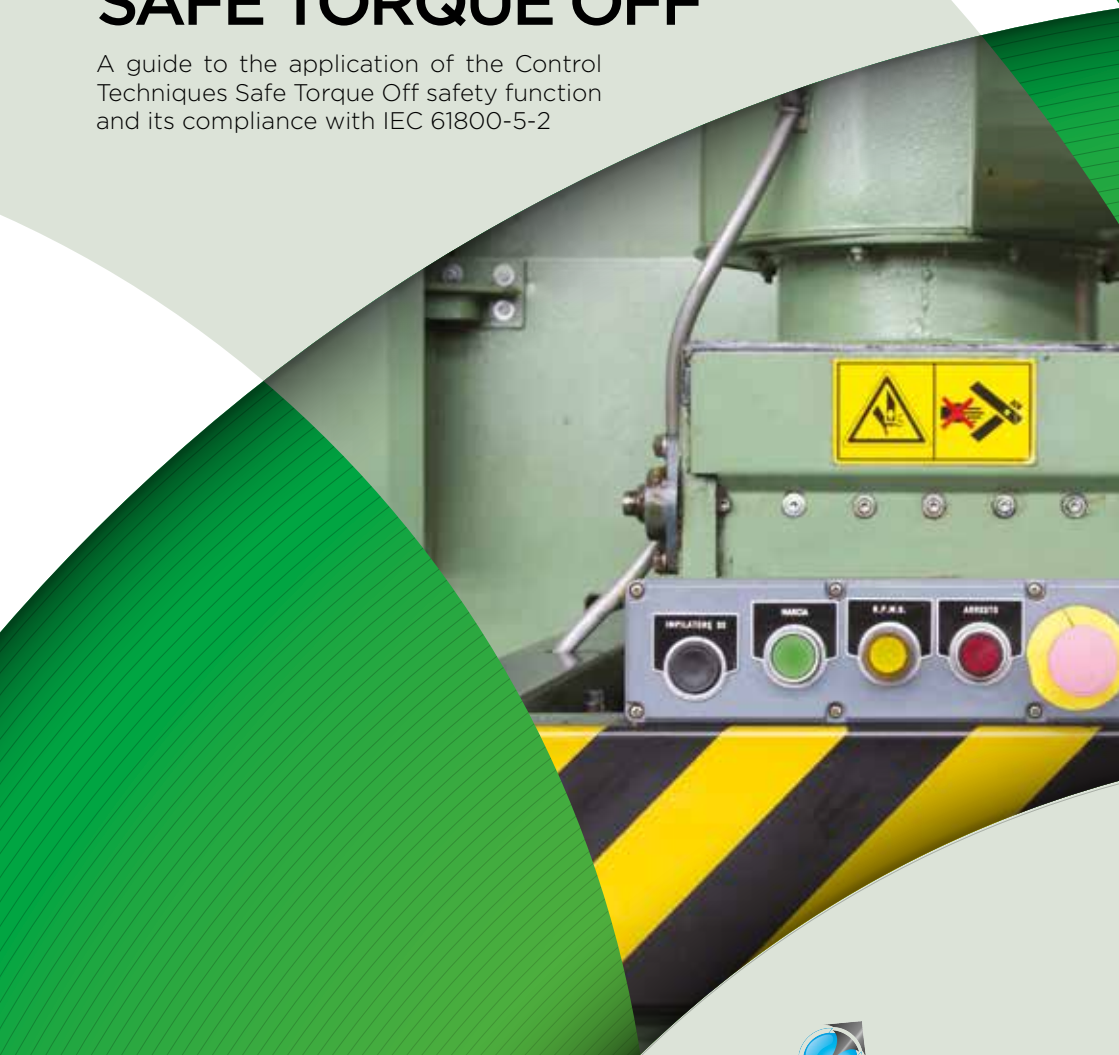
CONTROL TECHNIQUES™

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



Nidec
All for dreams

1. Purpose of this guide

This application guide gives general explanations, advice and guidance for the use of the Safe Torque Off (STO) feature which is provided in many of Control Techniques' variable speed drive products.
It supplements the specific product information given in the product Technical Guides. In the event of any discrepancy the product Technical Guide takes precedence.

