Safe Torque Off

ADL550

Safety User Manual

Language: English

Information about this manual

General information

NOTE!

In industry, the terms “Inverter”, “Regulator” and “Drive” are sometimes interchanged. In this document, the terms “Drive” and "Inverter" will be used.

WARNING!

A copy of this manual shall be near the device, or in any case easily available to the operator.

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.

WEG Automation Europe S.r.l. 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.

Thank you for choosing this WEG product.

We will be glad to receive any possible information which could help us improving this manual. The e-mail address is the following: techdoc@weg.net

Table of Contents

1 - Introduction

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 E/E/P (electrical electronic programmable) 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 protections are integrated into the drive, to perform safety function to minimize or delete 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 to control unexpected motor re-start, according to **UNI EN 81-20 (2020)** and **ASME 17.1/CSA B44.1 (2019)** and the application defined at integrator level.

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

To check those requirements, the whole safety related control system was analyzed by means of FMEA, Markov Models, etc...

The purpose of the document is to inform and instruct, for the safe application, the user about the following topics:

- Functional specification (description, fault reaction, application conditions, etc.)
- Safety Integrity Level (SIL) and PFH
- Definition of the environmental and operating conditions
- Indication of any constraints (mission profile, any testing, limits, etc.)
- The act of installing and commissioning guidance (settings and parameterization included)
- Operation and maintenance procedures, configuration, special tools to be used (if any)
- Any actions necessary to prevent an unsafe state and/or reduce the consequences of a hazard (hazardous event).

2 - Definitions

Diagnostic Test	Test intended to detect faults and/or failures and produce specific output information or activity when they are detected.
Fault tolerance	Ability of a functional unit to continue to perform a required function in the presence of faults or errors. A hardware fault tolerance of N means that N+1 is the minimum number of faults that could cause *a loss of the safety function*.
Integrator	A person or a company (final User) that puts together pieces/devices of equipment to form a complete system.
Hazard	Potential source of harm (physical injury or damage to the health of people or damage to property or the environment).
Mission Profile	Definition of the loads and stresses acting on the product in actual use (changes in temperature, temperature profile, vibration and working of electrical and mechanical fields, other environmental factors, etc.)
Recommendation	A suggestion or proposal as to the best course of action.

2.1 Symbols used in the manual

WARNING!

Indicates a procedure, condition, or statement that, if not strictly observed, could result in personal injury or death.

CAUTION!

Indicates a procedure, condition, or statement that, if not strictly observed, could result in damage to or destruction of equipment.

ATTENTION!

Indicates a procedure, condition, or statement that should be strictly followed in order to optimize these applications.

NOTE!

Indicates an essential or important procedure, condition, or statement.

3 - Reference documents

This safety user manual, the standards and rules are applicable for ADL550 and ADL550-ICS products belonging to ADL500 family.

3.1 Applicable Safety regulation and standards

UNI EN 81-20 (2020)

Safety rules for the construction and installation of lifts – Lifts for the transport of persons and good – Passenger and goods passenger lifts

UNI EN 81-50 (2020)

Safety rules for the construction and installation of lifts – Examinations and tests – Design rules, calculations, examinations and tests of lift components

CEI EN 61800-5-2 (2007)

Adjustable speed electrical power drive system – Safety requirements – Functional

ASME 17.1/CSA B44 (2019)

Handbook on Safety Code for Elevators and Escalators.

3.2 Additional standards as reference

EN 60204-1 (2018)

Safety of machinery – Electrical equipment of machines – General requirements

EN 60721-3-3 (2019)

Classification of groups of environmental parameters and their severities – Stationary use at weather protected locations

EN 60068-2-6 (2008)

Environmental testing – Test Fc: Vibration (sinusoidal)

EN 60068-2-27 (2012)

Environmental testing – Test Ea and guidance: Shock

3.3 ADL550 manuals

- **ADL500, Quick start up guide,** Specification and installation
- **ADL500 User Manual,** Functions description and parameters list
- **ADL500-ICS User Manual,** Integrated Control System for Elevator

4 - Acronyms

Acronym	Definition
E/E/P	Electrical/Electronic/Programmable
EB	Enable Signal
ECU	Elevator Control Unit
EMC	Electro-Magnetic Compatibility
FMEA	Failure Modes and Effect Analysis
FMEDA	Failure Modes Effect and Diagnostic Analysis
FSE	Functional Safety Engineer
HFT	Hardware Fault Tolerance
HW	Hardware
N.A.	Not Applicable
PCB	Printed Circuit Board
PD	Power Drive
PDS	Power Drive System
PDS (SR)	Power Drive System (Safety Related)
PFH	Average frequency of a dangerous failure per hour
PWM	Pulse-Width Modulation
ROE	Return of Experience
SE	Safety Enable Signal
SIL	Safety Integrity Level
STO	Safe Torque Off
SW	Software

5 - Safety Function

The safety function described in this manual is the STO (Safe Torque Off) as defined into **CEI EN 61800-5-2 (2007)**.

The correct classification concerning Safety category, SIL (Safety Integrity Level), is defined by the standards **UNI EN 81-20 (2020)** (see § 5.9.2.5.4 point d), **UNI EN 81-50 (2020) and ASME 17.1/CSA B44 (2019) (see 2.26.9.5.1(b)).**

A mechanical brake may be requested in some applications (see chapter **"10 - Safety Advices"**).

STO function provides independent safety channels/paths (see § **"6.1 STO Design"**).

Safety architecture has been designed to be fault tolerant with a fault tolerance at least of 1 (it's evaluated HFT = 2). 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 (see § **"6.1 STO Design"**).

ATTENTION!

A limit on probability of random failure per hour (PFH) should be calculated on a timespan of 20 years (mission profile). PFH is less than 9 E-09.

UNI EN 81-20 (2020), intended for safety in lift applications, specifies the functions, the safety integrity level and the configurations to be used to attain given system level functionalities.

The STO 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 STO being activated.

ASME A17.1/CSA B44 (2019) (par 2.26.9.5.1b) added the option of one of the means, in lieu of an electromechanical contactor, to be an E/E/PES with a SIL of no less than the highest SIL value of the applicable function for electrical protective devices involved.

