AC Drive

Safety Manual

for ADV family

English

User manual

Rev.0-9 –10-3-2017

1S5F94

GEFRAN

Changes

Doc. release	Changes	Revision
0.1	First release	10/09/2009
0.2	Specification of input command sequence following conservative request from MC during last design review. It will be removed only after tests on the field.	7/10/2009
0.3	Review based on comments of certification body email 22/12/2009	3/1/2010
0.4	SIL application drawing reviewed.	7/12/2010
0.5	Ch. 5.1 ADV200 product range extended to comprise 690v	10/02/2012
0.6	Mod pag 2. Ch 4.2 mod text. Ch. 4.4 add text after table Mod figure Ch 7.1 and text below figure	20/11/2013
0.7	Mod figure Ch 7.1 and text / Ch. 4.4 table 1 reviewed	18/04/2014
0.8	Pag 8 : “PL d according …” to “PL e according …”; add ch. 5.3 Leds	10/03/2015
0.9	Add text on page 2. Add ADV size 7/ADV200-LC size 8, INT-P-ADV and maintenance procedure. Ch 4.4 mod table 1. New ch. 5.3.1 LEDs on INT-P-ADV card. Ch. 7.1 mod figure 11 and text.	10/03/2017

Thank you for choosing this Gefran product.

We will be glad to receive any possible information which could help us improve this manual. The e-mail address is the following: techdoc@gefran.com.
Before using the product, read the safety instruction section carefully.
Keep the manual in a safe place and available to engineering and installation personnel during the product functioning period.
Gefran spa has the right to modify products, data and dimensions without notice.
The data can only be used for the product description and they can not be understood as legally stated properties.

Contents

1 Safety instruction and information for use

1.1 Motivations for integrated safety function

As a result of automation, demand for increased production and reduced operator physical effort, control systems of machinery and plant items play an increasing role in the achievement of overall safety. These control systems increasingly employ complex electrical/electronic/programmable electronic devices and systems.
Prominent amongst these devices and systems are adjustable speed electrical power drive systems (PDS) that are suitable for use in safety-related applications (PDS-SR).

Electronic protection are integrated into the drive in order to perform safety function to minimise or excrete hazards due to functional errors using machinery.

Integrated safety function replaces external safety components. STO integrated function can be used as an alternative to motor contactors in order to control unexpected motor re-start, whether risk assessment permit it. According to previous paragraph safety integrated function applicability depends application and applicable standards.

The whole safety related part of the control system, using the drive integrated safety function, has to work properly in normal and misuse state. It must be trouble-free and reach a safe state.

In order to check for those requirements, the whole safety related control system must be analysed by means of FMECA, fault tree, etc.

1.2 Safe torque off function description.

Safety function, “Safe Torque off” (STO) is a safety function used to break off power and current output onto the motor in order to prevent unexpected movements and voltages. **ADV200 drive family supports “Safe Torque Off” as an option by means of an integrated function called EXP-SFTY-ADV**. ADV biggest sizes 7, integrates and embed the same safety circuit in different position, onto a board called INT-P-ADV.

This safety function does not disconnect the machine from electrical power supply. It shall be stressed that safety equipped drive units are just one component in a safety control system whereas STO is system level function. Parts and components of the system must be chosen, applied and integrated appropriately to achieve the desired level of operational safety.

Safety function “Safe torque off” can sometimes be used to attain an Emergency Stop” while the power supply is still present on the drive (according to category 0 as described into EN 60204-1).

This document mainly focuses and describes the safety integrated function EXP-SFTY-ADV present on AC drive family ADV200 used to achieve the “Prevention of unexpected start-up” as described in EN 1037:1995+A1:2008 relating to the safety of machines.

EXP-SFTY-ADV is integrated in the drive unit family ADV200 as an optional feature, whereas safety capability could also be implemented externally. When Safety is an integrated feature the power disconnection between the drive controller and the motor, required to achieve a “safe stand-still”, is obtained without the use of external contactors and or relays.

Function should not be mistaken with “Mains supply disconnection (isolating) and switch-off “, section 5.3 isolation from power supply system, requested by EN 60204-1.
The mains supply switch-off function may performed only with the use of appropriate isolating switching devices.

The feature of STO safety function are:
- Unexpected movements of the motor shall not be possible.
- Power and current to the motor are safely switched off.
- Drive unit is not disconnected from DC-link, so short response time to a re-start command is possible

1.3 Safety recommendations

Specifications and instructions provided to support functional safety are essential part of function itself. Comprehension and knowledge are mandatory requirements for people getting involved in installation and commissioning activities.

Only qualified personnel is allowed to execute any activities during installation and commissioning procedures.

Qualified personnel
For the purposes of this Instruction Manual, a “Qualified person” is someone who is skilled to the installation, mounting, start-up and operation of the equipment and the hazards involved.

Qualified person should be:

- Trained for first aid emergencies
- Trained in the proper care and use of protective equipment according to established safety procedures.
- Trained and authorized to energize, de-energize, clear, ground and tag circuits and equipment according to established safety procedures.

Safety Manual complements and integrates instruction manuals for ADV200 drive family. It contains additional safety information complying with Machinery Directive for supporting use of drive safety-related functions. Use of this functions as a part of machinery control system shall be possible only after this document has been carefully understood.

Warning

Improper installation and commissioning of safety related parts of the control system, can cause an uncontrolled re-starting of the drive unit. This may cause death, serious injuries and significant material damage.

Safety function control system shall only be installed and commissioned by qualified personnel.

Emergency stop function (according to EN60204) must operate and take PDS into a safe state independently from the operational status of drive unit. Safety integrated system is not affected from operational status of the internal/external parts not related to safety.

Resetting emergency stop safety function must not result in uncontrolled re-start of the motor. PDS can be re-started only when STO function is no longer active. In order to comply with EN60204, drive will re-start only after operator manual confirmation.

In circumstances where external influences (with vertical loads for example) are present, additional measures (mechanical brakes for example) might be necessary to prevent any hazards.

Procedures to check the safety function periodically according to the result of risk assessment and prescriptions in §6.2 must be set-up.

STO integrated safety function is single fault safe system (within the drive unit). No single fault or component failure can cause a loss of safety state, inducing drive to produce motor torque.
Wiring and connections of the system must appropriately implemented and tested in order to support same fault tolerance (1) at system level.

Warning

In the event of the failure of two output IGBTs in the drive, when Safe Torque Off has been activated, the drive may provide energy for up to 180° of rotation in a 2-pole motor before torque production in the motor ceases.

In case of induction motor, no movement is possible even when several faults occur (in the IGBT power stage). That is, no failure on IGBT drivers, in absence of controlled pulses coming from regulation, can generate current able to establish rotating field.

It must be checked if this condition can cause a dangerous machine movement.

Warning

When the safety function is activated (motor unable to produce torque), the DC-link (high voltage dc bus) of the drive is still connected to mains supply.
In this case drive control is deactivated and after motor coasting to standstill or already stopped, high voltage are present on motor and drive terminals.

For authorised personnel to work on live parts, drive shall be electrical isolated from mains supply (mains switch) and appropriate time shall be elapsed (more than 5minutes) to allow high-voltage DC-link to discharge.

This is called “Mains supply disconnection (isolating) and switch-off“, isolation from power supply system, requested by EN 60204-1.

The mains supply switch-off function may performed only with the use of appropriate isolating switching devices.

2 Risk analysis and assessment

According to Machinery Directive 2006/42 EC, it is mandatory for the manufacturer of the machines to carry out risk analysis in order to identify the hazards related to the machine.

Risk analysis should be developed according to Standard EN 14121-1-Safety of Machinery- Risk assessment.

Risk assessment procedure is intended to prevent and identify:

- degree of injury
- frequency/duration of risk exposure
- possibility of turning away

In order to define risk level and to obtain a correct classification concerning Safety category, SIL (Safety integrity level), PL (Performance level) standards EN61800-5-2, IEC 61508, EN ISO 13849-1 should be used and applied.
These standards give information and procedure according to design principle and risk assessment for safety related part of control systems.

In the case of STO safety function the risk assessment must consider the fact that the motor coast to a standstill at STO activation. A mechanical brake may be requested in some applications. Latching devices preventing access to dangerous parts might also be necessary enabling automatically STO function.

Liability:

The **Manufacturer** shall be responsible for the safety of the machinery, in term of :

- risk analysis of hazards originating from machinery.
- implementation of measures either to minimize or eliminate any risks.
- documentation of residual risk.
- production of whole machinery documentation.

The **User/Operator** is responsible for safety concerning application and use.

Safety function implementation and selection according to application. STO safety function integration:

- Risk analysis and risk assessment according to EN 12100-1, EN 12100-2, EN 14121-1.
- Risk reduction by machine design.
- Risk reduction by protective equipment.
- Identification of safety requirements.
- PL, SIL, Category selection.

