



Control Techniques Safe Torque Off

A guide to the application
of the Control Techniques
Safe Torque Off safety function
and its compliance with
IEC 61800-5-2



This guide is one of a series covering subjects such as harmonics, safety features, EMC, feedback devices, industrial communications and motion control.

These can be accessed via www.controltechniques.com/guides.

Contents

	Page
1 Quick overview	4
2 Principles of machinery safety design	6
General principles	6
Risk assessment	6
Responsibilities	7
Standards for machinery control equipment	7
Note on Safety Integrity Level (SIL) and related data	8
3 Safety controllers using electromechanical components	9
General principles	9
Location of contactors when using drives	10
4 Control Techniques Safe Torque Off - how it works	11
Capabilities	12
Limitations	13
Approvals and conformity with standards	13
Why is there no relay and no feedback signal with Control Techniques Safe Torque Off?	14
5 How to apply Safe Torque Off	16
Single channel interlock with feedback	17
Two-channel interlock with feedback	19
Use of contactor for a second channel	20
Provision of electronic braking for rapid stop	21
6 Application of standards	22
7 Lift (Elevator) applications	22
8 Compatibility with safety digital outputs	23
9 Paralleling	23
10 Specification	23
11 Third party approvals	25
12 Glossary	25
13 References	27

1 Quick overview

Safe Torque Off (STO) is a functional safety feature which complies with IEC 61800-5-2 and is built in to Control Techniques Unidrive SP and Digitax ST drive products as standard. It allows the drive output to be disabled so that the drive cannot generate torque in the motor. In the absence of a +24V “Enable” input, the drive is disabled to a high degree of integrity, where no single component failure, and only very unlikely combinations of three component failures, could result in it being enabled. The drive can therefore be used as the final actuator in a machinery safety application to prevent unintended operation of the motor, typically as part of an interlock system, in place of the more conventional arrangements of contactors with cross-checking auxiliary contacts.

Unidrive SP



Digitax ST



The enable input operates exactly the same as a non-safety input and can be used for any of the usual applications, but in addition it has this high integrity property which allows it to be used for safety functions.

The reliability of STO is superior to that offered by any single channel electromechanical device such as a contactor. It is like having a special high integrity contactor built into the drive output, but there are no moving parts, no extra cost, and no difficulty over contact arcing if the drive is disabled on load. It offers the possibility of eliminating contactors, including special safety contactors, from systems where the prevention of unintended running is important to prevent safety hazards or expensive damage to plant or materials.

The term “Safe Torque Off” is defined in the standard for safety functions in adjustable speed drives, IEC 61800-5-2 (EN 61800-5-2). Before this standard was published this function was already provided in Control Techniques Unidrive SP products and named “Secure Disable” (SD). Both of these terms describe the exact same safety function, i.e. a function whereby when the “Enable” input is disconnected or set at a logic “low” value, the drive will not produce torque in the motor, with a very high level of integrity.

Note on emergency stop functions

Confusion can occur if the STO function is looked upon as an emergency stop function (E-stop). Depending on the standards and requirements for a particular application, it might be possible to use STO as part of an E-stop system. However its main purpose is for use in a dedicated safety control arrangement whose purpose is to prevent any hazard from occurring, without the use of an E-stop. An E-stop is often provided in a machine to allow for unexpected situations where an operator sees a hazard and can take action to prevent an accident. The design requirement for an E-stop is different from a safety interlock, generally it is required to be independent from any complex or “intelligent” control, and it may be required to use purely electromechanical devices to disconnect the power - in which case STO is not suitable.



Important warning

The design of safety-related systems requires specialist knowledge. To ensure that a complete control system is safe it is necessary for the whole system to be designed according to recognised safety principles. The use of individual sub-systems such as drives with Safe Torque Off functions, which are intended for safety-related applications, does not in itself ensure that the complete system is safe.

The information given in this publication gives guidance on the application of Control Techniques Safe Torque Off, and also some general background material on the design of safety-related systems for machinery control. This publication is not intended to form a complete guide to the subject. Some more detailed references are given at the end of the guide. The information provided is believed to be correct and to reflect accepted practice at the time of writing. **It is the responsibility of the designer of the end product or application to ensure that it is safe and in compliance with the relevant regulations.**

Section 2 of this guide gives an outline of the design principles for safety functions of machines, which sets in context the material in the later sections. If you are familiar with this subject we suggest you move on directly to section 3.

For further information on the Unidrive SP and Digitax ST drive families, refer to the following:

- Unidrive SP brochure
- Unidrive SP Free Standing brochure
- Unidrive SPM brochure
- Digitax ST brochure



2 Principles of machinery safety design

General principles

The design of safe machinery is a complex process which requires attention from the very beginning. This part of the guide gives a brief overview, which is intended to explain how the use of Control Techniques Safe Torque Off fits in to the overall scheme of safe machine design.

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 or safeguards which prevent the machine from functioning when entry or access is possible, e.g. through the opening of a guard etc. More complex 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 standards (CEN) 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”, which are supported by more detailed standards which focus on specific aspects of safety (“B standards”) or specific types of machine (“C standards”). Note that these standards originate with the international body ISO and have been adopted directly as EN standards for application under the EU Machinery Directive.

“A standards”:

EN ISO 12100–1	<i>Safety of machinery – Basic concepts, general principles for design</i> Part 1: Basic terminology, methodology
EN ISO 12100–2	<i>Safety of machinery – Basic concepts, general principles for design</i> Part 2: Technical principles and specifications
EN ISO 14121-1	<i>Safety of machinery. Risk assessment. Principles</i>
ISO TR 14121-2	<i>Safety of machinery. Risk assessment. Practical guidance and examples of methods</i> (This proposed standard was intended to supplement ISO 14121-1 but is not presently accepted by some safety bodies so it has the status of a Technical report only and is not harmonised.)

The initial risk assessment will indicate whether unacceptable risks exist which need to 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 safety-related control system will have been defined.

Responsibilities

From the above outline it should be 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 machinery control equipment

The applicable standards have undergone considerable changes in recent years, both through efforts towards global harmonisation and also the introduction of newer standards which use quantitative methods and allow for the application of software and complex hardware in safety-related applications. The new standards are based on the methods and requirements of an important basic standard IEC 61508 *Functional safety of electrical/electronic/programmable electronic safety-related systems*. The following notes give some guidance on aspects of standards relevant to drive applications. Generally the standards are referred to without dates, except where some important changes have occurred between versions.

IEC 60204-1 *Safety of machinery. Electrical equipment of machines. General requirements*

This is identical in content with EN 60204-1 and also closely related to NFPA79. This standard does not directly define integrity requirements for safety-related control systems, but it does include important definitions for aspects such as methods of stopping a machine and emergency stop facilities. The requirement in earlier versions that the removal of power from a machine following an emergency stop should be by electromechanical means has recently been removed.