5.1 Responsibility

The **Manufacturer** must perform all evaluations for safety solutions (and draw up the necessary documentation) and obtain a certification by an external assessment – Notified Body (that realised the specific certificate according to **CEI EN 61800-5-2 (2007)**.

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

NOTE!

Latching devices preventing access to dangerous parts might also be necessary enabling automatically STO function.

5.2 Safety Standard adherence

STO integrated safety function meets the following standard requirements:

- Safety integrity level SIL3 according to **CEI EN 61800-5-2 (2007)**.

STO is designed specifically for Lift Market to support:

- Single contactor operation for Car stop **UNI EN 81-20 (2020)** § 5.9.2.5.4 b) and **ASME A17.1/CSA B44** (2019) § 2.26.9.5.1b)
- Contactor-less operation for Car stop **UNI EN 81-20 (2020)** § 5.9.2.5.4 d)

For details, please refer to chapter **"9 - Lift Applications"**.

When STO is activated or fault detection is noticed, it avoids torque production onto the motor, which eventually could cause undue movements.

6 - Safe Torque Off description

The “Safe Torque Off” (STO) is a safety function used to break off power and current output onto the motor, in order to prevent undue movements and voltages.

ADL550 drives supports “Safe Torque Off” as an integrated feature.

NOTE! This function does not disconnect the machine from electrical power supply.

It shall be underlined that safety equipped drive units are just one component in a safety control system, whereas STO is system level function associated to PDS (SR).

NOTE! Parts and components of the system (or installation) must be chosen, applied and integrated appropriately to achieve the desired level of operational safety.

ADL550 are specialized drives intended for the Lift Market. Given this, STO function is designed to attain safety features permitted and described by **UNI EN 81-20 (2020)** and **ASME A17.1/CSA B44 (2019)**. Specifically (see chapter **"9 - Lift Applications"** for details), the STO safety integrated function allows getting rid of one or two contactors and implementation of:

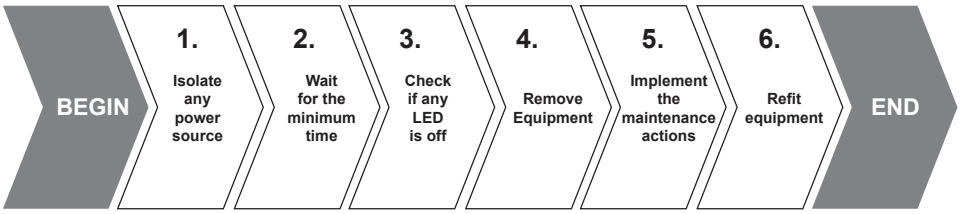
- Car safe stop using one contactor design
- Car safe stop using contactor-less design

STO function is integrated in drives ADL550, 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.

The STO function features 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;
- prevent the creation of a rotating magnetic field by disconnecting the control of power semiconductors;
- perform short operations (cleaning and/or maintenance work) on the non-electrical machine parts without disconnecting either the drive power supply or the connection between power and engine.

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



6.1 STO Design

Safe Torque Off safety function is integrated into the drives ADL550 and is managed by means of two enable signals “ENABLE” and “SAFETY ENABLE”.

The system, herein examined, is the Power Drive Systems (PDS) also called Inverter. A PDS is power device connected one side to the mains (three-phase system) and on the other side to the motor power lines. Motor and other devices are related to the system functionalities (relays, cables, etc.). The PDS makes the motor move according to the settings operator has defined.

From the safety and main functionality points of view all devices of the ADL550 can be modeled as the same thing, herein represented in figure below.

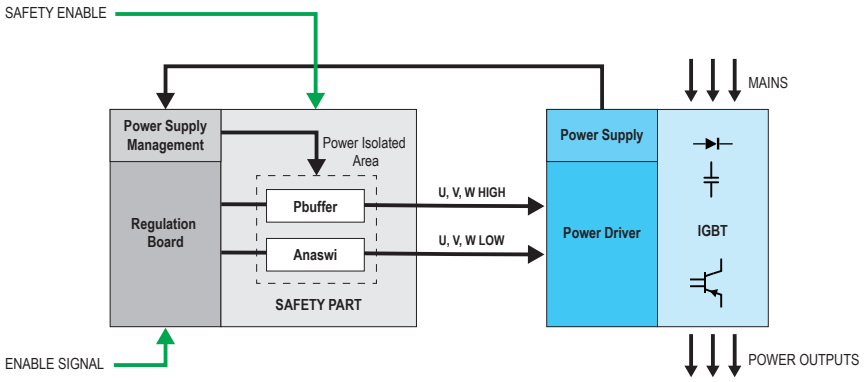


Figure 1 - Block Diagram ADL550 / ADL550-ICS

All ADL550 inverters 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

It exists as separate printed circuit board (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 (with dedicated settings) to provide given voltage, current, motor speed, motor acceleration and all additional options. PWM pulses can be deleted directly onto the regulation board by means of a HW PWM inhibition signal which acts directly of the hardware PWM generator (by ***ENABLE*** signal reception). Of course, the onboard software sees the ***ENABLE*** signal when asserted and stops the (software) generation. A power supply management (monitoring and distribution), providing voltages for all digital circuits. The Safety Part is included on this board. It should be highlighted that PWM pulses are differentially transmitted throughout all the stages. PWM pulses are made up of high part and low (negated) part.

2. Safety part

It exists an integrated part of components into the regulation board. This part takes in the output PWM signals high/low coming from regulation and according to its ***SAFETY ENABLE*** (SE) signal makes pulses pass/no pass on the output connector going to the IGBT driver.

3. Power driver

It exists as separate PCB. Power driver is the interface system between signals coming from Safety part and the power part. This section comprises an opto-isolation isle, a conditioning part, connected to mains supply driving IGBT gates. It should be noticed that a driver activates only when PWM positive signal goes high and corresponding negative signal goes low. Should not this condition be met current will not flow and driver is prevented from turning on. In addition, a power supply generation is implemented (by using a Fly back converter 24V IN / 5V OUT) for all digital circuits and Safety Part is included on this board.