Most of the information is general in nature and applies to all models. Some model-specific information is given in Annex 1.

Important warnings

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.

Index

2. Quick overview

Systems intended to control equipment which could cause or allow injury if the control system malfunctions are referred to as functional safety control systems. They have to be designed not only to operate as intended during normal conditions, but also so that no likely fault or combination of faults results in the loss of the safety function. They also have to be designed to minimise the risk that a systematic fault, i.e. some kind of error in specifying or implementing the safety function, results in the loss of the safety function.

Control Techniques STO is a functional safety feature which complies with standard IEC 61800-5-2 (and EN 61800-5-2) and is built in to the drive 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 signal, the drive is disabled to a high degree of integrity, where no single component failure, and only very unlikely combinations of multiple 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, for example as part of an interlock system, in place of the more conventional arrangements of contactors with cross-checking auxiliary contacts.

Under normal conditions the Safe Torque Off (STO) Drive enable input operates exactly the same as a non-safety enable 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 the STO safety function 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 in to the drive output, but there are no moving parts, no extra cost, and no difficulty over contact arcing if the drive is disabled when delivering output current. 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.

Commander C **Unidrive M** **Digitax HD** **E300**

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, designed to prevent foreseeable hazards 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 recognises 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.

Section 3 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 5.

For further information on Commander C, Unidrive M, Digitax HD and E300 Elevator drive families, refer to the following brochures, available online at www.controltechniques.com.

- Commander C
- Unidrive M400
- Unidrive M - High Power Modular AC Drives
- Unidrive M600
- Unidrive M700
- Powerdrive F300
- Digitax HD
- E300 Elevator Drive

3. Principles of machinery safety design

General principles

The design of safe machinery is a complex process which requires attention from the start of the machinery design planning. 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

As the design of a machine proceeds, a risk assessment has to be performed and then updated regularly.

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, 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.

The safety-related control measures have to be decided and specified by the machine designer, and the risk assessment is revised to take account of these measures until a satisfactory risk level is achieved.

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, in the form of a Safety Requirements Specification (SRS).

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 should be understood and agreed to by all parties involved.

Standards, and the EU Machinery Directive

For the purpose of the EU Machinery Directive, there is a single European harmonised standard (created by CEN) which lays down the essential principles for the procedure for designing safe machinery and carrying out a risk assessment. This is the so-called “A standard”, which is supported by more detailed standards which focus on specific aspects of safety (“B standards”) or specific types of machine (“C standards”).

These standards originate with the international bodies ISO and IEC, and have been adopted directly as EN standards for application under the EU Machinery Directive. International standards have the prefix IEC or ISO. European standards have the prefix EN. The two have identical technical requirements except sometimes briefly during transitions between versions. The international standards are valid worldwide. The EN versions have a particular legal value when used to comply with the EU Machinery Directive.

"A standard":

EN ISO 12100 Safety of machinery — General principles of design — Risk assessment and risk reduction (and internationally, ISO 12100)

"B standards" for machinery control equipment:

The main applicable standards for drive applications in machinery are listed here.

- **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.
- **ISO 13849-1 Safety of machinery** - Safety-related parts of control systems. General principles for design (and EN ISO 13849-1)
  - This standard was developed from EN 954-1, now superseded, which was intended only for safety controllers based on non-complex hardware with no programmable parts. It aims to maintain a simple approach to purely hardware systems whilst allowing for the use of software.
  - It uses a "Performance Level" as an indicator of integrity, with levels increasing from (a) to (e), as well as "Categories" which relate to the architecture. Unlike the following standards, it allows for the use of mechanical, hydraulic and pneumatic control methods. It is supplemented by ISO 13849-2 **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 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.
- **IEC 61508 parts 1 to 7 Functional safety of electrical/electronic/programmable electronic safety-related systems** (and EN 61508-)
  - This family of standards defines the principles for functional safety of programmable systems. It defines the SIL system of safety integrity metrics. It does not of itself apply directly to machinery safety, but is extensively referenced in the machinery standards.

