MANUFACTURER DOCUMENT PACKAGE

Manufacturer's Manual

Reference package for procurement and maintenance review

ABB

SM560-S-FD-4

SAFETY PROCESSOR MODULE

Used with the applicable AC500-S configuration.

REFERENCE PACKAGE

OFFICIAL DOCUMENT

Selected official manufacturer pages follow this cover.

Source: ABB AC500-S Safety User Manual 3ADR025091M0211

3 AC500-S safety modules

3.1 Safety CPU - SM560-S / SM560-S-FD-1 / SM560-S-FD-4

Elements of the module

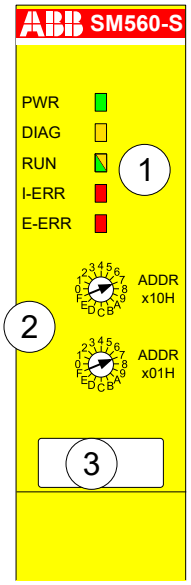

Fig. 5: SM560-S / SM560-S-FD-1 / SM560-S-FD-4

1 Five LEDs for status display
2 Rotary switch for address/configuration setting
3 Label

3.1.1 Purpose

SM560-S / SM560-S-FD-1 / SM560-S-FD-4 are safety CPUs for up to SIL 3 (IEC 61508), max. SIL 3 (IEC 62061) and PL e (ISO 13849-1) safety applications. The safety CPU is mounted on the left side of the non-safety CPU on the same terminal base. The communication between the non-safety CPU and the safety CPU takes place through the internal communication bus, which is integrated in the terminal base.

Depending on the used terminal base and used non-safety CPU, more than one communication module can be simultaneously employed at one non-safety CPU. However, only one safety CPU can be operated simultaneously at one non-safety CPU.

The safety CPU is programmed and configured via the DPRAM using safety system configurator and AC500-S Programming Tool which are a part of the Automation Builder software.

The configuration of the safety CPU is saved non-volatile in its flash EPROMs.

Information on how to combine safety CPUs with its non-safety environment can be found in the compatibility information ↬ *Appendix B.1 “Compatibility with AC500 V2 non-safety CPU” on page 381* ↬ *Appendix C.1 “Compatibility with AC500 V3 non-safety CPUs” on page 408*.

3.1.2 Functionality

3.1.2.1 Overview

AC500 safety CPUs are always used with non-safety CPUs.

Programming of the safety CPU is done using AC500-S Programming Tool in a similar way as programming of AC500 CPU, but in accordance with the safety programming guidelines. Programming is done by means of routing via the AC500 CPU using the serial interface or Ethernet. The user program is composed of:

- Compiled code of all POUs called in the program
- Initialization code for variables

SM560-S-FD-1 / SM560-S-FD-4 contains all features of SM560-S safety CPU. Additional features available on SM560-S-FD-1 / SM560-S-FD-4 safety CPUs are:

- PROFIsafe F-Device functionality
  - SM560-S-FD-1 is able to communicate with 1 PROFIsafe F-Host (controller)
  - SM560-S-FD-4 is able to communicate with up to 4 PROFIsafe F-Hosts (controllers)
- Bigger safety program size: 1.3 MB (SM560-S safety CPU has 1.0 MB)

Each safety CPU variant has its own product identifier in the production data. Thus, a download of a boot project to a wrong product variant is detected by its firmware.

3.1.2.2 Floating-point operations

Safety CPUs can perform floating-point operations.

DANGER!

Divisions by zero are not allowed and shall be caught latest during the formal safety CPU code review according to safety programming guidelines *Chapter 4.4 “Safety programming guidelines” on page 182*.

If case of exceptions during floating-point operations (e.g., due to usage of invalid arguments), the safety CPU goes to a SAFE STOP state or delivers a return value "Infinity".

Note that the range of valid arguments in safety CPU for floating-point functions is:

- SIN and COS: [-9×10^{15} ... 9×10^{15}]
- TAN: [-4.5×10^{15} ... 4.5×10^{15}]
- ATAN: [-3.402823×10^{38} ... 3.402823×10^{38}]
- LOG, LN and SQRT: up to 3.402823×10^{38}

The arguments outside the above-presented range will lead to a SAFE STOP state of the safety CPU.