4. 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.

STO safety function is designed and performed independently from any software (SW) components (purely hardware implementation). Software components might only be used to detect/issue additional feedback alarms.

Software is used also to support Safety inter-block function which is activated when the ***ENABLE*** signal is present without ***SAFETY ENABLE*** signal (drive remains in a locked state until the ***ENABLE*** will be low or 0). The *safety inter-block* is disabled when ***ENABLE*** switches from 1 to 0 with ***SAFETY ENABLE*** to 0.

The STO connector (usually recognizable by the yellow colour) is defined below:

Terminal name	Signal name	Function Description	Electrical limits and range
EN+	+SAFETY ENABLE	+24V for disabling the safety function	(IN) +18…+36Vdc with respect to EN-
EN-	- SAFETY ENABLE	0V COM for disabling the safety function	(IN) 0V

OK1	+ STO FBK (SAFETY OK1)	Normally closed contact for Safety feedback (contact 1)	125Vac / 36Vdc maximum operative voltage 200mA maximum DC current
OK2	- STO FBK (SAFETY OK2)	Normally closed contact for Safety feedback (contact 2)	125Vac / 36Vdc maximum operative voltage 200mA maximum DC current

Table 1 - STO Connector (SFT) Signal (SAFETY ENABLE / SAFETY OK)

Connector	Pin Name	Function
T1	9 – EN HW	Drive ENABLE signal. 24V DC should be applied
T1	10 – DI_COM	COM for ENABLE signal
T3	56 – RO_1NO	DRIVE OK feedback relay
T3	57 – RO_1COM	COM for DRIVE OK feedback relay

Table 2 – Connector Signal (ENABLE / DRIVE OK)

6.2 STO specification

STO function will be active whenever either ***ENABLE*** or ***SAFETY ENABLE*** signals are deactivated (zero voltage applied, open wires and no current flowing).

STO function will be disabled (when drive enabled) whenever both enable signals are asserted (24 Vdc applied). Both inputs will be properly excited (energized) in order to disable the STO function leading to PDS into normal operation. Functional logic is shown in table below:

ENABLE	SAFETY ENABLE	STO STATUS
Disabled (open/0V)	Disabled (open/0V)	Enabled (Torque off)
Enabled (24Vdc)	Disabled (open/0V)	Enabled (Torque off) *[Safety inter-block]*
Disabled (open/0V)	Enabled (24Vdc)	Enabled (torque off)
Enabled (24Vdc)	Enabled (24Vdc)	Disabled (drive operating)

Table 3 – STO Static Functional Logic

Although the STO function activates when at least one of the cited signals is deactivated, the safety integrity level of STO safety function is guaranteed only as long as the application of both signals is required simultaneously and they are both deactivated.

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

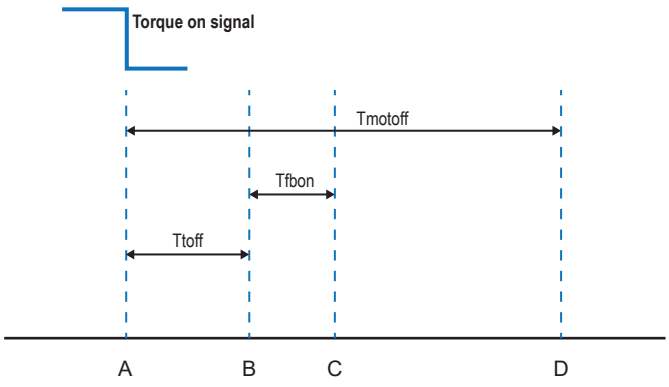


Figure 2 - STO Time event diagram

The phases A, B, C, D shown into figure above are recap below:

A: One or both control signals disabled

B: Motor Torque Off (STO intervention)

C: Feedback activated

D: Motor safely stopped

Time	DESCRIPTION
Ttoff	Time from control signal (Enable and/or Safety Enable) disabled to STO function intervention
Tfbon	Time from STO intervention to feedback signal changing state
Tmotoff	Time from control signal (Enable and/or Safety Enable) disabled to motor stop (depends on motor/load inertia)

Table 4 - Time Intervals Description

Looking at the Enable signals evolving dynamically in time, the allowed input configurations are less than those highlighted in **"Table 3 – STO Static Functional Logic"** In order to prevent PWM pulses to be applied suddenly, an additional function (Safety inter-block) is implemented to avoid that PDS can start with only the ***SAFETY ENABLE*** activation (in case the ***ENABLE*** is undue activated – high status). In any case, it is not considered relevant for STO safety application, only for a correct PDS availability. Following the figure is describing the dynamics of STO function.

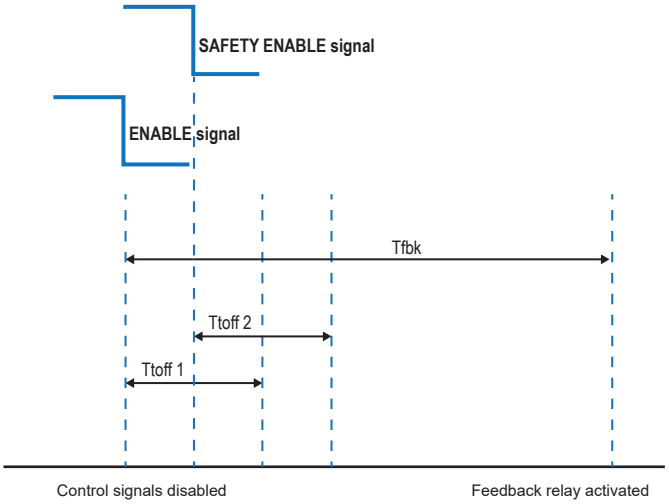


Figure 3 - Dynamic view of STO activation

All Time definitions and their acceptable delay can be recap as follow:

Time	DESCRIPTION	Max Delay [ms]
Ttoff1	Time between *ENABLE* signal intervention and PWM command disabling	< 2
Ttoff2	Time between *SAFETY ENABLE* signal intervention and safety channel activation (0V)	< 40
Tfbon	Time between *SAFETY ENABLE* and *SAFETY FEEDBACK* change of status	< 140
Tiblk	In case **SAFETY ENABLE** is issued (24V) before *ENABLE*, maximum allowed time before system goes into inter-block [1]	24

Table 5 - Time Interval values

[1] Inter-block function is not safety related

The response time considered for the safety function is the worst (highest) value between the two Ttoff.

