Emotron FDU/VFX 2.0

AC drive

Option Safe Stop
(STO – Safe Torque Off)

Technical description
English
Emotron FDU/VFX 2.0 AC drive
Option Safe Stop
(STO – Safe Torque Off)

Technical description
English
# Contents

1. General ........................................................... 3  
2. Safe stop option (STO – Safe Torque Off) .... 6  
3. Explanation .................................................... 7  
4.Possibilities for safe stops STO .................... 7  
5. Disconnecting time ....................................... 7  
6. Technical description of safe stop option - STO 8  
7. Recommended circuit arrangements ........ 9  
8. Certificate .................................................... 20
1. General

Increasing automation is making it more and more important to protect persons from dangerous movements. Functional safety defines the measures necessary, by electrical or electronic means, to minimise or eliminate dangers due to malfunctions.

In normal operation, safety devices prevent access of persons to hazard zones. For certain procedures such as setting up operations, persons must enter hazard zones. In these situations, machine operators must be protected by means of specific safety provisions within the drive and control system.

Integrated safety systems offer the prerequisites for optimal realisation of protective functions on the control and drive side. This reduces planning and installation complexity. The use of integrated safety systems increases the machine functionality and availability compared to conventional safety systems.

1.1 Integrated safety systems

Emotron FDU and VFX series variable speed drives Version 2.0, sizes B, C, D, E and larger are available with a safe stop option (STO – Safe Torque Off).

‘Integrated safety systems’ are application-related safety functions that can be used for the protection of persons at machines.

Motion functions are still controlled by variable speed drives. This option ensures that limiting values are reliably maintained and provides safe inputs and outputs. With a safe stop option, the safety modules initiate control functions directly in the variable speed drive as defined in EN 60204-1.

1.2 The replacement of EN 954-1

Up to now, machine builders have had to provide verification of compliance with the general safety requirements according to EN 954-1 (Safety-related parts of control systems – Part 1: General principles for design) in accordance with European Machinery Directives. This standard requires risk analysis with the resulting safety categories (B, 1, 2, 3, 4), where B stands for low to virtually no safety and 4 for high safety. Machine manufacturers select safety devices for their particular machines based on the resulting safety categories.

EN 954-1 was replaced because it did not adequately consider programmable electronic systems and took no account of the dynamic behaviour (e.g. test intervals, longevity) and failure probability of the specific components. The successor standards EN 13849-1 (Safety of machinery – Safety-related parts of control systems - Part 1: General principles for design) and EN 62061 (Safety of machinery – Functional safety of safety-related electrical, electronic and programmable electronic control systems) provide a remedy.

EN ISO 13849-1 includes the qualitative approach of EN 954-1 and also provides quantitative safety function considerations. For the classification of the various safety performance levels, EN ISO 13849-1 defines Performance Levels (PL) based on the corresponding specific categories. The five performance levels (a, b, c, d, e) indicate the different average probability values of a dangerous failure per hour.

1.2.1 Performance Level (PL) according to EN ISO 13849-1

Average probability of a dangerous failure per hour (1/h)

<table>
<thead>
<tr>
<th>Performance Level (PL)</th>
<th>Average probability of a dangerous failure per hour (1/h)</th>
</tr>
</thead>
<tbody>
<tr>
<td>a</td>
<td>≥ 10^{-5} to &lt; 10^{-4}</td>
</tr>
<tr>
<td>b</td>
<td>≥ 3 \times 10^{-6} to &lt; 10^{-5}</td>
</tr>
<tr>
<td>c</td>
<td>≥ 10^{-6} to &lt; 3 \times 10^{-6}</td>
</tr>
<tr>
<td>d</td>
<td>≥ 10^{-7} to &lt; 10^{-6}</td>
</tr>
<tr>
<td>e</td>
<td>≥ 10^{-8} to &lt; 10^{-7}</td>
</tr>
</tbody>
</table>

Determination of required performance levels (PLr)

To determine the required performance level for each safety function of a safety-related control system, a risk assessment must be carried out and documented.