DANGER!

The end-result of floating-point operation has to be checked for its validity before it is further used in the safety program.

DANGER!

It is important to take into account the following while programming with floating-point arithmetic *[5]*:

- Round or truncate results after each floating-point operation according to defined ULPs (MOD, EXPT, EXP, ABS, TAN, ASIN, ACOS, ATAN, SIN, COS, LOG and LN operations are executed with a maximum expected error of 2 ULP; ADD, SUB, MUL, DIV and SQRT are executed with a maximum error of 1 ULP in the safety CPU). *http://en.wikipedia.org/wiki/Unit_in_the_last_place* for more details on ULPs.
- If you compute a value which is the result of a sequence of floating-point operations, the error can accumulate and greatly affect the computation itself.
- Whenever subtracting two numbers with the same signs or adding two numbers with different signs, the accuracy of the result may be less than the precision available in the floating-point format.
- The order of evaluation can affect the accuracy of the result.
- When performing a chain of calculations involving addition, subtraction, multiplication and division, try to perform the multiplication and division operations first.
- When multiplying and dividing sets of numbers, try to arrange the multiplications so that they multiply large and small numbers together; likewise, try to divide numbers that have the same relative magnitudes.
- When comparing two floating-point numbers, always compare one value to see if it is in the range given by the second value plus or minus some small error value.

3.1.2.3 System functions

The safety CPU is not equipped with a battery. Therefore, all operands are initialized once the control voltage is switched on. Data exchange between safety and non-safety CPUs is possible *Appendix B.5 “Data exchange between safety CPU and AC500 V2 non-safety CPU” on page 392* *Appendix C.5 “Data exchange between safety CPU and AC500 V3 non-safety CPU” on page 419*.

DANGER!

It is not recommended to transfer data values from non-safety CPU to safety CPU. But if doing so, end-users have to define additional process-specific validation procedures in the safety program to check the correctness of the transferred non-safety data, if they would like to use those non-safety values for safety functions.

It is of no concern to transfer data values from safety CPU to non-safety CPU, e.g., for diagnosis and later visualization on operator panels.

Self-tests and diagnostic functions (both start-up and runtime), like CPU and RAM tests, program flow control, etc. are implemented in the safety CPU according to IEC 61508 requirements.

Selected data can be stored fail-safe and permanently in the flash memory of the safety CPU using special library POUs SF_FLASH_READ, SF_FLASH_WRITE and SF_FLASH_DEL *Chapter 4.6.7.10 “SF_FLASH_READ” on page 322* *Chapter 4.6.7.11 “SF_FLASH_WRITE” on page 325* *Chapter 4.6.7.12 “SF_FLASH_DEL” on page 327*.

NOTICE!
You can not update both boot project and firmware / boot code at the same time for the safety CPU. Perform these updates in two steps. It means that you may need two SD cards. One SD card with firmware / boot code update and the other SD card with boot project update.

Firmware and boot code update

The procedure for SD card creation with firmware / boot code for a safety CPU is handled in the same way as described for communciation modules in *[3]*.

Boot project update

The safety CPU boot project can be updated only if no boot project is present on the safety CPU. This is to avoid unintentional boot project update on the safety CPU. Before updating a new boot project, delete the existing boot project on the safety CPU, e.g., via setting the address switch to value 0xFE/0xFC *Chapter 3.1.2.5 "Address / configuration switch / F_Dest_Add settings " on page 38*, via PLC browser command `delappl` in AC500-S Programming Tool or *"Online ➔ Reset Origin"* in Automation Builder.

3.1.3 Mounting, dimensions and electrical connection

The safety CPU is mounted on the left side of the non-safety CPU on the same terminal base. The electrical connection is established automatically when mounting the safety CPU. Basic information on system assembly is shown here. Detailed information can be found in *[3]*.

Installation and maintenance have to be performed according to the technical rules, codes and relevant standards, e.g. EN 60204 part 1, by skilled electricians only.

Assembly of the safety CPU

DANGER!
Hot plug and hot swap of energized modules is not permitted. All power sources (supply and process voltages) must be switched off while working with safety modules.

