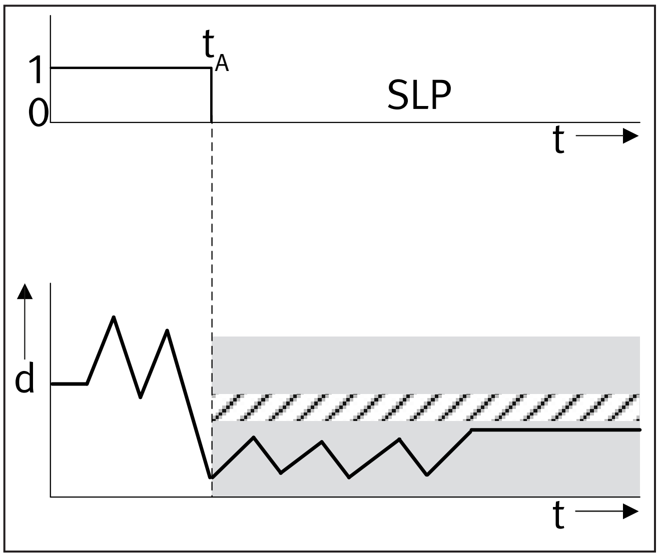


3.1.2.5 Safely-limited position (SLP)

"This function prevents the motor shaft (or mover, when a linear motor is used) from exceeding the specified position limit(s)." (Subclause 4.2.4.9 in [3]).

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

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



Safe limiting of the position results in the drive system assuming an STO or SOS (safe operating stop) state when a specified absolute position limit value is reached. The limit value must take account of the overrun arising for technical reasons. Below the limit value, unexpected movements of the drive may occur. Exceeding of a limit value is detected, and the drive system is stopped safely.

Application examples:

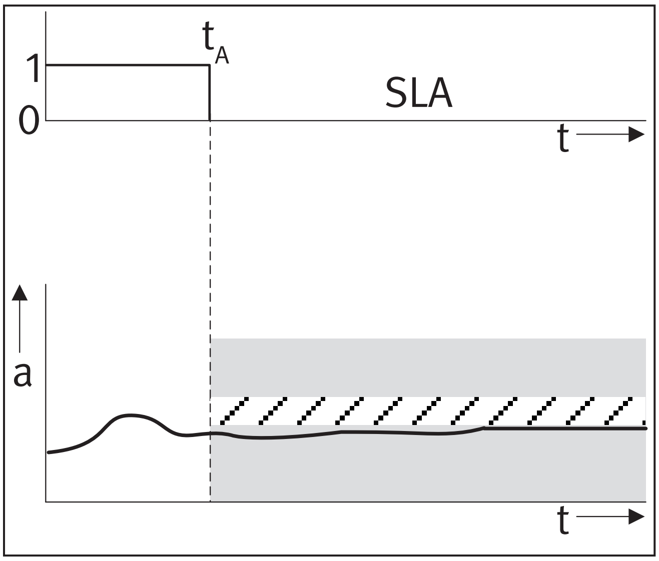
- Partitioning of a machine into manufacturing and feeding areas,
- Limitation of a range of travel (substitution for electromechanical limit switches),
- Limitation of the operating range of robot arms.

3.1.2.6 Safely-limited acceleration (SLA)

"This function prevents the motor from exceeding the specified acceleration and/or deceleration limit." (Subclause 4.2.4.3 in [3]).

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

Figure 10:
Example time characteristic of the SLA safety sub-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 deceleration rate.

Application examples:

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

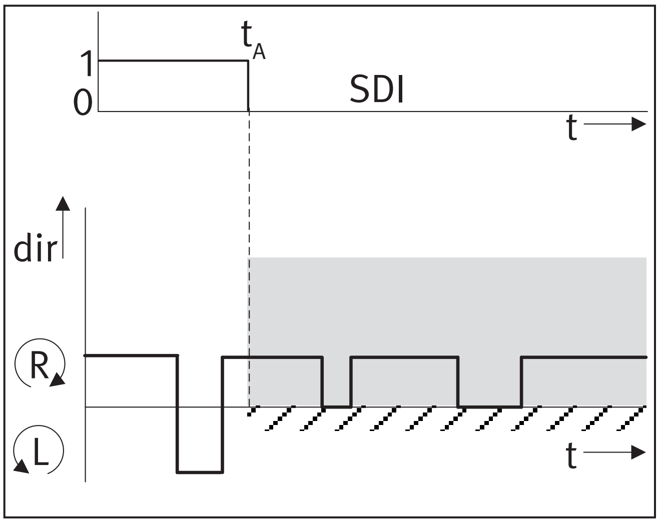
3.1.2.7 Safe direction (SDI)

"This function prevents the motor shaft from moving more than a defined amount in the unintended direction." (Subclause 4.2.4.11 in [3]).

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

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

Figure 11:
Example time characteristic of the SDI safety sub-function (safe direction)



Application examples:

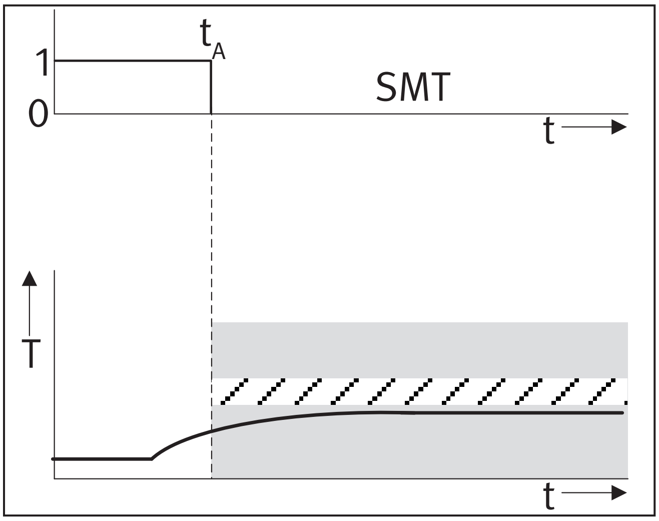
- Machine parts are prevented from moving towards the operator.
- A reversal in the direction of rotation of rolls is prevented, as this could otherwise give rise to entrapment points.

3.1.2.8 Safe motor temperature (SMT)

"This function prevents the motor temperature(s) from exceeding a specified upper limit(s)." (Subclause 4.2.4.12 in [3]).

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

Figure 12:
Example time characteristic of the SMT safety sub-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 a potentially explosive atmosphere,
- Fire protection.

3.1.2.9 Safe cam (SCA)

"This function provides a safe output signal to indicate whether the motor shaft position is within a specified range." (Section 4.2.4.13 in [3]).

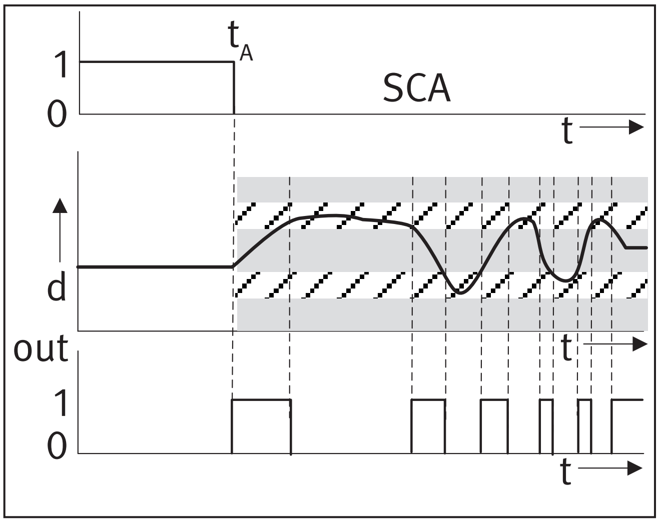
Figure 13 shows the time characteristics of the input signal for activation of SCA, of the motor position, and of the output signal.

Parameters are used to specify a travel range of an axis. Whenever the axis is within this range, a safe output signal is generated. Departure from the range has no effect upon the function within the PDS(SR); the effect is limited to generation of a corresponding output signal.

Application examples:

- Releasing of guard locking device 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 for position sensors,
- Position limitation of robot axes.

Figure 13:
Example time characteristic of the SCA safety sub-function (safe cam)

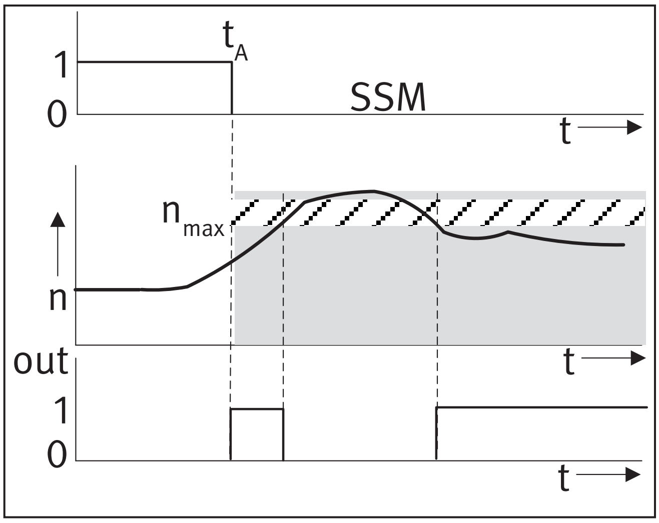


3.1.2.10 Safe speed monitor (SSM)

"The SSM function provides a safe output signal to indicate whether the motor speed is below a specified limit." (Clause 4.2.4.14 in [3]).

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

Figure 14:
Example time characteristic of the SSM safety sub-function (safe speed monitor)



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

Application example:

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

3.1.3 Output function: safe brake control (SBC)

"This function provides a safe output signal(s) to control an external brake(s)." (Subclause 4.2.5 in [3]).

Additional mechanical brakes may also be required on motors that are driven by frequency inverters. 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 sub-function. The point in time of actuation is specific to the application, for example immediately after stopping, in response to the detection of faults in the power drive control, in the event of an emergency stop, etc.

Application examples:

- Actuation of an external brake on a vertical axis, with simultaneous activation of STO,

- Actuation of an external brake on a vertical axis in the event of voltage breakdown.

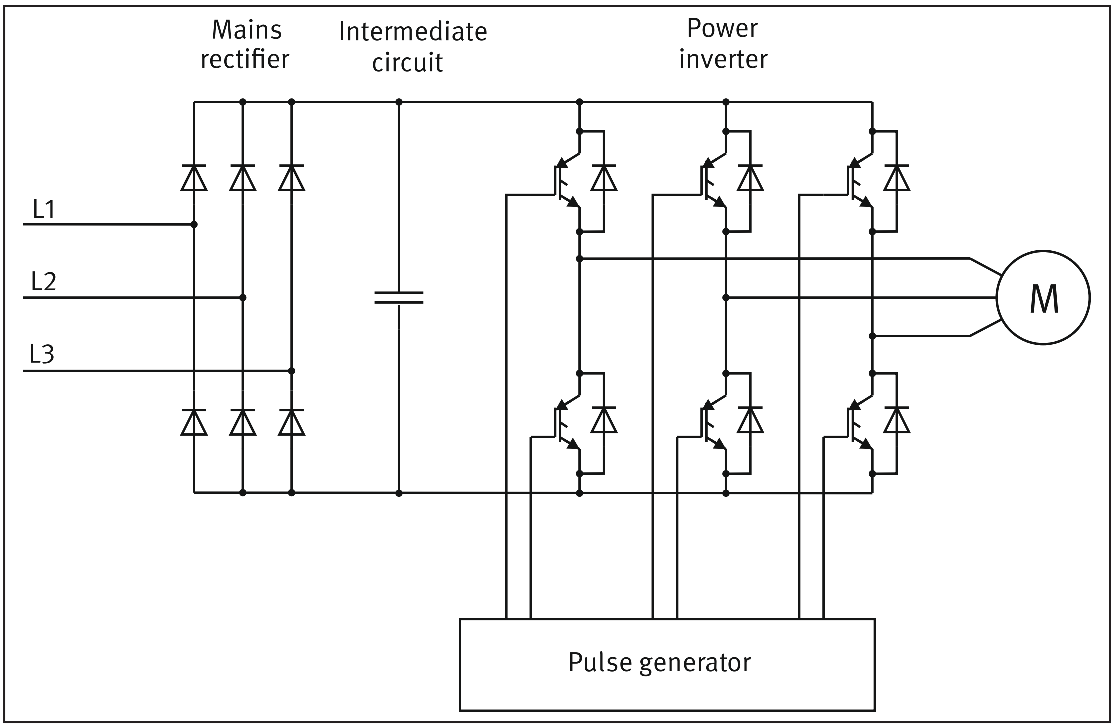
4 Frequency inverters and safety functions

4.1 Frequency inverters without integrated safety sub-functions (PDS)

Whereas only a few decades ago, the majority of adjustable speed drives still employed DC technology owing to its facility of control, this function is now provided primarily by means of three-phase drives employing frequency inverters. Developments in the area of microprocessors and power electronics have contributed substantially to this change.

The principle arrangement of a frequency inverter comprises a cascaded arrangement of a mains rectifier, an intermediate DC circuit and a power inverter. The arrangement is shown in Figure 15.

Figure 15:
Conceptual schematic diagram of a conventional frequency inverter



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

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

The power inverter of the frequency inverter 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 generated in the microprocessor of the inverter or in a separate module (such as an FPGA or ASIC).

Some types of frequency inverter can be used to brake motors as well as to drive them. In this case, the direction of 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 and 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 inverters, safety functions can be implemented directly only to a limited extent; additional components are usually required. This can be illustrated by the example of the safe torque off (STO) safety sub-function.

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

The signal is processed in this case 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. A mains contactor for example may be suitable for this purpose (see Section 3.1.1.1).

4.2 Frequency inverters with integrated safety sub-functions (PDS(SR))

Conventional frequency inverters as described in Section 4.1 are designed in the first instance to satisfy the functional requirements and to cope with the anticipated operational stresses, such as vibration, temperature, electromagnetic interference and faults in the power supply. This is assured in part by observation of the provisions of the IEC 61800 series of standards.

Based upon these conventional products, frequency inverters have been developed in which safety sub-functions such as STO or safe movement monitoring are already integrated. This yields a number of benefits, and simplifies the implementation of safe machinery control systems. In addition, certain applications are not possible without integrated safety technology, owing to impermissibly long response times.

Implementing specific safety sub-functions in the frequency inverter imposes different requirements upon the complexity and design of the hardware. The STO safety sub-function can be implemented relatively easily in a frequency inverter; by contrast, the SLS safety sub-function for example requires a substantially more complex design. The description below distinguishes between “pulse blocking” and “safe movement monitoring” for the implementation of safety sub-functions.

A fault analysis first identifies what faults and failures must be anticipated in frequency inverters, and what effects these faults have upon their function. Suitable measures for implementation of an STO safety sub-function are then presented.

4.2.1 Fault analysis

The fault analysis is taken from a study conducted at the IFA. The study made the following observations relevant to this analysis:

- Unintended power-up, loss of blocking capability (short-circuit) or delayed de-energization of one or more power semiconductors in the power inverter during operation (motor being driven) results in the intermediate circuit being short-circuited. Fuses are consequently blown or tripped or further semiconductors destroyed. In all cases, the fault is evident in the form of operating inhibition. Should these faults occur during braking, failure of the regenerative braking functionality must be anticipated.

- Loss of blocking capability (short-circuit) of one or more power semiconductors in the rectifier bridge of the mains rectifier leads to short-circuiting of at least two phases of the three-phase mains supply. The result is the blowing/tripping of fuses or destruction of further power semiconductors. In all cases, the fault is evident in the form of operating inhibition.

- Loss of conductivity (interruption) of one or more power semiconductors in the power inverter leads to a reduction in the power available at the output. The generated torque drops or is lost completely, in both driving and braking modes.

- Loss of conductivity (interruption) of one or more power semiconductors in the rectifier bridge of the rectifier leads to a reduction in the power available at the output of the rectifier bridge and in the intermediate circuit. The generated torque drops or is lost completely, in both driving and braking modes.

- The pulse patterns required for generation of a rotary field are very complex and can be generated only by means of complex electronic circuits. Random generation of a suitable pulse pattern, for example resulting from influence by electromagnetic interference or from component faults in the power unit as described above, can therefore be ruled out.

Consideration must however be given to possible component failures or influences upon the signal/control inputs of the frequency inverter that would give rise to any conceivable, unintended or incorrect triggering of pulse pattern generation. Such phenomena could cause spontaneous and unexpected fault behaviour, such as unexpected start-up, acceleration, and possibly abortion of the braking process, resulting in the drive running on or running up. Special measures adapted to the risk concerned are required for the avoidance of hazardous situations.

4.2.2 Pulse blocking

One means of implementing the STO safety sub-function is a suitable additional sub-circuit in the frequency inverter that reliably prevents the power semiconductors of the power inverter from being driven by pulse patterns. This prevents a rotary field from being generated in the power inverter, and consequently a torque cannot be generated in the motor. The STO safety sub-function can provide protection against unexpected start-up of the motor.

The transmission elements for the pulse patterns, which provide galvanic isolation between the microprocessor and the power 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 16). As soon as a voltage is no longer present on the anodes of the optocouplers, signals can no longer be transmitted, even if the microprocessor generates pulse patterns and supplies them to the optocouplers.

If pulse blocking in this manner is combined for example with a controller inhibit, the supply of suitable trigger pulse patterns to the power inverter is prevented in two channels. In combination with suitable means of fault detection (see Section 4.2.3), this enables a Category 3 or 4 safety-related circuit to ISO 13849-1 [2] to be achieved.

An alternative means of satisfying the requirements for Category 3 or 4 with respect to single-fault tolerance is a suitable division of the IGBTs into two groups. For this purpose, the three optocouplers of the upper IGBTs and the three optocouplers of the lower IGBTs are each grouped to form a single shut-off path (Figure 17, Page 24).

This solution exploits the fact that a suitable combination of upper and lower IGBTs must always be triggered in order to generate a current – and therefore a rotary field – in the motor. It thus follows that in the event of a fault, shutting off one of the two channels is sufficient to ensure that the STO safety sub-function is executed.

In addition to the examples shown, further conceivable solutions exist for implementation of the STO safety sub-function in a frequency inverter. These solutions will however not be discussed here.

Note:

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 should certain combinations of two faults in the power unit occur simultaneously. Start-up of the motor is however not possible. The specific 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 on both the frequency inverter and the motor terminals. A suitable switch with isolating function is therefore required in addition for the purposes of maintenance and repair.

Figure 16:
Interruption of the supply voltage to the optocouplers

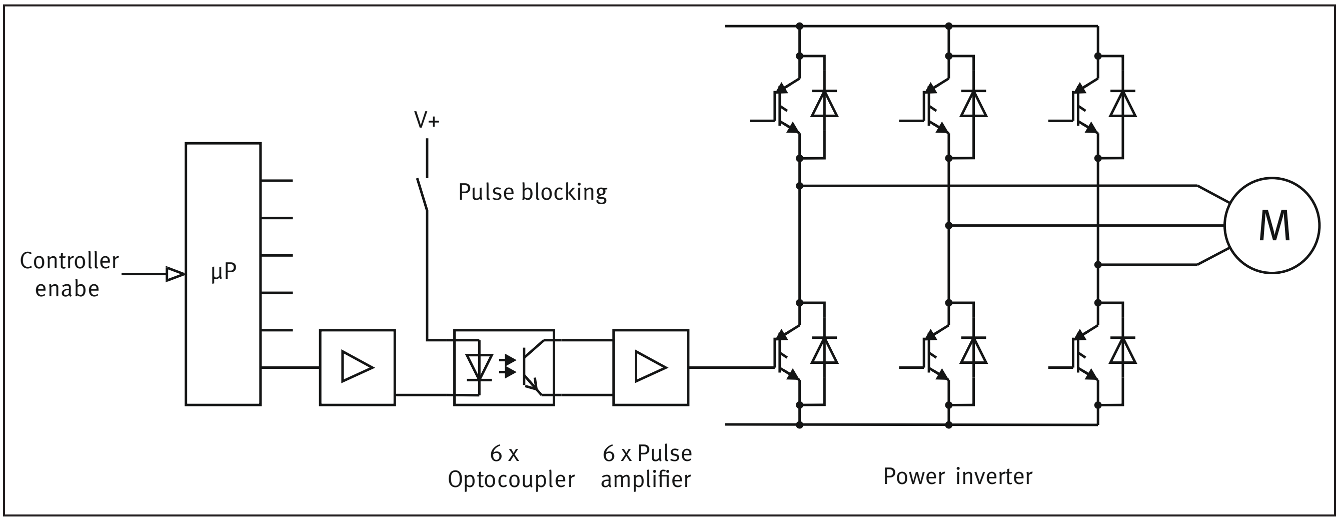
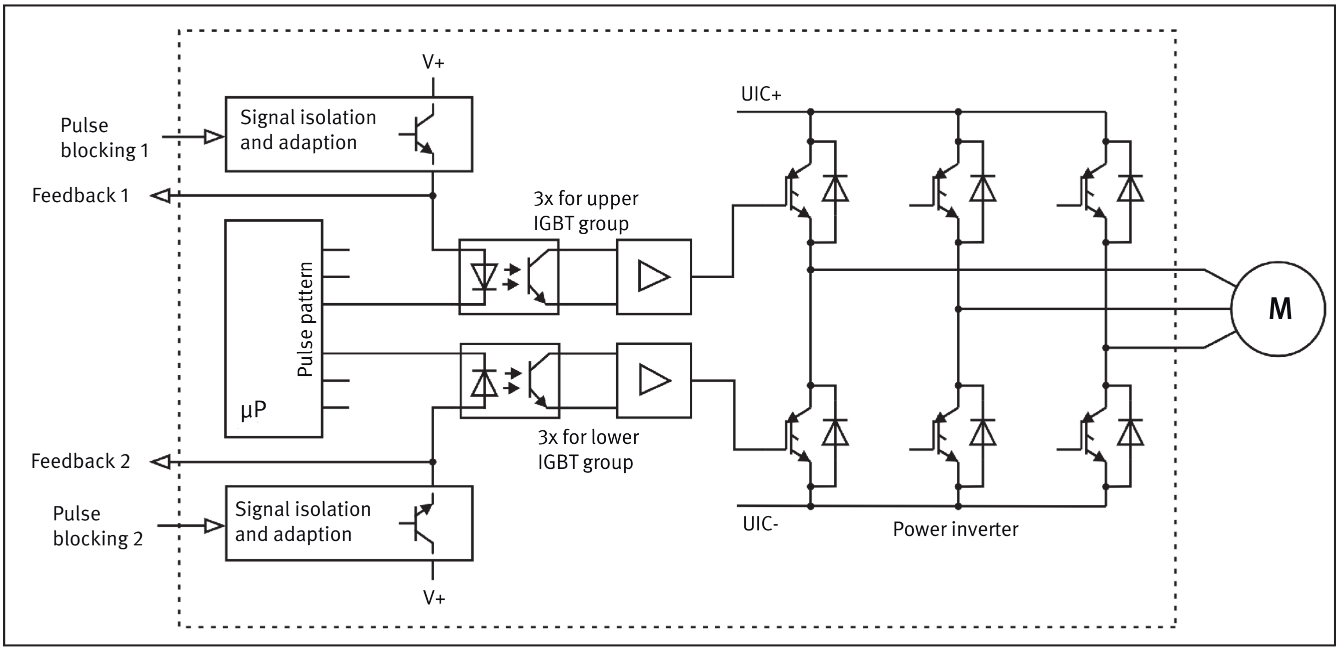


Figure 17:
Division into two IGBT groups



4.2.3 Fault detection

The shut-off paths in a frequency inverter, whether employing pulse blocking or controller enablecontroller 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 inverter, fault detection is performed within the inverter itself or must be achieved by means of external measures.

Where fault detection is performed internally, no further circuitry supplementing the frequency inverter is required: fault detection and the required safe response (generally the prevention of further movements) are performed by measures in the frequency inverter itself independently of the external circuitry.

Where the frequency inverter does not possess internal fault detection, this function must be assumed by external components. This can be achieved for example by means of a PLC that is already present and used for control tasks in the machine, or by a safety module, such as a safety guard monitor, which also activates the safety sub-function within the frequency inverter. Suitable feedback signals must be routed out of the frequency inverter for this purpose. These feedback signals must provide information on the status of the shut-off path concerned. The manufacturer of the frequency inverter sets out requirements for implementation of the measures in the information for use. Observance of these manufacturers‘ instructions is essential in order for the stated PL and the *PFH* to be attained.

Should no specific measures be taken for testing of the shut-off paths, faults can be detected only in the event of a demand upon the safety function. Depending upon the application concerned, this may not be sufficient for the required *PFH* and PL to be attained. The time intervals between demands may be too great.

In such cases, diagnostic testing of the safety function at regular intervals is required. The tests must be designed such that it is possible for faults or failures to be detected in the individual shut-off paths.

These diagnostic tests must not require deliberate action on the part of the operating personnel. At least the demand for the test must be implemented as a permanent element in the machinery control system. Should the tests not be performed within the required time, the machinery control system must prevent further operation of the machine. The machine must not be enabled again until the diagnostic tests have been passed.

In accordance with IEC 61800-5-2 [3], Subclause 6.2.2.1.4, the following maximum diagnostic test intervals can be considered as acceptable for redundant parts of a PDS(SR) which cannot be tested without disrupting the application in which the PDS(SR) is used (machine or plant) and where no justifiable technical solution can be implemented:

- one test per year for SIL 2, PL d / Category 3;
- one test per three months for SIL 3, PL e / Category 3;
- one test per day for SIL 3, PL e / Category 4.

Under certain circumstances, faults in a shut-off path can also be detected via the technical process. This is possible for example when a shut-off path such as a controller enable is used not only for activation of the safety function, but also for operational starting and stopping of the motor. A defect in this path would then be revealed during stopping by the faulty operational behaviour of the machine, provided another signal, such as the setpoint value, is not set to a speed of zero at the same time.

4.2.4 Safe movement monitoring

With the exception of STO – and in some implementations also SS1-t – all safety sub-functions require complex calculations of speeds, positions, ramps, etc. and are therefore implemented with correspondingly complex microprocessor controls. The requirements placed upon these power drive control systems generally result in two-channel processor structures that satisfy the requirements for Category 3 or Category 4 to ISO 13849-1 [2]. Figure 18 shows the concept of such a two-channel control.

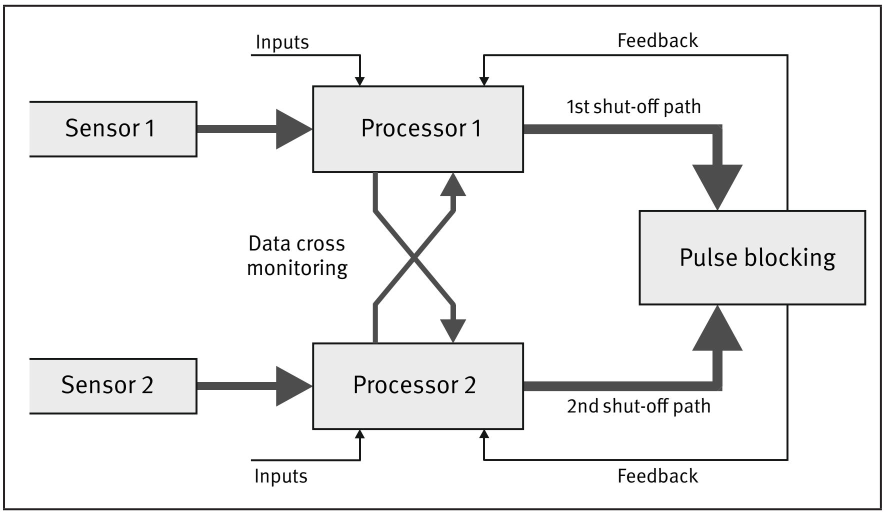


Figure 18:
Safe movement monitoring

The motor speed or axis positions are measured in Figure 18 by two independent encoders on the motor side . The signals generated in the encoders are interpreted in the respective processors 1 and 2. The speed, stationary status, final positions, 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. “Pulse blocking” in Figure 18 executes the STO function in two channels[5]. Its structure follows the principle described in Section 4.2.2. In the event of a fault, processor 1 and processor 2 therefore each have an independent shut-off path.

In order for faults in the control and sensor systems to be detected, the two processors perform not only self-tests, but other tests including cross monitoring 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_D). Depending upon the quality of the tests‘ fault detection (diagnostic coverage, *DC*) and the frequency with which testing is performed, the PFH_D for the safety function(s) is improved.

In their instruction manuals, the manufacturers state fault responses and fault response times. These must be suitable for the application concerned (see also Section 5.6).

4.3 Power drive control: integrated or external safety?

In principle, safety functions can be implemented with the use of purely functional power drive controls by the addition of further external components. Examples of this can be found in the present report (Annex A, Page 47). However, an integrated solution employing a PDS(SR) offers additional benefits, and the performance of an external solution may also be unsatisfactory, depending upon the application. Figure 19 shows by way of example the two conceptual solutions for the safely-limited speed (SLS) safety sub-function. The motor speed is monitored for its compliance with a specific limit value. Should this speed be exceeded, i.e. in the event of a fault, the safe torque off (STO) safety sub-function is activated.

If for example motors with very high acceleration and speeds are used, the shut-off times in the external monitoring path in the event of a fault may be so high that a hazard cannot be avoided in time. Integrated solutions

[5] The number of encoders to be employed is dependent upon the safety function and the required PL/SIL. Additional measures for the detection of encoder faults may enable fewer encoders to be used. Some manufactures have implemented alternative methods for use of an encoder in the processor controls (see Chapter 7).

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 motor cannot be moved again until the intermediate circuit in the frequency inverter has been recharged after being switched back on. This may lead to undesired delays. Older frequency inverters 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. Furthermore, the mains contactor itself 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 inverter forms part of the overall safety function on the machine, and must also 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 inverter software are not required. The integrated solution thus also simplifies calculation of the *PFH* for the safety function.

