Rail

Add value.
Inspire trust.

Report

on the

Certificate

Z10 18 04 83652 007

of the

AC500-S Safety PLC

Applicant

ABB Automation Products GmbH
ACP
Eppelheimer Straße 82
69123 Heidelberg
Deutschland

Report No. AH84732C
Revision 1.6 of 2019-06-07

Test Body

TÜV SÜD Rail GmbH
Rail Automation
Barthstraße 16
D-80339 München

Certification Body

TÜV SÜD Product Service GmbH
Ridlerstraße 65
D-80339 München

Table of Contents page

List of tables

page

List of figures

page

Revision History

Ver.	Status	Date	Author	SW / HW ver.	Changed chapters	Reason of change
1.0	final	2013-02-01	T. Kreten	See Table 2	-	Initial
1.1	final	2013-03-18		See Table 2		Review Comments from ABB Automation Products GmbH Explanation of “-XC”-variant
1.2	final	2015-02-05	Guido Neumann	See Table 2		new wording of programming tool Automation Builder Bugfixes in S-PlugIn
1.3	final	2015-02-11	Gert Effenberger	See Table 2		update of referenced version to Technical report
1.4	final	2016-09-19	Guido Neumann	See Table 2	 new: 5.4 3.2	update of certification number update of address information of TÜV SÜD Rail GmbH incorporation of information on application standards update of referenced documents (editorial)
1.5	final	2018-05-15	Adrian Spalinger	See Table 2	 2.1 2.2 3.2 3.x 5.4	update of certification number addition of F-Devices FD-1 and FD-4, add / update figures addition of F-Devices, added CRCs, added new libraries update of referenced Technical Report update / addition of standards standards shifted to 3.8
1.6	final	2019-06-07	Adrian Spalinger	See Table 2 new FW 2.1.0	2.2 3.2	AVI005: Flash Replacement Layout adjustments

Table 1: Revision history

1 Target of Evaluation (ToE)

ABB Automation Products GmbH requested TÜV SÜD Rail GmbH, department Rail Automation to test and certify the AC500-S Safety PLC. The ToE is a Safety Programmable Logic Controller (in the following named Safety PLC).

A programmable (logic) controller (PLC) is a digitally operating electronic system, designed for use in an industrial environment, which uses a programmable memory for the internal storage of user-oriented instructions for implementing specific functions such as logic, sequencing, timing, counting and arithmetic, to control, through digital or analogue inputs and outputs, various types of machines or processes. Both the Safety PLC and its associated peripherals are designed to be easily integrated into an industrial control system and easily used in all their intended functions.

2 System overview

2.1 Description

The AC500-S Safety PLC system consists of the following units:

Programmable Logic Solvers of the SM560-S Series

1.a) A central logic solver unit named SM560-S (-XC)* which supports F-Host functionality for PROFIsafe communication with safety modules supporting F-Device functionality.

1.b) A central logic solver unit named SM560-S-FD-1 (-XC)* offering the full SM560-S (-XC)* functionality with additional support of up to 32 F-Device instances (limited to communication with 1 F-Host via PROFINET).

1.c) A central logic solver unit named SM560-S-FD-4 (-XC)* offering the full SM560-S (-XC)* functionality with additional support of up to 32 F-Device instances (limited to communication with 4 separate F-Hosts via PROFINET).

Safety I/O Modules

2.) Digital Input Module “DI581-S (-XC)*” with 16 safety single channel inputs (up to SIL 2 or PL d) or 8 dual channel safety inputs (up to SIL 3 or PL e); 8 test pulse output channels

3.) Input/output module “DX581-S (-XC)*” with 8 safety output channels (up to SIL 3 or PL e) and 8 safety single channel inputs (up to SIL 2 or PL d) or 4 safety dual channel inputs (up to SIL 3 or PL e) with 4 test pulse output channels

* (-XC) extreme conditions

4.) Analogue Input Module “AI581-S (-XC)*” with 4 safety single channel current inputs 0...20 mA or 4...20 mA (up to SIL 2 or PL d) or 2 safety dual channel current inputs (up to SIL 3 or PL e)

5.) Mounting unit for I/O Modules “TU582-S(-XC)*”: interference free spring-type terminal unit TU582-S for Safety I/O modules

CoDeSys Safety programming environment

6.) The Safety CPU is programmed and configured via the dual-port RAM using the CoDeSys Safety programming environment, which is a part of the Automation Builder V1.1 (or higher) PC software

The individual components are physically connected using standard Ethernet cables, communicating via the safe fieldbus protocol PROFIsafe according to Figure 1:

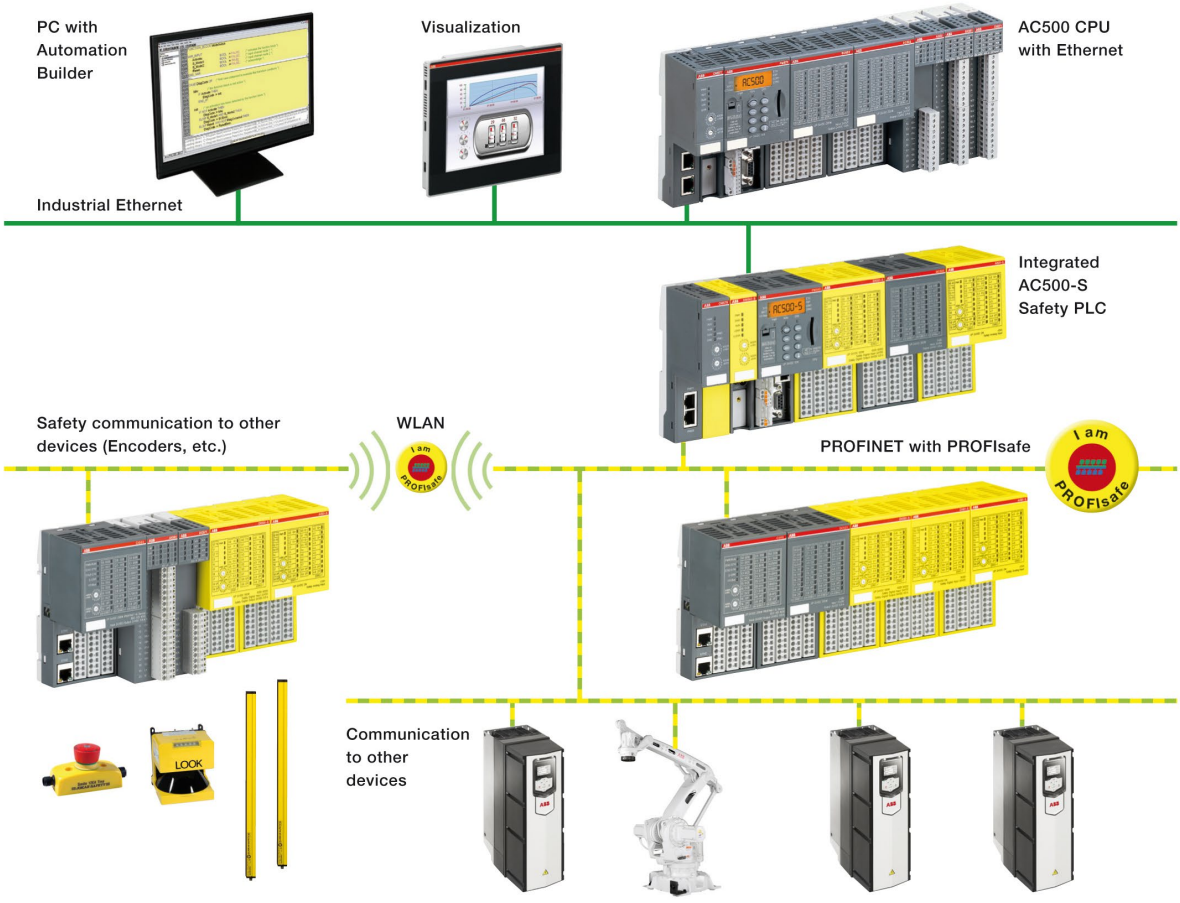

Figure 1: System Architecture

The AC500-S Safety PLC system is built by the combination of the logic solver unit with up to 10 central peripheral safety I/O modules and more than 160 decentralized safety I/O modules attached on the PROFINET bus.

The AC500-S Safety PLC system is closely linked to the non-safety components of the AC500 series PLC as shown in Figure 3. The operation of non-safety PLC and non-safety I/O units is free of interference to the safety functions. The non-safety PLC can monitor the status of the safety PLC via reading data from the dual ported RAM of the SM560-S module, but the non-safety PLC has no ability to manipulate the protection mechanism of the safety data protection (PROFIsafe layer with CRC).

Two new product variants (SM560-S-FD-1(-XC) and SM560-S-FD-4(-XC)) were developed to offer the possibility to interconnect AC500-S Safety PLCs without usage of an external PROFIsafe gateway (as shown exemplary in the Figure 2).

