

User's manual

FSO-21 safety functions module



Certificates

TÜV Nord certificate for the FSO-21 and ACS880 drive series is attached below.
Check the validity of the certificate with a specific drive variant from the ABB library.


Deutsche
Akkreditierungsstelle
D-ZE-11074-01-00



Certificate

No. SEBS-A.102621/15 V1.0

TÜV NORD Systems GmbH & Co. KG hereby certifies

ABB Oy
Hiomotie 13
00381 Helsinki
Finland

that the safety modules
FSO-21 with FSE-31
as plug-in modules for the ABB industrial drive ACS880 series
are capable for safety related applications up to SIL 3, SIL_{CL} 3 and PL e and meets the requirements listed in the following standards:

- IEC 61508 part 1, part 2, part 3: 2010
- IEC 61800-5-2: 2007
- ISO 13849 part 1: 2015, part 2: 2012
- IEC 62061: 2015

Beneath the integrated "Safe Torque Off (STO)" function within the industrial drive ACS880 series, the additional safety functions "(variable) Safely Limited Speed (SLS)", "Safe Maximum Speed (SMS)", "Safe Stop Emergency (SSE)", "Safe Stop 1 (SS1)", "Prevention Of Unexpected Start-up (POUS)", "Safe Direction (SDI)", "Safe Speed Monitor (SSM)" and "Safe Brake Control (SBC)" can be realized with the plug-in safety functions modules FSO-21 with FSE31.

The whole assembly can be used in safety applications up to SIL 3 according to IEC 61511.

Base of certification is the report SEBS-A.102621/15TB in the valid version.

This certificate entitles the holder to use the pictured safety approved mark.

Valid until: 2021-01-18
File reference: 8112485797

Hamburg, 2016-01-18

Bianca Pfuff

Certification Body SEECERT
TÜV NORD Systems GmbH & Co. KG
Große Bahnstraße 31, 22525 Hamburg, Germany



Voluntary Certification

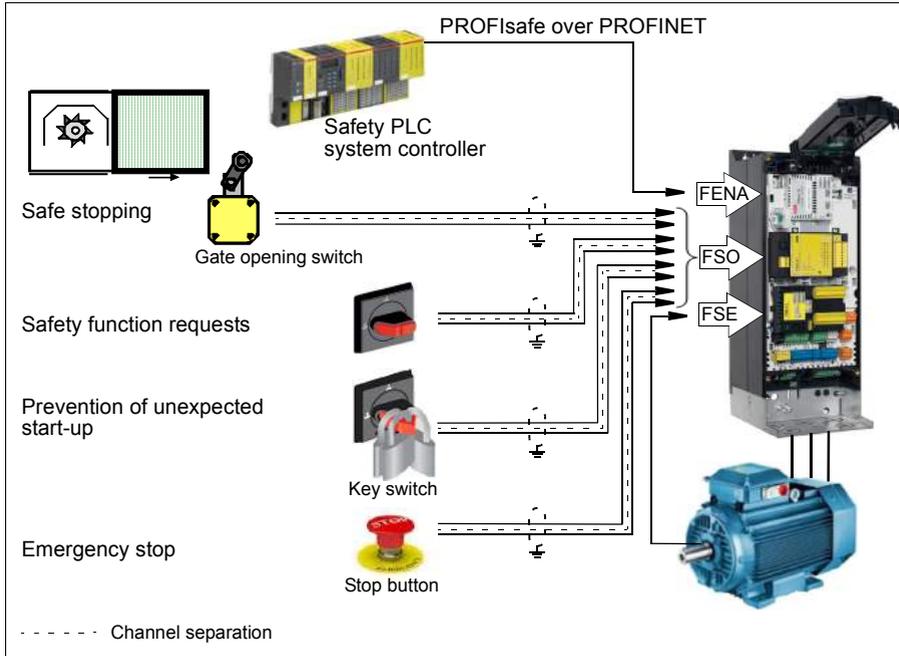
TUV NORD
TUV NORD Systems
GmbH & Co. KG
Safety Approved

FSO-21, FSE31
IEC 61508:2010 SIL 3
IEC 61800-5-2:2007 SIL 3
ISO 13849-1:2015 PL e
ISO 13849-2:2012 PL e
IEC 62061:2015 SIL_{CL} 3
SEBS-A.102621/15

System description

■ FSO module and safety system components

Example figure of a safety system with the FSO-21 safety functions module, the ACS880-01 drive, a safety PLC, the FENA-21 module, the FSE module, switches and buttons.