The informative Appendix A of the standard specifies a qualitative procedure for risk assessment and determination of the required performance level. The same risk parameters...
are used for the purpose of risk assessment as those defined in EN 954-1.

Risk parameters:

S  Severity of injury
S1  Slight (normally reversible injury)
S2  Serious (normally irreversible injury or death)
F  Frequency and/or exposure to hazard
F1  Seldom-to-less-often and/or exposure time is short
F2  Frequent-to-continuous and/or exposure time is long
P  Possibility of avoiding hazard or limiting harm
P1  Possible under specific conditions
P2  Scarcely possible

Risk graph for determination of the required performance level for each safety function:

![Risk Graph](source: EN ISO 13849-1)

Legend:

Start  Starting point for evaluation of safety function's contribution to risk reduction
L  Low contribution to risk reduction
H  High contribution to risk reduction
PLr  Required Performance Level

Determination of achieved performance level

For determination of the performance level of components/devices, the following safety parameters must be taken into consideration:

<table>
<thead>
<tr>
<th>Safety parameters defined in EN ISO 13849-1</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cat.</td>
<td>Category (B, 1, 2, 3, 4), structural design as a basis for achieving a specific performance level</td>
</tr>
<tr>
<td>PL</td>
<td>Performance level (a, b, c, d, e)</td>
</tr>
<tr>
<td>MTTFd</td>
<td>Mean time to dangerous failure</td>
</tr>
<tr>
<td>B10d</td>
<td>Number of cycles until 10 % of the components fail dangerously (for pneumatic and electromechanical components)</td>
</tr>
<tr>
<td>DC</td>
<td>Diagnostic coverage</td>
</tr>
<tr>
<td>CCF</td>
<td>Common cause failure</td>
</tr>
<tr>
<td>TM</td>
<td>Mission time</td>
</tr>
</tbody>
</table>

Further parameters to be considered are operating factors such as the demand rate and/or test rate for the safety function which can also have an influence on the resulting performance level.
1.3 Risk analysis
This documentation can only indicate the necessity of a risk analysis. Users of integrated safety systems must familiarise themselves with the relevant standards and legislation.

Before a machine can be marketed, machine manufacturers must perform a risk analysis in accordance with the Machinery Directive so as to determine the risk associated with the use of the machine. To achieve the highest level of safety, the Machinery Directive defines three basic principles:

- elimination or minimisation of risks due to the design;
- taking necessary protective measures against risks that cannot be eliminated;
- documentation of the residual risks and information of users about these risks.

1.3.1 Safe Stop Parameter
As determined by TÜV testing in accordance with ISO/EN 13849-1:2006 (see TÜV certificate, and based on the associated technical report no. 09 799 555179-001)

Requirements according to category 3 and Performance level d:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>PFHDssD</td>
<td>1.70 .10-9 rev per hour</td>
</tr>
<tr>
<td>DC</td>
<td>average (86%)</td>
</tr>
<tr>
<td>HFT</td>
<td>1 (Enable input and Safe Stop board)</td>
</tr>
<tr>
<td>MTTFd</td>
<td>380.52 years (high)</td>
</tr>
</tbody>
</table>

Outcome: SIL3, SILCL3 and Performance Level d

Requirements according to category 4 and Performance level e:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>PFHDssD</td>
<td>1.70 .10-9 rev per hour</td>
</tr>
<tr>
<td>DC</td>
<td>high (90% - indirect monitoring Safe Stop path, direct monitoring contactor contacts)</td>
</tr>
<tr>
<td>HFT</td>
<td>1 (pilot contactor and Safe Stop board)</td>
</tr>
<tr>
<td>MTTFd</td>
<td>380.52 years (high)</td>
</tr>
</tbody>
</table>

Outcome: SIL3, SILCL3 and Performance Level e

The following parameters were assumed and applied in the MTTFd calculation:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>B10d</td>
<td>2,000,000 (contactor under normal loading)</td>
</tr>
<tr>
<td>Dop</td>
<td>365 d/a</td>
</tr>
<tr>
<td>Hop</td>
<td>24 h/d</td>
</tr>
<tr>
<td>tcycle</td>
<td>600s</td>
</tr>
</tbody>
</table>

The MTTFd value must be recalculated in the event of different values for Dop, Hop and tcycle.