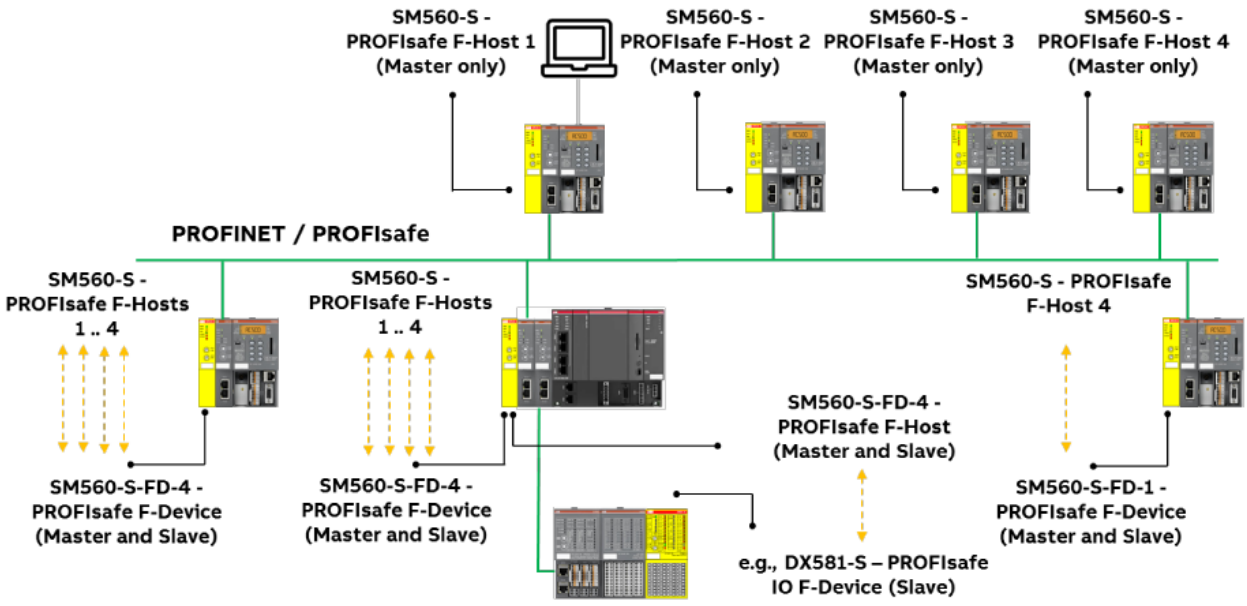

Figure 2: Safe CPU communication between Safety CPUs (SM560-S / -FD1 / -FD4) (Example)

The AC500-S Safety PLC also supports connection of AC31-S safety I/O devices via CS-31 protocol. This is for backward compatibility of the SM560-S module to the older AC31 system. Neither the used safety protocol nor the AC31-S safety I/O modules were subject to this assessment. They were not examined towards compliance to the standards and regulations listed in chapter 3.

