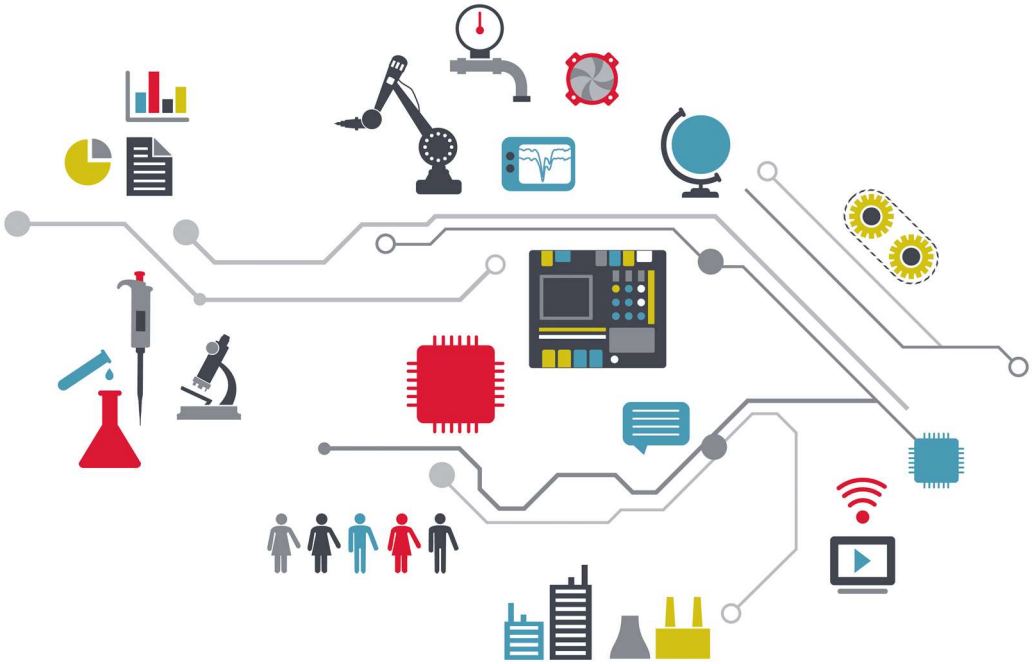
GAMBICA

Variable Speed Drives
And the Functional Safety
Of Machinery

A GAMBICA Technical Guide



Edition 2.2
August 2019

Variable Speed Drives and Functional Safety of Machinery

Summary

Some manufacturers of variable speed electrical Power Drive Systems and drive modules offer products with safety-related functionality. This guide sets out the functional safety considerations for the selection and application of these products to machinery. It does not set out requirements for the manufacture of these products.

It is the responsibility of the machine builder to ensure the safety of their machine. The control system of a machine can play a part in its safety performance (i.e. functional safety), and must be accounted for in the machine risk assessment. Any modification to the control system, such as the addition of a variable speed drive, requires a reappraisal of the risk assessment.

As the installation of a drive into a machine can represent a considerable modification to its control system, it has the potential to affect the safety performance of the machine. The implications of such a modification must therefore be carefully considered. Selection of a drive with appropriate safety functions is critical, as is the subsequent integration of that drive with other components into the control system of the machine.

The European Union Machinery Directive provides a legal framework within which the machine manufacturer can ensure that they fulfil their responsibility for safety. The range of European Harmonised Standards applicable under this directive facilitates the safe design of machinery, including the safe application of variable speed drives with safety functions. The guide outlines how the relevant international and European standards can be applied.

A drive with safety functionality can be used to implement specific safety functions. A drive with no safety functionality should not be relied upon to implement any safety functions, without the use of supplementary safety-related control systems

The use of a safety-related drive in a machine will not necessarily result in a safe machine.

Variable Speed Drives and Functional Safety of Machinery

Foreword

This document has been prepared by the GAMBICA Variable Speed Drives Technical Working Group to provide guidance on functional safety considerations when selecting and integrating a Power Drive System into the control system of a machine. Functional safety is that aspect of safety that relies upon the correct functioning of a control system. In machinery applications, it is typically associated with preventing injury arising out of contact with moving mechanical parts. Functional safety is distinct from other aspects of safety, such as the use of fixed guards to physically prevent access to moving mechanical parts or to prevent exposure to the live parts of electrical circuits.

In identifying factors to consider when selecting a Power Drive System and integrating it into the control system of a machine, this guide refers to various functional safety standards that are relevant to Power Drive Systems and the safety-related control systems into which they can be integrated. It also explains some of the common terminology that these standards use.

Guidance on installing Power Drive Systems from the perspective of mechanical/electrical safety and avoidance of EMC problems is provided by the GAMBICA/REMA[1] Installation Guidelines for Power Drive Systems, whilst standards that address more general safety considerations of drives are referred to in the GAMBICA CE Marking Guide. The guidance in this GAMBICA guide complements these other publications.

Although this guidance represents the views of the GAMBICA Variable Speed Drives Technical Working Group, it has no legal force. To ensure that machinery complies with legal requirements, readers are therefore advised to consult relevant national legislation and associated harmonised European standards.

Note on Version 2

Most references to standard EN 954-1 have been removed since this standard is replaced by EN ISO 13849-1 and should not be used for new designs. The guidance given is confirmed as current in September 2018.

Scope

This guide is applicable to safety-related control systems of machinery that incorporate an electrical Power Drive System.

It considers the use of Power Drive Systems with various functional safety capabilities. It distinguishes between Power Drive Systems that have no inherent functional safety capability, and those that are capable of the partial or complete implementation of specific safety functions of machinery. It highlights issues that persons with responsibility for one or more of the following tasks should consider:

---

[1] Now part of GAMBICA

- Selection of a Power Drive System for use in the safety-related control system of a machine, or

- Specification, design, development, integration, commissioning and validation of a safety-related control system of a machine that incorporates a Power Drive System.

The design of a Power Drive System itself is outside the scope of this document.

CONTENTS

1 INTRODUCTION

1.1 General

The use of variable speed drives in machinery continues to increase in accordance with the demand for improved automation and energy efficiency. The extent of applications is diverse, ranging from small self-contained machine tools through to large-scale manufacturing plant. One consequence of this has been the development of drives with enhanced functionality, which are capable of performing complex automation tasks that would have previously been assigned to supplementary systems incorporating Programmable Logic Controllers (PLC) for example. A more recent variant of this trend is the development of drives with in-built safety-related systems that provide some functional safety capability.

The acronym 'PDS' for an adjustable speed electrical Power Drive System has been adopted by the IEC 61800 series of International Standards for drives, with harmonised versions of these published as the EN 61800 series. IEC 61800-5-2[2] introduced the concept of a PDS (SR), which is essentially a type of PDS with some functional safety capability that can support the implementation of particular safety functions.

As illustrated in Fig.1, a PDS includes a Basic Drive Module (BDM) plus the necessary motor(s) and feedback sensor(s). The BDM covers those elements of a PDS that are generally referred to as a drive. In the case of a PDS(SR), relevant parts of it are capable of implementing particular safety functions.