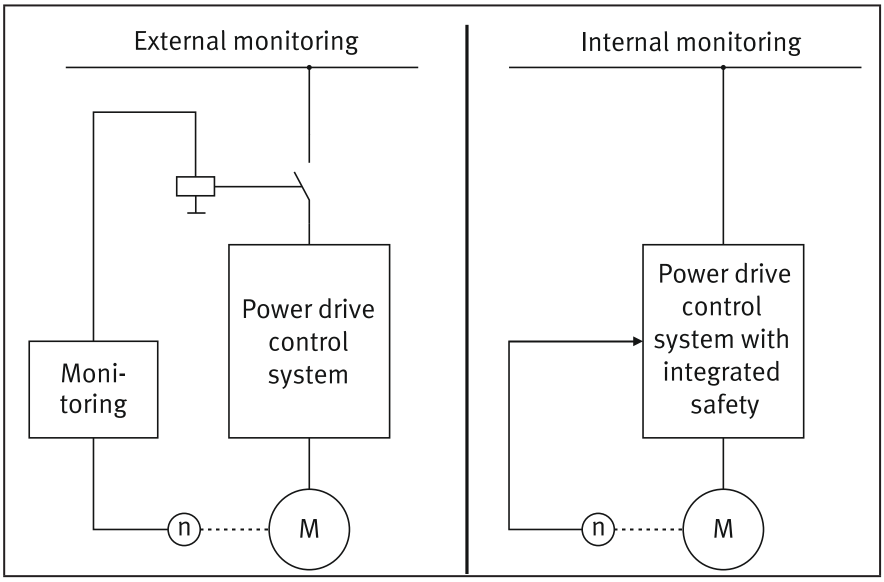

External monitoring
Internal monitoring
Moni-toring
Power drive control system
n
M
Power drive control system with integrated safety
n
M

Figure 18:
SLS with external monitoring and as an integrated solution

5 Safety functions in the application

5.1 PL, *PFH* and SIL

Frequency inverters with integrated safety sub-functions (PDS(SR)s) are safety components and logic units for safety functions in accordance with Annex IV of the Machinery Directive 2006/42/EC [6]. Information on their safety-related properties is required for their use. A PDS(SR) is used to implement one or more safety sub-functions for the purpose of risk reduction on a machine. The required scale of this risk reduction has been determined by the risk analysis of the hazardous zone 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 [12]) for the integral safety sub-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* value for each integrated safety sub-function of the PDS(SR). The *PFH* value may differ between multiple safety sub-functions, since they may make use of different components of the PDS(SR). If multiple safety sub-functions of a PDS(SR) are used at the same time, the individual *PFH* values can in principle be added together. Typically however, the safety sub-functions make use of largely identical hardware; the failure rate of many components must therefore be considered multiple times during this addition. The manufacturers of PDS(SR)s therefore frequently also state *PFH* values for the combination of integrated safety sub-functions.

$MTTF_D$ and *DC* values need not be stated for PDS(SR)s, since these values have already been considered during the determining of the PL and *PFH*. The achieved Category likewise need not be stated for the application of the frequency inverter. The “Information for use” clause of ISO 13849-1 does however require this information; certain type C standards also contain requirements concerning the Category.

5.2 Operating mode selection

Operating mode selector switches are employed on machinery for changes to control or work processes. Where diverse protective measures are used, an operating mode selector switch must be used that can be locked in any position. Each position of the selector switch must be clearly recognizable and 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 take priority over all other control and 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 operator. The requirements concerning the electrical circuits employed for this purpose and relevant to safety must however assure a comparable safety level.

Where certain work requires the machine to be operated with the protective action of the safeguards suspended, for example in setup mode or during fault clearance, the position of the selector switch must simultaneously be associated with the following criteria for the controls:

- 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 as long as the relevant control devices remain actuated (hold-to-run control device, such as inching control, enabling control).
- The operation of hazardous functions is possible only under conditions of reduced risk (such as limited speed, reduced power, step mode, limitation of the range of movement) and with the exclusion of hazards resulting from linked sequences.
- An intended or unintended action on the machine‘s sensors cannot give rise to any operation of hazardous functions.

These criteria for the controls are supplemented by those of Subclause 9.2.7 of IEC 60204-1 [9]. Worth mentioning 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 cause machine movements to start automatically; separate actuation of the start control must be required for this purpose. The starting of movements must always require deliberate action.

If the above criteria for the controls cannot be satisfied simultaneously, the control or operating mode selector switch must activate other protective measures. The design of these measures must assure a safe working area.

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

The above criteria for the controls concern safety functions, design requirements, and possibly further organizational measures. The operating mode selector switch therefore activates or deactivates the relevant safety sub-functions according to the operating mode. Consequently, component faults in the operating mode selection arrangement could lead to required safety sub-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 in 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 also prevents the operating mode selection from giving rise to an additional increase in the average probability of a dangerous failure per hour (*PFH_D*) in each individual safety function.

5.2.1 Safety sub-functions executed simultaneously

In some operating modes on machinery, the required risk reduction is attained by interaction between multiple measures, including the simultaneous execution of multiple safety sub-functions. This particularly applies to operating modes in which a machine must be operated with a guard open, for example for the purposes of setup or fault clearance. In these cases, safety sub-functions for limiting the speed (SLS) and for inching/enabling mode are frequently active simultaneously. The respective PL_r values for each of these safety sub-functions, which are intended to reduce the risk of the same hazardous movement, are determined by a risk analysis. Under certain circumstances, execution of the first safety sub-function may reduce the risk of the hazardous movement sufficiently for the risk analysis of the residual hazard for the second safety sub-function to result in a lower PL_r (see [4], Annex A, Example 4). Reduction of both PL_r values reciprocally by the safety sub-functions is not permissible, since this would lead to an unsatisfactory overall risk reduction. This can be prevented by iterative application of the risk graph. In the above example, the PL_r for SF 2 (safely-limited speed) was first determined. 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 operator and that he or she is able to avoid hazardous movements (risk parameter P1 instead of P2). Simultaneous execution of SF 2 and SF 3 therefore yields PL_r = c rather than PL_r = d for SF 3[6]. Refer also to SISTEMA Cookbook 6, Section 4.3.

5.2.2 Operating mode selection safety function

The provisions of the Machinery Directive governing operating mode selection require prevention of operation in an operating mode that has not been selected. This is generally achieved by means of safety technology which activates the safeguards required for the relevant operating mode and where applicable prevents unintended movements of individual machine parts. At the same time, other operating modes are blocked functionally via the machinery control system.

Operating elements commonly used for the selection of operating modes are described below.

a) Cam-operated selector switches:
Switches with positive mode of actuation (direct opening action) are considered well-tried components when they satisfy IEC 60947-5-1 [13], Annex K. They can therefore be classified in Category 1 to ISO 13849.

b) Cam-operated switches with further fault exclusions:

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

- Short-circuit of adjacent contacts that are mutually isolated
- Simultaneous short-circuit between the three terminals of changeover contacts

This can be demonstrated for example by a failure mode and effects analysis (FMEA). Categories higher than Category 1 are possible as a result (refer also to Example 8 in Annex A).

c) Other electromechanical switches:
An FMEA and possibly other measures must be taken for fault analysis.

d) Use of electronic equipment (such as a keypad or transponder) for selection of the operating mode

An FMEA and possibly other measures must be taken for fault analysis (refer in this context to IFA Report 2/2017e [4], Section I.3).

5.2.3 Inching control safety function

Standard pushbuttons with spring return are usually used as inching control devices. Observance of the closed-circuit current principle results in the movement being

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

halted when the actuator of the control device is released. The design of the pushbutton 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 it is released. Quantification of the inching control safety function requires the B_{10D} value of the pushbutton to be known. The component manufacturer usually states this value. Alternatively, suitable data can be found in ISO 13849-1 [2]. 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 an emergency-stop control device in the proximity of the inching button (refer to IFA Report 2/2017e [4], Section D.2.5.6).

5.2.4 Enabling control safety function (enabling control 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 their being bypassed is reduced to a minimum.

Two-stage and three-stage enabling switches are available. Fully depressing a three-stage enabling switch 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 button or by fully depressing it, 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. Use of enabling control devices/enabling switches that satisfy the provisions of the GS-ET-22 test principles of DGUV Test [14] is recommended (for modelling, refer to IFA Report 2/2017e, Section D.2.5.5). Should two-stage control devices be used, an emergency-stop control device must be fitted in addition in the proximity of the enabling switch.

5.2.5 Lower risk conditions

Should it be necessary for instance for persons to 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 anticipate the movement behaviour of parts of machinery. This includes limiting the travel range of axes (SLP, SDI), and where possible limiting travel to a single axis. Limitation of power (SLT) and step mode (SLI) may also be necessary. In addition, hazards resulting from linked sequences must be excluded, so that no automatic (sub-)processes are executed on the machine.

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

5.2.6 Influence upon the sensors of the machine

For automatic processes on machines, sensors are generally used that for example detect the position of workpieces. Based upon these sensor signals, a PLC may then start the next production step in automatic mode. In other words, a movement is initiated. Work performed on the machine with the safeguards open 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 [6] imposes the criterion for the 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 in which the sensors are deliberately influenced (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, for example during validation of the machine's safety functions.

5.2.7 Use of a portable control terminal

The control criterion of "use of a portable control terminal" is 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.

5.3 Stopping in case of an emergency

In accordance with the provisions of the Machinery Directive 2006/42/EC [6], Annex I, all machinery (with certain exceptions) must be fitted with one or more emergency stop devices that are able to avert actual or impending danger.

The emergency-stop function is triggered by a single human action by actuation of the emergency-stop device. This must cause the hazardous process to be brought to a standstill as quickly as possible and without creating additional hazards. The emergency-stop function must be available and operational at all times, irrespective of the operating mode, in order to enable a machine or installation to be brought to a standstill 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. Such a control command can for example be activation of the STO safety sub-function in the power drives.

Manual reset of the emergency-stop control device must however not trigger a re-start, and must be possible only 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 once again clear.

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 IEC 60204-1 [9]. Whether the appropriate measure is for the supply of energy to the machine drives to be interrupted immediately (STO) and the motors allowed to coast to a halt, or for the process to be controlled such that the hazardous movements are stopped as quickly as possible (SS1), must be assessed for each machine on a case-by-case basis.

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

Bringing a machine to a standstill as quickly as possible in an emergency can be achieved by controlled stopping by the power drive control. The SS1 safety sub-function is used for this purpose. This function can be implemented in a number of forms (see Section 3.1.1.2). However, compared to the form involving activation of the STO function following a predefined time delay, the SS1 function comprising a monitored deceleration 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 emergency stop is implemented must in addition feature suitable measures for electric shock protection, thereby obviating the need for an emergency-off function. Consideration must also be given to the fact that the final power removal following stopping does not necessarily mean isolation from the energy supply. Pulse blocking in the frequency inverter for example prevents a rotary field being generated in the motor; however, 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. Contactors are not generally suitable for isolation from the mains supply (refer also to Section 5.7 of this report).

The emergency-stop function is therefore an unsuitable means of isolation in order for work to be performed on the electrical equipment. Even “emergency off” may not necessarily guarantee isolation, since measures for emergencies described as emergency off are in fact often emergency stop. The terminological distinction between emergency off and emergency stop was introduced in 2005 in IEC 60204-1 [9], but has yet to become universally adopted.

5.4 Stopping and holding in position

5.4.1 Stopping of loads

Braking a movement to standstill constitutes a safety function, and must be evaluated in accordance with ISO 13849-1 [2], when the risk assessment indicates that the coasting movement presents a hazard, and in the interests of risk reduction the movement must be brought rapidly to a halt by braking of the drive. This is the case for example with hazardous movements involving overrun that are not safeguarded by locked safety guards up until the stationary state has been reached. On such machines, the hazardous zone may become accessible 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.

Adjustable speed power drives are generally driven by frequency inverters. These are typically suitable not only for driving the motors, but also for controlled stopping. The kinetic energy generated in the frequency inverter during braking is either fed back into the mains system or converted into thermal energy in a braking resistor.

Mechanical brakes serve either to stop movements (service brake) or to hold loads in position once stationary (holding brake). The braking force is generally provided by springs. The brake is released electrically, pneumatically or hydraulically. With this concept, braking action is also provided in the energy-free state (closed-circuit current principle).

Requirements concerning stopping of adjustable speed drives

Risk assessment on the machine yields certain requirements upon the "stopping" safety function. In particular, the behaviour of the control system in the event of a fault and in the event of voltage breakdown, together with the resulting additional hazards, must be considered in accordance with the PL_r. In accordance with ISO 12100 [7] Subclause 5.4 b), the following two operating states must also be considered when frequency inverters are used for stopping:

- **Normal operation**

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

- **Malfunction**

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

Extended run-down times may therefore arise during a malfunction. Since the power unit of all known inverter-actuated power drive controls is of single-channel architecture, a fault immediately results in failure or reduced performance of the braking function. This applies both to conventional frequency inverters, and to those with an integrated SS1 or SS2 safety sub-function in which – following the incidence of a fault – the drive is de-energized (STO); controlled stopping is therefore no longer possible (see Sections 3.1.1.2 and 3.1.1.3). It must be determined on a case-by-case basis whether the behaviour is acceptable for the application concerned. It is unacceptable for example where calender rolls are braked to a halt: if persons are working close to the entrapment point, the availability of the braking function is crucial.

Depending upon the PL_r that must be satisfied for the function of safe stopping, braking to a halt by frequency inverters may have to be supplemented by other measures, such as the use of a mechanical (linear or rotary) service brake, or braking by means of a DC voltage.

Note:

Some frequency inverters/servo controllers supply their control electronics from the intermediate circuit and are thus able to bring a movement to a controlled stop despite a voltage breakdown (see Section 5.5.1).

5.4.2 Holding of loads against gravity (vertical axes)

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

In accordance with ISO 12100 [7] Subclause 5.4 b), the following two operating states must be considered for vertical axes:

Normal operation:

The machine executes the intended function:

a) Once the frequency inverter has performed a controlled stop, it also assumes the function of safe holding against gravity (SS2).

b) Alternatively, once the frequency inverter has performed a controlled stop (SS1), a holding brake is actuated (SBC) that maintains the load in position.

Malfunction:

A failure of the power supply or of the frequency inverter as a result of a fault leads to the frequency inverter being unable to hold the load against gravity.

In the event of a malfunction, the functions of stopping and holding against gravity must be performed by a mechanical brake (such as a spring-operated brake with emergency-stop capability, see [15]). The particular 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 IEC 60204-1 [9], Subclause 9.2.3.4.2, the emergency-stop function must take the form of either stop category 0 or stop category 1. In other words, the drive energy is always switched off, making mechanical brakes indispensable.

Requirements concerning holding against gravity

Risk assessment on the machine yields certain requirements upon the "holding against gravity" safety function. Detailed information on determining the PL_r and on suitable protective measures can be found in Expert Committee Information Sheet 005, Gravity-loaded axes (see Annex B). The comments in Section 5.5, Failure of the power supply, are also useful.

5.4.3 Mechanical brakes serving as components for safety functions

Where placed on the market separately, holding brakes intended by the manufacturer for the safe holding of loads against gravity constitute safety components in accordance with Article 2 (c) of the Machinery Directive [6]. The same applies to service brakes used to reduce the run-down 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 solely the responsibility of the machinery manufacturer to implement the relevant safety functions correctly [16].

Requirements to be met by mechanical brakes in safety functions exist at this time only for emergency brakes with holding brake function for linear movements. They are described in the GS-MF-28/04.2015 test principles [15] of DGUV Test.

Besides design requirements, tests are set out for demonstrating the mechanical life. 1,000,000 operation cycles under static load and 2,000 operation cycles under dynamic load must be demonstrated under testing.

5,000,000 operation cycles are generally required for rotary brakes for machine tools.

Note:

A spring-operated brake is frequently employed. The braking force is generated by several braking springs, which force 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, ISO 13849-1 [2] requires fault-detection measures in the application for Category 2 upwards. 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, 1.3 times the maximum load torque is applied to the brake by the drive motor. Provided the position of the load is held within the specified range, the brake is considered properly functional. Should the position depart from the specified range, the brake must be checked in accordance with the instruction manual and if necessary 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 run-down time must be measured and compared with the permissible values. Should a permissible value be exceeded, further use of the machine must be prevented. The mechanical brake must be replaced if necessary.

Note:

The dynamic test has the purpose of ensuring that the overrun during braking does not lengthen impermissibly in the course of the 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 due in part 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.

5.5 Failure of the power supply

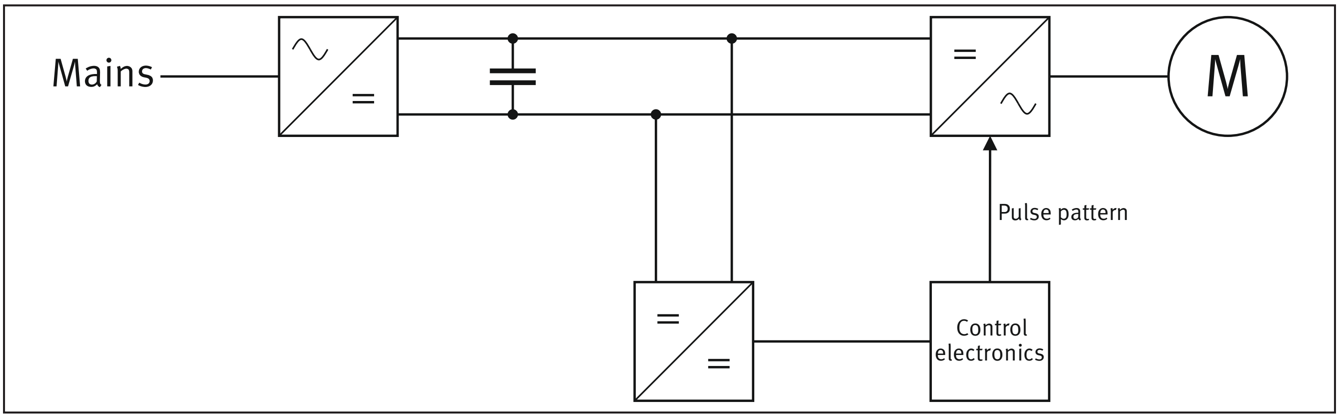
Failure of the power supply can occur at any time. This situation must be considered during engineering of a frequency inverter for a machinery control system, and does not constitute a fault condition (ISO 12100 [7] Subclause 5.4b, Possible states of the machine: disturbance of its power supply; ISO 13849-1 [2], Subclause 5.2.8, Fluctuations, loss and restoration of power sources). The risk analysis of a machine must consider a voltage breakdown and in particular the time characteristics of safety functions. Should stopping as fast as possible (SS1 or SS2) be necessary but no longer be achievable by means of the frequency inverter, additional mechanical brakes can for example be employed. This is also always the case for vertical axes.

The impact of a voltage breakdown upon a frequency inverter and its ability in this situation to generate a torque in a motor or a force in a linear motor is dependent upon the inverter‘s internal design. The deciding factor is the source of the electrical energy supplied to the frequency inverter‘s control electronics. A distinction must be drawn here between frequency inverters in which the power for the control electronics is supplied from the intermediate DC circuit (see Section 5.5.1) and those in which it supplied from the mains system (Section 5.5.2).

5.5.1 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 20).

Figure 20:
Supply of power to the control electronics from the intermediate DC circuit



At the instant of voltage breakdown, 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 patterns for driving the IGBTs (insulated-gate bipolar transistors) in the power unit of the frequency inverter.

This enables torque to be generated in the motor. In many applications, the motor should be brought to a standstill as swiftly as possible in the event of voltage breakdown. Owing to the intermediate DC circuit being charged, this is still possible for a certain duration, particularly since, depending upon their design, frequency inverters 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 still 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 sub-function.

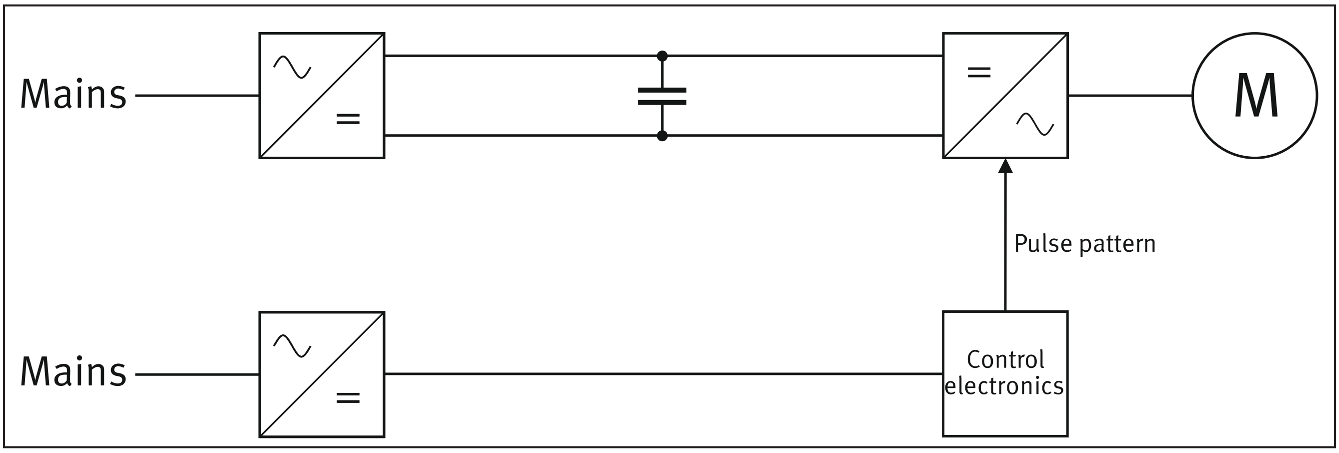
The feeding back of energy into the supply system may no longer be possible following a voltage breakdown. The kinetic energy generated by the braking process must therefore be consumed even where the frequency inverters possess energy recovery capability. This is achieved by braking resistors. Were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

5.5.2 Power supply to the control electronics from the supply system

In this type, the control electronics receive their operational voltage from the supply system via a power supply unit (Figure 21, Page 34). Supply from a separate 24 V system is also common; such a system also fails however in the event of a mains voltage breakdown, unless an uninterruptible power supply (UPS) is employed.

Should the mains supply fail, the control electronics also no longer receive power and are not able to generate pulse patterns for the power unit of the frequency inverter. The motor is no longer able to generate torque, and neither controlled stopping nor the holding of a load against gravity is possible. The motor coasts to a halt; loads held by vertical axes drop. This behaviour is also exhibited by frequency inverters with integral SS1, SS2 and SOS safety sub-functions. Should this situation give 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 sub-function.

Figure 21:
Power supply to the control electronics from the supply system



5.5.3 Consideration of voltage breakdown in safety functions in accordance with 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_D values. Since its third edition, the standard proposes in this case that different safety functions be provided for the two states:

a) With energy available,

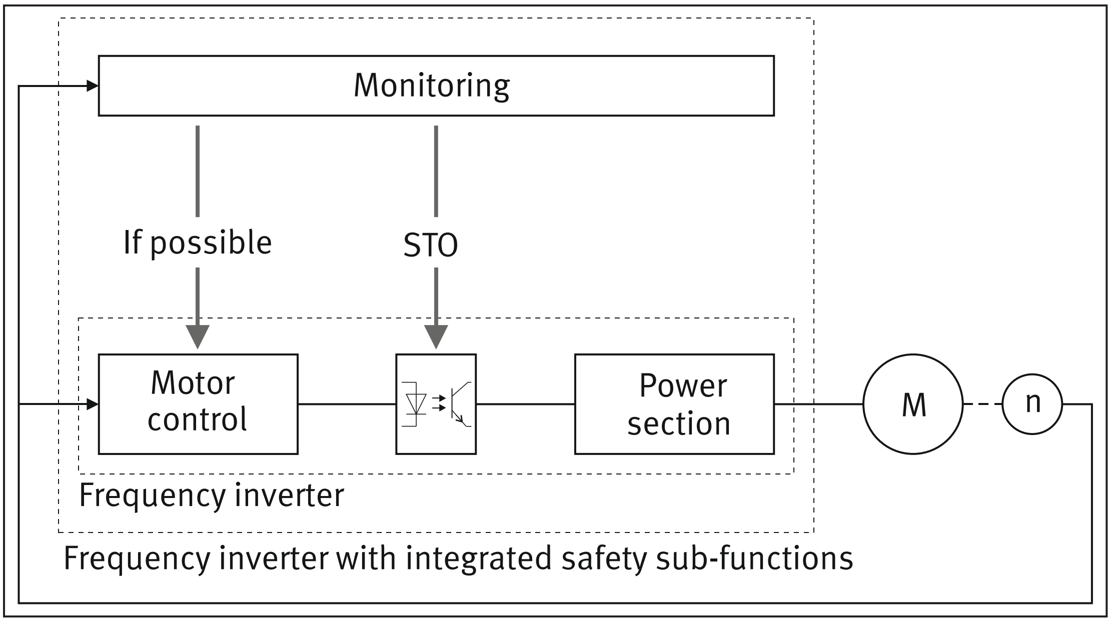
b) Without energy available.

If it is assumed that under normal circumstances, power is available, this approach may result in evaluation of the risk parameters to ISO 13849-1 [2] yielding different results for the two safety functions. In certain cases, this may enable safety functions to be achieved with a lower PL_r in the state in which energy is not available, depending upon the specific risk parameters.

5.6 Limitations of safety sub-functions

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

Figure 22:
Frequency inverter + monitoring + pulse blocking = frequency inverter with integrated safety sub-functions



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 sub-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 exceeding of the maximum speed limit is detected (SLS safety sub-function), stopping is initiated. Whether controlled stopping is still possible, or merely coasting to a halt, depends upon the functions still available in the frequency inverter. If the closed-loop motor control is still functioning properly and the power unit is not malfunctioning, the motor can be stopped as fast as possible. If however a fault is present in the closed-loop motor control of the frequency inverter, 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 in the event of a fault but to activate the STO safety sub-function and allow the motor to coast to a halt. The possibility of this behaviour must be considered during specification of the safety functions required for a machine, and additional measures taken if necessary. If for example a prolonged stopping time in the event of failure of SS1 or SS2 is not acceptable, or loads held 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 inverters featuring integral safety sub-functions. As far as the authors are aware, redundancy has not as yet been implemented in the control and power units in order to ensure availability. Even were such redundancy to be available, a solution would still have to be found for the voltage breakdown.

Many safety sub-functions require parameters to be specified that determine their behaviour. Particular attention must be paid here to the time characteristic. A fault must first be detected before a suitable reaction can be triggered and the safe state brought about.

Figure 23 shows by way of example the time characteristic for the SLP safety sub-function.

The set maximum value for the position of an axis is surpassed at time t_0. At t_1, monitoring detects exceeding of the value and activates STO. The drive coasts down and comes to a halt at t_2. From time t_0 to time t_2, 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 sub-function, and the limit value must be set correspondingly lower in order to prevent departure from the legal range.

The STO safety sub-function is not a monitoring function; it merely ensures that functional driving 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 unit. 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.

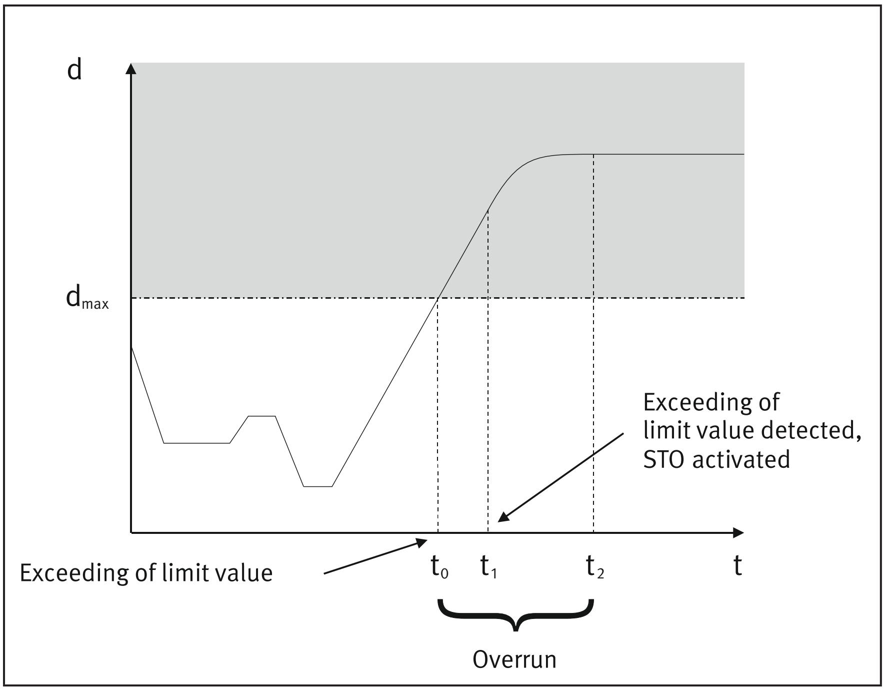


Figure 23:
Distance/time chart of the SLP (safely-limited position) safety sub-function

In applications employing STO, it must be determined whether jerking in the event of a fault can be tolerated. If not, a supplementary mechanical brake may have to be employed. This is the case for example on 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 sub-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 relevant information in the instruction manual. The following must be noted during engineering of a power drive control with integral safety sub-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 sub-function?
- What reaction time must be considered before the safe state is brought about?
- What hazard exists as a result in the application?
- Are additional measures required (such as a mechanical brake or a greater distance between the light curtain and the hazardous zone)?

5.7 Isolation from the sources of energy during repair and maintenance work

The preceding sections have described a range of safety functions and safety sub-functions that are implemented by means of power drive control devices and other safety-related parts of control systems without the drive having to be disconnected from the power supply.

These safety functions are however not suitable for all application scenarios and operating modes of the machine. Maintenance work, in particular, requires isolation from the sources of energy.

5.7.1 Requirements deriving from the Machinery Directive

The Machinery Directive 2006/42/EC [6] sets out the following requirements in Annex I, Section 1.6.3, Isolation of energy sources:

- *“Machinery must be fitted with means to isolate it from all energy sources. Such isolators must be clearly identified. They must be capable of being locked if reconnection could endanger persons. Isolators must also be capable of being locked where an operator is unable, from any of the points to which he has access, to check that the energy is still cut off.”*
- *“In the case of machinery capable of being plugged into an electricity supply, removal of the plug is sufficient, provided that the operator can check from any of the points to which he has access that the plug remains removed.”*
- *“After the energy is cut off, it must be possible to dissipate normally any energy remaining or stored in the circuits of the machinery without risk to persons.”*
- *“As an exception to the requirement laid down in the previous paragraphs, certain circuits may remain connected to their energy sources in order, for example, to hold parts, to protect information, to light interiors, etc. In this case, special steps must be taken to ensure operator safety.”*

The “Guide to application of the Machinery Directive 2006/42/EC” [17] provides further explanatory information in this respect.

According to the guide, the objective of the requirements set out in the first paragraph of Section 1.6.3 [6] is to keep machinery in a safe condition while maintenance is being carried out. Operators carrying out maintenance operations while the machinery is stopped must be able to isolate the machinery from its sources of energy before intervening in order to prevent dangerous occurrences such as unexpected start up of the machinery, whether due to machinery faults, to the action of other persons who may ignore the presence of maintenance operators or to inadvertent actions of the maintenance operators themselves.