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

This standard had an international version ISO 13849-1:1999, which is now obsolete, and EN 954-1 is withdrawn at the end of 2009. This standard and its previous version were used for many years as the basis for classifying safety-related controllers. It gives integrity categories increasing from 1 to 4 together with guidelines on the level of risk reduction offered. It cannot be applied to equipment using software for safety functions, nor complex hardware if it is not amenable to FMEA. Although obsolescent, the EN 954 concept of integrity categories is likely to persist for some years.

EN ISO 13849-1:2006 *Safety of machinery. Safety-related parts of control systems.*

General principles for design

This standard replaces EN 954-1 and ISO 13849-1:1999 but is fundamentally different from them and is based on IEC 61508 principles. It uses a “Performance Level” as an indicator of integrity, with levels increasing from (a) to (e). Unlike the following standards, it allows for the use of mechanical, hydraulic and pneumatic control methods. It is supplemented by EN ISO 13849-2:2008 *Validation*, which gives detailed guidelines such as fault exclusion lists for commonly-used machinery components..

IEC 62061 *Safety of machinery. Functional safety of safety-related electrical, electronic and programmable electronic control systems* (and EN 62061)

This standard overlaps with ISO 13849-1:2006 to some extent, and is cross-referenced within it. It is based on IEC 61508 and uses the SIL measure of integrity. It allows for the use of software and complex hardware in machinery safety functions.

IEC 61800-5-2 *Adjustable speed electrical power drive systems. Safety requirements.*

Functional (and EN 61800-5-2)

This standard specifically relates to drives which offer safety functions. It uses the same SIL measure of integrity as IEC 62061 and is therefore directly compatible with it. In practice it can also readily be integrated with approaches using ISO 13849-1:2006.

Note on Safety Integrity Level (SIL) and related data

SIL can take values from 1 to 4, with machinery applications being restricted to a maximum level of 3. In principle a SIL can only be allocated to a complete safety-related electrical/electronic control system (SRECS), and not to sub-systems or components. This is because only once the whole system is designed and placed in its context with defined safety requirements can its capability be properly analysed. In practice it is necessary to provide information regarding the safety integrity contribution which a sub-system can offer, and this is generally referred to as a “SIL capability”. The implication is that the capability can only be realised by appropriate incorporation into a complete SRECS.

In addition to a SIL capability, the sub-system must also have a value for the probability of failure of hardware in the dangerous direction - referred to as PFH or PFH₀¹. This data has to be combined with the corresponding data for other sub-systems to calculate an overall PFH₀ for the complete SRECS.

¹Probability of Failure of Hardware (Dangerous) - per hour

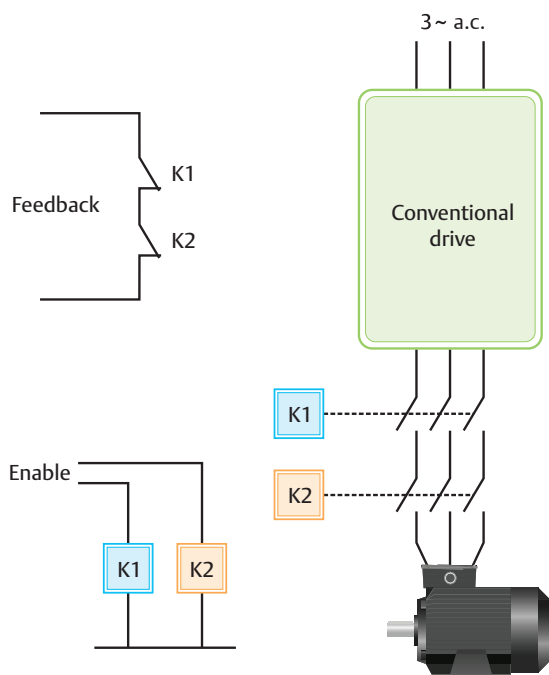
3 Safety controllers using electromechanical components

The purpose of this section is to explain how a STO function is realised using conventional electromechanical components, in order to show how a STO function in the drive can replace and give better performance than an electromechanical arrangement.

General principles

Generally the machine motor is a three-phase a.c. motor, which may be connected directly to a 3-phase a.c. supply, or through an a.c. variable speed drive. In either case the method for preventing unwanted torque is to interpose an electromechanical contactor to separate the motor from its supply when the contactor coil is disconnected. When a drive is used the contactor might be placed in the input or the output, the choice is discussed later.

Figure 1: Safety-related disable function implemented using contactors



Since the three-phase supply is always present and capable of generating a rotating magnetic field in the motor and developing continuous rotating torque, it is only the separation of the contactor contacts which prevents torque. Therefore the failure modes of the contactor must be analysed, and in a case where a failure is likely to result in injury it is necessary to ensure that a single contactor failure cannot result in a loss of the safety function. This means that typically two contactors must be used in series, and both contactors must be monitored in order to detect an unsafe failure and arranged so that a single failure prevents the second contactor from closing. Figure 1 illustrates this technique.

Safety relays are available which carry out the monitoring and management of series contactors, and offer for

example two-channel redundant inputs to maintain this redundant approach throughout the safety chain. A system of this kind can be made to meet the requirements of EN 954-1 category 4, where it is necessary for no single fault to result in a loss of the safety function, and for all faults to be revealed (i.e. an unrevealed fault cannot remain undetected and later combine with a single additional fault to result in a loss of safety function).

Location of contactors when using drives

When contactors are used with a.c. drives there is a choice of locating them either at the drive input or output. There are advantages and disadvantages to both arrangements, but one very important stipulation must be made if the contactors are to be located at the drive output: the contactors must not be opened when motor current is present, because of the risk of severe arcing if the output frequency is low when trying to interrupt the inductive circuit.



Warning

A.c. contactors are designed to interrupt a.c. current at typically 50 or 60 Hz. They rely on the current being interrupted every half-cycle to extinguish the arc formed when the contact opens the current. When connected to a drive output the frequency can vary over a wide range down to 0Hz (d.c.), so it is essential that the drive output current be reduced to zero before the contactors open. This can be achieved by disabling the drive and allowing time for the current to decay. Failure to observe this requirement may result in a dangerous situation. Sustained d.c. arcing might cause a fire risk, but also it could result in welding of contacts, which represents a potential common mode of failure of both contactors and could result in the loss of the safety function.

By incorporating the STO function within the drive, using solid-state components, the costs and risks of contactors can be avoided.

4 Control Techniques Safe Torque Off - 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.

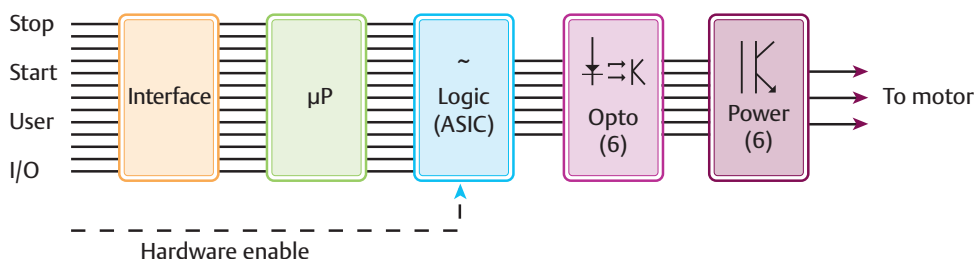
(Note when a permanent magnet motor such as a servo motor is used, a single transient alignment torque could be produced by a multiple IGBT failure. The motor could rotate by a maximum $360^\circ/p$ (where p is the number of poles.))