In case of single fault, the response time is guaranteed within 150 ms.

Values defined into table above are in line with the safety intervention time needs (the motor inertia is usually estimated at around 300 ms before the stop).

6.3 STO Fault Reaction

6.3.1 STO FBK

Hardware mechanisms on both Regulation and Safety circuits have been established to detect and react to a fault detection. All detectable faults are detected when the safety function is executed.

STO FBK is provided to issue fault alarms to external monitoring devices. Normal behaviour of these signals is described in Table 7.

STO signal levels are defined in Table 6.

STO FBK is normally change status according to the input levels and it is opto-isolated, normally open status and supplied with a low voltage DC.

Asserting an alarm on a feedback signal means the feedback signal status does not comply with behaviour described into table below:

ENABLE / SAFETY ENABLE	Level
0 V	0
24 Vdc	1

Table 6 – Levels of Safety signals

SAFETY ENABLE	STO FBK	STO Status	STO Status
1	0	Open	Activated (Safety Stop)
0	1	Open	Activated (Regulation Stop)
0	0	Closed	Activated (STO Enabled)
1	1	Open	Disabled (Drive Active)

Table 7 – STO Status summary

In case the Safety circuit detects a dangerous hardware fault (leading to the loss of at least one channel of the safety circuit), at least one channel used to manage the STO function is in fault.

In order to make failures more evident and take system to a safe state independently of external monitoring device, STO function has been designed so that most of the detected failures actually block the ADL550 when drive is being normally operated. All detected failures raise alarm issues by means of feedback signals.

WARNING!

If any the Safety feedback signal does not comply with Table 6, a detected failure should be assumed and countermeasures applied (repair/replacement of the regulation board).

WARNING!

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.

6.3.2 DRIVE OK

Signal ***DRIVE OK*** is provided as an option to issue fault alarms to external monitoring devices.

This feedback signal can be used to improve the fault detection of safety circuit, but it is not necessary to reach the SIL3 for STO safety function.

The ***DRIVE OK*** is configurable via software. The default configuration works in such a way that the relay is closed if the ADL550 drive is ready to receive an ***ENABLE*** signal.

Normal behaviour of these signals is described in **"Table 8 – Feedback status of EB input"** and it is based on an open contact relay, it indicates that the Drive is available (when the contact is closed).

Default configuration acts so that relay is closed if drive ADL550 is ready for receiving an ***ENABLE*** signal.

NOTE!

DRIVE OK configuration must be mandatorily changed into Digital Input Monitor for ***ENABLE*** signal in case of contactor-less applications (chapter **"9 - Lift Applications"** see contactor-less car stop.

Asserting an alarm on a feedback signal means the feedback signal status does not comply with behaviour described into table below (feedback must have a behaviour similar to relay).

ENABLE	DRIVE OK
0 V	Open
24 Vdc	Closed

Table 8 – Feedback status of EB input

In case the hardware/software into regulation circuit (Enable chain) can detect some faults; they will assert a type of alarms, depending on conditions DRIVE OK to stop generation of PWM gate pulses.

NOTE!

DRIVE OK configuration could be an additional check (SW configurable) for ***ENABLE*** chain in case the Integrator needs an additional trustiness for detection.

NOTE!

A dedicated configuration for all ADL550 / ADL550-ICS products is detailed into § **"9.3 Design supporting contactor-less car stop (Only with EN 81.2 (2020) rules)"**. The ***DRIVE OK*** functionality is replaced by CONTACTORLESS OK.

6.3.3 Additional Checks

In addition, Regulation board executes all possible integrity checks (by SW) any time before starting to generate PWM pulses:

- Check ***ENABLE*** signal
- Check ***SAFETY ENABLE*** signal
- Check STO FBK consistency

WARNING!

Should any of the previous checks be failed ADL5xx 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.

7 - Installation and Commissioning Guidance

Installation and commissioning shall be performed only by qualified personnel fully aware of the risks generally and specifically involved in the operations (see chapter **"10 - Safety Advices"**).

NOTE!

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

- Both enable signals must be used with full wiring redundancy in order to sustain fault tolerance equal or greater than 1 (this function is HFT = 2)
- STO FBK signal shall be used in order to reach SIL 3 for the STO safety function
- DRIVE OK must be used for application described into § **"9.3 Design supporting contactor-less car stop (Only with EN 81.2 (2020) rules)"**
- All devices used to assist/monitor/actuate safety related signals shall claim a compliant safety integrity level.

WARNING!

During a phase of drive parameters regulation for installation and/or commissioning, the safety condition is guarantee with the application of STO function. In case it is necessary the forced exclusion of STO function by the operator, appropriate risk reduction means must be made available.

WARNING!

The operator or electrical installer is responsible for correct earthing and compliance with all relevant national and local safety regulations.

7.1 STO Function Integrated on ADL550 drives

Drives ADL550 support STO function as a standard integrated function tested on each unit shipped from authorized manufacturing plants.

WARNING!

It must be understood and accepted by the users that safety function cannot 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.

7.2 Connections and use of STO function

The correct use of the STO function has to be made using two safety related signals (as described into § **"6.1 STO Design"**) and usual START drive command and sequence. The signals are:

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

WARNING!

In all cases where application SIL level is required STO FBK feedback must be used.

ATTENTION!

ENABLE MISSING alarm occurs if interval between SAFETY ENABLE and ENABLE signals, wichever occur first, is more than 4 seconds.