3 STO safety normative adherence

"Safe Torque Off" integrated safety function meets the following standard requirements:

- ❖ safety integrity level SIL3 according to EN 61508 and EN61800-5-2
- ❖ PL e according to EN13849-1

In case of activation or error the safety function STO avoids torque production onto the motor, which eventually could cause mechanical movements.

If STO function is integrated in a system supporting Emergency stop function, it is mandatory to design appropriate and dedicated control systems, according to EN 60204-1 "Arresto di emergenza in categoria 0", to support stop category 0 or stop category 1.

Emergency stop function can be designed to support either:

- **Stop category 0:** uncontrolled stop coasting to standstill. Stop by means of energy supply disconnection.[1]
- **Stop category 1:** Stop is obtained by means of a controlled phase (torque control) in order to minimize braking time. When standstill is reached or after a time delay the energy supply is disconnected. A latching device to prevent access to hazard zones is also mandatory.

[1] Drive might be not stop immediately due to supply disconnection. Whether a mechanical brake isn't installed a risk has to be evaluated .

4 Safety function description

Safe Torque Off safety function is implemented by means of internal circuitry of ADV200. Safety circuits are embedded in control board which manages **CONTROLLER ENABLE** signal and another dedicated circuit which can be hosted in either a separated board called EXP-SFTY-ADV (optional card board for ADV sizes up to 6) or a signal conditioning board called INT-P-ADV (for ADV biggest size, 7 and ADV200-LC size 8). Both INT-P-ADV and EXP-SFTY-ADV manage a signal called "**SAFETY ENABLE**" and a feedback signal named "SAFETY FEEDBACK ENABLED".

4.1 Device functionality and architecture

The system here examined are Power Drive Systems (PDs) also called Inverters. A PDS is power device connected one side to the mains (three-phase system) and on other side to the motor power lines. The PDS makes the motor move according to the settings operator has defined.
From the electrical point of view PDS takes power from mains to the motor lines.
Inverter device family ADV is the subject of this document. From the safety and main functionality points of view all devices belonging to the family are the same, herein represented in Figure 1 and Figure 2.

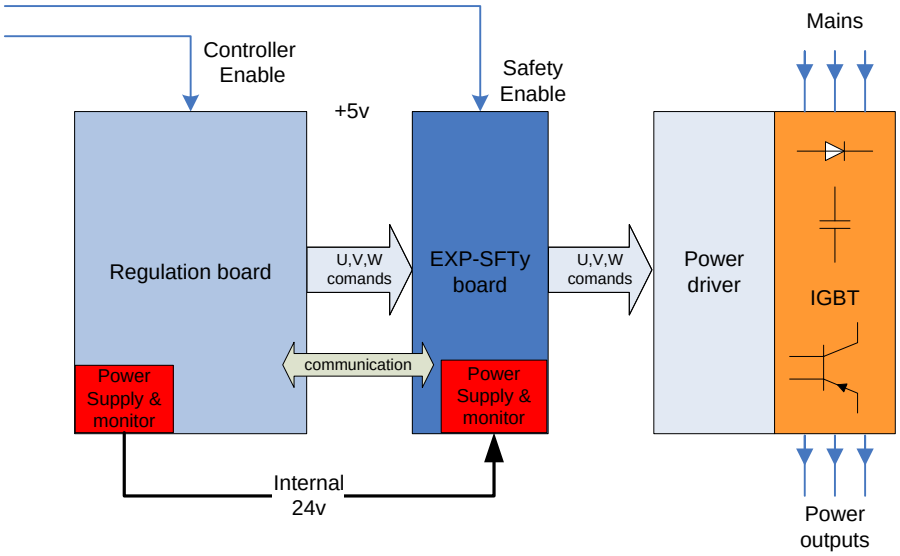


Figure 1. block diagram of ADV PDs size 1-6.

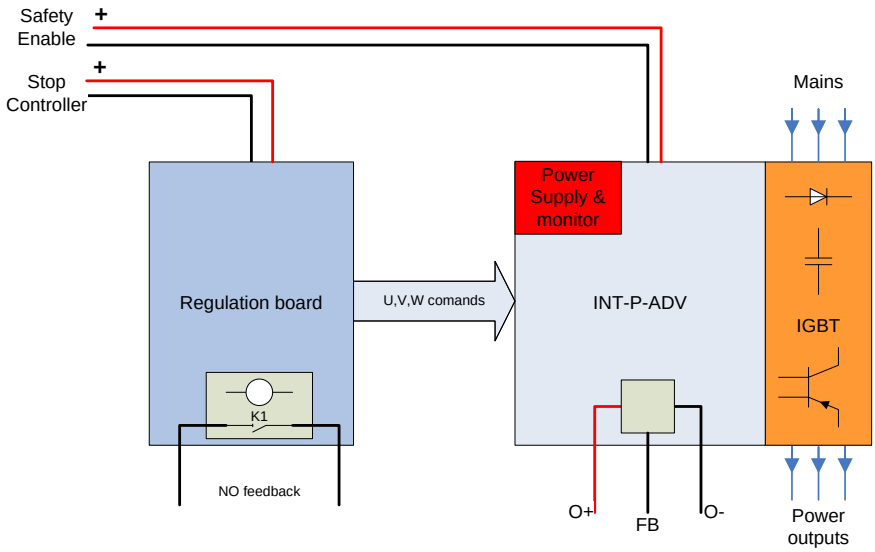


Figure 2. block diagram of ADV PDs size 7 and ADV200-LC size 8

From the safety perspective the ADV size 7 (the biggest size) is different from the other in that it duplicates and integrates two safety channels on the driver board: the regulation safety channel and the EXP-SFTy safety circuit. The driver board is called INT-P-ADV and integrates the mentioned circuits as said.

All ADV PDs are integrated PD devices featuring different power ratings, dimensions as well as enclosures. Though from the functional point of view all devices are made up of the same fundamental four parts:

1. Regulation board
2. Driver board
3. Safety board
4. IGBT power module

For size 1-6 the four parts listed above relate to separate printed circuit boards (PCB) or electric modules each featuring different functions within the system. For size 7 functional units 2 and 3 are hosted onto the same physical printed circuit though the areas and functionalities are well separated.

Follows a brief description of four parts:

- **Regulation board:** exists as separate PCB, main purpose of this board is to generate coordinated PWM pulses going to the IGBT gates. PWM pulses are controlled and generated by the software according to the settings to provide given voltage, current, motor speed, motor acceleration, etc options. PWM pulses can be cancelled out directly onto the regulation board by means of a PWM inhibit signal which acts directly on a gating buffer. This signal is called **Controller Enable** and when turned on (circuit input draws current) enables the regulation to output coordinated PWM pulses. Of course the onboard software monitors the enable signal and starts/stops the (software) generation accordingly. A power supply stage, providing voltages for all onboard digital circuits is included on this board.
- **EXP-SFTY-ADV board/Safety circuit INT-P-ADV**: exists as separate part optional expansion board implementing two safety paths for the safety function. This board is necessary to claim a SIL3 safety level. The PWM signals are physically routed through this board before reaching the power board. When $\overline{\textbf{SAFETY ENABLE}}$ signal is unasserted it assures gate commands cannot reach drive stage. When $\overline{\textbf{SAFETY ENABLE}}$ is turned off (input draws current) disables the safety mechanisms and allows gate command signals through the board.
- **IGBT driver:** exists as separate PCB. IGBT driver is the interface system between signals coming from EXP-SFTY-ADV card and the power part. This subsystem comprises an opto-isolation isle, a conditioning part, connected to mains supply driving IGBT gates.
- **IGBT Module**: IGBT is the actual power module comprising heatsink, fans, electrical shield, electric power wires.

From the operator point of view system is managed by means of either remote PC like interface connected to the PDs or using an onboard keypad. Both way operator may set/change parameters that modify the system functions accordingly: speed, torque, position, acceleration, etc. All functions are translated and implemented by means of a different gate command sequence arriving to the IGBT gates.

4.2 Safety function specifications

Safety function “Safe Torque Off” used in ADV200 family assures that drives safely disable motor movements taking off torque onto the motor.

The Safety integrity level SIL3 is guaranted if both CONTROLLER ENABLE (terminal 7 of the drive ADV200) and SAFETY ENABLE (terminal 1 of the Safety card) are deactivated.

Functionally speaking it does not matter which one comes first. Though STO function activates when either of the mentioned signals is deactivated, STO Safety Integrity Level cannot be guaranteed as long as both signals are not deactivated.

Whenever STO function is enabled PDS will no longer provide torque onto the motor, meaning that motor will come to a stop safely. Time event sequence that takes motor stopped depends onto motor inertia as shown in Figure 3 STO function only specifies times at which torque is no longer applied onto the motor (Ttoff) and time elapsed before signal feedback assertion (Tfbon).