Where the operators carrying out maintenance operations cannot easily check that the means of isolation remain in the isolating position, the isolators must be designed so that they are lockable in this position. When it is foreseeable that several operators may have to carry out maintenance operations simultaneously, the isolator should be designed so that each of the operators concerned can place his or her lock on the isolator for the duration of his or her intervention.

The second paragraph applies mainly to hand-held power tools or transportable machinery, where the operator can check from any of the points to which he has access whether or not the electricity supply is connected.

The stored energy referred to in the third paragraph may include, for example, kinetic energy (inertia of moving parts), electrical energy (capacitors in intermediate circuits), fluids under pressure (in fluidic systems), or potential energy (in springs or parts of the machinery that may move due to their own weight).

The circuits referred to in the fourth paragraph, which need not be isolated from the source of energy, include those for the operation of tools or for the extraction of hazardous substances. In such cases, the safety of operators can be assured by measures such as preventing access to the circuits concerned or providing appropriate warnings or warning devices.

The manufacturer‘s instruction manual or maintenance manual must include information on the isolation of energy sources, the locking of the isolator, the dissipation of residual energies and the verification of the safe state of the machinery (refer to the Guide to the Machinery Directive [17] Section 272: Comments on section 1.7.4.2 (letter s)).

A special requirement concerning the isolation of batteries on mobile machines is set out in the Machinery Directive [6], Annex I, Section 3.5.1.

5.7.2 Requirements deriving from IEC 60204- 1

Regarding the electrical equipment of machinery, IEC 60204-1 [9] contains the relevant specifications for reliable disconnection from the power supply.

In accordance with Section 5.3.1 of [9], a supply disconnecting device shall be provided for:

- *Each incoming source of supply to one or more machines,*

- *Each on-board power supply.*

Where required, the supply disconnecting device must disconnect the electrical equipment of the machine from the power supply (for example for the performance of work on the machine, including work on the electrical equipment).

Depending upon the work to be performed in the course of maintenance, IEC 60204-1 [9] distinguishes between:

a) Devices for switching off for prevention of unexpected start-up (Subclause 5.4)

b) Devices for disconnecting electrical equipment (Subclause 5.5)

The requirements in Subclauses 5.4 and 5.5 permit the following overview:

a) Prevention of unexpected start-up	**b) Disconnecting of the electrical equipment**
Devices and equipment **with** disconnector characteristics • All work required in the course of maintenance (servicing, fault clearance, repairs).	Devices and equipment **with** disconnector characteristics • All work required in the course of maintenance (servicing, fault clearance, repairs).
Devices and equipment **without** disconnector characteristics • Inspections, • Adjustments, • Work on the electrical equipment, where: – There is no hazard arising from electric shock or burn; – The device for switching off remains effective throughout the work – The work is of a minor nature (for example replacement of plug-in devices without disturbing existing wiring).	Devices and equipment **without** disconnector characteristics • Not permissible.

The permissible devices and equipment for a) and b) and the requirements concerning the suitability, accessibility, marking and the prevention of re-closure are to be taken from IEC 60204-1 [9], Subclauses 5.3 to 5.6.

Conclusion:

As shown by EN 60204-1 [9], devices for switching off for prevention of unexpected start-up that do not possess disconnector characteristics are suitable only for minor work under certain conditions. Inspection and adjustment work for example is permitted. Work on the electrical equipment is permissible only when no risk of electric shock or burns caused by arcing exists and the device for switching off remains effective at all times.

This applies even if a higher Performance Level to ISO 13849, such as PL d, is observed for the safety-related part of the control system/the safety function.

For any work of a more extensive kind, such as repair work and fault clearance, devices and equipment with disconnector characters are required.

Conventional contactors do not generally have disconnector characteristics.

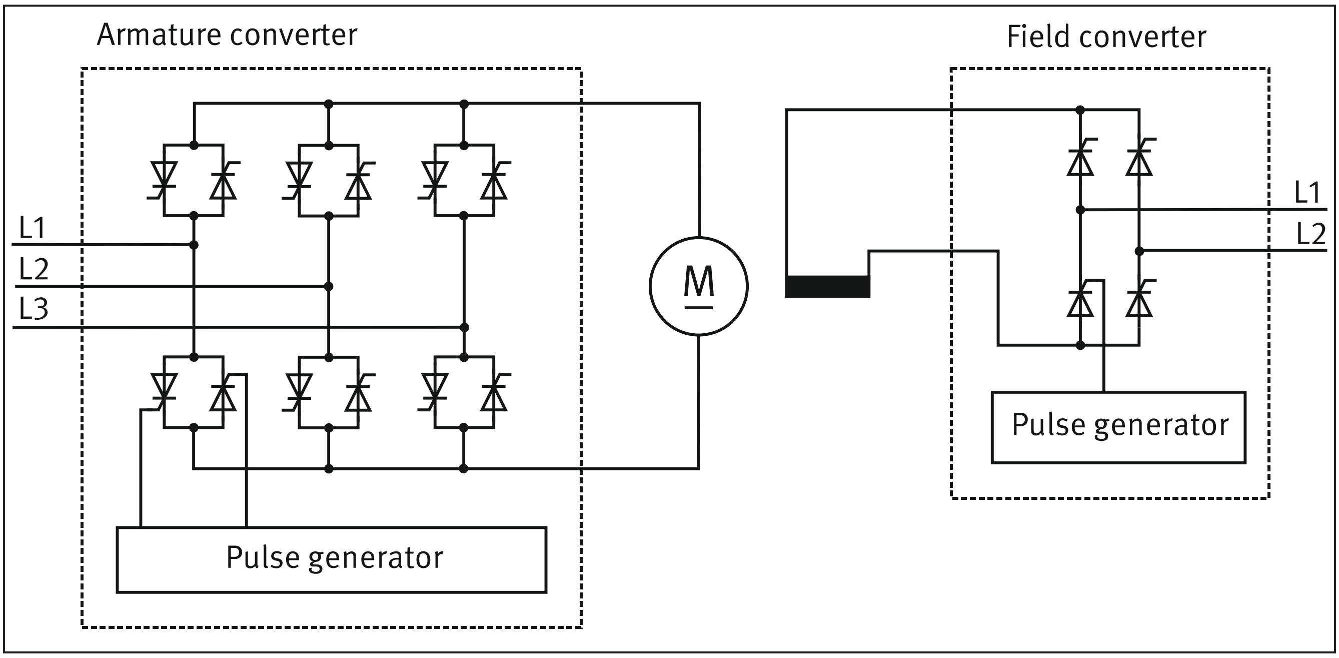
6 Safety functions on DC drives

As already stated, as recently as a few decades ago, the majority of adjustable speed drives employed DC technology, owing to the associated ease of control. This function is now assumed almost exclusively by three-phase drives employing frequency inverters or servo controllers. For this reason, this report concentrates on the safety functions implemented in conjunction with power drive controls for three-phase motors.

DC drives should not be ignored completely however, since they are still used in some applications, particularly in heavy industry (such as in two-roll 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 with the current supplied by the field converter. The armature draws its energy from the armature converter. The speed of the motor can be adjusted up to its rated speed by variation of the armature voltage. At a constant load, an increase in the armature voltage results in a corresponding 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-angle control, the firing pulses of which are 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 (Figure 24).

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



For the speed of the machine to be increased beyond its rated speed, the excitation field must be attenuated. This can be achieved by a reduction in the current in the excitation winding. The circuit used for this purpose is part of the separate field converter.

In principle, safety sub-functions are integrated into power drive controls for DC motors in the same way as with three-phase motors. A major difference exists with regard to the STO safety sub-function, however.

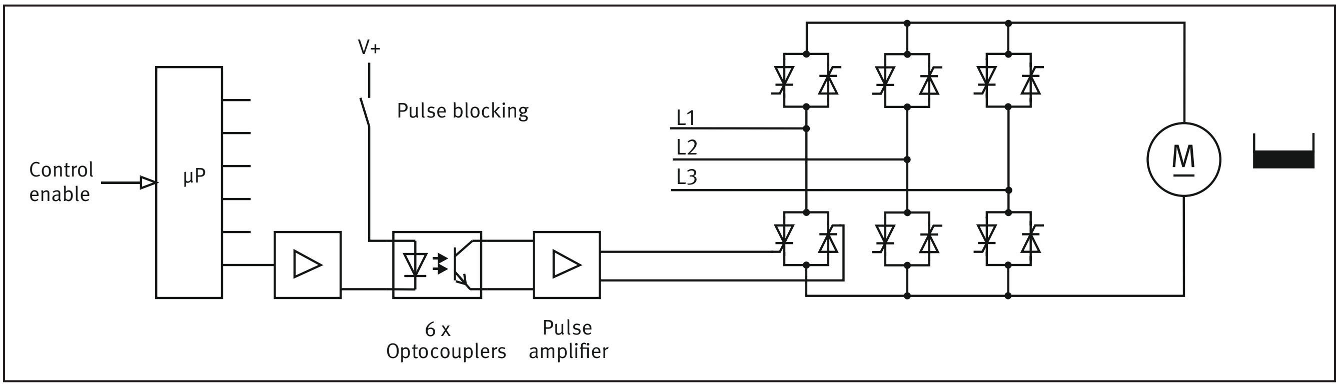
In order for the STO safety sub-function to be implemented, generation of a torque in the motor must be prevented. One means of achieving this is by preventing the flow of current in the armature. This is possible for example by the use of a mains contactor to shut off the power supply to the motor armature. For a number of reasons, power switchgear is not always suitable for this purpose, however (see Section 4.3). Integrating the safety sub-function into the power drive control has advantages. Pulse blocking has already been described as a suitable measure for implementing the STO safety sub-function within the power drive controls of three-phase motors. Shutting off the supply voltage for the transmission elements (such as optocouplers) disables excitation of the power semiconductors.

Figure 25 illustrates this concept with reference to the example of the armature converter of a DC motor.

In contrast to three-phase drives, for which complex pulse patterns are required for 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 sub-function, and constitutes the crucial difference between three-phase and DC drives. In the case of three-phase drives, it can be assumed that if the transmission of pulses is reliably blocked, random component faults in the final stage cannot generate a rotary field – and therefore torque – in the motor. 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 controller enable shut 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 unit for the three-phase motor; in this case however, it could cause only 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), pulse blocking in the armature converter is not a sufficient measure on its own. For these Categories, an additional shut-off path is required, even if pulse blocking is of two-channel or single-fault-tolerant design. This additional shut-off path could for example take the form of an additional mains contactor or circuit breaker in the armature circuit.

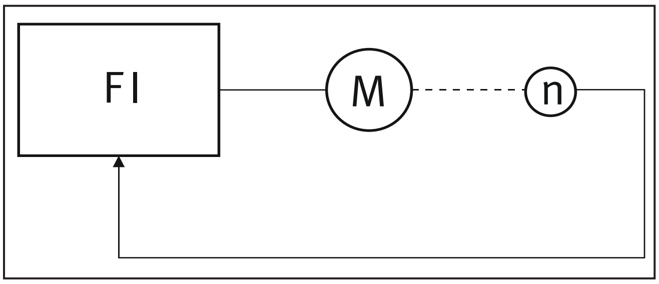
Figure 25:
Pulse blocking inside the armature converter



7 Position encoders in safety functions

For commutation and control of a motor, the instantaneous position must be known to the frequency inverter/servo controller. This information is normally provided by a rotary or linear encoder[7]. This enables a closed control loop to be created that is used for example for positioning tasks (see Figure 26).

Figure 26:
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. Depending upon the requirements of the safety sub-function to be implemented, a power drive control connected to the encoder can use this information for example to determine speed (safely-limited speed, SLS) and/or acceleration (safely-limited acceleration, SLA). Knowledge of the absolute position is not required in these cases.

If, however, safety functions are for example to safeguard crushing points on a machine, certain parts of the machine must not depart from the permissible travel range. This can be achieved by means of the SLP (safely-limited position) safety sub-function, for which knowledge of the absolute position is required. A reliable reference position of the incremental encoders must first be obtained at start-up. This is generally achieved by travel to a defined position in the machine at which an additional position sensor is fitted. Once the machine has travelled to this reference point, the absolute position can be computed in the power drive control by the addition or subtraction of increments.

The use of absolute value encoders is simpler. In this case, a digital position signal is already available and referencing is not needed. A distinction is drawn between single-turn and multi-turn rotary encoders. On single-turn encoders, a unique 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 it has completed, thereby also providing a unique absolute value after several turns.

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 inverter 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 safety 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 hazardous failure of a safety function may occur even on safety encoders; measures for fault detection are therefore required. This is often not possible in the encoder itself, but must be implemented in the frequency inverter 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. Testing for $\sin^2 + \cos^2 = 1$ is often used on sin/cos encoders.

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 allow a hazardous fault to arise undetected. This imposes constraints, particularly for use on gravity-loaded vertical axes. A solution is the use of encoders that have been mechanically overdimensioned by the manufacturer, thereby enabling encoder shaft breakage to be excluded (see [3], Table D.8).

Note:

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

[7] Frequency inverters 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 sub-functions, however.

Should safety encoders not be 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 way 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 is met (see [16] and [19]). For this purpose, an FMEA must be conducted of the possible failure types of all components involved in signal generation and processing and of their effects upon the safety function (refer to the GS-IFA-M21 test principles [20]). 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 $\sin^2 + \cos^2 = 1$, further means exist of detecting encoder faults: the encoder can for example be integrated into the frequency inverter/motor control loop. Faulty encoder signals then generally lead to an incorrect value being delivered for the motor position, and correct commutation of the motor consequently no longer being possible. This leads to an operating fault and thus to detection of the fault via the technical process. It must be considered however that modern control algorithms may function temporarily without requiring an encoder, even when an encoder is connected; swift fault detection on the machine is not therefore assured in this case.

Processing of signals from safe sine/cosine encoders

If encoders are employed in conjunction with safe frequency inverters, speed monitors or standstill monitors, 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 control unit and – where applicable – the configuration of parameters. Signals are interpreted in the control units according to the PL/SIL stated. If dedicated circuits are designed, however, the following must be considered.

Sin/cos encoders supply two signals at the output – the sine signal and the cosine signal. If these two signals are interpreted independently of each other and the required fault exclusions within the encoder can be demonstrated, the encoder and control unit could constitute a continuous two-channel arrangement. This is relevant when Category 3 or 4 to ISO 13849-1 [2] is to be attained. This two-channel characteristic is lost however when the sine and cosine signals are both used for implementation of a safety function. This is the case for example when, for the purpose of the safety function, the absolute position is formed (for which the direction of rotation/movement must be determined from both sine AND cosine), the hardware in the control unit employs quadrature decoder ICs (see [19]), or intermediate values are formed from sine AND cosine by interpolation. Depending upon the required PL, a second channel may then have to be added, for example by the use of a second encoder.

8 Configuration test

The system behaviour of each power drive control is adapted to the application in question by means of configurable parameters. This entails, for example, the setting of maximum permissible speed values or limits for the time characteristic during stopping of a drive. The settings must be reviewed, irrespective of whether safety sub-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, speed, etc.), and thereby to detect any engineering or input errors.

Transmission errors, for example in the connection between the non-safe PC and the safe parameter memory, are not assumed during the configuration test. Specific requirements apply to the parameter configuration procedure; these requirements are described in ISO 13849-1 [2], Subclause 4.6.4. The purpose of the configuration test is to detect parameters for which incorrect values have been selected, notwithstanding the fact that setting of the values in the safe control system has been performed correctly. The following sources of faults are possible:

- Setting of unsuitable limit values for speed, braking to standstill, time delays, position, etc.

- Parameter values have in principle been selected correctly, but are unsuitable for certain machine states

- Input errors during parameter configuration

- Priority conflicts with other safety sub-functions

- Different requirements for parameter assignment depending upon the operating mode

A configuration test must be performed following commissioning of a machine and following any modifications to the machine‘s hardware or software. This includes modifications made by remote data transfer.

In his user documentation, the drive manufacturer must include instructions for performance of a configuration test, for example in the form of a checklist. The test must be performed by authorized personnel and be documented in a suitable form.

The configuration test must consider the behaviour in the event of a voltage breakdown and in response to faults arising within the safety function.

For series production machines, the configuration test need not be repeated for all machines when a complete configuration test has been performed on a model machine and the safety-related parameter data are subsequently transferred with assured integrity to the series production machines, or it is ensured that the safety sub-functions are configured in all devices as intended.

References

[1] EN 954-1: Safety of machinery – Safety-related parts of control systems – Part 1: General principles for design (1997).

[2] ISO 13849-1: Safety of machinery – Safety-related parts of control systems – Part 1: General principles for design (2015).

[3] IEC 61800-5-2: Adjustable speed electrical power drive systems – Part 5-2: Safety requirements – Functional (2016).

[4] *Hauke, M.; Schaefer, M.; Apfeld, R.; Bömer, T.; Huelke, M.; Borowski, T.; Büllesbach, K.-H.; Dorra, M.; Foermer-Schaefer, H.-G.; Uppenkamp, J.; Lohmaier, O.; Heimann, K.-D.; Köhler, B.; Zilligen, H.; Otto, S.; Rempel, P.; Reuß, G.:* Functional safety of machine controls – Application of EN ISO 13849. IFA Report 2/2017e. Published by: Deutsche Gesetzliche Unfallversicherung (DGUV), Berlin, Germany 2017. http://publikationen.dguv.de/dguv/ pdf/10002/rep0217.pdf

[5] IEC 61508: Functional safety of electrical/electronic/programmable electronic safety-related systems – Parts 0 (2005) to 7 (2010).

[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/legal-content/EN/TXT/PDF/?uri=CELEX:32006L0042&from=DE

[7] ISO 12100: Safety of machinery – General principles for design – Risk assessment and risk reduction. Beuth, Berlin, Germany 2010.

[8] ISO 13849-2: Safety of machinery – Safety-related parts of control systems – Part 2: Validation (2012).

[9] IEC 60204-1: Safety of machinery – Electrical equipment of machines – Part 1: General requirements (2005).

[10] *Apfeld, R.; Portmann, M.:* Festlegen von Maximalgeschwindigkeiten für manuelle Eingriffe an laufender Maschine (code 330 216). In: IFA-Handbuch Sicherheit und Gesundheitsschutz am Arbeitzplatz. 2nd edition, Vol. XII/2011. Published by: Deutsche Gesetzliche Unfallversicherung (DGUV), Berlin, Germany. Erich Schmidt, Berlin, Germany – loose-leaf. 2nd edition 2003.
www.ifa-handbuchdigital.de/330216

[11] Grenzwerteliste 2017 – Sicherheit und Gesundheitsschutz am Arbeitsplatz. IFA Report 3/2017. Published by: Deutsche Gesetzliche Unfallversicherung (DGUV), Berlin, Germany 2017.
www.dguv.de/ifa/grenzwerteliste

[12] IEC 62061: Safety of machinery – Functional safety of safety-related electrical, electronic and programmable electronic control systems (2015).

[13] IEC 60947-5-1: Low-voltage switchgear and controlgear – Part 5-1: Control circuit devices and switching elements – Electromechanical control circuit devices (2016).

[14] Grundsätze für die Prüfung und Zertifizierung von Elektromechanischen Zustimmungsschaltern und Zustimmungseinrichtungen (GS-ET-22). 7/2016 edition. Published by: Fachausschuss Elektrotechnik, Prüf- und Zertifizierungsstelle im DGUV Test, Cologne, Germany.
www.bgetem.de, Webcode 12204269

[15] Prüfgrundsatz für Notfallbremsen mit Haltefunktion für lineare Bewegungen (GS-MF-28). 04/2015 edition. Published by: Prüf- und Zertifizierungsstelle Maschinen und Fertigungsautomation im DGUV Test, Mainz, Germany 2015.
www.dguv.de/dguv-test/prod-pruef-zert/pruefgrundsaetze-erfahrung/pruefgrundsaetze/maschinen/index.jsp

[16] *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, Germany 2011. http://publikationen.dguv.de/dguv/pdf/10002/standardkomponenten.pdf

[17] Guide to application oft he Machinery Directive 2006/42/EC. Edition 2.1 – Juli 2017. Published by: Bundesministerium für Arbeit und Soziales (BMAS), Berlin, Germany. https://www.bmas.de/SharedDocs/Downloads/DE/Thema-Arbeitsschutz/guide-to-application-of-the-machinery-directive.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 (2010).

[19] *Apfeld, R.*: Brauchen sichere Antriebssteuerungen auch sichere Positionsgeber? Published by: Institut für Arbeitsschutz der Deutschen Gesetzlichen Unfallversicherung (IFA) 2017.
www.dguv.de/medien/ifa/de/pub/rep/pdf/reports2013/ifar0713/positionsgeber_ifa.pdf

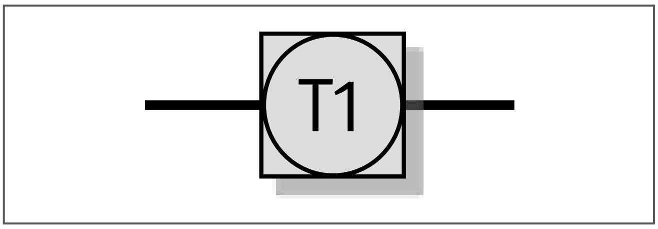
[20] Prüfgrundsatz GS-IFA-M21. Grundsätze für die Prüfung und Zertifizierung von Winkel- und Wegmesssystemen für die Funktionale Sicherheit. Published by: Deutsche Gesetzliche Unfallversicherung (DGUV), Berlin, Germany 2015.
www.dguv.de, Webcode d11973 (the tool for static analysis is also available here).

Annex A:
Circuit examples employing frequency inverters

The following collection of circuit examples was compiled in order to illustrate the use of frequency inverters in practice. The examples are the product of many years‘ experience in consulting and testing in the area of safety-related machinery control systems, but do not discuss manufacturer-specific proposals for implementation. For the sake of simplicity, some of the control equipment used for satisfaction of the criteria for the controls (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 taken from ISO 13849-1 ([S]) or assumed values ([A]).

As in IFA Report 2/2017e, the symbols used in the presentation of the safety-related block diagrams in the circuit examples below include the encapsulated subsystem:



Encapsulated subsystems describe safety components for which the manufacturer states PL (or SIL) and *PFH* values. These data are sufficient for consideration in safety functions; the influence of the category, basic and well-tried safety principles, $MTTF_D$, *DC*, CCF and the measures taken against systematic failure, including software, has already been considered. Should SISTEMA be used for quantification, only the PL and *PFH* need be entered (refer also to SISTEMA Cookbook Volume 1, Section 4.5).

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

Table A.1:
Overview of the circuit examples

Keyword	Circuit example with		
	PL c	PL d	PL e
Safe guard monitoring, STO	1, 2, 8	3, 6, 7, 8, 9, 10, 15	12
Park position monitoring	1, 2		
SLS		4, 8, 9	
Enabling control	8, 9	4	
Emergency stop		5, 11	
SS1		5, 9, 10	
Guard locking		7, 11	
Operating mode selection		8, 9	
Manual reset		10	
Safe motion control		11	
Force-operated door		13	
Holding of vertical axis against gravity	14 (voltage breakdown)	14	
DC-drive, STO		15	
Safe roll stop		16	

Example 1: Stopping in response to departure of an axis from the safe park position when the safety guard is open – PL c

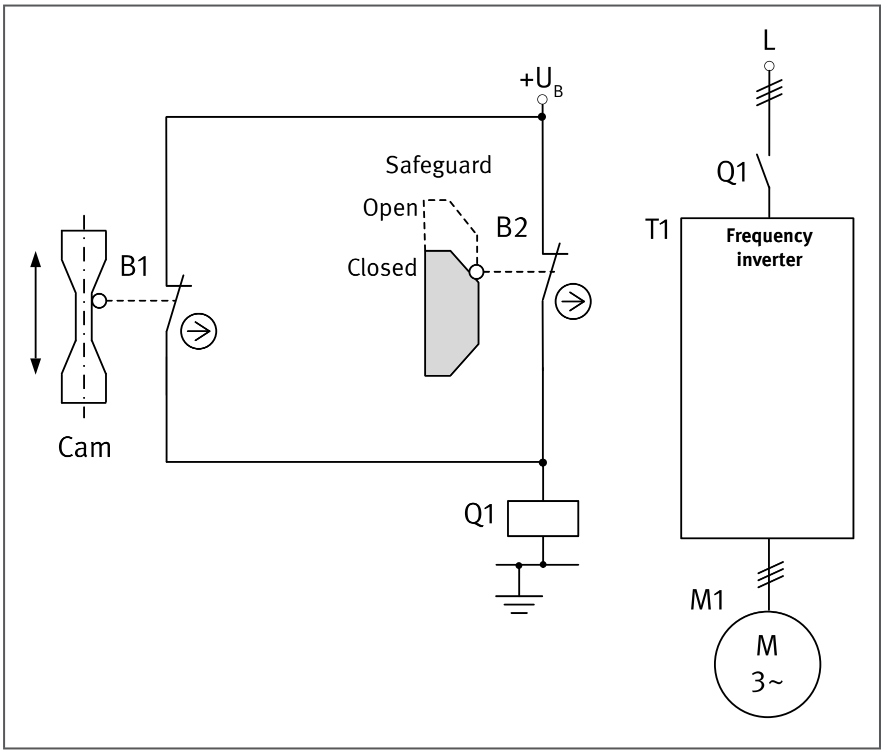


Figure A.1:
Combined position monitoring of an axis with the aid of a cam switch

Safety function

- SF 1: Should the axis depart from 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).

Functional description

- Before a manual intervention is performed, 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 start up unintentionally, B1 is actuated and the shunt of B2 removed. If the safety guard is open, dropping out of the mains contactor Q1 causes an uncontrolled stop (stop category 0 to IEC 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

- Basic and well-tried safety principles and the requirements for Category B are observed. Protective circuits (such as contact protection), as described in the first sections of Chapter 8 of IFA Report 2/2017e, are present. This example employs basic safety principles including the closed-circuit current principle and earthing of the control circuit. Well-tried safety principles include overdimensioning of the contact ratings of B1, B2 and Q1. The frequency inverter is equipped with a precharging circuit for the intermediate circuit.
- Cross-circuits and short-circuits in electrical supply lines must be considered in accordance with ISO 13849-2, Table D.4.

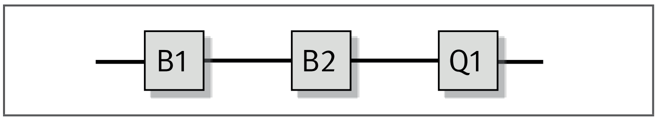


Figure A.2:
Safety-related block diagram for Example 1

- 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 ISO 13849-2, Table D.3 with direct opening contacts in accordance with IEC 60947-5-1, Annex K. The position switches and their actuators 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 IEC 60947-4-1.

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

Comments:

- Where hazardous zones can be accessed from behind the safety guard, 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 standstill monitor satisfying at least PL c can be employed as an alternative to B1.

- Should B1 not be used, the frequency inverter T1 is disconnected from the mains supply 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

- A B_{10D} value of 2,000,000 operation cycles [M] each is stated for B1 and B2 with direct opening electrical contact and separate actuator. At 365 working days, 16 working hours per day and a cycle time of 10 minutes, the result is an n_{op} of 35,040 cycles per year and $MTTF_D$ of 571 years.

- The B_{10} value for the contactor Q1 is 1,300,000 operation cycles [M] under inductive load (AC3). With 50% of failures assumed to be dangerous, the B_{10D} value is produced 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.

- The evaluation of SF 1 is as follows: the control system satisfies Category 1 with a high $MTTF_D$ (100 years). This yields an average probability of dangerous failure (PFH_D) of $1.1 \cdot 10^{-6}$ per hour. This satisfies PL c.

Example 2: Stopping in the event of departure from the safe park position whilst the safety guard is open – PL c

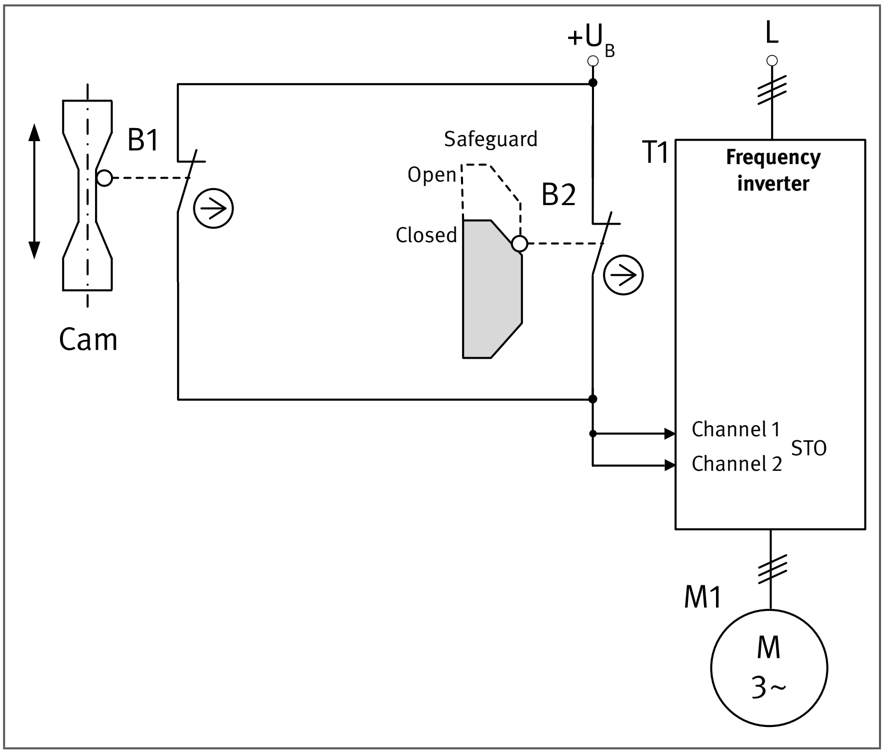


Figure A.3:
Combined position monitoring of a safety guard and position monitoring of an axis with the aid of a cam switch

Safety function

- SF 1: Should the axis depart from 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).

Functional description

- Before a manual intervention is performed, 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 start up unintentionally, B1 is actuated and the shunt of B2 removed. If the safety guard is open, an uncontrolled stop occurs by activation of STO in the frequency inverter T1 (stop category 0 to IEC 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

- Basic and well-tried safety principles and the requirements for Category B are observed. Protective circuits (such as contact protection), as described in the first sections of Chapter 8 of IFA Report 2/2017e, are present. This example employs basic safety principles including the closed-circuit current principle and earthing of the control circuit. The well-tried safety principles applied include overdimensioning of the contact ratings of B1 and B2.

