

Safety Manual

Safety Analog Input Module HART (S-AIMH)

- > 9462/12-06-11
- > 9462/12-08-11



1 Contents

1	Contents	2
2	General Information	2
3	General Safety Information	4
4	Characteristics for the Functional Safety	5
5	Installation	6
6	Diagnostic Data	7
7	Parametrization	9
8	Commissioning	10
9	Operation	10
10	Proof Test	10
11	Repair work	11
12	Release notes	11

2 General Information

2.1 Manufacturer

R. STAHL Schaltgeräte GmbH
 Am Bahnhof 30
 D-74638 Waldenburg


Phone: +49 7942 943-0
 Fax: +49 7942 943-4333
 Internet: www.stahl.de

2.2 Information regarding the Safety Manual

ID-No.: 168027 / 946260310050
 Publication Code: 2010-04-28·SM00·III·en·01

Additionally to the Safety Manual the following documents must be observed:

- X Operating Instructions for the IS1 system
- X Operating Instructions for the S-AIMH 9462/12 (946260310020)
- X PROFIBUS - Installation Guideline for Commissioning, Order No: 8.032
- X PROFIBUS - Installation Guideline for Cabling and Assembly, Order No: 8.022
- X PROFIsafe - Environmental Requirements, Order No: 2.232

	The documents PROFIBUS - Installation Guideline for Commissioning, PROFIBUS - Installation Guideline for Cabling and Assembly and PROFIsafe - Environmental Requirements are available at www.profibus.org .
---	--

We reserve the right to make technical changes without notice.

2.3 Area of application

This Safety Manual applies to the Safety Analog Input Module HART (S-AIMH), Type 9462/12-0.-11.

Hardware version: Rev. A
Software version: V02-03
IS1 GSD file: 3.02

The S-AIMH enables the connection of explosion protected analog circuits with requirements according to IEC 61508 up to SIL 2 onto the IS1 remote I/O system. The S-AIMH 9462/12-06-11 provides 6 inputs for two wire 4-20 mA transmitters. The S-AIMH 9462/12-08-11 provides 8 inputs for two wire 4-20 mA transmitters. The safety function of the S-AIMH modules can be used for example in safety process shut-down applications in e.g. oil, gas or chemical industries. The modules are suitable for low demand mode of operation (worst case internal fault detection time is 35 minutes).





2.4 Terms and Definitions

DC _S	Diagnostic Coverage of safe failures ($DC_S = \lambda_{sd} / (\lambda_{sd} + \lambda_{su})$)
DC _D	Diagnostic Coverage of dangerous failures ($DC_D = \lambda_{sd} / (\lambda_{dd} + \lambda_{du})$)
FIT	Failure In Time (1x10 ⁻⁹ failures per hour)
FMEDA	Failure Mode Effect and Diagnostic Analysis
HART	Highway Addressable Remote Transducer
HFT	Hardware Fault Tolerance
low demand mode	Mode, where the frequency of demands for operation made on a safety-related system is not greater than twice the proof test frequency.
MTBF	Mean Time between Failures
MTTR	Mean Time To Repair
PFD	Probability of Failure on Demand
PVD _{AVG}	Average Probability of Failure on Demand
SIL	Safety Integrity Level
SFF	Safe Failure Fraction
T[proof]	Proof Test Intervall
XooY	X out of Y redundancy

2.5 Conformity to Standards

- X IEC 61508:
“Functional safety of electrical/electronic/programmable electronic safety-related systems“
- X IEC 61511:
“Functional safety - Safety instrumented systems for the process industry sector “
- X IEC 61326-1:
“Electrical equipment for measurement, control and laboratory use - EMC requirements - Part 1: General requirements“
- X IEC 61326-3-2:
“Electrical equipment for measurement, control and laboratory use - EMC requirements - Part 3-2: Immunity requirements for equipment performing or intended to perform safety related function (functional safety) - Industrial applications with particular EM environment.“
- X NAMUR NE 21




2.6 Symbols used

	A call to take action: Describes the actions which the user should undertake.
	Reaction sign: Describes the results or the reactions to the actions taken.
	Checklist sign
	Commentary sign: Describes the notes and recommendations.