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 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.

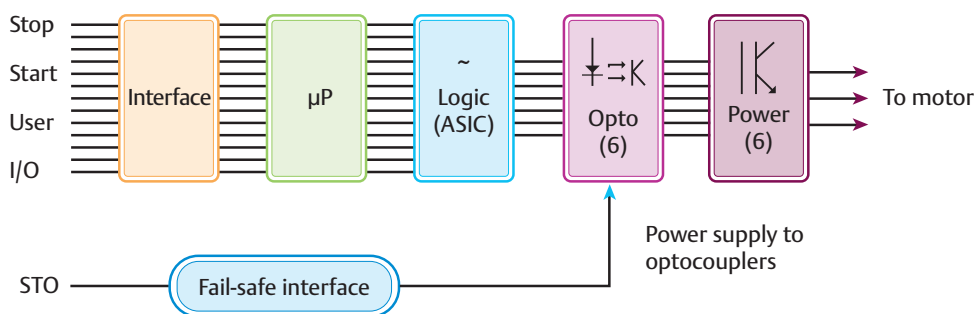
In some conventional drive designs a “hardware enable” input is provided which operates through some simple electronic logic to prevent the operation of the power stage, as illustrated in Figure 2. The disable function provided by this arrangement is likely to be more reliable than one operating through 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 2: Conventional drive hardware enable



The switching signals are conveyed from the complex control circuit to the IGBTs by optocouplers which use light-emitting diodes (LEDs) to transmit simple on/off commands across the electrical isolation barrier. In the Safe Torque Off arrangement shown in Figure 3, 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.

Figure 3: Safe Torque Off



Capabilities

Safe Torque Off performs a safety function such that when the Enable input is not asserted, i.e. open-circuit or set at nominally 0V, the drive will not develop torque in the motor.

Control Techniques STO is implemented purely in simple solid state hardware for which substantial failure data exists, allowing meaningful quantitative FMEA to be carried out. The function does not use software or complex hardware.

The probability of failure of the safety function due to a hardware fault has been estimated by Control Techniques Ltd as 8×10^{-10} per hour, and assessed by the independent notified body BGIA as less than 10^{-8} per hour, which is the lowest value considered in IEC 62061 and IEC 61800-5-2.

The input is compatible with self-testing digital outputs of controllers such as PLCs, where the test pulse is a maximum of 1ms. This means that the drive is not disabled by logic-low input pulses with a maximum of 1ms duration.

The state of the enable input can be monitored through parameter **8.09**.

Limitations

- STO uses solid-state techniques, it does not provide physical separation of electrical connections and is not intended to provide electrical isolation.
- STO does not provide braking, it disables the drive and motor so no motor braking is available. If motor braking is a requirement then an external arrangement must be made to stop the drive conventionally and then to safely remove the enable input to activate STO. Time-delay safety relays are available for this task. Braking by the drive is not a high-integrity function, if braking is a safety requirement then an independent fail-safe brake must be provided.
- STO offers a single input channel, so that a single fault in the external circuit which unintentionally energises the input within its operating voltage range could cause a failure of the safety function. The wiring connected to the enable input must be protected from faults which might unintentionally energise it. According to EN ISO 13849-2 this can be achieved by physical separation of wiring or by using a shielded wire with the shield connected to ground/logic low. Alternatively the state of the input can be monitored and the system disabled by an independent route if an error is detected.
- When using a permanent-magnet motor, there is a small possibility that a fault in the drive power stage could result in a momentary alignment torque in the motor, i.e. the motor might attempt to turn by one electrical pole pitch. For this to happen, IGBT devices or their drivers in opposite poles of two arms of the three-phase inverter bridge would have to fail in the short circuit mode during a single period when the drive was disabled. If the drive were to be run after one IGBT failure then the fault would be revealed because the drive would trip, since it cannot run with a short-circuit IGBT. Running the drive is in effect a proof test and the risk of a double IGBT failure is only significant in applications where the drive spends long periods disabled (i.e. weeks or months). The drive has been extensively tested and no common cause failure mode has been found which could result in such a double failure, but it is recommended that this possible failure mode be taken into account when a permanent-magnet motor is used.

Approvals and conformity with standards

The Safe Torque Off function conforms to the following standards:

EN 954-1:1997 category 3 *Safety of machinery. Safety related parts of control systems.*

General principles for design - Independently approved by BGIA (previously known as BIA)

IEC 61800-5-2:2007 (EN 61800-5-2:2007) *Adjustable speed electrical power drive systems.*

Safety requirements. Functional.

SIL = 3 PFH = 0 (as assessed by BGIA. Actual value is negligible, i.e. $<10^{-8,2}$)

Independently approved by BGIA

² Control Techniques estimate 8×10^{-10}

EN ISO 13849-1:2006 *Safety of machinery. Safety-related parts of control systems. General principles for design.*

$PL = e \text{ MTTF}_D > 10^5 \text{ yr}$ (assumed mission time 20 yr) – Independently approved by BGIA

EN 81-1:1998 clause 12.7.3 *Safety rules for the construction and installation of lifts. Electric lifts*
- Independently approved by TÜV Süd & TÜV Nord

Standard IEC 61800-5-2 uses the same parameters as standards IEC 62061 and IEC 61508 (-1 to -7) (and their EN equivalents) for indicating safety integrity, i.e. SIL or SILCL (SIL capability level) and PFH or PFH_D (probability of dangerous failure, per hour). Therefore the data provided under this standard can be used to incorporate STO into systems which have been designed according to those related standards.

Why is there no relay and no feedback signal with Control Techniques Safe Torque Off?

Safe Torque Off has been designed into specific Control Techniques drives 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 at lower cost.