- Cross-circuits and short-circuits in electrical supply lines must be considered in accordance with ISO 13849-2, Table D.4.

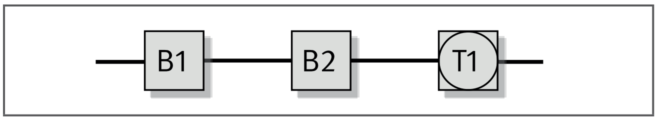


Figure A.4:
Safety-related block diagram for Example 2

- 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 ISO 13849-2, Table D.3 with direct opening contacts in accordance with IEC 60947-5-1, Annex K. The position switches and their actuators must be secured against displacement. Only rigid mechanical components (not spring elements) may be used.

- The frequency inverter T1 possesses the integrated STO safety sub-function.

Comments:

- Where hazardous zones can be accessed from behind the safety guard, 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 standstill monitor satisfying at least PL c can be employed as an alternative to B1.

- Should B1 not be used, the frequency inverter T1 is disconnected from the mains supply 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

- A B_{10D} value of 2,000,000 operation cycles [M] each is stated for B1 and B2 with direct opening electrical contact and separate actuator. At 365 working days, 16 working hours per day and a cycle time of 10 minutes, the result is an n_{op} of 35,040 cycles per year and an $MTTF_D$ of 571 years.

- DC_{avg} and measures against common cause failure are not relevant in Category 1.

- The manufacturer states Category 3, PL d, SIL 2 and a *PFH* of $3.2 \cdot 10^{-7}$ per hour for the frequency inverter T1.

- The evaluation of SF 1 is as follows: the combination of the subsystems yields an average probability of dangerous failure (PFH_D) of $1.1 \cdot 10^{-6}$ per hour + $3.2 \cdot 10^{-7}$ per hour = $1.5 \cdot 10^{-6}$ per hour. This satisfies PL c.

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

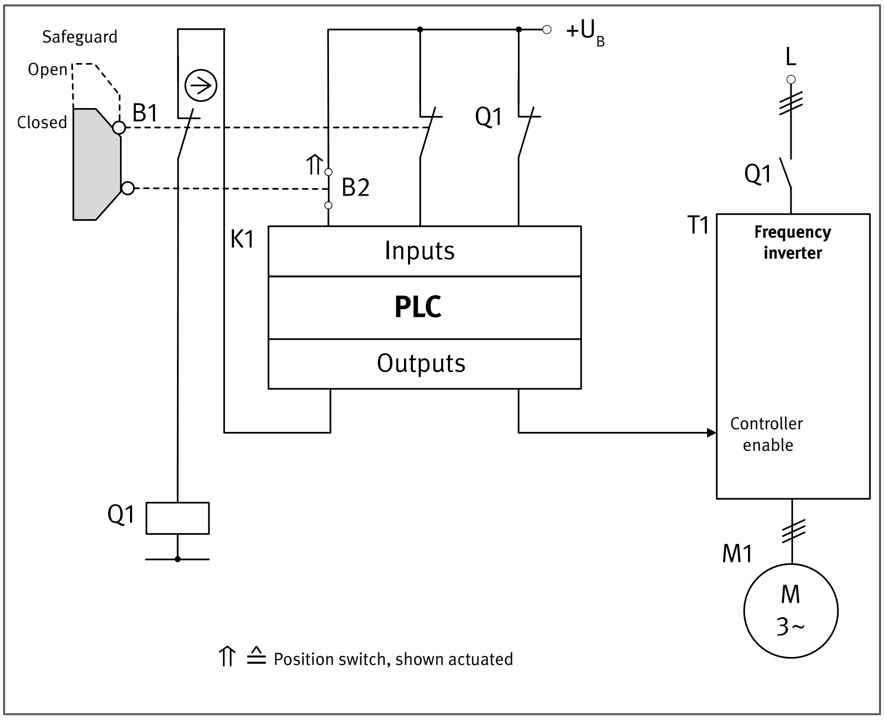


Figure A.5:
Conceptual schematic diagram of position monitoring

Safety function

- SF 1: Opening of the safeguard leads to STO of the drive.

Functional 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 shuts off the controller enable of the frequency inverter 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 controller enable of the frequency inverter T1.
- The controller 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, provided motor movements are enabled solely via the controller 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 4.2.3, “Fault detection”).
- Faults in the PLC are also detected by way of the technical process.

Design features

- Basic and well-tried safety principles and the requirements for Category B are observed. Protective circuits (such as contact protection, earthing of the control circuit), as described in the first sections of Chapter 8 of IFA Report 2/2017e, are present.
- Cross-circuits and short-circuits in electrical supply lines must be considered in accordance with 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.

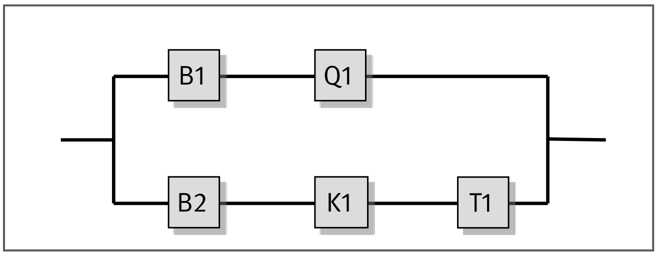


Figure A.6:
Safety-related block diagram for Example 3

- The actuating mechanisms of the electromechanical position switches B1 and B2 must be designed and fitted as specified. Actuators 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 ISO 13849-2, Table D.3 with direct opening contact in accordance with IEC 60947-5-1, Annex K.

- The mains contactor Q1 possesses a mirror contact in accordance with IEC 60947-4-1, Annex F. Reading back of this auxiliary contact on Q1 provides information on the switching position of the contactor‘s main contacts.

- The frequency inverter T1 is a standard product without integrated safety sub-functions and with precharging of the intermediate circuit.

- The standard components K1 (PLC) and T1 (frequency inverter) are used in accordance with the information in Subclause 4.6.2 (requirements concerning SRESW) of ISO 13849-1.

- The safety-related application software (SRASW) is programmed in accordance with the requirements for PL c (downgraded owing to diversity) and the information in Section 9.3.4 of IFA Report 2/2016.

Calculation of the probability of failure

- A B_{10D} value of 2,000,000 operation cycles [M] is stated for B1 with direct opening electrical contact and separate actuator. 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 2,604 years.

- A B_{10D} value of 1,000,000 operation cycles [M] is stated for the 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 400,000 operation cycles [M] is stated for the mains contactor Q1. At an n_{op} of 7,680 cycles per year, the $MTTF_D$ is 521 years.

- An $MTTF_D$ of 30 years [M] is stated both for the PLC K1 and for the frequency inverter T1.

- The *DC* of 99% for B1 and B2 is based upon the plausibility monitoring of the two switching states in the PLC K1.

- A *DC* of 99% can be stated for the mains contactor Q1, since the mirror contact is constantly monitored directly in the PLC K1.

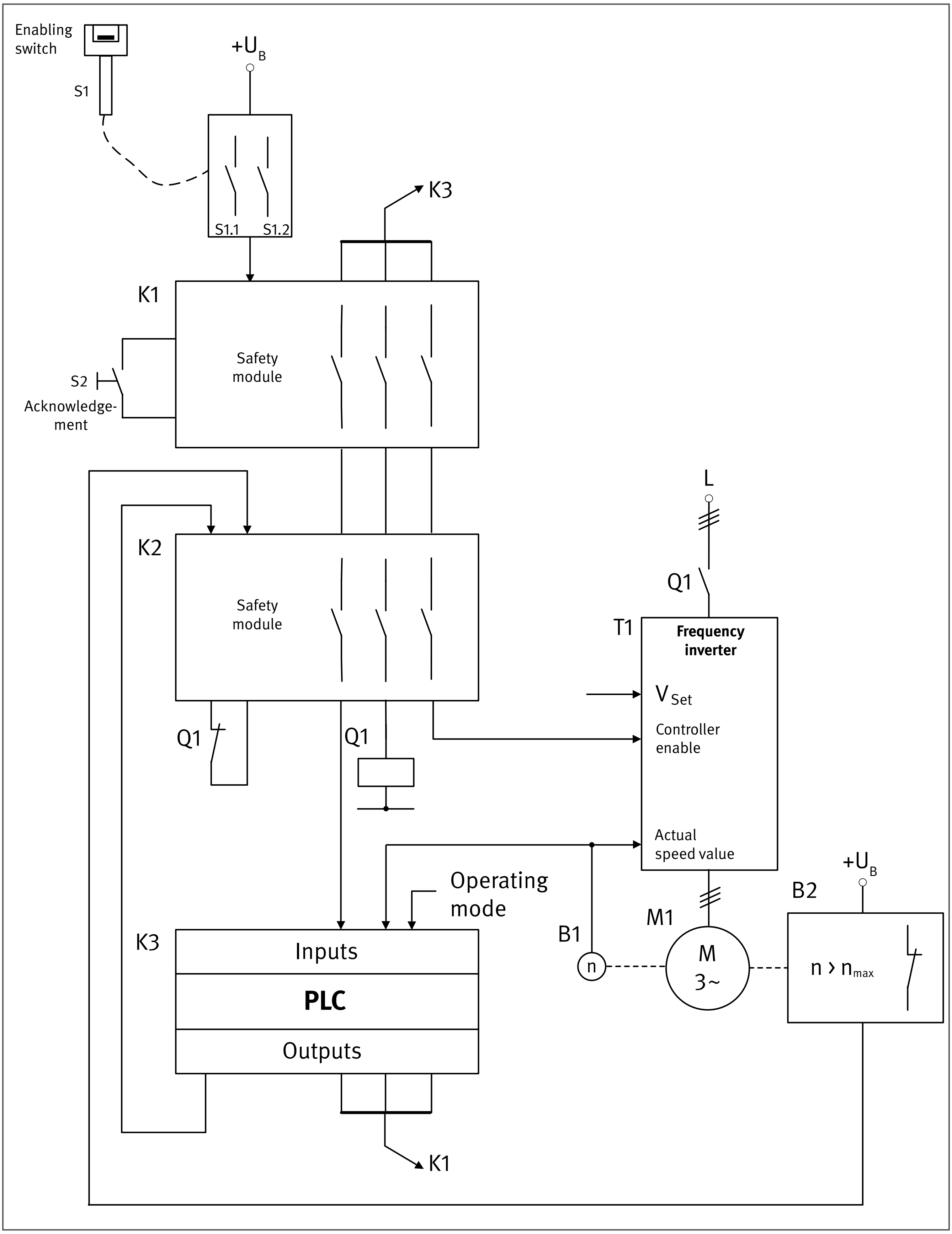
- A *DC* of 60% (fault detection by way of the technical process) each is stated for the PLC K1 and the controller enable in the frequency inverter T1.

- Adequate measures against common cause failure are taken (80 points): separation (15), diverse technologies (20), use of well-tried components (5), overvoltage protection etc. (15) and protection against environmental conditions (25).

- The evaluation of SF 1 is as follows: the combination of the subsystems yields an average probability of dangerous failure PFH_D of $1.8 \cdot 10^{-7}$ per hour. This satisfies PL d.

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

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



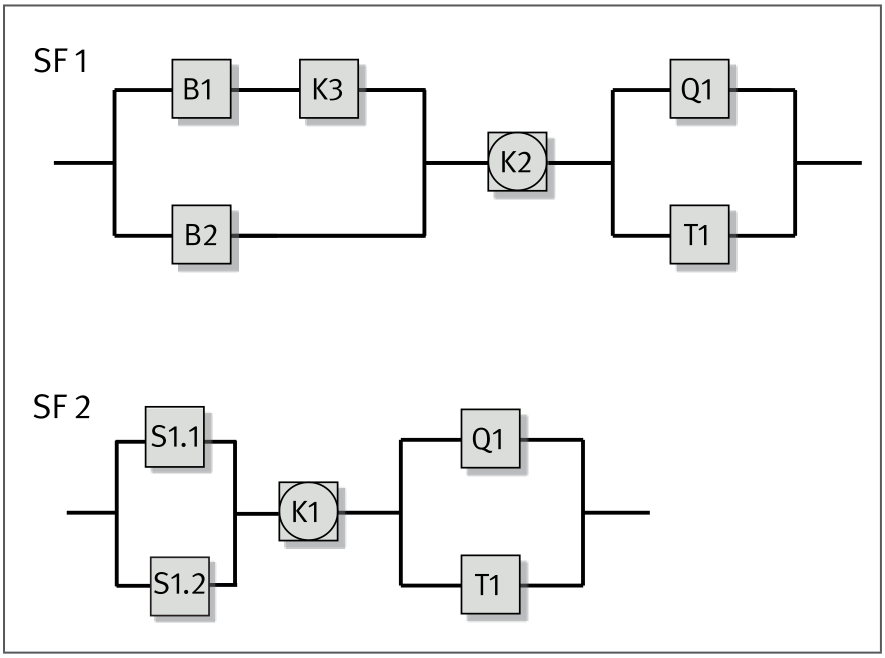


Figure A.8:
Safety-related block diagrams for Example 4

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.

Functional description

- This part of the control system implements the "safely-limited speed" (SLS) safety sub-function in the "setup" operating mode. Overspeed leads to uncontrolled stopping by means of STO.
- In this operating mode, drive movements are enabled by actuation of the enabling switch S1. They are prevented when S1 is not actuated. The signals from the enabling switch S1 act upon the safety module K1.
- For the sake of clarity, selection of the operating mode is not shown.
- Speed monitoring employs a two-channel arrangement. In one channel, the signal is processed by means of the rotary encoder B1 and the PLC K3. The second channel is implemented by means of the speed monitoring device B2. The outputs of the two channels act upon the safety module K2.
- The safety modules K1 and K2 are cascaded. Breaking of the enabling paths of either of the two safety modules leads to the drive being shut off by STO.
- The STO arrangement is two-channel in form, involving blocking of the controller enable of the frequency inverter T1 and interruption of the mains supply by means of the mains contactor Q1.
- Cascading of the safety modules enables further safeguards and control devices to be integrated in order to trigger the STO safety sub-function.

Design features

- Basic and well-tried safety principles and the requirements for Category B are observed. Protective circuits (such as contact protection, earthing, precharging of the frequency inverter's intermediate circuit), as described in the initial sections of Chapter 8 of IFA Report 2/2017e, are present.

- Cross-circuits and short-circuits in electrical supply lines must be considered in accordance with 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 IEC 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 inverter T1 and the PLC K3 are standard items of equipment without integrated safety sub-functions. They are used in accordance with the information in Subclause 4.6.2 (requirements concerning SRESW) of ISO 13849-1.
- The speed detection arrangement employs diversity. B1 is a sin/cos encoder connected to the PLC K3. B2 is a tachometric relay with integrated 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 safety-related application software (SRASW) is programmed in accordance with the requirements for PL c (downgraded owing to diversity) and the information in Section 9.3.4 of IFA Report 2/2016.
- The stopping time (run-down time) with STO following exceeding of the speed limit value at maximum possible acceleration must not give rise to any hazard.
- The enabling switch S1 is of two-stage design. It possesses two make contacts per stage. The design of the enabling switch employs two signal channels. The enabling switch S1 satisfies the requirements of IEC 60204-1, Section 10.9.

Note:

The enabling switch S1 and the safely-limited speed in conjunction with the operating mode selector switch etc. are criteria for the 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 $2.3 \cdot 10^{-9}$ per hour [M].
- An $MTTF_D$ of 132 years [M] is stated for the rotary encoder B1.
- The manufacturer states an $MTTF_D$ of 60 years [M] for the tachometric relay B2.
- The contactor Q1 has a B_{10D} value of 1,000,000 operation 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 inverter T1 does not possess integrated safety sub-functions. Since no information on the $MTTF_D$ is available from the manufacturer, it is estimated conservatively at ten years for the purpose of calculation [S] (see ISO 13849-1, Subclause 4.5.2).
- The two-stage enabling switch S1 satisfies GS-ET-22 and its number of actuating cycles is below 100,000. In accordance with IFA Report 2/2017e, Table D.7, the B_{10D} for release of the switch is 100,000 for each channel. At 200 actuations per year, the resulting $MTTF_D$ is 5,000 years.
- A *DC* of 99% is assumed for the make contacts S1.1/S1.2 of the enabling switch S1, since the safety module K1 performs a plausibility check.

- A *DC* of 60% is assumed for the rotary encoder B1, 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 speed monitoring device B2 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 inverter T1 is estimated at 60%, since functional stopping of the motor occurs solely by cancellation of the controller enable and a fault is detected by way of the technical process.

- Adequate measures against common cause failures are taken for the B1/B2/K3 subsystem (80 points): separation (15), diverse 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), diverse technologies (20), protection against overvoltage etc. (15), failure mode and effects analysis (5) and protection against environmental influences (25+10).

- The evaluation for the SF 1 safety function, “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 (B1, B2, K3) and shut-off paths (Q1, T1) satisfy Category 3 and PL d. In combination with the encapsulated subsystem of the safety module K2, the result for SF 1 is an average probability of dangerous failure PFH_D of $5.5 \cdot 10^{-7}$ per hour. This satisfies PL d.

- The evaluation for the SF 2 safety function, “STO is triggered when the enabling switch S1 is released”, yields the following result: the combination of the subsystems of the enabling switch (S1), safety module (K1) and shut-off paths (Q1, T1) yields an average probability of dangerous failure PFH_D of $2.1 \cdot 10^{-7}$ 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/docsroom/documents/25221

Example 5: Stopping in an emergency – PL d

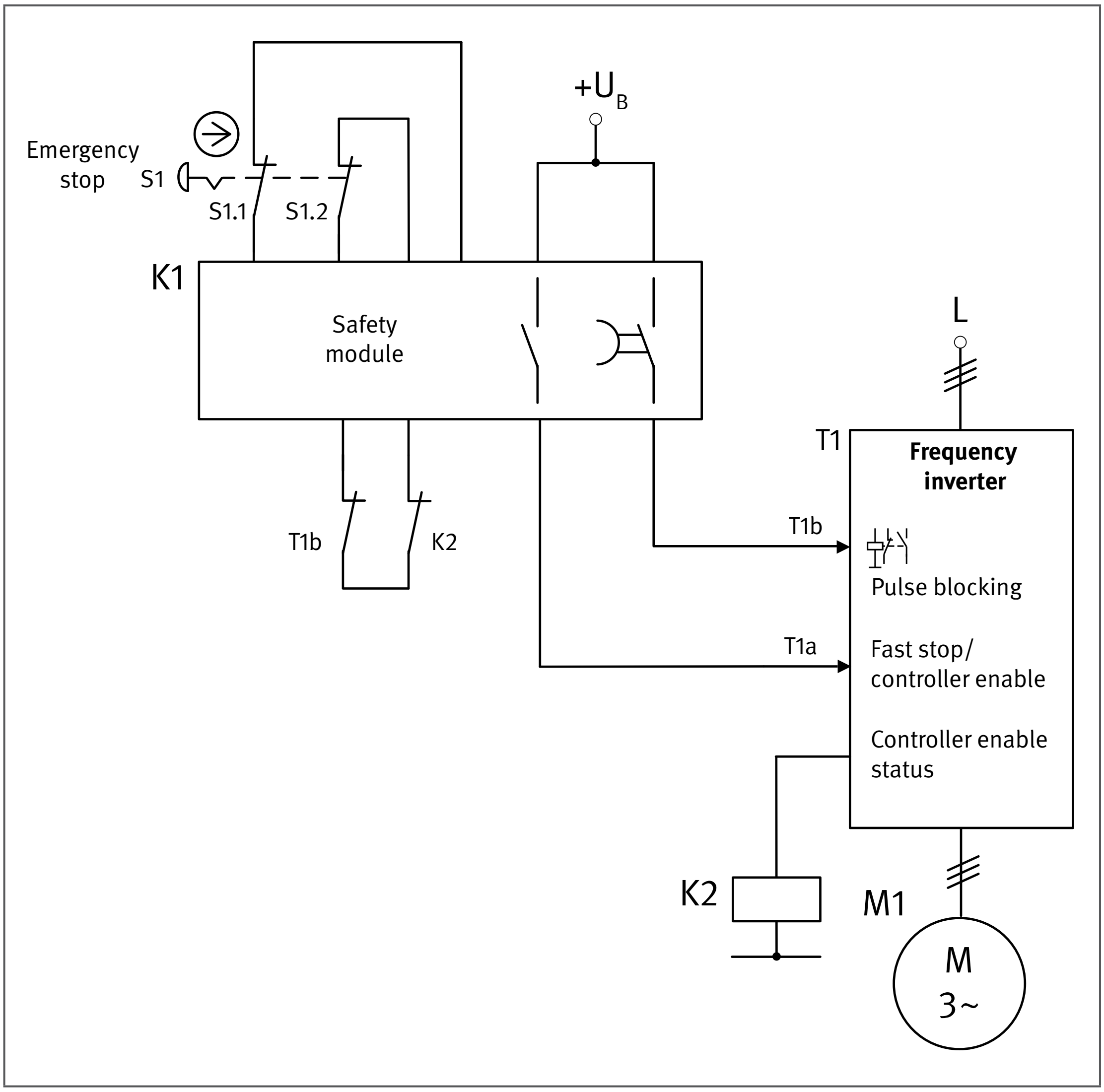


Figure A.9: Conceptual schematic diagram of the power drive control

Safety function

- SF 1: Fastest possible stopping in the event of an emergency-stop (SS1-t)

Functional description

- Hazardous movements are stopped as fast as possible by actuation of the emergency-stop device S1. The redundant contacts S1.1/S1.2 are evaluated in the safety module K1.

- The instantaneous switching contact of the safety module K1 activates the rapid-stop function in the frequency inverter T1 with subsequent cancellation of the controller enable, causing the drive to be brought to a halt as quickly as possible. Following a time suitably configured for this application, pulse blocking by the frequency inverter T1 is activated via the delayed switching contact of K1, and the drive torque is de-activated. The delay in K1 is selected such that the frequency inverter T1 has just enough time to shut the drive down in a controlled manner.

- The emergency-stop device S1 employs redundant contacts; these are monitored together with the wiring by the safety module K1. The two shut-off paths in the frequency inverter T1 possess feedback signals that are integrated into the enabling circuit of K1 (one directly, the other via a coupling device K2). Faults in the frequency inverter T1 thus become apparent before the drive is next started.

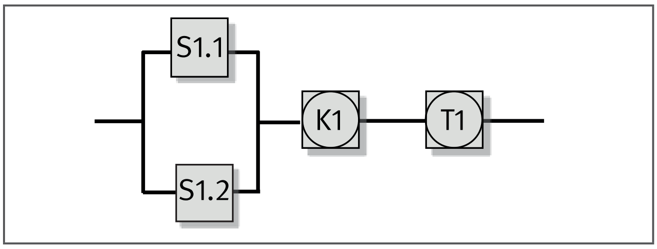


Figure A.10:
Safety-related block diagram for Example 5

Design features

- Basic and well-tried safety principles and the requirements for Category B are observed. Protective circuits (such as contact protection, earthing, precharging of the frequency inverter‘s intermediate circuit), as described in the initial sections of Chapter 8 of IFA Report 2/2017e, are present.

- Cross-circuits and short-circuits in electrical supply lines must be considered in accordance with 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 device S1 satisfies the requirements of ISO 13850 and is equipped with direct opening contacts S1.1/S1.2 in accordance with IEC 60947-5-1, Annex K.

- The safety module K1 possesses instantaneous and delayed enabling paths and satisfies the requirements for Category 3 and PL d.

- T1 is a frequency inverter with integrated STO safety sub-function. The safety sub-function is achieved by a two-channel arrangement through the fast stop/controller enable (T1a) and pulse blocking (T1b) inputs. The SS1 safety sub-function is implemented by combination with a suitable safety module. In this example, the fast-stop function is activated by cancellation of the controller enable.

- Both shut-off paths of the frequency inverter T1 are monitored by the safety module K1. In order to detect faults, the relay of the pulse block T1b possesses a mechanically linked break contact, and the status of the controller enable T1a is detected by means of the coupling element K2.

- Note that the fast-stop function of the frequency inverter T1 is purely functional in its design, i.e. it is not engineered as a safety component. Should a fault in T1 arise simultaneously with actuation of the emergency-stop device, stopping as fast as possible may not take place at all, or deceleration 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 the time delay in K1 expires and pulse blocking is activated, 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 fault behaviour described here 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 deceleration ramp and the additional use of mechanical brakes.

Calculation of the probability of failure

- A B_{10D} of 100,000 operation cycles [S] each may be assumed for the emergency-stop device S1 and for the contacts S1.1 and S1.2 in accordance with ISO 13849-2, Table D.8, and IFA Report 2/2017e, Table D.6. At an n_{op} of 120 operation cycles per year, the resulting PFH_D for the configuration is $2.5 \cdot 10^{-8}$ per hour. Owing to the plausibility check of the safety module K1, a *DC* of 99% is assumed.

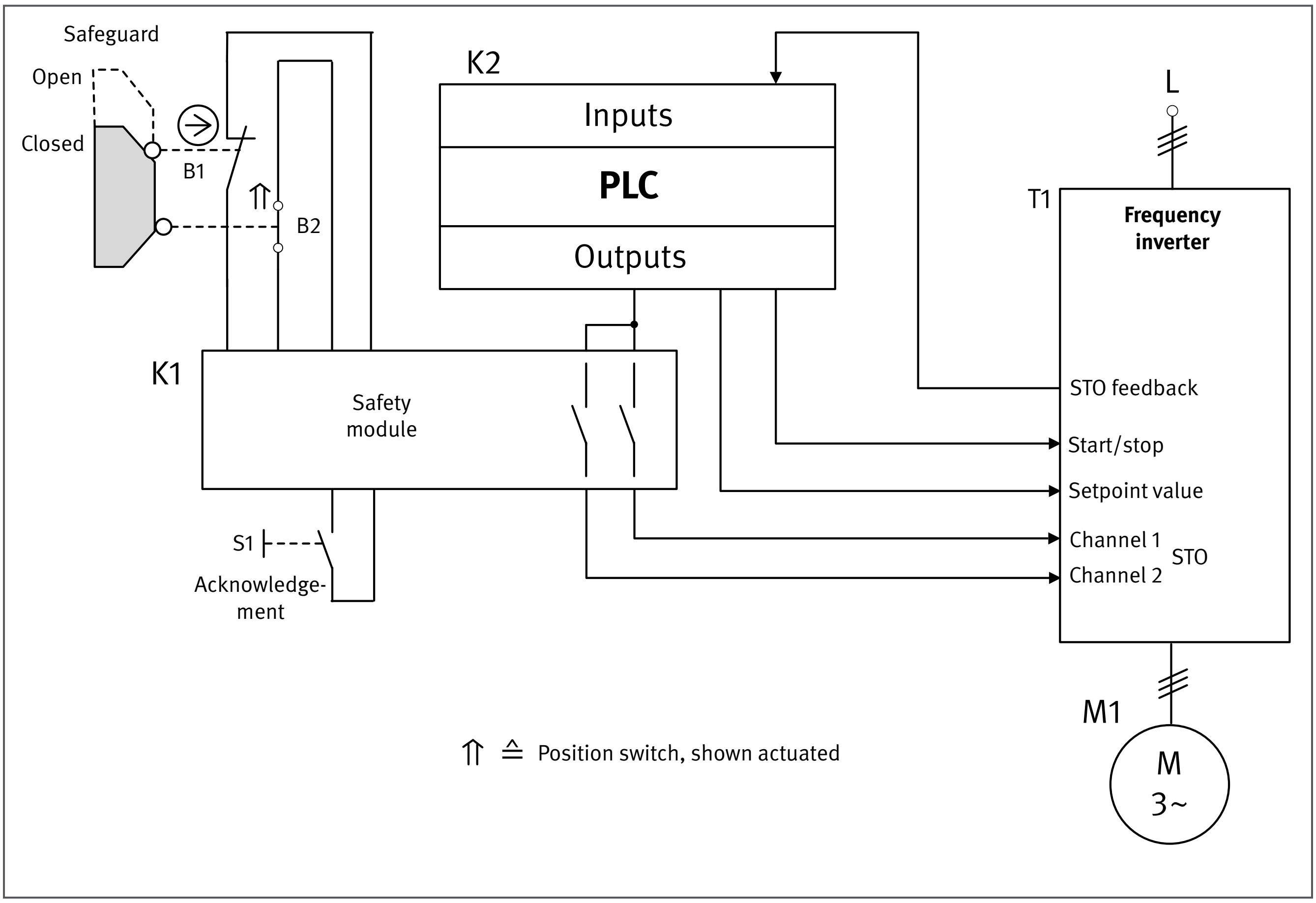
- The safety module K1 satisfies the requirements for Category 3, PL d and SIL 2. The PFH_D is $3.2 \cdot 10^{-7}$ per hour [M].

- T1 is a frequency inverter with integrated STO safety sub-function. It satisfies the requirements for Category 3, PL d and SIL 2. The PFH_D is $3.2 \cdot 10^{-7}$ per hour [M]. These data for T1 are valid only when the manufacturer‘s criteria for fault detection by external components are satisfied and implemented in accordance with the instruction manual.

- For the SF 1 safety function, “fastest possible stopping in an emergency stop (SS1-t)”, the evaluation yields the following result: the combination of the S1.1/S1.2, K1 and T1 subsystems yields an average probability of dangerous failure PFH_D of $6.6 \cdot 10^{-7}$ per hour. This satisfies PL d.

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

Figure A.11:
STO of a frequency inverter



Safety function

- SF 1: Opening of the movable safeguard leads to STO of the frequency inverter drive.

Functional description

- The inverter-actuated power drive is controlled functionally by the PLC K2. It specifies the setpoint value for the frequency inverter T1, switches the two STO inputs, and is able to start and stop the drive. The PLC K2 is however not involved in the safety function.

- The hazardous zone is safeguarded by a movable guard. Opening of the guard is detected by the position switches B1 and B2 and interpreted in a safety module K1. The STO inputs are switched off in the frequency inverter T1 via the enabling paths of K1, independently of the PLC K2. Generation of a rotary field in the drive is thereby reliably prevented.

- Faults in the position switches B1 and B2 are detected by the plausibility check in the safety module K1. The frequency inverter T1 is equipped with an internal STO monitoring function. This prevents the drive from restarting in the event of a fault. A corresponding fault signal is issued to the PLC K2.