Note on Safety Integrity Level (SIL), Performance Level (PL), and related data

SIL can take values from 1 to 4, with standards for 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 capability can only be realised by appropriate incorporation into a complete SRECS.

In addition to a SIL capability, the sub-system must also have data giving a value for the probability of failure of hardware in the dangerous direction - referred to as PFH or PFH_D[1] . This data has to be combined with the corresponding data for other sub-systems to calculate an overall PFH for the complete SRECS.

Performance Level is used in standards based on ISO 13849-1. It can take values from a to e. There is a correspondence between this and SIL, where SIL1 corresponds to PL c and SIL3 corresponds to PL e. This correspondence is useful as a general guide, but should not be considered as an exact equivalence, the standards should be consulted since there are differences in procedure.

In association with the PL, the failure rate data is referred to in terms of $MTTF_D$[2] , i.e. the mean time to failure of the safety function.

[1] Probability of Failure of Hardware (in the Dangerous direction) - per hour

[2] Mean Time To Failure in the Dangerous direction - years

4. Safety controllers using electromechanical components

General principles

The purpose of this section is for those unfamiliar with the STO concept in a drive, to explain how before its availability in drives the STO function might have been realised using conventional electromechanical components. We will then see how a STO function in a drive can replace and give better performance than an electromechanical arrangement.

Generally the machine motor is a three-phase a.c. motor, which may be connected directly to a three-phase a.c. supply, or through an a.c. variable speed drive or servo 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 de-energised. When a drive is used the contactor might be placed in the input or the output, the choice is discussed later.

When the contactor is open the motor can produce no torque, neither motoring nor braking, other than from friction and stray losses. The machinery normally coasts to a halt when the torque is removed, but of course there are some applications where movement might occur as a result of the loss of torque.

Since the three-phase a.c. 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[3] . 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.

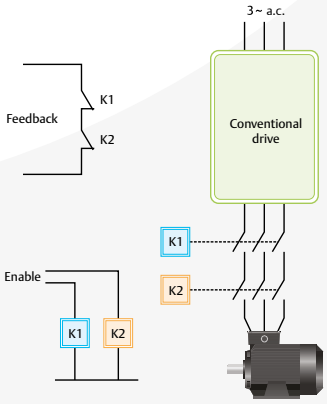


Figure 1: Safety-related motor disable function implemented using contactors

[3] All three contacts must connect in order to produce torque. However, unless special design measures are taken, a single welded contact pair might result in all three pairs remaining connected.

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 50 or 60 Hz. They rely on the current passing through zero every half-cycle to extinguish the arc formed when the contact opens. When connected to a drive output the frequency can vary over a wide range down to 0 Hz (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 hazard, but also it could result in welding of contacts, which represents a potential common cause 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.

5. Control Techniques Safe Torque Off - how it works

General 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[4]. The drive has available a single internal d.c. supply, which is converted to three-phase a.c. by the continual active switching action of six power semiconductor devices (IGBTs) in the inverter stage. Figure 2 shows the main power components.