Some STO systems use relays to interrupt the power supply to the gate drive opto-couplers and to provide galvanic isolation. This is illustrated in Figure 4 , which includes a typical external monitoring 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 guided contact 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 4: Typical drive disable function using relay having guided contacts

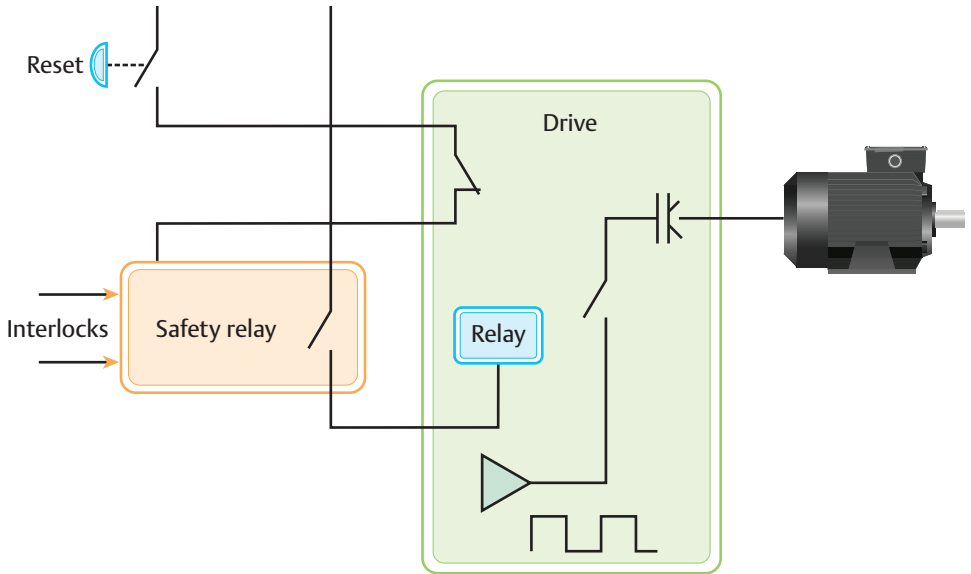
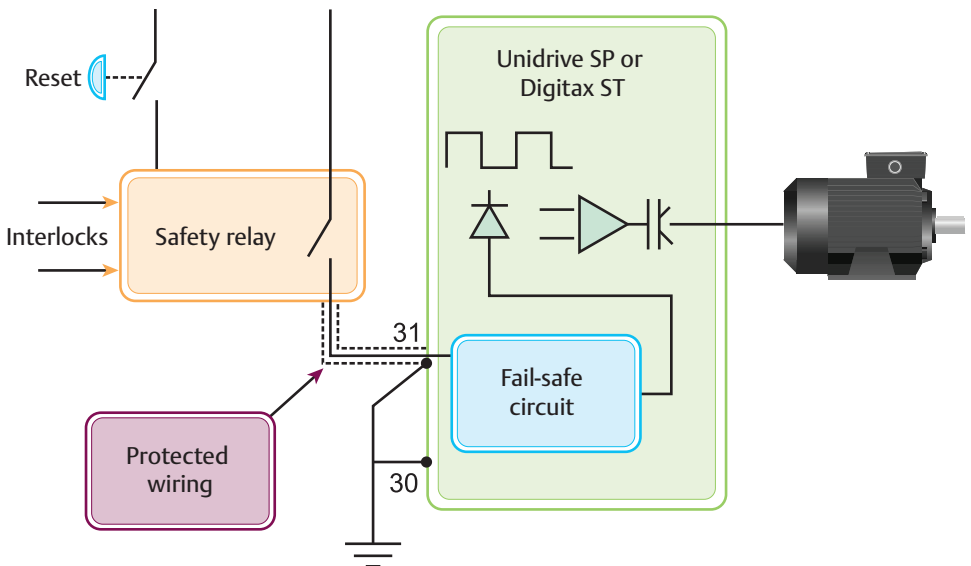


Figure 5: Safe Torque Off in a typical safety circuit



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. Safe Torque Off uses a fully solid-state circuit which avoids this problem. The only disadvantage of STO is that a wiring fault in the single input channel would not be detected. This can be excluded under EN ISO 13849-2 by the use of protected wiring, as illustrated in Figure 5.

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.

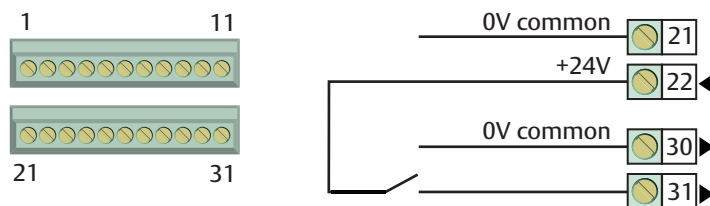
or

Shielded, with the shield connected to ground, in a positive-logic grounded control circuit

5 How to apply Safe Torque Off

Safe Torque Off 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 6: Control connections, showing Enable input (Terminal 31) for Safe Torque Off function

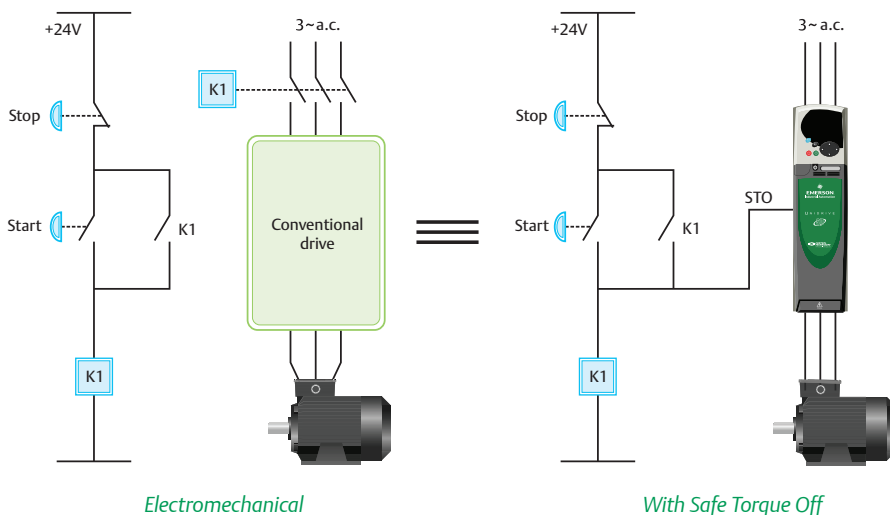


The only difference from other drive digital inputs is that the Enable input cannot be configured to operate with negative logic. This is a requirement of most standards and conventions for safety functions, which ensures that an earth fault in the control circuit results in a safe failure (drive disabled).

STO 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. STO can eliminate the use of a contactor.

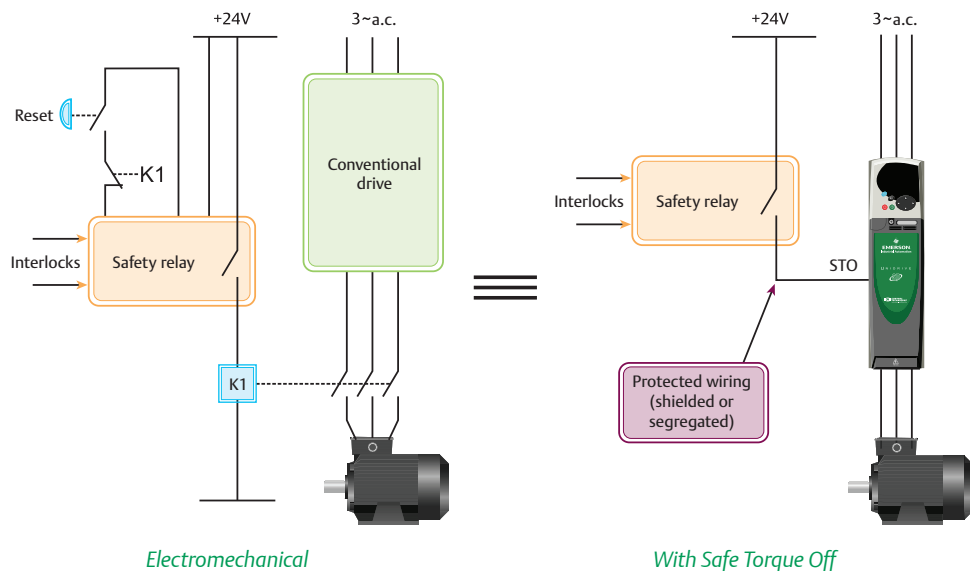
In the following examples, the diagrams show a typical implementation using electromechanical devices, contrasted with an implementation using STO. The diagrams are intended to illustrate methods of application and principles. They are not complete detailed designs. In every case it is the machine designer's responsibility to carry out a risk analysis and to ensure that the complete machine, and the safety-related control system of the machine, meet the required design criteria for functional safety.

