ADL300

Safety User manual

Language: English

Contents

Doc. release	Issued by	Doc. Changes	Doc. Date
0.1	FNT	First release	20/03/2012
0.2	FNT	Contactor-less description	20/06/2012
1.0	FNT	External consultant corrections and suggestions	27/06/2012
1.1	FNT	Added single contactor diagram.	28/01/2013
1.2	BRI	Add manual code, “prEN81-..” to “EN81-..”, pag 3 add EN81-50.	26/05/2017
1.3	BRI	Pag. 7/28/29: EN81-20 5.9.2.5.3 d) to EN81-20 5.9.2.5.4 d)	1/12/2020
1.4	BRI	Pag 31 removed text	8/7/2022

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. **ADL300 drive family supports “Safe Torque Off” as an integrated feature.**

This 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.

ADL300 is a specialized drive family intended for the Lift Market. Given this ADL300 STO function will be primarily exploited to attain safety features permitted and described by C class normative **EN81-1, EN81-20, EN81-50**. Specifically the safety integrated function allows getting rid of one or two contactors and implementation of:

- Car safe stop suing one contactor design
- Car safe stop using contactor-less design

STO is integrated in the drive unit family ADL300, whereas safety capability could also be implemented externally. When Safety is used 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 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 ADL300 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 12100 - 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), 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.

EN81-1 intended for safety in lift applications specifies, functions, safety integrity level and configuration to be used to attain given system level functionalities.

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.
- Risk reduction by machine design.
- Risk reduction by protective equipment.
- Identification of safety requirements.
- 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

Safe Torque Off function can be exploited specifically for Lift Market to support:

- Single contactor operation for Car stop EN81-1 §12.7.3 b)
- Contactor-less operation for Car stop EN81-1 and EN81-20 5.9.2.5.4 d)

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

4 Safety system description

Safe Torque Off safety function is integrated into the drive family ADL300, and is managed by means of two enable signals "**ENABLE**" and "**SAFETY ENABLE**".

4.1 Device functionality and architecture

The system herein examined are Power Drive Systems (PDs) also called Inverter. A PDS is power device connected one side to the mains (three-phase system) and on other side to the motor power lines. Motor and other devices which are related to the system functionalities (relays, cables 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 called ADL300 is subject of this document. From the safety and main functionality points of view all devices of the family can be modeled as the same thing, herein represented in Figure 1.

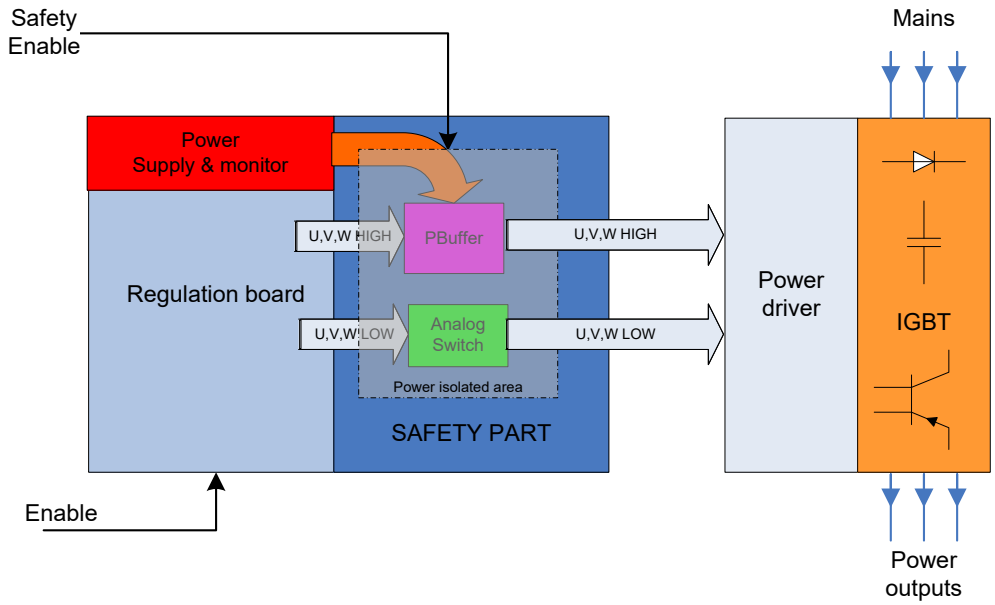


Figure 1 block diagram of PDs ADL300.

All ADL300 PDs are integrated PD devices featuring different power ratings, dimensions as well as enclosures. Though from the functional and electrical points of view all devices are made up of the same fundamental four parts:

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

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

of the hardware PWM generator. Of course the onboard software sees the enable signal when asserted and stops the (software) generation. A power supply stage, providing voltages for all digital circuits and EXP-SFTY-ADV board is included on this board.

- **Safety part**: exists an isolated isle integrated onto the regulation PCB. This part takes in the output PWM signals coming from regulation and according to its ENABLE signal (SAFETY ENABLE) makes pulses pass/not pass on the output connector going to the IGBT driver.
- **IGBT driver:** exists as separate PCB. IGBT driver is the interface system between signals coming from Safety part 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 ADL300 family assures that drives safely disable motor movements taking off torque onto the motor.

STO function becomes active whenever either **ENABLE** or **SAFETY ENABLE** are deactivated (zero voltage applied or open wires and no current flowing). The other way STO function is disable (drive enabled) when both enable signals are asserted (DC 24v applied). Functional logic diagram is shown is Table 1.

ENABLE	SAFETY ENABLE	STO STATUS
Disabled (open/0v)	Disabled (open/0v)	Enabled (Torque off)
Enabled (24v)	Disabled (open/0v)	Enabled (torque off) *[Safety interlock block]*
Disabled (open/0v)	Enabled (24v)	Enabled (torque off)
Enabled (24v)	Enabled (24v)	Disabled (drive operating)

Table 1 Static Functional Table for Safe Torque Off Function.

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 1. STO function only specifies times at which torque is no longer applied onto the motor (Ttoff) and time elapsed before signal feedback assertion (Tfbk).

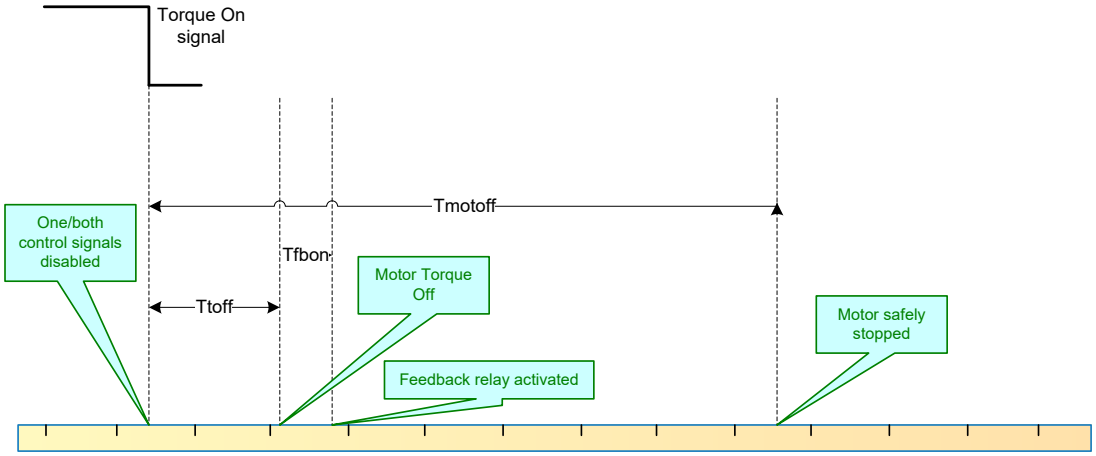


Figure 2 Time event diagram for STO function.