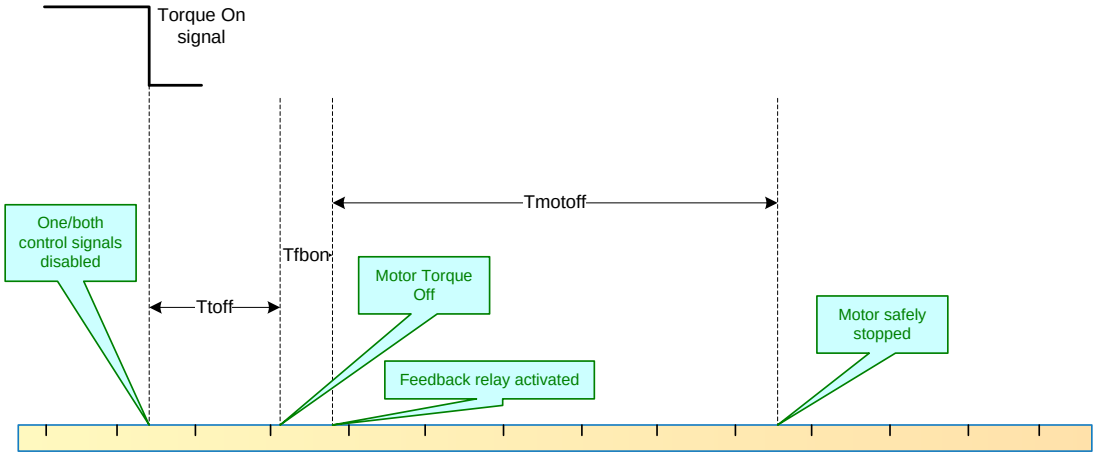


Figure 3. Time event diagram for STO function.

Times are equal or less than which stated in the following table:

- T_{toff} time from control signal disabled to STO function activation: max 14msec
- T_{fbon} time from STO function activation to feedback signal changing state: max 4msec
- T_{motoff} time from STO function activation to motor stop: depends on motor/load inertia

STO function provides two independent safety channels/paths within the integrated drive unit. A fault on a channel does not interfere with operation on the other channel. Fault tolerance for the drive unit is 1. In order for the system to support the same fault tolerance wiring and connections must be properly designed and implemented.

Each channel will be activated/deactivated by a different input. Inputs are safely separated and far from each other to guarantee electrical and functional isolation.

Each safety channel provides a feedback signal issuing alarms in case of diagnosed failures or bad-operations. Safety channels shall be used in order to provide a safety integrity level equal to that claimed in following specifications.

PDS STO function uses one channel implemented on the controller (regulation board) and one channel on a different board (safety board).

Inputs are called respectively:

- **CONTROLLER ENABLE**
- **$\overline{\text{SAFETY ENABLE}}$**

4.3 Safety integrity level

A limit on probability of random failure per hour (PFH) should be calculated on a time-span of 20 years (mission time). PFH will be not greater than $1x10^{-10}$.

According to applying standards EN 61508 and EN61800-5-2, safety integrity is SIL3 classified.

4.4 Safety Fault Reaction System

Hardware mechanisms on both Regulation and Safety board have been established to detect and react to a fault detection.

Signals **DRIVE OK** and **SAFETY ENABLED** are provided to issue fault alarms to external monitoring devices.
Normal behavior of these signals is described in Table 1. In order to exploit dynamic principle feedback signals shall normally change status according to the input levels.

Asserting an alarm on a feedback signal means the feedback signal status does not comply with behavior described in Table 1.

In case hardware/software onto Regulation board detects some faults it will assert an alarm on **DRIVE OK** and (if software intervenes) stop generation of PWM gate pulses.

In case hardware onto Safety board detects some faults it will issue an alarm on **SAFETY ENABLED** and possibly activate one of the safety channels so that PDS is stopped anyway.

In order to make faults more evident and take system to a safe state independently of external monitoring device, safety function has been designed so that most of the detected failures actually block the PDS when drive is being normally operated. All detected failures shall raise alarm issues by means of feedback signals.

Feedback signals shall be designed to react to fault detection in a time no longer than 10ms.

Feedback signal status is described in next table as function of inputs

CONTROLLER ENABLE	$\overline{\text{SAFETY ENABLE}}$	K1 feedback (Drive OK)	FB Feedback (Safety Enabled)
24v	Open	Closed	O-
Open	24v	Open	O+
Open	Open	Open	O-
24v	24v	Closed	O+

Table 1. Feedback relay contact status as function of enable inputs.

The Safety feedback is not only the recognition of the implementation of the Safety Enable command, it take care also to report a possible unexpected failure into the safety circuit or the drive power supply. For example if a failure in the power supply of the regulation board (+5Vdc) is detected the safety circuit blocks the gate commands and issues feedback On.

The Safety functionality must give a different feedback than expected. So:
- if Safety Enable is On and the +5Vdc of the regulation board is correct, the Safety feedback will be On
- if Safety Enable is On and the +5Vdc of the regulation board is not correct, the Safety feedback will be Off
- if Safety Enable is Off and the +5Vdc of the regulation board is correct, the Safety feedback will be Off
- if Safety Enable is Off and +5Vdc is not correct then the Safety feedback will be always On.

In case external supply of the Safety card is provided and main power supply of the drive (AC or DC) is not, the Safety Feedback will change its state when the regulation +5Vdc falls below its rated value:
- Supplying the Safety card with the 24Vdc of the drive (ADV200), when the DC bus value will give under the minimum value necessary to supply the regulation card, also the +24Vdc of the drive will go down and the Safety feedback will be Off.

- Supplying both Safety card and regulation board of the drive with an external +24Vdc (not from the drive) the feedback will follow the Safety Enable command until a real problem on the regulation board will lead to an IGBT inter-block and feedback state change.

5 Installation and commissioning guidance

EXP-SFTY-ADV or INT-P-ADV are integrated safety features of drive series ADV200. They must be regarded as parts of safety related control system of a machine. Only risk analysis and assessment of the machine as in §2 can verify adequacy of the safety control system.

Risk analysis and assessment shall be developed with full knowledge of STO safety function characteristics and limits.

Installation and commissioning shall be performed only by qualified personnel fully aware of the risks generally and specifically involved in the operations (see §1).

Generally speaking installation sustaining highest integrity levels requires some basic principles:

- Both enable signals shall be used with full wiring redundancy in order to sustain fault tolerance equal or greater than 1
- Both feedback signals shall be used in order to maximise failure detection capabilities
- Dynamic principle exploited for all signals
- All devices used to assist/monitor/actuate safety related signals shall claim a compliant safety integrity level

Operators shall take machine into operations only after functional and safety tests have been fully performed to verify compliance with respect to risk analysis.

5.1 INT-P-ADV and EXP-SFTY-ADV optional safety feature on ADV200 drive family

Family drives ADV200 support safe torque off function as integrated function only when an optional feature is purchased as a separate feature. Safety option consist of an additional board (EXP-SFTY-ADV) which is installed and tested onto the drive at production stage.

Exception to previous feature exists for ADV size 7 (and ADV200-LC size 8) which embeds the safe torque off safety function as standard into a different board and position called INT-P-ADV.

EXP-SFTY-ADV can be either:

- Installed when a drive is first purchased
- Installed with an revamping procedure performed at production facilities

It must be understood and accepted by the users that EXP-SFTY-ADV can not be installed, accessed, mounted or maintained. Only authorized production facilities or Safety Qualified Experts can access EXP-SFTY-ADV in order to assure safe integrity.

Safety Qualified experts might eventually maintain SR ADV parts being trained to do specific activities and being equipped with instruments and knowledge necessary to re-qualify Safety functions.

Only Gefran can issue the time-limited and device-specific qualification of “Safety Qualified experts” to specialized trained personnel.