Figure 7: Simple stop/start control - no SIL capability



The power contactor is replaced here by a signal relay, saving in space and power wiring and allowing the drive power to remain connected when the machine is not running.

Figure 8: Single channel interlock with feedback - SIL1 capability



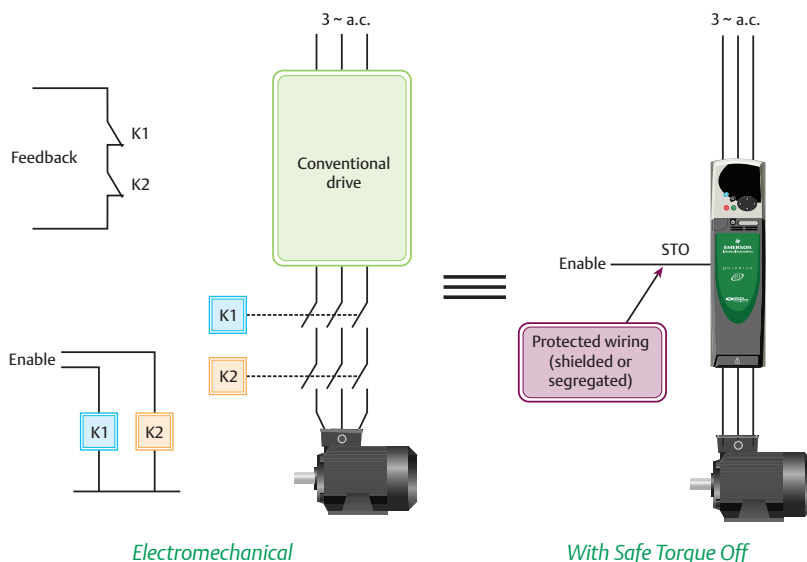
In this example, the electromechanical arrangement has a safety relay which monitors an interlock network, and also monitors the correct operation of the output contactor which disconnects the motor. If the contactor fails in the dangerous direction then the safety relay cannot be reset, but operator action is required in order to prevent further running of the machine. This is suitable for protecting a machine where the interlocks are regularly exercised, so that a failure of the contactor would be revealed without causing a hazard.

With Safe Torque Off the contactor is eliminated. Since STO has no failure mode equivalent to the contactor sticking closed, there is no need for contactor monitoring. If the relay or safety controller requires feedback, this can be arranged from a drive digital output using parameter **8.09**³.

The wiring from the relay to the STO (Enable) input on the drive must be protected, as discussed in chapter 4.

³ The monitoring path is not of high integrity, but this has no impact on the overall risk analysis because of the very low PFH for STO.

Figure 9: Two-channel interlock with feedback - SIL3 capability

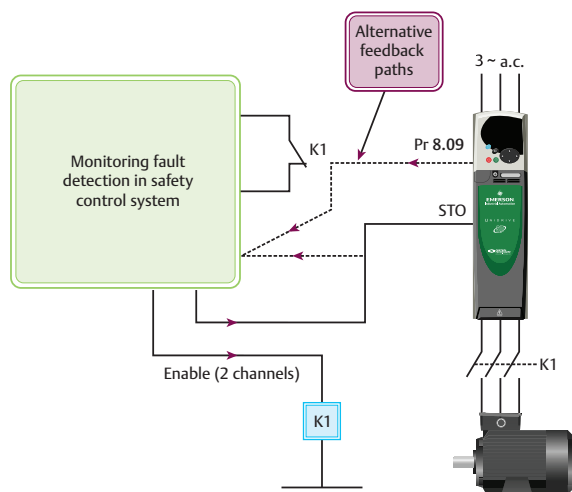


In this example the electromechanical implementation uses two contactors in series, each with monitoring contacts which are used to provide feedback to the safety controller (not shown) to detect a contactor fault. In this case if a single contactor fails then this is detected and the system remains safe because the other contactor prevents application of power to the motor.

With Safe Torque Off both contactors are eliminated. The integrity of STO is equivalent to that of the two contactors with fault detection. In order for this to be maintained it is clearly essential that the wiring protection and the source of the “Enable” signal should be of corresponding integrity.

As an alternative to relying on protection of wiring, or if the system risk analysis demands a two-channel architecture, the arrangement shown in Figure 10 can be used.

Figure 10: Use of contactor for a second channel - SIL3 capability



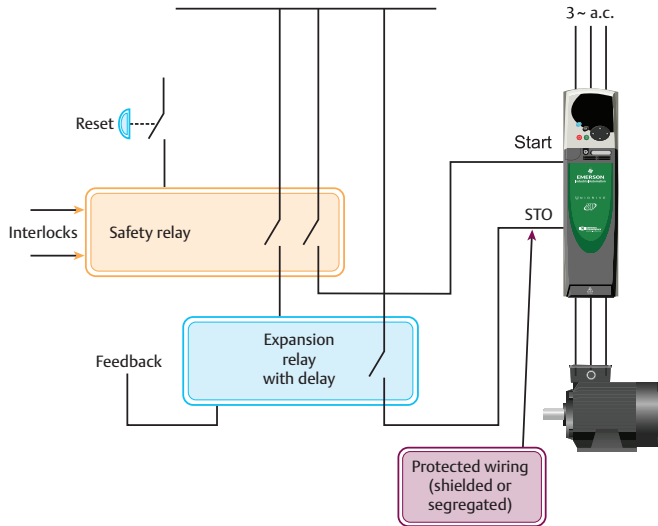
Where the safety control system design requires two channels for the STO function, one channel can be implemented by Control Techniques STO and the other by a contactor, which may be connected in either the drive input or output power circuits.

The contactor must be monitored through an auxiliary guided contact, shown as K1 in the diagram.

The drive STO input can be monitored in several possible ways. The diagram illustrates a monitor connection (shown dashed) to the safety controller. This could be through using a safe digital output on a safety controller, with built-in monitoring, or by a safe digital input. Alternatively a digital output of the drive could be used to provide the monitoring feedback, linked to parameter **8.09**.