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

Name	Description	Max delay [ms]
Ttoff	Time between **ENABLE/SAFETY ENABLE** signal deactivation and safety channel activation (the same for both **ENABLE** and **SAFETY ENABLE**)	14
Tfbk	Time between **SAFETY ENABLE** and **SAFETY FEEDBACK** change of status	20
Tton	Time between **ENABLE** signal activation and drive activation (Drive Active)	8
Tiblk	In case **SAFETY ENABLE** is issued before ENABLE maximum allowed time before system goes into interblock	8

Table 2 Safety Intervention times.

Looking at the Enable signals evolving dynamically in time, the allowed input configuration are less than those highlighted in Table 1: in order to prevent pwm pulses to be applied suddenly **ENABLE** signal will always follow **SAFETY ENABLE** or, at least be applied before 4ms within it. Should **ENABLE** come first before **SAFETY ENABLE**, ADL drive goes into interlock block and it will be necessary to disable and issue **ENABLE** high again in order to reactivate ADL.

Following figures are describing the dynamics of STO. function:

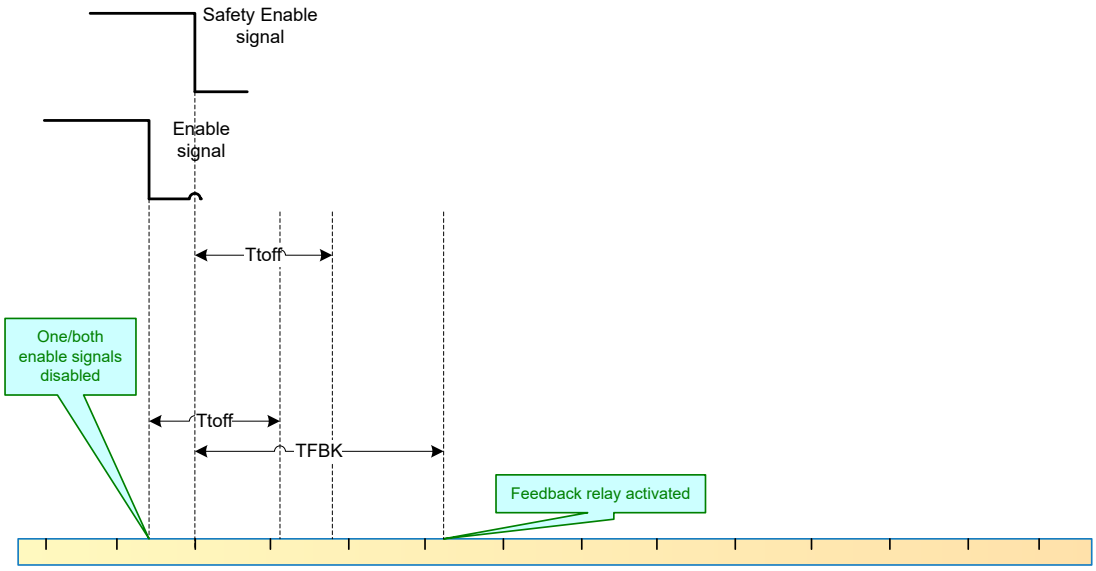


Figure 3 Dynamic view of activation of STO Safety Function.

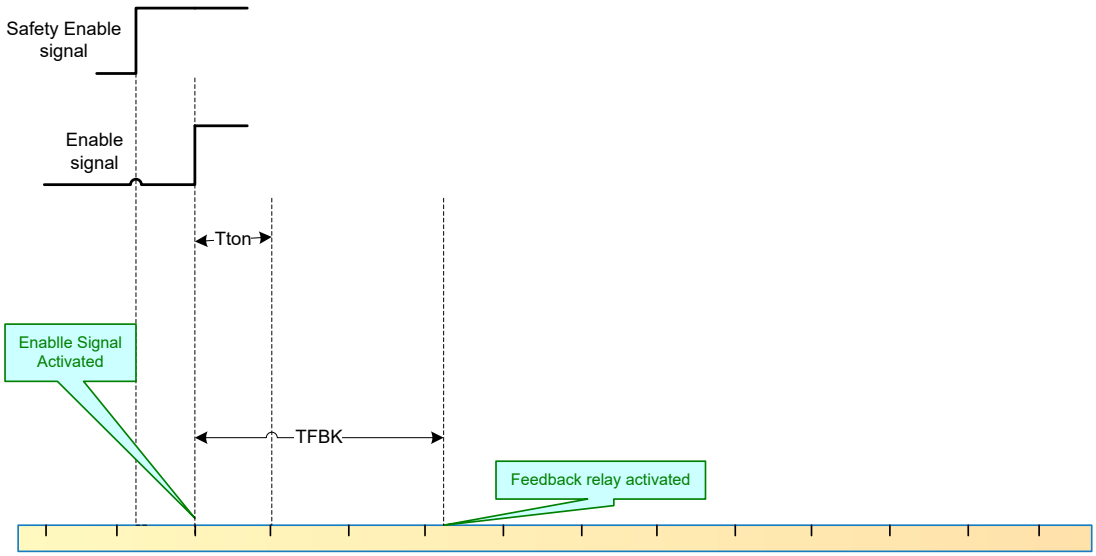


Figure 4 Dynamic view of deactivation of STO Safety Function.

4.3 Safety integrity level

PDS STO function provides two independent safety channels/paths. A fault on a channel should not interfere with operation on the other channel.

Safety architecture has been designed to be fault tolerant with a fault tolerance of 1. This means that whatever failure occurs in the system safety is still guaranteed.

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.

Inputs will be called respectively:

- **ENABLE**
- **SAFETY ENABLE**

A limit on probability of random failure per hour (PFH) should be calculated on a time-span of 20 years (mission time). PFH is less than $1x10^{-9}$. Safety Integrity Level classification according to EN61800-5-2/EN61508 is SIL3.

4.4 Safety Fault Reaction System

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

Signals **DRIVE OK** and **SAFETY OK** are provided to issue fault alarms to external monitoring devices.

Normal behavior of these signals is described in ADL300 User Manual:

- SAFETY OK signals are internally connected to a fixed hardware controlled relay which diagnoses and identifies failures into the safety circuit. SAFETY OK relay behavior is described in Table 4. Asserting an alarm on a SAFETY OK signal means the feedback signal status does not comply with behavior described in Table 4.
- DRIVE OK relay behavior is software configurable. Default configuration acts so that relay is closed if drive ADL300 is ready for receiving an ENABLE signal. *DRIVE OK configuration must be mandatorily changed into **Digital Input Monitor for ENABLE signal** in case of contactor-less applications (§ 7.2* Lift Application Design supporting contactor-less car stop.*).*

In case hardware/software onto Regulation board detects some faults it will assert a Safety Failure Alarm, preventing drive from restarting again till the alarm is manually cleared by qualified personnel.

In order to make failures 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 ADL300 when drive is being normally operated. All detected failures shall raise alarm issues by means of feedback signals.

Regulation board executes all possible integrity checks anytime before starting generating PWM pulses:

- Check ENABLE signal
- Check SAFETY ENABLE signal
- Check SAFETY OK consistency

Should any of the previous checks be failed ADL300 will not start generating PWM pulses. Only qualified personnel after performing all necessary maintenance procedures are authorized to clear the alarm into the drive alarm menu.

