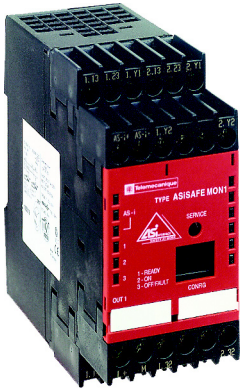
Telemecanique

ASISAFEMON1 /..1B
ASISAFEMON2 /..2B

AS-interface
Safety Monitor

Operating Manual

10/2006



a brand of Schneider Electric

Telemecanique

Contents

Edition: 10/2006

Table of Contents

Edition: 10/2006

Table of Figures

Edition: 10/2006

1 General Information

1.1 Explanation of symbols

Notice: Read these instructions carefully, and look at the equipment to become familiar with the device before trying to install, operate, or maintain it. The following special messages may appear throughout this documentation or on the equipment to warn of potential hazards or to call attention to information that clarifies or simplifies a procedure.

These are the safety alert symbols. They are used to alert yout to potential personal injury hazards. Obey all safety messages following these symbols to avoid death, injury, or equipment damage.

⚠ DANGER

DANGER indicates an imminently hazardous situation, which, if not avoided, **will result** in death, serious injury or equipment damage.

⚠ WARNING

WARNING indicates a potentially hazardous situation, which, if not avoided, **can result** in death, serious injury, or equipment damage.

⚠ CAUTION

CAUTION indicates a potentially hazardous situation, which, if not avoided, **can result** in injury or equipment damage.

NOTICE: Only qualified personnel should service electrical equipment. No responsibility is assumed by Schneider Electric for any consequences arising out of the use of this material or the associated User Manual. This document is not intended as an instruction manual for untrained persons.

Edition: 10/2006

⚠ WARNING

LOSS OF CONTROL

• The designer of any control scheme must consider the potential failure modes of control paths and, for certain critical control functions, provide a means to achieve a safe state during and after a path failure. Examples of critical control functions are emergency stop and overtravel stop.
• Separate or redundant control paths must be provided for critical control functions.
• System control paths may include communication links. Consideration must be given to the implications of unanticipated transmission delays or failures of the link. [a]
• Each implementation of an ASi Safe Safety Monitor and its associated components must be individually and thoroughly tested for proper operation before being placed into service.

Failure to follow these instructions can result in death, serious injury, or equipment damage.

[a] For additional information, refer to NEMA ICS 1.1 (latest edition), “Safety Guidelines for the Application, Installation, and Maintenance of Solid State Control” and to NEMA ICS 7.1 (latest edition), “Safety Standards for Construction and Guide for Selection, Installation and Operation of Adjustable-Speed Drive Systems”.

1.2 Declaration of Conformity

The AS-interface safety monitor has been developed and manufactured in accordance with the applicable European standards and directives.

Note: The corresponding Declaration of Conformity is in the packaging of each AS-interface safety monitor.

The manufacturer of the product possesses a certified quality assurance system in accordance with ISO 9001.

Edition: 10/2006

1.3 Standards

- Draft: Fundamentals for the testing and certification of "Bus systems for the transmission of safety-relevant messages"
- EN 954-1 - Safety of machines – safety-related elements of control systems
- EN 50295 - Low-voltage switching devices; control-system and device interfaces; actuator sensor interface (AS-interface)
- EN 60204-1 - Safety of machines – electrical equipment for machines – Part 1: general requirements
- EN 60947-5-1 - Low-voltage switchgear and controlgear - Part 5-1: control devices and switching elements; electromechanical control devices
- EN 61496-1 - Non-contact safety guards
- IEC 61508 1-7 - Functional safety of electric/electronic/programmable electronic systems with safety function

1.4 Definition of terms

Output switching element (safety output) of the AS-interface safety monitor

Element activated by the logic of the monitor which is able to switch off the downstream control elements. The output switching element may switch to or remain in the ON state only when all components are functioning as intended.

Output circuit

Consists of the two logically connected output switching elements.

OSSD

The safe AS-interface components and functional components assigned to an output circuit. They are responsible for releasing the machine element which generates the hazardous movement.

Integrated slave

Component in which sensor and/or actuator functions are grouped together with the slave to form a unit.

Configuration operation

Operating state of the safety monitor in which the configuration is loaded and checked.

Master

Component for data transmission which controls the logical and temporal behaviour on the AS-interface line.

Edition: 10/2006

External device monitoring circuit (contactor monitoring)

The external device monitoring circuit allows the switching function of the contactors connected to the AS-interface safety monitor to be monitored.

Safety output

See output switching element.

Safe input slave

Slave which reads in the safe ON or OFF state of the connected sensor or command device and transmits it to the master or safety monitor.

Safe slave

Slave for connecting safe sensors, actuators and other devices.

Safety monitor

Component which monitors the safe slaves and the correct function of the network.