In the diagram the contactor is shown as dedicated to the one particular drive. Alternatively where a safety controller is used to carry out multiple functions it may be arranged to open a single overall contactor which provides power to all drives, in the event of a fault being detected anywhere in the system.

Figure 11: Provision of electronic braking for rapid stop - SIL3 capability



Where braking of the load is desirable prior to entering the STO state, the normal stop/start function of the drive can be used with the appropriate braking arrangement set up on the drive. These functions are not designed to be used in safety-related applications. The diagram shows how a separate signal from the safety relay can be used to stop the drive using the drive braking and ramping functions, by removing the “start” input. The safety relay has an expansion safety relay fitted with time delay, the output from which is connected to the drive STO input. Once the time delay has elapsed, the drive is placed securely in the STO state. Once this has happened, braking is no longer available because the motor braking facility is also disabled by STO.

Note that if the braking function is itself a safety requirement then this arrangement is not suitable, because braking requires all or most of the drive to be operational, i.e. it is not “fail-safe”. Then a more complex braking supervision function is required or alternatively a fail-safe mechanical brake.

6 Application of standards

The Control Techniques drive with Safe Torque Off is intended to be incorporated into a complete safety control system. The machine designer is responsible for specifying the required safety integrity level (SIL, PL or category) which is required from the control system. The drive with STO must then be incorporated into the control system in such a way as to achieve the required safety integrity.

The complete safety control system must be analysed to determine its integrity, using the applicable standards, taking account of the contribution of the individual components which are required to operate in order to carry out safety functions. The standards which have been applied to Control Techniques STO are compatible with the family of standards based on the IEC 61508 series, e.g. IEC 62061 and IEC 61511 as well as IEC 61508 itself, and also ISO 13849-1:2006.

For the newer standards using SIL or PL, the PFH_D or $MTTF_D$ data for the drive STO function has to be combined with the equivalent data for the other functions in the safety controller to give an overall PFH_D or $MTTF_D$. The very low value of PFH_D for Control Techniques STO means that in most cases its contribution to the overall failure rate will be negligible. In addition, architectural requirements and control of systematic failures must be considered.

Architectural requirements will decide whether typically one or two channels are to be used. Application examples are given above for both cases. For high integrity applications it is very common to require two channels, rather than rely on a very high integrity in a single channel.

Control of systematic failures is also required to be sufficient for the required integrity. Since Control Techniques STO achieves SIL3 this means that it can be incorporated into a SIL3 system, which is the highest level of safety integrity applicable to machinery safety controllers. Note that the SIL of a system cannot exceed the SILCL of its components, because of the requirement for control of systematic failures. For example, a drive offering STO at SIL2 cannot be used in a SIL3 system by adding redundant additional channels.

7 Lift (Elevator) applications

Control Techniques Safe Torque Off can be used for the prevention of unintended drive in lift (elevator) applications. It can be used directly in order to replace one of the usual two contactors which are used for prevention of drive, in accordance with European standard EN 81-1:1998 clause 12.7.3. It can also be used to replace both contactors, provided that the STO input is controlled by two series-connected relays with guided auxiliary contacts. Separate guidance notes are available from Control Techniques Ltd for lift applications.

8 Compatibility with safety digital outputs

Control Techniques Safe Torque Off has been designed to be compatible with safe digital outputs on safety controllers which use a regular test pulse to monitor for faults when the output is set high (true). The maximum width of a periodic test pulse for which the drive will not be disabled is 1 ms.

9 Paralleling

Unidrive SP Safe Torque Off inputs may be connected directly together if it is required to control multiple drives from the same control line.

Connecting inputs together increases the probability of a fault in the unsafe direction, since a fault in one drive might result in all drives becoming enabled. The probability of a fault is so low, at 8×10^{-10} per hour, that the resulting probability still meets the requirements for SIL3 for realistic numbers of drives. It is recommended that no more than 12 inputs should be connected in parallel if SIL3 is required.

10 Specification

The STO input is a digital input intended for a nominal 24V d.c. input, positive logic (i.e. enabled when high).

Electrical data:

Absolute maximum voltage range	-30V to +30V
Logic threshold	15.5V $\pm$ 2.5V
Low state maximum voltage for SIL3	2V (or open-circuit)
Typical input current at +24V	3.5mA

Response time at nominal voltage:

Nominal	8ms
Maximum	20ms

Will not respond to 1 ms “disable” test pulses with frequency less than 100Hz.

EMC:

In addition to the standard immunity tests according to EN 61800-3 and EN 61000-6-2, the Safe Torque Off function has been tested at higher levels according to the following standards:

EN 61000-4-2 (electrostatic discharge)	to 15kV
--	---------

EN 61000-4-3 (RF field)	to 30V/m
-------------------------	----------

EN 61000-4-4 (fast transient burst)	to 4kV
-------------------------------------	--------

It is possible that directly coupled ESD or fast transient events at these levels might damage the drive and render it inoperable. They will not cause unintended enabling when the STO input is in the disabled state (open circuit or 0V).

Safety Specification

Safety function

When the “Enable” input is de-energised the drive will not produce torque in the motor

Fault reaction

All single component faults either have no discernible effect or else result in the drive being disabled

Fault reaction time

STO is designed to be inherently fail-safe, it does not use any form of monitoring with fault detection. There is therefore no fault reaction time.

Standards

EN 954-1:1997	Category 3
---------------	------------

EN 61800-5-2:2007	SIL3 PFH < 10^{-8} , Control Techniques estimate 8×10^{-10} Diagnostic coverage (DC) - not applicable
-------------------	--

EN ISO 13949-1 :2006	PL = e MTTF _D > 10^5 yr (based on assumed mission time of 20 years)
----------------------	---

Note : EN 954-1 category is 3 because not all faults are revealed, however under quantitative analysis the probability of an accumulation of unrevealed faults is shown by FMEA to be so low that SIL 3 and PL e are achieved.

11 Third party approvals

Specific approvals have been obtained for Unidrive SP frame sizes 0 to 6 and Digitax ST, 400V rating. The STO system is identical on all frame sizes and voltage ratings.

EN 954-1:1997 category 3	BIA (now BGIA)
--------------------------	----------------

IEC and EN 61800-5-2:2007	BGIA
---------------------------	------

ISO and EN ISO 13849-1:2006	BGIA
-----------------------------	------

BGIA is a notified under the EU Machinery Directives 98/37/EC and 2006/42/EC

Copies of approval certificates and other documents are available from Control Techniques Ltd.

12 Glossary

This is a brief glossary of important terms used in this note. For a more complete glossary consult the references or standards such as IEC 62061.

Note: In discussions of safety functions it is generally taken that a fault means a fault which tends to make a hazard more likely, i.e. faults in the safe direction are not considered unless specifically stated.