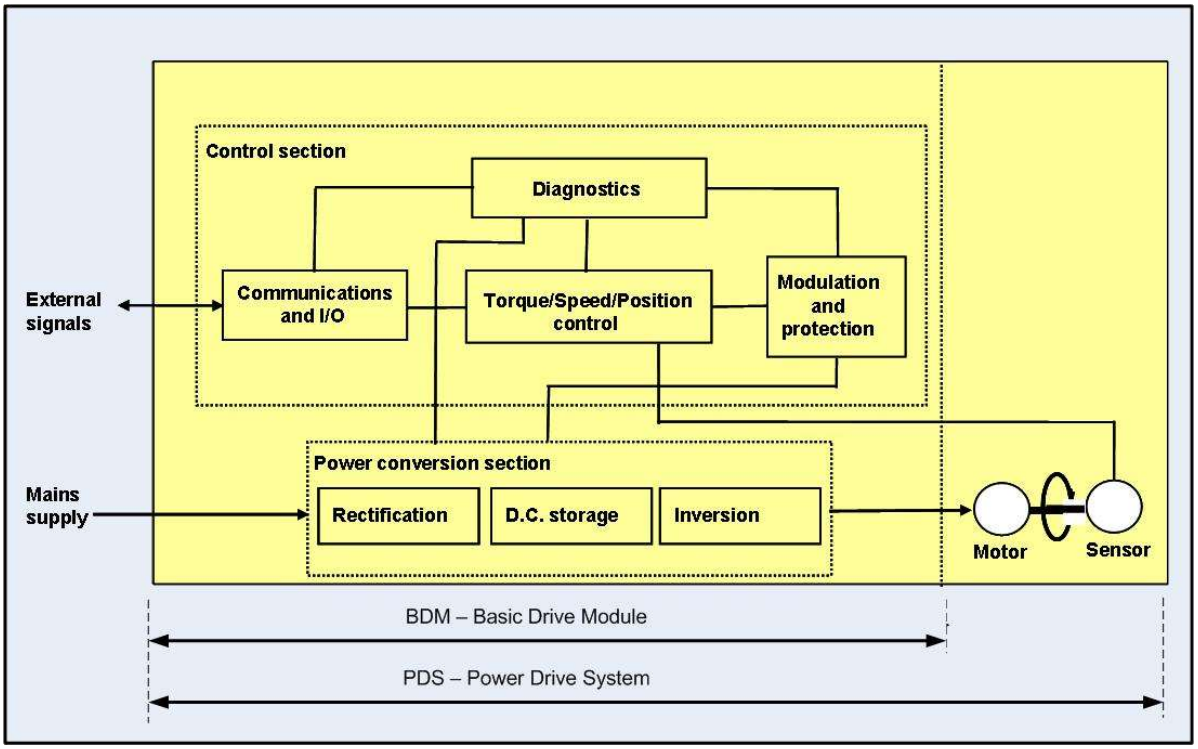


Figure 1 - General architecture of an a.c. Power Drive System

Most modern motion control systems utilise a.c. motors and drives, reflecting the lower maintenance requirements of a.c. motors compared to their d.c. counterparts, and also the improved affordability of a.c. drives. Synchronous a.c. motors, such as brushless servomotors, are typically used in motion control applications requiring highly accurate position control, whereas asynchronous (e.g. induction) motors can be adequate for less precise speed control applications. The basic architecture of an a.c. drive in Figure 1 is, however, applicable to both classifications of a.c. motor.

[2] EN 61800-5-2 Adjustable speed electrical power drive systems – Part 5-2: Safety requirements - Functional

A control system will typically consist of input devices, some logic solving functionality and output devices. Input devices can be sensors or switches that provide information on the status of particular variables, whilst the logic solver processes this information and initiates any appropriate response of the output device.

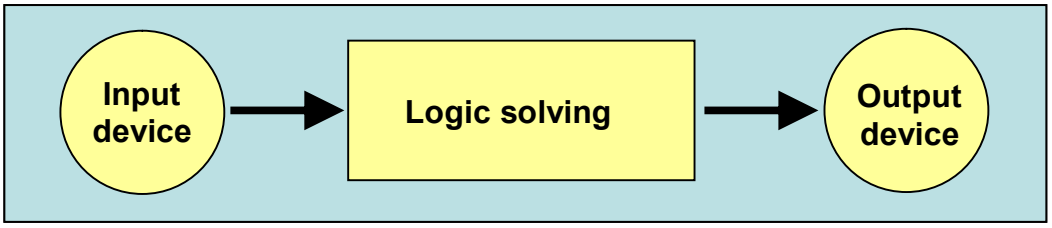


Figure 2 – Basic elements of a control system

This basic description is equally applicable to control systems that implement safety functions, and to those that implement process functions that are not safety-related.

It was previously regarded as essential for safety functions to be performed by simple low complexity control systems, operating independently of the more complex control systems that perform process functions. However, just as microprocessor-based systems are now widely used to perform complex control tasks, the demand for increasingly complex safety functions often requires implementations using electronic technology. The use of complex technology in safety-related systems requires a standardised approach, which has led to the development of functional safety standards such as IEC 61508 (see Annex A) and its derivatives.

2 DRIVES AND MACHINERY SAFETY

2.1 General

As the use of a drive in a machine can impact upon its safety performance, it is necessary to firstly consider the overall requirements for machinery safety.

Machinery that is supplied[3] within the European Economic Area (EEA) must comply with the Machinery Directive[4] and other applicable European Directives. This can be achieved by complying with relevant harmonised European standards listed in the Official Journal of the European Union (OJEU)[5], because these grant a presumption of conformity with particular requirements of a European Directive.

In accordance with the breadth of their scope, harmonised European standards for the Machinery Directive are categorised as type-A, type-B and type-C standards.

The type-A standard is EN ISO 12100[6]. It is directly applicable to all machines, and also sets out a strategy for developers of more specific type-B and type-C machinery safety standards.

[3] The Machinery Directive applies to 'manufacturers' of machinery, but it can also apply to an importer of machinery into the EEA or to a user who substantially modifies their own machinery.

[4] A revised version of the Machinery Directive, 2006/42/EC, superseded 98/37/EC on 29/12/09. In the UK this is implemented as the Supply of Machinery (Safety) Regulations 2008.

[5] A record of current harmonised European standards applicable to the Machinery Directive can be found at: https://ec.europa.eu/growth/single-market/european-standards/harmonised-standards/machinery_en

[6] EN ISO 12100 - Safety of machinery – General principles for design – Risk assessment and risk reduction

The various type-B standards relate to particular safety aspects of machinery (type-B1), or to particular protective devices (type-B2). For example, the type-B1 standards EN 62061[7] and EN ISO 13849-1[8] provide a methodology for achieving an adequate level of functional safety in a machine's safety-related control system, whilst relevant parts of EN 60204[9] address safety requirements for electrical equipment of machines. As an example of a type-B2 standard, EN 1088[10] applies to protective devices that provide an interlocking function, such as interlock switches for movable guards.

Type-C standards provide safety requirements for particular types of machinery. They take account of type-A and type-B standards, referring extensively to their requirements and adapting these to the specific machinery.

After machinery has been taken into service, the user bears responsibility for its ongoing safety. This will include a requirement to comply with the Provision and Use of Work Equipment Regulations 1998 (PUWER), which are the UK implementation of the Use of Work Equipment Directive. Amongst the requirements of this legislation is the ongoing need for safety-related control systems to achieve a sufficient level of functional safety.