1.4 Stop categories and emergency stop
The following information is important if emergency stop circuits are used or needed in the installation where a variable speed drive is used. EN 60204-1 defines 3 stop categories:

Category 0: Uncontrolled STOP
Stopping by switching off the supply voltage. A mechanical stop must be activated. This STOP may not be implemented with the help of a variable speed drive or its input or output signals.

Category 1: Controlled STOP
Stopping until the motor has come to a standstill, after which the mains supply is switched off. This STOP may not be implemented with the help of a variable speed drive or its input or output signals.

Category 2: Controlled STOP
Stopping while the supply voltage is connected. This STOP can be implemented with each variable speed drive STOP command.

**WARNING!**
The standard specifies that all machines must be provided with a category 0 stop. If the application prevents this from being implemented, this must be explicitly stated.

Furthermore, every machine must be provided with an emergency stop function. This function must ensure that any dangerous voltage on the machine is disconnected as quickly as possible without the risk of further danger. In such an emergency stop situation, a category 0 or 1 stop may be used; the choice of category depends on the possible risks to the machine.

### Abbreviations

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>PFHDssD</td>
<td>Average probability of a dangerous failure per hour</td>
</tr>
<tr>
<td>DC</td>
<td>Diagnostic coverage</td>
</tr>
<tr>
<td>HFT</td>
<td>Hardware Fault Tolerance</td>
</tr>
<tr>
<td>Dop</td>
<td>Days of operation per year</td>
</tr>
<tr>
<td>Hop</td>
<td>Hours of operation per year</td>
</tr>
<tr>
<td>tcycle</td>
<td>Cycle time</td>
</tr>
<tr>
<td>SIL</td>
<td>Safety Integrity Level</td>
</tr>
</tbody>
</table>
2. Safe stop option (STO – Safe Torque Off)

In conformity with the machinery standard and certified by an approved body, this safety function can allow:

- easy machine certification
- omission of electromechanical redundancy
- reduction of wiring and installation complexity
- space-saving control cabinet use

Fig. 2 Safe stop option for sizes B to D

Fig. 3 Safe stop option for size E and up
3. Explanation

The safe stop option prevents unintended starting of a motor and ensures the safety of the operator and machine. This is achieved in that the power supply to the drive is reliably interrupted. The drive must not be able to generate any torque and perform any dangerous movements. Zero-speed monitoring is unnecessary. Interruption of the power supply can, but does not have to take place with contacts. Where external forces prevail, additional measures such as mechanical brakes must be provided for safe stops to reliably prevent possible movements.

4. Possibilities for safe stops STO

Suitable measures for a safe stop are, for example:

- contactor between power supply and drive system (mains contactor) or
- contactor between power section and drive motor (motor contactor) or
- blocking control pulses to the power semiconductor (pulse blocking).

Emotron FDU and VFX variable speed drives are available with safe stop option which is realised by pulse blocking. This obviates the necessity of further contactors which increases the operational reliability and incurs no further costs. This allows variable speed drives to be directly included without additional components in standard safety concepts where, for example, operating areas are protected with safety switches on protective devices or the devices are directly included in the emergency stop circuits.

5. Disconnecting time

The disconnecting time on initiating a safe stop is typically < 50 ms.
6. Technical description of safe stop option - STO

Emotron FDU and VFX variable speed drives with safe stop option are supplied with the safety function jumpered. This makes commissioning without safe stop easily possible. To use this function, the jumpers must be removed from the terminal strip on the option board (jumper between terminals 1 and 6 and jumper between terminals 2 and 5).