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

Terminal name	**Signal name**	**Function Description**	**Electrical limits and range**
EN+	+SAFETY ENABLE	+24v for disabling the safety function	(IN) +12…+35v with respect to EN-
EN-	-SAFETY ENABLE	0v COM for disabling the safety function	(IN) 0v
OK1	SAFETY OK1	Normally closed contact for Safety feedback (contact 1)	250mA maximum DC current
OK2	SAFETY OK2	Normally closed contact for Safety feedback (contact 2)	250mA maximum DC current

Table 3 Description of Signals onto Safety Connector.

SAFETY ENABLE+/-	**SAFETY OK CONTACTS**
Open/0v	**Closed**
+24vDC	**Open**

Table 4 Feedback relay contact status as function of enable input.

5 Installation and commissioning guidance

STO integrated safety function must be regarded as a part 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 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 Safety Function Integrated on ADL300 drive family

Family drives ADL300 support safe torque off function as a standard integrated function tested on each unit shipped from authorized manufacturing plants.

It must be understood and accepted by the users that safety function can not be accessed, modified or maintained outside of the condition herein described. Only authorized production facilities can access the integrated safety function in order to assure safe integrity.

ADL300V-SWWW-PPP-(X)-CC-(O)
Where:
- V: Regulation Version, [A]= Advanced, [B] = Basic
- S: mechanical size of the device [1],[2]…[5]
- WWW: Output power (kW)
- PPP: coding braking unit/Keyboard [KBL] = keypad and brake unit
- X: [F] = internal EMI filter
- CC: Power supply type [4] = 400vAc tree-phase, [2T] = 200vAc tree-phase, [2M] = 200vAc single-phase
- O: Optional features, C= CAN

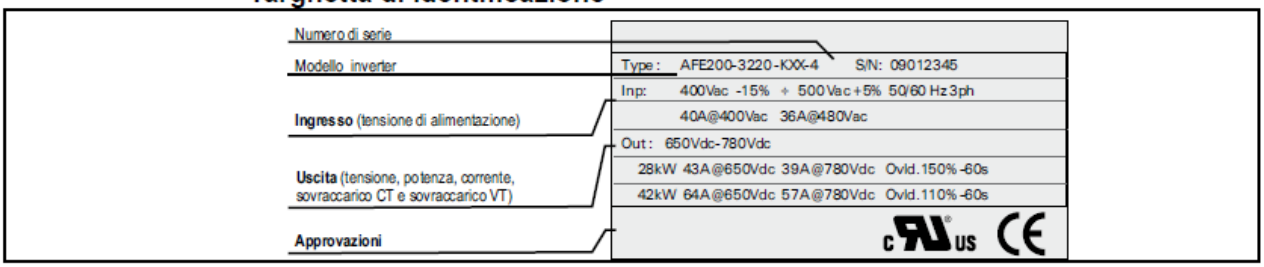
Example:

- ADL300A-2110-KBL-4 = ADL300 Advanced, size 2, power 11kW, 400vAC power supply, Keypad, brake unit, without filter, without CAN

- ADL300B-2110-KBL-F-4-C =ADL300 Basic, size 2, power 11kW, 400vAC power supply, Keypad, brake unit, with filter, with CAN

Every apparatus is equipped with identification label as follows:

Targhetta di identificazione



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.

The correct use of “SAFE TORQUE OFF” function has to be made using two safety related signals and usual START drive commands and sequence:

- **ENABLE**
- **SAEFTY ENABLE**

In all cases where application/highest SIL level is required feedback system should be used. Two feedback signals are allowed for system fault detection as described in §4.4 Safety Fault Reaction System.

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

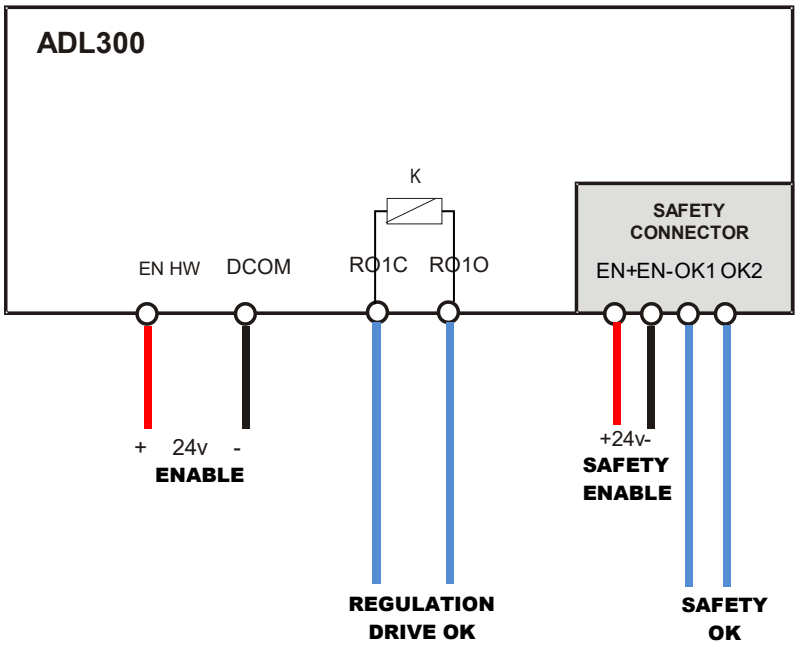
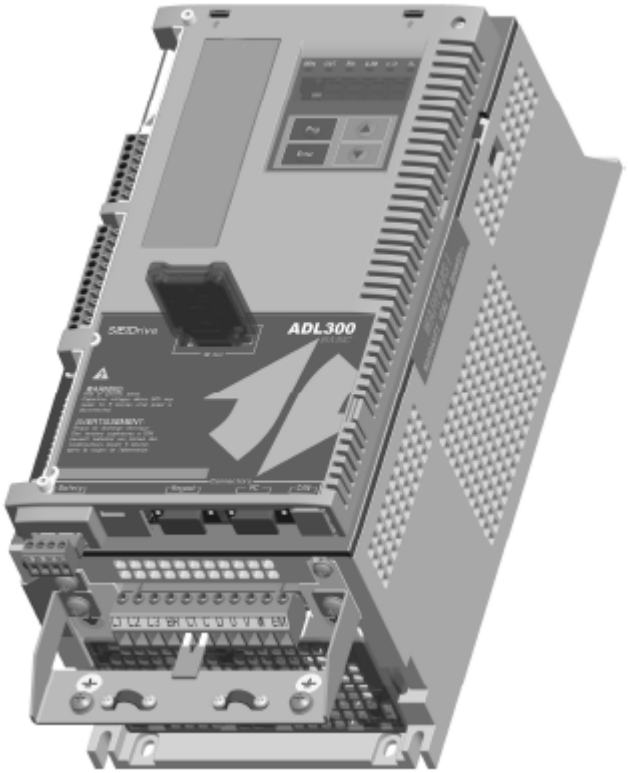


Figure 5 Simplified connection diagram for STO function.

Two set of interface connectors are used onto ADL300 drives.

1. Regulation Enable and Feedback Drive OK
2. Safety Dedicated Connector

Safety system is activated by means of dedicated connections hosted at the bottom of ADL300 case made up of 4 poles input connector hosted on the safety board.



Safety connector layout is shown in Figure 6

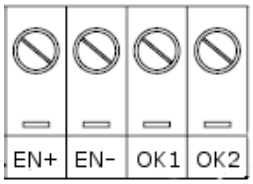


Figure 6 Safety Connector Layout

Table 3 is a description of signals onto Safety Connector.

