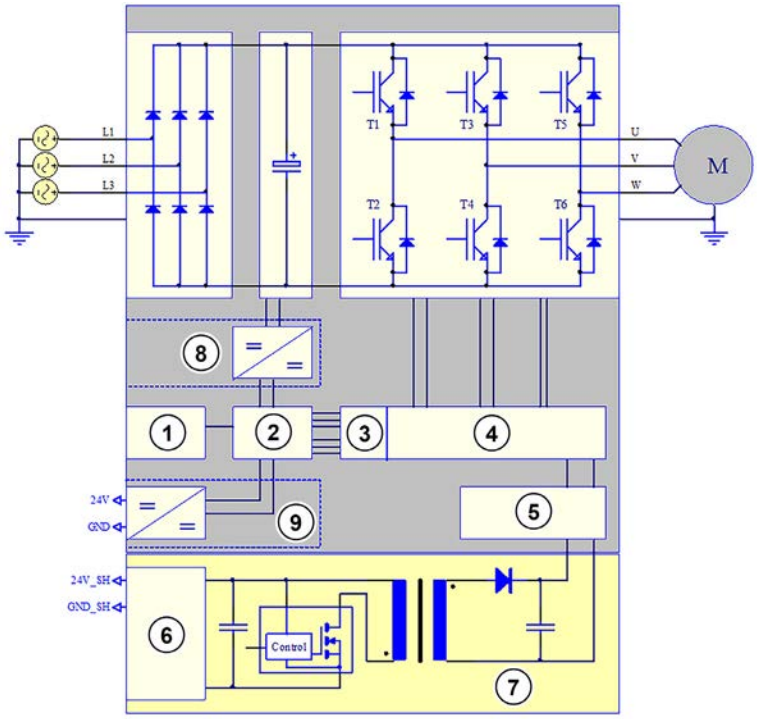
Explanation of STO with PFH = 0 / PFD = 0

Frequency inverters from the NORD DRIVESYSTEMS Group support the functional safety of machines. They can be delivered with safe shutdown methods that allow electrical machines to be shut down safely. The torque can be safely shut down using the “Safe Pulse Block” by interrupting the motor’s flow of current. This is the safe function “Safe Torque Off (STO)”.

For devices with low to medium powers, the “Safe Pulse Block” has been designed to reveal the probability of a hazardous failure per hour of PFH = 0 and the probability of a hazardous failure on call-up of PFD = 0. This results in the diagnostic coverage level not being determinable due to division by zero. This results in questions from customers and experts on the accuracy since, for example, the PFHD value must be indicated as not equal to zero in the former version of the SISTEMA V1.1 calculation tool of the Institute for Occupational Safety and Health of the German Social Accident Insurance (IFA). SISTEMA V2.0 now allows for the entry of the PFHD value as equal to zero.



1	I/O quick stop
2	Microcontroller
3	Logic
4	Driver
5	Undervoltage detection, current limitation
6	Input wiring
7	“Safe Pulse Block” option
8	DC/DC converter (SK 2x0E only)
9	DC/DC converter (SK 2x5E only)

Illustration 1: Structure of Safe Pulse Block, sizes 1 to 3

The top image shows the structure of frequency inverters with low and medium powers that contain the Safe Pulse Block. The resulting basic functionality is as follows.

The mains voltages are rectified and the resulting intermediate circuit voltage is inverted according to the requirements of the motor’s operating status (frequency and voltage).

The inverter's semiconductor switches (T1 to T6) are controlled via a very complex pulse pattern. This pulse pattern is generated by the microcontroller (µC) and amplified by the driver. The driver takes over the conversion of the logic signals to the control voltages of the semiconductor switches. The semiconductor switches are switched via the control voltage and the pulse pattern is amplified and applied to the motor terminals. Due to the low-pass effect of the motor, a three-phase system results

from the pulsed voltage, a three-phase pulse width modulated sine-wave voltage. The motor generates a torque.