When the safety stop function is activated, this circuit arrangement ensures that the motor cannot start. This is achieved by the following actions:

- The 24 V DC signal at the safe stop input (Inhibit+ and Inhibit-) is interrupted. Safety relay K1 is de-energised. The supply voltage to the driver circuits of the power is interrupted. This will inhibit the trigger pulses to the power conductors.
- The trigger pulses from the control board are cancelled. The signal is monitored by the control board.

To make sure that the safety relay K1 is de-energised, it should be externally monitored. For this purpose, the safe stop option board generates a feedback signal via a second safety relay that is energised when the supply voltage to the driver circuits is shut down.

<table>
<thead>
<tr>
<th>X1 Pin</th>
<th>Name</th>
<th>Function</th>
<th>Specification</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Inhibit +</td>
<td>Inhibit driver circuits of power conductors</td>
<td>DC 24V (20 - 30V)</td>
</tr>
<tr>
<td>2</td>
<td>Inhibit -</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>NO contact relay K2</td>
<td>Feedback: Confirmation of activated inhibit</td>
<td>48V DC / 30V AC/2A</td>
</tr>
<tr>
<td>4</td>
<td>P contact relay K2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>GND</td>
<td>Supply ground</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>+ 24V DC</td>
<td>Supply Voltage for operating inhibit input only</td>
<td></td>
</tr>
</tbody>
</table>

Safe output K2 (terminals 3 and 4)
Information can be output to a higher-level unit (e.g. safety PLC) or external operating elements (actuators) via the safe output on the option board. The feedback output is isolated and must be separately supplied with 24 V.

When the safe stop input is active, the variable speed drive display will show a blinking 'SST' symbol in section C (bottom left corner) of the display and the red warning/fault LED on the control panel will blink. To resume normal operation, the following steps have to be taken:

- enable safe stop input (terminals 1 and 2)
- Give a STOP signal to the VSD, according to the set Run/Stop Control in menu [215]
- Give a new RUN command, according to the set Run/Stop Control in menu [215]

**WARNING!**
The safe stop function must never be used for electrical maintenance purposes. Before carrying out any electrical maintenance, the variable speed drive must always be disconnected from the power supply.
7. **Recommended circuit arrangements**

The standard specifies the use of a stop button with double contact (S1). The variable speed drive logic output signals cannot be regarded as safety-related signals.

Recommended circuit arrangements are shown on the following pages as examples:

**Fig. 5, page 10**
This circuit arrangement is suitable for free coasting machines with short stopping times.
When the emergency stop circuit is activated, the 'safe stop' safety function is activated.
The connected motor coasts freely.

**Fig. 7, page 12**
Circuit arrangement according to standards EN 954-1, category 3 and IEC/EN 61508, capacity SIL2, stop category 1 according to standard IEC/EN 60204-1
This circuit arrangement is suitable for free coasting machines with long stopping times (with strong moment of inertia or weak counter-torque).
When the emergency stop circuit is activated, the variable speed drive causes the motor to coast controlled and the 'safe stop' safety function is activated with a delay corresponding to the coasting time.

**Fig. 9, page 14**
Circuit arrangement according to standards EN 954-1, category 3 and IEC/EN 61508, capacity SIL3, stop category 1 according to standard IEC/EN 60204-1
This circuit arrangement is suitable for free coasting machines with long stopping times (with strong moment of inertia or weak counter-torque).
When the emergency stop circuit is activated, the variable speed drive causes the motor to coast controlled and the 'safe stop' safety function is activated with a delay corresponding to the coasting time.

**Fig. 10, page 15**
Circuit arrangement according to standards EN 954-1, category 4 and IEC/EN 61508, capacity SIL3, stop category 0 according to standard IEC/EN 60204-1 (only for sizes B, C, and D)
This circuit arrangement is suitable for free coasting machines with short stopping times.
When the emergency stop circuit is activated, the 'safe stop' safety function is activated and the power supply is disconnected via the power contactor.
The connected motor coasts freely.