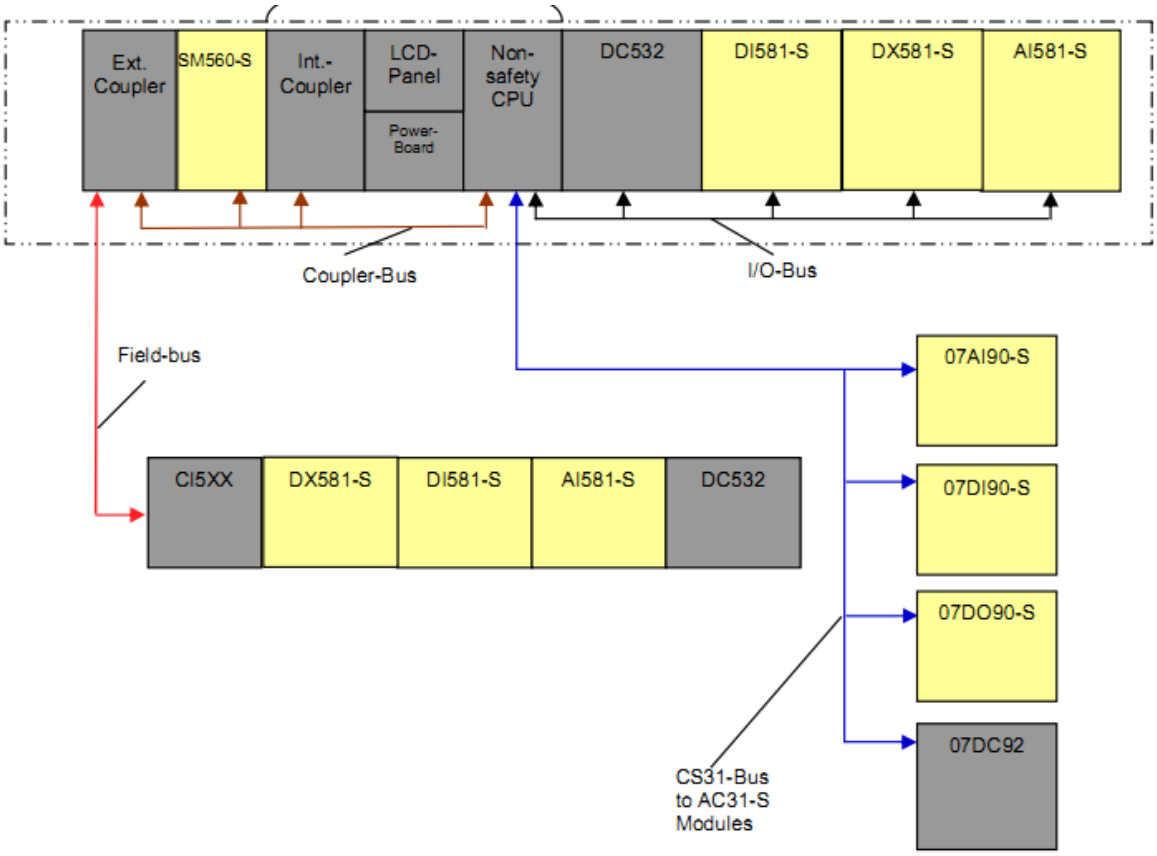

Figure 3: Overview of Safety PLC and non-safety components

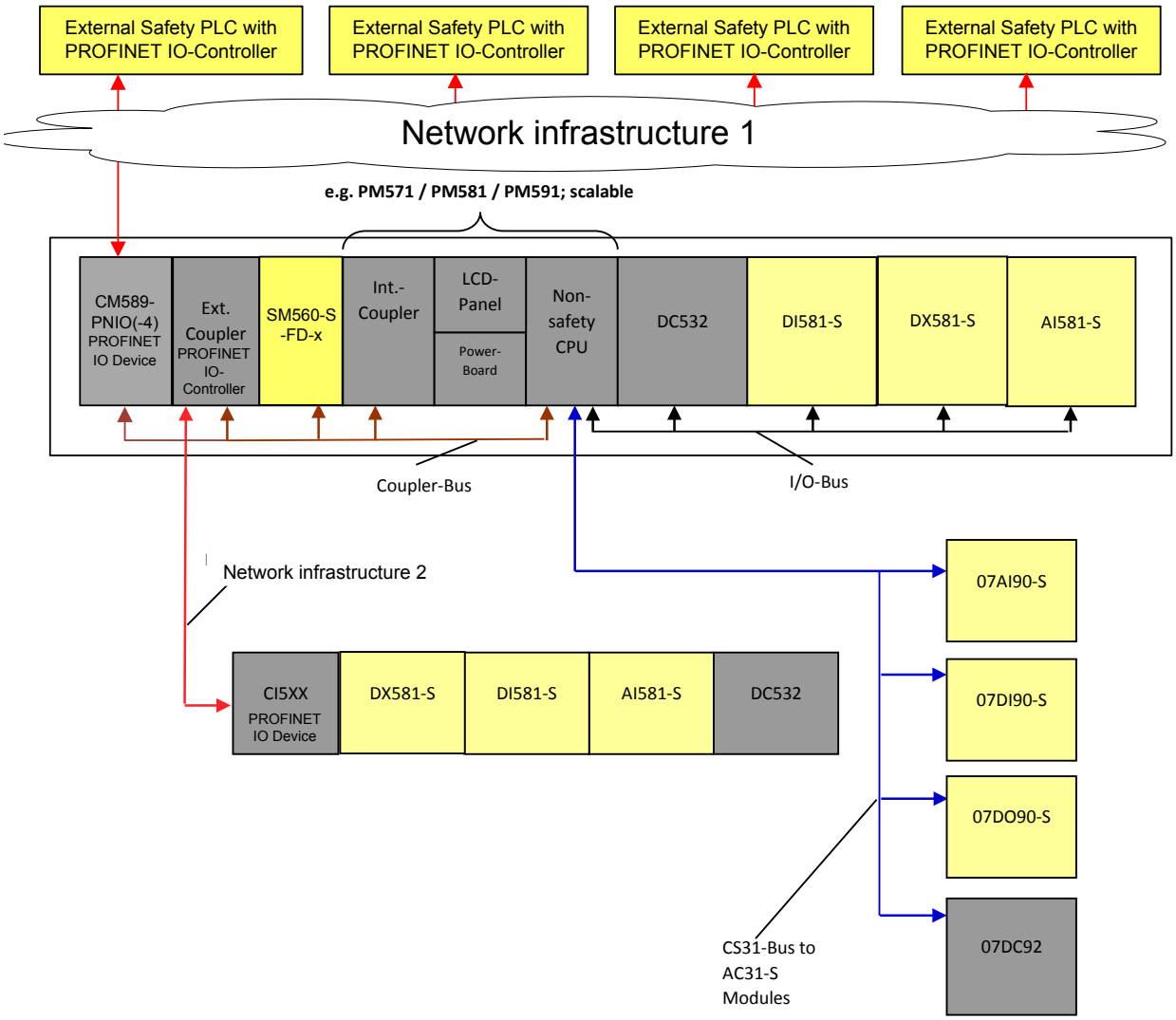

Figure 4: Extended overview of Safety PLC „SM560-S-FD-1/-4“ and non-safety components

2.1.1 Application development tool Automation Builder

The AC500-S safety controller system is programmed and configured with the "Automation Builder" programming tool including the CoDeSys[1] programming tool of the supplier "3S – Smart Software Solutions".

Various tasks are running on the AC500 controller system: One or more non-safety tasks for standard application on standard controller system AC500 and only one task on the safety related controller system AC500-S (module SM560-S) for the safety application. It is guaranteed that standard and safety related tasks are interference free. Communication between standard and safety application is handled via an internal dual ported RAM.

To ensure the safe build process of the safety application, several measures are included in the Programming Tool Automation Builder.