2.2 Risk Assessment

It is a requirement that machinery is the subject of a risk assessment during its initial design, and also when any modification or change of use is considered. Any proposal to modify the control system of a machine, by installing a new drive for example, should therefore be risk assessed.

The harmonised European standard EN ISO 12100 provides a methodology for the risk assessment of machinery. With reference to Figure 3, the objective of risk assessment is to determine whether the actual risk exceeds a tolerable level. If this is found to be the case, it will be necessary to implement protective measures to reduce the actual risk, and to then reassess this risk. This iterative process should continue until the risk has been reduced to a level that is at or below the tolerable level.

---

7 EN 62061 - Safety of machinery – Functional safety of safety-related electrical, electronic and programmable electronic control systems.

8 EN ISO 13849-1 - Safety of machinery – Safety-related parts of control systems – Part 1: General principles for design

9 EN 60204 - Safety of machinery – Electrical equipment of machines

10 EN 1088 - Safety of machinery – Interlocking devices associated with guards – Principles for design and selection

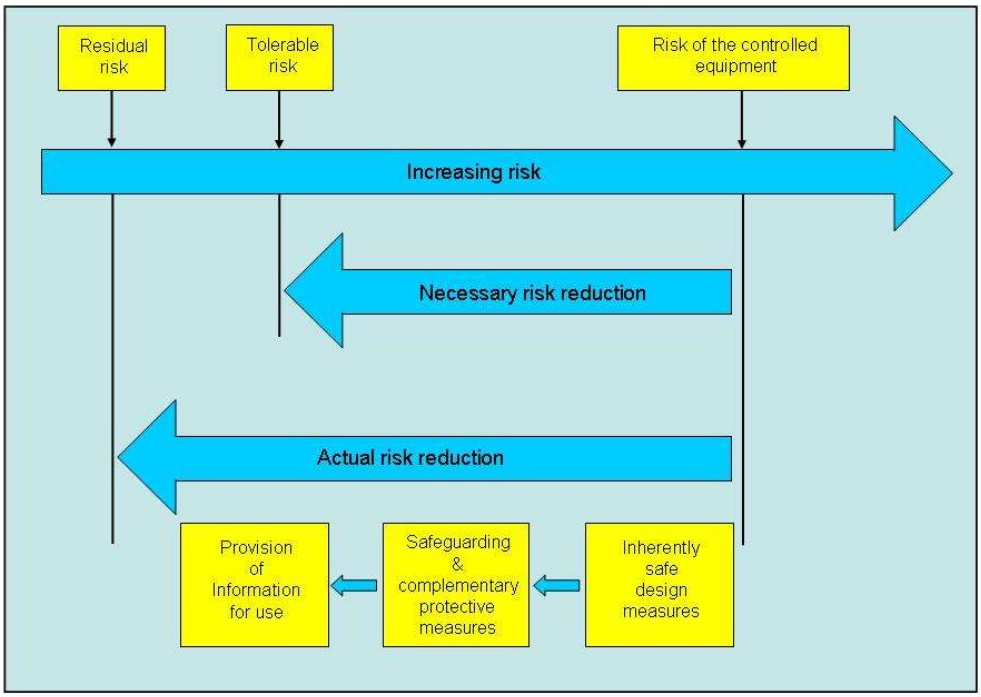


Figure 3 - The concept of risk reduction

A risk assessment of a machine must consider all aspects of its use, including normal operation, maintenance, and foreseeable misuse. The risk associated with a particular hazard can be considered as a combination of the severity of the harm that can occur, and the likelihood of that harm occurring.

If a particular hazard presents an unacceptable risk, then where practicable, the hazard should be eliminated by implementing appropriate design changes. For example, it may be possible to re-dimension or reposition machinery parts so that they no longer present a trapping hazard.

If a hazard cannot be eliminated using this inherently safe design approach, then the associated risk can be reduced by applying safeguards (e.g. fixed guards, interlocking guards, protective devices) and complementary protective measures. Where it is not practicable to use fixed guarding to prevent access to a moving part of a machine - for example, because a particular type of intervention must be performed frequently - then other safeguards such as interlocking guards and/or protective devices are typically used[11].

When a machine supplier has implemented inherently safe design measures and safeguards and complementary measures so far as is practicable, further risk reduction can be achieved by providing the user with relevant information and instructions.

Risk reduction provided by interlocking guards and/or protective devices relies on the correct functioning of a control system, of which the interlocking/protective device will be a part. Similarly, for the complementary protective measure of an emergency stop function, the emergency stop actuator will form part of a control system that must function correctly for the emergency stop function to be performed.

[11] Although it is generally necessary to isolate a machine in order to prevent its unexpected start-up, measures such as interlocking can provide sufficient risk reduction in specific circumstances. See EN ISO 14118 (clauses 4.2 & 6) and EN 60204-1 (clause 5.4).

Control systems that incorporate these interlocking/protective devices or emergency stop devices constitute 'safety-related control systems'[12], because they must function correctly in order for safety to be achieved. An element of the machine's safety is thus provided by functional safety measures, with the relevant control systems considered to implement particular 'safety functions'[13] that contribute towards reducing risk to a tolerable level,

It is essential that a machine's risk assessment is reviewed whenever consideration is given to any modification or upgrade, including changes that affect the control system. Any proposal to incorporate a drive into the control system of a machine, or to replace an existing drive with an alternative type, should therefore prompt a review of the risk assessment. This should identify any new or changed risks that such a modification could introduce.

Installing a drive into a machine can affect the general performance of its control systems, and could introduce new risks such as the potential to exceed the original design speed or for bi-directional motion. Caution must also be exercised to ensure that the drive does not compromise existing safety functions, which could unintentionally become reliant upon functions of the drive that do not have sufficient functional safety capability.

2.3 Risk reduction and functional safety

As an example of functional safety, if an access point on a machine is safeguarded using an interlocking guard, then the interlocking device and other control devices that it interacts with in order to restrict moving parts of the machine will form part of a safety-related control system. The associated safety function could require moving parts to stop, or to operate at a reduced speed, whenever the guard is open.

A safety-related control system of a machine must be designed and configured so that it can:

a) perform all safety functions that are necessary to maintain or achieve the safety of the machine, and

b) perform each of these safety functions with a measure of integrity that is appropriate for the potential consequences of its failure.

A functional description of all of the safety functions, together with a measure of their required integrity, forms the basis of what is generally referred to as a 'Safety Requirements Specification'. The formulation of this is a fundamental requirement of the machinery functional safety standards described in Chapter 3.2 of these guidelines.

2.4 Functional safety considerations for a PDS

2.4.1 Non safety-related drives

For most variable speed drives, the complex electronics and software that provides their functionality will not have been designed, developed, integrated and validated in accordance with an appropriate functional safety standard, such as EN 61800-5-2. Such drives are therefore unsuitable, by themselves, for fully implementing safety functions of machinery.

For example, if a drive output is configured to control an electromechanical brake that constrains a mechanical load, but the parts of the drive that control this output have insufficient integrity for the specific application, then it will be necessary to provide supplementary interlocking measures for brake control.