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

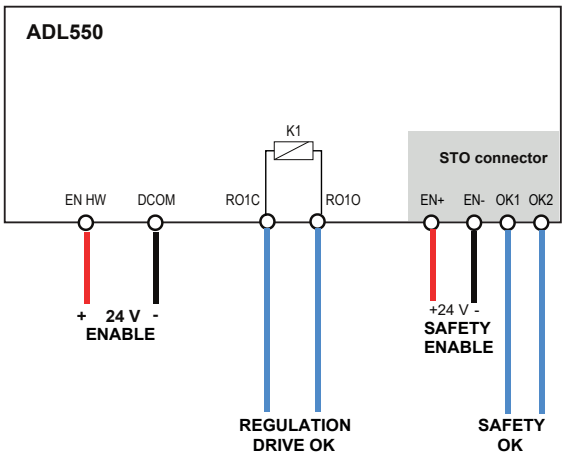


Figure 4 - Simplified connection diagram for STO function

Two set of interface connectors are used into ADL550 drives.

1. Regulation Enable (Feedback ***DRIVE OK*** see § **"9.3 Design supporting contactor-less car stop (Only with EN 81.2 (2020) rules)"**
2. Safety Dedicated Connector

Figure 5 - ADL550 Product (as example)

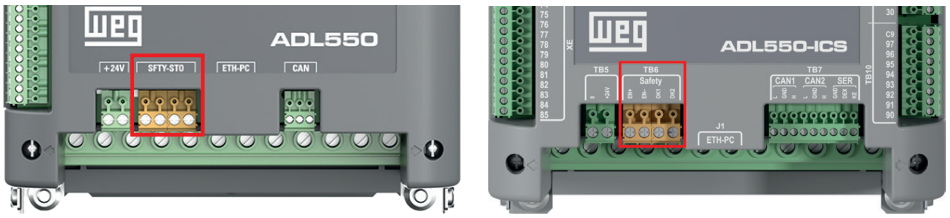


Figure 6 - STO connector

Safety system is activated by means of dedicated connections (identified with yellow colour for all products with STO function) hosted at the bottom of ADL550 case made up of four poles input connector hosted on the safety board.

7.3 STO Management

As defined into § **"6.1 STO Design"**, two signal inputs are provided to enable/disable STO function into the ADL550. Both inputs are controlled so that:

- STO function is enabled (ADL550 disabled) when either input is not excited (voltage not applied on input)
- Both inputs will be properly excited (energized) in order to disable the STO function and lead ADL550 to a normal operation. The **"Table 3 – STO Static Functional Logic"** (see § **"6.2 STO specification"**) specifies STO function behaviour.

System also provides two 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 an opto-isolated normally closed ***STO FBK*** relay which switches according to § **"6.3 STO Fault Reaction"**(see **"Table 7 – STO Status summary"**).

NOTE!

If any of the feedback signals does not comply with anticipated behaviour, a detected failure must be assumed and all countermeasures applied. Ensure that all safety and warnings sign on/at the lift system are always clearly legible.

7.4 STO Electrical levels

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

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

Table 9 - EN/SE Electrical levels

STO FBK relay characteristics are shown below:

Nominal operative voltage	24 Vdc / 115 Vac
Max operative voltage	36 Vdc / 115 Vac
Max blocking voltage	400 V
Max operative current (25°C)	200 mA (DC) 200 mArms (AC)

Table 10 - SAFETY FBK Electrical levels

DRIVE OK feedback relays characteristics are shown in:

Nominal output voltage	24 Vdc / 115 Vac
Maximum Voltage	30 Vdc / 125 Vac
Maximum Isolation Voltage	4 kV
Max current (25°C)	500 mA (DC) 500 mArms (AC)

Table 11 - DRIVE OK relay characteristics

Terminals	**Maximum cable cross-section**			**Recommended stripping**	**Tightening torque** (min ... max)
	(mm^2)	(AWG)	Conductor	(mm)	(Nm)
SAFETY EN + SAFETY EN –	0.2 ... 2.5	24 ... 12	One conductor	7	0.5 … 0.6
	0.2 ... 1.5	24 ... 15	Two conductors (same section, flexible)		
STO FBK (OK1, OK2)	0.2 ... 1	24 ... 17	Two conductors (same section, rigid)		

Table 12 - Cable cross-sections (Safety Connector)

7.5 Control sequence

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

DISABLING STO FUNCTION

Drive is in stop condition; both ***ENABLE*** and ***SAFETY ENABLE*** signals are disabled. In order to disable STO function properly following action sequence applies (by lift controller):

1. ***STO FBK, DRIVE OK*** signals are checked with tables defined int §**"6.3 STO Fault Reaction"**
2. ***SAFETY ENABLE*** signal issued high (24 Vdc applied)
3. ***ENABLE*** is issued high (24 Vdc applied)
4. Feedback signals ***DRIVE OK*** and ***STO FBK*** are checked as point 1
5. ***START*** command can now be issued to start motor and provide power

ENABLING STO SAFETY FUNCTION

Drive is running and powering a motor, both ***ENABLE*** and ***SAFETY ENABLE*** signals are put on 0 V. In order to activate STO function properly following action sequence is recommended:

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

In case of ***SAFETY ENABLE*** be issued high (24 Vdc) while ***ENABLE*** is already high (24 Vdc), drive will go into inter-block mode and will allow motor to start only when ***ENABLE*** is correctly taken low and high again.

NOTE!

Should ENABLE and SAFETY ENABLE be tied together (both electrically or logically), it must be assured that ENABLE does not change from low level (0V) to high level (24V) before Safety Enable or within 24 ms.