The Development environment is depicted in Figure 5:

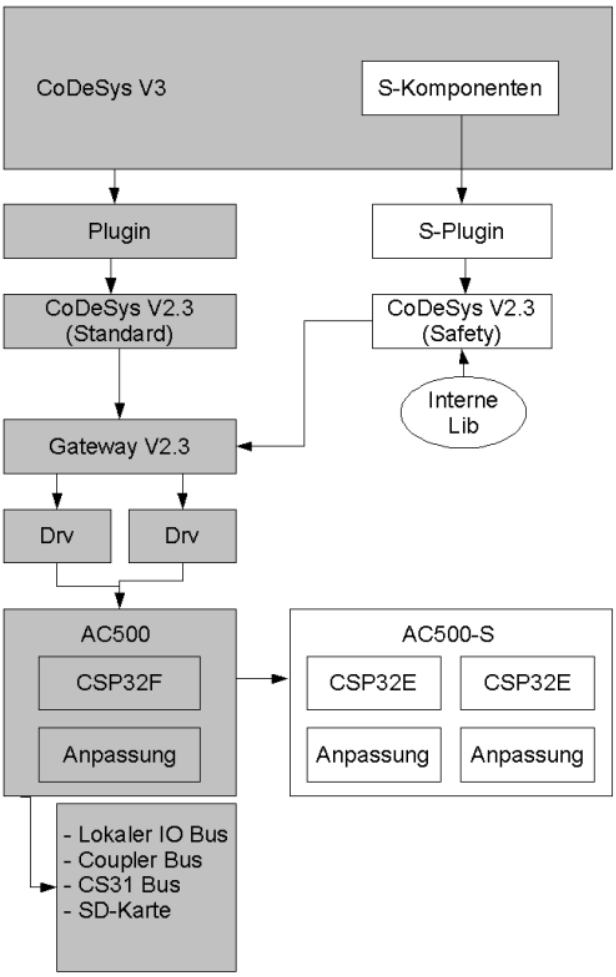

Figure 5: Overview of application development Tool

[1] CoDeSys: Controller Development System by 3S - Smart Software Solutions

2.2 Module Versions

The safety related Hard- and Software is identified by the referenced version lists indicated in Table 2:

Module / Unit	Identification number	Hardware Circuit diagram	Firmware CRC/revision
SM560-S	1SAP280000R0001, SM560-S:AC500, Safety module - CPU	SCHALTPLAN CPU-Platine SM560-S, Index: A1	V2.1.0 CRC Channel A: 0xB181FFAC CRC Channel B: 0x88224E6E Note: The previously released versions V2.0.0 (old flash memory) for SM560-S/SM560-S-FD-1/ SM560-S-FD-4 CRC Channel A: 0x31110FFB CRC Channel B: 0x1121A9EC and V1.0.0 (old flash memory) for SM560-S CRC channel A: 0x70a5a6d3; CRC channel B: 0xb5112750 may be further used if required on safety CPU modules with the old flash memory.
SM560-S-XC	1SAP380000R0001, SM560-S:AC500, Safety module - CPU, Extreme Conditions	SCHALTPLAN CPU-Platine SM560-S XC, Index: A0	See above SM560-S
SM560-S-FD-1	1SAP 286 000 R0001, SM560-S-FD-1: AC500, Safety module - CPU	See above SM560-S	See above SM560-S
SM560-S-FD-1-XC	1SAP 386 000 R0001, SM560-S-FD-1-XC: AC500, Safety module - CPU, Extreme Conditions	See above SM560-S-XC	See above SM560-S
SM560-S-FD-4	1SAP 286 100 R0001, SM560-S-FD-4: AC500, Safety module - CPU	See above SM560-S	See above SM560-S
SM560-S-FD-4-XC	1SAP 386 100 R0001, SM560-S-FD-4-XC: AC500, Safety module - CPU, Extreme Conditions	See above SM560-S-XC	See above SM560-S
DI581-S	1SAP284000R0001, DI581-S:S500,Safety Dig. Input Mod.16SDI	3 Boards SCHALTPLAN Power-Platine, Index: A1 -SCHALTPLAN I/O-Platine 8DI LL 24VDC, Index: A0 -SCHALTPLAN I/O-Platine 8DI LR 24VDC, Index: A0	V3.0.13 Channel A: 0x3FC831C1 Channel B: 0x3FC831C1