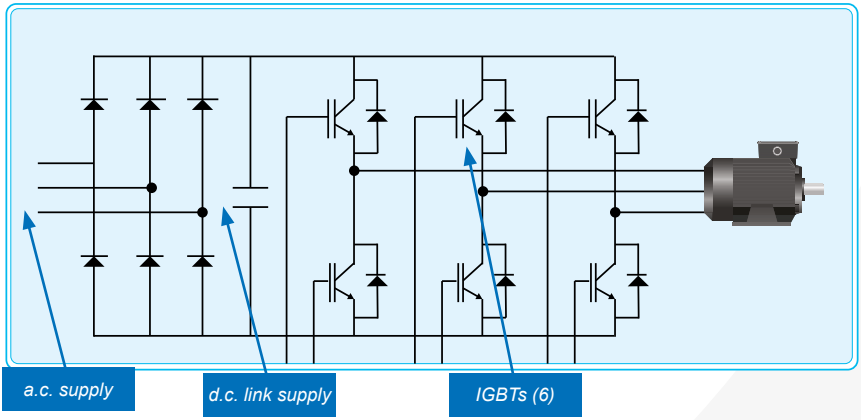


Figure 2: Basic power circuit for an inverter drive

If the IGBTs are not switched on then no current or torque can be produced in the motor, and it behaves just as if there were an open contactor in the motor supply[5]. However the integrity level of the disabled inverter goes far beyond this. Failure of any or all of the individual IGBTs or their drive circuits either into the on or off state cannot generate a rotating magnetic field, and therefore cannot generate torque. In the worst case, if two opposed IGBTs in different legs of the inverter both conduct unintentionally, a temporary d.c. current flows into the motor. The d.c. current produces no torque in an induction motor. The current soon rises to such a high level that the protection system such as fuse or circuit breaker operates to interrupt the current, but in any case no torque is produced. The inverter power circuit therefore provides an inherently fail-safe drive, because faults in this circuit cannot produce torque.

Note that with permanent magnet motors such as servo motors, or motors with magnetic saliency such as reluctance motors, a single transient alignment torque could be produced by a multiple IGBT failure. A permanent magnet motor could rotate by a maximum 360°/p, and a reluctance motor by 180°/p, where p is the number of poles.

[4] With a single phase supply the motor might be able to run, but it can produce no torque when stationary so it cannot start

[5]The presence of the freewheel diodes means that there is a slight difference which might have an effect with a permanent magnet motor, but there cannot be a motoring torque in any case.

It now remains to consider how to interface the drive control signal or signals which control the STO state, with the inverter power circuit. 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 is very difficult to provide the disable feature within this part, because the complexity of the arrangement makes it difficult to ensure and 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 3. The logic circuit, shown here in an ASIC, prevents the complex pulse sequences which are required to generate torque from reaching the inverter driver circuits (opto-couplers). The disable function provided by this arrangement is likely to be more reliable than one operating through the software, in the sense that it is unlikely to have unexpected behavior or failure modes. However the logic circuit is not fail-safe - it is equally likely to fail in the unsafe and safe directions. This is usually not acceptable for a safety-related application.

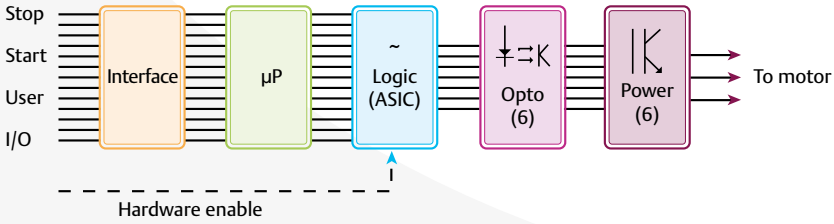


Figure 3: Conventional drive hardware enable

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 4, 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.