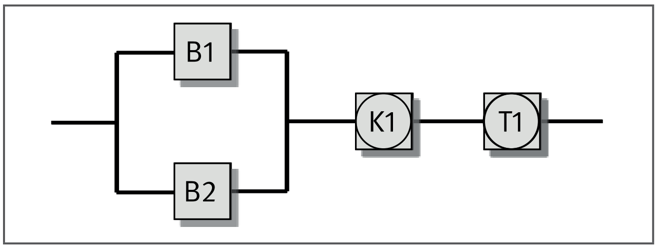


Figure A.12:
Safety-related block diagram for Example 6

Design features

- Basic and well-tried safety principles and the requirements for Category B are observed. Protective circuits (such as contact protection, earthing of the control circuit), as described in the first sections of Chapter 8 of IFA Report 2/2017e, are present.

- Cross-circuits and short-circuits in electrical supply lines must be considered in accordance with 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. Actuators 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 ISO 13849-2, Table D.3 with direct opening contact in accordance with IEC 60947-5-1, Annex K.

- The safety module satisfies the requirements for Category 4 and PL e.

- T1 is a frequency inverter with integrated STO safety sub-function. The requirements for Category 3 and PL d are met.

Calculation of the probability of failure

- A B_{10D} value of 20,000,000 operation cycles [S] is stated for the position switch B1 with direct opening contact. 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 52,083 years. A B_{10D} value of 1,000,000 operation cycles [M] is stated for the 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 safety module K1 satisfies the requirements for Category 4, PL e and SIL 3. The PFH_D is $2.3 \cdot 10^{-9}$ per hour [M].

- The frequency inverter T1 with integrated STO safety sub-function satisfies the requirements for Category 3, PL d and SIL 2. The PFH_D 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.

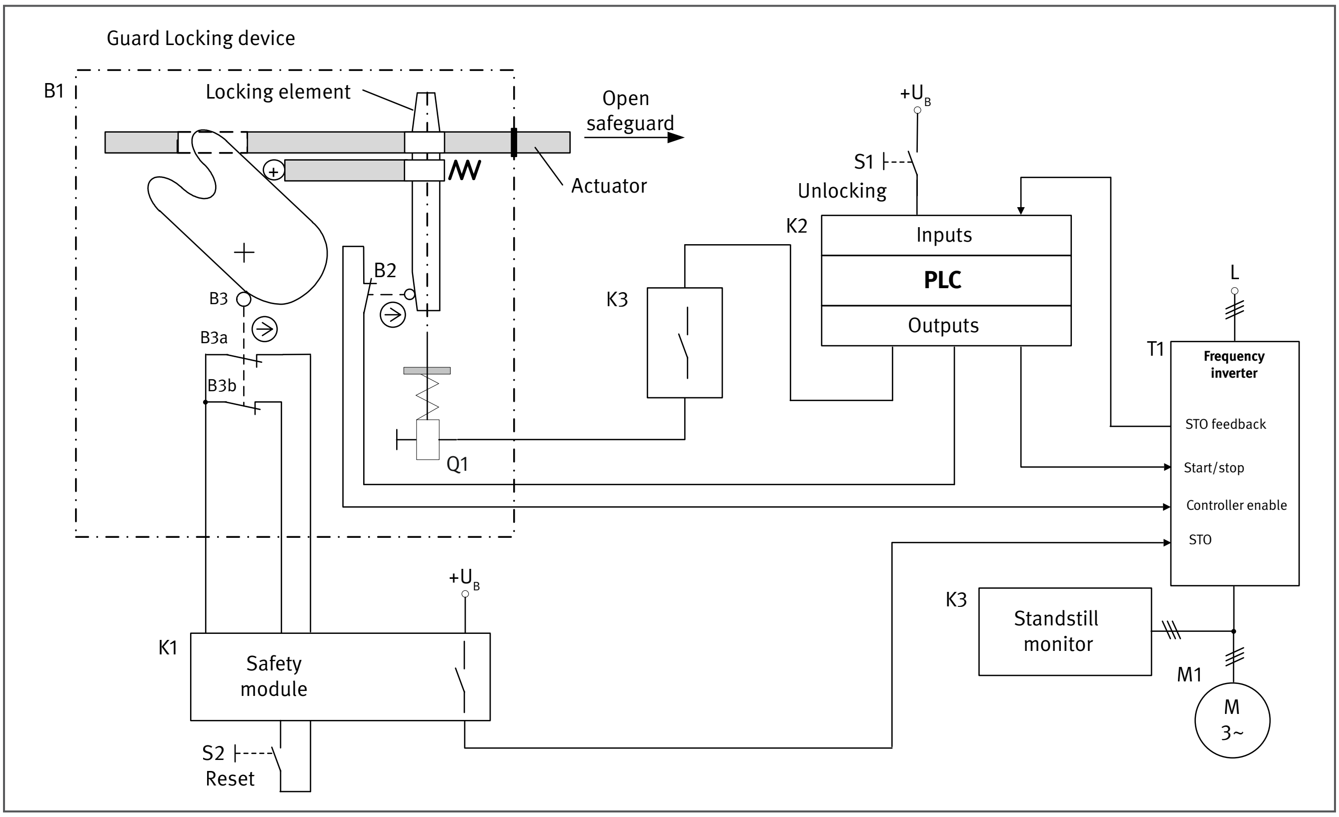
- Adequate measures against common cause failure are taken for the subsystem of the position switches B1/B2 (70 points): separation (15), use of well-tried components (5), protection against overvoltage etc. (15) and protection against environmental conditions (25 + 10).

- The subsystem B1/B2 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 $2.5 \cdot 10^{-8}$ per hour.

- The evaluation of the safety function is as follows: the combination of the subsystems of position switches B1/B2, safety module K1 and frequency inverter T1 yields an average probability of dangerous failure PFH_D of $2.3 \cdot 10^{-7}$ per hour. This satisfies PL d.

Example 7: Safeguarding of a hazardous zone by a movable safeguard with guard locking device – PL d

Figure A.13:
Safeguarding of a hazardous zone by a movable guard with guard locking device



Safety functions

- SF 1: Releasing of guard locking device only when the drive is stationary
- SF 2: STO of the drive when the movable safeguard with guard locking device is opened

Functional description

- Access to a hazardous movement is prevented by means of a safety guard with guard locking device B1 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 from being withdrawn from the switch head.
- Access to the hazardous zone is requested by actuation of the pushbutton S1. This causes the standard PLC K2 first to initiate stopping of the drive by the frequency inverter T1. Once standstill has been reached, the standstill monitor K3 enables the guard locking solenoids to be actuated by the PLC K2, and guard locking thus to be released.
- The position of the locking mechanism is monitored. The pin of the solenoid acts upon the position switch B2, which interrupts the controller enable of the frequency inverter T1 when actuated.
- Opening of the guard is detected by the two break contacts B3a/B3b of the position switch B3 and interpreted in a safety module K1. The STO input on the frequency inverter 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.
- The hazardous movement can be restarted only when the guard is closed and guard locking activated.

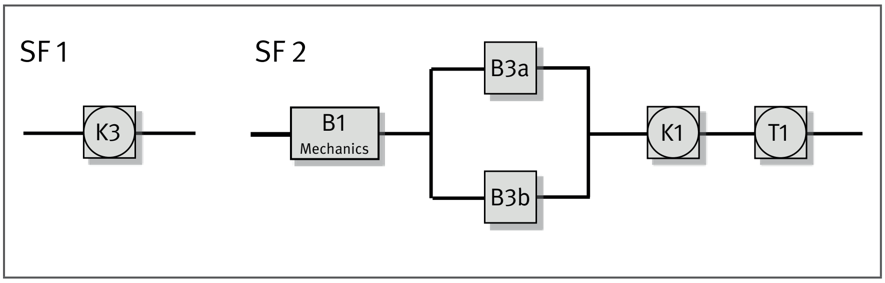


Figure A.14:
Safety-related block diagrams for Example 7

- Faults in the position switch B3 are detected by the plausibility check in the safety module K1.

- The integrated STO safety sub-function in the frequency inverter 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

- Basic and well-tried safety principles and the requirements for Category B are observed. Protective circuits (such as contact protection, earthing of the control circuit), as described in the first sections of Chapter 8 of IFA Report 2/2017e, are present.

- Cross-circuits and short-circuits in electrical supply lines must be considered in accordance with 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.

- B1 is a guard locking device with guard position monitoring. The break contacts B3a and B3b and the monitoring contact B2 for the locking mechanism are direct opening contacts that satisfy the requirements of IEC 60947-5-1, Annex K. The locking mechanism is held in the locked position by spring force (closed-circuit current principle).

- The guard locking device B1 satisfies the requirements of ISO 14119 for interlocked guards and of the GS-ET-19 test principles.

- The safety module K1 satisfies the requirements for Category 4 and PL e.

- T1 is a frequency inverter with integrated STO safety sub-function. The requirements for Category 3 and PL d are met. Single-channel activation for STO is sufficient for this product.

- The standstill monitor K3 satisfies the requirements for 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 can be assumed for the mechanical components of the guard locking device, including mechanical failure of the locking mechanism, provided 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 self-loosening
  – 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 unlock solenoid until the guard door is closed; refer in this context also to DGUV Informative publication 203-079 concerning the selection and fitting of interlocking devices
  – 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
  – Dropping of the door does not lead to the actuator being used outside the range specified by the manufacturer
  – Damage that could be caused by foreseeable external influences (such as the ingress of dirt and dust, mechanical shock) is prevented by the form of mounting or need not be anticipated owing to the conditions of use.

  The fault exclusion must be confirmed by the manufacturer.

- A B_{10D} value of 2,000,000 operation cycles [S] can be assumed for the direct opening electrical contacts B3a and B3b. 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 5,208 years.

- The safety module K1 satisfies the requirements for Category 4, PL e and SIL 3. The *PFH* is $3.0 \cdot 10^{-8}$ per hour [M].

- T1 is a frequency inverter with integrated STO safety sub-function. It satisfies the requirements for Category 3, PL d and SIL 2. The PFH_D is $2.0 \cdot 10^{-7}$ per hour [M].

- The standstill monitor K3 satisfies the requirements for Category 3, PL d and SIL 2. The PFH_D is $2.3 \cdot 10^{-7}$ per hour [M].

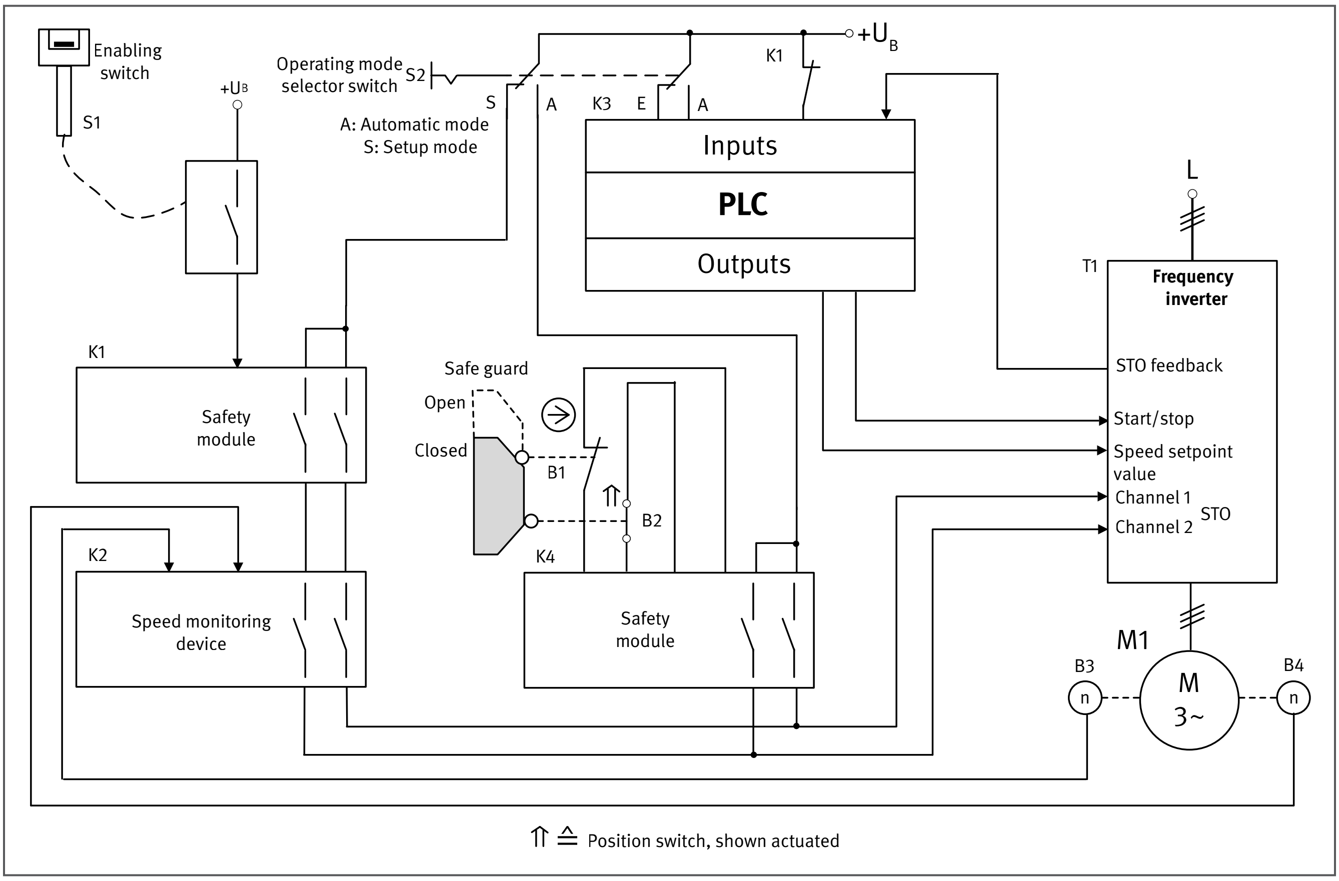
- Owing to the plausibility check by the safety module K1, a *DC* of 99% can be assumed for the electrical contacts of B3.

- Evaluation of the SF 1 safety function, “release of guard locking device only when the drive is stationary”, yields the following result: for the speed detection subsystem (K3), the average probability of dangerous failure PFH_D is $2.3 \cdot 10^{-7}$ per hour. This satisfies PL d.

- Evaluation of the SF 2 safety function, “STO of the drive following opening of the movable guard with guard locking device”, yields the following result: the combination of the subsystems of mechanical components B1, position switches B3a/B3b, safety module K1 and frequency inverter T1 yields an average probability of dangerous failure PFH_D of $2.5 \cdot 10^{-7}$ per hour. This satisfies PL d.

Example 8: Power drive control for automatic and setup mode with limited speed PL d and enabling switch PL c

Figure A.15:
Safeguarding of a hazardous zone by a movable guard with guard locking device



⥣ ≙ Position switch, shown actuated

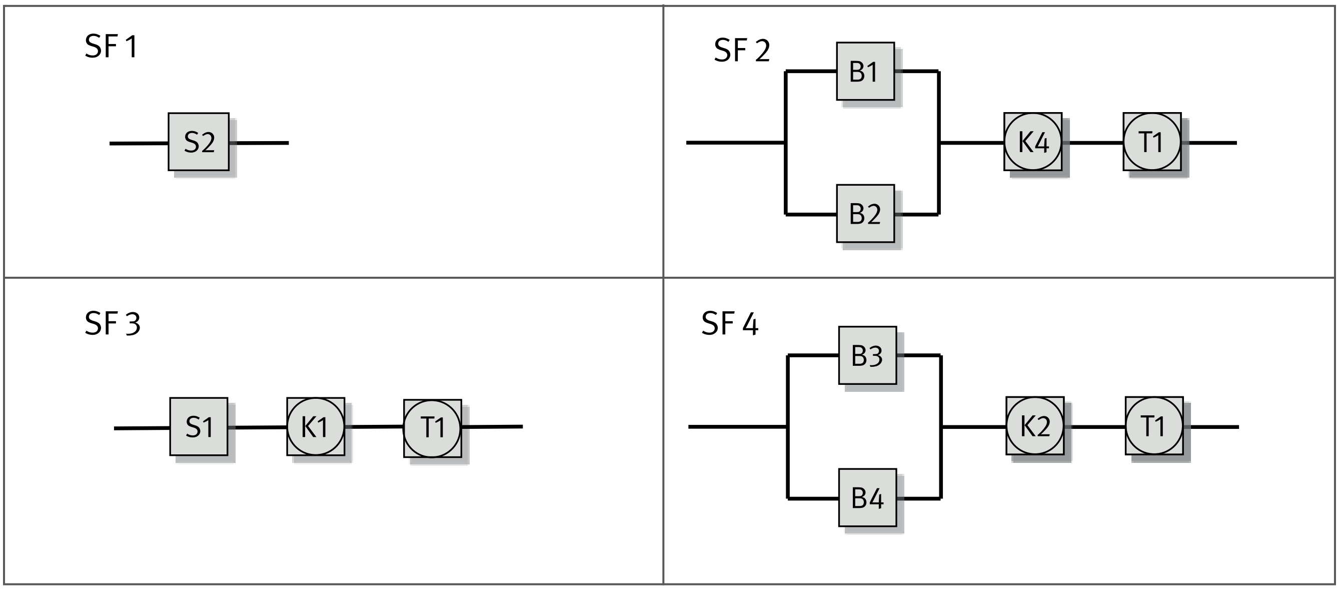
Safety functions

- SF 1: Operating mode selection
- SF 2: Automatic mode; opening of the movable safeguard 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)

Functional description

- The operating mode selector switch S2 permits selection between automatic and setup modes. In automatic mode, the contacts of the position switches B1/B2 on the guard are closed, and the drive can be operated at any speed. Opening of the guard is detected via B1/B2 and the safety module K4, and leads to activation of the STO safety sub-function in the frequency inverter 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 S1. The movement is initiated by a separate control device on a hand-held terminal (not shown).
- When the enabling switch S1 is released, the hazardous movement is brought to a halt via the safety module K1 by de-energization of the STO inputs of the frequency inverter T1.

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



- The speed is monitored in setup mode by a monitoring device K2 (Category 3, PL d). Two encoders, or alternatively one encoder and the speed signal from the frequency inverter, are used to register the speed. When the maximum speed set in the monitoring device is exceeded, the output relays drop out and the STO function of the frequency inverter is activated.

- Faults in the position switches B1 and B2 are detected by plausibility check in the safety module K4. The frequency inverter T1 is equipped with an internal STO monitoring function. This prevents the drive from restarting in the event of a fault. A corresponding fault signal is issued to the PLC K3.

- Speed monitoring employs a two-channel arrangement. Faults in the encoder signals are detected by the plausibility check in the speed monitoring device K2.

Design features

- Basic and well-tried safety principles and the requirements for Category B are observed. Protective circuits (such as contact protection, circuit earthing, precharging of the frequency inverter‘s intermediate circuit), as described in the initial sections of Chapter 8 of IFA Report 2/2017e, are present.

- Cross-circuits and short-circuits in electrical supply lines must be considered in accordance with 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 S2 is a cam-operated selector switch with positive mode of actuation. The design of the operating mode selector switch permits fault exclusions in accordance with ISO 13849-2, Table D.8.

- The actuating mechanisms of the electromechanical position switches B1 and B2 must be designed and fitted as specified. Actuators 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 ISO 13849-2 with direct opening contact in accordance with IEC 60947-5-1, Annex K.

- The two-stage enabling switch S1 is a single-channel device with make contact. The enabling switch S1 satisfies the requirements of IEC 60204-1, Subclause 10.9.

- The safety modules K1 and K4 satisfy the requirements for Category 4 and PL e.

- The speed monitoring device K2 satisfies the requirements for Category 3 and PL d.
- T1 is a frequency inverter with integrated STO safety sub-function. The requirements for Category 3 and PL d are met.
- K3 is a standard commercial programmable logic controller that is not involved in the safety functions.

Comments:

- The stopping time (run-down time) of the STO safety sub-function triggered by exceeding 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 S1, 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 B3, B4 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 S2 is a cam-operated selector switch with positive mode of actuation (direct opening action) in accordance with IEC 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, a fault is excluded for the two changeover contact levels having different positions. Owing to the control architecture employed and installation in a switching cabinet with a minimum ingress protection of IP 54, faults such as short-circuits between adjacent tracks, contact points and conductors can be excluded. The conditions for fault exclusion to ISO 13849-2, Subclause D.5 are met. Faults in the operating mode selection arrangement cannot lead to hazardous 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.
- A B_{10D} value of 20,000,000 operation cycles [S] is assumed for the position switch B1 with direct opening contacts. 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 52,083 years.
- A B_{10D} of 1,000,000 operation cycles [M] is stated for the position switch B2 with make contact. 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 safety modules K1 and K4 satisfy the requirements for Category 4, PL e and SIL 3. The PFH_D is $2.3 \cdot 10^{-9}$ per hour [M].
- The frequency inverter T1 with integrated STO safety sub-function satisfies the requirements for Category 3, PL d and SIL 2. The PFH_D is $2.0 \cdot 10^{-7}$ per hour [M].
- The two-stage enabling switch S1 features a make contact. The manufacturer states a B_{10D} value of 100,000 operation cycles [M]. At an n_{op} of 480 cycles per year, the $MTTF_D$ is 2,083 years.
- The speed monitoring device K2 is a safety module that satisfies the requirements for Category 3, PL d and SIL 2. The PFH_D is $2 \cdot 10^{-7}$ per hour [M].
- The rotary encoders B3 and B4 are flanged to the right and left-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 criteria for such a fault exclusion are set out in the GS-IFA-M21 test principles, Table A.1.

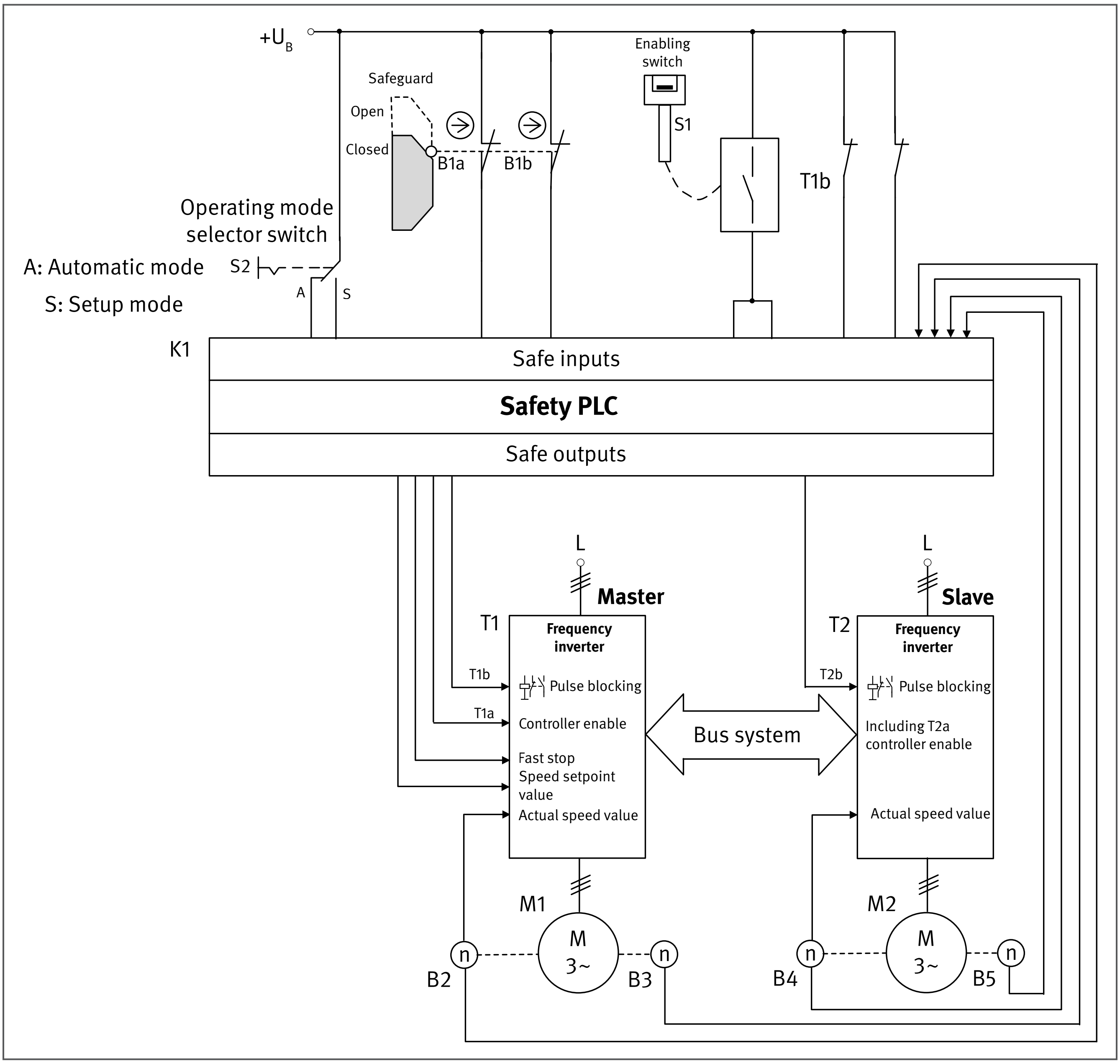
- The *DC* for the position switches B1 and B2 is 99%, owing to the plausibility check by the safety module K4.
- The *DC* for the rotary encoders B3 and B4 is estimated at 99%, owing to the cross monitoring of the signals by the speed monitoring device K3.
- Adequate measures against common cause failure 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).
- Adequate measures against common cause failure are taken for the subsystem of the rotary encoders B3/B4 (65 points): separation (15), protection against overvoltage etc. (15) and protection against environmental conditions (25 + 10).
- Evaluation of the SF 1 safety function, “operating mode selection”, yields the following result: the formulation of the fault exclusions based upon the design characteristics enables the separation of automatic, setup and function control modes to be assigned to PL d. The restriction to PL d is due to the fact that PL e must not be based solely upon fault exclusion (see ISO 13849-2, Table D.8).
- Evaluation of the SF 2 safety function, “automatic mode; opening of the movable guard brings the drive to a halt (STO)”, yields the following result: the subsystem B1/B2 satisfies Category 3 with a high $MTTF_D$ (100 years) and a high DC_{avg} (99%). This yields an average probability of dangerous failure PFH_D of $2.5 \cdot 10^{-8}$ per hour.

  The combination of the subsystems of position switches B1/B2, safety module K1 and frequency inverter T1 yields an average probability of dangerous failure PFH_D of $2.3 \cdot 10^{-7}$ per hour. This satisfies PL d.
- Evaluation of the SF 3 safety function, “setup mode; release of the enabling switch S1 on the hand-held terminal brings the drive to a halt (STO)”, yields the following result: the combination of the subsystems of enabling switch S1, safety module K1 and frequency inverter T1 yields an average probability of dangerous failure PFH_D of $1.3 \cdot 10^{-6}$ per hour. This satisfies PL c.
- Evaluation of the SF 4 safety function, “setup mode; exceeding of the maximum permissible speed leads to the drive being brought to a halt (SLS)”, yields the following result: the subsystem B3/B4 satisfies Category 3 with a high $MTTF_D$ (40 years) and a high DC_{avg} (99%). This yields an average probability of dangerous failure PFH_D of $6.9 \cdot 10^{-8}$ per hour.

  The combination of the respective subsystems of the rotary encoders B3/B4, speed monitoring device K2 and frequency inverter T1 yields an average probability of dangerous failure PFH_D of $4.7 \cdot 10^{-7}$ per hour. This satisfies PL d.

Example 9: Power drive control for automatic and setup mode with limited speed PL d and enabling switch PL c

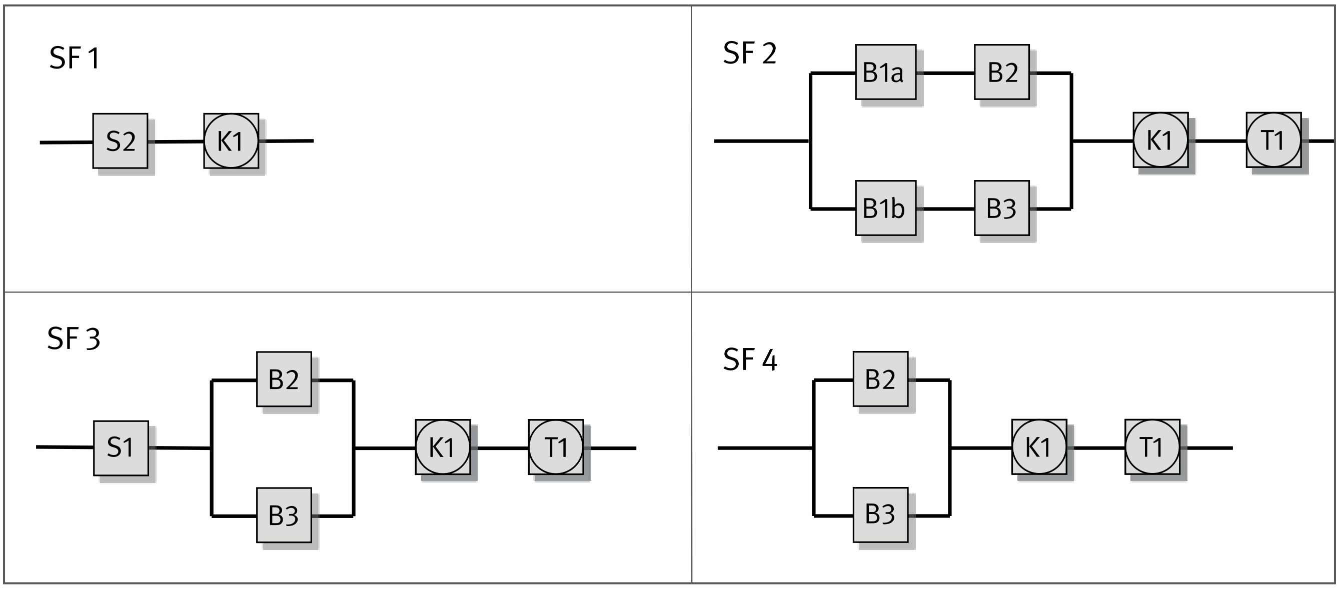
Figure A.17:
Conceptual schematic diagram of the power drive control



Safety functions

- SF 1: Operating mode selection
- SF 2: Automatic mode; SS1 following opening of a safeguard
- SF 3: Setup mode; releasing or fully depressing the three-stage enabling switch S1 brings the drive to a halt (SS1)
- SF 4: Setup mode; safely-limited speed – exceeding of the maximum permissible speed leads to stopping of the drive (STO)

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



Note:
Hazards presented by individual machine components are considered during determining of the Performance Level for SF 2 and the following safety functions. Only one drive is involved in the movement of a part of a machine. This means in this case that each drive that gives rise to a hazardous movement is considered separately. The calculation of the respective PL need not therefore consider both frequency inverters, nor all rotary encoders. This example considers the safety functions in which the frequency inverter T1 is involved. During the analysis for T2, signal processing for the controller enable via T1 must also be considered. Further information concerning the analysis of individual machine components can be found in Section 2.2 of this report ("overlapping hazards").