---

[12] EN ISO 13849-1 defines a safety-related part of a control system (SRP/CS) as part of a control system that responds to safety-related input-signals and generates safety-related output signals, whilst EN 62061 defines a safety-related electrical control system (SRECS) as an electrical control system of a machine whose failure can result in an immediate increase of the risk(s).

[13] EN ISO 13849-1 and EN 62061 both cite the EN 12100 definition of a safety function as a function of a machine whose failure can result in an immediate increase of the risk(s)

In addition, it is possible for the use of a variable-speed drive in a machine to introduce new hazards compared with a fixed-speed direct motor drive. For example the speed might increase abnormally or reverse rotation might occur due to a fault. These possibilities must be considered in the risk assessment.

Although non safety-related drives can be capable of performing an extensive range of motion control functions, such as holding a motor at rest or limiting its position, speed or torque, the lack of verified integrity for such motion control functions means that the drives cannot be regarded as safety-related.

When integrating such a drive into a machine, it is therefore necessary to implement any safety functions independently of it, or across a combination of the drive and a supplementary safety-related control system. This will ensure that any failure within the complex electronics and software of the drive cannot, by itself, lead to an unsafe situation, i.e. the safety functions do not depend solely upon the drive for their correct operation. Figure 4 illustrates the approach to implementing safety functions using a non safety-related drive and supplementary safety-related control systems.

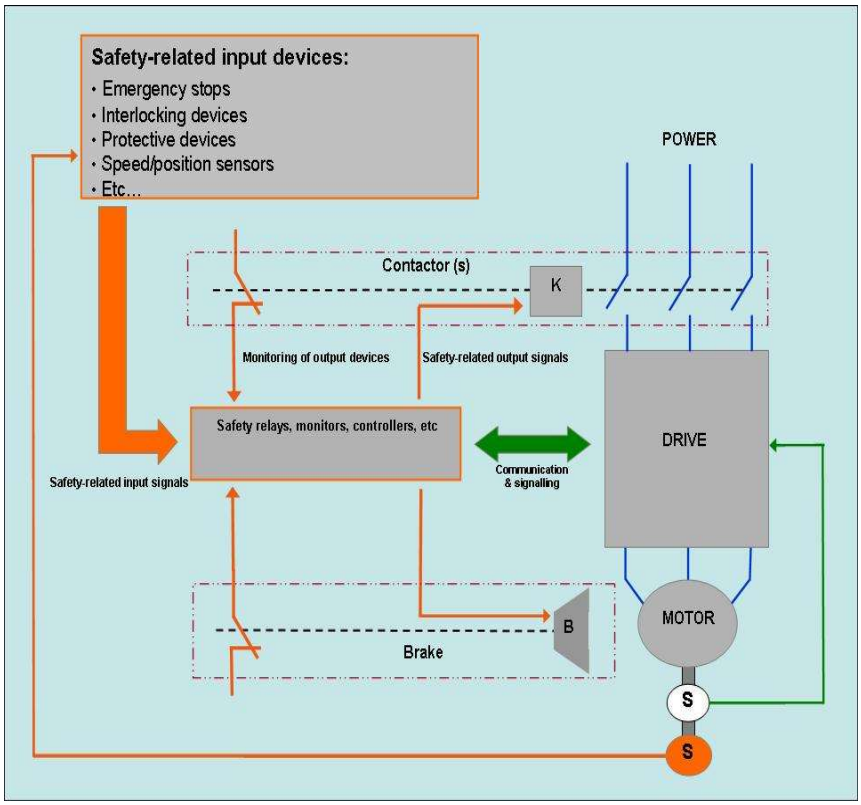


Figure 4 – Example of non safety-related drive supplemented by safety-related control measures

A safety function that is implemented independently of a drive will generally monitor some variable, and then initiate an appropriate reaction if this exceeds a set limit. For example, the position, speed or acceleration of a moving part of the machine, or the status of an emergency-stop actuator, could be monitored by a suitable controller, which initiates a response when the monitored variable violates a set limit, or if the emergency-stop actuator is pressed[14].

The safety-related reaction to a violation of the limit must be specific to the application, but will typically require the safety-related control system to disable moving parts by de-energising terminal devices such as electromechanical contactors, clutches, or brakes. For example, one or more electromechanical

[14] Subject to the requirements of EN 60204-1 and ISO 13850 for emergency stop equipment

contactor(s) could be de-energised in order to prevent moving parts from starting-up unexpectedly from rest [15].

Although safety functions implemented in this way do not depend solely on the drive for their correct operation, it is often necessary for the safety-related control system to interact with the drive. For example, a motor can be stopped very rapidly by commanding the drive to decelerate it to a standstill before it switches off motor power. A safety function that prevents motion can then be initiated, by de-energising an electromechanical contactor(s) which controls motor and/or drive power.

A safety-related control system used in conjunction with a non safety-related drive should be designed, developed, integrated and validated in accordance with relevant harmonised European standards, the most pertinent of which are described in Chapter 3.

Regardless of which standard is used, the resulting safety-related control system must provide the level of risk reduction assigned to it, which it does by performing the necessary safety-function(s) with an appropriate degree of integrity.

2.4.2 Safety-related drives

A PDS(SR) incorporates a 'safety-related drive' that has been designed to be capable of implementing (either completely or partially) one or more safety functions. In some of these drives the functional safety capability is provided by safety modules that supplement the standard version of the drive, whereas in other drives it is an inherent design feature.

The emergence of safety-related drives prompted the development of IEC 61800-5-2 (EN 61800-5-2 in Europe), which is a product-specific implementation of the IEC 61508 basic safety publication. It specifically addresses the functional safety requirements for PDS(SR)s, and is described in more detail in Chapter 4.

The hardware and software that implements safety functions in a safety-related drive will have been produced in accordance with a suitable functional safety standard.

EN 61800-5-2 recognises that the particular functionality and integrity of safety functions can vary between safety-related drives. For example, some products might provide only one safety function, such as the removal of output power in response to a disabling input, whereas others can provide several complex motion control safety functions.

It also recognises that the safety functions provided by a particular safety-related drive can have dissimilar integrity values, although an implementation in common hardware and/or software often results in a uniform value being declared.

Prospective users of PDS(SR)s need to be aware of this variation in the quantity, functionality and integrity of safety functions provided by different products. Appropriate decisions can then be taken when selecting a PDS(SR) for a particular application, so as to ensure that it can adequately perform all of the required safety functions.

As the use of a safety-related drive can lead to simplification or elimination of some supplementary safety-related control systems, it can reduce the requirement for devices such as safety monitors, limit switches, position cams, contactors and relays. In some cases, it can also result in faster response times than when supplementary safety-related control systems are used.

The use of a safety-related drive in a machine will not necessarily result in a safe machine. Having selected a safety-related drive that can perform the required safety functions with a suitable integrity, the overall safety-related control system into which it is incorporated should then be designed, developed, integrated and validated using the methodology within EN 62061 or EN ISO 13849-1, which are described in Chapter 3.2.

---

[15] For considerations regarding positioning of the contactors see Annex B.

Where the configuration of a safety function involves the setting of parameters within a PDS(SR), then measures to ensure the accuracy of these parameters and to restrict their reconfiguration to competent personnel are necessary.