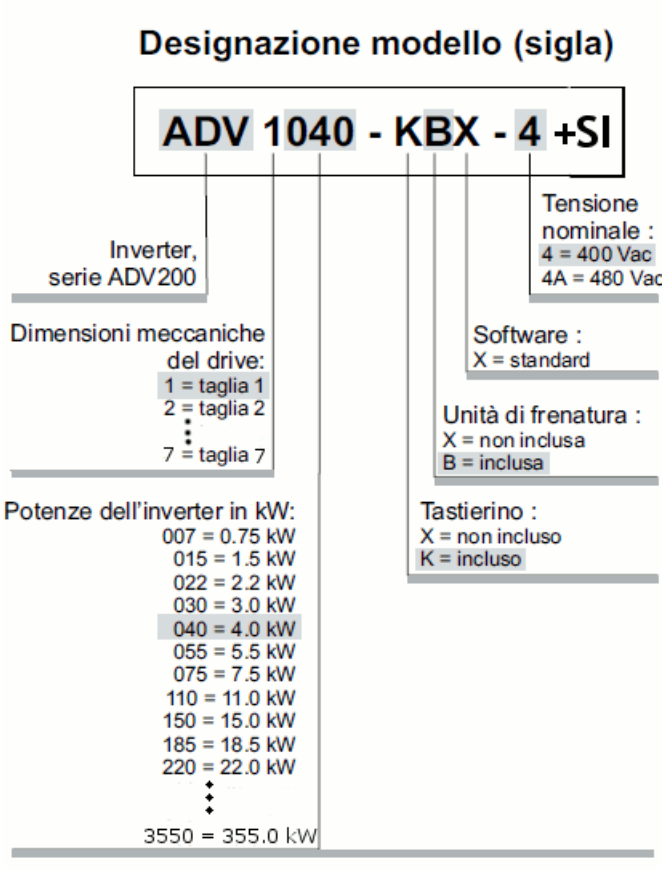
Safety functions herein described is supported by drive family ADV200, according to the following code building description table:

ADVSWWW-PPP-(OOO)**+SI**

Where S = mechanical size of the device
WWW = Output power (kW)

PPP = coding braking unit/Keyboard/Software version
(OOO)= Optional features
+SI = Safe Torque Off Integrated function

Example:



5.2 Connections and use of the "SAFE TORQUE OFF" function

The "SAFE TORQUE OFF" function shall be used to prevent unexpected starting from standstill of the motor. In case motor is running, standstill condition should be achieved with controlled braking, before "SAFE TORQUE OFF" function being activated.
The safety function breaks off power and current onto the drive outputs and makes motor coast. The motor has to be taken to standstill by means a dedicated function.

Connection to safety terminal block (XSC for EXP-SFTY-ADV or TB1 for INT-P-ADV boards) must be protected against external damage (armouring, cable ducting) and isolation protected by means sleeve rated to 600V.

The correct use of "SAFE TORQUE OFF" function has to be made using two safety related signals and usual START drive command:

- "**CONTROLLER ENABLE**" to terminal #7 of drive. The safety function is active with "LOW" signal.
- " $\overline{\textbf{SAFETY ENABLE}}$ signal to terminals #1,2 of SFTy". The safety function is active with "LOW" signal

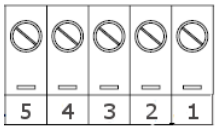
Both connections must be protected against external damage (armouring, cable ducting) and protected by means sleeve rated to 600V.

Separate wirings are necessary for fault tolerance of 1 to be supported at system level.
It should be noticed that any damage to wirings can take conductors either to:

- Short circuit
- Open circuit

Any of the above cases would prevent current from flowing in conductors making Safety function active. Same design philosophy should be used for feedback conductors: current flow in wirings is the normal condition, so that any damage would issue an alarm and be easily identified.

The signals to and from Safety Connector XSC terminal block are shown in following tables
Safety board XSC (or TB1 for INT-P-ADV) Input/Output connector



Following is the position of Safety Connector on both EXP-ADV-SFTY and INT-P-ADV.

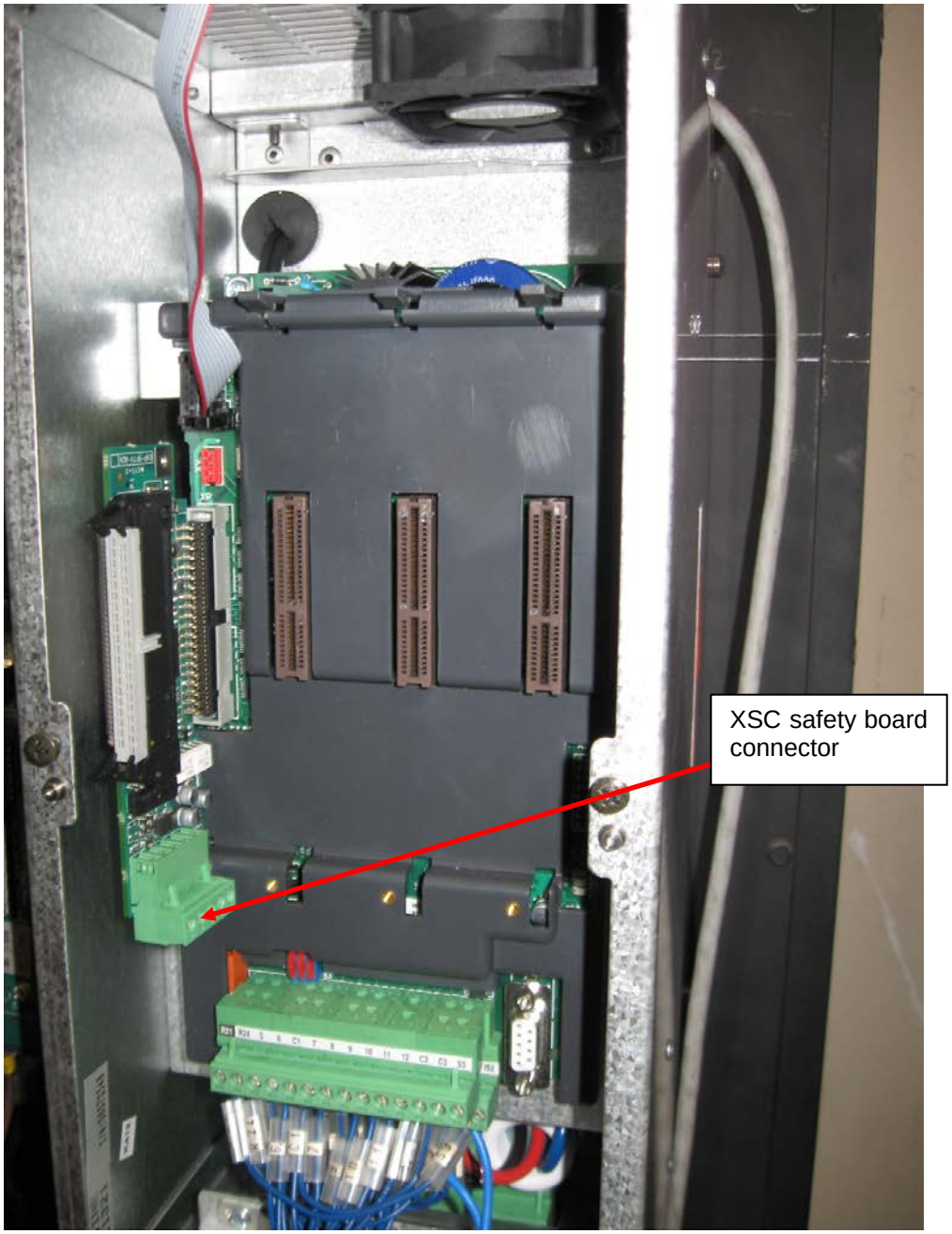


Figure 4. Position of XSC safety board connector

Figure 4 shows position of XSC connector with respect to X1 regulation connector and ADV body whereas Figure 5 shows XSC terminal details.

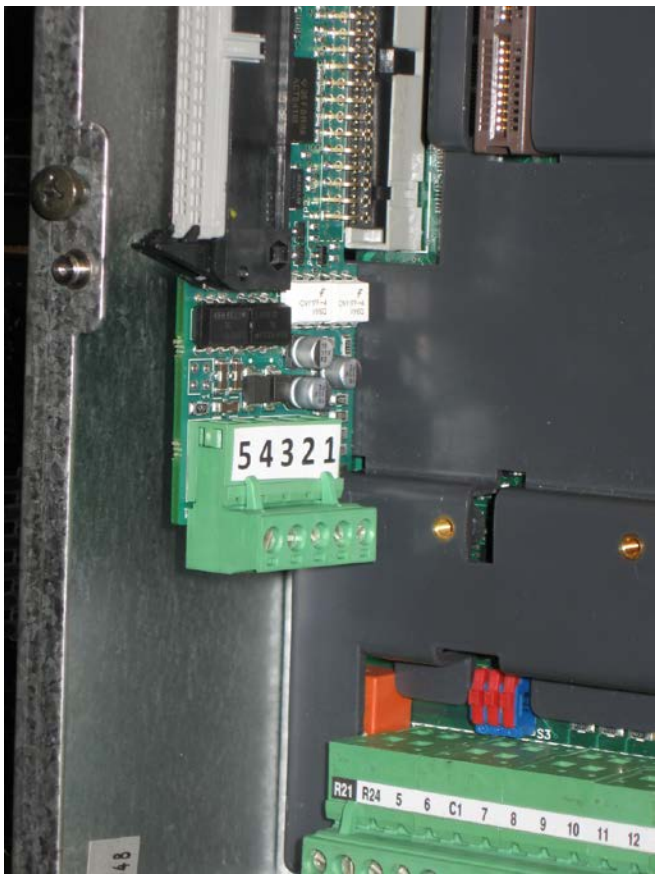


Figure 5. Terminal numbers on XSC

Figure 6 shows position of TB1 connector with respect to INT-P-ADV MASTER board.
Figure 7 shows position of X1 on regulation board