Functional description

- The power drive control implements synchronized movements at safely-limited speed in setup mode. The frequency inverters T1/T2 are operated as master and slave. The first frequency inverter T1 (master) receives a setpoint value and drives the downstream frequency inverter T2 (slave) over a data bus.

- The operating mode selector switch S2 permits selection between automatic and setup modes (SF 1). In automatic mode, the contacts of the position switch B1 on the safeguard are closed, and the drive can be operated at any speed. Opening of the safeguard in automatic mode (triggering of SF 2) is detected by the safety PLC K1, which responds by initiating a fast stop of the drive via the relevant input of the master frequency inverter. The slave frequency inverter T2 receives this command over the bus and follows the master. The safety PLC K1 monitors the deceleration ramp, deactivates the controller enable of the frequency inverters T1a/T2a once the drive has reached a standstill, and deactivates pulse blocking of T1b/T2b. The SS1 safety sub-function (corresponding to stop category 1 to IEC 60204-1) is implemented by supplementing the frequency inverters with the STO safety sub-function with ramp monitoring in the safety PLC K1.

- Whilst the guard is open, only setup mode with limited speed is possible (SF 4). The enabling switch S1 must also be actuated (SF 3). The movement is initiated by a separate control device on a hand-held terminal (not shown).

- When the enabling switch S1 is released or fully depressed to the third stage, 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 inverters T1 and T2. Stopping is monitored by the safety PLC K1. Following stopping, STO is activated in the frequency inverters. This process implements SS1.

- The speed of each axis is monitored in setup mode (SF 4) by the safety PLC K1. Two encoders for each axis (B2/B3 and B4/B5) are used to detect the speed. Should the maximum permissible speed be exceeded, the hazardous movement is halted by activation of the STO safety sub-function in the frequency inverters T1/T2.
- Faults in the position switch B1, the pulse blocking relays of T1b/T2b and the rotary encoders B2 to B5 are detected by the safety PLC K1. The fast-stop ramp is also monitored and the stationary state recognized by the safety PLC K1, with the aid of the rotary encoders.
- Both shut-off paths of T1 and T2 are monitored. In order to detect faults, the relays of the pulse blocks T1b/T2b each possess a mechanically linked break contact that is read in by the safety PLC K1. Faults in the controller enable are apparent in the form of disruptions to operation of the machine.

Design features

- Basic and well-tried safety principles and the requirements for Category B are observed. Protective circuits (such as contact protection, earthing of the circuit, precharging of the frequency inverter‘s intermediate circuits), as described in the first sections of Chapter 8 of IFA Report 2/2017e, are present.
- Cross-circuits and short-circuits in electrical supply lines must be considered in accordance with 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 S2 is a cam-operated selector switch with positive mode of actuation. The design of the operating mode selector switch permits fault exclusions in accordance with ISO 13849-2, Table D.8.
- B1 is a position switch with separate actuator. The switch features two direct opening contacts B1a/B1b that satisfy the requirements of IEC 60947-5-1, Annex K. The actuating mechanism must be designed and fitted as specified.
- The three-stage enabling switch S1 is a single-channel device. The enabling switch S1 satisfies the requirements of IEC 60204-1, Subclause 10.9.
- T1 and T2 are frequency inverters with integrated STO safety sub-function satisfying Category 3 and PL d. STO is activated by deactivation of pulse blocking and controller enable.
- The safety PLC K1 satisfies the requirements for Category 4 and PL e.
- The safety-related application software (SRASW) for the safety PLC K1 is programmed in accordance with the requirements for PL d and the instructions in Subclause 4.6.3 and where applicable 4.6.4 of ISO 13849-1.

Note:

- The rotary encoder pairs B2/B3 and B4/B5 must be fitted to the respective motors in such a way that simultaneous failure 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 operating mode selector switch S2 with positive mode of actuation and to separation of the operating modes in this switch. Owing to the implemented control architecture and installation in a switchgear cabinet with a minimum ingress protection of IP 54, faults such as short-circuits between adjacent tracks, contact points and conductors can be excluded. The conditions for fault exclusion up to a maximum of PL d to ISO 13849-2, Table D.8 are met. Based upon an analysis, faults in the operating mode selection arrangement that could prevent the required safety functions being effective can be excluded.

- A B_{10D} of 20,000,000 operation cycles [S] each is stated for the direct opening contacts B1a/B1b of the position switch B1. 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 26,042 years.
  Among the measures taken is shrouded mounting of the position switch, which reduces the impact of environmental effects to a minimum and at the same time prevents tampering.

- Only release of the enabling switch S1 (stage 2 to stage 1) is considered in this example. A B_{10D} of 100,000 operation cycles [S] is assumed here. Setup once daily and 10 operations per day of the enabling switch S1 yield an n_{op} of 2,400 cycles per year. This yields an $MTTF_D$ of 416.7 years, and an average probability of dangerous failure of $1.1 \cdot 10^{-6}$ per hour in Category 1.

- The safety PLC K1 satisfies the requirements for Category 4, PL e and SIL 3. The PFH_D is $3.2 \cdot 10^{-8}$ per hour [M].

- T1 and T2 are frequency inverters with integrated STO safety sub-function. They satisfy the requirements for Category 3, SIL 2 and PL d. The *PFH* is $3.2 \cdot 10^{-7}$ per hour [M]. These data for T1 and T2 are valid only when the manufacturer‘s specifications for fault detection by external components are implemented.

- The rotary encoder pairs B2/B3 and B4/B5 are flanged to the right and left-hand sides of their respective 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 B2/B3 and B4/B5 is estimated at 99%, owing to the cross monitoring of the signals by the safety PLC K1.

- Adequate measures against common cause failure are taken for the subsystem comprising the position switch B1 and the rotary encoders B2/B3 (65 points): separation (15), protection against overvoltage etc. (15) and protection against environmental conditions (25 + 10).

- Evaluation of the SF 1 safety function, “operating mode selection”, yields the following result: the formulation of fault exclusions for S2 based upon the design characteristics enables the separation of setup and automatic modes to be classified as PL d. The limitation to PL d is due to the fact that the evaluation of the operating mode selector switch is based solely upon fault exclusions (see ISO 13849-2, Table D.8). The PFH_D value is determined solely by the contribution of the safety PLC K1, and is $3.2 \cdot 10^{-8}$ per hour.

- Evaluation of the SF 2 safety function, “automatic mode; SS1 following opening of a safeguard”, yields the following result: the subsystem comprising B1/B2/B3 satisfies Category 3 with a high $MTTF_D$ (40 years) and a high DC_{avg} (99%). This yields an average probability of dangerous failure PFH_D of $6.9 \cdot 10^{-8}$ per hour. The combination of the respective subsystems of the position switch/rotary encoders B1/B2/B3, safety PLC K1 and frequency inverter T1 yields an average probability of dangerous failure PFH_D of $4.2 \cdot 10^{-7}$ per hour. This satisfies PL d.

- Evaluation of the SF 3 safety function, “setup mode; releasing or fully depressing the three-stage enabling switch S1 brings the drive to a halt (SS1)”, yields the following result: the subsystem B2/B3 satisfies Category 3 with a high $MTTF_D$ (40 years) and a high DC_{avg} (99%). This yields an average probability of dangerous failure PFH_D of $6.9 \cdot 10^{-8}$ per hour.

  The combination of the respective subsystems of the enabling switch S1, rotary encoders B2/B3, safety PLC K1 and frequency inverter T1 yields an average probability of dangerous failure PFH_D of $1.6 \cdot 10^{-6}$ per hour. This satisfies PL c.

- Evaluation of the SF 4 safety function, “setup mode; safely-limited speed – exceeding of the maximum permissible speed leads to the drive being brought to a halt (STO)”, yields the following result: the subsystem B2/B3 satisfies Category 3 with a high $MTTF_D$ (40 years) and a high DC_{avg} (99%). This yields an average probability of dangerous failure PFH_D of $6.9 \cdot 10^{-8}$ per hour.

  The combination of the respective subsystems of the rotary encoders B2/B3, safety PLC K1 and frequency inverter T1 yields an average probability of dangerous failure PFH_D of $4.2 \cdot 10^{-7}$ per hour. This satisfies PL d.

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

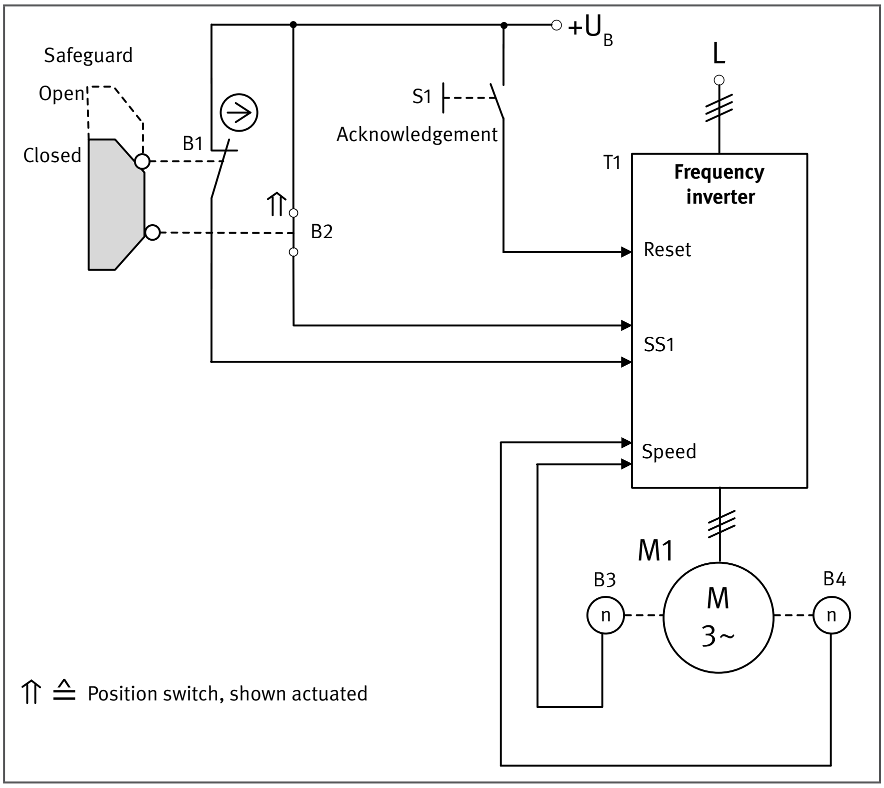


Figure A.19:
Conceptual schematic diagram of position monitoring

Safety functions

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

Functional description

- When the safeguard is opened, the “safe stopping” (SS1) input of the frequency inverter T1 is interrupted in two channels via the position switches B1 and B2. The frequency inverter T1 initiates stopping and monitors the deceleration ramp of the motor. When standstill is reached, STO is activated.
- The rotary encoders B3 and B4 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 inverter T1.
- The frequency inverter monitors the function of the position switch B1 in comparison with B2. In the event of a fault, continued operation is prevented.
- The hazardous zone can be accessed from behind the safeguard; 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 sub-function is implemented by monitoring of the deceleration ramp (SS1-r).
- The control voltage Uop and the internal control voltage of the frequency inverter T1 are generated from the intermediate circuit voltage of the frequency inverter. The drive is brought to a controlled halt even in the event of a voltage breakdown.

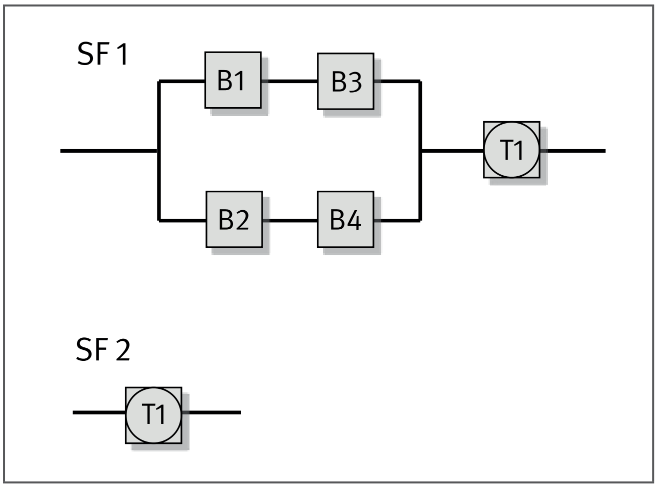


Figure A.20:
Safety-related block diagrams for Example 10

Design features

- Basic and well-tried safety principles and the requirements for Category B are observed. Protective circuits (such as contact protection, circuit earthing, precharging of the frequency inverter's intermediate circuit), as described in the initial sections of Chapter 8 of IFA Report 2/2017e, are present.
- Cross-circuits and short-circuits in electrical supply lines must be considered in accordance with 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 inverter T1 is equipped with the integrated SS1 safety sub-function with ramp monitoring (SS1-r) satisfying Category 3 and PL d.
- Actuators and position switches must be secured against displacement. Only rigid mechanical components (not spring elements) may be used.
- The position switch B1 is a position switch with direct opening action that satisfies the requirements of IEC 60947-5-1, Annex K.
- Malfunctions in the actuating and operating mechanism of the safeguard are detected by two counter-operated position switches B1 and B2 (break contact and make contact combination).
- The frequency inverter T1 is equipped with an acknowledgement function (manual reset).
- The requirements for the manual reset function in accordance with ISO 13849-1, Subclause 5.2.2 are met. These include the requirement for T1 to activate the reset function only once S1 has been released and for resetting alone not to lead to restarting 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

- The position switch B1 has a B_{10D} of 20,000,000 operation cycles [S]. At an n_{op} of 7,680 cycles, the $MTTF_D$ is 26,041 years.
- A B_{10D} value of 1,000,000 operation cycles [M] is stated for the position switch B2. At an n_{op} of 7,680 cycles per year, the $MTTF_D$ is 1,302 years.

- The frequency inverter T1 with integrated SS1 safety sub-function and acknowledgement function satisfies the requirements for Category 3 and PL d. The PFH_D is $2.0 \cdot 10^{-7}$ per hour [M].

- The pushbutton S1 for manual reset is a standard pushbutton. Since a trailing signal edge caused by release of the pushbutton is required for signalling (see ISO 13849-1, Subclause 5.2.2), failure of the button does not lead to a hazardous fault. For this reason, S1 is not considered in the quantification.

- The encoder manufacturer states an $MTTF_D$ of 40 years each for the rotary encoders B3 and B4 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 inverter T1.

- The *DC* for the rotary encoders B3 and B4 is estimated at 99%, owing to the cross monitoring of the signals in the frequency inverter T1.

- Adequate measures against common cause failure are taken for the subsystem comprising the position switches B1/B2 and the rotary encoders B3/B4 (65 points): separation (15), protection against overvoltage etc. (15) and protection against environmental conditions (25 + 10).

- Evaluation of the SF 1 safety function, “safe stopping when the safety guard is opened”, yields the following result: the subsystem B1/B2/B3/B4 satisfies Category 3 with a high $MTTF_D$ (38 years) and a high DC_{avg} (99%). This yields an average probability of dangerous failure of $7.0 \cdot 10^{-8}$ per hour. The combination of the subsystems of position switches/rotary encoders (B1/B2/B3/B4) and frequency inverter T1 yields an average probability of dangerous failure PFH_D of $2.7 \cdot 10^{-7}$ per hour. This satisfies PL d.

- For the SF 2 safety function, “manual reset by release of the actuated acknowledgement pushbutton S1 with the safeguard closed”, the resulting average probability of dangerous failure PFH_D is $2.0 \cdot 10^{-7}$ per hour. This satisfies PL d.

Example 11: Inverter-actuated power drive control with integrated safe movement monitoring

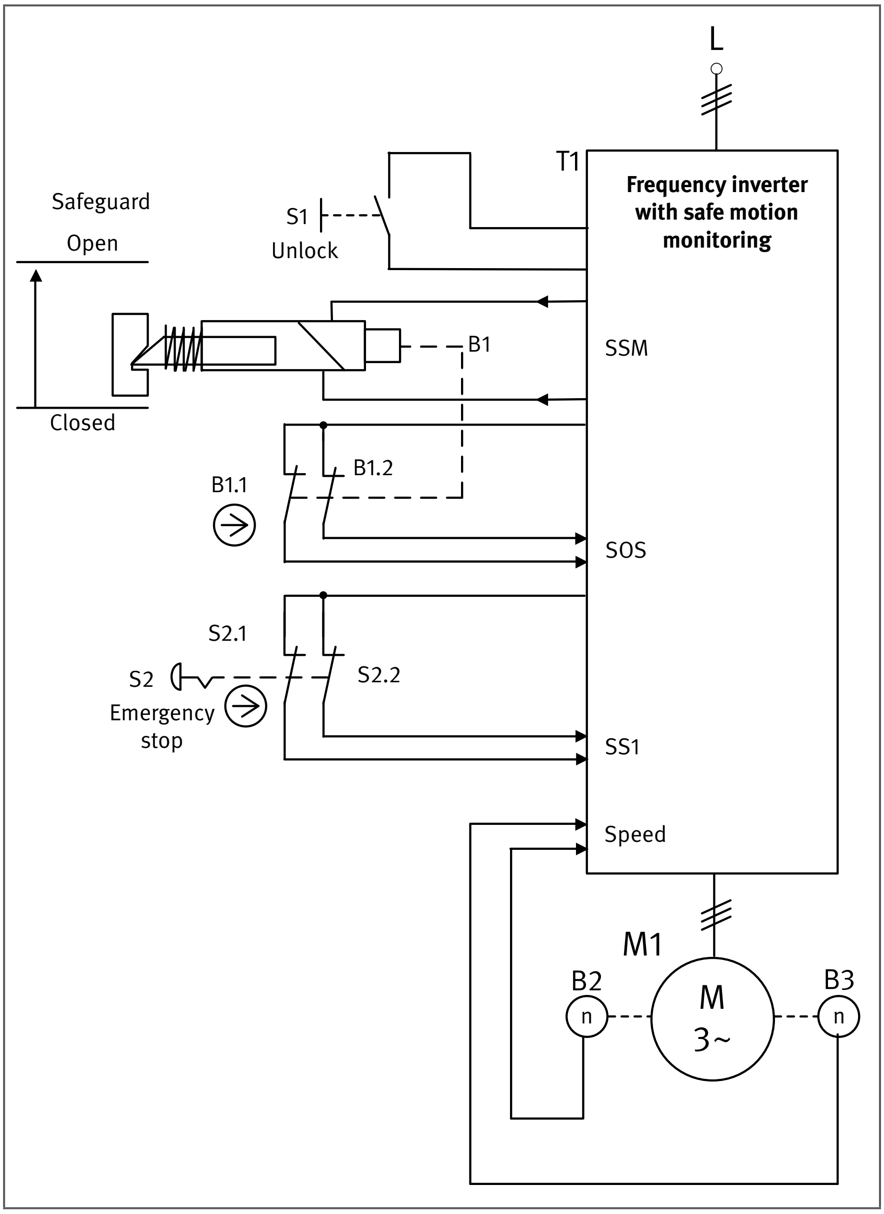


Figure A.21:
Position monitoring of a safeguard with guard locking device and emergency stop

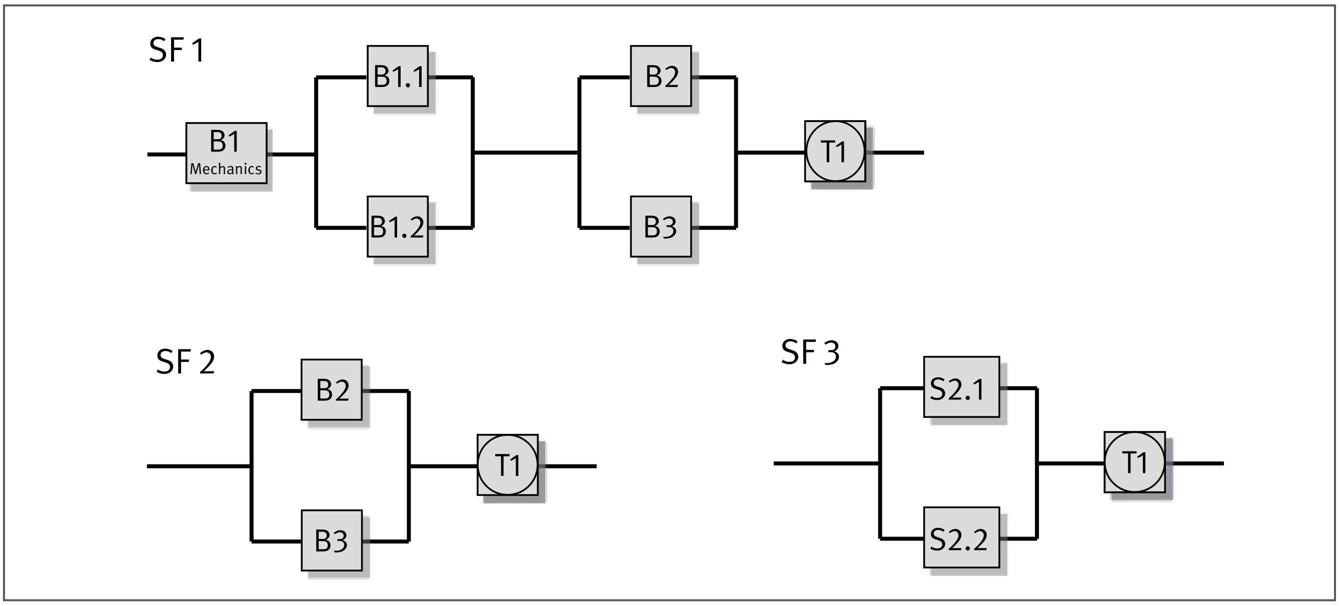
Safety functions

- SF 1: Safe operating stop (SOS) when the guard locking device is released
- SF 2: Release of guard locking device at standstill
- SF 3: Actuation of the emergency-stop device leads to controlled stopping (SS1-r)

Functional description

- Unlocking of the safeguard is requested by actuation of the inch button S1. This causes the frequency inverter T1 to reduce the drive speed to zero. Opening of the safeguard is possible only with the drive at standstill. At a motor speed of (almost) zero, the frequency inverter uses the safety sub-function SSM (safe speed monitoring) to generate a safe output signal to release the locking mechanism in the guard locking device B1.

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



- Unlocking of the safeguard is detected by the position switches B1.1 and B1.2. The safety sub-function SOS (safe operating stop) is then activated in the frequency inverter T1.

- When the emergency-stop device S2 is actuated during a motor movement, the drive is brought to a controlled stop as fast as possible by SS1 (safe stop 1 with monitoring of the deceleration ramp, SS1-r).

- Where hazardous zones can be accessed from behind the safeguard, an acknowledgement facility (manual reset) 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.

Design features

- The frequency inverter T1 possesses the integrated safety sub-functions SOS, SS1-r, SSM and STO (not used in this example).

- Note that with the SS1-r function, the available braking torque may be reduced in the event of a fault in the frequency inverter.

- The two rotary encoders B2 and B3 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 (B2 and B3) in a two-channel arrangement. Depending upon the frequency inverter 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 laid down by the frequency inverter manufacturer regarding the use of rotary encoders must be observed.

- Cross-circuits and short-circuits in electrical supply lines must be considered in accordance with 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 safeguardis a safety guard with guard locking device B1. Access to the hazardous movementis prevented until the movement has come to a halt (SF2). 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 unlock solenoid has been actuated. According to the manufacturer, the guard locking device prevents the assumption of an inadvertent locking position. Unexpected start-up of the motor is prevented whilst the safety guard is open by virtue of the fact that prevention of assumption of an inadvertent locking position prevents the contacts B1.1 and B1.2 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

- B1.1 and B1.2 are the direct opening contacts for monitoring the locking mechanism of the guard locking device. In conjunction with the guard locking mechanism‘s protection against assumption of an inadvertent locking position, this results in the closed position of the safety guard also being detected. A B_{10D} value of 2,000,000 operation cycles [S] each is assumed for B1.1 and B1.2. At an n_{op} of 46,080 cycles per year, the $MTTF_D$ is 434 years each.

- Fault exclusion can be assumed for the mechanical components of the guard locking device, including mechanical failure of the locking mechanism, provided 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 unlock solenoid until the guard door is closed; refer in this context also to DGUV Informative publication 203-079 concerning the selection and fitting of interlocked guards
  – 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
  – Dropping of the door does not lead to the actuator being used outside the range specified by the manufacturer
  – Damage that could be caused by foreseeable external influences (such as the ingress of dirt and dust, mechanical shock) is prevented by the form of mounting or need not be anticipated owing to the conditions of use

  The fault exclusion must be confirmed by the manufacturer.

- A B_{10D} value of 100,000 operation cycles [S] is assumed for each contact of the emergency-stop device S2, which is constructed in accordance with the IEC 60947-5-5 product standard. At 30 operations per year, the $MTTF_D$ of each contact is 33,333 years. Owing to capping of the $MTTF_D$ to 100 years per contact, the resulting PFH_D for the emergency-stop device S2 is $4.3 \cdot 10^{-8}$ per hour.

- The rotary encoders B2 and B3 are fitted to the same shaft. They are conventional encoders with pulse outputs. The signals are evaluated within the frequency inverter. The manufacturer states an $MTTF_D$ of 50 years for the encoders.

- The frequency inverter T1 with safe movement monitoring possesses the following integrated safety sub-functions:

  – Safe torque off (STO)
  – Safe stop 1 ramp monitored (SS1-r)
  – Safe operating stop (SOS)
  – Safe speed monitoring (SSM)

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

- Owing to cross monitoring by the frequency inverter T1, a *DC* of 90% each is assumed for the rotary encoders B2 and B3. The *DC* for the contacts B1.1/B1.2 monitoring the position of the locking mechanism is estimated at 99% each.

- Adequate measures against common cause failure are taken for the subsystem of B2/B3 (65 points): physical separation (15), protection against overvoltage etc. (15), protection against contamination and EMC and protection against environmental conditions (25 + 10).

- Adequate measures against common cause failure are taken for the subsystem of B1.1/B1.2 (70 points): physical separation (15), protection against overvoltage etc. (15), use of well-tried components (5), protection against contamination and EMC and protection against environmental conditions (25 + 10).

- The guard locking device subsystem B1.1/B1.2 satisfies Category 3 and PL e with a high $MTTF_D$ (100 years) and a high DC_{avg} (99%). This yields a PFH_D of $2.5 \cdot 10^{-8}$ per hour.

- The subsystem B2/B3 satisfies Category 3 with a high $MTTF_D$ (50 years) and medium *DC* (99%). This yields an average probability of dangerous failure PFH_D of $1.2 \cdot 10^{-7}$ per hour in the PL d range.

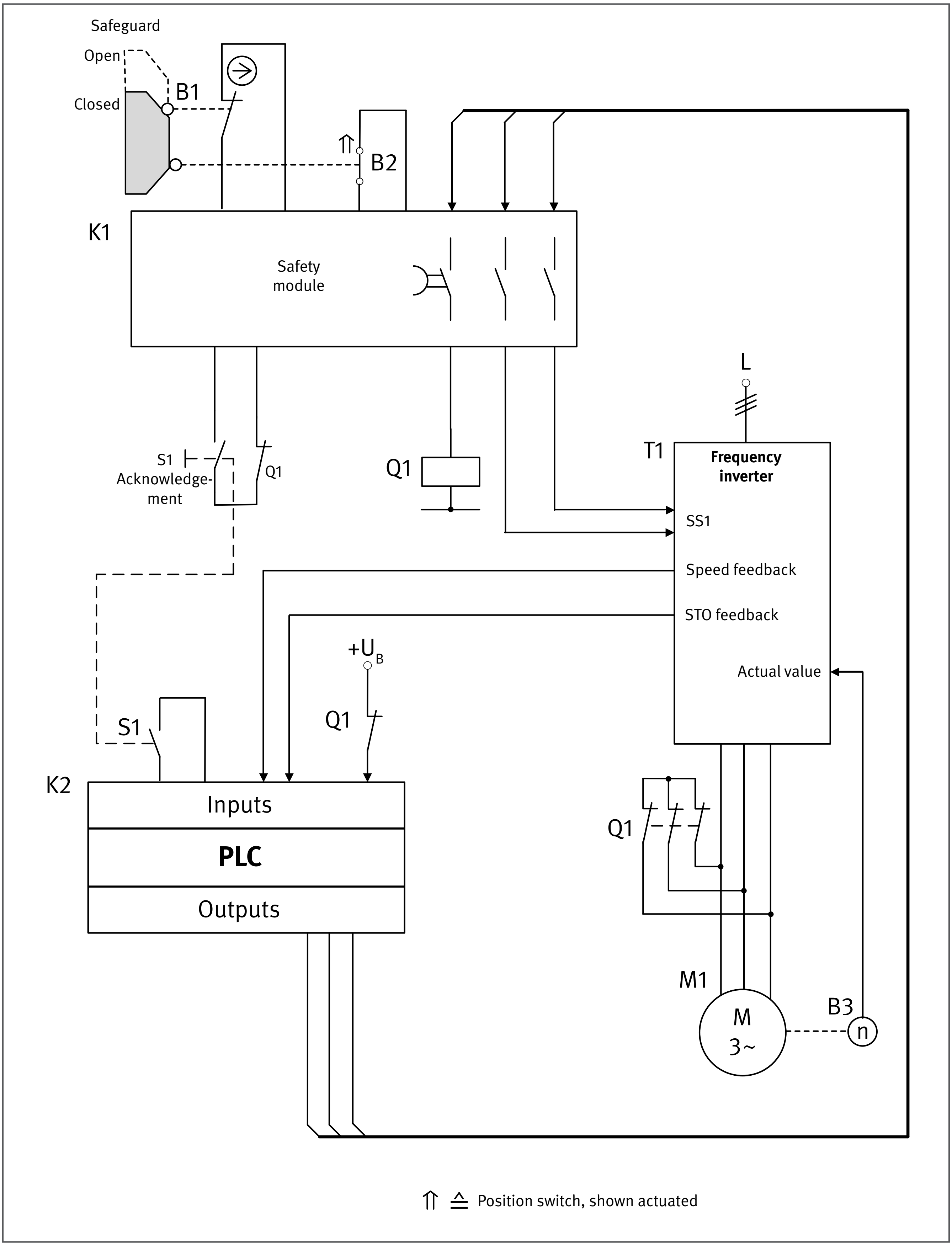
- For the SF 1 safety function, “ Safe operating stop (SOS) when the guard locking device is released”, the evaluation yields the following result: the combination of the subsystems of position switch B1.1/B1.2, rotary encoders B2/B3 and frequency inverter T1 yields an average probability of dangerous failure PFH_D of $2.0 \cdot 10^{-7}$ per hour. This satisfies PL d.

