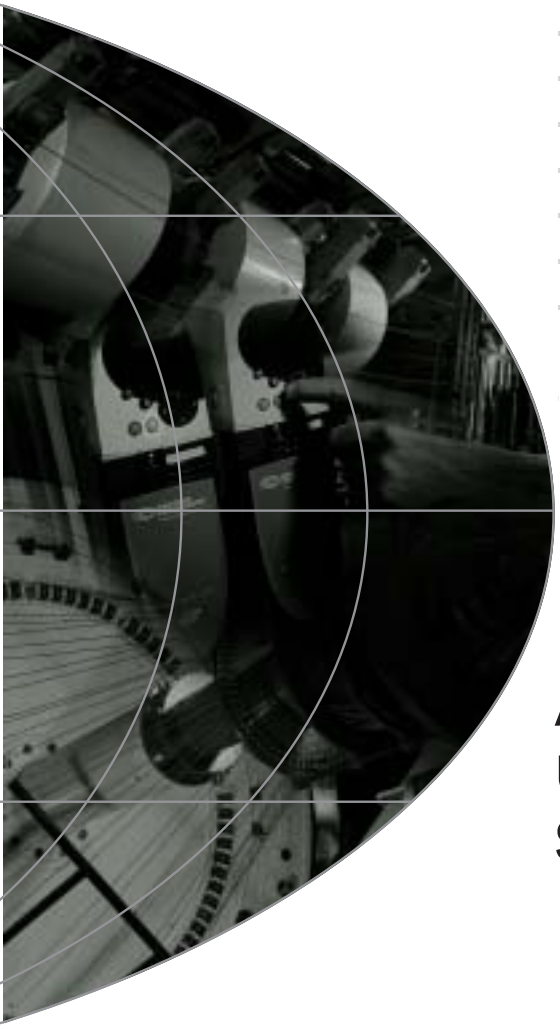


A Guide to the Unidrive SP Secure Disable Function

A Guide to the Unidrive SP Secure Disable Function

Index

1.Quick overview - SECURE DISABLE

The Secure Disable feature on the Unidrive SP AC drive allows the drive output to be disabled so that the drive cannot generate torque in the motor. Secure Disable also provides a normal “enable” input to the drive, and can be used in the same way. A +24V logic level must be applied in order to enable the drive power functions. However the internal circuitry has been designed using in-depth fail-safe approved techniques and principles so that no single fault or component failure can cause a disabled drive to produce motor shaft torque. Only in extremely unlikely combinations of faults could this function be defeated. Secure Disable can therefore be used in safety-related applications to prevent unintended operation of the motor.

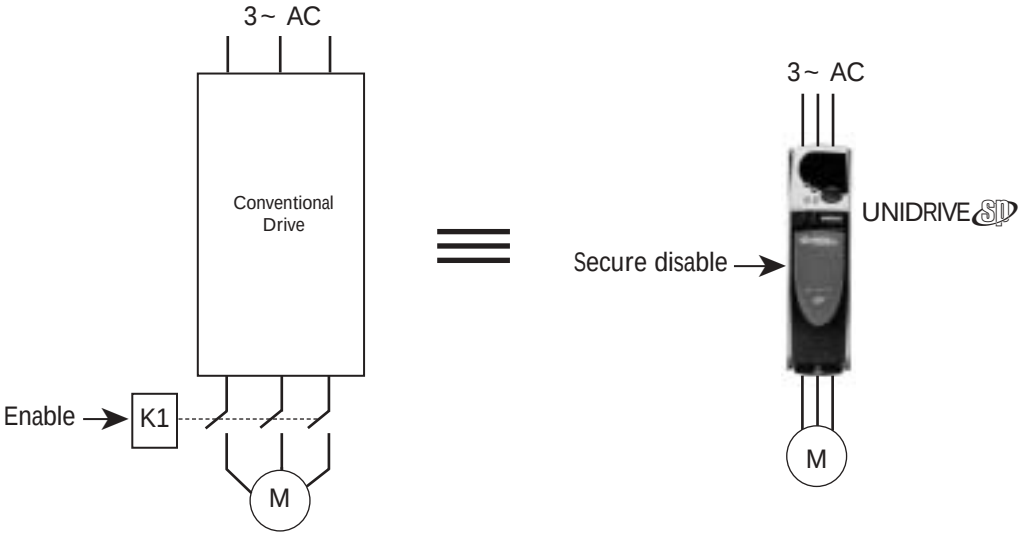


Figure 1 The Secure Disable function can take the place of control gear, saving components and space for the same level of safety and security

The reliability of the Secure Disable function is superior to that offered by virtually any single-channel electromechanical device such as a contactor. It is like having a special highly reliable contactor built in to the drive output, but there are no moving parts, no extra cost, and no special requirements for preventing the contactor from opening on load. It offers the possibility of eliminating contactors, including special safety contactors, from systems where the prevention of movement is important to prevent safety hazards or expensive damage.

The remainder of this publication explains the essential principles of safety-related systems, focussing primarily on machine applications and the requirements of the European Union Machinery Directive 98/37/EC, and then explains how the Secure Disable feature can be used to help implement safety requirements. If you are familiar with the principles of the design of safety-related machine control systems, then we suggest you move on directly to section 3

Important warning

The design of safety-related systems requires specialist knowledge. To ensure that a complete system is safe requires an overall risk assessment. The use of Secure Disable and other equipment intended for safety-related applications does not of itself ensure safety. They must be correctly incorporated into the complete design.

The information in this publication gives guidance on the use of Unidrive SP Secure Disable, and also some general background material on the design of safety-related systems. This information is believed to be correct and to reflect accepted practice at the time of writing. However it is the responsibility of the designer of the end product or application to ensure that it is safe and in compliance with relevant regulations.

Section 2: Principles of machine safety design.

The design of safe machinery is a complex activity which requires attention from the very beginning of the design process. This part of the guide gives a simple overview which is intended to explain how the use of the Unidrive SP Secure Disable feature fits in to the overall scheme of safe machine design.
The references section at the end of this publication gives some useful sources of further guidance on the subject.

Risk assessment

A variety of measures can be used to ensure the safety of a machine. As far as possible, the machine should be designed to be inherently safe, i.e. so that hazards are eliminated from the basic design. However in many cases some risks remain at an unacceptable level and have to be actively reduced by the use of suitable control measures, which may use pneumatic, hydraulic, electrical or other control methods. These often take the form of various kinds of interlocks which prevent the machine from functioning when entry or access is possible, e.g. through the opening of a guard etc.. More complex safety functions may sometimes be necessary, e.g. limitation of speed or the prevention of certain operations depending on the state of the machine.

In order to ensure the safety of the complete design, the machine must be subjected to a risk assessment. In this assessment the effect of the safety features in the control system will be taken into account when looking at the overall risk of each possible hazardous event.
For the purpose of the EU Machinery Directive, there are European harmonised (CEN) standards which lay down the essential principles for the procedure for designing safe machinery and carrying out a risk assessment. These are the so-called "A standards".[1]

EN 292 parts 1 and 2
Safety of machinery - Basic concepts and general principles for design
EN 1050
Safety of machinery - Principles for risk assessment

[1] An alternative approach is laid down in the EN 61508 series of standards. These are not currently listed in the Official Journal of the EU under the Machinery Directive. Some information is given in appendix 1.