The FSO safety functions module is an option for the ACS880 drives. The Safe torque off (STO) function is a standard feature on the ACS880 drives.

The FSO module does not operate the drive; it only monitors the actions of the drive and commands safety functions to be executed. The request for safety functions can come from an external safety system, for example, a push button, a safety PLC, or from an FSO internal fault. Some safety functions can be permanently active. If the drive does not fulfill the commands of the FSO, the FSO shuts down the drive using the Safe torque off (STO) function.

If the drive is connected to a safety PLC, the safety of the fieldbus communication can be secured with the PROFIsafe over PROFINET technology. The safety PLC is connected to the FENA-21 fieldbus adapter module, which communicates with the FSO module. For more information, see chapter [PROFIsafe](#).

If a pulse encoder is used in the safety system, it is connected to the FSE-31 module, which communicates with the drive and the FSO-21 module.

Safety functions supported by the FSO module are presented in chapter [Safety functions](#).

■ FSO module version handling

To ensure backward and forward compatibility with the ACS880 drives, the FSO-21 module has a version handling system. Both the FSO module and the ACS880 drive firmware must support the used safety functions.

You can always replace the FSO-21 module with a newer revision and use the same configuration file with the new revision. If you replace an FSO-12 module with an FSO-21 module, you have to re-configure the FSO module and safety functions. Each time you make any changes in the safety system, you must do the acceptance test to each safety function using the checklists described in chapter [Verification and validation](#).

Each new revision of the FSO-21 module supports all functions of previous FSO-21 module revisions and it can be used together with previous ACS880 drive firmware versions. In addition, previous FSO-21 module revisions can be used together with new ACS880 drive firmware versions. In this case, the drive supports only the functions of the previous FSO-21 module revision.

Each safety function and parameter group has a separate version parameter. With these parameters, the user selects the desired versions according to the drive firmware and FSO-21 module combination at the start-up. Only the versions that both the used ACS880 drive firmware and the FSO-21 module support are shown in the Drive composer pro PC tool.

System description

Required components

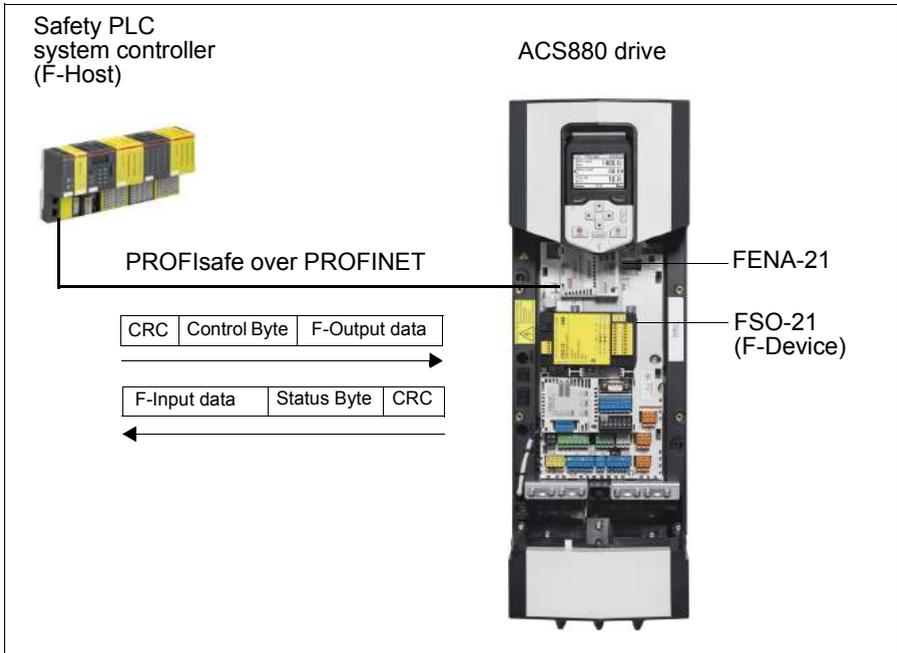
- FSO-21 safety functions module
- ACS880 Primary control program: version 2.12 or later
- FENA-21 Ethernet adapter module: version 3.05 or later
- compatible safety PLC system, for example, ABB AC500-S Safety PLC or Siemens SIMATIC Fail-safe S7 PLC

Tools

- Drive composer pro: version 1.7 or later
- For ABB PLCs: Automation builder: 1.0 or later (includes PS501 Control Builder Plus version 2.3.0), safety license PS501-S
- For Siemens PLCs: SIMATIC Step 7 V5.5 + S7 Distributed Safety V5.4 and SIMATIC Step 7 V 11 (TIA Portal) + Step 7 Safety Advanced V 13

System overview

This figure shows an overview of a safety PLC that is connected to the ACS880 drive via the PROFIsafe communication bus.