Slave

Component for data transmission; the master cyclically addresses this component by its address. Only then does it generate an answer.

Standard slave

Slave for connecting non-safe sensors, actuators and other devices.

Synchronisation time

The maximum permissible temporal offset between the occurrence of two events which are dependent on one another.

Edition: 10/2006

1.5 Abbreviations

AS-interface	Actuator Sensor Interface
AOPD	Active Optoelectronic Protective Device
CRC	Cyclic Redundancy Check
I/O	Input/Output
EDM	External Device Monitoring
EMC	Electromagnetic compatibility
ESD	Electrostatic Discharge
PELV	Protective Extra-Low Voltage
PFD	Probability of Failure on Demand
PLC	Programmable Logic Control

Edition: 10/2006

1.6 Brief description

The actuator-sensor interface (AS-interface) has established itself as a system for networking primarily binary sensors and actuators at the lowest level of the automation hierarchy. The high number of installed systems, the ease of use and the reliable operating behaviour also make the AS-interface interesting in the area of machine safety.

The **safe** AS-interface system is intended for safety applications up to Category 4 in accordance with EN 954-1. Mixed operation of standard components and safe components is possible.

Note: A brief description of the safe AS-interface transmission can be found in chapter 12 at the end of this operating manual.

The AS-interface safety monitor monitors within an AS-interface system the safe slaves which have been assigned according to the configuration specified by the user with the configuration software. Depending on the device model, up to two dependent or independent OSSDs, each with external device monitoring circuit, are available. In the event of a stop request or a defect, the AS-interface safety monitor switches off the system in protective operation mode with a maximum reaction time of 40 ms.

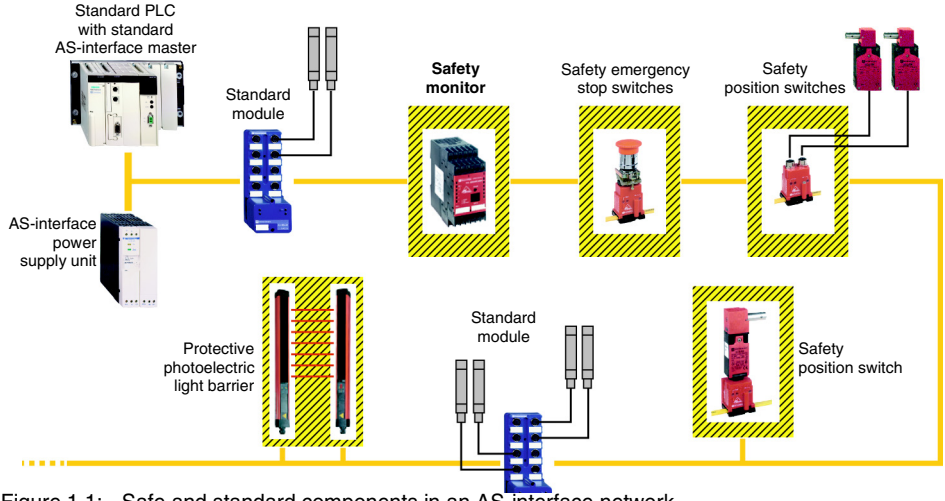


Figure 1.1: Safe and standard components in an AS-interface network

Multiple AS-interface safety monitors can be used within an AS-interface system. In this way, a safe slave can be monitored by multiple AS-interface safety monitors.

Edition: 10/2006

1.7 Different types of AS-interface safety monitors

The safety monitor is available in a total of four versions which differ with regard to the functions provided by the operating software and the initial configuration.

The **"Basic"** ASISAFEMON1/2 and **"Enhanced"** ASISAFEMON1B/2B function ranges differ as follows:

	"Basic"	**"Enhanced"**
Number of functional components at logic level	32	48
OR gates (inputs)	2	6
AND gates (inputs)	–	6
Safe time function, switch-on and switch-off delay	no	yes
Function "button"	no	yes
Safety guard/module with debouncing	no	yes
Deactivation of functional components	yes	yes
Reset of error condition	yes	yes
Diagnosis stop	yes	yes
Support of A/B technology for non-safe slaves	yes	yes
New functional components (flip-flop, pulse with pos. edge, etc.)	no	yes
Dummy device (NOP)	yes	yes

Table 1.1: "Basic" and "Enhanced" function ranges

Note: A detailed description of all functions can be found in the user manual for the **ASISWIN2** configuration software.

Output configuration

ASISAFEMON1 and ASISAFEMON1B : One output circuit

ASISAFEMON2 and ASISAFEMON2B : Two output circuits

Features of device versions

		Function range	
		"Basic"	**"Enhanced"**
Number of output circuits	1	ASISAFEMON1	ASISAFEMON1B
	2	ASISAFEMON2	ASISAFEMON2B

Table 1.2: Features of device versions

Edition: 10/2006

2 Safety Notices

2.1 Safety standard

The AS-interface safety monitor has been designed, manufactured, tested and presented for prototype design testing in accordance with the safety standards applicable at the time of testing. The technical safety requirements acc. to Category 4 as per EN 954-1 and SIL 3 as per IEC 61508 are fulfilled for all devices.