The basic concept contained in EN 1050 is that hazards which can result in harm to a person can be analysed. The risk associated with the hazard is measured in terms of the combination of several factors:

- The degree of harm which would result
  (e.g. scratch/bruise.....death)
- The likelihood of occurrence (i.e. whether the hazard could be avoided during exposure)
  (e.g. occurrence almost impossible.....certain)
- The frequency of exposure
  (e.g. once yearly.....constant)
- Number of persons exposed

EN 1050 gives a method for combining these factors to give an overall risk level, and also an indication of what level is acceptable.

The initial risk assessment will indicate whether unacceptable risks exist which must be reduced. Typically an initial assessment would be made with no special control measures. If necessary, risk reduction measures would be added and the design of the machine would proceed iteratively until the residual risk was acceptable. At this stage the requirements for the integrity of the control system will have been defined.

Responsibilities

From the above outline it should become clear how responsibility for the safety of the machine is allocated.

The machine manufacturer takes overall responsibility for the safety of the machine. It is not possible for this responsibility to be delegated to component suppliers or contractors. As part of this responsibility, the manufacturer must allocate specific safety requirements to any purchased components or sub-assemblies. These requirements have to be exactly specified in the purchase specification.

The supplier of components or sub-assemblies is responsible for ensuring that these items meet their purchase specification, including any safety-related aspects. This would normally include reference to any relevant safety standards for such parts. It is clearly vital that these requirements be understood and agreed to by all parties involved.

Standards for control systems

European harmonised standards exist for specific safety aspects of machines, the so-called “B standards”. For control systems the relevant standard is:

EN 954-1

Safety of machinery. Safety related parts of control systems. General principles for design.

This standard identifies several categories for control systems, depending on the integrity of their design and the degree of fault tolerance and fault revelation. The following is an outline and explanation of the categories. Please refer to the standard for a definitive statement

Category	Requirements	Comments
B	Parts designed in accordance with relevant standards, able to withstand the expected operating stresses - i.e. “well engineered”.	Not generally suitable for safety-related applications
1	In addition to the requirements of B, parts are well-tried and designed according to established safety principles.	Only suitable for low risks (e.g. minor injury hazards)
2	In addition to the requirements of 1, a safety function check is carried out at suitable intervals.	Although a fault in the unsafe direction is detected by the check, a hazardous condition could still arise between checks.
3	In addition to the requirements of 1, a single fault does not cause the loss of the safety function. As far as possible, a single fault is detected before the next call on the safety function. Not all faults are detected however.	This gives a “fail-safe” system, but an accumulation of undetected faults could cause a loss of the safety function
4	In addition to the requirements of 1, a single fault does not cause the loss of the safety function. Either a first fault is detected before the next call on the safety function, or else an accumulation of faults does not lead to a loss of the safety function.	This gives a “fail-safe” system. The residual risk is likely to be from “common cause” failures, i.e. where an unexpected outside influence causes all of the safety provisions to fail.

Guidance in EN 954-1 indicates the suitability of these categories for various evels of risk:

Category	Severity of injury	Frequency/duration of exposure	Possibility of avoidance
B			
1	Slight	Any	Any
	Serious	Seldom/short	Possible
2	Serious	Seldom/short	Possible
	Serious	Seldom/short	Scarcely possible
3	Serious	Seldom/short	Scarcely possible
	Serious	Frequent/long	Possible
4	Serious	Frequent/long	Scarcely possible

In assessing a system against EN 954-1, some faults can be “excluded”, i.e. it is considered that they are too unlikely to require consideration. A draft standard prEN 954-2, which is expected to be published as a harmonised standard late in 2002, gives a list of such excluded faults.

Section 3: Conventional electromechanical control system design using EN 954-1

This section considers some electromechanical designs for safety-related control systems. In all cases it is assumed that the machine risk assessment has been carried out and that the need has been identified for a control system with a safety function to prevent the machine motor from being driven inadvertently.

The examples considered use an a.c. motor driven from the a.c. mains through a conventional variable-speed drive. The conventional drive cannot contribute to the safety functions, because it uses complex advanced hardware and software, which do not meet the requirements of EN 954-1 category 1. For the purpose of the safety design it has to be assumed therefore that an a.c. supply capable of driving the motor is always available when power is applied to the conventional drive, regardless of the existence of any stop/start and inhibit features which it may offer.

The device used to disconnect the conventional drive (or motor) is a three-phase electromechanical contactor. This is a simple and reliable device which has been manufactured in large quantities for many years, so that its failure modes are well known. If it is used within its ratings and replaced before its predictable wear-out time it offers a low failure rate. However there are definite unsafe failure modes which cannot be excluded, and have to be allowed for in the design:

– Mechanical fault causing the contactor to remain closed when control signal removed - e.g. weak spring, mechanical jamming.

– Welding of contacts, with the same result.

Case 1 - Simple stop/start control

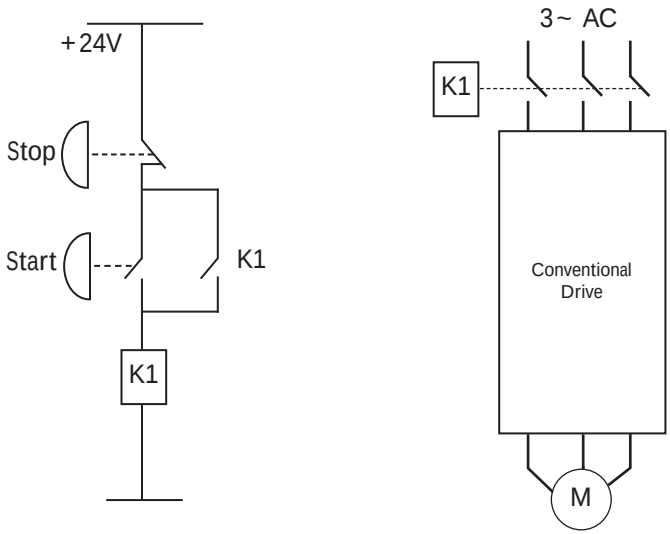


Figure 3A: Simple stop/start control using contactor, to EN 954-1 category 1

This widely-used arrangement requires a button press before the machine can start. After loss of power the button must be pressed again to re-start the machine, thus removing the risk of unexpected start-up after a power failure. The buttons can be designed with forcible actuation[2], and the start button provided with a shroud, to minimise the risk of an unintended contact closure. Broken connections and earth faults cause the machine to stop provided the components are intact. However a jammed or welded contactor causes the machine to continue running, and is not detected except by operator observation.

Depending on the choice of parts, this arrangement could meet EN 954-1 categories B or 1. It therefore would only be suitable where the hazard was small, and in practice it is most likely to be used where there are no significant safety hazards but there might be risks of damage to expensive machinery or materials from inadvertent start-up.