Status Byte and CRC2 bit order

PROFIsafe messages sent from the FSO module to the safety PLC include the F-Input user data, the Status Byte and CRC2.

This table shows the bit order of the Status Byte and CRC2.

N_i is the length of F-Input user data.

Octet	Bit	Name	Description
Status Byte			
N_i	7	Reserved	The value is always 0. Must be ignored by the F-Host.
	6	cons_nr_R	Vconsnr_d has been reset.
	5	Toggle_d	Toggle bit
	4	FV_activated	Fail-safe values (FV) activated.
	3	WD_timeout	Communication fault: Watchdog timeout
	2	CE_CRC	Communication fault: CRC error
	1	Device_Fault	Failure exists in the F-Device.
	0	iPar_OK	F-Device has new iParameter values assigned. Not in use. The value is always 0.
CRC2			
N_i+1	7	CRC bit 23	Octet 3 (MSB) of 24 bit CRC
	...		
	0	CRC bit 16	
N_i+2	7	CRC bit 15	Octet 2 of 24 bit CRC
	...		
	0	CRC bit 8	
N_i+3	7	CRC bit 7	Octet 1 (LSB) of 24 bit CRC
	...		
	0	CRC bit 0	

■ FSO PROFIsafe profiles

The content of the F-Input and F-Output user data is configured with FSO specific PROFIsafe profiles. The FSO-21 module supports the ABB_PS1 and ABB_PS2 profiles.

The ABB_PS1 profile provides the functionality to control and monitor the safety functions, the SLS limits, the safe speed value and the states of the FSO I/O. In addition to the functionality in the ABB_PS1 profile, the ABB_PS2 profile includes the safe position value. The ABB_PS2 profile requires that an encoder is used in the safety system.

Basic safety data

The FSO-21 module is a type B safety component as defined in IEC 61508-2.

The FSO-21 data related to safety standards IEC 61508, EN/IEC 61800-5-2, EN ISO 13849-1 and EN/IEC 62061 is listed below for the different subsystems within the FSO module.

The given safety data applies with proof test interval $T1 = 20$ years (high demand and continuous mode of operation) and $T1 = 2$ years or $T1 = 5$ years (low demand mode of operation). Make sure that the proof test is performed within this time (see also section [Proof tests](#) on page 424).

EN 61508	
SIL	up to 3
SC	3

EN ISO 13849-1	
PL	up to e

EN/IEC 62061	
SILCL	3

3AXD10000289254.xlsm G

	PROFI-safe ¹⁾	1-ch. DI, pulses	2-ch. DI, pulses	1-ch. DI, no pulses	2-ch. DI, no pulses	Logic 1, 1-ch. DI or DO, no pulses ²⁾	Logic 2, other cases ²⁾
SIL/SILCL	3	3	3	2	3	1	3
PL	e	d	e	c	e	c	e
PFH (1/h)	1.0E-09	5.1E-10	1.8E-12	9.0E-09	2.3E-12	4.5E-09	4.4E-11
PFD _{avg} (T1 = 2 a)	8.8E-05	4.8E-06	2.4E-08	7.9E-05	2.8E-08	5.2E-05	4.1E-07
PFD _{avg} (T1 = 5 a)	8.8E-05	1.2-E5	4.8E-08	2.0E-04	5.8E-08	1.3E-04	9.9E-07
MTTF _D (a)	114155	17844	12648	12648	12648	5048	5048
HFT	N/A	0	1	0	1	0	1
Cat.	N/A	2	3	1	3	1	3
SFF (%)	N/A	99.64	99.94	94.02	99.92	86.82	93.48
DC (%)	N/A	91.99	99.00	0.00	98.74	80.26	90.23

3AXD10000289254.xlsm G

¹⁾ We assume conservatively that $PFH = \lambda d = 1$, $FIT = 1e-9$ 1/h, $MTTF_D = 1/\lambda d = 1/(1e-9$ 1/h) = $1e9$ h = 114155 a. Based on the BGIA Report 2/2008e: Functional Safety of Machine Controls – Application of EN ISO 13849, ch. 6.2.17.

²⁾ Either logic subsystem (Logic 1 or Logic 2) is included in each safety function implemented with the FSO. If the safety function contains any 1-channel digital input or output of the FSO with non-pulsed signals, the subsystem "Logic 1" must be used. Otherwise the subsystem "Logic 2" is used.