Terminal name	Signal name	Function Description	Electrical limits and range
EN+	+SAFETY ENABLE	+24v for disabling the safety function	(IN) +12…+35v with respect to EN-
EN-	-SAFETY ENABLE	0v COM for disabling the safety function	(IN) 0v
OK1	SAFETY OK1	Normally closed contact for Safety feedback (contact 1)	250mA maximum DC current
OK2	SAFETY OK2	Normally closed contact for Safety feedback (contact 2)	250mA maximum DC current

Table 5 Description of Signals onto Safety Connector.

Concerning the Regulation signals, the interface is more complex given the number of available configurations for ADL300:

- ADL300 Basic the ENABLE signal is fixed onto the regulation board interface is shown in Figure 8 and Table 6.
- ADL300 Advanced, ENABLE and feedback signals are placed onto the ADL-IO expansion card. ADL-I/O optional cards are listed in Appendix A.2 of Specification and Installation User manual. Figure 10 and Table 7 show a sample example of ADL300 configuration and safety related pin description.

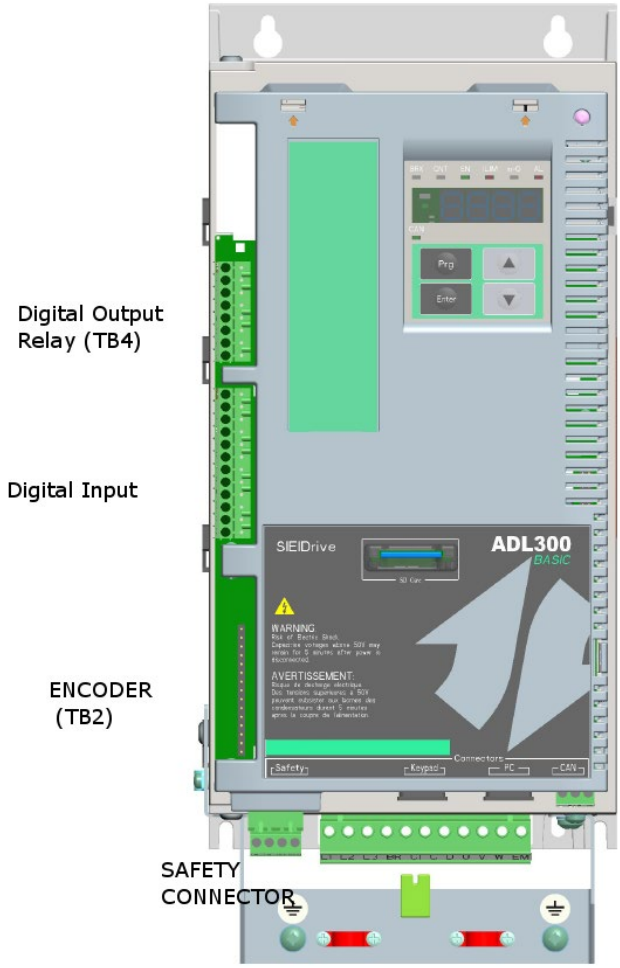


Figure 7 Fixed Connector Layout for ADL300.

TB4	Name	Description
1	RO4O	Dig Out 4
2	RO4C	Dig Out 4
3	RO3O	Dig Out 3
4	RO3C	Dig Out 3
5	RO2O	Dig Out 2
6	RO2C	Dig Out 2
7	RO1O	Dig Out 1
8	RO1C	Dig Out 1

TB3	Name	Description
1	DI 8	Dig In 8
2	DI 7	Dig In 7
3	DI 6	Dig In 6
4	DI 5	Dig In 5
5	DI 4	Dig In 4
6	DI 3	Dig In 3
7	DI 2	Dig In 2
8	DI 1	Dig In 1
9	EN_HW	ENABLE
10	DICOM	
11	0V	0v power supply
12	24V	Power supply

TB2	Name	Description
1	DI F2	
2	DI F1	
3	DI CM	
4	COS-	
5	COS+	
6	SIN-	
7	SIN+	
8	Z-	
9	Z+	
10	B-	
11	B+	
12	A-	
13	A+	
14	0VE	
15	+VE	

Figure 8 Standard PinOut for ADL300 Basic

Regulation connector description with regard to signals related to safety function for ADL300 Basic.

Pin name	Function
TB3 9 - EN HW	Drive ENABLE signal. 24v DC should be applied
TB3 11 - DCOM	COM for ENABLE signal.
TB4 7- RO 1O	DRIVE OK feedback relay
TB4 8- RO 1C	COM for DRIVE OK feedback relay

Table 6 Connector pin-out concerning safety related function onto ADL300 Basic.

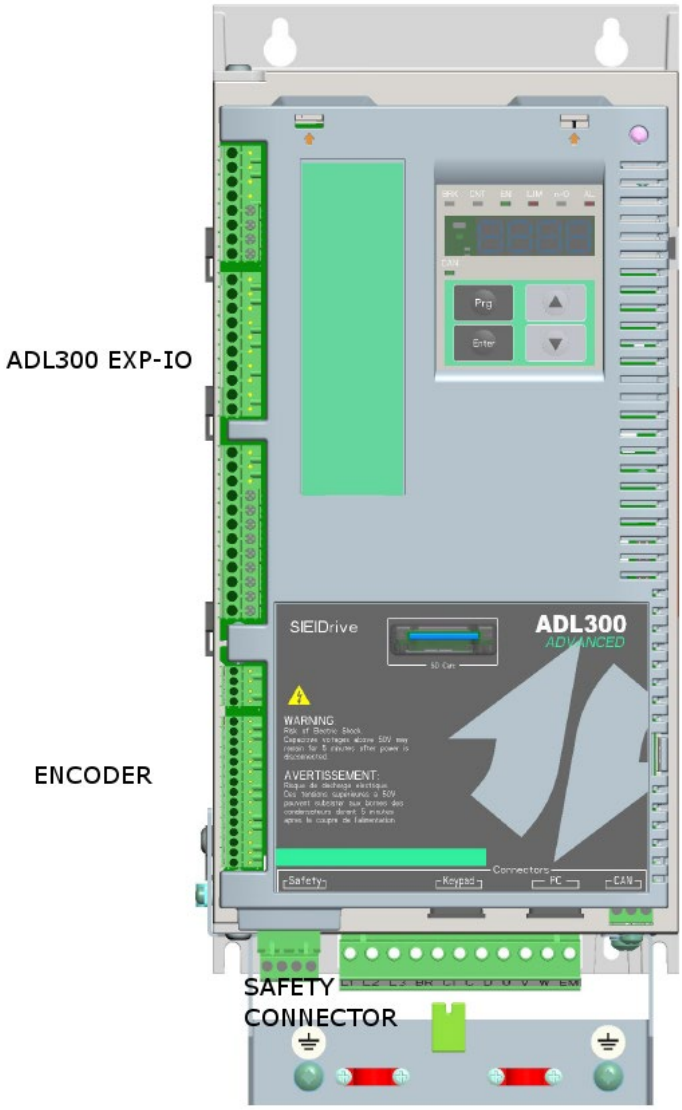


Figure 9 ADL300 with option card configuration.

Following figure show the safety related pin names and positions on EXP-IO-D5R3. ENABLE signal always uses the EN HW name.