[2] i.e. if the button moves the contact must operate - see EN 418

Case 2 - Interlock with feedback

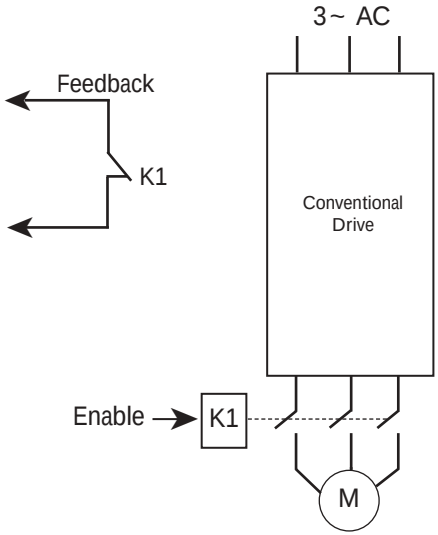


Figure 3B: Output disable function with feedback, using contactor having contacts with connected movement

In this case some form of interlock arrangement has been provided which prevents the conventional drive from operating when a gate or other safety device is not in the safe position. Its output is the "enable" signal. The final control element is the contactor K1, which is a special safety contactor having "contacts with connected movement".[3] Such a contactor has the same failure modes as any other, i.e. it may fail in the closed condition, but is designed so that the auxiliary (normally-closed) contact is always in the corresponding state to the main (normally-open) contacts, even when these are in the wrong state. Therefore the hazardous fault can be detected at any time when the enable signal is absent. Usually the detection arrangement comprises a series circuit with a reset push-button which has to be operated manually before the interlock can be released - for example using a safety interlock relay as shown in Figure 3C.

[3] Also sometimes referred to as 'forcibly guided contacts' - see EN 50205

Case2: Interlock with feedback (shown with safety relay)

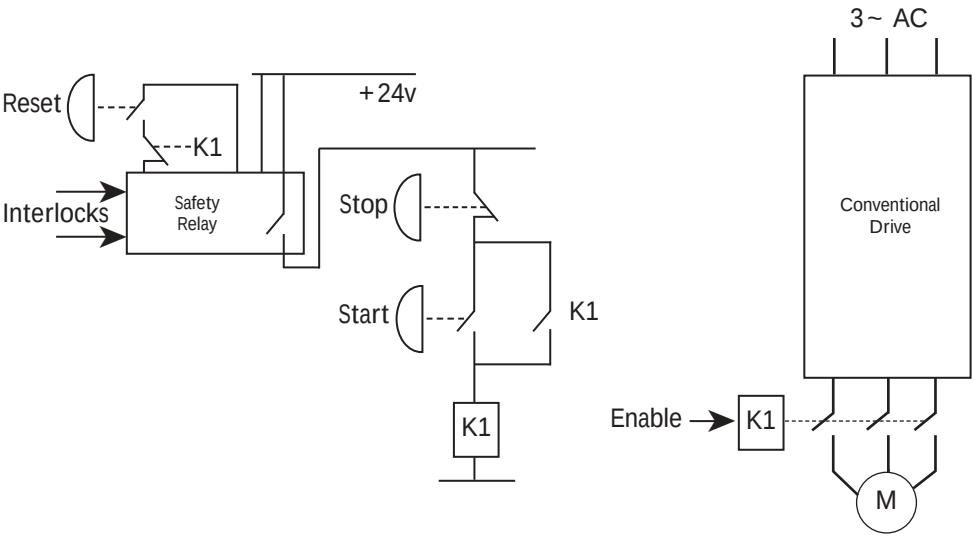


Figure 3C: Typical use of feedback contact to detect a fault and prevent further operation to EN 954-1 category 2

The arrangement in Fig 3C meets category 2 of EN 954-1. It can still fail in the unsafe direction as a result of a single fault, but the fault would be detected whenever the interlock circuit was next activated. Whether this was acceptable would depend on the details of the machine operation - for example, if the interlocks were activated frequently but the operator only rarely exposed to the hazard, it is more likely to be acceptable than where the interlocks are rarely operated.

Note that in principle a short-circuit in the power wiring could cause the motor to be energised, and not be detected. However there would need to be two separate short-circuits for this to happen, which is sufficiently unlikely to be excluded.

Case 3 - Fail-safe interlock with feedback

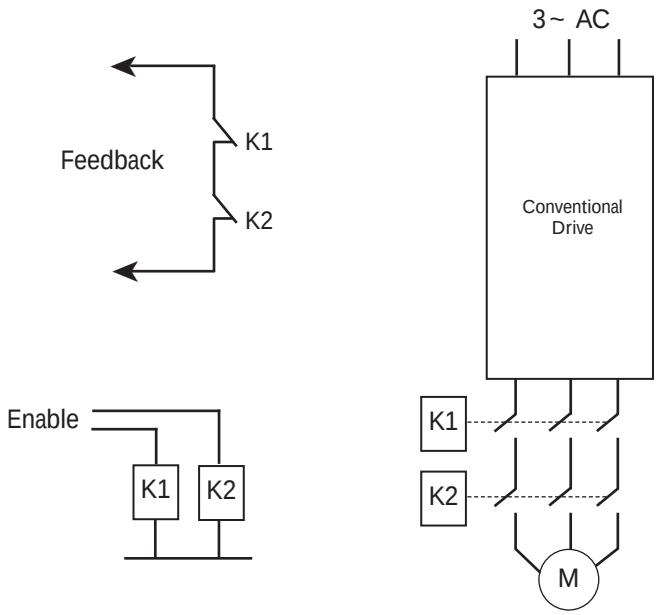


Figure 3D: Fail-safe output disable function using two contactors having contacts with connected movement, to EN 954-1 category 3 (or 4)

In this case two contactors are provided with their output contacts in series, so that a single fault does not cause the motor to be driven. A faulty contactor is detected at the next operation of the safety system, and further movement prevented. Depending on the other control arrangements, this could meet categories 3 or 4 of EN 954-1. The residual risk is of either the second contactor failing before the next test was carried out, i.e. two random failures within the test interval, or more likely a common-mode failure, i.e. some influence causing both contactors to fail at the same time.

Disadvantages of electromechanical systems

Safety relays and contactors are very well-established components with a long history of development into their present form, which gives good reliability and moderate cost.

However as well as the cost there are some serious disadvantages:

– Mechanical and electrical wear, requiring periodic maintenance or replacement
– Sparking and electrical interference
– When using contactors with a.c. variable speed drives, including servo drives:
  – With contactors at the input, the other functions of the conventional drive are lost in the inhibited state. Data communications are lost unless the data network has a separate power supply. The drive may have restrictions on the frequency of power up/down cycles, and may require an inconveniently long time for power-up initialisation.
  – At the output, great care must be taken to ensure that the contactor does not open with the motor on load at low speed, because severe arcing and destruction is likely - unless an expensive d.c. rated type is used. This kind of malfunction could even be a possible common cause for both contactors failing concurrently in the closed (unsafe) direction, by welding of contacts.