Module / Unit	Identification number	Hardware Circuit diagram	Firmware CRC/revision
DI581-S-XC	1SAP484000R0001, DI581-S:S500,Safety Dig. Input Mod.16SDI, Extreme Conditions	3 Boards -SCHALTPLAN Power-Platine XC, Index: A0 -SCHALTPLAN I/O-Platine 8DI LL 24VDC XC, Index: A0 -SCHALTPLAN I/O-Platine 8DI LR 24VDC XC, Index: A0	See above DI581-S
DX581-S	1SAP284100R0001, DX581-S:S500,Safety Dig.I/O Mod.8SDI/SDO	3 Boards -SCHALTPLAN Power-Platine, Index: A1 -SCHALTPLAN I/O-Platine 4DI/4DO LL 24VDC, Index: A1 -SCHALTPLAN I/O-Platine 4DI/4DO LR 24VDC, Index: A1	V3.0.13 Channel A: 0xF37E8483 Channel B: 0xF37E8483
DX581-S-XC	1SAP484100R0001, DX581-S:S500,Safety Dig.I/O Mod.8SDI/SDO, Extreme Conditions	3 Boards -SCHALTPLAN Power-Platine XC, Index: A0 -SCHALTPLAN I/O-Platine 4DI/4DO LL 24VDC XC, Index: A0 -SCHALTPLAN I/O-Platine 4DI/4DO LR 24VDC XC, Index: A0	See above DX581-S
AI581-S	1SAP282000R0001, AI581-S:S500,Safety Anal. Input Mod.4SAI	3 Boards -SCHALTPLAN Power-Platine, Index: A1 -SCHALTPLAN I/O-Platine 2AI LL 24VDC, Index: A0 -SCHALTPLAN I/O-Platine 2AI LR 24VDC, Index A0	V3.0.13 Channel A: 0x072CD806 Channel B: 0x072CD806
AI581-S-XC	1SAP482000R0001, AI581-S:S500,Safety Anal. Input Mod.4SAI, Extreme Conditions	3 Boards -SCHALTPLAN Power-Platine XC, Index: A0 -SCHALTPLAN I/O-Platine 2AI LL 24VDC XC, Index: A0 -SCHALTPLAN I/O-Platine 2AI LR 24VDC XC, Index A0	See above AI581-S
TU582-S	1SAP281200R0001, TU582-S:S500,Safety I/O Term. Unit,24VDC	- SCHALTPLAN T-Mod.I/O 1/2w spring 24VDC, Index: A0	n/a
TU582-S-XC	1SAP481200R0001, TU582-S:S500,Safety I/O Term. Unit,24VDC, Extreme Conditions	- SCHALTP. T-Mod.I/O 1/2w spring 24VDC XC, Index: A0	

Module / Unit	Identification number	Hardware Circuit diagram	Firmware CRC/revision
CoDeSys Safety programming environment	Automation Builder 2.1	n/a	part of Automation Builder (or higher) PC software
			SafetyBase_PROFIsafe _LV200_AC500_V22.lib Library CRC: 1d881052 Note: Older library versions listed below are not for use in new customer projects, but can be further used in old projects for maintenance reasons: - SafetyBase_PROFIsafe_AC500_ V22_Ext.lib, Version 1.0.1, Library-CRC: f34d9a48; - SafetyBase_PROFIsafe_AC500_ V22. lib, Version 1.0.0, Library-CRC: 7f64e267, license activation with PS501-S License Enabling Package; - SafetyBase_PROFIsafe_AC500_ V22. lib, Version 1.0.0, Library-CRC: c688eb23, special OEM version of PROFIsafe library.
			Safety_Standard.lib, Library-CRC: fd5d3581
			SafetyExt_AC500_V22.lib, Library-CRC: 72a88162
			SafetyExt2_LV100_AC500 _V27.lib Library-CRC: f3eb2fbc Note: for SM560-S FW V2.0.0 (or newer) only
			SafetyDeviceExt_LV100 _PROFIsafe_AC500_V27.lib Library-CRC: 2eadeae9 Note: for SM560-S FW V2.0.0 (or newer) only
			SafetyUtil_CoDeSys_AC500_V22 .lib Library-CRC: 6b29c54
			Safety_SysLibTime.lib Library-CRC: 672b8325
			SysLibCallback.lib Library-CRC: 6b29c54 or 62ad210d

Module / Unit	Identification number	Hardware Circuit diagram	Firmware CRC/revision
			Target_AC500_V22.lib Library-CRC: 8daa436
			Safety-Blocks_PLCopen_AC500_v22.lib, Library-CRC: b6e0bc60
			SafetyCS31_AC500_V22.lib, Library-CRC: b66081df
			CoDeSys V2.3.x Safety
			SPT, V1.0
			S-PlugIn, V2.1.x.x[2]
			AC500-S Safety Code Analysis (SCA) v1.0.x Software Tool for verification of safety-relevant Software (developed using CoDeSys V2.3) up to SIL 3 according to IEC 61508:2010

Table 2: Identification of the safety relevant system components of AC500-S

[2] The S-PlugIn was maintained according to the Jira tickets. The major/minor version was not affected with this change the version is identified by V2.1.23.20700

3 Certification Requirements

3.1 Basis of Certification

The certification of the AC500-S Safety PLC will be according to the regulations and standards listed in clause 3.3 to 3.8 of this document. This will certify the successful completion of the following test segments:

I. Functional safety
   - Analysis of the system structure (FMEA system)
   - Analysis of the hardware (FMEA component, quantitative analysis)
   - Analysis of the software
   - Fault simulations and software tests
   - Test of the fault prevention measures
   - Functional test

II. Electrical safety

III. Susceptibility to environmental errors
   - Climate and temperature
   - Mechanical effects

IV. Electromagnetic compatibility

V. Safety information in the product documentation (safety manual, operating instructions)

VI. Product-related Quality Management in manufacturing and product care.

Certification is dependent on successful completion of all above listed test segments. The testing follows the basic certification scheme for Safety Components of TÜV SÜD Rail GmbH.