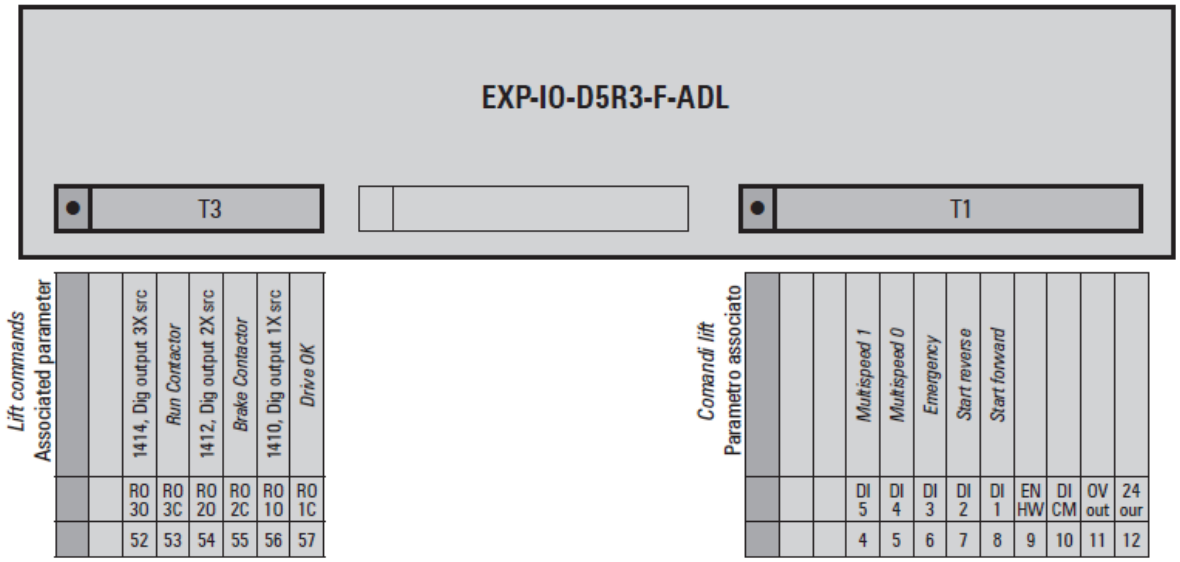


Figure 10 An example for regulation IO configuration: EXP-IO-D5R3.

Regulation connector description with regard to signals related to safety function for ADL300 Advanced.

Pin name	Function
9 - EN HW	Drive ENABLE signal. 24v DC should be applied
11 - 0v	COM for ENABLE signal.
56- RO 1O	DRIVE OK feedback relay
57- RO 1C	COM for DRIVE OK feedback relay

Table 7 Connector pin-out concerning safety related function onto ADL300 EXP-IO-D5R3.

Two signal inputs are provided to enable/disable STO function onto the ADL300. Both inputs are controlled so that:

- STO function is enabled (ADL300 disabled)when either input is not excited (voltage not applied on input).
- Both inputs will be properly excited (energized) in order for the STO function to be disabled and ADL300 to normally operate. Table 1 specifies STO function behavior.

System also provides 2 feedback signals, which must be used according to manual and installation guide in order to increase the safety integrity level of the system. One feedback signal is based on a open contact relay (DRIVE OK). The other feedback signal is an opto-isolated normally closed SAFETY OK relay which switches according to Table 4.

If any of the feedback signals does not comply with anticipated behavior a detected failure should be assumed and countermeasures applied.

Electrical levels

ENABLE and **SAFETY ENABLE** input signals comply with following electrical characteristics:

Nominal excitation voltage	24v
Min excitation voltage	18v
Max excitation voltage	36v
Max steady state current (25°C)	30mA
Disabling condition	Open circuit
Max in-rush peak current	50mA

*Table 8 **ENABLE-SAFETY ENABLE** electrical levels.*

SAFETY OK and DRIVE OK feedback relays characteristics are shown in

Nominal output voltage	24v
Maximum Voltage	125v
Maximum Isolation Voltage	400v
Max current (25°C)	350mA DC 250mArm AC

*Table 9 **SAFETY OK** relay characteristics.*

5.2.1 Control sequence

Normal use of STO 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 STO function properly following action sequence applies:

1. **SAFETY OK, DRIVE OK** signals are checked for congruency
2. **SAFETY ENABLE** signal issued high (24v applied)
3. **ENABLE** is issued high (24v applied)
4. FEEDBACK signals DriveOK and SAFETY DISABLED are checked for congruency
5. START command can now be issued 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 EXP-SFTY-ADV function properly following action sequence is applied:

1. **STOP** command is issued to stop motor and power generation
2. **ENABLE** issued low
3. Finally **SAFETY ENABLE** signal is issued low

Should **ENABLE** and **SAFETY ENABLE** be tied together (both electrically or logically) it must assured that they delays exceeding 4ms is not introduced. In case of SAFETY ENABLE be issued high before ENABLE drive will go into interblock mode and will allow motor to start before ENABLE is correctly taken low and high again.

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:

Signals	Electrical safety constrains
SAFETY ENABLE+, SAFETY ENABLE-	Voltage shall not exceed 35v and shall not be inverted applied.
SAFETY OK1, SAFETY OK2	Voltage shall not exceed 125v. Current shall not exceed 250mA
Input ENABLE HW_EN, DCOM	Voltage shall not exceed 35v and shall not be inverted applied.
DRIVE OK-C, DRIVE OK-O	Voltage shall not exceed 125v. Current shall not exceed 250mA
Digital Inputs	Voltage shall not exceed 35v on any of the pins
Encoder inputs	Voltage shall not exceed 12v on any of the pins
+24v, 0v24	Voltage Supply 24vDC shall not exceed 35vDC. It shall not be inverted applied. It shall not be an AC voltage.

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.

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.

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 **ENABLE** or **SAFETY ENABLE** are activated
- Feedback signal are properly controlled as functions of **ENABLE**/**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 is powered but does not work	Electrical level missing or inverted onto **ENABLE**	Check ENABLE signal, for basic version contacts 9=+24vDC, 10=COM
	Electrical level missing or inverted onto **SAFETY ENABLE**	Check SAFETY connector, contacts 1=+24vDC, 2=COM
	SAFETY OK does not work	Check for Safety Failure Alarm. In case of assertion contact WEG Service & Assistance
	Drive has not been properly connected.	Check ADL300 configuration. See ADL300 user manual.
Regulation Feedback signal (drive OK) does not change status according to table 1.	Drive has not been properly connected.	Check ENABLE signal, for basic version contacts 9=+24vDC, 10=COM
Safety feedback signal (SAFETY OK) does not change status	Safety Enable signal does not activate SAFETY circuits	Check electrical level and current capability of SAFETY ENABLE signal.
Safety feedback signal (SAFETY OK) does not change status according to Table 4	Safety part might have failed	Qualified personnel might assess ADL300 integrity

7 Lift Applications

Following are some application examples specifically intended for Lift Market which show how to implement Safety functions according to EN81-1 using ADL300 safety integrated function.