Locating contactors either at the input or the output of a drive causes practical difficulties and additional costs. In principle, when using an a.c. variable speed drive in a safety system the use of contactors could be made unnecessary through good design. The drive itself contains the essential elements to prevent the motor from being driven. By utilising good design a suitable safe interface between the drive power circuit and the safety control system is achievable. This is what the Secure Disable function on the Unidrive SP does.

Section 4: Unidrive SP Secure Disable - how it works

Principles

The a.c. induction motor requires a rotating magnetic field to produce torque, and this requires a three-phase source of alternating current at the connections. The drive has available a single internal d.c. supply, which is converted to a.c. by the continual active switching action of six power semiconductor devices (IGBTs). Failure of the individual IGBTs or their drive circuits either into the on or off state cannot generate torque.
(Note when a permanent magnet motor such as a servo motor is used, a single transient alignment torque could be produced by a multiple IGBT failure. The motor could rotate by a maximum 360°/p (where p is the number of poles.))

The drive contains a complex control circuit using digital logic and one or more microprocessors to generate the correct switching sequence for the IGBTs. It would not be satisfactory to provide the disable feature within this part, because the complexity of the arrangement makes it very difficult to prove that all failure modes have been considered and eliminated. This applies both to the drive designer, who would have to prove that no unexpected effects in the hardware or software could cause a loss of of the disable function, and also to the system designer, because the drive offers many advanced control features which might have unforeseen effects on motor operation in some unusual circumstances. From all points of view, what is needed is a very simple and reliable method for preventing the drive from producing torque in the motor, regardless of any other complex intelligent operations which it might be carrying out.
In some conventional drive designs a “hardware enable” input is provided which operates through some simple electronic logic to prevent the operation of the power stage, as illustrated in Figure 4A. The disable function provided by this arrangement is likely to be more reliable than one operating through the software, but the logic circuit is not fail-safe - it is equally likely to fail in the unsafe and safe directions. This is not acceptable for a safety-related application.

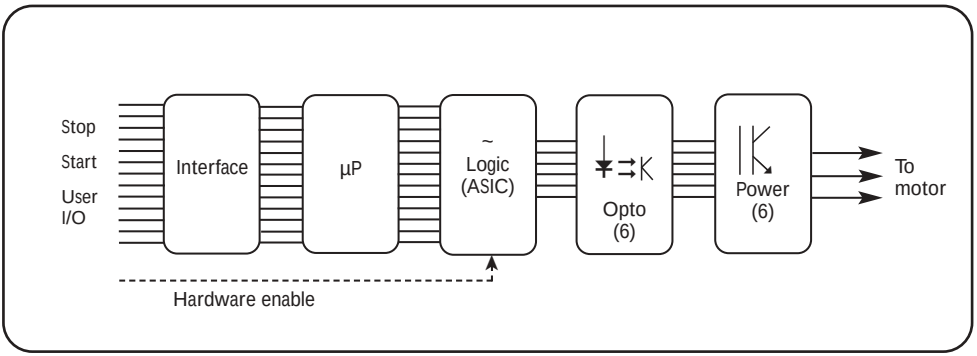


Figure 4A: Conventional drive hardware enable

The switching signals are conveyed from the complex control circuit to the IGBTs by opto-couplers which use light-emitting diodes (LEDs) to transmit simple on/off commands across the electrical isolation barrier. In the Unidrive SD Secure Disable system shown in Figure 4B, the power supply to the LEDs is provided by a fail-safe circuit from the enable input. The switching sequence can therefore only reach the IGBTs if the enable input is present, or if a highly unlikely combination of unrevealed faults has occurred which has allowed the enable input to receive power. The resistor from the enable input to the logic ASIC allows the drive to inhibit the output in a controlled sequence in the absence of a fault, but it has no safety function. If the ASIC were to fail in the unsafe direction, the drive would then be securely disabled through loss of the LED power supply.

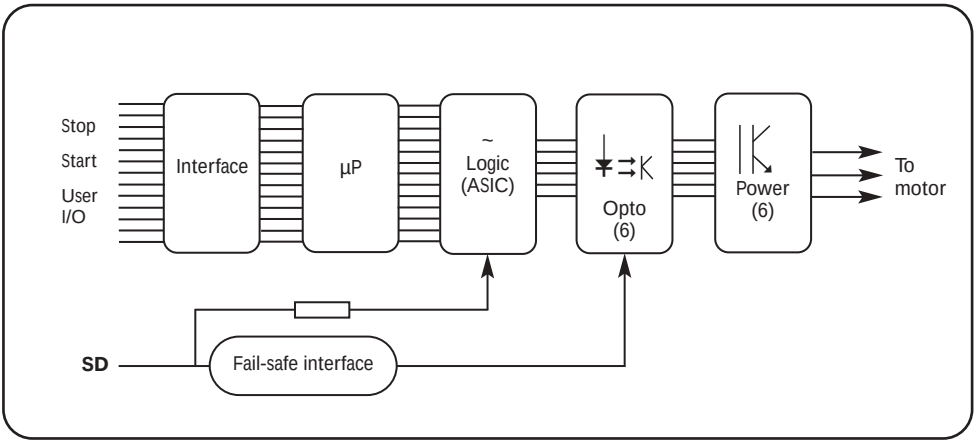


Figure 4B: Unidrive SD Secure Disable

Failure analysis, conformity and approval

The novel part of the Secure Disable feature is the fail-safe circuit which converts the incoming 24V digital control signal to the correct level for supplying the opto-couplers. This circuit has been designed to be inherently fail-safe, i.e. no single component failure causes it to enable the drive inadvertently, and most failures cause it to be disabled. Only an extraordinary combination of failures could cause it to enable the drive inadvertently. This meets the requirements of EN 954-1:1997 category 3.

The design has been independently verified by the German safety organisation BIA.[4]

What Secure Disable does

When the drive enable input is not connected, the drive is in a high integrity disabled state. It will not produce torque in the motor even if internal faults are present. The drive remains active, i.e. its internal circuits are operational, parameters can be altered, signal inputs and outputs are active and it continues to communicate.

When the enable input is connected to a digital level of +24V nominal, the drive operates in the normal way.

What Secure Disable can not do

Secure Disable has the same functional effect as a contactor in the drive output circuit, but is superior because it cannot stick or weld closed. The following limitations must be taken into account. They are the exactly the same as for an output contactor.

Secure Disable does not provide braking. If a running drive is disabled, it immediately ceases to produce torque, either motoring or braking.
If a braking function is required, the drive must not be disabled until braking is complete. An example is given in section 5 showing a simple time-delayed disable arrangement. Braking by the drive is not a high-integrity function. If braking is a safety requirement then an independent fail-safe braking mechanism must be provided.

[4] Berufsgenossenschaftliches Institut für Arbeitssicherheit, i.e. professional co-operative institute for safety at work

Secure Disable does not provide electrical isolation of the drive output. If access is required to the motor circuit electrical connections, the drive power input must be isolated by an approved isolating device, and the required discharge time (usually 10 minutes) must elapse before access is permitted.

Secure Disable cannot detect if the enable input has been energised inadvertently. There is only a single input channel, so if this becomes inadvertently connected to a positive digital signal within the specified range, the drive will be enabled. For the highest integrity the installer must protect this wiring from accidental contact with digital signals or supplies.