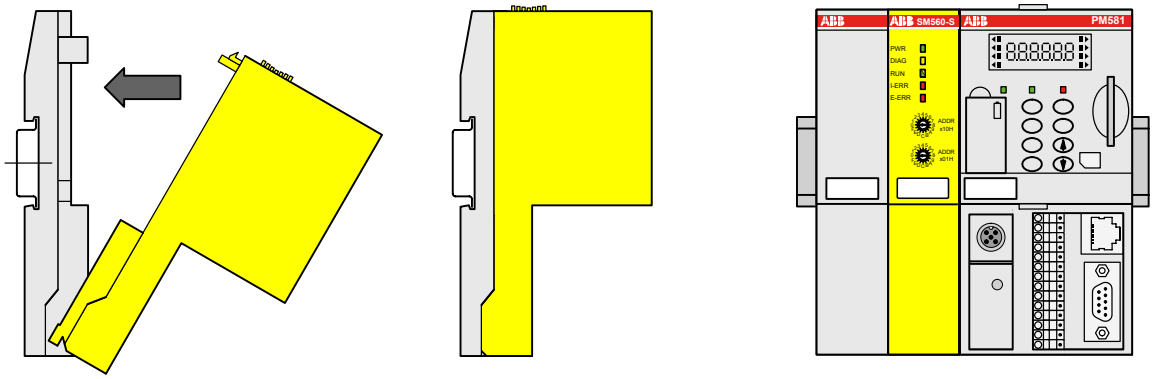

Fig. 7: Assembly instructions

▷ Insert the module below, and then click-in above.

Disassembly of the safety CPU

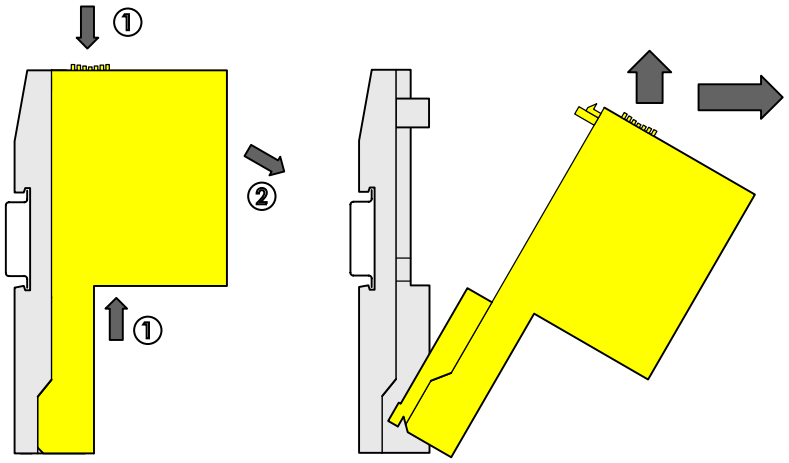

Fig. 8: Disassembly instructions

▷ Press above and below, then swing out the module and remove it.