3 General Safety Information

3.1 Safety Instructions for Assembly and Operating Personnel


The Safety Manual contains basic safety instructions which are to be observed during installation, operation, parametrization and maintenance. Non-observance can lead to persons, plant and the environment being endangered.

 WARNING	
Risk due to unauthorised work being performed on the device!	
	There is a risk of injury and damage to equipment.
	Mounting, installation, commissioning and servicing work must only be performed by personnel who are both authorised and suitably trained for this purpose.




When installing the device:

-  Observe the PROFIBUS - Installation Guideline for Cabling and Assembly, Order No: 8.022.
-  Observe the Operating Instructions for the IS1 system.
-  Observe the Operating Instructions for the S-AIMH 9462/12.


Before Commissioning:

-  Ensure, that the module address and the adjusted F-destination address conforms to system configuration and parameterization in the F-Host.


When operating the device:

-  Ensure, that the HART protocol is only used for setup, calibration and diagnostic purposes, not for safety critical operation.
-  Ensure, that the mean time to restoration (MTTR) after a safe failure is < 8 hours.
-  Feed the PROFIsafe output signal to a SIL 2 compliant PROFIsafe input board of a safety PLC.


If you have questions:


-  Contact the manufacturer.

4 Characteristics for the Functional Safety

	Confirmation of meeting the requirements of IEC 61508 is done by an assesment report of EXIDA (Report No.: Stahl 05/08-05 R011, V0, R1). The failure rate of the module is calculated by a FMEDA. The failure rate of the components are taken from Siemens standard SN29500 at a mean temperature of 40 °C and a MTTR of 8 hours.
---	--

4.1 Functional Safety Data

	For the calculation of the Safe Failure Fraction (SFF) the following has to be noted: $\lambda_{total} = \lambda_{safe} + \lambda_{dangerous} + \lambda_{residual} + \lambda_{annunciation}$ $SFF = 1 - \lambda_{DU} / \lambda_{total}$
---	---

	The S-AIMH with PROFIsafe output is considered to be a Type B subsystem with a hardware fault tolerance of 0. For Type B subsystems with a hardware fault tolerance of 0 the SFF shall be > 90% for SIL 2 subsystems according to IEC 61508-2, table 3.
---	---

T _{Proof} = 1 year	T _{Proof} = 5 years	T _{Proof} = 10 years	SFF
PFD _{AVG} = 5.45E-05	PFD _{AVG} = 1.09E-04	PFD _{AVG} = 2.72E-04	98 %

It is the responsibility of the Safety Instrumented Function designer to do calculations for the entire Safety Instrumented Function (SIF).

For SIL 2 applications the sum of the PFD_{AVG} values of all devices of a Safety Instrumented Function (SIF) needs to be $\geq 1.00E-4$ and $< 1.00E-03$.

4.2 Technical Data

Usefull Lifetime	10 years
Hardware structure	1001D
MTTR	8 hours
Ambient temperature	-20 °C ... +65 °C (For a higher average temperature of 60 °C, the failure rates should be multiplied with an experience based factor of 2.5. A similar multiplier should be used if frequent temperature fluctuation (daily fluctuation of > 15 °C) must be assumed.
Storage temperature	-40 °C ... + 70 °C
Transport temperature	-40 °C ... + 70 °C

5 Installation

⚠ WARNING

Danger due to improper Installation

- ▶ Install the device according to the Installation Guidelines of the PNO and the Operating Instructions of the device.
- ▶ For safe communication use only PROFIsafe masters (F-hosts) which are compatible to the PNO PROFIsafe Specification (V1 or V2 Mode).



The line break detection leads to a line break message for all not used inputs. Therefore resistors ($4K7 \pm 1 \text{ k}\Omega$, $\geq 0,6 \text{ W}$) must be connected to all open inputs.

5.1 System Requirements

CPM	9440/15-01-11, from Revision F 9440/22-01-11, all Revisions 9440/15-01-21, all Revisions
CPM Firmware	from version 02-40 (DPV1)
GSD file	from version V3.02
F-host	PROFIBUS class 1 master according to PROFIsafe specification PROFIsafe Mode V1 or V2
I/O-modules	IOM Firmware from Revision 2.00 for all none PROFIsafe modules

Systembehavior if newer and older Versions are used together:

The usage of GSD V3.xx with older CPM Firmware Revisions is not permitted! While the start up procedure of the DP slave the device specific diagnostics will respond with 'parameter error' in the 6 Byte standard DP diagnosis telegram. The following diagnosis informations are according DPV0 and do not fit to GSD V3.xx.