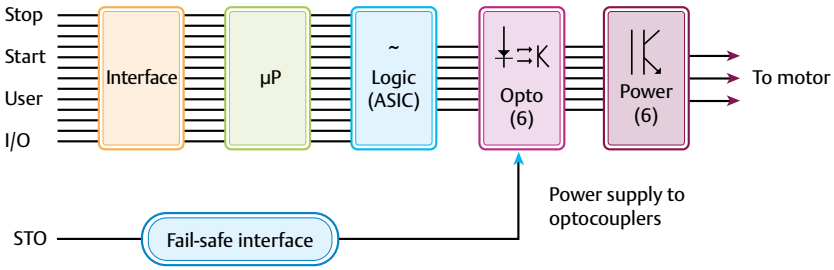


Figure 4: Control Techniques Safe Torque Off

Capabilities

1. Safe Torque Off (STO) 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.
2. STO provides a category 0 stop in accordance with IEC 60204-1 (EN 60204-1). Power is removed immediately from the motor. (see limitation 2.)
3. When the drive is disabled during running, the output current decays rapidly but without oscillatory transients or sparking such as occurs with contactors if the current has not decayed. Since no motor contactor is needed the motor cable screening (shielding) can be maintained right to the drive terminals without needing to be interrupted at contactors, giving best EMC (radio frequency emission) behaviour.
4. 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.
5. Information regarding the probability of failure of the safety function due to a hardware fault per hour (PFH), and mean time to failure in years ($MTTF_D$), is given in the user guide and technical data. For most of Control Techniques' products PFH is much less than 10^{-8}. This gives ample scope for incorporation into a SIL3 system. (In order to meet SIL3 the highest value of PFH permitted by the standards is 10^{-7}, and values below 10^{-8} are outside of the scope of SIL3. In order to allow the complete system to meet SIL3 when the failure probability of sub-systems accumulates, it is necessary that the PFH for the sub-systems such as the drives should be as low as possible, and certainly less than 10^{-7}.)
6. For all products offering STO the data provided by Control Techniques has been independently verified by a EU Notified Body.
7. For current products such as Unidrive M, the electrical characteristics and thresholds of the STO input(s) comply with IEC 61131-2 type 1. In order to maintain SIL3 the low-state voltage must be below 5 V and current below 0.5 mA. It is essential that the STO wiring be arranged so that voltage drops in the wiring and/or leakage currents could never cause these levels to be exceeded.

8. The STO input is compatible with self-testing digital outputs of controllers such as PLCs, sometimes referred to as OSSD, where the test pulse is a maximum of 1 ms. This means that the drive is not disabled by logic-low input pulses with a maximum of 1 ms duration.
9. The state of the enable input can be monitored through a drive parameter which is defined in the technical guide. The monitor data is not classified as safety-related data.

Limitations

1. STO uses solid-state techniques, it does not provide physical separation of electrical connections and it is not intended to provide safe electrical isolation to allow access to the electrical connections.
2. 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. 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.
3. Basic STO offers a single input channel. Some Control Techniques products offer dual-channel STO, this is explained further in section 6. For a single channel there are no single internal drive faults which could result in the drive becoming enabled, but 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 the fault lists and fault exclusions given in Annex D of ISO 13849-2, this can be achieved by physical separation of wiring or by using a screened wire with the screen connected to ground/logic low.
4. The STO Enable input cannot be configured to operate with negative logic. This is a requirement of most standards and conventions for safety functions, operating with positive logic and the return connection connected to earth (ground). This ensures that an earth fault in the control circuit results in a safe failure (drive disabled).
5. Because the STO Enable input is compatible with self-testing safe digital outputs, the response time to disable is relatively long, for example 20 ms maximum.
6. When using a permanent-magnet or reluctance motor, there is a small possibility when the STO is active 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 into the short circuit state 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 without generating torque, because the drive would either trip or the power device be destroyed, 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 or reluctance motor is used.

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

Those who are familiar with relay-based safety control logic sometimes ask this question. A relay logic system is usually designed to allow for feedback from the auxiliary contacts on the final actuator, e.g. the output contactors described in section 4. This allows a stuck contactor to be detected. Control Techniques STO does not provide a feedback contact, because there is no relay or contactor which might be stuck. Faults in the internal interface circuit which might cause a logic level to be stuck always result in the drive being disabled. If feedback is required for compatibility with other parts of the control system, it can be provided by using the STO monitoring parameter in the drive to set a digital output.

Safe Torque Off has been designed into our drives from first principles. By careful design of fail-safe electronic circuits, it has eliminated failure modes equivalent to a stuck contactor or relay, so no feedback is required for SIL 3 or PL e. This avoids the need for expensive additional option modules or safety relays, and offers superior integrity at lower cost.

Some STO systems of older design offered by other drive manufacturers use relays to interrupt the power supply to the gate drive opto-couplers and to provide galvanic isolation. This is illustrated in Figure 5, 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 and it is still necessary to use one external contactor to prevent the motor from being driven because of this first fault.