3 FUNCTIONAL SAFETY STANDARDS FOR MACHINERY

3.1 EN 60204-1

Safety of machinery – Electrical equipment of machines – Part 1: General requirements

IEC 60204-1, which CENELEC[16] have adopted within Europe as EN 60204-1, is the generic harmonised European standard for electrical equipment of machines. Its broad scope covers both electrical safety and functional safety, and in respect of the latter it specifies requirements for electrical control devices, circuits, and functions. In particular, it refers to harmonised European Standards EN 62061 and EN ISO 13849-1 (see Chapter 3.2) for the integrity requirements of safety functions and safety-related control systems,

EN 60204-1 introduces the concept of a 'stop category', which classifies stop functions according to whether or not power is removed from the machine actuators, and the timing of this power removal. This concept is relevant to a machine's emergency stop function, and to any safety functions that involve bringing hazardous movements to a stop (for example, when an interlocking guard is opened).

It should be noted that a stop category classification is distinct from an integrity classification assigned to a safety function. In particular, EN ISO 13849-1 'categories' of integrity and EN 60204-1 'stop categories' should not be confused.

Stop category	Function
0	Stopping by immediate removal of power to the machine actuators (i.e. an uncontrolled stop)
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
2	A controlled stop with power left available to the machine actuators

Table 1 - Stop categories according to EN 60204-1 (Clause 9.2.2)

The concept of stop categories can be particularly relevant if a machine incorporates a drive, because drives can perform the controlled deceleration of a motor that is required by stop categories 1 and 2.

EN 60204-1 also stipulates the use of stop category 0 or 1 for the emergency stop function of a machine, so that power is ultimately removed from the machine actuators.

3.2 EN 62061 and EN ISO 13849-1

Regardless of which of these harmonised European standards is applied to the design of a safety-related control system of a machine, their overall methodology is essentially the same.

[16] Comité Européen de Normalisation Electrotechnique (European Committee for Electrotechnical Standardisation)

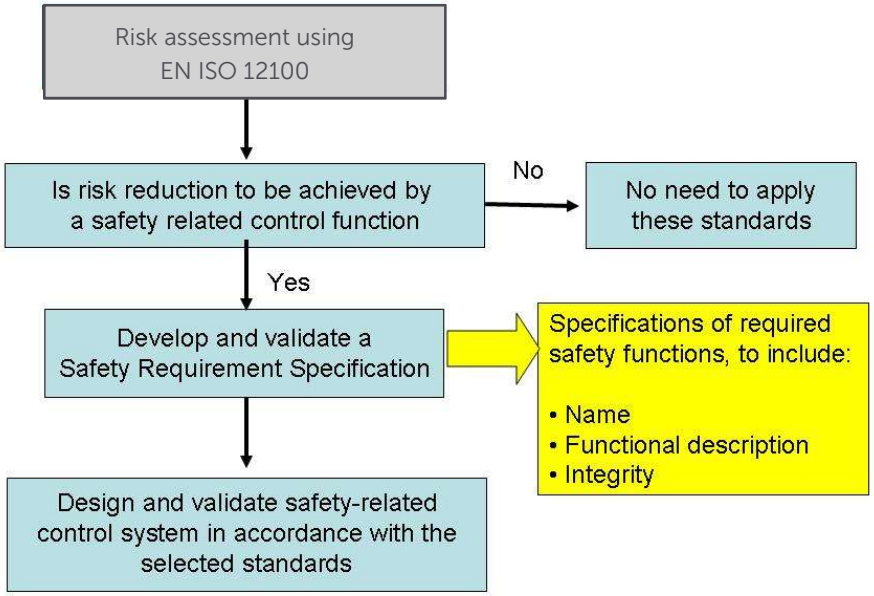


Figure 5 – Application of EN 62061 and EN ISO 13849-1

When it has been determined that a safety-related control system contributes towards the required risk reduction on a machine, application of the selected standard involves specifying the required safety functions and assigning an integrity to each of these based on the amount of risk reduction required. Safety-related control systems that perform the safety functions can then be designed according to the requirements of the selected standard.

Where a safety related drive is to be used for the implementation of any safety functions:

- Select the PDS(SR) with appropriate capabilities in terms of particular safety functions and their integrity.
- Interface the PDS(SR) with other subsystems and consider the validity of signals and commands from these.
- Design, develop, integrate and validate the overall safety-related control system, including the hardware, software, parameterisation, etc.

3.2.1 EN 62061

Safety of machinery – Functional safety of safety-related electrical, electronic, and programmable electronic control systems

IEC 62061 is the machinery sector implementation of IEC 61508 (see Annex A), and in Europe it has been adopted by CENELEC as EN 62061. It is applicable to safety-related control systems consisting of electrical, electronic, or programmable electronic (E/E/PE) technology of any complexity, but not to other technologies such as mechanical, hydraulic, or pneumatic. In particular, the

emergence of machinery safety devices incorporating complex E/E/PE technology prompted its development as a means of integrating such devices into safety-related control systems.

EN 62061 specifies a safety function's integrity in terms of the quantitative SIL17 (Safety Integrity Level) measures of integrity introduced by IEC 61508. However, it disregards SIL 4, the highest level of integrity, because the risk reduction associated with this is beyond typical machinery applications. It also restricts the expression of ranges of probability of dangerous failure for each SIL to 'per hour' (PFHD) values, because only the continuous and high demand modes of operation are considered relevant to machinery applications. Table 2 shows the ranges of probability of dangerous failure per hour corresponding to each relevant SIL.

EN 62061 Safety Integrity Levels: target failure values	
SIL	Probability of a dangerous failure per hour (PFH_D)
3	$\geq 10^{-8}$ to $<10^{-7}$
2	$\geq 10^{-7}$ to $<10^{-6}$
1	$\geq 10^{-6}$ to $<10^{-5}$

Table 2 - EN 62061 SILs

EN 62061 provides a risk matrix method for assigning a SIL to a safety function on the basis of required risk reduction. Once this has been determined, a safety-related control system can be developed in accordance with the standard's requirements for that SIL. The term Safety-Related Control Function (SRCF)[18] to used to denote a safety function that is implemented by a Safety-Related 'Electrical' Control System (SRECS)[19].

SILs are a comprehensive measure of integrity, taking account of factors such as component reliability, system structure, fault detection and the control and avoidance of systematic failures[20]. The range from SIL 1 (lowest) up to SIL 3 (highest) can therefore be regarded as a hierarchy. With increasing SIL of a SRCF, the requirements for the associated SRECS, in terms of these factors that influence its integrity, are increasingly rigorous.

EN 62061 considers a SRECS to consist of one or more series subsystems, each of which can generally be classified as an input device, a logic solving device, or an output device. The SIL that the overall SRECS can achieve will be constrained by either the lowest SILCL[21] (SIL Claim Limit) amongst the series subsystems, or by the overall probability of dangerous random hardware failure calculated as a sum of individual subsystem PFH_D values.

Although the scope of EN 62061 does not extend to the actual design of complex and/or programmable electronic subsystems, it does cover their integration into a SRECS. For these subsystems, standards

17 A discrete level that specifies the required integrity of a safety function, and therefore determines requirements for the safety-related control system that performs the safety function.

18 Defined as a control function implemented by a SRECS with a specified integrity level that is intended to maintain the safe condition of the machine or prevent an immediate increase of the risk(s).