7.1 Lift Application Design using 2 contactors for car stop

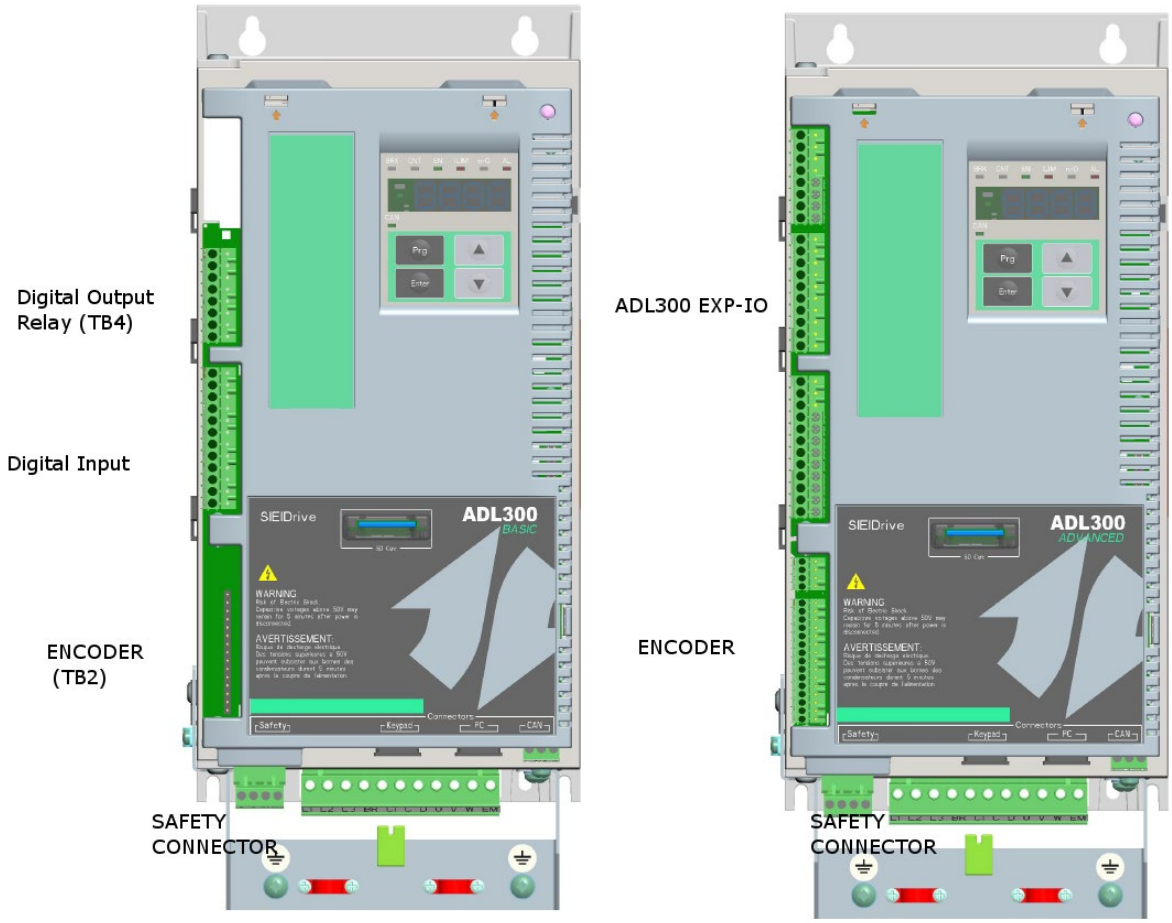
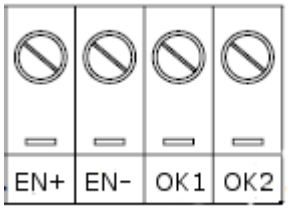


Figure 11Safety connector position on the ADL300 Advanced and Basic versions.

In case of two external contactors used to disconnect motor wirings, no ADL300 safety feature is used. It is important for installation personnel to remind to bypass the integrated safety feature.

Integrated feature is disabled by powering the safety connector on ADL300 Basic/Advanced as follows:

- apply a 24vDC to safety connector enable contacts 1, 2.



EN+	+ SAFETY ENABLE	+24v for disabling the safety function
EN-	-SAFETY ENABLE	0v COM for disabling the safety function

7.2 Lift Application Design supporting car stop with one contactor

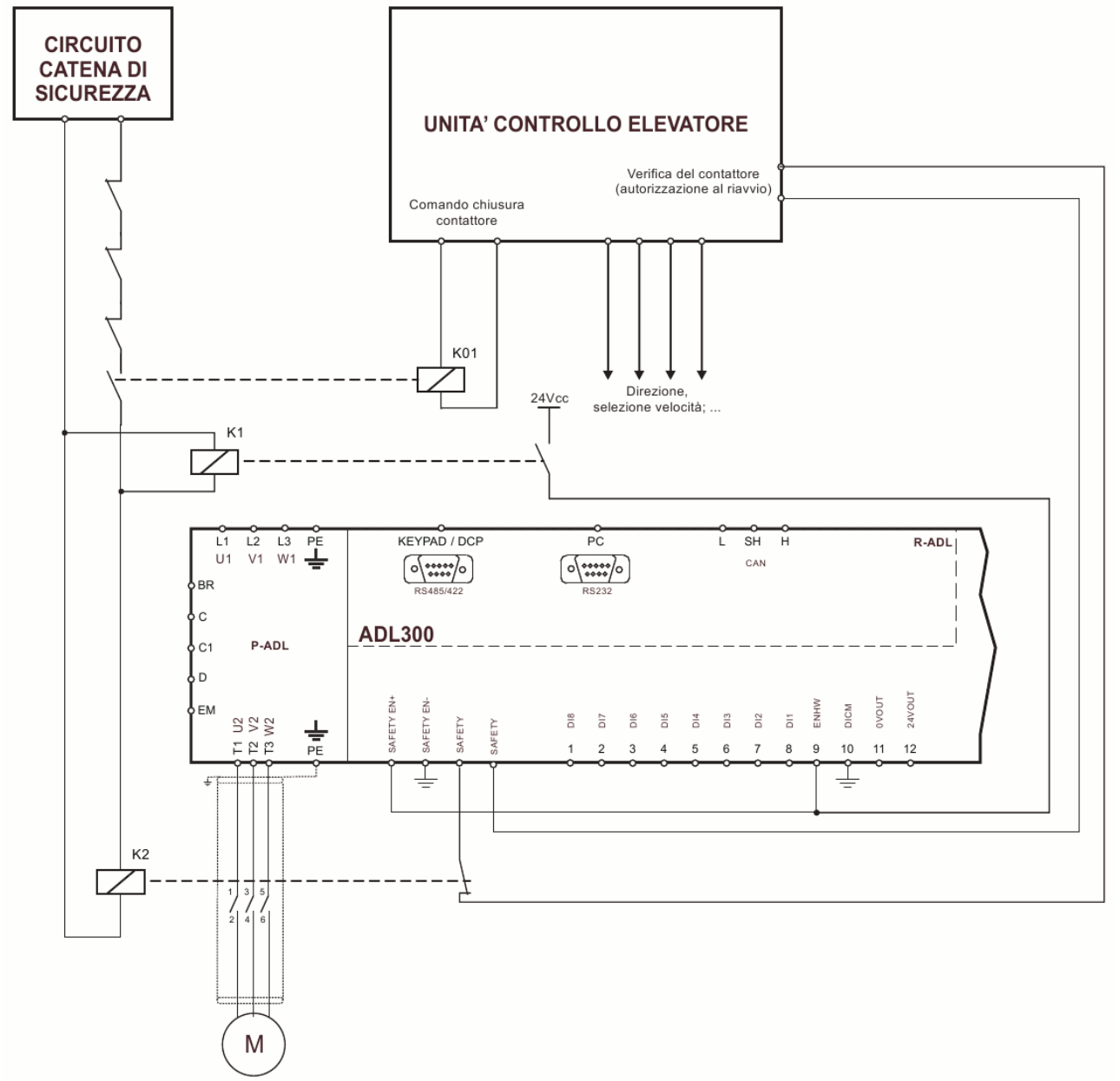


Figure 12 ADL300 Lift system reference design to use a single contactor onto the motor.

Figure 12 is a Lift reference design to be used to implement a Lift System according to EN81-1 12.7.3 b) using one contactor and safety integrated function instead of 2 contactors.