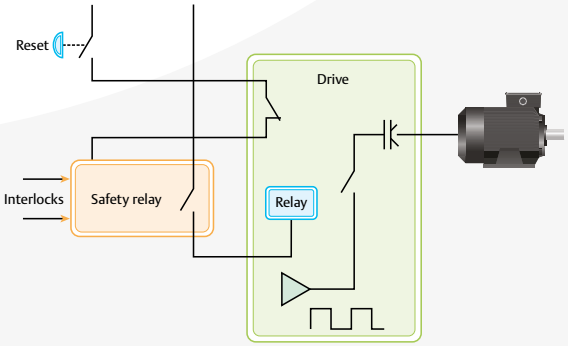


Figure 5: Typical drive disable function using relay having guided contacts

6. Single and dual channel Safe Torque Off

The basic Control Techniques STO function offers a single input with SIL3 and PLe integrity. When this is incorporated into a complete system, system faults must be considered, which would include a possible wiring fault inadvertently setting the STO input to logic high and allowing the drive to be enabled. This risk can be managed in a number of ways, depending upon system details and the fault exclusions being applied. For example:

Where the STO signal originates in a safety controller such as a safety PLC, a forced logic high STO signal would be detected by the safe digital output of the PLC. The PLC could then disable the machine by a separate route, for example by opening a power contactor if one is present. This is illustrated in Figure 6. The contactor might be arranged to interrupt the power to the whole machine, or to one or more drives as appropriate.
The STO signal could be carried in protected wiring in accordance with ISO 13849-2, and derived from a source with sufficiently low failure rate such as a self-testing safe digital output. This is illustrated in Figure 7.
Where this is not possible, the dual-channel STO might be an effective solution. In this case the controller generates two STO signals, and if it detects a fault on one channel it can still disable the drive through the other. This is illustrated in Figure 8.

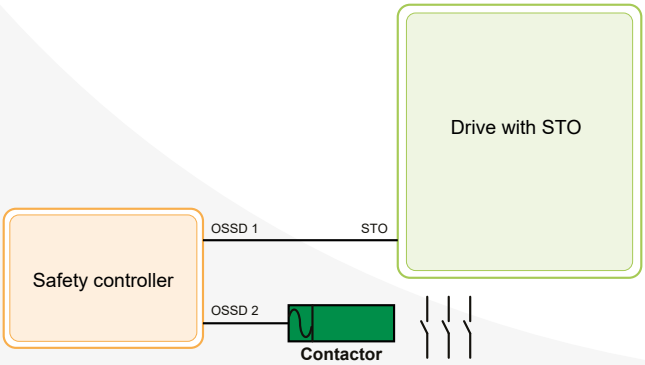


Figure 6: Second channel external

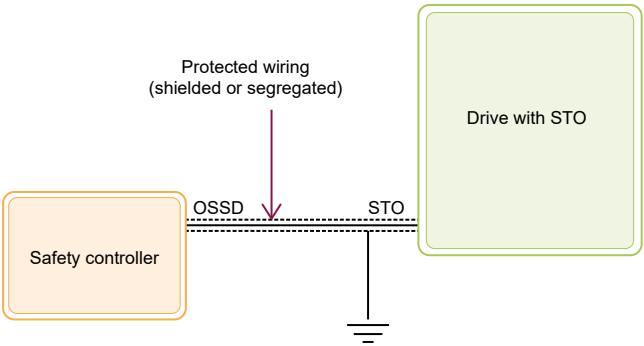


Figure 7: Single channel with protected wiring

Figure 8: Dual channel STO

7. 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.

The PFH 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 or $MTTF_D$. The very low value of PFH 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.

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.

8. Certification

In the European Union and EEA machinery safety is governed by the Machinery Directive, one of whose requirements is that safety components of a machine are required to undergo a special approval process leading to a EC Type Examination Certificate from a EU Notified Body (i.e. an accredited independent approvals body), as well as a CE mark and a Declaration of Conformity under the Machinery Directive.