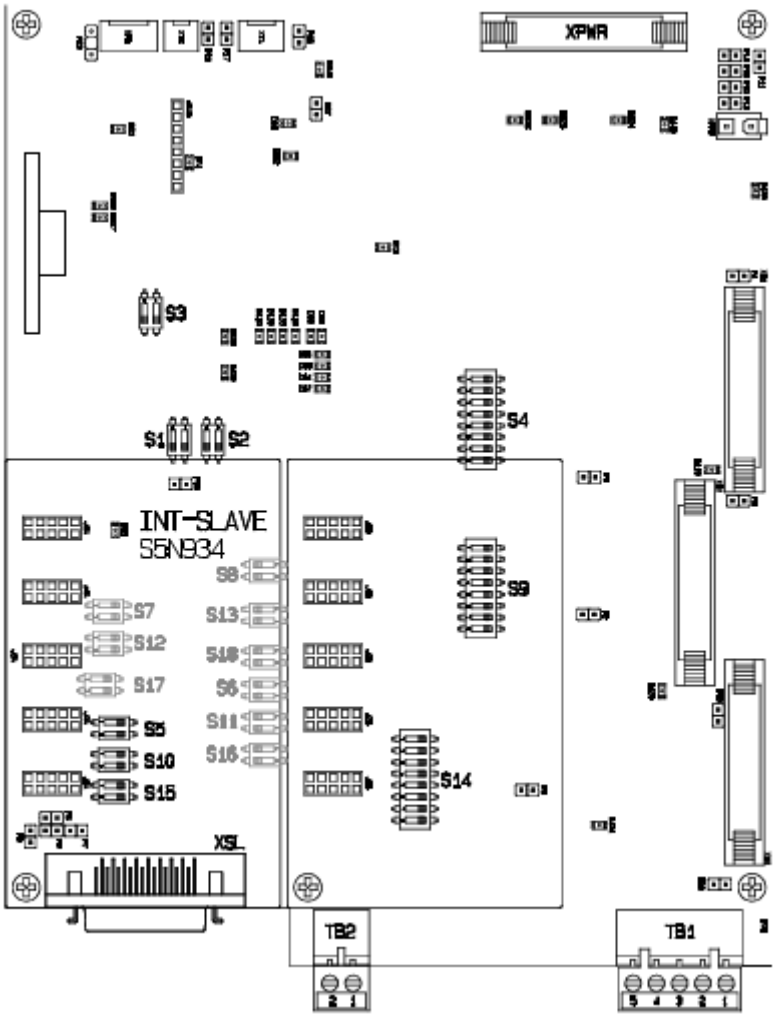


Figure 6. Safety connectors TB1 and TB2 on INT-P-ADV MASTER board (ADV200 size 7 and ADV200-LC size 8)

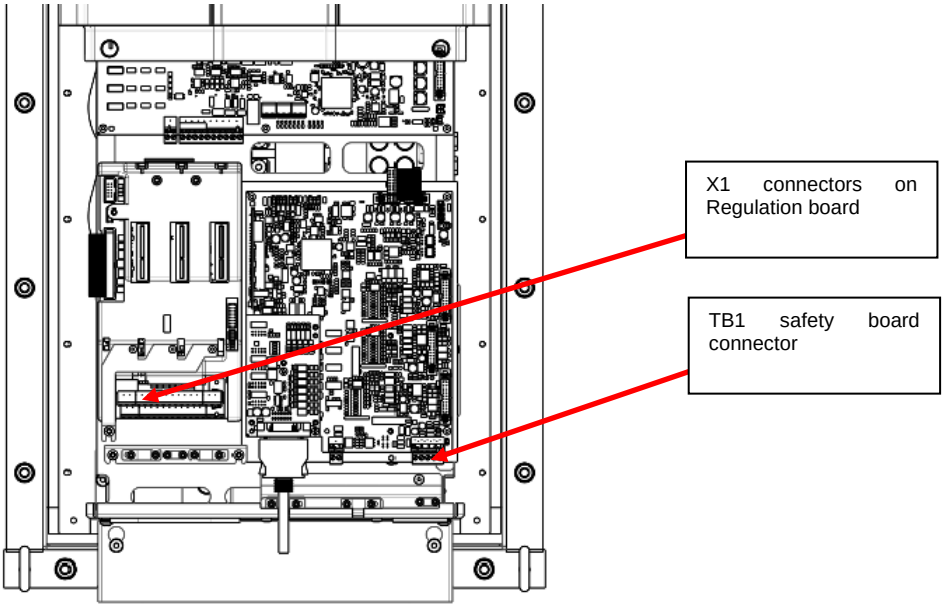


Figure 7. Location of X1 and TB1 connectors (ADV200 size 7 and ADV200-LC size 8)

Safety board connector description

Terminal name	Signal name	Function Description	Electrical limits and range
5	O-	+0 COM power supply for alarm feedback circuit	(IN) 0v
4	FB	+24v@100mA output feedback signal SAFETY DISABLED	(OUT) 0…35v; 150mA maximum DC current
3	O+	+24v power supply for alarm feedback circuit	(IN) +5v…35v with respect to #5
2	- $\overline{\text{SAFETY ENABLE}}$	0v COM for disabling the safety function	(IN) 0v
1	+ $\overline{\text{SAFETY ENABLE}}$	+24v for disabling the safety function	(IN) +12…+35v with respect to #2

Signals to and from main drive connector “X1” are shown in following tables:

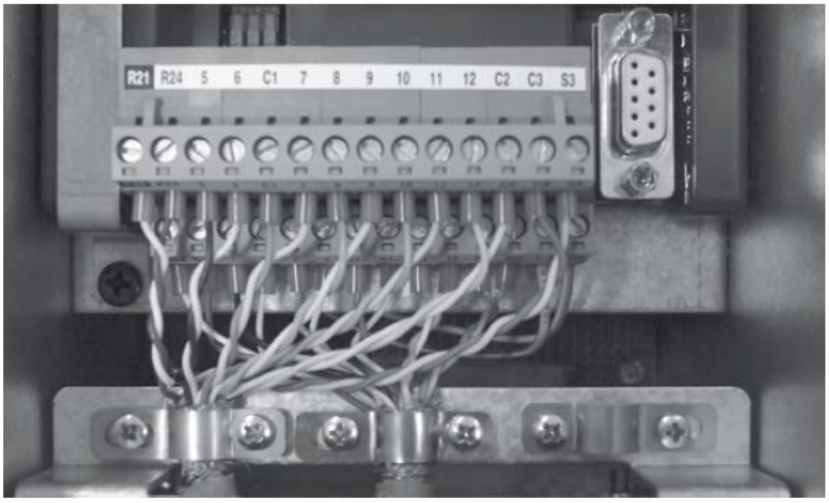
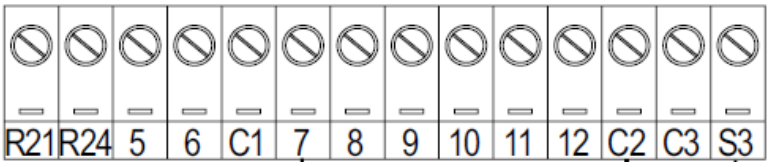
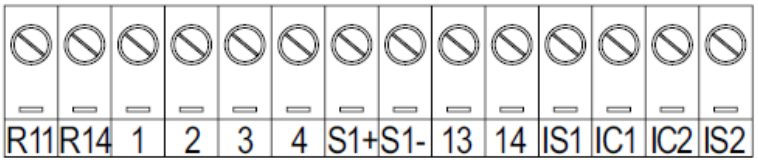


Figure 8. Main regulation connector

Regulation Input / Output connectors (X1)





Terminal name	Function
7	Drive activation signal
C2	COM for activation signal
R14	Drive activation feedback signal (Drive Ok)
R11	COM for Drive activation feedback (Drive Ok)

The “SAFE TORQUE OFF” function prevents unexpected movement of the motor controlled by the drive against undesired starting during shut-down.

Both enable inputs are negatively controlled: STO function is enabled when either input is not exited (voltage not applied on input). Both inputs will be properly excited (energized) in order for the STO function to be disabled and PDS to normally operate. Following table specifies STO function behaviour.

CONTROLLER ENABLE	$\overline{\text{SAFETY ENABLE}}$	STO function status
24v	OPEN	ENABLED[2]
OPEN	24v	ENABLED[2]
OPEN	OPEN	ENABLED
24v	24v	DISABLED

Table 2. STO function status as controlled by inputs.

System also provides 1 feedback signal, which must be used according to manual and installation guide in order to increase the safety integrity level of the system. The feedback signal is opto-isolated and based on a three wire system (O+,FB,O-). O+, O- should be supplied with a low voltage DC.

Following is a simplified diagram showing all electrical connection necessary for using STO safety function.