How is Secure Disable used

Secure Disable is used in exactly the same way as a conventional enable input, so all existing applications are unchanged. It has the additional benefit that it disables the drive with a very high integrity, so that it can be used in safety-related applications which are discussed in more detail below.

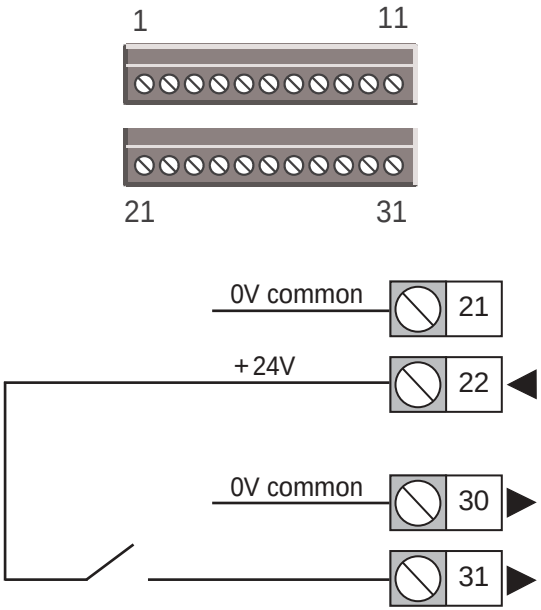


Figure 4C: Unidrive SP control connections, showing Enable input (Terminal 31) for Secure Disable function

It can also be used in other applications where a highly reliable disable function is required. For example, it is common for a start/stop function to use a simple reliable contactor latch circuit in order to avoid expensive, non-safety-related damage from inadvertent start-up. Secure Disable can eliminate the use of a contactor.

How does Secure Disable compare with competing systems? Why is there no relay in Secure Disable?

Secure Disable has been designed into the Unidrive SP from first principles. By careful design of fail-safe electronic circuits it has avoided the need for expensive additional option modules or safety relays, and offers superior integrity for lower cost.

Most systems available in competing drives use the same basic principle as Secure Disable, which is to interrupt the power supply to the IGBT gate-drive opto-couplers. However they generally use a relay to interrupt the power and provide electrical isolation and/or signal level shifting. This is illustrated in Figure 4D, which includes a typical external test circuit for the relay feedback contact.

Even though the relay is a special highly reliable type, it still has the possibility to fail in the closed direction. In order to detect this it must be of the connected-movement design, so that if the main contacts remain closed this can be detected by an external circuit through an auxiliary contact. In the example shown, the auxiliary contact is wired in series with the reset input of the external safety circuit, so the relay in the drive is tested every time the interlocks are tested. This is a standard method for monitoring safety relays. However if the relay does fail in the closed direction then the drive may become enabled before the failure is detected. This means that the drive with an external test circuit can only meet category 2 of EN 954-1. For a category 3 application it is still necessary to use one external contactor to prevent the motor from being driven because of this first fault.

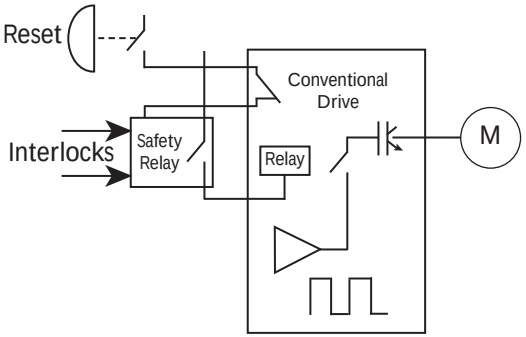


Figure 4D: Typical drive disable function using relay having contacts with connected movement

With Secure Disable, as shown in Figure 4E, there are no credible single faults which can cause the drive to become enabled. Therefore there is no need for an external fault detection circuit in order to meet category 3 of EN 954-1. The only special requirement is for the use of protected wiring (see box) to the enable (SD) input, in order to exclude the possibility of a short-circuit to a positive supply. In this illustration the external safety relay has been retained, since it might be used for example to detect discrepancies between redundant interlock signals, but it is no longer necessary to monitor the drive disable function.

PROTECTED WIRING

Protected wiring is arranged so that no short circuit is credible to any source of voltage which might cause a failure in the unsafe direction. A practical implementation is either:

Fully segregated, i.e. in dedicated trunking etc.

or

Screened, with the screen connected to ground, in a positive-logic grounded control circuit

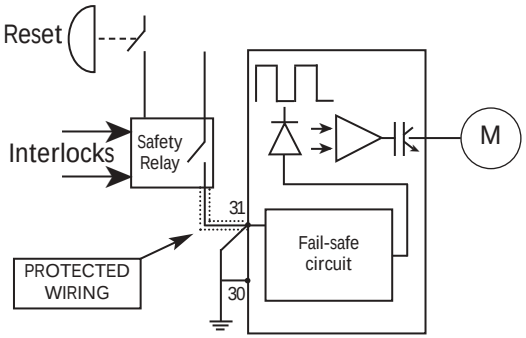


Figure 4E: Secure Disable in a typical safety circuit

The use of a relay with a feedback contact may feel reassuringly familiar to those used to working with relay safety logic systems. However it has very little benefit, and introduces its own new failure mode which has to be detected by a monitoring circuit and defended against by the additional contactor. Secure Disable uses a fully solid-state circuit which avoids this problem. The only disadvantage of SD is that a wiring fault in the single input channel would not be detected. This can be excluded under prEN 954-2 by the use of protected wiring.

Location of contactor

When a contactor is used with a drive to prevent motor operation, it can be located either at the drive power input or the output. The best choice of location depends on the application, but the following issues must be considered:

Contactor at output:

This is often seen as desirable since the motor is clearly separated from any possible source of stored energy or unexpected drive behaviour. However:

- It is essential to arrange that the drive is disabled and the output current has decayed to zero before the contactor is opened, otherwise arcing will occur which can cause interference, premature contact wear or even severe damage to the contactor if it opens a high current at low frequency. This may require some form of time delay in the contactor circuit, which must itself be of fail-safe design. Alternatively a d.c. contactor must be used.
- Drive braking is not available once the contactor is open, so if required then a time delay arrangement must be included, which must be fail-safe.

Contactor at input:

This ensures that a conventional a.c. contactor is suitable without special provisions, and drive dynamic braking is available. However:

- The drive may have a restriction on the number of starts per hour from the input power supply. There will be a time delay from application of the supply to the drive becoming available.
- Auxiliary drive functions such as data communications, control computations and provision of auxiliary user supplies are lost.

The use of Unidrive SP Secure Disable provides most of the benefits of both methods.

✓ The contactor is eliminated so there is no risk of arcing and no need for early-disable arrangements

✓ The drive remains powered so the auxiliary functions are not lost

✓ There are no problems with power-up restrictions or delays.