**Fig. 11, page 16**
Circuit arrangement according to standards EN 954-1, category 4 and IEC/EN 61508 capacity SIL3, stop category 2 according to standard IEC/EN 60204-1 (only for sizes B, C and D)
This circuit arrangement is suitable for free coasting machines with long stopping times (with strong moment of inertia or weak counter-torque).
When the emergency stop circuit is activated, the variable speed drive causes the motor to coast controlled, the 'safe stop' safety function is activated with a delay corresponding to the coasting time and the power supply is disconnected via the power contactor.
Fig. 5  
IEC/EN 61508, Sicherheitskategorie 1, Stoppkategorie 0

Sicherer Halt

IEC/EN 61508
Sicherheitskategorie 1
Stoppkategorie 0
IEC/EN 61508, Level SIL 3

Safety category 3, stop category 1

IEC/EN 61508 Stufe SIL3
Sicherheitskategorie 3
Stopkkategorie 1

Plot rhema CG 1 vom 13.04.2012

14 Recommended circuit arrangements
Fig. 10  IEC/EN 61508, level SIL 3
Safety category 4, stop category 0
Fig. 11  IEC/EN 61508, level SIL 3
Safety category 4, stop category 2
IEC/EN 61508, level SIL 3

Safety category 3, stop category 1

Fig. 12

IEC/EN 61508 Stufe SIL3
Sicherheitskategorie 3
Stopkkategorie 1
8. Certificate

# Zertifikat

**Registrier-Nr.**  
Registration No.: 44 799 09 555179

<table>
<thead>
<tr>
<th>Zeichen des Auftraggebers</th>
<th>Auftragsdatum</th>
<th>Aktenzeichen</th>
<th>Prüfbericht Nr.</th>
<th>Testreport no.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Customer’s reference</td>
<td>Date of order</td>
<td>File reference</td>
<td>09 799 555179-001</td>
<td>09 799 555179-001</td>
</tr>
</tbody>
</table>

**Name und Anschrift des Auftraggebers**  
Emotron AB  
Mörsaregatan 12  
SE-250 24 Helsingborg

**Geprüft nach**  
- EN 61800-5-2:2007  
- EN ISO 13849-1:2008  
- EN 62061:2005  
- EN 61508:2001

**Anforderungen bis Kategorie 4 und Performance Level e**  
- Requirements according to category 4 and performance level e

**Anforderungen bis SIL3**  
- Requirements according to SIL3

**Anforderungen bis SIL3**  
- Requirements according to SIL3

**Beschreibung des Produktes**  
*(Details siehe Anhang 1)*

**Frequenzumrichter mit der sicheren Funktion STO**  
*(sicher abgeschaltetes Moment)*

**Frequency converter with safety function STO**

**Typenbezeichnung**  
Seriel/Series VFX 2.0 und FDU 2.0

**Bemerkung**  
Die Anforderungen gemäß EN 61800-1 waren nicht Bestandteil der Prüfung  
Requirements according to EN 61800-1 are not part of the examination

Dieses Zertifikat bescheinigt das Ergebnis der Prüfung an dem vorgestellten Prüfgegenstand. Eine allgemein gültige Aussage über die Qualität der Produkte aus der laufenden Fertigung kann hieraus nicht abgeleitet werden.  
This certifies the result of the examination of the product sample submitted by the manufacturer. A general statement concerning the quality of the products from the series manufacture cannot be derived there from.

**TÜV NORD CERT GmbH**  
Certification body for product safety

**Gültig bis / Valid to:** 07.08.2014  
Hannover, 07.08.2009

**Bitte beachten sie auch die umseitigen Hinweise**  
Please also pay attention to the information stated on the back

Langemarckstr. 20  • 45141 Essen  •  Fon: +49 (0)201 825 5120  •  Fax: +49 (0)201 825 3268  •  Email: machinery@tuev-nord.de