Requirements to comply to reference design and EN81 12.7.3 b) are:

1. SYSTEM CONTROL UNIT shall use both one contactor and ADL300 safety integrated function as means to stop cabin.
2. SAFETY CONTROL UNIT will monitor both DRIVE OK and SAFETY OK relay.
3. ADL300 shall be enabled using both ENABLE and SAFETY ENABLE signals
4. Any time Motor comes to a stop SAFETY OK relay shall be monitored by SYSTEM CONTROL UNIT. In case of unexpected SAFETY OK relay status is found SYSTEM CONTROL UNIT will not issue a restart (K1, K2 remain open) until condition is cleared.

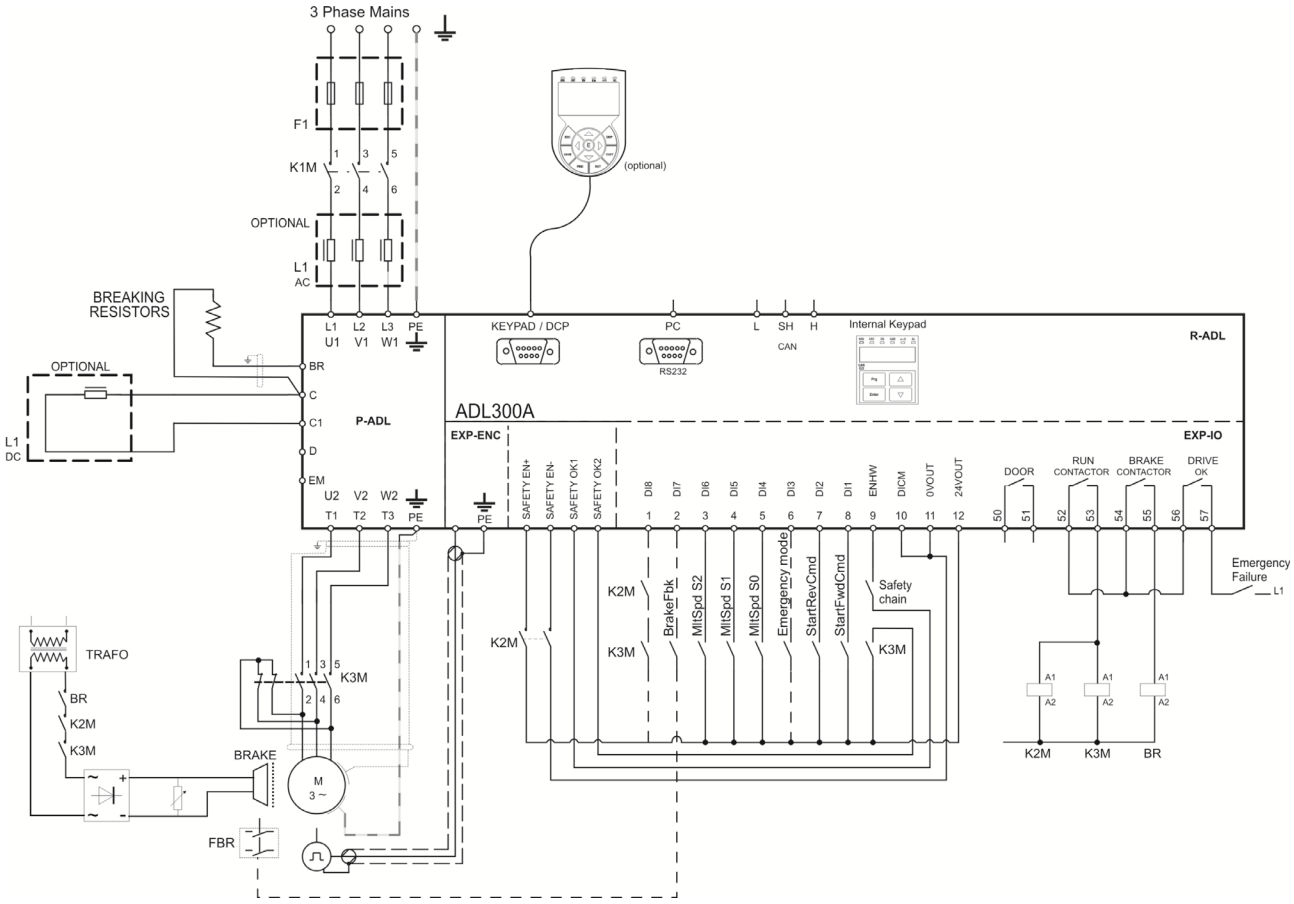


Figure 13 ADL300 specific reference design to use a single contactor onto the motor.

Figure 13 is a more specific ADL300 design case using single contactor and AC motors.

According to previous prescriptions it can be noticed that:

1. The system control unit uses both K3M contactor and ADL300 safety integrated mechanism
2. The System control unit will still be in charge for controlling K2M and K3M which in turn act on both SAFETY ENABLE and ENABLE commands.
3. SAFETY OK relay is monitored by means of a series connections onto ENABLE (ENHW).
4. DRIVE OK is monitored by means of a series connection onto L1 main command.