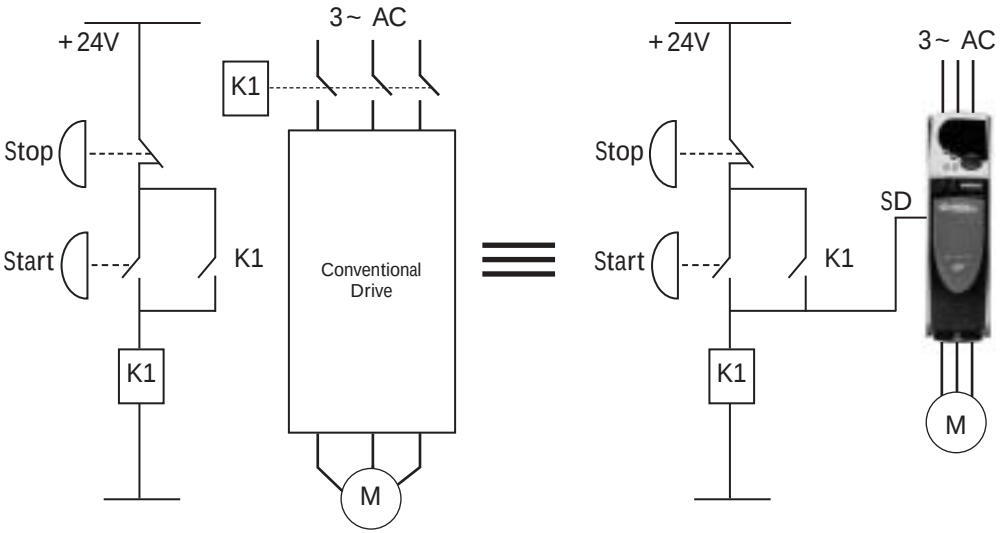
Only where dynamic braking is required must an additional time delay arrangement be added.

Section 5: Secure Disable Applications

As well as in conventional non-safety-related applications, Secure Disable can also be used in any position where contactors or safety contactors with connected movement are used to achieve safe disable.

The following examples correspond to the relay logic arrangements described in the previous section as cases 1, 2 and 3.

Case 1 - Simple stop/start control to EN954-1 Cat1



Electromechanical *With Unidrive SP Secure Disable*

Figure 5A: Simple hard-wired stop/start control using Secure Disable to EN954-Cat 1

The benefits of using Secure Disable on the Unidrive SP are:

- ✓ Power contactor replaced by a signal relay (Cost and Space saving)
- ✓ Drive can now have power applied continuously, so that its auxiliary functions remain active
- ✓ 24V dc logic supply can be taken from the drive, eliminating an external supply (Cost and Space saving)

Case 2 - Interlock (previously with feedback) to EN 954-1 Cat 2

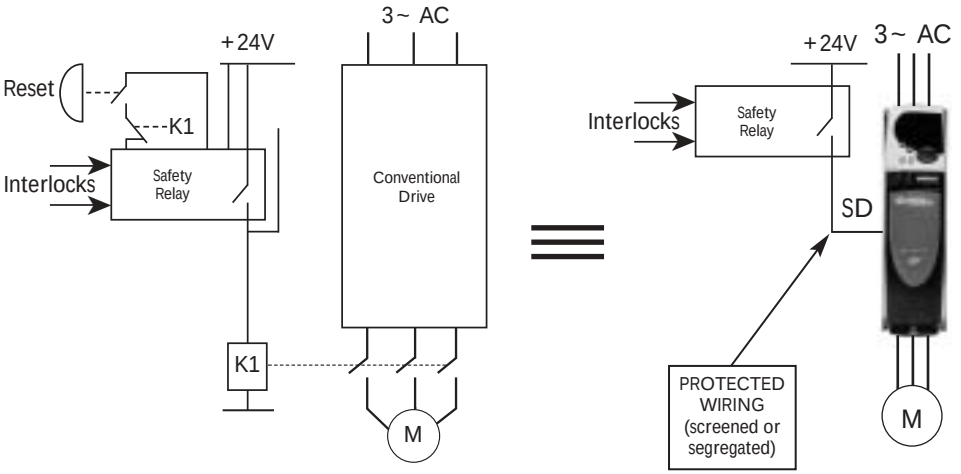


Figure 5B: Secure Disable used in place of contactor having contacts with connected movement acheiving EN954-1 Cat 2

The failure mode where the relay closes (or stays closed) when not energised no longer exists, so the feedback contact is not required. The enable input wiring has to be protected in order to avoid the possibility of a short circuit to a positive d.c. supply or digital logic signal which could cause inadvertent enable. Protection is achieved either by ensuring physical separation from all other circuits or else by the use of a cable with an earthed screen so that a short circuit always results in an earth fault and a loss of the logic signal (see prEN 954-2).

The benefits of using Secure Disable are:

✓ Power contactor (with connected movement) eliminated (cost and space saving)

✓ Feedback checking arrangement eliminated

✓ No need for drive early-disable arrangement.

The additional cost of arranging protected wiring for the drive enable input is small compared with these benefits.

Case 3 - Fail-safe interlock (previously with feedback) to EN954-1 Cat 3

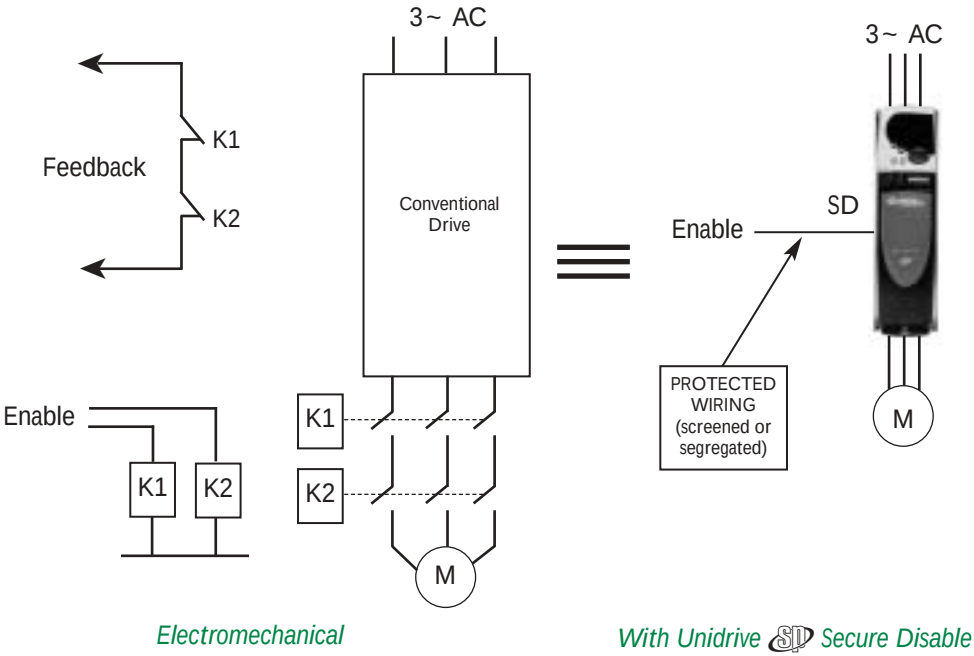


Figure 5C: Secure Disable used for fail-safe application to replace two contactors having contacts with connected movement achieving EN954-Cat 3

Again the failure mode where a relay closes (or stays closed) when not energised no longer exists, so the feedback contacts are not required. This also means that in order to achieve EN 954-1 category 3 it is no longer necessary to provide two channels for interrupting the power, because no single faults cause the motor to be driven. As in the previous case, the enable input wiring has to be protected in order to avoid the possibility of a short circuit to a positive d.c. supply or digital logic signal which could cause inadvertent enable.