5.2 Engineering rules

The maximum number of modules is restricted by the length of configuration data. The length of the configuration data depends on the type of the used I/O-modules.

The maximum length of configuration data is 122 Byte.

Module type	Length config data (Byte)	Format
CPM	1	General Identification Format (GIF)
Standard IOM without DIM16+CF	4	Special Identification Format (SIF)
DIM16+CF	5	Special Identification Format (SIF)
All IOM without SIL in GIF	1	General Identification Format (GIF)
S-AIMH 9462/12-06-11	11	Extended Special Ident. Format (ESIF)
S-AIMH 9462/12-08-11	13	Extended Special Ident. Format (ESIF)

Example: If the IS1 System is assembled only with S-AIMH Type 9462, the following maximum module numbers are possible:

S-AIMH	maximal number per IS1 fieldstation
9462/12-06-11	11 (max. 8 using Zone 1 CPM)
9462/12-08-11	9 (max. 8 using Zone 1 CPM)

6 Diagnostic Data

The basic behavior of S-AIMH Modules corresponds to standard IS1 IO-Modules. For safety relevant diagnose there are following extensions:

6.1 PROFIsafe specific extension of signal diagnosis

Diagnostic informations of the PROFIsafe stack of the S-AIMH are reported according PROFIsafe spec. within channel specific diagnostic part of PROFIBUS DP with reserved "ChannelErrorType" numbers.

Hex	Number	Diagnosis Information
0x40	64	Mismatch of safety destination address (F_Dest_Add)
0x41	65	Safety destination address not valid (F_Dest_Add)
0x42	66	Safety source address not valid (F_Source_Add)
0x43	67	Safety watchdog time value is 0 ms (F_WD_Time)
0x44	68	Parameter "F_SIL" exceeds SIL from specific device application
0x45	69	Parameter "F_CRC_Length" does not match the generated values
0x46	70	Version of F-Parameter set incorrect
0x47	71	CRC1-Fault

6.2 Error detection

The following values have to be used for error detection by the F-host:

Range	Units		%	Range	Alarm / Diagnoses
	decimal	Hex			
4 - 20 mA					
> 22.814 mA	*1)	*1)			Short circuit
22.814 mA	32511	7EFF	117.6 %	Over range	-
20 mA	27648	6C00	100 %	Nominal range	-
12 mA	13824	3600	50 %		
4 mA	0	0000	0 %		
3.999 mA	-1	FFFF		Under range	-
2.4 mA	-2765	F533	-10 %		
< 2.4 mA	*1)	*1)			Line break

*1) Transmitted value in case of error:

Behaviour in case of error	Type of error	Value transmitted if an error occurs	
Alarm code General rule to generate status information in AS for all AI signals	Short circuit	32767	7FFF
	Open circuit	-32762	8006
	HW error	-32751	8011
	Overtemperature	-32750	8012
Signal is disturbed if value ≥ 32512 or value ≤ 32512		-32731	8025

6.3 Indications

The following combinations of LED and LCD Indications are possible:

LED green	LED red	Text in LCD Display	IOM status	Error source	Possible actions (solutions)
On	Off	RUN 0-----7	All signals of the F-module are OK. The IOM is in safety operation	none	-
On	flashes	RUN 0xxxxxxx7	Signal diagnosis. Data Exchange with DP- and PROFISafe master is OK.	Signal(s) x inoperative -Short circuit -Line break -HW error	Rectify source of signal diagnosis HW error: exchange module
	On	F-para.Fail yy *)	No safety operation. Data Exchange with DP Master is OK. Signals in safe position	Error in F-Parameter	Check F-Parameter in F-Host
		Wait op-ackn.		No user acknowledge after error correction or system startup	OA_C (Operator Acknowledge Command) on F Channel Host Driver required.
		Stop 0xxxxxxx7		Error in PROFISafe operation (Watchdog)	Check F-Host operation Check timeout settings
flashes	Off	Wait for Cfg/Prm	Ready (after switch on, before data exchange with master) Module is OK Outputs are in a powerless condition (the AOM HART 9466 outputs 4 mA) .	No Data Exchange with DP master!	Initiate cyclical data exchange with the master. Check master, bus connection and CPM.
	flashes	Stop1 7xxxxxxx0	Data exchange is left (output signals in safe position)	Cyclical data exchange with master is interrupted (DP or internal communication) Clear data command	Initiate cyclical data exchange with the master. Check master, bus connection and CPM.
	On	Config Fail	Configuration fault	Configuration incorrect or wrong module	Change configuration in master or plug right module type
Off	On or flashes	Device_Fault yy *)	IOM hardware error	- Hardware-Check error - EPROM error - EEPROM error	Document error code and change module. Return module to R.STAHL.
	Off	-	Off	No supply voltage to IOM or defective IOM	check CPM power supply check CPM check Bus Rail engage I/O module correctly on the rail exchange I/O module


*) error codes „yy“:

Display priority	message	code xx	Diagnosis Information
1	Device fault	01-99	Replace Module
3	F-para. fail	01	Safety destination address not valid (F_Dest_Add)
4	F-para. fail	02	Mismatch of safety destination address (F_Dest_Add)
5	F-para. fail	03	Safety source address not valid (F_Source_Add)
6	F-para. fail	04	Safety watchdog time value is 0 ms (F_WD_Time)
7	F-para. fail	05	Parameter "F_SIL" exceeds SIL from specific device application
8	F-para. fail	06	Parameter "F_CRC_Length" does not match the generated values
9	F-para. fail	07	Version of F-Parameter set incorrect
10	F-para. fail	08	CRC1-Fault

7 Parametrization

7.1 I-Parameters (Functional Parameters)

The S-AIMH has no individual parameters (I-parameter) and has no functionality, which can be changed via parameters.

	The line break detection leads to a line break message for all not used inputs. Therefore resistors ($4K7 \pm 1 \text{ k}\Omega$, $\geq 0,6 \text{ W}$) must be connected to all open inputs.
---	--

7.2 F-Parameters (PROFIsafe Parameters)

The PROFIsafe F-parameters of the S-AIMH module must be set in the configuration software of the F-host using the IS1 GSD file.

F-parameters of the S-AIMH:

Byte No.	Parameter	area / selection	settings in IS1 GSD			
			fix	default	visible	
0	DPV1-Header	Block length F-parameters	0x0E	-	N	
1	DPV1-Header		0x05	-	N	
2	DPV1-Header	slot F-module	0x00	-	N	
3	DPV1-Header	reserved	0x00	-	N	
4	F_Prm_Flag 1	F_Check_SeqNr	No Check (0)	(0x0)	N	
		F_Check_iPar	No Check (0)	(0x0)	N	
		F_SIL	SIL 1, SIL 2, SIL 3, NoSIL	SIL 2 (0x01)	-	Y
		F_CRC_Length	2 Byte, 3 Byte, 4 Byte	4 Byte (0x02) *1	-	Y
		F_Check_IO_Structure	No Check (0)	(0x0)	-	N
		reserved		(0x0)	-	N
5	F_Prm_Flag 2	reserved		(0x0)	N	
		F_Block_ID		(0x00)	N	
		F_Par_Version	V1 (0x0), V2 (0x1)	V1 (0x00) or V2 (0x01)	-	Y
6, 7		F_Source_Add	1 ... 65534		1	Y
8, 9		F_Dest_Add	1 ... 65534		1	Y
10, 11		F_WD_Time	0 ... 65535 (* 1 ms)		1000	Y
12, 13	CRC1	F_Par_CRC	0 ... 65535	calculated	-	N

*1: CRC Length is different depending on signal number and PROFIsafe mode of S-AIMH:

Byte 4 (F_Prm_Flag 1):

Mode	Byte 4	CRC
8 AI V1	0010 0100	0x24 4 Byte
8 AI V2	0010 0100	0x24 4 Byte
6 AI V1	0000 0100	0x04 2 Byte
6 AI V2	0001 0100	0x14 3 Byte

7.3 Adjustment of F-Destination Address

- ▶ Press the <up> and the <down> button simultaneously while the module is in non cyclic operation.
- ▷ The Display Level changes to Adjustment Level.
- ▶ Increment or decrement the address by pressing the <up> or the <down> button.
- ▶ Press the <up> and the <down> button simultaneously.
- ▷ A verification question has to be answered.
- ▶ Select „Yes“ and set the adjusted address by pressing the <up> or the <down> button simultaneously.