7.3 Lift Application Design supporting contactor-less car stop

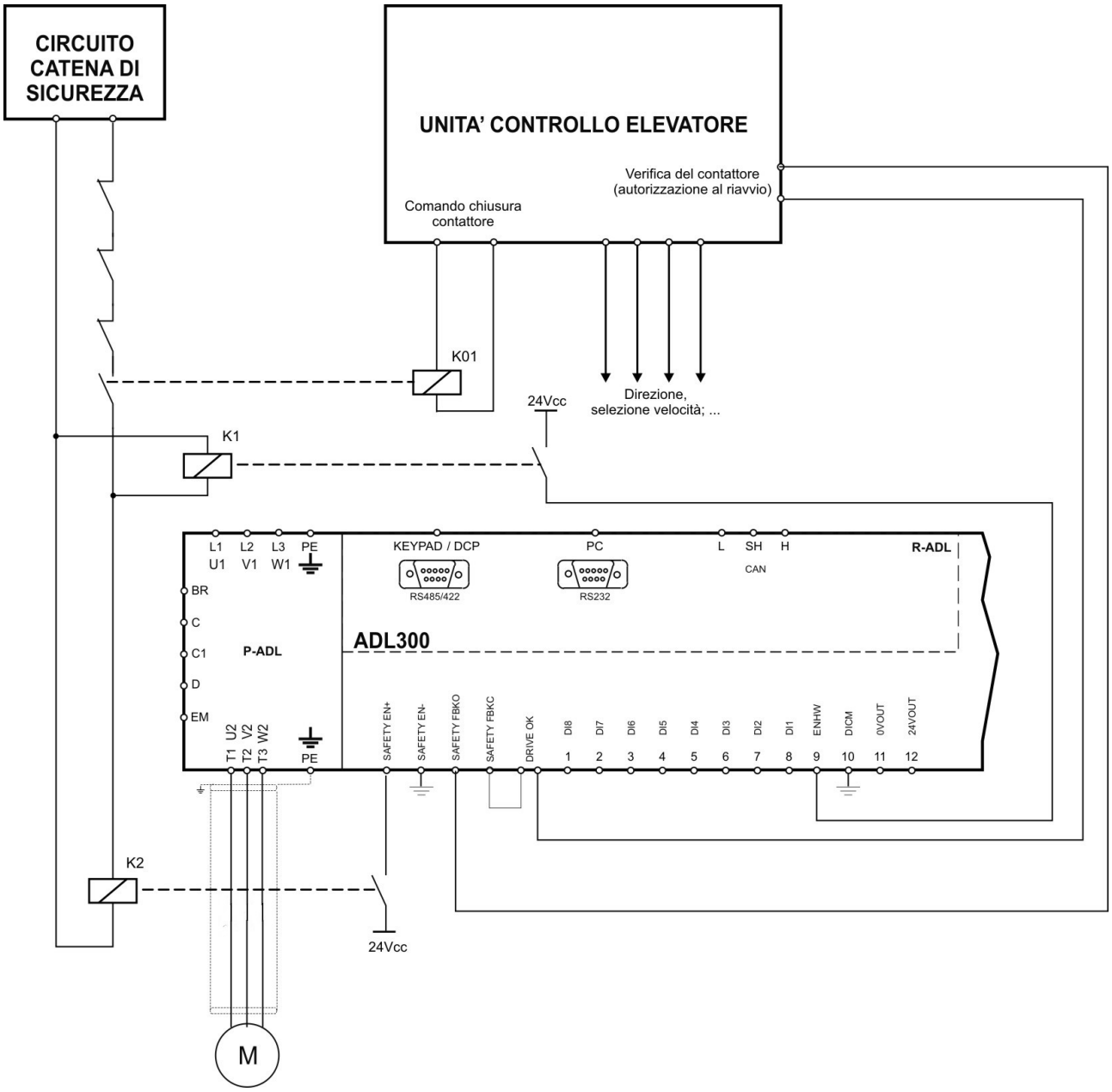


Figure 14 ADL300 Lift system reference design to use onto the motor.

Figure 14 is a Lift reference design to be used to implement a Lift System according to EN81-20 5.9.2.5.4 d) using no contactors and safety integrated function STO (EN61800-5-2- SIL3) instead of 2 contactors.

In order to fulfil the contactor-less design one of the relays must be mandatorily configured as Digital Input Monitor of ENHW (inverted) so that its status directly links to ENABLE signal status. In Figure 14 the status DRIVE OK plays the role of inverted ENHW monitor (the current flows in both relays when car is stopped).

Generally speaking the feedback signal must always be monitored by the SYSTEM CONTROL UNIT either parallel independently or in series.

Requirements to comply to reference design and EN81-20 5.9.2.5.4 d) are:

1. SYSTEM CONTROL UNIT (SCU) shall use ADL300 safety integrated function STO as means to stop cabin. Two separated and independent wirings shall be used to activate/deactivate ENABLE and SAFETY ENABLE signals.
2. SCU will monitor both DRIVE OK and SAFETY OK relay.
3. ADL300 shall be enabled using both ENABLE and SAFETY ENABLE signals
4. Any time Motor comes to a stop SAFETY OK relay and DRIVE OK shall be monitored by SCU, switch from open status to closed status. In case of unexpected relay status (SAFETY OK, DRIVE OK) is found SCU will not issue a restart (K1, K2 remain open) until condition is cleared.

ADL300 will log any unexpected relay conditions. Operators witnessing unexpected relay conditions shall return ADL300 unit for revamping.

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.

Following is a specific ADL300 design case using no contactors.

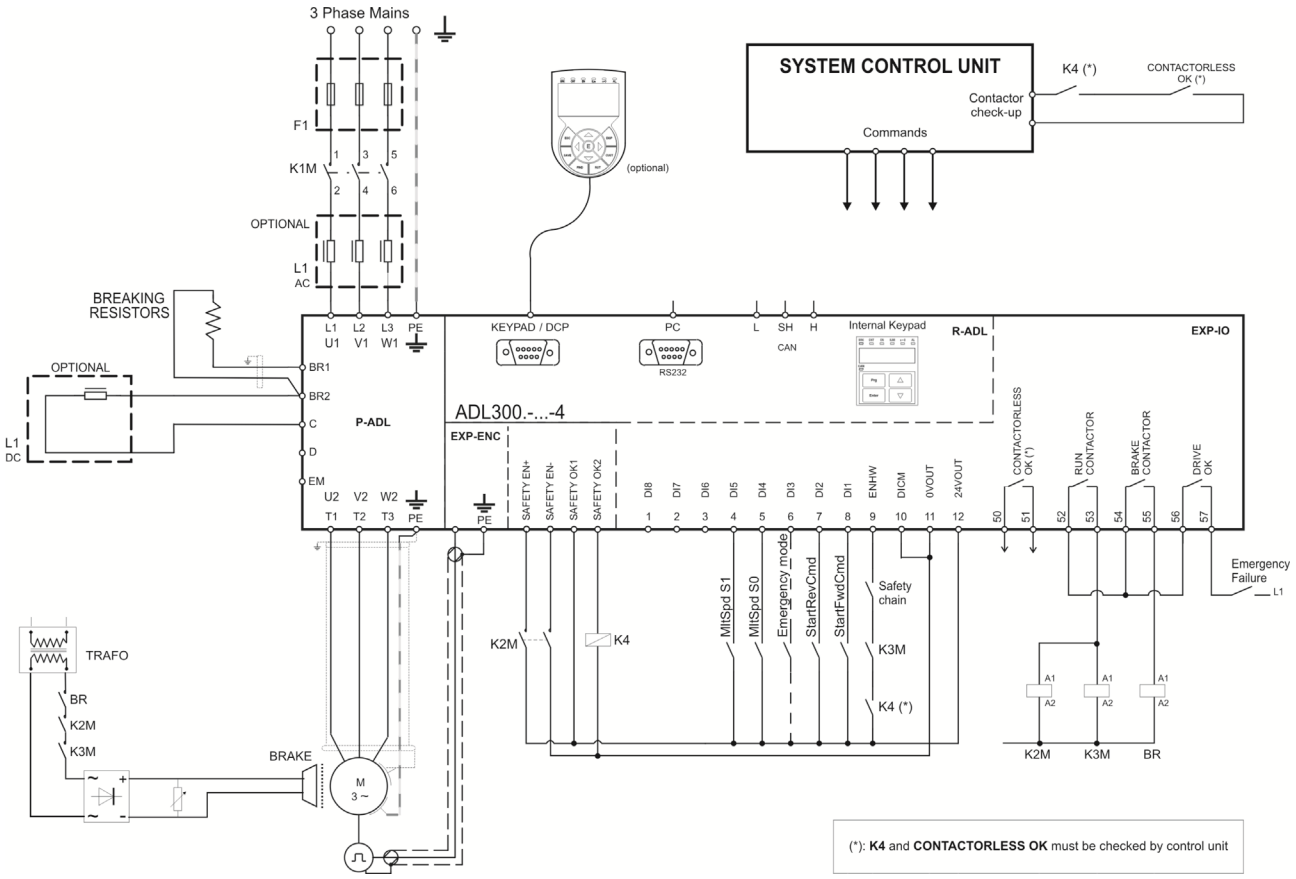


Figure 15 ADL300 contactor-less application design case

With respect to above prescriptions we can notice that:

1. System Control Unit uses both ENABLE and SAFETY ENABLE signals by means of two different relays (K2M, K3M)
2. SCU monitors both feedback relays: SAFETY OK and CONTACTORLESS OK (which is configured as Digital Inp Monitor ENHW)
3. Any time Motor comes to a stop SAFETY OK relay and CONTACTORLESS OK shall be monitored by SCU, switch from open status to closed status. In case of unexpected relay status (SAFETY OK, CONTACTORLESS OK) is found SCU will not issue a restart (K2M, K3M, Emergency Failure remain open) until condition is cleared.

Safety User manual
Series: ADL300
Revision: 1.5
Date: 15-12-2022
Code: 1S9STOEN

WEG Automation Europe S.r.l.
Via Giosuè Carducci, 24
21040 Gerenzano (VA) · Italy

www.weg.net

Driving efficiency and sustainability