19 Defined as an electrical control system of a machine whose failure can result in an immediate increase of the risk(s).

20 Failure related in a deterministic way to a certain cause, which can only be eliminated by a modification of the design, or of the manufacturing process, operational procedures, documentation or other relevant factors. They generally arise out of deficiencies (e.g. logic and software errors) that are built-in to the hardware/software, and can therefore be induced by simulating the failure cause.

21 Maximum SIL that can be claimed for a SRECS subsystem on account of its architectural constraints and systematic safety integrity

such as IEC 61508, EN ISO 13849-1, or a product-specific functional safety standard (e.g. EN 61800-5-2 for drives) can be applicable.

The EN 62061 methodology is particularly amenable to safety-related drives that are compliant with EN 61800-5-2, as both standards are direct implementations of IEC 61508 and therefore have compatible methodologies. Furthermore, the terms that EN 61800-5-2 uses to specify the integrity of a safety-function (i.e. SIL Capability and PFH)[22] of a safety-related drive directly relate to the SILCL and PFH_D values that EN 62061 requires for SRECS subsystems. Figure 6 illustrates this process.

EN 62061 can also be applied if a safety-related drive is compliant with other standards, such as IEC 61508 or EN ISO 13849-1. For IEC 61508 products, the integrity of safety functions will be expressed in compatible terms, whilst EN 62061 provides guidance on using supplementary information on Safe Failure Fraction (SFF)[23] and Diagnostic Coverage (DC)[24] to facilitate the integration of subsystems with integrity expressed as an EN ISO 13849-1 Performance Level.

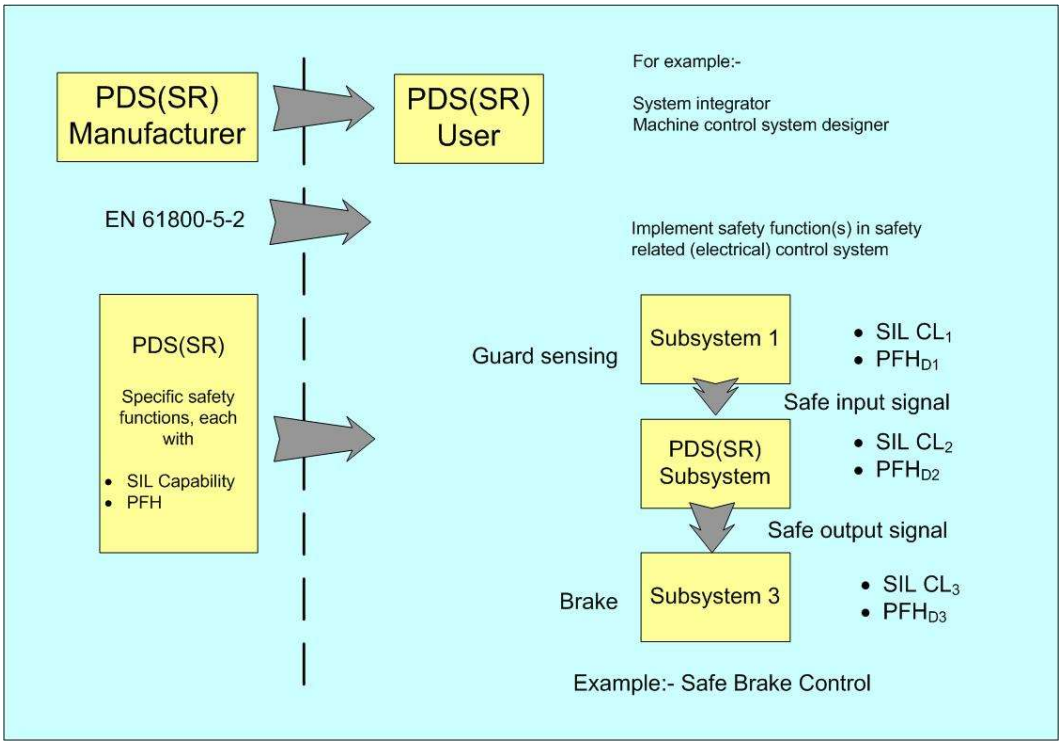


Figure 6 – Application of EN 62061 to integration of a PDS(SR) into a safety related control system of a machine

3.2.2 EN ISO 13849-1

Safety of machinery – Safety-related parts of control systems – Part 1: General principles for design

ISO 13849-1 has been adopted in Europe by CEN25 as EN ISO 13849-1. It was developed as a direct revision of and replacement for EN 954-1, with an unchanged scope covering electrical, mechanical, hydraulic, and pneumatic technologies. It is an improvement upon EN 954-1, resolving many of the

22 See Chapter 4.2.3 for descriptions.

23 The fraction of the overall failure rate of a subsystem that does not result in a dangerous failure.

24 Decrease in the probability of dangerous hardware failures resulting from the operation of the automatic diagnostic tests.

25 Comité Européen de Normalisation (European Committee for Standardisation)

deficiencies that hampered its predecessor's application to higher complexity systems, and consequently it is a considerably more complex standard.

EN ISO 13849-1 specifies a safety function's integrity as a quantitative PL (Performance Level). As shown in Table 3, a total of 5 PLs are used, each corresponding to a range of probability of dangerous failure per hour. By comparing the failure rates associated with PLs (Table 3) and SILs (Table 2), it is apparent that PLs generally provide a level of risk reduction from below SIL1 up to SIL 3.

EN ISO 13849-1 Performance Levels: target failure values	
PL	Average probability of a dangerous failure per hour (1/h)
e	$\geq 10^{-8}$ to $<10^{-7}$
d	$\geq 10^{-7}$ to $<10^{-6}$
c	$\geq 10^{-6}$ to $<3x10^{-6}$
b	$\geq 3x10^{-6}$ to $<10^{-5}$
a	$\geq 10^{-5}$ to $<10^{-4}$

Table 3 - EN ISO 13849-1 PLs

EN ISO 13849-1 provides a risk graph for assigning a PL to a safety function on the basis of required risk reduction. After determining this PL, the standard can then be used to develop a safety-related control system that performs the particular safety function at the required PL. The term SRP/CS is used to denote a safety-related (part of a) control system that performs the safety function.

In considering factors that influence the integrity of a SRP/CS, EN ISO 13849-1 provides quantifiable requirements for system structure, component reliability ($MTTF_d$[26]), fault detection capability (DC_{avg}[27]) and measures against Common Cause Failures (CCF) for multi-channel structures. It also specifies qualitative measures for the control and avoidance of systematic failures.

With this comprehensive consideration of integrity, the PL of a safety function can be regarded as a 5-step hierarchical scale of its risk reduction capability, ranging from PLa (lowest) up to PLe (highest). With increasing PL, the standard's requirements for the SRP/CS, in terms of these considerations, are increasingly arduous.

To aid their integration into safety-related control systems using the EN ISO 13849-1 methodology, some safety-related drives are supplied with the integrity of their safety functions expressed in accordance with EN ISO 13849-1 as well as EN 61800-5-2.

Although EN ISO 13849-1 is not a direct implementation of IEC 61508, it does take account of broadly similar factors in its consideration of integrity.

A further harmonised European standard, EN ISO 13849-2:2012, deals with validating the design of a SRP/CS.