- For the SF 2 safety function, “release of the guard locking device at standstill by SSM”, the evaluation yields the following result: the combination of the subsystems of rotary encoders B2/B3 and frequency inverter T1 yields an average probability of dangerous failure PFH_D of $1.7 \cdot 10^{-7}$ per hour. This satisfies PL d.

- For the SF 3 safety function, “actuation of the emergency stop control device leads to controlled stopping SS1”, the evaluation is as follows: the combination of the subsystems of emergency stop device S2 and frequency inverter T1 yields an average probability of dangerous failure PFH_D of $9.3 \cdot 10^{-8}$ per hour. This computes to PL e. However, since the frequency inverter 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 inverter and short-circuit contactor – PL e

Figure A.23:
Conceptual schematic diagram of the power drive control



⥣ ≙ Position switch, shown actuated

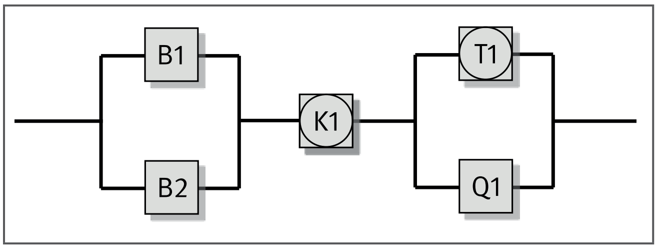


Figure A.24:
Safety-related block diagram for Example 12

Safety function

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

  Note:

  Different components are employed for “stopping” and “prevention of unexpected start-up”, since the additional short-circuit contactor Q1 is required only for the prevention of unexpected start-up. The short-circuit contactor Q1 constitutes a third shut-off path, by means of which a higher PL is attained. This division into two separate safety functions is made for calculation of the *PFH*. Only the prevention of unexpected start-up will be considered at this point, however.

Functional description

- Opening of the safeguard is detected by the safety module K1 via the position switches B1 and B2. The instantaneous enabling paths of the safety module K1 drop out. SS1 of the frequency inverter T1 is initiated and the drive is brought to a standstill in a controlled manner. The short-circuit contactor Q1 then drops out with a delay. Closing of the break contacts of the short-circuit contactor Q1 short-circuits the supply conductors to the motor. The drive is in STO.

- Welding of the contacts of the short-circuit contactor Q1 would always be evident when voltage is supplied to the motor via the inverter T1, since the output protective device would trip. The short-circuit contactor Q1 is monitored by the return circuit of the safety module K1. In addition, further fault detection exists in the PLC K2, which monitors for “sticking”.

- 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 the frequency inverter T1 to be supplied from the intermediate DC circuit;
  – the safety module K1 to have an uninterruptible power supply.

Design features

- Basic and well-tried safety principles and the requirements for Category B are observed. Protective circuits (such as contact protection), as described in the first sections of Chapter 8 of IFA Report 2/2017e, are present. In this example, the basic safety principles include the closed-circuit current principle and earthing of the control circuit. Well-tried safety principles include overdimensioning of the contact ratings of B1, B2 and Q1.

- Cross-circuits and short-circuits in electrical supply lines must be considered in accordance with 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 inverter T1 possesses the integrated safety sub-functions of STO and SS1.

- The position switch B1 is a position switch with direct opening action to IEC 60947-5-1, Annex K.

- Malfunctions in the actuating and operating mechanism of the safeguard are detected by two counter-operated position switches B1 and B2 (break contact and make contact combination).
- Actuators 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 behind the safeguard, an acknowledgement facility (manual reset) 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 nevertheless used, for example on presses, for the assurance of 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 safety sub-function fail, the contactor Q1 short-circuits the operational voltage of the motor, and damage to the contactor can be expected. The short-circuit contactor Q1 must therefore then be replaced, and any other faults eliminated by repairs.
- Only a part of the function of the control system is presented here. Selection of the operating mode for example is not shown.

Caclculation of the probability of failure

- The position switch B1 has a B_{10D} value of 20,000,000 operation cycles [S]. 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 2,083 years.
- A B_{10D} value of 1,000,000 operation cycles [M] is stated for the 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 position switch exhibits a limited life T_{10D} of 10 years. It must be replaced when this time has expired. SISTEMA generates a warning message with yellow status for this.
- The safety module K1 is a standard commercial component for use in PL e and Category 4. The PFH_D is $1.8 \cdot 10^{-8}$ per hour [M].
- The short-circuit contactor Q1 has a mechanical life of 2,000,000 operation cycles. In this application, it is under virtually no electrical load; the mechanical life is therefore set as the B_{10D} value. At an n_{op} of 96,000 cycles per year, the $MTTF_D$ is 208 years.
- The frequency inverter T1 possesses the integrated STO safety sub-function with a check-back output. It is suitable for use in PL d and Category 3. The PFH_D value of the STO is $2 \cdot 10^{-7}$ per hour.

  As shown in the safety-related block diagram (Figure B.24), the frequency inverter 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 ISO 13849-1. The *PFH* for this subsystem is therefore calculated by means of the procedure described in SISTEMA Cookbook 4, Chapter 2:

  The relationship $MTTF_D = 1/PFH_D$ yields an $MTTF_D$ of 570 years for the frequency inverter T1. The internal DC of the frequency inverter T1 cannot be used again, since it has already been used to reduce the *PFH* of T1. An additional DC achieved by way of other components can however be taken into account.
- The additional fault detection relating to the STO safety sub-function of the frequency inverter T1 is external, being provided in this case in the PLC K2 by comparison of the contactor Q1 and STO check-back. A *DC* of 99% is assumed for this fault detection.

- The *DC* for the position switches B1 and B2 is stated as 99%, owing to monitoring by the safety module K1.
- A *DC* of 99% is assumed for the contactor Q1. The short-circuit contactor Q1 is monitored by the return circuit of the safety module K1. In addition, further fault detection exists in the PLC K2, which monitors for "sticking".

  Note:

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

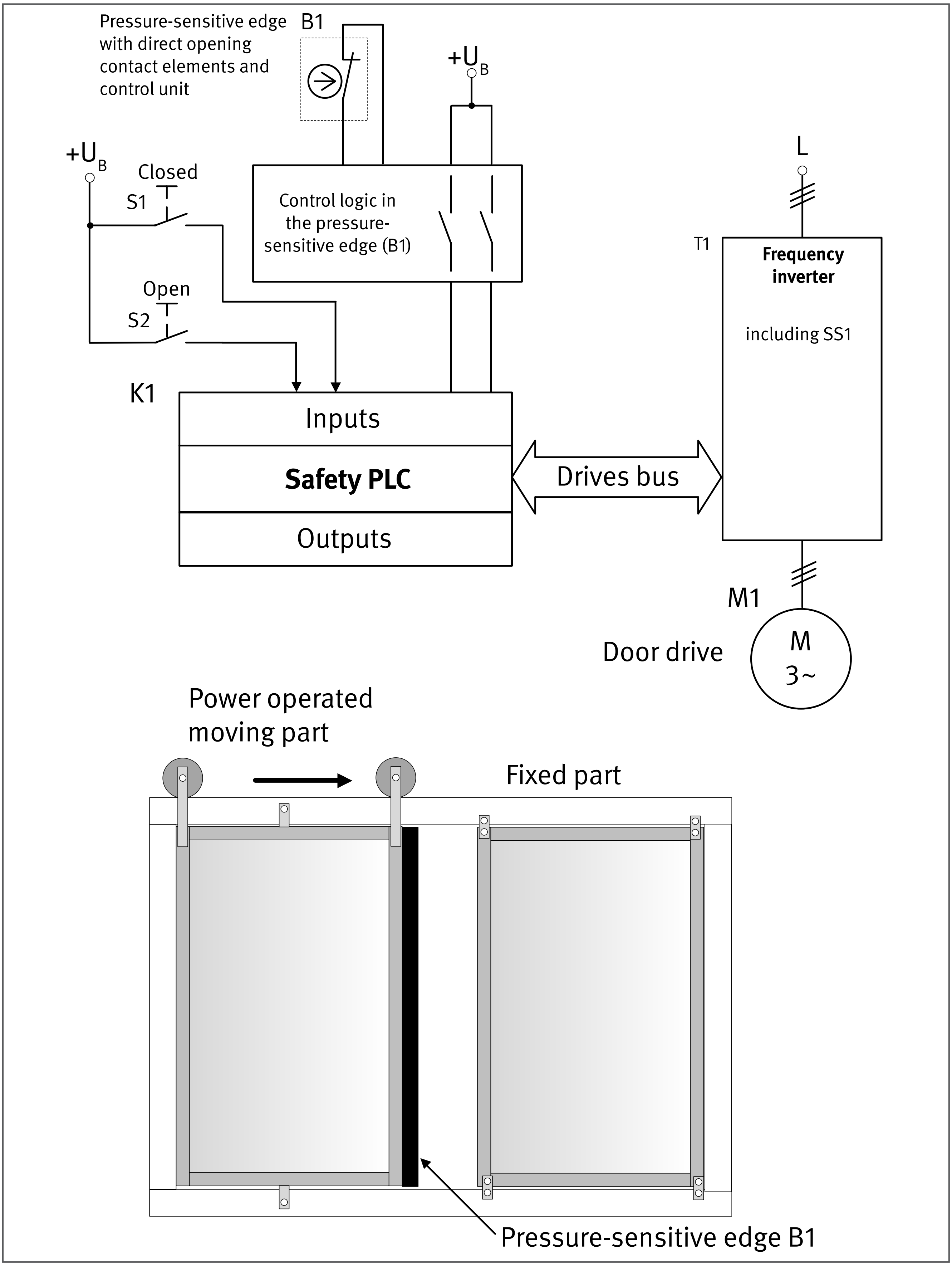
  Execution of the safety function requires the break contacts of the short-circuit contactor Q1 to close, thereby enabling current to flow in the event of a fault in the frequency inverter T1 (deviation from the closed-circuit current principle).

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

- Adequate measures against common cause failure are taken for the subsystem comprising B1 and B2 (75 points): separation (15), protection against overvoltage etc. (15), well-tried components (5), FMEA (5) and protection against environmental conditions (25 + 10). Adequate measures against common cause failure are taken for the subsystem of the frequency inverter T1 and the short-circuit contactor Q1 (90 points): separation (15), diversity (20), protection against overvoltage etc. (15), FMEA (5) and protection against environmental conditions (25 + 10).
- The subsystem B1/B2 satisfies Category 4 with a high $MTTF_D$ per channel (1,392 years) and a high *DC* (99%). This yields an average probability of dangerous failure PFH_D of $1.6 \cdot 10^{-9}$ per hour.
- Owing to the limited life of the position switch B2 in this application, timely replacement after ten years is required.
- 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 PFH_D of $5.5 \cdot 10^{-9}$ per hour.
- For the SF 1 safety function, "STO of the motor following opening of the safeguard and stopping of the drive", the evaluation yields the following result: the combination of the subsystems B1/B2, K1 and T1/Q1 yields an average probability of dangerous failure PFH_D of $2.5 \cdot 10^{-8}$ per hour. This satisfies PL e.

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

Figure A.25:
Conceptual schematic diagram of the power drive control


Pressure-sensitive edge with direct opening contact elements and control unit
B1
$+U_B$
$+U_B$
Closed
S1
Open
S2
Control logic in the pressure-sensitive edge (B1)
L
T1
Frequency inverter
including SS1
K1
Inputs
Safety PLC
Outputs
Drives bus
M1
Door drive
M
3~
Power operated moving part
Fixed part
Pressure-sensitive edge B1

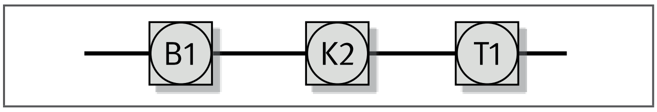


Figure A.26:
Safety-related block diagram for Example 13

Safety function

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

Functional 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 and retrieval by robots. Opening and closing of the safety guard must not give rise to hazards, such as crushing of the operator by a closing movement. Provided the limit values for power operated guards are observed, it is assumed that no hazard exists (see comments).

  If the limit values cannot be observed, the hazardous zone must be guarded by additional safeguards.

  In the present example, a pressure sensitive edge B1 is fitted on the closing edge of the safety guard. Actuation of the pressure sensitive edge B1, which occurs only when the operator is present in the hazardous zone of the safety guard as it is being closed, brings the drive so rapidly to a halt by means of the integrated logic in the pressure sensitive edge, the safety PLC K1 and the frequency inverter T1 that the permissible closing forces are not exceeded.

Comments: Limit values for power operated guards

- The static force on 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 an additional safeguard that triggers automatic opening (reversal of movement) when it makes contact with an obstruction, the static force and kinetic energy must not exceed 150 N and 10 Joules respectively (see EN 953, Subclause 5.2.5.2). These provisions apply only where the closing edges are at least 8 mm in width and no shearing 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: Subclause 5.1.1.5.3 of EN 12453

- 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 A.27 and Table A.2 in this report).

  Where

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

  F_s: Maximum force, measured with an instrument to EN 12453 Subclause 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

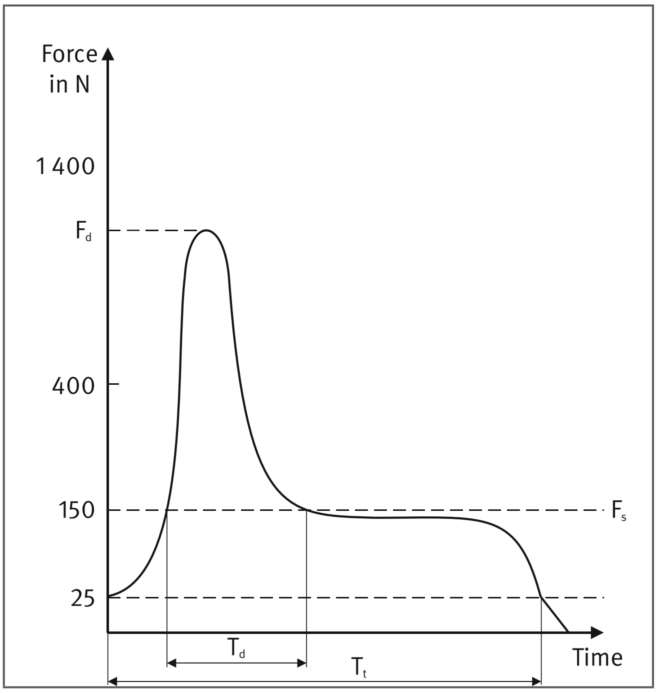


Figure A.27:
Closing forces as a function of time, from EN 12453

Table A.2:
Admissible dynamic forces

Admissible dynamic forces in N	Between closing edges and counterclosing edges		Between flat areas other than closing edges and counterclosing edges, › 0.1 m² with no side ‹ 100 mm
	In opening gaps of 50 to 500 mm	In opening gaps › 500 mm	
Horizontally moving gate	400	1,400	1,400
Gate rotating around an axis perpendicular to the floor	400	1,400	1,400
Vertically moving gate	400	400	1,400
Gate rotating sround an axis parallel to the floor – barriers	400	400	1,400

- The values specified in Table A.2 are maximum values permitted for a duration of no more than 0.75 s (T_d ≤ 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 protection device or similar must be provided for the operator.

Design features

- Basic and well-tried safety principles and the requirements for Category B are observed. Protective circuits (such as contact protection, earthing of the circuit), as described in the first sections of Chapter 8 of IFA Report 2/2017e, 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 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 with integrated logic B1 satisfies the requirements of ISO 13856-2 and has the function of safeguarding crush and shear points. The pressure sensitive edge B1 is connected to the safety PLC K1 via the integrated logic. The pressure sensitive edge with integrated logic B1 satisfies the requirements of ISO 13849-1 for Category 3, PL d.

- The machine manufacturer must review the suitability of the pressure sensitive edge for the application concerned (for example with respect to adequate deformation distance, consideration of the ambient influences and actuation range).

- The power drive control T1 possesses the SS1 safety sub-function.

- The safety PLC K1 and the power drive control T1 are safety components for use up to Category 4 and PL e (K1) and Category 3 and PL d (T1). Faults are detected when they occur and bringing about of the safe state is triggered. The safety PLC K1 and the power drive control T1 are connected over a safety bus system for use in PL d in accordance with IFA Report 2/2017e, Section 6.2.18.

- The safety-related application software (SRASW) for the safety PLC K1 is programmed in accordance with the requirements for PL d and the instructions in Subclauses 4.6.3 and 4.6.4 of ISO 13849-1.

Calculation of the probability of failure

- The manufacturer states Category 3, PL d and a PFH_D of $3.2 \cdot 10^{-7}$ per hour [M] for the pressure sensitive edge with integrated logic B1.

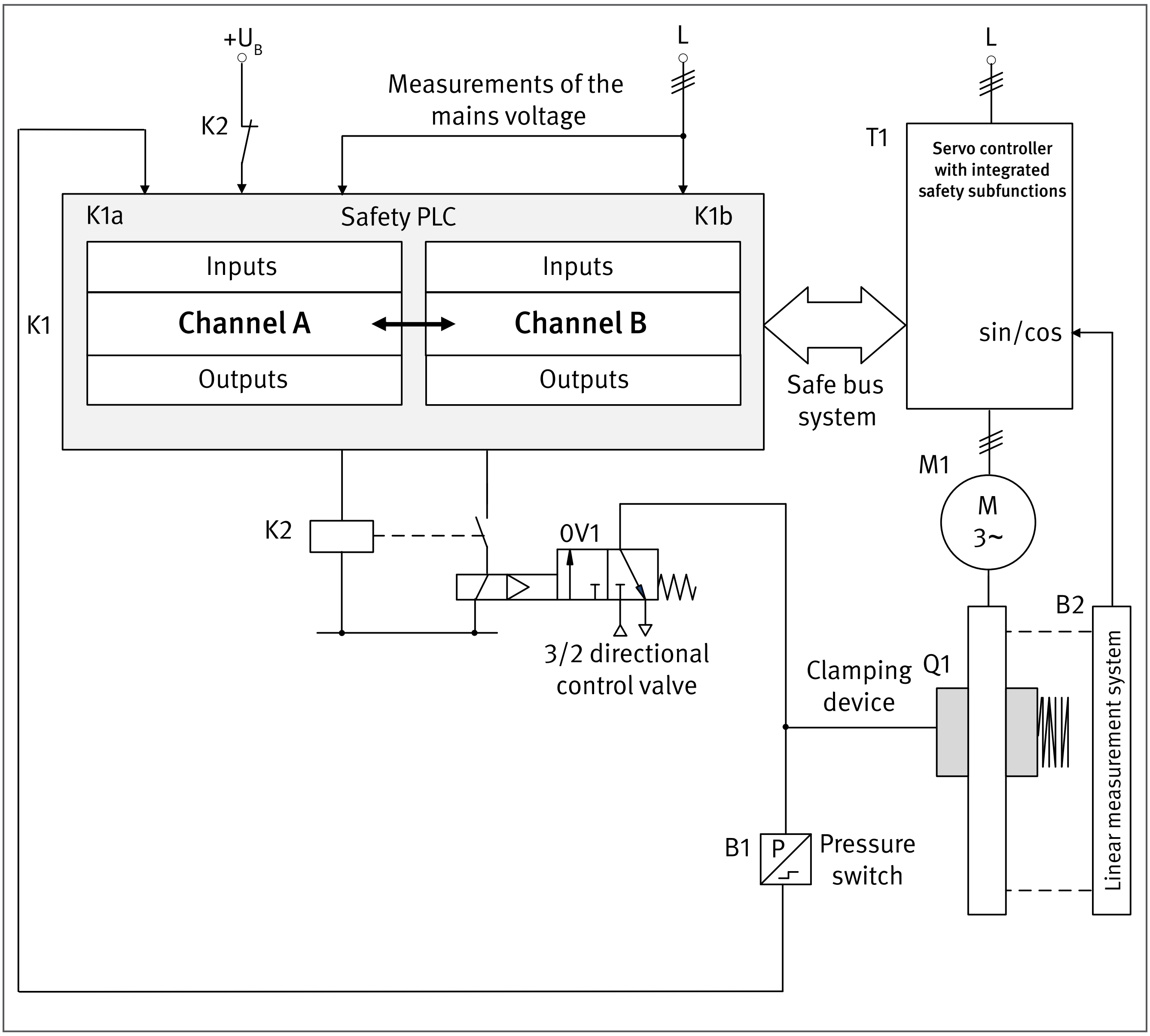
- The safety PLC K1 has a PFH_D of $1.0 \cdot 10^{-8}$ per hour [M].

- The power drive control T1 is included in the analysis with a PFH_D of $1.5 \cdot 10^{-8}$ per hour [M] and PL d.

- For the SF 1 safety function, “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 B1/K1/T1 yields an average probability of dangerous failure PFH_D of $3.4 \cdot 10^{-7}$ per hour in the PL d range.

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

Figure A.28:
Conceptual schematic diagram of the power drive control



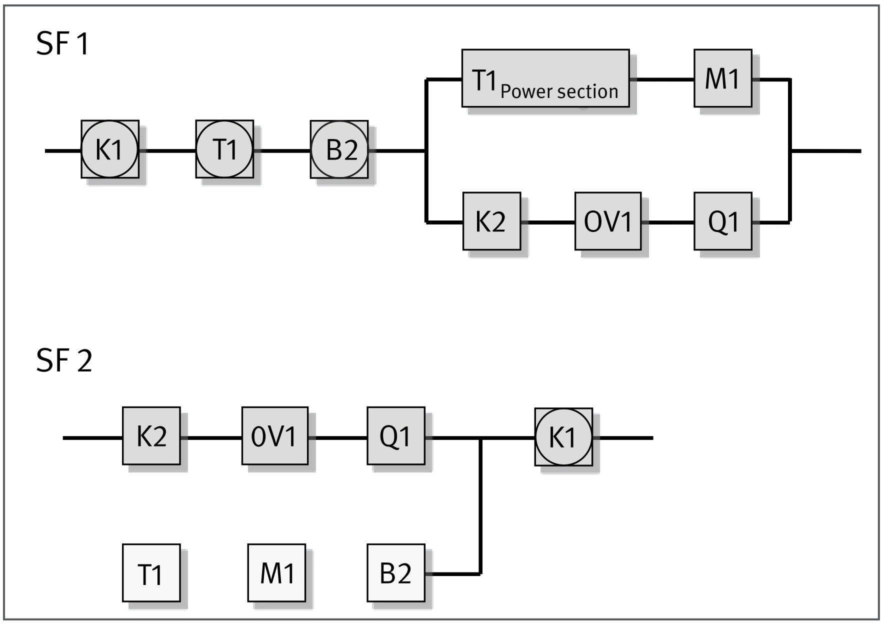
Safety functions

- SF 1: Safe holding against gravity in setup and automatic mode (SOS)
- SF 2: Safe holding against gravity in the event of voltage breakdown

Functional description

- The gravity-loaded vertical axis is controlled by the safety PLC K1 in conjunction with the servo controller T1. The safety PLC K1 comprises a PLC K1a in combination with an NC axis control K1b. The safety PLC K1 performs plausibility checks, for example regarding the control pressure of the clamping device Q1 and its actuation.

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



- In SF 1, “safe holding against gravity in setup and automatic mode (SOS)”, the axis is braked to standstill in setup and automatic mode by SS2. During subsequent safe holding against gravity, the load of the vertical axis is held in position by the integrated safety sub-function SOS (safe operating stop: the motor is at a standstill and withstands external forces) of the servo controller T1. The position of the load is detected in a two-channel architecture by the linear measurement system F1 and the servo controller 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 the servo controller T1 triggering an STO and the pneumatically released clamping device Q1 being engaged by the safety PLC K1 and the contactor relay K2. Following a delay, determined by the control chain (K1-K2-0V1-Q1), the axis is brought to a standstill. The delay in engagement of the clamping device does not give rise to a hazard in this case (minor overrun travel).

- SF 2, “safe holding against gravity in the event of voltage breakdown”, refers to the behaviour of the control system in consideration of interruption of the power supply, in accordance with ISO 12100 [7], Subclause 6.2.11.5. Interruption of the power supply is detected in the safety PLC K1 (monitoring of the mains voltage). Since the control voltage for the safety PLC K1 possesses an adequate buffer time, the clamping device Q1 is engaged not by the “slow” drop in the output voltage of the safety PLC K1, but as quickly as possible by de-energization of the output signal. Following stopping of the motor M1, the clamping device Q1 prevents dangerous descent 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 mains voltage is detected by the servo controller T1 and the clamping device Q1 is actuated directly (for example by SSM). For this purpose however, the control voltage for the servo controller 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 against gravity is assured by the servo controller T1 in the SF 1 safety function, “safe holding against gravity in setup and automatic mode (SOS)”.

2. Voltage breakdown:

SF 2 is activated when a voltage breakdown is detected by the safety PLC K1. Should a voltage breakdown occur, the servo controller T1 is no longer able to hold the vertical axis in position in a controlled manner. The safety PLC receives power from a buffered power supply and causes the spring-operated clamping device Q1 to engage.

In the event of a voltage breakdown, the clamping device Q1 and its actuation by the contactor relay K2 and the 3/2-directional control valve 0V1 constitute the functional channel of a Category 2 system in accordance with ISO 13849-1. The clamping device Q1 is tested statically every eight hours and dynamically every six months as required. Testing is performed by the safety PLC K1, the servo controller T1, the motor M1 and the linear measurement system B2. The specified test intervals are adequate in this application, since the clamping device engages only in the event of a voltage breakdown.

- Test of the clamping device Q1, including actuation by the contactor relay K2 and the 3/2-directional control valve 0V1:

  1. Static test

  Proper operation of the clamping device Q1 including its actuation arrangement is tested daily (or at intervals of eight hours). For the purposes of the test, the clamping device Q1 is subjected to 1.3 times the load torque by the linear motor M1. If the load is held within the specified position range, the clamping device Q1 is deemed to be properly functional. Should the position depart from the specified range, the clamping device Q1 must be checked in accordance with the instruction manual, and if necessary replaced. The position is determined by means of the linear measurement system B2.

  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 Q1, the torque of the drive motor M1 is switched off, as is the 3/2-directional control valve 0V1.

  The overrun travel is measured during the dynamic test of the clamping device Q1. The measured value is compared with the permissible values. Should a measured value exceed the permissible value, the machine must be taken out of operation. The clamping device Q1 must be replaced if necessary.

  Note:

  The test has the purpose of ensuring that the overrun travel does not lengthen impermissibly in the course of the 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

- Basic and well-tried safety principles and the requirements for Category B to ISO 13849-1 are observed. Protective circuits (such as contact protection) and overdimensioning are implemented.

- Cross-circuits and short-circuits in electrical supply lines must be considered in accordance with 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 servo controller T1 with integrated sub-functions are safety components for use in PL d which satisfy Category 3 and the relevant product standards. The servo controller T1 possesses the safety sub-functions SOS, SS2 and STO in this case.

- The contactor relay K2 features mechanically linked contact elements to IEC 60947-5-1, Annex L. The contact position is read back into the safety PLC K1 and checked for plausibility.
- The 3/2-directional control valve 0V1 features a spring return. The safe switching position is reached by means of the contactor relay K2 by removal of the control signal. Basic and well-tried safety principles of design, installation and operation (ISO 13849-2) are a precondition.
- The linear measurement system B2 supplies redundant position information (sine/cosine) and is integrated into the position control loop. The measurement system is connected to the servo controller T1. Fault exclusion is assumed for mechanical failure of the mounting of the linear measurement system‘s detection head and for loss of the material measure (glass measuring rod). The manufacturer must demonstrate the fatigue limit for the fault exclusions (see also IEC 61800-5-2, Table D.16). The manufacturer‘s specific information concerning maintenance must also be observed.
- The software (SRASW) for the safety PLC K1 and the servo controller T1 is programmed in accordance with the requirements for PL d and the information in Subclause 4.6.3 and where applicable 4.6.4 of ISO 13849-1.
- The data bus between the servo controller T1 and the safety PLC K1 is a safety bus system for use in PL d.
- The supply voltage (mains voltage) is monitored in a two-channel architecture in the safety PLC K1.

Remarks

- This example relates to a vertical axis without counterbalancing, and which 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 against gravity. 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 the arrangement for bringing to a standstill and holding against gravity. Where they exist, these standards take priority over type A and type B standards such as ISO 13849-1 (refer to the introduction of ISO 13849-1).
- Comment on the clamping device Q1 in the event of failure of the motor M1:
  A failure of the motor is detected before descent of the suspended load is able to give rise to a hazard. 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_D is $9.0 \cdot 10^{-8}$ per hour [M]. Category 3 and PL d are confirmed by the manufacturer.
- The servo controller T1 possesses the integrated safety sub-functions SOS, SS2 and STO. The PFH_D for the safety sub-functions of the servo controller is $2.3 \cdot 10^{-8}$ per hour [M]. For SF 1 however, the power unit of the servo controller T1 must also be considered in the analysis, since the vertical axis must be held actively against gravity in order to prevent it from dropping. The power unit of the servo controller T1 is included in the analysis of SF 1 in the form of an assumed $MTTF_D$ of 40 years [A].
- A B_{10D} value of 2,000,000 operation cycles [S] is stated for the contactor relay K2. With actuation daily and performance of the static test on six days of the week and 50 weeks of the year, this yields an n_{op} of 600 operation cycles per year. If 20 actuations as a result of voltage breakdown are assumed, the result is an n_{op} of 620 operation cycles per year and an $MTTF_D$ of 32,258 years.

- M1 is a linear motor with insulation class F [3]. The temperature is 20 K below the specified insulation class temperature. As a result, a life of 80,000 hours is assumed for the windings [1]. The daily operating time is eight hours. This yields 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 in this case.

- Table C1 of ISO 13849-1 states a B_{10D} value of 20,000,000 operation cycles [S] for the pneumatic valve 0V1. At 620 operation 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 B_{10D} value of 200,000 operation 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) at 1.5 times the anticipated loading must be performed every eight hours. The manufacturer was consulted regarding use of the brake for emergency-stop braking. The rating for emergency-stop (dynamic braking) is 2,000 operation cycles [M] and serves as the estimate for B_{10D}. At an estimated frequency erring on the safe side of 20 operations per year, the resulting $MTTF_D$ 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 ISO 13849-1, Subclause 4.5.4, a demand rate of ≤ 1/100 of the test rate is a criterion for Category 2, and the $MTTF_{DTE}$ must be greater than 0.5 · $MTTF_D$ of the function channel. The test rate (100 times more frequent than the demand upon the safety function) is not met in SF 2. An additional 10% was therefore added for the Category 2 subsystem. This represents a worst-case estimate, which is described in the IFA Report (see IFA Report 2/2017e, Section 6.2.14, p. 57, 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 B2. 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 inverter 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. The requirements for Category 3 are met.