3.2 Certification Documentation

- Technical Report by TÜV SÜD Rail GmbH
  Report No. AH84732T Rev. 2.0 of 2019-06-06
- User Manual by ABB Automation Products GmbH and reviewed by TÜV SÜD Rail GmbH.

Based on the specified purpose of use of the AC500-S Safety PLC in safety critical process applications, the certification is based on the following set of standards. The issuance of the certificate states compliance with these references unless specifically noted otherwise.

3.3 European guidelines and national laws and regulations

2006/42/EC	European Directive on Safety of Machinery Council Directive of 17 May 2006 on the harmonisation of the laws of the Member States relating to machinery

Table 3: Directives and regulations

As a supplement to and to lend greater precision to legal requirements as well as the EC directives named "Basic Health and Safety Requirements", the test was performed based on the following additional standards and technical rules.

3.4 Product Standard

EN 61131-2:2007	Programmable controllers – Part 2: Equipment requirements and tests
PLCopen Specification	PLCopen_TC5_Safety_V10

Table 4: Product Standard

3.5 Functional Safety

The testing for functional safety is to be performed using the following standards and guidelines:

IEC 61508/ EN 61508: 2010 part 1 –4 (SIL 3)	Functional safety of electrical/electronic/programmable electronic safety-related systems
EN ISO 13849-1/ ISO 13849-1: 2015 (PL e, Cat. 4)	Safety of machinery — Safety-related parts of control systems — Part 1: General principles for design
IEC 62061/ EN 62061: 2005/A2:2015 (SILCL 3)	Safety of machinery – Functional safety of safety-related electrical, electronic and programmable electronic control systems
EN 61784-3:2010 Corrigenda 1: 2006 Corrigenda 2: 2009	Industrial communication networks – Profiles – Part 3: Functional safety fieldbuses – General rules and profile definitions
IEC 61511-1: 2016 EN 61511-1: 2017	Functional safety – Safety instrumented systems for the process industry sector – Part 1: Framework, definitions, system, hardware and software requirements
IEC 61131-6:2012	Programmable controllers – Part 6: Functional safety

Table 5: Functional Safety

3.6 Basic Safety and Environmental Safety

To complete and to specify the technical requirements resulting from the essential requirements of the directives listed above the testing of Basic Safety is to cover the following standards:

EN 61131-2:2007	Programmable controllers – Part 2: Equipment requirements and tests

Table 6: Basic and Environmental safety

3.7 Electromagnetic Compatibility

To complete and to specify the technical requirements resulting from the essential requirements of the directives listed above, the testing of Electromagnetic Compatibility is to cover the following standards:

EN 61131-2:2007	Programmable controllers – Part 2: Equipment requirements and tests
IEC 61496-1: 2012 (only for EMC related requirements)	Safety of machinery – Electro-sensitive protective equipment
IEC 61326-3-1: 2017	Electrical equipment for measurement, control and laboratory use – EMC requirements – Part 3-1: Immunity requirements for safety-related systems and for equipment intended to perform safety-related functions (functional safety) – General industrial applications

Table 7: Electromagnetic compatibility

3.8 Application Standards

EN 12622: 2013	Machine tools – Safety of machine tools – Hydraulic press brakes
EN 692: 2005/A1:2009	Machine tools – Mechanical presses – Safety
EN 693: 2001/A1:2011	Machine tools – Safety – Hydraulic presses
IEC 60204-1: 2016 (EN 60204-1: 2006/AC:2010)	Safety of machinery – Electrical equipment of machines – Part 1: General requirements
IEC 61496-1: 2012	Safety of machinery – Electro-sensitive protective equipment
NFPA 79: 2015	NFPA 79 - Electrical Standard for Industrial Machinery
UL 1998: 2013	Standard for Safety-Related Software
IEC 61131-6:2012	Programmable controllers – Part 6: Functional safety
IEC 61511-1: 2016 EN 61511-1: 2017	Functional safety – Safety instrumented systems for the process industry sector – Part 1: Framework, definitions, system, hardware and software requirements

Table 8: Application Standards

4 Results

4.1 Functional Safety

The tests performed and quality assurance measures implemented by the manufacturer have shown that the AC500-S Safety PLC complies with the testing criteria specified in clause 3 subject to the conditions defined in clause 5 and its subsections, and is suitable for safety-related use in applications up to SIL 3 in accordance with EN/IEC 61508, SILCL 3 according to IEC 62061 and PL e, Cat. 4 according to ISO 13849-1.