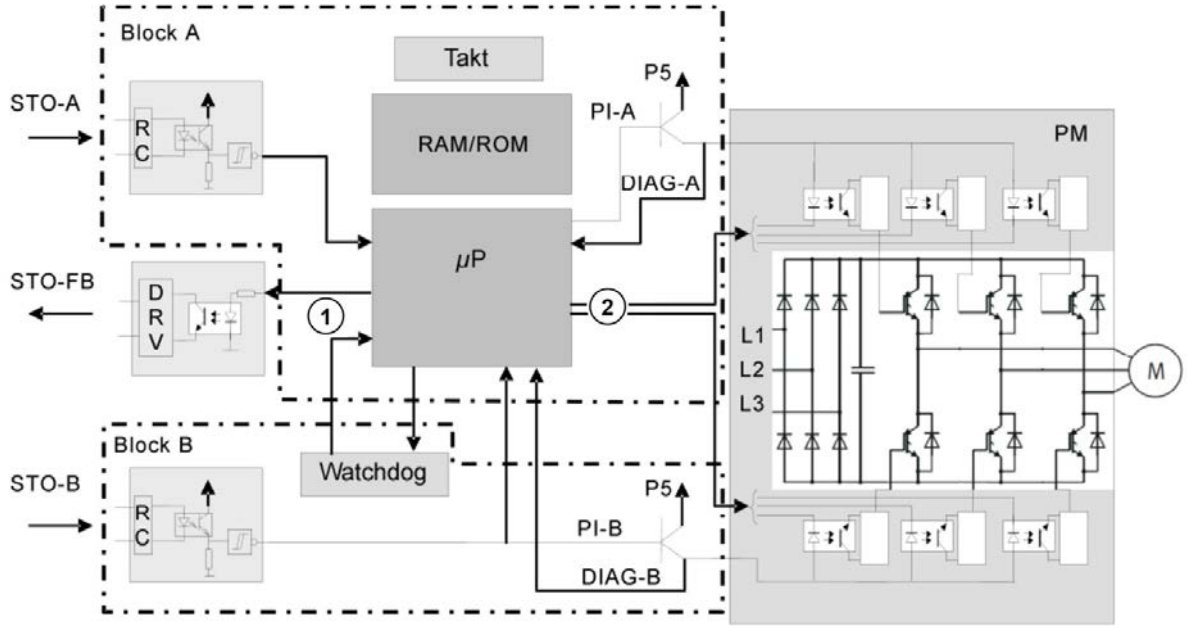
Devices equipped with the “Safe Pulse Block” have an additional DC/DC converter, which produces the supply voltage for the drivers from a 24 V voltage (contacts 24V_SH, GND_SH).

If this 24 V voltage is switched off, the DC/DC converter does not transmit any power to the drivers. As the drivers are now no longer supplied with power, no control pulses reach the semiconductor switches (T1 to T6) of the inverter. The flow of current in the semiconductor switches and in the motor is interrupted. In other words, after a certain reaction time of the electronics and the reduction time of the motor current, the motor does not develop a driving torque.

Switching off the drivers’ supply voltage is a simple approach to implement the safe function “Safe Torque Off (STO)”.

The trend, however, is towards signal-based solutions where the microcontroller’s output signals are switched off. These output signals generate the pulse pattern. The following image shows an example.

The safety function is triggered via one or more digital inputs that can be evaluated analogously or via the microcontroller. As the control signals are switched off via the microcontroller or other electronic switches, hazardous failures are to be expected at least to a small extent. Such solutions with a PFH value not equal to zero are well known to the majority of drive technology and control technology experts.



Legend

(1)	Reset
(2)	Pulse signals
P5	Supply voltage 5 V
PI-A(B)	Pulse channel A(B)
DIAG-A(B)	Diagnostic channel A(B)
RC	Resistor-capacitor filter
DRV	Output driver
PM	Power module
µP	Microprocessor

Illustration 2: Example of the signal-based approach on establishing the safe function “Safe Torque Off (STO)” according to EN 61800-5-2 (VDE Verlag, 2017, DIN EN 61800-5-2 (VDE 0160-105-2)).

The “Safe Pulse Block” safety function was evaluated by an FMEA. Individual and multiple failures of the module and its switching components were analysed down to the component level.

Potential failures that occur in the functional safety’s or frequency inverter’s switching component do not result in hazardous failures. This means that even in case of multiple failures it is not possible to power the drivers via external voltage to control the IGBTs despite a triggered safety function.

A potential failure would be that the IGBT is controlled with 5 V via an internal or external short circuit on the IC driver, although the drivers’ supply voltage (15 V) is switched off. The IGBT – provided it switches at all – would be operated in the linear range and, in case of a new failure where no current flow is established in the IGBT, thermally destroyed.