- $MTTF_D$ values for the individual blocks are required for quantification of the Category 2 subsystem of SF 2. Since only *PFH* values are available for the servo controller T1 and the linear measurement system B2, $MTTF_D$ can be assumed approximately equal to $1/PFH_D$ (refer in this context to SISTEMA Cookbook 4, Section 2). This yields an $MTTF_D$ of 7,610 years for the linear measurement system B2. For the servo controller T1 (power unit + control), the resulting probability of failure is $MTTF_D$ = (1/40 + 1/4,942)-1 years = 39.6 years.

- A *DC* of 99% can be stated for the contactor relay K2, since a signal is always read back into the safety PLC K1.

- A *DC* of 60% is assumed for the linear motor M1, since fault detection is provided 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 owing to static and dynamic testing.

- Adequate measures against common cause failure are provided for the subsystem of the position control or clamping facility of the SF 1 safety function comprising T1power unit, M1/K2, 0V1, Q1 (65 points): separation (15), protection against overvoltage etc. (15) and protection against environmental conditions (25 + 10).

- For the SF 1 safety function, “safe holding against gravity in setup and automatic mode (SOS)”, the evaluation yields the following result: the combination of the subsystems K1/T1/B2/position control or clamping device yields an average probability of dangerous failure PFH_D of $3.1 \cdot 10^{-7}$ per hour. This satisfies PL d.

- For the SF 2 safety function, “safe holding against gravity in the event of voltage breakdown”, the evaluation yields the following result: the combination of the subsystems yields an average probability of dangerous failure PFH_D of $2.1 \cdot 10^{-6}$ per hour. This satisfies PL c.

References

[1] *Farschtschi, A.*: Elektromaschinen in Theorie und Praxis. 2nd ed. VDE, Berlin, Germany 2001

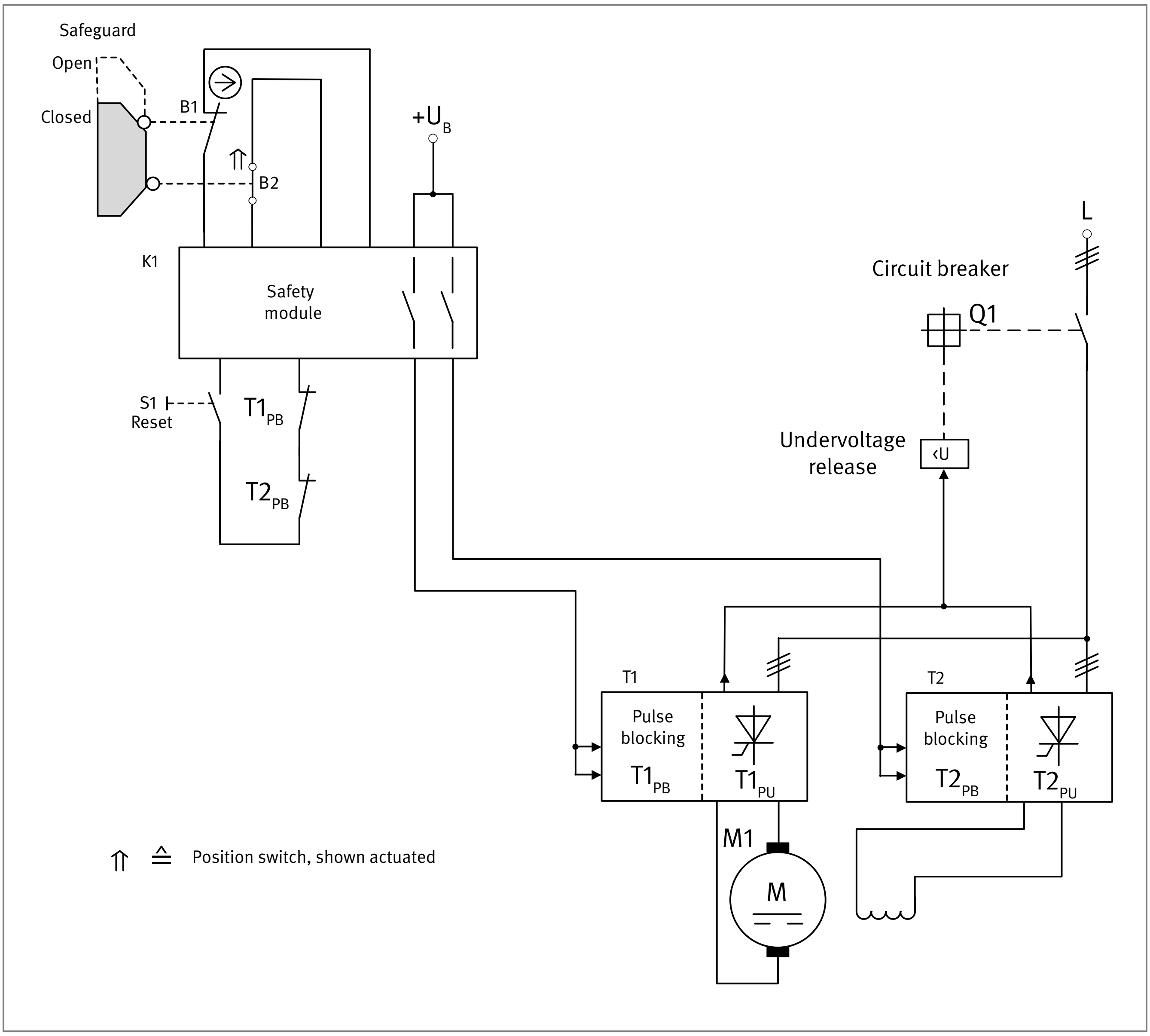
[2] Expert Committee Information Sheet 005. Gravity-loaded axes – vertical axes. 9/2012 edition. Published by: Fachbereich Holz und Metall der Deutschen Gesetzlichen Unfallversicherung, Mainz, Germany. https://www.bghm.de/fileadmin/user_upload/Arbeitsschuetzer/Praxishilfen/Fachbereichs-Informationsblaetter/005_FBHM-MAF_##Vertikalachsen.pdf

[3] IEC 60085:2007: Electrical insulation – Thermal evaluation and designation

[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 e. V., Berlin, Germany 2012. www.dguv.de, Webcode: e109249

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

Figure A.30:
Conceptual schematic diagram of the power drive control



Safety function

- SF 1: Opening of the movable safeguard leads to STO of the DC drive.

Functional description

- The hazardous zone is safeguarded by a movable guard. Opening of the guard is detected by the position switches B1 and B2 and interpreted in a safety module K1. The respective pulse blocking inputs of the DC-DC converters T1 and T2 for the armature current (T1) and excitation field (T2) are de-energized in a two-channel architecture via the enabling paths of the safety module K1. This prevents generation of a torque in the DC motor M1.

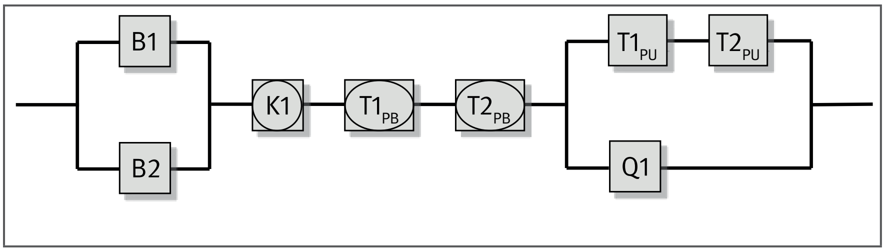


Figure A.31:
Safety-related block diagram for Example 15

- The DC drive, which is supplied with three-phase current, is controlled functionally by a PLC. The PLC itself is not involved in the safety function, and is not shown in Figure A.30. The conceptual schematic diagram (Figure A.30) is limited to the safety-related control, which takes priority over the functional control.

- Each of the DC-DC converters (DC power converters) T1 and T2 comprises a control unit with redundant pulse blocking $T1_{PB}$ and $T2_{PB}$ and a single-channel power unit $T1_{PU}$ and $T2_{PU}$.

- Faults in the position switches B1 and B2 are detected by the safety module K1.

- Each of the DC-DC converters T1 and T2 is equipped internally with a pulse blocking monitoring function (readback contacts $T1_{PB}$ and $T2_{PB}$). In the event of a fault, these contacts prevent the drive from restarting, since they are integrated into the return circuit of the safety module K1.

- Faults in the power units of the DC-DC converters T1 and T2 are detected by internal diagnostics functions, in which case fault signals $T1_{PU}$ and $T2_{PU}$ respectively are output. These fault signals de-energize the circuit breaker Q1 on the three-phase side via an undervoltage release. Q1 in turn disconnects the DC motor from the mains supply. The circuit breaker Q1 is not de-energized with each demand upon the safety function, but only in the event of faults in the power units of the DC-DC converters T1 or T2.

  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 unit of the armature converter result in only the field converter being reliably de-energized when the safeguard is opened, the extreme attenuation of the excitation field can cause the DC motor to turn when unwanted armature current is flowing. In order to prevent this, the circuit breaker for the mains supply is also de-energized in the event of faults in the power unit of a converter. Consequently, the power unit of the DC-DC converter must also be included in the safety analysis of the STO.

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

Design features

- Basic and well-tried safety principles and the requirements for Category B are observed. Protective circuits (such as contact protection, earthing of the control circuit), as described in the first sections of Chapter 8 of IFA Report 2/2017e, are present.

- Cross-circuits and short-circuits in electrical supply lines must be considered in accordance with 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. Actuators 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 ISO 13849-2, Table D.3 with direct opening contacts in accordance with IEC 60947-5-1, Annex K.

- The safety module K1 satisfies the requirements for Category 4 and PL e.

- The DC-DC converters T1 and T2 are products with integrated pulse blocking. The requirements for Category 3 and PL d are satisfied for the pulse blocking. The power units of the DC-DC converters T1 and T2 must be considered separately.

- The circuit breaker Q1 is a well-tried component in accordance with ISO 13849-2, Table D.3. Q1 (including the undervoltage release) must be tested regularly by means of a manual test function that is to be implemented. Such a test can be performed for example during the proof tests.

Calculation of the probability of failure

- The position switch B1 has a B_{10D} of 20,000,000 operation cycles [S]. 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 52,083 years.

- A B_{10D} value of 1,000,000 operation cycles [M] is stated for the 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 safety module K1 satisfies the requirements for Category 4 and PL e. The PFH_D is $2.3 \cdot 10^{-9}$ per hour [M].

- The control unit of the DC-DC converters with pulse blocking $T1_{PB}$ and $T2_{PB}$ can be regarded as an encapsulated subsystem. It satisfies the requirements for Category 3 and PL d. The PFH_D of each control unit is $3.2 \cdot 10^{-7}$ per hour [M].

- The power unit of the DC-DC converters $T1_{PU}$ and $T2_{PU}$ is implemented in a single-channel architecture; each has an $MTTF_D$ of 300 years [M].

- A B_{10D} of 5,000 operation cycles [M] is stated for the circuit breaker Q1. At an n_{op} of 100 cycles per year, the $MTTF_D$ is 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 unit in the DC-DC converters $T1_{PU}$ and $T2_{PU}$ 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 $T1_{PU}$ or $T2_{PU}$. Owing to the brevity of the fault response time, no hazard arises as a result. Loss of the safety function between the tests is not possible. Single-fault tolerance in this subsystem is thus assured, and the requirements for Category 3 in this respect are satisfied.

- Owing to the manual tests performed during the proof tests, 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-DC converters $T1_{PU}/T2_{PU}$ 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 SF 1 is as follows:

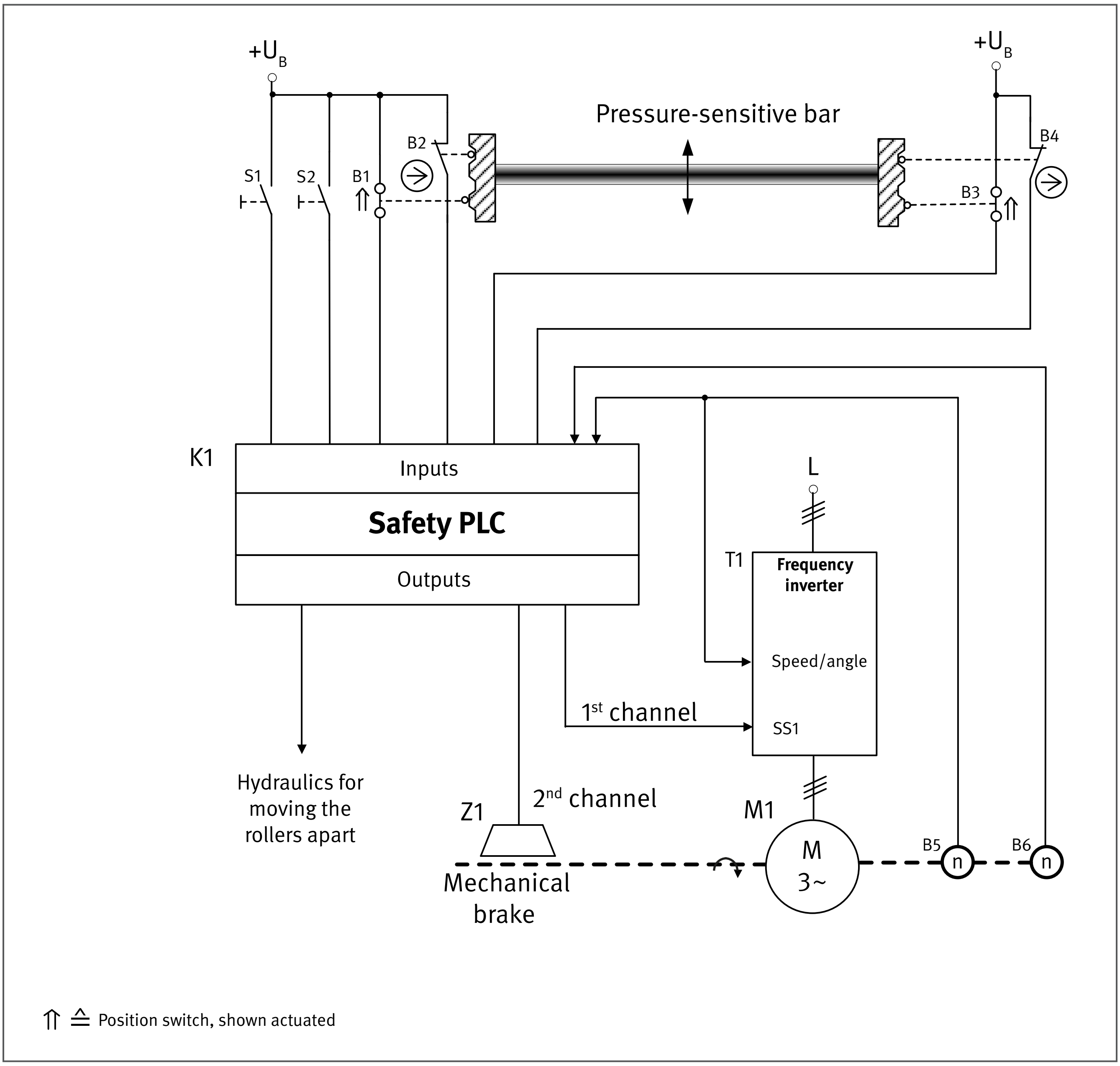
  The subsystem B1/B2 satisfies Category 3 with a high $MTTF_D$ per channel (100 years) and a high DC_{avg} (99%). This yields an average probability of dangerous failure PFH_D of $2.5 \cdot 10^{-8}$ per hour. This satisfies PL e.

  The subsystem $T1_{PU}/T2_{PU}/Q1$ satisfies Category 3 with a high $MTTF_D$ per channel (100 years) and medium DC_{avg} (97%). This yields an average probability of dangerous failure PFH_D of $2.9 \cdot 10^{-8}$ per hour. This satisfies PL e.

  For SF 1, "opening of the movable guard leads to STO of the DC drive", the combination of the subsystems yields an average probability of dangerous failure PFH_D of $6.9 \cdot 10^{-7}$ per hour. This satisfies PL d.

Example 16: Safety-related stop function on two-roll mills for the processing of rubber and plastics – PL d

Figure A.32:
Safety-related stop function of the roller drive following actuation of a safeguard



Safety function

- SF 1: Safe stop following actuation of the safeguard (pressure-sensitive bar) with a maximum braking angle of 60°

Functional description

- The frequency inverter drive T1 of the rolls is controlled by the safety PLC K1. The safety PLC K1 sets the speed setpoint value, controls the start/stop function of the frequency inverter T1, and is responsible for actuating the mechanical brake Z1.

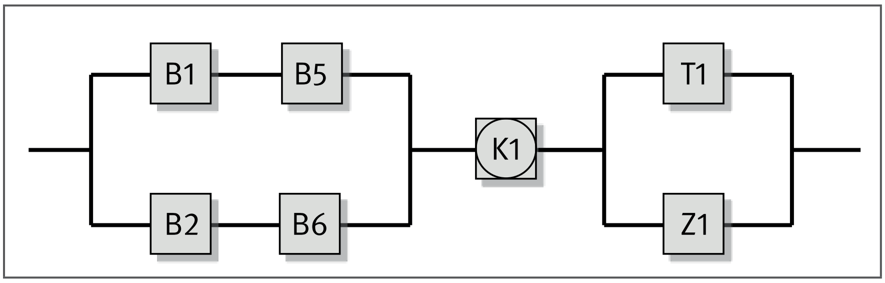


Figure A.33
Safety-related block diagram for Example 16

- When the pressure-sensitive bar is actuated, the safety PLC K1 activates a fast stop in the frequency inverter T1. On new two-roll mills to EN 1417:2014, the command to reverse and separate the rolls must be issued automatically. The rolls are separated by hydraulic apparatus by means of the switch S1.

  Note:

  The step mode for reversing of the rolls, or operation of the rolls at reduced speed for a limited period of time, must be retrofitted to legacy machines.

- The hazardous zones on the roll intake are safeguarded in this example by a pressure-sensitive bar that extends over the entire length of the rolls. Two position switches B1/B2 and B3/B4 comprising break/make contact combinations are fitted at the ends of the pressure sensitive bar, and detect actuation of the bar. Faults in the position switches are detected by plausibility check in the safety PLC K1.

- When released, the pressure sensitive bar returns to its initial position and the contact elements B1/B2 and B3/B4 close again. In order to prevent the machine from starting up again automatically, a manual reset device S2 for the safeguard must be provided.

- The roll drive is braked via the frequency inverter T1, normally in four-quadrant operation. The mechanical brake engages after a rotation of 30° or once standstill has been reached. Exceeding of the permissible overrun is detected in the safety PLC K1 with the aid of the rotary encoders B5 and B6. In addition, the overrun must not exceed 60° in the event of a fault in the frequency inverter T1.

  Note:

  The drive and brake system is not an electronic braking system (EBS), which serves to reduce the response time of a mechanical brake and which works on the open-circuit current principle. Such electronic brakes are not permissible in accordance with EN 1417:2014.

- In order to assure the safety-related stop function of the roll drive even in the event of a mains voltage breakdown, the frequency inverter T1 is capable of using the energy from the intermediate circuit to bring the drive to a standstill in a controlled manner. In the present example, the safety PLC K1 is also supplied with a control voltage generated from the intermediate circuit of the frequency inverter T1. This enables the safety PLC K1 temporarily to perform the control functions required for safety.

  Should the mains power fail, the braking energy cannot be fed from the intermediate circuit back into the mains. In this case, the energy can for example be converted into heat by means of a braking resistor.

- The safety function is checked automatically by the control system before each shift (eight hours). The mechanical brake Z1 is also tested statically for slip at 1.3 times load and with the brake engaged before each shift (eight hours). In addition, a dynamic brake test is performed for example once a month at reduced roll speed.

  The manufacturer‘s information must be observed with regard to the dynamic brake test.

Design features

- Basic and well-tried safety principles and the requirements for Category B to ISO 13849-1 are observed. Protective circuits (such as contact protection) and overdimensioning are implemented.
- Cross-circuits and short-circuits in electrical supply lines must be considered in accordance with 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 mechanical brake Z1 is a spring-operated brake (closed-circuit current principle). The following well-tried safety principles were applied:

  a) Mechanical components
  – Well-tried springs
  – Securing of threaded connections of non-movable constructional elements
  – Positive-locking connections or equivalent for constructional elements used in frictional connections
  – Demonstration of suitability of the brake linings, for example by several years‘ experience in use

  b) Electrical components
  – Insulation coordination to overvoltage category III
  – Overdimensioning of rectifiers (e.g. operational current 0.5 times the rated current of the rectifier)
- The braking torque of the mechanical brake Z1 is greater over the entire speed range than the drive torque of the motor.
- The actuating mechanisms of the electromechanical position switches B1 to B4 of the pressure sensitive bar must be designed and fitted as specified. Actuators and position switches must be secured against displacement.
- Only rigid mechanical components (not spring elements) may be used.
- The position switches B2 and B4 are well-tried components to ISO 13849-2, Table D.3 with direct opening contact in accordance with IEC 60947-5-1, Annex K.
- The safety PLC K1 satisfies the requirements for Category 4, PL e and SIL 3 [M].
- The frequency inverter T1 is a standard inverter without integrated safety functions. It is suitable for four-quadrant operation with power flow back into the grid. The control voltage is generated from the inverter‘s own intermediate circuit and can also be used to supply external circuits.
- Standard incremental encoders are used for detection of the braking angle (B5, B6). 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.

Calculation of the probability of failure

- Of the four position switches on the safeguard (pressure sensitive bar), only two (B1 and B2) are considered a redundant system. This is due to the fact that actuation at one end is sufficient to trigger the safety function.
- The position switch with direct opening action B2 has a B_{10D} of 20,000,000 operation cycles [S]. At 365 working days, 24 working hours per day and 6 actuation cycles per day (two per shift), the $MTTF_D$ is 91,324 years.
- For the position switch B1 (make contact), the B_{10D} is 100,000 operation cycles [M]. At 365 working days, 24 working hours per day and 6 actuation cycles per day (two per shift), the $MTTF_D$ is 456 years.
- The rotary encoders B5 and B6 each have an $MTTF_D$ of 190 years [M].

- The safety PLC K1 satisfies the requirements for Category 4, PL e and SIL 3. The PFH_D is $3.2 \cdot 10^{-8}$ per hour [M].

- The frequency inverter T1 satisfies the requirements for Category B. The $MTTF_D$ is 20 years [M].

- The mechanical brake Z1 exhibits a B_{10D} of 2,000,000 operation cycles [M] for static braking (holding brake). At 365 working days, 24 working hours per day and a cycle time of 10 minutes, the result is an n_{op} of 52,560 cycles per year and an $MTTF_D$ of 380 years.
  Note: the brake Z1 employed here is dimensioned for 2,000 dynamic braking operations.

- The *DC* for the position switches B1 and B2 is 99%, owing to the plausibility check by the safety PLC K1.

- The *DC* for the rotary encoders B5 and B6 is 99%, owing to cross monitoring by the safety PLC K1.

- A *DC* of 90% is substituted for the frequency inverter T1. The frequency inverter is tested for proper execution of the safety sub-function at each actuation of the safeguard and additionally every eight hours.

- A *DC* of 60% is assumed for the spring operated brake Z1 in this example owing to static and dynamic testing. A static test and a dynamic test are performed automatically on the spring operated brake every eight hours and once a month respectively by the control system.

- Adequate measures against common cause failure are taken for the subsystem of the position switches and rotary encoders B1/B2/B5/B6 (70 points): separation (15), use of well-tried 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 the frequency inverter T1 and mechanical brake Z1 (70 points): separation (15), diversity (20), protection against environmental conditions (25 + 10).

- Evaluation of the SF 1 safety function yields the following result: the subsystem comprising B1/B2/B5/B6 satisfies Category 3 with a high $MTTF_D$ (100 years) and a high DC_{avg} (99%). This yields an average probability of dangerous failure PFH_D of $2.5 \cdot 10^{-8}$ per hour.

  The subsystem T1/Z1 satisfies Category 3 with a high $MTTF_D$ (68.9 years) and a low DC_{avg} (88%). This yields an average probability of dangerous failure PFH_D of $8.1 \cdot 10^{-8}$ per hour.

  The combination of the subsystems of the position switches B1/B2/G1/G2, safety PLC K1, and frequency inverter/mechanical brake T1/Z1 yields an average probability of dangerous failure PFH_D of $1.4 \cdot 10^{-7}$ per hour. This satisfies PL d.

Further literature:

EN 1417: Plastics and rubber machines — Two roll mills — Safety requirements (2014).

Annex B:
Expert Committee information sheet

The following information sheet issued by the DGUV Expert Committee Woodworking and Metalworking can be downloaded from the DGUV website:

Number and title of the information sheet		Web URL
005	Gravity-loaded axes – vertical axes	https://www.dguv.de/medien/fb-holzundmetall/publikationen-dokumente/infoblaetter/infobl_englisch/005_vertical-axes.pdf

DGUV
Fachbereich Holz und Metall
Berufsgenossenschaft
Holz und Metall

No. 005
Edition 09/2012

Division Information Sheet

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.

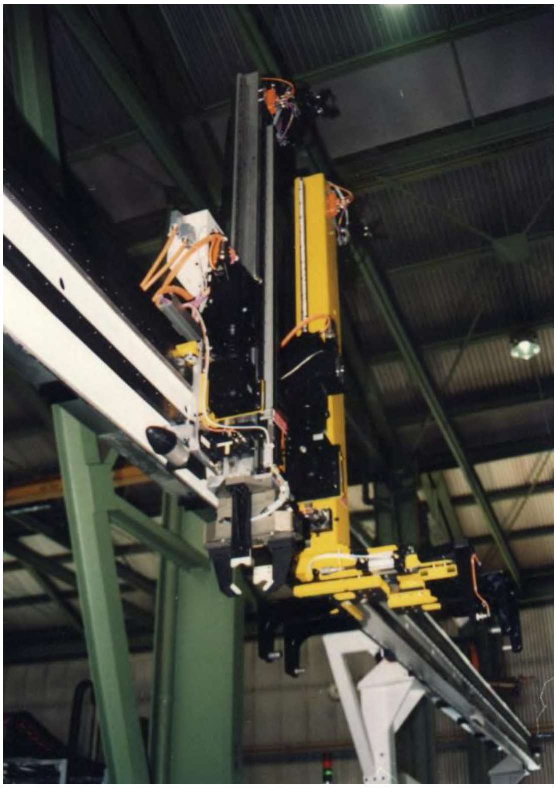


Figure 1: Vertical axes

Table of Contents

1 Motor brakes

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 Risik 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 inacceptable 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 Arbeitschutzes (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-Römheld-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

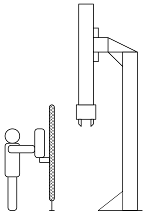
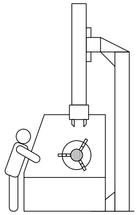
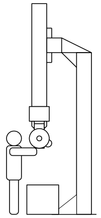
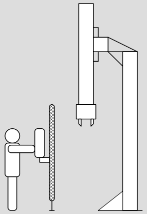
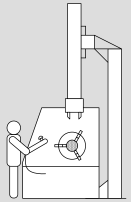
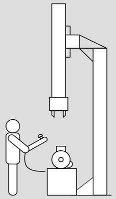
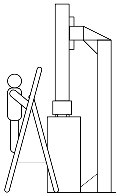
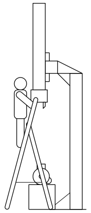
Mode of operation	Hazardous situation/ Intended use	Safety measures Technical	 Organizational
Automatic-Manual intervention A1	 During manual intervention, the vertical axis is located in a safe position for the operator (access-protected area).	- Guards have to be provided with guard lockings. - In case of access, unintended start of the vertical axis shall be safely prevented.	- 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	 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.	- 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 prevented [1)].	- 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	 The vertical axis is located within the hazardous area. Staying under the vertical axis cannot be prevented (e.g. intended feeding or assembling activities).	- 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 prevented [1)].	- 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	 The vertical axis is located in a safe position for the operator during set-up (access-protected area).	- Guards have to be provided with guard lockings - In case of access, unintended start of the vertical axis shall be safely prevented).	- 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/		Safety measures	
	Intended use		Technical	Organizational
E2		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.	- 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).	- 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		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.	- 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).	- 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 W1		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.	- 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	- 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		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.	- 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.	- 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: - 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	Suitable for mode of operation A2	Suitable for mode of operation A3	Suitable for mode of operation E1	Suitable for mode of operation E2	Suitable for mode of operation E3	Suitable for mode of operation W1	Suitable for mode of operation W2
		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.	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.	The vertical axis is located within the hazardous area. Staying under the vertical axis cannot be avoided.	The vertical axis is not operated in 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.	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.	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.	Maintenance, cleaning and repair works are carried out at the vertical axis. Safe support of the vertical axis is feasible.	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.

Annex C:
List of abbreviations

Table C.1 contains the abbreviations used in this report; Table 1 (see Page 12) contains the abbreviations and further information on the safety sub-functions in IEC 61800-5-2.

Tabelle C.1:
Abbreviations used in this report

Abbreviation	Bezeichnung
[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 ISO 138491
ASIC	Application-specific integrated circuit
B_{10D}	Nominal life: the average number of switching operations/cycles at which 10% of the units under analysis have failed
BIA	Berufsgenossenschaftliches Institut für Arbeitssicherheit (BG Institute for Occupational Safety, now: IFA)
CCF	Common cause failure
DC	Diagnostic coverage
DC_{avg}	Average dignostic coverage
DGUV	Deutsche Gesetzliche Unfallversicherung (German Social Accident Insurance)
DKE	Deutsche Kommission Elektrotechnik Elektronik Informationstechnik im DIN und VDE (German Commission for Electrical, Electronic and Information Technologies of DIN and VDE)
EMC	Electromagnetic compatibility
FI	Frequency inverter
FMEA	Failure mode and effect analysis
FPGA	Field programmable gate array
IC	Integrated circuit
IFA	Institut für Arbeitsschutz der Deutschen Gesetzlichen Unfallversicherung (Institute for Occupational Safety and Health of the German Social Accident Insurance)
IGBT	Insulated-gate bipolar transistor
$MTTF_D$	Mean time to dangerous failure
NC	Numeric control
n_{op}	Mean number of annual operations
PDS	Power Drive Systems
PDS(SR)	Power Drive Systems Safety Related
PFH_D	Average probability of 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	Sicherheit von Steuerungen an Maschinen (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