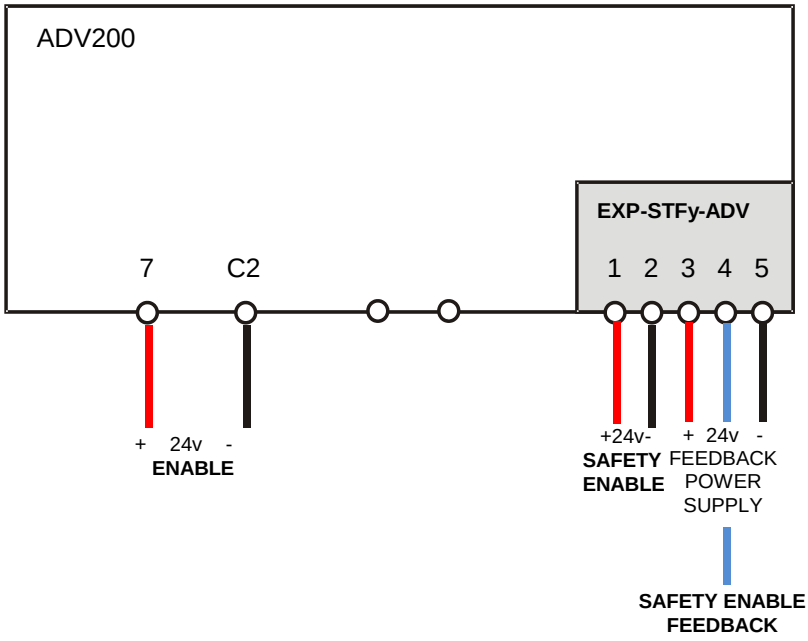


Figure 9. Simplified connection diagram for STO function

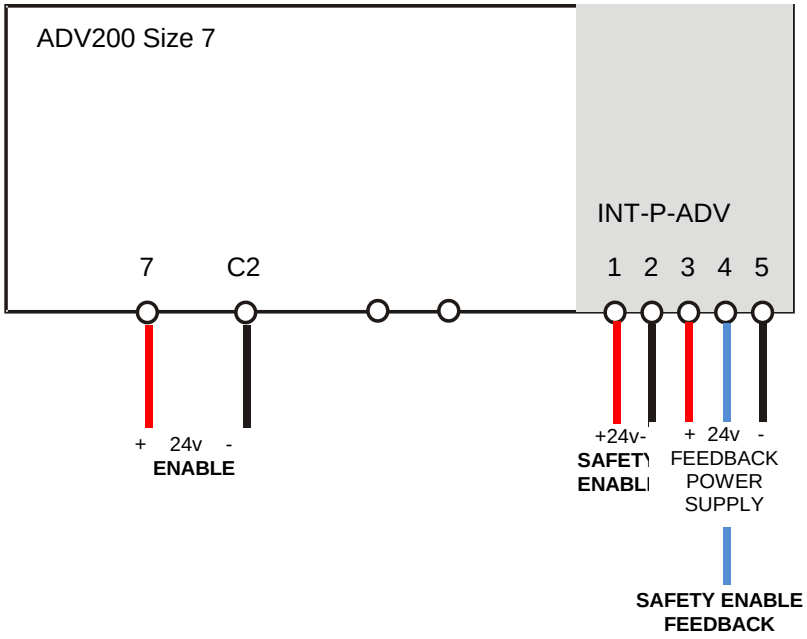


Figure 10. Simplified connection diagram for STO function (ADV200 Size 7 and ADV200-LC size 8)

[2] Safety functionality is actually activated, but SIL3 level is not achieved if both input signals are not deactivated

As above showed the signals involved are:

1. Input control signal 0V…24V dc, that controls disabling of the drive via SFTy circuit. Terminals 1, 2 of Safety Connector.
2. A second input control signal 0V…24V dc, that controls disabling of the drive via "**CONTROLLER ENABLE**" command to regulation board on drive, at terminal 7.
3. An output monitor of the status of the AC drive concerning the pulses cancellation due to "**CONTROLLER ENABLE**". The monitor is by means a free potential contact at terminals #R14 and #R11. The contact in always closed when the cancellation of the pulses is active, i.e. the motor is not permitted to rotate.
4. Two contacts used to power the output feedback circuit. Contacts are at terminals #3 and #5.
5. An output feedback signal from safety board to monitor safety integrity of EXP-SFTY-ADV. Contact is at terminal #4.

5.2.1 Control sequence

Normal use of EXP_SFTY_ADV safety function shall follow a predefined sequence as for enabling as well as for disabling safety function.

DISABLING SAFETY FUNCTION

Drive is in stop condition, both enable signals are disabled. In order to disable SAFETY STO function properly, following action sequence applies:

1. FEEDBACK signals DriveOK and SAFETY DISABLED are checked for congruency
2. $\overline{\textbf{SAFETY ENABLE}}$ signal issued high (24v applied)
3. **CONTROLLER ENABLE** is issued high (24v applied)
4. FEEDBACK SAFETY DISABLED is checked for congruency
5. START command can now be applied to start motor and provide power

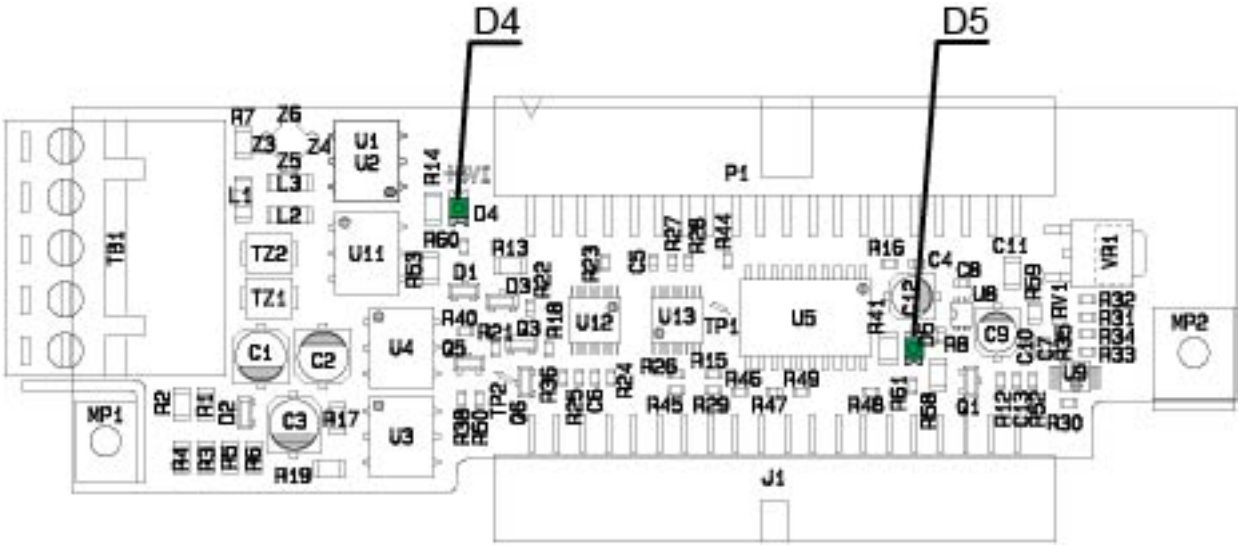
ENABLING SAFETY FUNCTION

Drive is running and powering a motor, both enable signals are enabled. In order to activate SAFETY STO function properly following action sequence is applied:

1. STOP command is issued to stop motor and power generation
2. CONTROLLER ENABLE issued low
3. $\overline{\textbf{SAFETY ENABLE}}$ signal issued low

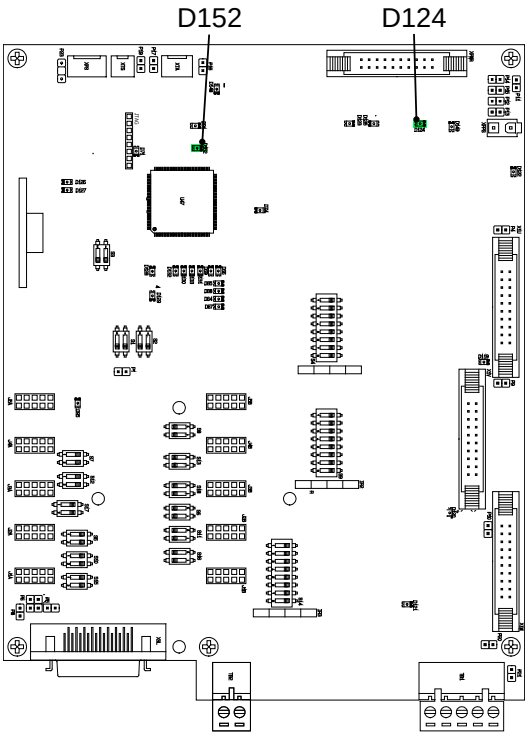
5.3 LEDs

5.3.1 LEDs on EXP-SFTy-ADV card, from Rev E and higher



Leds	Colour	Meanings
D4	Green	ON when the EXP-SFTY-ADV card is powered
D5	Green	ON when the safety input is bypassed (drive enabled)