7.4 HART support

WARNING

Danger due to change of safety relevant functions of the field device

Safety relevant changes of functions of the field device by HART commands (e.g. scale of signal) are not examined or prevented by the S-AIMH.

The operator is responsible to preserve the save function of the HART field devices, for example by locking the parameters on the field device in touch with organizationally measures.

The integrated HART Multiplexer offers acyclic, bidirectional HART communication.

The S-AIMH is fully transparent for HART commands.



The HART functionality is not part of functional safety functions.
The HART variables PV1, PV2, PV3 and PV4 are not transportet in the cyclic communication of DP.

8 Commissioning

Before Commissioning:

- ▶ Ensure that the device is undamaged.
- ▶ Ensure, that the module address and the adjusted F-destination address conforms to system configuration and parameterization in the F-Host.

9 Operation

WARNING

Danger due to errors or malfunctions

If errors or malfunctions were recognized during the operation, the system has to be set out of service immediately and the safety of the process has to be keep ahead by other measures.

Errors or malfunctions within the IS1 Remote I/O System shall be reported to the manufacturer R. STAHL.

10 Proof Test

WARNING


Routine proof tests are mandatory to keep alive the functional safety of the system. They are required to detect failures, which are not detectable in safe operation of the system. The time interval has to be choosen in accordance with the wanted PFD_{AVG} - Level.

WARNING

Danger due to errors or malfunctions

If errors or malfunctions were recognized during the test, the system has to be set out of service immediately and the safety of the process has to be keep ahead by other measures.

Errors or malfunctions within the IS1 Remote I/O System shall be reported to the manufacturer R. STAHL.

	The execution of the prooftests, test conditions and results of the testing has to be documented.
---	---

After expiration of the Proof test intervall (T_{proof}) (see chapter 4.1), it shall be tested, if:

- ✗ the real Profibus DP module address and the adjusted F-destination address conforms to system configuration and parameterisation in the F-Host.
- ✗ the functionality and safety shut down of the loop is working (while the test the safe interaction of all components of the safety system shall be tested. If it's not possible to drive the process up till the safety system intervenes, because of process-related reasons, the system has to be forced to intervention by suitable simulation).
- ✗ the LED and LCD display is working and no faulty conditions are displayed.

Possible Proof Test to test the functionality and safety shut down of the loop

- ▶ Take appropriate action to avoid a false trip.
- ▶ Power on test:
Remove the module from the BusRail and plug it in again.
The module should perform a self test and continuous normal operation afterwards.
- ▶ Generate a signal < 2.4 mA and verify that the information in the PROFIsafe telegram corresponds to the error code for line break (see chapter 6.2).
- ▶ Generate several signals within the allowed range of 2.4 mA to 22.814 mA and verify that the information in the PROFIsafe telegram corresponds to the set value.
- ▶ Generate a signal > 22.814 mA and verify that the information in the PROFIsafe telegram corresponds to the error code for short circuit (see chapter 6.2).
- ▶ Restore the loop to full operation.
- ▶ Restore normal operation.

	This test will detect approximately 99% of possible „du“ failures.
---	--

11 Repair work

WARNING

Danger due to improper repair!

- ▶ The device must be repaired only by the manufacturer!
- ▶ No changes to the device are permitted!

12 Release notes

HW-Rev.	FW-Vers.	GSD	Wizard	Type	Date	Description Hardware changes	Description Firmware changes
	02-03				2009-12-03		known errors of FW-Vers. 02-02 fixed
	02-02				2008-04-30		internal driver for LCD display changed
A	02-01	3.02			2008-04-09		PROFIsafe certified with CPM FW V02-40