8 - Operation and Maintenance Requirements

8.1 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	Safety Electrical Constrains
SAFETY ENABLE+, SAFETY ENABLE-	Voltage shall not exceed 35 Vdc and shall not be inverted applied
STO FBK (OK1, OK2)	Voltage shall not exceed 36 Vdc / 115 Vac. Current shall not exceed 200 mA (DC) / 200 mArms (AC)
Input ENABLE HW_EN, DCOM	Voltage shall not exceed 35 Vdc and shall not be inverted applied
DRIVE OK-C, DRIVE OK-O	Voltage shall not exceed 30 Vdc / 115 Vac. Current shall not exceed 500 mA (DC) / 500 mArms (AC)
Digital Inputs	Defined into ADL550 / ADL550-ICS Quick Start (Input / Output features), see **"3 - Reference documents".**
Encoder inputs	
+24V, 0V24	Voltage Supply 24Vdc shall not exceed 35Vdc. It shall not be inverted applied. It shall not be an AC voltage

Table 13 - Safety Electrical Constraints

The drive 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 EN 60721-3-3 (2019)	No conductive dust allowed		
Boards without coating	Chemical gases: N.A.	Chemical gases: N.A.	
	Solid particles: No conductive	Solid particles: no conductive	
Boards with coating	Chemical gases: N.A.	Chemical gases: N.A.	
	Solid particles: No conductive	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 (2008)	Sinus 10...150Hz 2g Random 5....200 0.005g 2Hz	N.A.	N.A.
Shock EN 60068-2-27 (2012)	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 sunlight, vibration, dust, corrosive or inflammable gases, fog, vapour oil and dripped water, avoid saline environment)		
Degree of protection	IP20 (*)		
EMC	EN 61800-3		

Table 14 - Environmental Conditions

(*) It is possible an additional protection IP54 for cabinet with externally mounted heatsink (applicable for size major than 3)

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

8.2 Maintenance

Expected operation lifetime of the safety function is 20 years. When it is exceeded, drive shall be returned to manufacturer.

For any malfunctions/failures, the users/assisting personnel must notify the support immediately and take appropriate action to resolve the problem

Periodic maintenance is not necessary nor scheduled.

8.3 Operational Tests

Qualified personnel shall periodically verify the drive unit as black-box unit. Assisting personnel shall verify the input – output tables (see Table **"Table 3 – STO Static Functional Logic"**) with respect to what is above specified (see § **"6.2 STO specification"**).

NOTE!

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.

NOTE!

Periodic test shall be performed at least once a YEAR.

8.4 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 (see **"Table 2 – Connector Signal (ENABLE / DRIVE OK)"**)
	Electrical level missing or inverted onto SAFETY ENABLE	Check SAFETY connector, contacts 1=+24Vdc, 2=COM (see**"Table 1 - STO Connector (SFT) Signal (SAFETY ENABLE / SAFETY OK)"**)
	SAFETY OK does not work	Check for Safety Failure Alarm. In case of assertion contact WEG Automation Europe Service & Assistance
	Drive has not been properly connected.	Check ADL500 / ADL550-ICS configuration. (See ADL500 / ADL550-ICS Quick Start)
Regulation Feedback signal (DRIVE OK) does not change status according to **"Table 8 – Feedback status of EB input"**	Drive has not been properly connected.	Check ENABLE signal (see **"Table 2 – Connector Signal (ENABLE / DRIVE OK)"**)
Safety feedback signal (STO FBK) does not change status according to **"Table 7 – STO Status summary"**	SAFETY ENABLE signal does not activate SAFETY circuits	Check electrical level and current capability of SAFETY ENABLE signal
	Safety part might have failed	Qualified personnel might assess ADL500 / ADL550-ICS integrity

Table 15 - STO Troubleshooting Table

9 - Lift Applications

Following are some application examples specifically intended for Lift Market which show how to implement Safety functions according to **UNI EN 81-20 (2020)** and **ASME A17.1/CSA B44 (2019)** using ADL550/ADL550-ICS with safety integrated function. The purpose is to manage the power supply interruption that can cause motor rotation.

9.1 Design using two contactors for a car stop

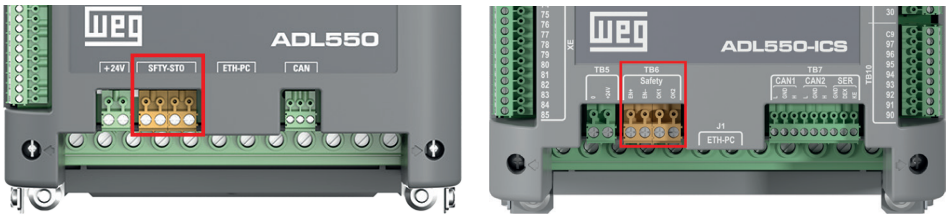


Figure 7 - STO Safety connector position (ADL550 = SFTy-STO), ADL550-ICS = TB6 / Safety)

In case of two external contactors used to disconnect motor wirings, no ADL550 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 ADL550 as follows:

• apply a 24 Vdc to STO safety connector enable contacts 1, 2.

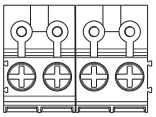


Figure 8 - STO connector details

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

Table 16 - STO input command characteristics

ATTENTION!

The wiring diagrams in the following paragraphs are just an example of how the STO function can be realized. All wiring that respects the operating principles indicated in the previous chapters are valid.