	Architectural Requirement	The requirement for the functional structure of the safety control system - typically this is a choice of the degree of redundancy and therefore the fault tolerance
	Category	A qualitative measure of safety integrity used in EN 954-1:1997. Values of B, and 1 - 4 are available
DC	Diagnostic Coverage	In systems using fault detection, this gives the proportion of faults which are detected (%)
FMEA	Failure Modes and Effects Analysis	Analysis of the effects of all component failures. This may be qualitative, i.e. a description of the effect of every fault with identification of its safety relevance, or quantitative, where component failure rate data is used to predict the probability of each failure mode. It may be restricted to the effect of single component faults only, or extended to consider accumulations of faults where the initial faults are not revealed.

	Fault Reaction	Action when a fault occurs
	Fault Reaction Time	Time between the occurrence of a fault and the fault reaction - typically the time taken to detect a fault and to take preventive action.
	Feedback	Information about the state of the controller or some part of it, used in the fault detection arrangement.
	Interlock	A structure of sensors arranged so that all have to be in a safe state in order for a particular machine function to be able to operate.
$MTTF_D$	Mean Time to Failure (Dangerous)	Mean time to failure in the dangerous direction - as used in EN ISO 13849-1:2006
	Monitoring	An arrangement for detecting faults
PL	Performance Level	Measure of the safety integrity of a control system for a machine, used in standard EN ISO 13849-1:2006. Values between a and e are available.
PFH^4	Probability of Hardware Failure	Probability of hardware failure in the dangerous direction, per hour (as used in IEC 61800-5-2)
PFH_D	Probability of Hardware Failure in the Dangerous Direction	Probability of hardware failure in the dangerous direction, per hour (as used in IEC 62061)
STO	Safe Torque Off	Safety function for power drive systems whereby the drive will not provide energy to the motor which can generate torque. Defined in IEC 61800-5-2.
SIL	Safety Integrity level	Measure of the safety integrity of a control system, used in standards IEC 61508-x and related standards such as IEC 62061 and IEC 61800-5-2. Values of 1 to 4 are available, in machinery applications a maximum of 3 is considered.
SR	Safety Related	Applied to a function whose failure could lead to injury to a person
$SRECS$	Safety-Related Electrical or Electronic Control System	A control system whose failure might result in injury to a person

⁴ **Note** this usage in IEC 61800-5-2 differs from that in most other standards where PFH denotes the total failure probability in both safe and dangerous directions.

<i>SD</i>	Secure Disable	The term used by Control Techniques for Safe Torque Off before the publication of IEC 61800-5-2
<i>SIL CL</i>	SIL Claim Limit or Capability Level	Measure of the safety integrity of a sub-system or module, such as a drive, in carrying out its specified safety-related functions. This term is used to make it clear that the overall system SIL has to be calculated in its own right from a knowledge of the safety requirement specification and the capability of all sub-systems. The term emphasises that the SIL of the complete system cannot exceed the SIL of any sub-system. IEC 62061 uses the term “claim limit” IEC 61800-5-2 uses the term “SIL capability”
	Systematic Failure	A failure of the safety function which is caused by an inherent function of the system, rather than a fault which develops over time. Typically this would be a function whose action had not been appreciated during the design, verification and validation process, i.e. a design error in the most general sense of the term. Particularly applicable to software, which does not develop random faults but which may behave in an obscure fashion because of its complexity, and cannot be tested for all possible combinations of state transitions.

13 References

Applicable standards are cited in detail in the text

A full account of failure analysis techniques for systems comprising hardware and software is given in: **Control Systems Safety Evaluation & Reliability**, William M. Goble, ISA, ISBN 1-55617-636-8

This document contains material taken, with permission, from the 2nd edition of **“The Control Techniques Drives and Controls Handbook”** published in 2009 by The Institution of Engineering and Technology.

Our simple, flexible product lines make choosing the right drive very easy. For more demanding solutions our engineers, located within our Drive Centre and Reseller network, are available to discuss your needs and provide advice. For further details, please refer to the brochures below.

	Control Techniques Company Profile	Company overview		
	Drives, Drive Systems and Servos	Product Overview	100V / 200V / 400V / 575V/ 690V	0.25kW to 1.9MW
	Commander SK	General purpose AC drive	100V / 200V / 400V / 575V/ 690V	0.25kW to 132kW
	Unidrive SP panel mounting	High performance AC and servo drive	200V / 400V / 575V / 690V	0.37kW to 132kW
	Unidrive SP Free Standing	Higher power performance AC drive	400V / 575V / 690V	90kW to 675kW
	Unidrive SP Modular	High power modular AC drive	200V / 400V / 575V / 690V	45kW to 1.9MW
	Mentor MP	High performance DC drive	400V / 575V / 690V	25A to 7400A
	Digitax ST	Intelligent, compact and dynamic servo drive	200V / 400V	0.72Nm to 19.3Nm (57.7Nm Peak)
	Affinity	Dedicated HVAC/R drive for building automation and refrigeration	200V / 400V / 575V / 690V	0.75kW to 132kW
	Unimotor fm	Performance AC brushless servo motor	0.72Nm to 136Nm (408Nm Peak)	