All Control Techniques products incorporating STO have the relevant type approval certificates and declarations.

9. Lift (Elevator) applications

Control Techniques STO can be used to prevent the unintended operation of the motor in the lift (Elevator) applications. The type approval certificates include confirmation of compliance with this clause.

The STO can be used directly in order to replace one of the two contractors to prevent operation of the motor, in accordance with European standards EN 81-20 and EN 81-50.

STO can also be used to replace both contactors from EN 81-20 and EN 81-50, provided that the STO input is controlled by two series-connected relays with guided auxiliary contacts. In this case compliance is directly with the EU Lifts Directive, and separate certification is available from a Notified Body.

The dual-channel version of STO complies inherently with the requirements of EN 81-20 and EN 81-50, because they allow for the use of a drive with STO complying with EN 61800-5-2 SIL3 provided that the hardware fault tolerance is at least 1.

10. 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). These may be referred to as OSSD.

The maximum width of a periodic test pulse for which the drive will not be disabled is 1 ms.

The STO input has a resistance-capacitance filter in the input circuit, to prevent the risk of high-frequency noise picked up in the wiring from being rectified and causing an incorrect enable action. Capacitance values are given in Annex 1. It is possible that some designs of digital output with short test pulses and relatively low current sinking capability might falsely detect a fault with this capacitive load. The supplier of the controller should be asked for the maximum allowable capacitive load.

The impedance of the STO input is given in Annex 1. Some safe digital outputs are intended to be used with relay loads and they indicate a fault if the current falls too low. The supplier of the controller should be consulted for the maximum resistance or minimum current required to indicate a healthy circuit.

11. Parallel connection of Safe Torque Off inputs

Control Techniques 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 (highly unlikely) 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.

Consideration must also be given to the effect of the cumulative input capacitance of these inputs on a safe digital output driving them.

12. Differences between Safe Torque Off functions in drive families

There are some detailed differences between the STO functions offered in various drive families. A list of the relevant models and families is given in Annex 1.

Connection of STO signal return line (0V or reference connection)

There are two arrangements for the return or negative or reference connection for the STO signals. These are classified here as type 1 and type 2.

In type 1 drives, the STO input has its return connection in common with the other digital inputs of the drive. Figure 9 shows an example of the connections for the dual channel version, the same applies for the single channel version except for the terminal numbers.

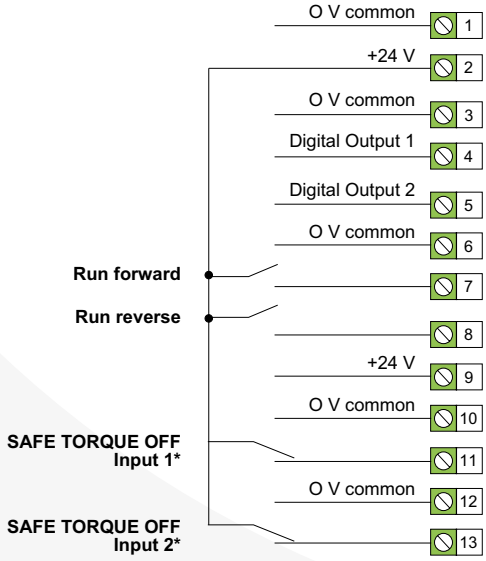
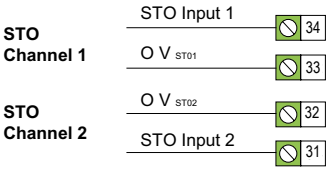


Figure 9: Control connections for type 1 drives

**The Safe Torque Off (STO), Drive enable terminals are positive logic input only.*

All of the terminals marked “0V common” are connected together internally. Where the STO inputs are used for safety functions it is normal practice for these to be connected to the system ground. In order to maintain the specified SIL and PL, terminals 10 and 12 (or their equivalents for other models) must always be connected by dedicated wires to the corresponding 0V (or ground or reference or negative) connections of the signal source. This is to avoid the risk that the signal source 0V connection becomes energised (logic high) by an electrical fault, which might include a broken ground connection for the signal source.