9.2 Design supporting car stop with one contactor

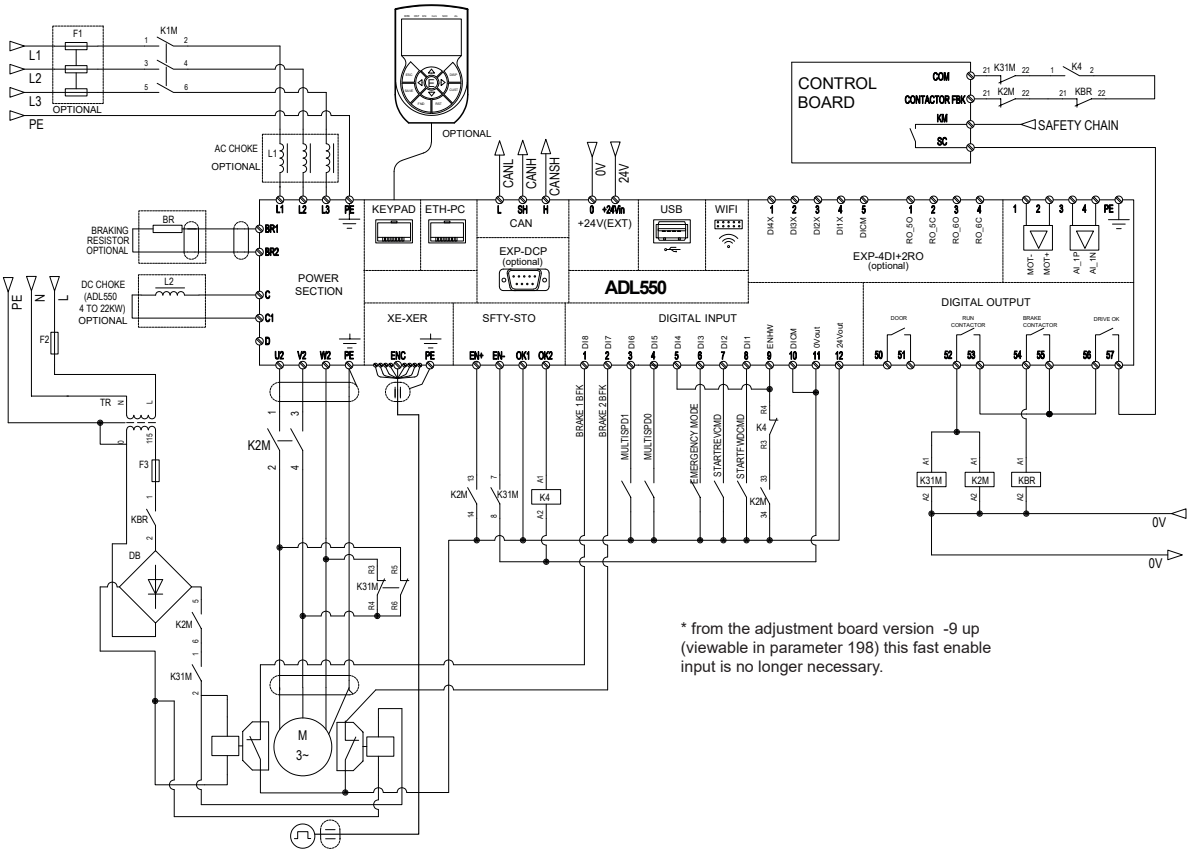


Figure 9 - ADL500 Reference design using a single contactor (onto the motor)

The figure above is a Lift reference design to be used to implement a Lift System according to **UNI EN 81-20 (2020)** and **ASME A17.1/CSA B44 (2019)** (see 5.9.2.5.4 – b) using one contactor and safety integrated function instead of two contactors.

Requirements to comply to reference design and standard **UNI EN 81-20 (2020)** and **ASME A17.1/CSA B44 (2019)** are:

1. ELEVATOR CONTROL UNIT (ECU) shall use one contactor and ADL550/ADL550-ICS safety integrated function as means to stop cabin
2. SAFETY CONTROL UNIT will monitor both ***DRIVE OK*** and STO FBK relay
3. ADL550/ADL550-ICS shall be enabled using both ***ENABLE*** and ***SAFETY ENABLE*** signals
4. Any time Motor comes to a stop STO FBK relay shall be monitored by ECU. In case of unexpected STO FBK relay status is found ECU will not issue a restart (K4, K2M remain open) until condition is cleared.

9.3 Design supporting contactor-less car stop (Only with EN 81.2 (2020) rules)

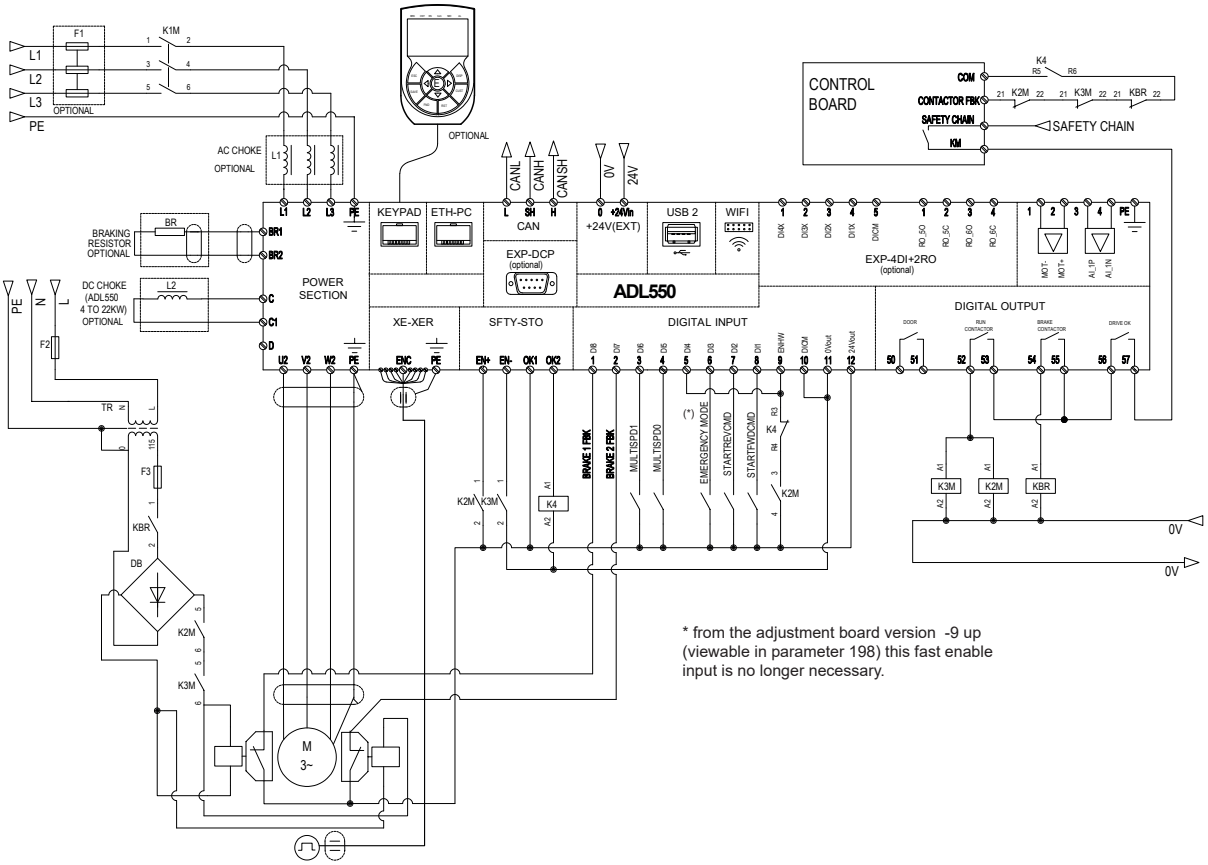


Figure 11 - ADL500 contactor – less application design case

The figure above is as Lift reference design to be implemented for a Lift System according to **UNI EN 81-20 (2014)** (see 5.9.2.5.4 – d) using no contactors and a safety integrated function STO SIL3 (according to **CEI EN 61800-5-2 (2007)**) instead of two contactors.