Another failure would be a permanently actuated IGBT due to an internal short circuit. Since the motor requires a complex pulse pattern generating sine voltage to rotate, no movement is possible.

Two permanently short-circuited IGBTs would lead to direct current flowing through the motor. This could result in a 90° adjustment movement of the 4-pole motor.

The increased standard requirements for clearance and creepage distances on the circuit board and in the device are met. Operation in an IP54 housing is mandatory and the maximum EMC limit values for the interference resistance have been specified. Based on this, an exclusion of failures has been applied to the short circuit of adjacent conductors.

During operation of the frequency inverter within the framework defined in the manual, it may be normatively assumed that the safety function’s switching component cannot be supplied via an external or internal voltage of the frequency inverter’s common switching component.

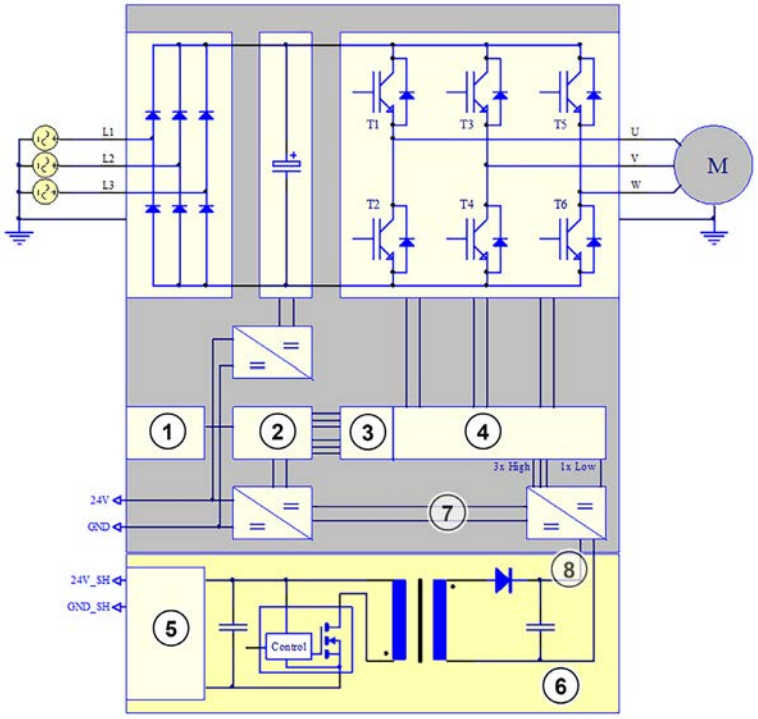
The evaluation of the “Safe Pulse Block” safety function via an FMEA has revealed the probability of a hazardous failure per hour of PFH = 0 and the probability of a hazardous failure on call-up of PFD = 0.

For frequency inverters with higher powers, the protective switching device’s power is insufficient for the driver supply. For that reason, the drivers are supplied by a separate power supply unit whose control voltage is supplied by the protective switching device. If the power supply unit’s control voltage is switched off, the power supply unit cannot transmit any more energy to the drivers. The IGBTs cannot be controlled anymore and the motor runs down to a standstill.

The FMEA has revealed hazardous multiple failures. For this, several components of the power supply unit for the internal voltage (image below, item 7) must be defective (conductive/high-resistance). Oscillating voltage (AC voltage) on the input terminal of the 24 V supply voltage may allow the transfer of energy to the drivers via the power supply unit.

This failure case has been evaluated in the FMEA and for the size 4 SK 200E a very low probability of a hazardous failure per hour of PFH = 0.0058 FIT and a very low probability of a hazardous failure on call-up of PFD = 5.23x10-5 have been revealed.

The proportion of safe failures (SFF) is greater than 99%.



1	I/O quick stop
2	Microcontroller
3	Logic
4	Driver
5	Input wiring
6	“Safe Pulse Block” option
7	Internal voltage (primary power))
8	Control voltage

Illustration 3: Structure of Safe Pulse Block, size 4

Technical data, such as PFH and PFD, specified in the NORD DRIVESYSTEMS Group’s manuals are correct. They have been checked and confirmed by the TÜV NORD CERT GmbH. The product in its current form has been successful in the market for many years.