4 FUNCTIONAL SAFETY STANDARD FOR POWER DRIVE SYSTEMS

4.1 EN 61800-5-2

Adjustable speed electrical power drive systems - Part 5-2: Safety requirements - Functional

26 Mean time to dangerous failure.

27 Average diagnostic coverage, which is a measure of the effectiveness of dangerous failure detection.

IEC 61800-5-2 is a product-specific implementation of IEC 61508. It specifies functional safety requirements for the design and development, integration[28], and validation of PDS(SR)s, and considers them as prospective subsystems of higher level safety-related control systems. It is applicable to adjustable speed electric drive systems that are covered by the scope of other parts of the IEC 61800 series of standards.

EN 61800-5-2, which is the CENELEC adoption of this standard in Europe, is a harmonised European standard with respect to the Machinery Directive. This means that a PDS(SR) designed in accordance with its provisions can, if appropriately used in a safety-related control system of a machine, be presumed to support certain aspects of the machine's conformity with the Machinery Directive.

EN 61800-5-2 specifies the integrity of safety functions provided by a safety-related drive in terms of IEC 61508 SILs, and like EN 62061, it also omits SIL 4 and restricts the expression of their performance to a probability of dangerous failure per hour. This is because only a level of risk reduction up to SIL 3 and the continuous and high demand modes of operation are considered relevant to a PDS(SR).

4.2 Safety Functions according to EN 61800-5-2

Safety-related drives can provide an extensive and diverse range of safety functions. As machines account for a large proportion of their applications, many of these safety functions deal with hazards associated with motor-driven moving parts of machinery. They can either monitor or control some aspect of the drive's performance, typically preventing motion of moving parts or limiting their position, speed or torque.

With monitoring-type safety functions, an input signal (e.g. an interlocking switch) or some variable (e.g. speed, position, etc) is monitored by the drive, and an appropriate reaction (e.g. remove power from motor) is triggered if this violates a limit. For control-type safety functions, there is no corresponding reaction to a limit being violated. However, both classifications of safety function will require a 'fault reaction function' that attempts to initiate a safe state if the drive's diagnostics detect a fault within the hardware/software that performs the safety function.

Although basic monitoring safety functions can be implemented using a standard drive in conjunction with supplementary safety-related control systems (see 2.4.1), complex motion control safety functions can be difficult to implement using a standard drive.

4.2.1 Stopping functions

EN 61800-5-2 refers to 4 safety functions associated with stopping and preventing motion of a motor controlled by a safety-related drive:

- Safe Torque Off (STO)
- Safe Stop 1 (SS1)
- Safe Stop 2 (SS2)
- Safe Operating Stop (SOS)

The STO safety function corresponds to an uncontrolled stop in accordance with EN 60204-1 stop category 0, but with a defined integrity level. It requires removal of power that can generate torque from the motor, and its implementation in a safety-related drive is typically accomplished by a robust disablement of power semiconductor firing pulses. An implementation of the STO safety function

[28] This relates to integration of parts within the PDS(SR) rather than the PDS(SR)s integration into a safety-related control system, for which EN 62061 and EN ISO 13849-1 are available.

externally to a (non safety-related) drive would typically use one or more electromechanical contactor(s) to remove power from the drive and/or motor (see 2.4.1).

For an a.c. drive and motor combination, torque is produced only if different pairs of power semiconductors attain a conductive state in sequence. So if a single failure causes a power semiconductor to conduct unintentionally whilst the STO safety function is active, this will not produce torque, and multiple static failures will not result in sustained rotation.

The STO safety function does not constitute electrical isolation of a machine to allow safe access to electrical connections, which requires the use of a suitable supply disconnecting (isolating) device (see EN 60204-1, clause 5.3).

The STO safety function can be used to prevent an unexpected start-up of moving parts of a machine, or to achieve an uncontrolled stop. For some applications, this could result in an unacceptably long stopping time depending on the effects of friction and the inertia of a motor and its mechanical load. Furthermore, as there is no torque produced in a motor whilst the STO safety function is initiated, measures (e.g. a supplementary brake) may need to be taken to prevent the movement of mechanical loads that are under the influence of an external force such as gravity.

If a motor must be brought to a standstill more rapidly, this can be accomplished by either supplementary mechanical braking or by using the SS1 safety function. The SS1 safety function corresponds to a controlled stop in accordance with stop category 1 of EN 60204-1, but with a defined integrity level. It can be considered as a 2-stage safety function, consisting of controlled deceleration of the motor to a standstill followed by initiation of the STO safety function. EN 61800-5-2 affords some flexibility on whether the deceleration phase is safely monitored or controlled, and on whether the STO safety function is initiated when standstill is detected or after an application-specific time delay.

The SS2 safety function corresponds to a controlled stop in accordance with stop category 2 of IEC 60204-1, but with a defined integrity level. As with the SS1 safety function, it involves a controlled deceleration of the motor to a standstill, but this is followed by initiation of the SOS safety function rather than the STO safety function. With the SOS safety function, the drive holds a motor in an energised but stopped state, with a holding torque that resists external forces and is therefore able to prevent the motor moving from the stopped position.

4.2.2 Other safety functions

Although not an exhaustive list, EN 61800-5-2 refers to various other safety functions that can be implemented by a safety-related drive. Some of the more complex safety functions incorporate or combine simpler safety functions.

- Safely-Limited Acceleration (SLA)
- Safe Acceleration Range (SAR)
- Safely-Limited Speed (SLS)
- Safe Speed Range (SSR)
- Safely-Limited Torque (SLT)
- Safe Torque Range (STR)
- Safely-Limited Position (SLP)
- Safely-Limited Increment (SLI)
- Safe Direction (SDI)
- Safe Motor Temperature (SMT)

- Safe Brake Control (SBC)
- Safe Cam (SCA)
- Safe Speed Monitor (SSM)

4.2.3 Specification of safety functions

EN 61800-5-2 requires the manufacturer of a safety-related drive to provide details of all safety functions that it can perform. For each safety function, this information must include:

- A functional specification, including details of the reaction when a monitored variable violates its limit, the fault reaction function, the response times, any order of priority in relation to other safety functions, and
- An integrity expressed in terms of a 'SIL Capability'[29] and a 'PFH'[30].

4.2.4 Applying a safety-related drive

The user/integrator of a safety-related drive that complies with EN 61800-5-2 will need to:

- Conduct a risk assessment for the particular application
- Identify all safety functions required and allocate a SIL to each of these (i.e. formulate a Safety Requirements Specification – see 2.3 and 3.2)
- Select a PDS(SR) with appropriate capabilities in terms of its safety functions and their integrity (specified in terms of a SIL Capability and PFH).
- Interface the PDS(SR) with other subsystems and consider the validity of signals and commands from these
- Design, develop integrate and validate the overall safety-related control system, including the hardware, software, parameterisation, etc.

Where the solution requires a PDS(SR) to interface with other subsystems in the safety-related control system, any input and/or output signalling will need to be of sufficient integrity.

An appropriate fault reaction will need to be selected for each safety function, and an appropriate response to violation of a limit will also need to be selected for those safety functions that perform a monitoring task. The timings associated with these reactions/responses will need to be suitable for the application.

It will also need to be established whether the priority of any simultaneously active safety functions that could present a conflict is suitable for the application.