The function is enabled through parameter PAR 11088.

With respect to the above prescriptions we can notice that:

1. ECU uses both ***ENABLE*** and ***SAFETY ENABLE*** signals by means of two different relays (K2M, K4)
2. ECU monitors both feedback relays: ***STO FBK*** and ***CONTACTORLESS OK*** (which is contactor a configured as ***Digital Input Monitor ENHW;*** DRIVE OK in this case is not used)
3. Any time Motor comes to a stop ***STO FBK*** relay and ***CONTACTORLESS OK*** shall be monitored by ECU, switch from open status to closed status. In case of unexpected relay status (***STO FBK, CONTACTORLESS OK***) is found ECU will not issue a restart (K2M, K4 and K3M, Emergency Failure remain open) until condition is cleared.

NOTE!

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

The above case would prevent current from flowing in conductors making STO safety function active.

NOTE!

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*.

10 - Safety Advices

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.

NOTE!

Only Qualified Personnel are allowed to execute any activities during installation and commissioning procedures.

WARNING!

All people working with or on the ADL500 / ADL550-ICS device must have read the STO safety manual and the warnings in this document. Before carrying out any work, they must be instructed in the correct handling of the device.

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.

He / She 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 ADL500 / ADL550-ICS drive family. It contains additional safety information complying with Machinery Directive. for supporting use of drive safety-related functions. Use of this function 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.

STO is a stop category 0 function, according to **EN 60204**. It must operate and take the Drive into a safe state independently from the operational status of drive unit.

Safety integrated system is not affected from operational status of the internal parts not related to safety.

Safety integrated system is not affected from operational status of the external parts not related to safety if the installation and commissioning activities are made correctly.

WARNING!

Resetting 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 EN 60204, drive will re-start only after operator manual confirmation.

WARNING!

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 § **"8.2 Maintenance"** must be set-up.

STO integrated safety function is double fault tolerant 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 be appropriately implemented and tested in order to support same fault tolerance (at least 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 is stopped (or in any case equal to 180°/n mechanical degrees; with n: number polar motor couples).

NOTE!

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 voltages 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 5 minutes) to allow high-voltage DC-link to discharge.

WARNING!

If some handheld radio transmitter is used closer than 20 cm, the PDS(SR) could be disturbed.

WARNING!

For Lift applications, the ECU (Elevator Control Unit) shall use ADL500 STO safety integrated function as means to stop cabin. Two separated and independent wirings shall be used to activate/deactivate ENABLE and SAFETY ENABLE signals.

WARNING!

The wiring used for ENABLE and SAFETY ENABLE connections must be protected against external damage (armouring, cable ducting) and protected by means sleeve rated to 600V.

11 - Overview STO

European standards

Safety Rules for the construction and installation of lifts: Lifts for the transport of persons and goods	EN 81-20 (2020)
Safety rules for the construction and installation of lifts: Examinations and tests	EN 81-50 (2020)
Electromagnetic compatibility: Emission	EN 12015 (2020)
Electromagnetic compatibility: Immunity	EN 12016 (2013)
Adjustable speed electrical power – Safety requirements: Electrical, thermal and energy	EN 61800-5-1 (2007)

Safety Function Standards

Adjustable speed electrical power drive systems – Safety requirements: Functional	IEC 61800-5-2 (2007)

Safety Performances

Safety Integrity Level	SIL 3
Probability Dangerous Failure on Demand (High Demand)	< 9 E-09/h
Hardware Fault Tolerance (HFT)	2 (1oo3)
Mission Time	20 Years

Reaction Time

Input to intervention response time	< 40 ms

12 - Description of the product code

Following the code description of the products implementing the STO safety function.

ADL550 - ### - 1 040 - X B L - F - 4 - EMS - ## - ####

SW/HW personalization:
[empty] = standard software
[not empty] = SW/HW personalisation

IT version:
[empty] = not included
IT = included

Emergency supply module:
[empty] = only UPS
UB = UPS or Battery + aux voltage supply (new standard)
EMS = UPS or direct battery connection without aux voltage supply

Rated voltage:
4 = 230 Vac - 400 Vac - 480 Vac, three-phase
2T = 200 Vac, three-phase
2M = 200 Vac, single-phase

EMI Filter:
[empty] = not included
F = included

Lift application:
L = standard LIFT application
X = other applications (TBD)

Braking unit:
X = not included
B = included

Keypad:
X = not included
K = included

Inverter power in kW:

011 = 1.1 kW	**110** = 11 kW
015 = 1.5 kW	**150** = 15 kW
022 = 2.2 kW	**185** = 18.5 kW
030 = 3 kW	**220** = 22 kW
040 = 4 kW	**300** = 30 kW
055 = 5.5 kW	**370** = 37 kW
075 = 7.5 kW	**450** = 45 kW

Drive mechanical dimensions:
1 = size 1
2 = size 2
3 = size 3
4 = size 4

Integrated control system:
[empty] = not included
ICS = included

Inverter series:
50
30
10

Figure 13 - ADL550 product

Safety User Manual
Series: ADL500 STO
Revision: 0.5
Date: 12/03/2025
Code: 1S9STOEN

WEG Automation Europe S.r.l.
Via Giosuè Carducci, 24
21040 Gerenzano (VA) · Italy
info.motion@weg.net

Technical Assistance: technohelp@weg.net
Customer Service: salesmotion@weg.net

www.weg.net

Driving efficiency and sustainability