Dimensions of the safety CPU

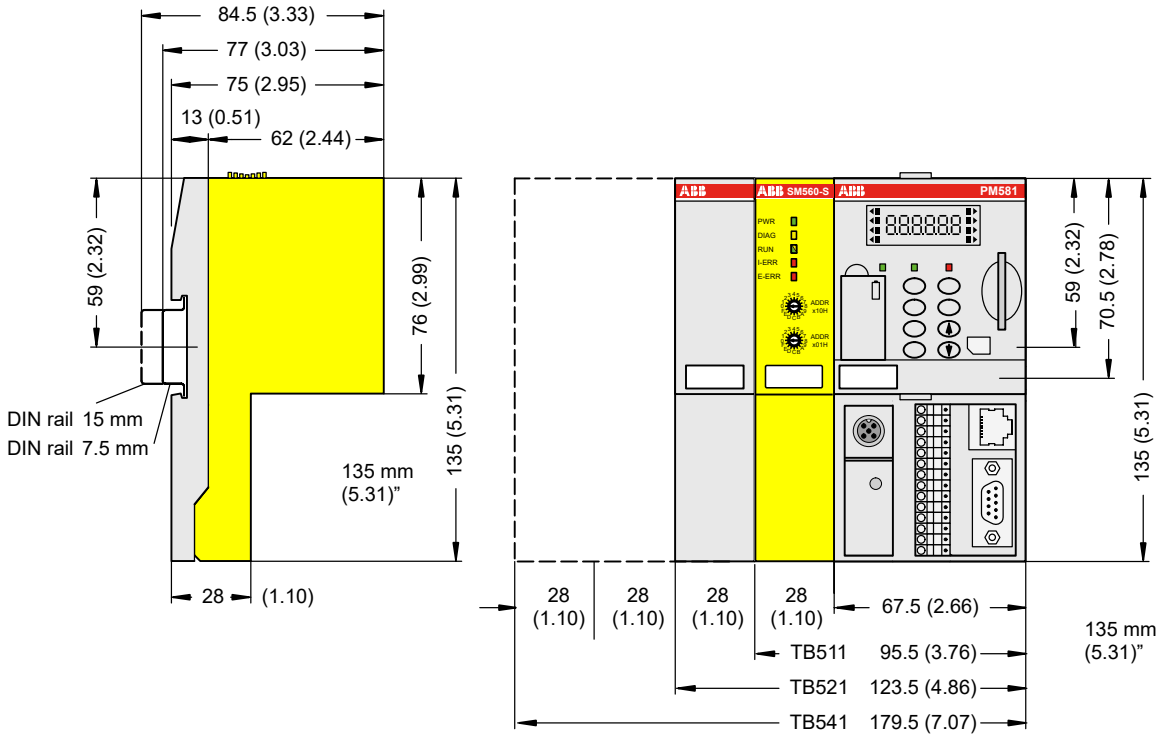

Fig. 9: Dimensions of the safety CPU

3.1.4 Diagnosis and LED status display

Safety CPU status is shown by its LEDs. RUN LED is bicolored. The following figure and table show positions and functions of 5 LEDs.

"Min update time" / "Update cycle time"

Depending on the used non-safety AC500 CPU the parameter for cycle time is called in a different way. The meaning of both parameters is identical.

Note, that this parameter influences the safety function response time. The smaller the value is, the faster the safety function response time will be ↳ *Chapter 5.1 "Overview" on page 333*. However, at the same time, the load on non-safety CPU increases with smaller values of *"Min update time"* / *"Update cycle time"*.



DANGER!
Big values (e.g., > 10 ms) of *"Min update time"* / *"Update cycle time"* parameter increase the chance of not delivering input pulse signals with a length < *"Min update time"* / *"Update cycle time"* value to the safety CPU.

"Enable debug"

If this parameter is set to *"Off"*, then no new boot project can be loaded to the safety CPU and debugging is not possible.

If a new boot project has to be loaded to the safety CPU, then, in advance, a new boot project with *"Enable debug"* parameter set to *"On"* for the safety CPU shall be loaded to non-safety CPU. After the reboot of non-safety CPU, a new boot project can be loaded to the safety CPU.

Note that the following PLC browser commands are supported on the safety CPU only if *"Enable debug"* parameter is set to *"On"* ↳ *list of all PLC browser commands*:

- resetprg - reset safety CPU program
- resetprgorg - reset safety CPU program original
- setpwd - set safety CPU login password
- delpwd - delete safety CPU login password
- delappl - delete user program
- deluserdat - delete user data segments

"PROFIsafe startup timeout"

This safety CPU parameter defines the time how long the safety CPU shall wait during start-up for the F-Device communication. In case of expired timeout, the safety CPU passivates the F-Device which enforces a reintegration by the user.

Value = 0 disables any timeout supervision for all F-Devices (no timeout supervision).

The value of this parameter is valid for all F-Devices.

3.1.8 Technical data

Additional technical data is available in ABB PLC catalog at www.abb.com/plc.



NOTICE!
Safety CPU -XC version is available for usage in extreme environmental conditions ↳ *Appendix A "System data for AC500-S-XC" on page 375*.