4.1.1 Fault Reaction and Timing

Fault detection in the AC500-S Safety PLC is assured by means of following basic techniques:

- Self-test at power up and during operation
- two channel control logic with cross check
- redundancy
- dynamic signals
- de-energizing in case of over- and under-voltage
- de-energizing by watch dog monitoring

4.1.2 Evaluation of fault prevention measures

For the avoidance of failures the following techniques and measures were used:

- Project management
- Documentation
- Structured specification
- Inspection of the specification or walk-through of the specification
- Observance of relevant guidelines and standards
- Structured design
- Modularization
- Use of well tried components
- Inspection of the hardware
- Functional testing (also under environmental conditions)
- Operational and maintenance instructions
- User- and maintenance friendliness

The individual measures for the avoidance of failures provide the required degree of effectiveness and are specified in the relevant documents.

4.1.3 Analysis of the hardware safety integrity and hardware fault simulations (FIT)

The Failure Mode Effect and Diagnostic Analysis (FMEDA) showed that the occurrence of a single fault does not lead to loss of the safe functioning. The individual architectural constrains are sufficient and their corresponding degree of fault detection provide the required degree of effectiveness.

4.2 Basic Safety and Electromagnetic Compatibility

4.2.1 Electrical Safety

The results about the electrical safety are documented by the certificates and test reports of an accredited test centre. The documentation of the tests has been reviewed for completeness.
These certificates show that the standards specified in clause 3 are covered.

4.2.2 Environmental Testing

The environmental stress tests are documented by the certificates of an accredited test centre.
The above mentioned certificates and tests and the quality assurance measures implemented by the manufacturer have shown that the AC500-S Safety PLC complies with the testing criteria specified in clause 3 subject to the conditions defined in clause 5 and its subsections.

4.2.3 Electromagnetic Compatibility

The tests of the electromagnetic compatibility are documented by the certificates and test reports of an accredited test centre. The documentation of the tests has been reviewed for completeness.
These certificates show that the standards specified in clause 3 are covered.

4.3 Product Specific Quality Assurance and Control

The software and hardware components developed and manufactured in course of the safety evaluation are governed by an ISO 9001 certified quality assurance and control system.
As part of the certification process TÜV Product Service also performs a procedure that is tailored to the assessed product in order to assess the consistency of product quality while accounting for product modifications and their identifiability (follow-up service).

5 Implementation Conditions and Restrictions

The use of the AC500-S Safety PLC shall comply with the current version of the safety parts of the user manual, and the following implementation and installation requirements have to be followed if the AC500-S Safety PLC is used in safety-related installations.

5.1 General Application Conditions

- The guidelines specified in the instruction manuals shall be followed.
- Only modules certified for safety-related operation shall be used for safety-critical functions.
- The fault tolerance period of the process controlled by the system shall be greater than the worst-case response time of the system.
- The AC500-S Safety PLC can be used in applications up to PL e, Cat. 4 according to ISO 13849-1.
- The AC500-S Safety PLC can be used in applications up to SIL 3 according to EN/IEC 61508 and SILCL 3 according to IEC 62061.
- The power supply has to fulfil the requirements of SELV according to EN 61140.
- The AC500-S Safety PLC has to be placed within a cabinet with at least IP54.
- The AC500-S Safety PLC also supports connection of safety I/O devices via CS-31 protocol. This is for compatibility of the SM560 module to the older AC31 system. Neither the used safety protocol nor the AC31 I/O modules were subject to this assessment. They were not examined towards compliance to the standards and regulations listed in chapter 3.

5.2 General Commissioning Conditions

- The guidelines and the instructions for commissioning, described in the instruction manual, have to be followed.

5.3 General Run-time Conditions

- The operating conditions as specified in the instruction manuals shall be met.
- The procedures of modification of safety related data and components described in the user manual have to be followed.
- The maintenance and repair instructions described in the instruction manual of the AC500-S Safety PLC have to be followed.

5.4 Compliance to Application Standards

AC500-S confirms to the applicable parts of the standards mentioned in chapter 3.8, Table 8. The implementation conditions and restrictions mentioned in chapter 5.1, 5.2 and 5.3 have to be applied.

The following additional conditions of use apply with respect to the standards mentioned in Table 8:

1.) NFPA79:
   a. No application for battery operated vehicles without additional measures for undervoltage handling.
   b. Chapter 4.4.6 “Contaminants” fulfilled only by using –XC modules of AC500-S.

2.) EN 61496-1
   a. Chapter 4.2.1 “Electrical supply: DC supplies from batteries” without additional measures for undervoltage handling.
      The system is not suitable for use in battery-operated vehicles.
   b. Chapter 4.3.2.2 “Supply voltage interruptions” are tested in accordance to IEC 61131-2.

6 Certificate Number

This report specifies technical details and implementation conditions required for the application of AC500-S Safety PLC to the certificate:

Z10 18 04 83652 007

Munich, 2019-06-07

TÜV SÜD Rail GmbH
Rail Automation


Digital unterschrieben von Christian Dirmeier
Datum: 2019.06.07 15:25:14 +02'00'

Christian Dirmeier
(Technical Certifier as on certificate)