Notes

Notes

Notes

Control Techniques Drive & Application Centres

AUSTRALIA Melbourne Application Centre T: +613 973 81777 controltechniques.au@emerson.com Sydney Drive Centre T: +61 2 9838 7222 controltechniques.au@emerson.com AUSTRIA Linz Drive Centre T: +43 7229 789480 controltechniques.at@emerson.com BELGIUM Brussels Drive Centre T: +32 1574 0700 controltechniques.be@emerson.com BRAZIL Emerson do Brazil Ltda T: +5511 3618 6569 controltechniques.br@emerson.com CANADA Toronto Drive Centre T: +1 905 201 4699 controltechniques.ca@emerson.com Calgary Drive Centre T: +1 403 253 8738 controltechniques.ca@emerson.com CHINA Shanghai Drive Centre T: +86 21 5426 0668 controltechniques.cn@emerson.com Beijing Application Centre T: +86 10 856 31122 ext 820 controltechniques.cn@emerson.com CZECH REPUBLIC Brno Drive Centre T: +420 541 192111 controltechniques.cz@emerson.com DENMARK Copenhagen Drive Centre T: +45 4369 6100 controltechniques.dk@emerson.com	FRANCE* Angoulême Drive Centre T: +33 5 4564 5454 controltechniques.fr@emerson.com GERMANY Bonn Drive Centre T: +49 2242 8770 controltechniques.de@emerson.com Chemnitz Drive Centre T: +49 3722 52030 controltechniques.de@emerson.com Darmstadt Drive Centre T: +49 6251 17700 controltechniques.de@emerson.com GREECE* Athens Application Centre T: +0030 21 57 86086/088 controltechniques.gr@emerson.com HOLLAND Rotterdam Drive Centre T: +31 184 420555 controltechniques.nl@emerson.com HONG KONG Hong Kong Application Centre T: +852 2979 5271 controltechniques.hk@emerson.com INDIA Chennai Drive Centre T: +91 44 2496 1123/ 2496 1130/2496 1083 controltechniques.in@emerson.com Pune Application Centre T: +91 20 2612 7956/2612 8415 controltechniques.in@emerson.com New Delhi Application Centre T: +91 11 2 576 4782/2 581 3166 controltechniques.in@emerson.com	IRELAND Newbridge Drive Centre T: +353 45 448200 controltechniques.ie@emerson.com ITALY Milan Drive Centre T: +39 02575 751 controltechniques.it@emerson.com Reggio Emilia Application Centre T: +39 02575 751 controltechniques.it@emerson.com Vicenza Drive Centre T: +39 0444 933400 controltechniques.it@emerson.com KOREA Seoul Application Centre T: +82 2 3483 1605 controltechniques.kr@emerson.com MALAYSIA Kuala Lumpur Drive Centre T: +603 5634 9776 controltechniques.my@emerson.com REPUBLIC OF SOUTH AFRICA Johannesburg Drive Centre T: +27 11 462 1740 controltechniques.za@emerson.com Cape Town Application Centre T: +27 21 556 0245 controltechniques.za@emerson.com RUSSIA Moscow Application Centre T: +7 495 981 9811 controltechniques.ru@emerson.com SINGAPORE Singapore Drive Centre T: +65 6468 8979 controltechniques.sg@emerson.com	SLOVAKIA EMERSON A.S T: +421 32 7700 369 controltechniques.sk@emerson.com SPAIN Barcelona Drive Centre T: +34 93 680 1661 controltechniques.es@emerson.com Bilbao Application Centre T: +34 94 620 3646 controltechniques.es@emerson.com Valencia Drive Centre T: +34 96 154 2900 controltechniques.es@emerson.com SWEDEN* Stockholm Application Centre T: +468 554 241 00 controltechniques.se@emerson.com SWITZERLAND Lausanne Application Centre T: +41 21 637 7070 controltechniques.ch@emerson.com Zurich Drive Centre T: +41 56 201 4242 controltechniques.ch@emerson.com TAIWAN Taipei Application Centre T: +886 22325 9555 controltechniques.tw@emerson.com THAILAND Bangkok Drive Centre T: +66 2962 2092 99 controltechniques.th@emerson.com TURKEY Istanbul Drive Centre T: +90 216 4182420 controltechniques.tr@emerson.com	UAE* Emerson FZE T: +971 4 8118100 ct.dubai@emerson.com UNITED KINGDOM Telford Drive Centre T: +44 1952 213700 controltechniques.uk@emerson.com USA California Drive Centre T: +1 562 943 0300 controltechniques.us@emerson.com Charlotte Application Centre T: +1 704 393 3366 controltechniques.us@emerson.com Chicago Application Centre T: +1 630 752 9090 controltechniques.us@emerson.com Cleveland Drive Centre T: +1 440 717 0123 controltechniques.us@emerson.com Florida Drive Centre T: +1 239 693 7200 controltechniques.us@emerson.com Latin America Sales Office T: +1 305 818 8897 controltechniques.us@emerson.com Minneapolis US Headquarters T: +1 952 995 8000 controltechniques.us@emerson.com Oregon Drive Centre T: +1 503 266 2094 controltechniques.us@emerson.com Providence Drive Centre T: +1 401 541 7277 controltechniques.us@emerson.com Utah Drive Centre T: +1 801 566 5521 controltechniques.us@emerson.com
--	---	--	---	---

Control Techniques Distributors

ARGENTINA Euro Techniques SA T: +54 11 4331 7820 eurotech@eurotechsa.com.ar BAHRAIN Emerson FZE T: +971 4 8118100 ct.bahrain@emerson.com BULGARIA BLS - Automation Ltd T: +359 32 968 007 info@blsaautomation.com CENTRAL AMERICA Mercado Industrial Inc. T: +1 305 854 9515 rsaybe@mercadoindustrialinc.com CHILE Ingeniería Y Desarrollo Tecnológico S.A T: +56 2741 9624 idt@idt.cl COLOMBIA Sistronic LTDA T: +57 2 5556 600 sistronic@telesat.com.co	CROATIA Zigg-Pro d.o.o T: +385 1 3463 000 zigg-pro@zg.htnet.hr CYPRUS Acme Industrial Electronic Services Ltd T: +3572 5 332181 acme@cycitanet.com.cy EGYPT Samiram T: +202 97033868/+202 97033869 samiramz@samiram.com FINLAND SKS Control T: +358 207 6461 control@skis.fi HUNGARY Control-VH Kft T: +361 431 1160 info@controlvh.hu ICELAND Samey ehf T: +354 510 5200 samey@samey.is	INDONESIA Pt Apikon Indonesia T: +65 6468 8979 info.my@controltechniques.com Pt Yua Esa Sempurna Sejahtera T: +65 6468 8979 info.my@controltechniques.com ISRAEL Dor Drives Systems Ltd T: +972 3900 7595 info@dor1.co.il KENYA Kassam & Bros Co. Ltd T: +254 2 556 418 kassambros@africaonline.co.ke KUWAIT Emerson FZE T: +971 4 8118100 ct.kuwait@emerson.com LATVIA EMT T: +371 760 2026 janis@emt.lv LEBANON Black Box Automation & Control T: +961 1 443773 info@blackboxcontrol.com	LITHUANIA Elinta UAB T: +370 37 351 987 sigitas@elinta.lt MALTA Mekanika Limited T: +35621 442 039 mfrancica@gasan.com MEXICO MELCSA T: +52 55 5561 1312 melcsamx@iserve.net.mx SERVITECK, S.A de C.V T: +52 55 5398 9591 servitek@data.net.mx MOROCCO Leroy Somer Maroc T: +212 22 354948 lsmaroc@wanadoopro.ma NEW ZEALAND Advanced Motor Control. Ph. T: +64 (0) 274 363 067 info.au@controltechniques.com	PHILIPPINES Control Techniques Singapore Ltd T: +65 6468 8979 info.my@controltechniques.com POLAND APATOR CONTROL Sp. z o.o T: +48 56 6191 207 drives@apator.torun.pl PORTUGAL Harker Sumner S.A T: +351 22 947 8090 drives.automation@harker.pt PUEERTO RICO Powermotion T: +1 787 843 3648 dennis@powermotionpr.com QATAR Emerson FZE T: +971 4 8118100 ct.qatar@emerson.com SAUDI ARABIA A. Abunayyan Electric Corp. T: +9661 477 9111 aec-salesmarketing@abunayyan-group.com	SERBIA & MONTENEGRO Master Inzenjering d.o.o T: +381 24 551 605 master@eunet.yu SLOVENIA PS Logatec T: +386 1 750 8510 ps-log@ps-log.si TUNISIA SIA Ben Djemaa & CIE T: +216 1 332 923 benjemaa@planet.tn URUGUAY SECOIN S.A. T: +5982 2093815 secoin@secoin.com.uy VENEZUELA Digimex Sistemas S.A. T: +58 243 551 1634 VIETNAM N.Duc Thinh T: +84 8 9490633 infotech@nducthinh.com.vn
--	---	--	--	---	--