5.3.2 LEDs on INT-P-ADV card, from Rev L and higher



Leds	Colour	Meanings
D124	Green	+ 5V monitor
D152	Green	+ 5V monitor

6 Operation and maintenance requirements

6.1 Operations

Operations must comply with electrical precautions and ranges so far claimed and explained. Following a table of the most important electrical drive precautions to comply with:

Signal	Electrical safety constrains
Input $\overline{\text{SAFETY ENABLE}}$ #1,#2	Voltage shall not exceed 35v and shall not be inverted applied.
Safety feedback power contacts #3,#5	Voltage and current shall not exceed 35v.
Safety feedback contact #4	Current shall not exceed 150mA.
Input CONTROLLER ENABLE #7,#C2 X1 connector	Voltage shall not exceed 35v and shall not be inverted applied.
Drive feedback output relay #R14,#R11 X1 connector	Voltage shall not exceed 35v and current shall not exceed 200mA

PDS shall only be operated according to environmental conditions specified in device manual herein reported.

Type	Operation installed for stationary use	Storage in the protective package	Transportation in the protective package
Max Installation Site Altitude	Up to 2000m		
Air Temperature	-10…50°C	-25...55°C (class 1k4 EN50178)	-25...55°C (class 2k3 EN50178)
Relative Humidity	5...85% (Class 3k3 as per EN50178)	5...95% (Class 1k3 as per EN50178)	5...95% (Class 1k3 as per EN50178)
	No condensation or icing allowed.		
Contamination Levels (IEN 60721-3-3)	No conductive dust allowed.		
	Boards without coating: Chemical gases: n.a. Solid particles: no conductive **Boards with coating:** Chemical gases: n.a. Solid particles: no conductive	**Boards without coating:** Chemical gases: n.a. Solid particles: no conductive **Boards with coating**: Chemical gases: n.a. Solid particles: EN 60068-2-52: test Kb, salt solution 5%, duration test 24 h	
Atmospheric Pressure	86 to 106 Kpa (class 3K3 as per EN50178)	86 to 106 Kpa (class 1K4 as per EN50178)	70 to 106 Kpa (class 2K3 as per EN50178)
Vibration (EN 60068-2-6) (EN 60068-2-34)	Sinus 10...150Hz 2g Random 5....200 0,005g^{2}Hz	n.a	n.a.
Shock (EN 60068-2-29)	no allowed	n.a	n.a.
Free Fall	n.a.	250mm	250mm
Approvals	CE		
Degree of pollution	Pollution degree 2 or better (free from direct sunligth, vibration, dust, corrosive or inflammable gases, fog, vapour oil and dripped water, avoid saline environment)		
Degree of protection	IP20 IP54 for cabinet with externally mounted heatsink (size types 1007 and 3150)		
EMC	EN 61800-3		

Any differences with respect to claimed operating conditions could overstress the device and diminish the safety integrity of the system.

6.2 Maintenance

Expected operation life-time of the system is 20 year or 10milion operations. After one of the two parameters is exceeded drive should be returned to manufacturer to proper safety revamping procedures.
Any malfunctions/failures shall summon users/assisting personnel to immediately inform assistance and take proper actions to fix the problem.
Periodic maintenance is not necessary nor scheduled unless specific conditions or machine integration is necessary.

Only “Safety Qualified Experts” are authorized to replace, maintain, test or repair SR-PDS parts of ADV PDS. This not only implies to be qualified person as described in §1 but to be also trained on specific procedure to manage, investigate, assembly and test all internal safety related parts of ADV.

Safety Qualified experts might eventually maintain SR ADV parts being trained to do specific activities and being equipped with instruments and knowledge necessary to re-qualify Safety functions.
Only Gefran can issue the time-limited and device-specific qualification of “Safety Qualified experts” to specialized trained personnel.

6.3 Operational tests

Qualified personnel shall periodically verify the drive unit as black-box unit. Assisting personnel shall verify the input-output tables with respect to what is above specified. Periodic test will verify:

- Motor torque is deactivated when either **CONTROLLER ENABLE** or **$\overline{\text{SAFETY ENABLE}}$** are activated
- Feedback signal are properly controlled as functions of **CONTROLLER ENABLE**/ **$\overline{\text{SAFETY ENABLE}}$** inputs.

Periodic test shall be performed at least once a YEAR.

6.4 Troubleshooting

Following is a troubleshooting table to be used in case of not proper functioning or doubts about safety functionality.

Effect	**Possible cause**	**Action**
Drive does not work in any input signal configuration	Electrical level inverted onto **CONTROLLER ENABLE**	Check contact #7 onto X1 connector be +24v DC with respect to #C2 contact.
	Electrical level inverted onto **$\overline{\text{SAFETY ENABLE}}$**	Check contact #1 onto Safety connector be +24v DC with respect to #2 contact.
	START command is not properly issued.	Check START command is properly issued after **CONTROLLER ENABLE** is asserted.
Regulation Feedback signal (drive OK) does not change status according to table 1.	Drive has not been properly configured.	Check ADV200 configuration. See ADV200 user manual.
Safety feedback signal (SAFETY DISABLED) does not change status according to table 1.	Contacts #3-#5 are not powered with +24v.	Check contact #5 onto Safety Connector connector be +24v DC with respect to #3 contact.
Safety feedback signal (SAFETY DISABLED) is high (+24v) when drive is stopped.	**CONTROLLER ENABLE** is still enabled. Drive is still producing PWM pulse on the Safety input.	Properly enable/disable both **CONTROLLER ENABLE** and **$\overline{\text{SAFETY ENABLE}}$**

7 Application examples

Following are some application examples which show how to implement and use suitable safety control devices together with STO integrated function for different emergency stops as defined in EN60204.

7.1 Reference design example for supporting STO at SIL3

Following is a reference design to use as example to implement a SIL3 STO safety function at system level. It is underlined that this is not a complete machine design in that application specific safety features have to be properly evaluated and integrated into the design. Use of STO function must be correctly linked to the safety function at system level designer wants to implement.

Reference design assumes that any dangerous operations (e.g. access to dangerous areas) makes the **SAFETY ENABLE** press-button pressed. Once safety standstill is activated, SAFETY RESET pushbutton must be pressed in order to re-activate the machine.

One safety monitoring device and one double contacts relay are used. Safety monitoring device always acts on both enable signals so that maximum degree of reliability is achieved.
Safety monitoring device can be restarted only when S33-S34 is closed. In order to stay into activated status safety device verifies circuits S11-S12 and S21-S22 are closed.

Safety feedbacks are used to open either

- open a normally closed circuit (#R14-#R11 and K1) to immediately stop the machine
- open the normally closed circuit (K1) to make it impossible for the machine to be restarted.

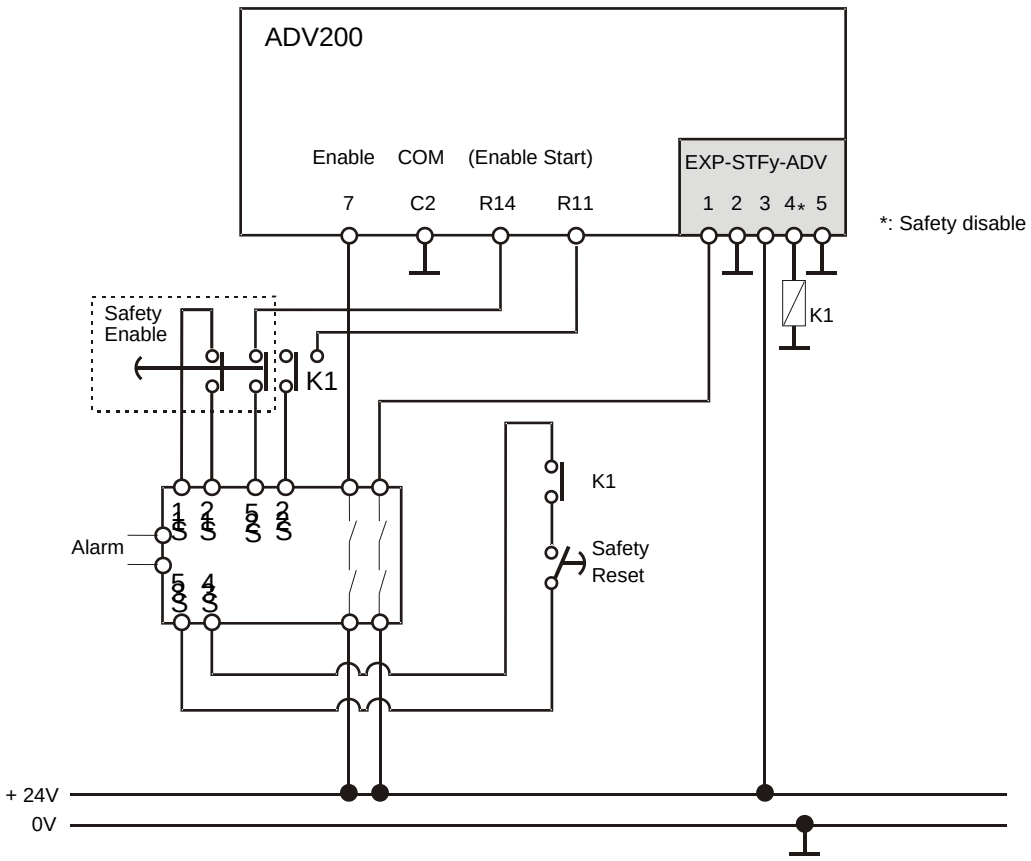


Figure 11. SIL3 connection diagram

It is worth pointing out some general safety rules used in the reference design:

- both safety channels and enable signals have to used to enable/disable the safety function at the proper safety integrity level
- safety feedback have to used in order to prevent the machine from restarting if a fault is diagnosed and/or make the fault evident to operators.