In the type 2 drives, the STO inputs are completely galvanically isolated from the other inputs. Figure 10 shows an example of the connections for type 2 drives.



STO	Frame 1 to 4	Frame 5 and larger
STO1	34	31
0V STO1	33	32
0V STO2	32	35
STO2	31	36

Figure 10: Control connections for type 2 drives

The 0V terminals are not connected internally. In order to maintain the specified SIL and PL, terminals 0V STO1 and 0V STO2 must be connected by dedicated wires to the corresponding 0V (or ground or reference or negative) connections of the signal source.

For both drive types the wiring requirements are the same. The 0V terminals must be connected by dedicated wires for the STO circuit, to the origin (controller) of the STO signal(s). The difference is that for type 1 the STO would still operate if this instruction were to be ignored, but with an increased risk of a dangerous error in the event of the ground or negative connection to the controller becoming broken. For type 2 the drive would not be enabled if this instruction were to be ignored.

Logic thresholds

The product user guide gives two values for the logic threshold. The nominal value shows the range of variation and therefore the minimum voltage for logic “high” and maximum for logic “low”. This defines the behaviour under normal (healthy) conditions. A further pair of values is given which is the maximum voltage and current for disable to SIL3 and PLe integrity. This value is maintained in the event of an internal fault or faults. In order to maintain the integrity, the circuit driving the input must hold the terminal voltage and current below this threshold in the event of an external fault.

Current products have a threshold of 5V and 0.5 mA. Legacy products have lower thresholds.

13. Specifications

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

Safety specification:

Safety function

When the Safe Torque Off (STO), Drive enable is de-energised (i.e. in the logic low state) 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.

For detailed electrical and failure rate specifications please consult the relevant user guide.

EMC immunity testing:

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).

14. Glossary

This is a brief glossary of important terms used in this guide. For a more complete glossary consult the references or standards such as IEC 61508-4 or 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 or number of channels, and therefore the fault tolerance.
	Category	A qualitative measure of safety integrity used in ISO 13849-1. 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 is detected.
	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 ISO 13849-1.
	Monitoring	An arrangement for detecting faults
PL	Performance Level	Measure of the safety integrity of a control system for a machine, used in standard ISO 13849-1. Values between a and e are available.
PFH	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 persons
SIL CL	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.

15. 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: 1-934394-80-7

16. Annex 1 - Model-specific information

Annex 1 last update: 28/06/2019

Product family	0V connection type	Logic threshold for SIL3/PL e	Capacitance (nF)	Resistance (k)
Unidrive M300 M400 series, frame sizes 1 to 4	2	5 V/0.5 mA	22 nF	3.3
All remaining Unidrive M series with single channel STO	1	5 V/0.5 mA	44 nF	1.65
All remaining Unidrive M series with dual channel STO	1	5 V/0.5 mA	22 nF	3.3
Powerdrive F300	1	5 V/0.5 mA	44 nF	1.65
HVACR Drive H300	1	5 V/0.5 mA	44 nF	1.65
Elevator Drive E300	1	5 V/0.5 mA	44 nF	1.65
Unidrive HS30	2	5 V/0.5 mA	22 nF	3.3
Unidrive HS70, HS71, HS72	1	5 V/0.5 mA	22 nF	3.3
Digitax HD M750, M751, M753	2	5 V/0.5 mA	32 nF	7.5

Notes

Notes

Connect with us at:

THE AUTOMATION ENGINEER

www.controltechniques.com

TRILTECHNIEKSHOP.NL

Control Techniques is your global drives specialist. With operations in over 70 countries, we're open for business wherever you are in the world.

For more information, or to find your local drive centre representatives, visit

www.controltechniques.com

Nidec All for dreams | CONTROL TECHNIQUES™

Nidec Control Techniques Limited. Registered Office: The Gro, Newtown, Powys SY16 3BE. Registered in England and Wales. Company Reg. No. 01236886.

P.N. 0704-0000-05 06/19