The benefits of using Secure Disable are:

✓ Two power contactors with connected movement eliminated (cost and space saving)

✓ Feedback checking arrangement eliminated

✓ no need for drive early-disable arrangment.

Again the additional cost of arranging protected wiring for the drive enable input is small compared with these benefits.

Category 4 applications EN954-1

Secure Disable alone meets the requirements of category 3. It can form part of a category 4 application. The additional requirements are:

– A further channel for inhibiting motor operation in the event of an accumulation of faults, for example a contactor with contacts having connected movement and a test arrangement.

– A method for testing that Secure Disable is intact. This can be done by testing that no voltage is present at the SD input, since the only credible failure modes result in voltage appearing at that point. The test can be done by a conventional relay, but the relay must itself be tested.

For an electromechanical system, the arrangement is the same as for case 3. The difference from category 3 applications is in the degree of checking in the control circuit which provides the two inhibit channels.

Figure 5D shows a possible arrangement. “Feedback 1” is used in the same way as for the electromechanical systems in section 3, allowing a test of the safety function whenever the control relay (or other control circuit) is reset. “Feedback 2” is used to test the monitoring relay, for example it may be included to latch in a start circuit so that if the relay does not operate the circuit fails to latch. In an electronic control system, this feedback could be provided by a logic input on the controller.

Case 4 Secure Disable used in EN954-1 Cat 4 applications

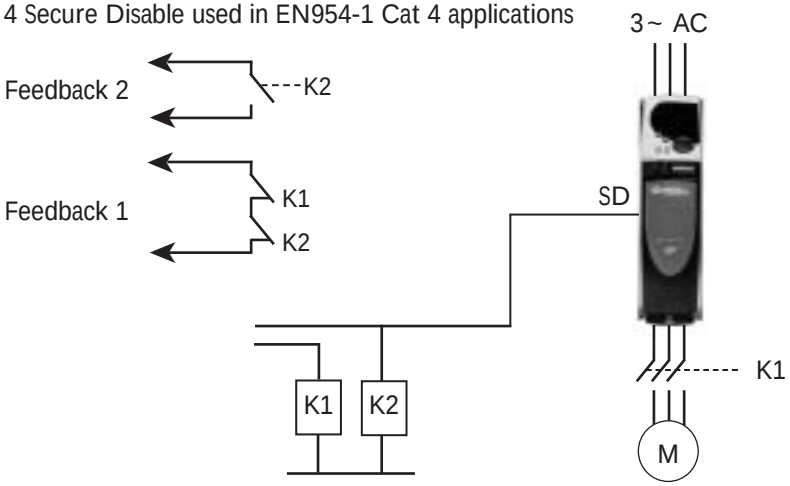


Figure 5D: Secure Disable used for EN954-1 category 4

The benefits of Secure Disable are:

✓ Power contactor with connected movement replaced by relay or controller logic input (cost and space saving)

✓ No need for drive early-disable arrangement.

Provision of electronic braking for rapid stop

As explained in section 4, the drive is capable of active braking through the motor, but this is not a high-integrity function. Where braking is desirable, such as in an emergency stop function, but the actual safety function is the removal of power from the motor, a time delay is required between instructing the drive to stop and then disabling it.

A fail-safe time delay relay can be used for this function, as shown in Figure 5E. Safety relay ranges (such as those from Pilz GmbH) include relay expansion units with a delay feature. In this arrangement the drive brakes as soon as the gate is opened, and is disabled securely after the delay relay de-energises.

It must be emphasised that if braking is itself a safety requirement, i.e. if the braking does not operate then there is an unacceptable risk of injury, then a fail-safe brake must be provided, such as a mechanical brake with electrical hold-off.

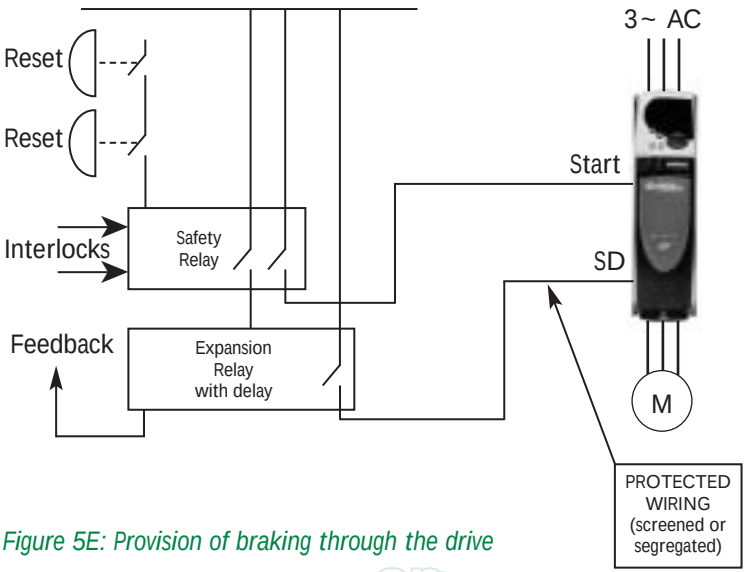


Figure 5E: Provision of braking through the drive

Appendix 1: Other standards

This guide is based on the standards which are listed in the Official Journal of the European Communities under the Machinery Directive, and primarily on EN 954-1. This is the preferred standard for the design of safety-related control systems of machines for supply within the EU, which when used with other relevant harmonised standards gives the "presumption of conformity" with the essential requirements of the Directive. It is also widely used outside of Europe since until recently there have been no generally applicable international standards.

The field of safety-related control systems has been changing in recent years, driven most particularly by the move towards incorporating software into safety arrangements. This has caused a review from first principles of safety-related control design, leading to the publication of a new 7-part family of standards in the IEC 61508 series (and their EN equivalents) "Functional safety of electrical/electronic/programmable electronic safety-related systems". A key difference from the foregoing standards is the use of numerical indications of risk, leading to the concept of a "Safety Integrity Level" (SIL) for systems and sub-systems, which can be used in the design and specification of safety-related parts. It is intended that future specific sector standards will be based on and fully compatible with this family of basic standards, and already two relevant standards are in preparation:

(future) IEC 62061 Safety machinery - Functional safety of electrical, electronic and programmable control systems for machinery

(future) IEC 61800-5-2 Adjustable speed power drive systems - safety requirements - functional safety

It is expected that in due course these standards will be published as European harmonised standards and listed in the OJ under the Machinery Directive. Given the complexity of the subject and the difficulty in changing product design procedures to meet new standards, this is likely to happen some years in the future.

IEC 62061 will eventually, as EN 62061, replace EN 954-1, and this may well require a review of machine control system design.