- Double redundancy is necessary at wiring level on the whole system in order to support fault tolerance of 1

7.2 Reference design example for SIL2 applications

Following is a reference design to correctly use Safety integrated ADV200 drives for SIL2 safety applications (where risk assessment permits it). As shown in the Failure Analysis, not using the feedback signals makes the integrity level of STO function diminish at SIL2 level. Nonetheless using a simplified connection diagram might be valuable where risk allows it.
In any case EXP-SFTY-ADV function must be correctly activated/deactivated to avoid any damages to drive and connected equipments. Particularly important is to implement a correct start/stop sequence in order not to suddenly break off currents through the power lines.

Correct start sequence requires:

- **CONTROLLER ENABLE** being asserted after SAFETY DISABLED (de-asserted).
- Motor comes to a stop before asserting $\overline{\textbf{SAFETY ENABLE}}$ signal.
- If motor is running de-asserting **CONTROLLER ENABLE** before $\overline{\textbf{SAFETY ENABLE}}$

Reference design assumes that any dangerous operations (e.g. access to dangerous areas) makes the SAFETY ENABLE press-button pressed to open. Once safety standstill is activated, $\overline{\textbf{SAFETY ENABLE}}$ press-button must be pressed into close status.

Following design does not use feedback signals resulting in a much simpler connection diagram.

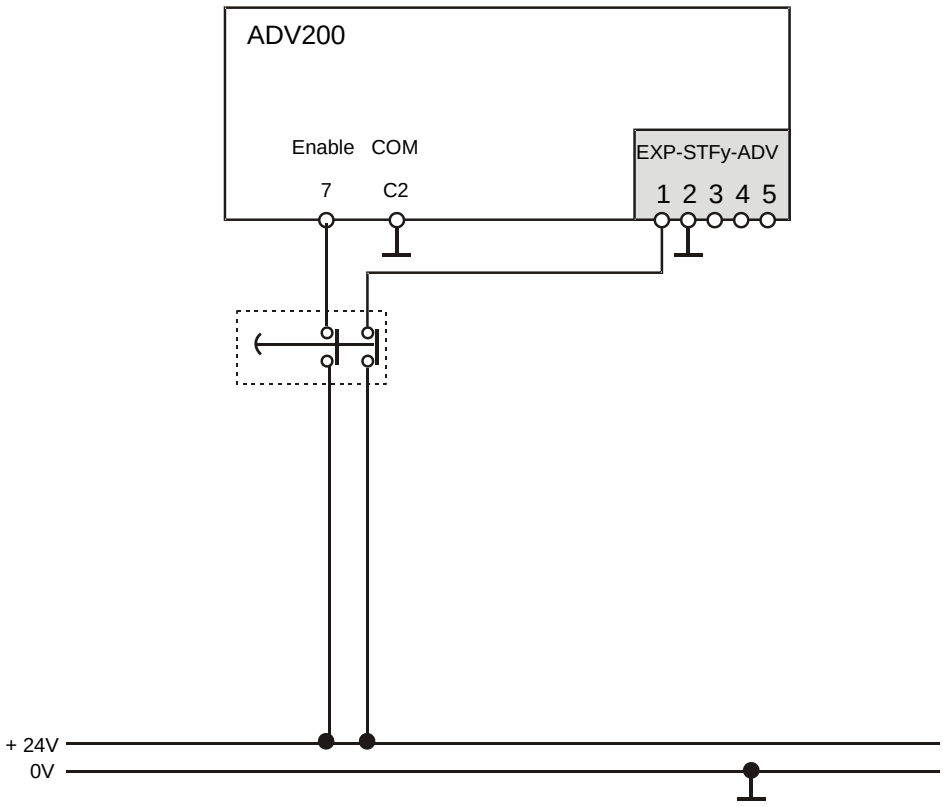


Figure 12. SIL2 connection diagram

It is worth noticing that:

- $\overline{\textbf{SAFETY ENABLE}}$ signal is activated before **CONTROLLER ENABLE**
- **CONTROLLER ENABLE** and $\overline{\textbf{SAFETY ENABLE}}$ are deactivated simultaneously; design requires motor came to a stop before de-activating drive.

Gefran worldwide

GEFRAN DEUTSCHLAND GMBH
Philipp-Reis-Straße 9a
D-63500 Seligenstadt
Ph. +49 (0) 61828090
Fax +49 (0) 6182809222
vertrieb@gefran.de

SIEI AREG - GERMANY
Gottlieb-Daimler Strasse 17/3
D-74385 - Pleidelsheim
Ph. +49 (0) 7144 897360
Fax +49 (0) 7144 8973697
info@sieiareg.de

SENSORMATE AG
Steigweg 8,
CH-8355 Aadorf, Switzerland
Ph. +41(0)52-2421818
Fax +41(0)52-3661884
http://www.sensormate.ch

GEFRAN FRANCE SA
4, rue Jean Desparmet - BP 8237
69355 LYON Cedex 08
Ph. +33 (0) 478770300
Fax +33 (0) 478770320
commercial@gefran.fr

GEFRAN BENELUX NV
ENA 23 Zone 3, nr. 3910
Lammerdries-Zuid 14A
B-2250 OLEN
Ph. +32 (0) 14248181
Fax +32 (0) 14248180
info@gefran.be

GEFRAN UK LTD
Unit 7, Brook Business Centre
54a Cowley Mill Road, Uxbridge,
UB8 2FX
Ph. +44 (0) 8452 604555
Fax +44 (0) 8452 604556
sales@gefran.co.uk

GEFRAN MIDDLE EAST ELEKTRIK VE ELEKTRONIK SAN. VE TIC. LTD. STI
Yesilkoy Mah. Ataturk
Cad. No: 12/1 B1 Blok K:12
D: 389 Bakirkoy /Istanbul
TURKIYE
Ph. +90212 465 91 21
Fax +90212 465 91 22

GEFRAN SIEI
Drives Technology Co., Ltd
No. 1285, Beihe Road, Jiading
District, Shanghai, China 201807
Ph. +86 21 69169898
Fax +86 21 69169333
info@gefran.com.cn

GEFRAN SIEI - ASIA
31 Ubi Road 1
#02-07, Aztech Building,
Singapore 408694
Ph. +65 6 8418300
Fax +65 6 7428300
info@gefran.com.sg

GEFRAN INDIA
Survey No. 191/A/1,
Chinchwad Station Road,
Chinchwad,
Pune-411033, Maharashtra
Ph. +91 20 6614 6500
Fax +91 20 6614 6501
gefran.india@gefran.in

GEFRAN INC.
8 Lowell Avenue
WINCHESTER - MA 01890
Toll Free 1-888-888-4474
Fax +1 (781) 7291468
info.us@gefran.com

GEFRAN BRASIL
ELETROELETRÔNICA
Avenida Dr. Altino Arantes,
377 Vila Clementino
04042-032 SÂO PAULO - SP
Ph. +55 (0) 1155851133
Fax +55 (0) 1132974012
comercial@gefran.com.br

GEFRAN

GEFRAN S.p.A.
Via Sebina 74
25050 Provaglio d'Iseo (BS) ITALY
Ph. +39 030 98881
Fax +39 030 9839063
info@gefran.com
www.gefran.com

Drive & Motion Control Unit
Via Carducci 24
21040 Gerenzano [VA] ITALY
Ph. +39 02 967601
Fax +39 02 9682653
infomotion@gefran.com

Technical Assistance :
technohelp@gefran.com

Customer Service :
motioncustomer@gefran.com
Ph. +39 02 96760500
Fax +39 02 96760278