---

29 Maximum SIL that can be claimed based on systematic safety integrity and architectural constraints

30 Probability of dangerous failure per hour.

Annex A

IEC 61508[31]

IEC 61508 was published first in 2002 and in revised form in 2010. It provides cross-sector guidance on the specification, design and validation of electrical, electronic and programmable electronic (E/E/PE) safety-related control systems, and is accepted as the authoritative good practice in the field of functional safety. Although CENELEC have ratified it as EN 61508 within Europe, it is not listed in the OJEU because its scope is too broad for any relevant European Directives. Consequently, application of EN 61508 does not automatically grant a presumption of conformity with any particular European Directive.

Prior to the publication of IEC 61508 there was a reluctance to use complex and/or programmable electronic technology in control systems that perform safety functions. This was primarily because of its susceptibility to unpredictable failure modes, with resulting indeterminable behaviour. Safety-related control systems were therefore restricted to low complexity technology, such as electromechanical switches, relays and contactors, placing no reliance on the correct operation of complex electronic devices such as drives and PLCs.

IEC 61508 provides a comprehensive methodology that can be applied to E/E/PE safety-related control systems of any complexity, from low complexity electromechanical systems through to complex and/or programmable electronic systems. As well as its deterministic and structural considerations for integrity, it quantitatively considers component reliability, fault detection and failure direction. Requirements for the control and avoidance of systematic failures are also set out, and one part is dedicated to software considerations.

IEC 61508 specifies the required integrity of a safety function in terms of a discreet SIL (Safety Integrity Level), which is an indicator of risk reduction capability ranging from SIL 1 (lowest) through to SIL 4 (highest). With increasing SIL, the requirements for a safety-related control system are correspondingly more onerous. As each SIL is specified quantitatively as a range of probability of dangerous failure, it can generally be considered as the probability of a safety-related control system satisfactorily performing the required safety function.

Although IEC 61508 can be applied directly to systems and products that incorporate E/E/PE safety-related control systems, as a basic safety publication its primary role is to serve as a framework for developing sector-specific and product-specific derivatives. With reference to Figure 7, IEC 62061 was developed as the machinery sector implementation of IEC 61508, whilst IEC 61800-5-2 has been developed as a product implementation for PDS(SR)s.

31 IEC 61508 - Functional safety of electrical/electronic/programmable electronic safety-related systems (7 parts).

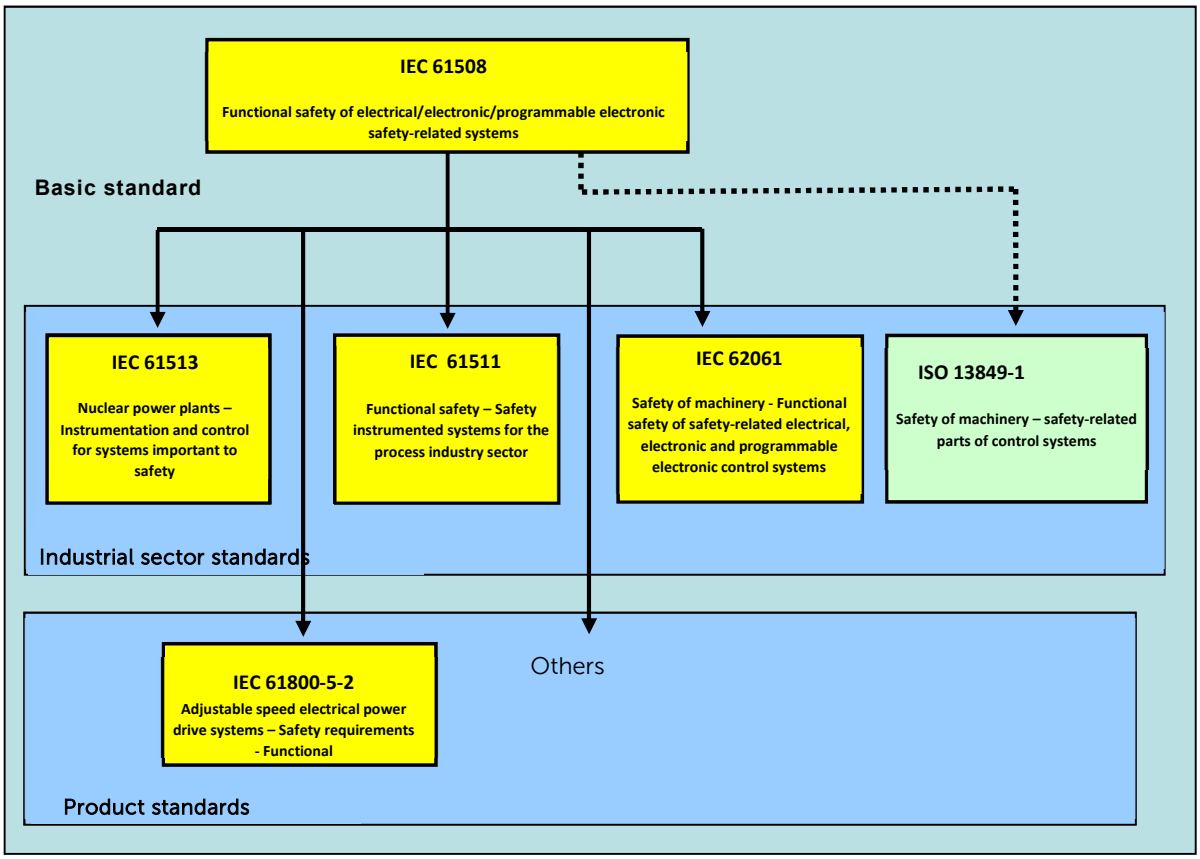


Figure 7 - The IEC 61508 family of functional safety standards (EN versions are also described in the text)

Annex B

Using contactors to remove torque.

If contactors are used to prevent the drive applying torque to a motor, the following points should be considered

Most contactors are only rated to break current at the mains frequency, i.e. 50 Hz or 60 Hz. If such a contactor in the output of a drive is opened while the PDS is supplying motor current, especially at low speed, the contactor may not be able to safely interrupt the current. This could result in excess arcing within the contactor, causing a fire risk, or a risk to the converter.

Many drives are equipped with input terminals that can be used to inhibit the drive's output current. If output contactors or isolating switches are to be installed in the drive output, then these terminals can be used to ensure the removal of output current before the output circuit is interrupted.

If a contactor is placed at the input of a drive, the contactor will not be subjected to currents at lower frequencies than the mains supply. However, because it removes power from the BDM, it will increase the time required to achieve an intended restart of the motor. Even if the BDM has an auxiliary input to maintain control power, it will still take some time to re-establish the d.c. link voltage before the BDM can restart the motor.

Therefore, it is necessary to select a contactor that can safely break current in the required location and the BDM manufacturer should be consulted about the impact on the BDM of placing the contactor in a particular location.

These factors can be avoided by using a drive with a Safe Torque Off function of suitable integrity instead of contactors. The solid state output circuit terminates the motor current smoothly without arcing and without the need to separately inhibit the drive output current.

The GAMBICA Association Ltd

Rotherwick House
3 Thomas More Street
London E1W 1YZ

T +44 (0) 20 7642 8080
E info@gambica.org.uk
W gambica.org.uk