Memory

Data	Value	Unit
User program memory of SM560-S	1	MB
User program memory of SM560-S-FD-1 and SM560-S-FD-4	1.3	MB
User data memory (thereof 120 kB saved)	1	MB

Performance

Data	Value	Unit
Cycle time - binary	0.05	µs/instruction
Cycle time - word	0.06	µs/instruction
Cycle time - floating-point	0.50	µs/instruction

Voltages, according to EN 61131-2

Data	Value	Unit
Process and supply voltage (without ripple)	24 (-15 %, +20 %)	V DC
Absolute limits (including ripple)	19.2 ... 30	V DC
Ripple	< 5	%
Protection against reverse polarity	10	s



DANGER!
Exceeding the permitted process or supply voltage range (< -35 V DC or > +35 V DC) could lead to unrecoverable damage of the system.

Allowed interruptions of power supply, according to EN 61131-2

Data	Value	Unit
DC supply interruptions	< 10	ms
Time between 2 DC supply interruptions, PS2	> 1	s

Environmental conditions

Data	Value	Unit
Operating temperature*	0 ... +60	°C
Storage temperature	-40 ... +85	°C
Transport temperature	-40 ... +85	°C
Humidity without condensation	max. 95	%
Operating air pressure	> 800	hPa
Storage air pressure	> 660	hPa
Operating altitude	< 2000	m above sea level
Storage altitude	< 3500	m above sea level

* Extended temperature ranges (below 0 °C and above +60 °C) can be supported in special versions of the safety CPU ↳ *Appendix A "System data for AC500-S-XC" on page 375*.

Creepage distances and clearances

The creepage distances and clearances meet the overvoltage category II, pollution degree 2.

Power supply units

For the supply of modules, power supply units according to PELV/SELV specifications must be used.

Electromagnetic compatibility

For information on electromagnetic compatibility refer to the latest TÜV SÜD Report ↳ *[1]*.

Mechanical properties

Data	Value	Unit
Mounting	horizontal (or vertical with derating (maximal operating temperature reduced to +40 °C))	
Degree of protection of the PLC system	IP 20 (with all modules, option boards and terminals plugged in and with all covers closed)	
Housing	according to UL 94	
Vibration resistance acc. to EN 61131-2 (all three axes), continuous 3.5 mm	2 ... 15	Hz
Vibration resistance acc. to EN 61131-2 (all three axes), continuous 1 g *	15 ... 150	Hz
Shock test (all three axes), 11 ms half-sinusoidal	15	g
MTBF	168	years

* Higher values on request

Self-test and diagnostic functions

Start-up and runtime tests: Program flow control, RAM, CPU, etc.

Dimensions, weight

Data	Value	Unit
W x H x D	28 x 135 x 75	mm
Weight	~ 100	g

Certifications

CE, cUL (further certifications at *www.abb.com/plc*)

3.1.9 Ordering data

Type	Description	Part no.
SM560-S	Safety module - CPU, safety related module up to SIL 3	1SAP 280 000 R0001
SM560-S-XC	Safety module - CPU, safety related module up to SIL 3, extreme conditions	1SAP 380 000 R0001
SM560-S-FD-1	Safety module - CPU, safety related module up to SIL 3 with F-Device functionality for 1 PROFIsafe network	1SAP 286 000 R0001
SM560-S-FD-1-XC	Safety module - CPU, safety related module up to SIL 3 with F-Device functionality for 1 PROFIsafe network, extreme conditions	1SAP 386 000 R0001

Type	Description	Part no.
SM560-S-FD-4	Safety module - CPU, safety related module up to SIL 3 with F-Device functionality for up to 4 PROFIsafe networks	1SAP 286 100 R0001
SM560-S-FD-4-XC	Safety module - CPU, safety related module up to SIL 3 with F-Device functionality for up to 4 PROFIsafe networks, extreme conditions	1SAP 386 100 R0001

3.2 Generic safety I/O module behavior

3.2.1 Overview

All safety I/O modules (AI581-S, DI581-S and DX581-S) can be used in a centralized or remote configuration with PROFINET/PROFIsafe (Fig. 3 on page 22). PROFINET devices CI501-PNIO, CI502-PNIO, CI504-PNIO and CI506-PNIO can be used to attach safety I/O modules in remote configurations. Safety I/O modules can be freely mixed with any non-safety I/Os from AC500 and AC500-eCo product families.

NOTICE!
Safety I/O module firmware update can be currently performed only by the qualified personnel in the ABB factory.

3.2.2 Safety I/O module states

Safety I/O module system states can be described using the following two state charts.