It is not entirely clear how IEC 61800-5-2 will integrate with machinery safety standards, since a "power drive system" is invariably part of a machine and therefore IEC 62061 will always apply to the overall safety-related control system. The expectation is that since both standards are based on the same basic standard IEC 61508, they will use the same philosophy and metrics and therefore be fully compatible. In that case IEC 61800-5-2 can be used for a purchasing specification for drives and drive systems which have a role in the safety of the machine.

References

Croner's Industrial Equipment Safety. Croner Ltd. www.croner.co.uk
- a comprehensive guide to the legal and managerial issues relating to machinery safety. With subscription update service.

BIA Report: Categories for safety-related control systems in accordance with EN 954-1. ISBN 3-88383-528-5. HVBG www.hvbg.de
- a guide to EN 954-1 with examples using electrical, electronic, pneumatic and hydraulic control, lists of faults and excluded faults etc.

Pilz Guide to machine safety. www.pilz.com
- a guide with numerous electrical examples. Also covers US standards.

EN 954-1:1997 Safety of machinery. Safety related parts of control systems. General principles for design.

prEN954-2 Safety of machinery. Safety-related parts of control systems. Part 2. Validation. Available in the UK from BSI as a draft for public comment 99/717672 DC. Publication in final form expected late 2002.

driving the world...

Control Techniques
Drive & Application Centres

AUSTRALIA
Melbourne Application Centre
A.C.N. 003 815 281
Tel: 61 3 9563 4550
Fax: 61 3 9563 4545

Sydney Drive Centre
A.C.N. 003 815 281
Tel: 61 2 9838 7222
Fax: 61 2 9838 7764

AUSTRIA
Linz Drive Centre
Tel: 43 7229 789480
Fax: 43 7229 7894810

BELGIUM
Brussels Drive Centre
Tel: 32 2725 2721
Fax: 32 2725 4940

CANADA
Toronto Drive Centre
Tel: 1 905 475 4699
Fax: 1 905 475 4694

CHINA
Shanghai Drive Centre
Tel: 86 21 64085747
Fax: 86 21 64083282

CZECH REPUBLIC
Brno Drive Centre
Tel: 420 541 192111
Fax: 420 541 192115

DENMARK
Århus Application Centre
Tel: 45 8625 5755
Fax: 45 8625 1755

Copenhagen Drive Centre
Tel: 45 4369 6100
Fax: 45 4369 6101

FINLAND
Helsinki Drive Centre
Tel: 358 985 2661
Fax: 358 985 26823

FRANCE
Leroy Somer
Angoulerne Drive Centre
Tel: 33 5 4564 5454
Fax: 33 5 4564 5400

GERMANY
Bonn Drive Centre
Tel: 49 2242 8770
Fax: 49 2242 877277

Chemnitz Drive Centre
Tel: 49 3722 52030
Fax: 49 3722 520330

Darmstadt Drive Centre
Tel: 49 6251 17700
Fax: 49 6251 177098

Stuttgart Drive Centre
Tel: 49 7156 95560
Fax: 49 7156 955698

HOLLAND
Rotterdam Drive Centre
Tel: 31 1844 20555
Fax: 31 1844 20721

HONG KONG
Hong Kong Application Centre
Tel: 852 2979 5271
Fax: 852 2979 5220

HUNGARY
Budapest Drive Centre
Tel: 361 431 1162
Fax: 361 260 5483

INDIA
Bombay Drive Centre
Tel: 91 212 751201/751202/750930
Fax: 91 212 750105

Madras Drive Centre
Tel: 91 44 4961123/
4961130/4961083
Fax: 91 44 4961602

New Delhi Application Centre
Tel: 91 44 581 3626
Fax: 91 44 581 3626

INDONESIA
Jakarta Drive Centre
Tel: 62 21 4525146
Fax: 62 21 4525142

Surabaya Application Centre
Tel: 62 31 5682775/5623565
Fax: 62 31 5622402

IRELAND
Dublin Drive Centre
Tel: 353 (0) 45 433044
Fax: 353 (0) 45 433622

ITALY
Milan Drive Centre
Tel: 39 02575 751
Fax: 39 02575 12858

Vicenza Drive Centre
Tel: 39 0444 396200
Fax: 39 0444 341317

KOREA
Seoul Application Centre
Tel: 82 2 3445 6183/6184/6185
Fax: 82 2 3445 6181

MALAYSIA
Kuala Lumpur Drive Centre
Tel: 60 3734 9776
Fax: 60 3733 9592

REPUBLIC OF SOUTH AFRICA
Johannesburg Drive Centre
Tel: 27 11 462 1740
Fax: 27 11 462 1941

RUSSIA
Moscow Application Centre
Tel: 7 095 245-8631 (89)
Fax: 7 095 956-4862

SINGAPORE
Singapore Drive Centre
Tel: 65 271 6377
Fax: 65 272 1302

SPAIN
Barcelona Drive Centre
Tel: 34 93 680 1661
Fax: 34 93 680 0903/2823
/34 93 680 0763

Bilbao Application Centre
Tel: 34 94 620 3646
Fax: 34 94 681 1406

Valencia Drive Centre
Tel: 34 96 1542900
Fax: 34 96 1532906

SWEDEN
Stockholm Drive Centre
Tel: 46 8 58 352045
Fax: 46 8 58 353223

SWITZERLAND
Lausanne Application Centre
Tel: 41 21 634 0408
Fax: 41 21 635 8596

Zurich Drive Centre
Tel: 41 56 201 4242
Fax: 41 56 201 4243

TAIWAN
Taipei Application Centre
Tel: 886 22325 9555
Fax: 886 22705 9131

THAILAND
Bangkok Drive Centre
Tel: 66 2580 7644
Fax: 66 2591 4559

TURKEY
Istanbul Drive Centre
Tel: 90 216 4182420
Fax: 90 216 4182423

UNITED KINGDOM
Birmingham Drive Centre
Tel: 44 121 544 5595
Fax: 44 121 544 5204

Leeds Drive Centre
Tel: 44 113 2423400
Fax: 44 113 2423892

Luton Drive Centre
Tel: 44 1582 567700
Fax: 44 1582 567703

Warrington
Application Centre
Tel: 44 1925 413537
Fax: 44 1925 242808

USA
Charlotte
Application Centre
Tel: 1 704 393 3366
Fax: 1 704 393 0900

Chicago Drive Centre
Tel: 1 630 893 5249
Fax: 1 630 893 4156

Cleveland Drive Centre
Tel: 1 440 717 0123
Fax: 1 440 717 0133

Dallas Application Centre
Tel: 1 972 783 1831
Fax: 1 972 783 9978

Minneapolis Drive Centre
Tel: 1 612 474 1116
Fax: 1 612 474 8711

Providence Drive Centre
Tel: 1 401 333 3331
Fax: 1 401 333 6330

San Francisco Application Centre
Tel: 1 510 264 4940
Fax: 1 510 264 4949

VIETNAM
Ho Chi Minh Application Centre
Tel: 84 8 842 5157
/84 8 849 1980
Fax: 84 8 842 5157

CONTROL TECHNIQUES

www.controltechniques.com

0175-0305 03/99