Note: A detailed list of failure probability values (PFD values) can be found in chapter 3.2.

Following a risk analysis, you may use the AS-interface safety monitor in accordance with its Safety Category (4) as a disconnecting protective device for securing danger areas.

2.2 Intended use

2.2.1 Application requirements

The AS-interface safety monitor has been designed as a **disconnecting protective device** for securing danger areas on power-driven working materials.

⚠ WARNING

UNINTENDED EQUIPMENT OPERATION

- This device must be applied in a manner that is described in this manual.
- Adhere to all applicable inspection, maintenance, and service intervals for the equipment.
- Make no changes to the device except where expressly described in this operating manual.

Failure to follow these instructions can result in death, serious injury, or equipment damage.

2.2.2 Residual risks (EN 292-1)

The wiring suggestions shown in this manual have been tested with utmost care. The relevant standards and regulations are adhered to if the shown components and appropriate wiring are used. Residual risks remain if:

- the suggested wiring concept is not adhered to and, as a result, the connected safety-relevant components or protective devices are not or are inadequately integrated into the safety circuit.
- relevant safety regulations specified for the operation, adjustment and maintenance of the machine are not adhered to by the operator. Here, the inspection and maintenance intervals for the machine should be strictly adhered to.

Edition: 10/2006

2.2.3 Areas of application

When used as intended, the AS-interface safety monitor allows the operation of sensor-controlled systems for the protection of persons and other protective components up to and including Category 4 acc. to EN 954-1.

The safety monitor also performs the mandatory emergency shutdown function for all non-hand-operated machines (Stop Category 0 or 1), the dynamic monitoring of the restart function and the contactor control function.

Examples for the use of the AS-interface safety monitor:

The safety monitor is used commercially in machines and systems in which the standard AS-interface bus functions as the local bus. Thus, by using the safety monitor as a bus subscriber, existing AS-interface bus configurations can be expanded easily and safety elements with corresponding "AS-interface safety at work" interface easily integrated. If a safety component does not have an "AS-interface safety at work" interface, a so-called coupling module can be used to make the connection. Existing AS-interface master and AS-interface power supply units can continue to be used.

There are no branch-specific restrictions. Several of the primary areas of application are listed here:

- Machine tools
- Expanded machining machines with multiple control elements and safety sensors for wood and metal applications
- Printing and paper processing machines, cutting machines
- Packaging machines, single and as part of a system
- Food processing equipment
- Piece and bulk material transport systems
- Machinery in the rubber and plastics industry
- Assembly machines and manipulators

Edition: 10/2006

2.3 Organizational measures

⚠ WARNING

UNINTENDED EQUIPMENT OPERATION

-Read and understand the Installation Manual before installing or operating the ASi-Safe Safety Monitor. Installation, adjustment, repair, and maintenance must be performed by qualified personnel.
-The user is responsible for compliance with all international and national electrical standards in force concerning protective grounding of all equipment.

Failure to follow these instructions can result in death, serious injury, or equipment damage.

Documentation

All entries in this operating manual must be heeded, in particular those in the sections "Safety Notices" and "Commissioning".

Keep this operating manual in a safe place. It should be accessible at all times.

Safety regulations

Observe the locally applicable legal regulations and the rules of the employer's liability insurance association.

Qualified personnel

Mounting, commissioning and maintenance of the device may only be carried out by qualified personnel.

Work on electrical installations may only be carried out by qualified personnel.

Settings and changes of the device configuration via PC and **ASISWIN2** configuration software must only be performed by an authorised qualified personnel.

The **password** for changing a device configuration is to be held under lock and key by the qualified personnel.

Repair

Repairs, in particular the opening of the housing, may only be carried out by the manufacturer or a person authorised by the manufacturer.

Disposal

Note: Electrical scrap is a special waste product! Observe the local regulations regarding disposal of the product.

The AS-interface safety monitor contains no batteries of any type which would need to be removed prior to disposal of the product.

Edition: 10/2006

3 Specifications

3.1 General technical data

Electrical data

Operating voltage U_b	24V DC +/- 15%
Residual ripple	< 15%
Rated operating current	ASISAFEMON1 and ASISAFEMON1B: 150mA; ASISAFEMON2 and ASISAFEMON2B: 200mA
Peak switch-on current [1)]	all types: 600mA
Reaction time (safety-relevant)	< 40ms
Delay before start-up	< 10s

1) Simultaneous switch-on of all relays; the current for the message outputs is not taken into consideration

AS-interface data

AS-interface profile	Monitor 7.F
AS-interface voltage range	18.5 … 31.6V
AS-interface current consumption	< 45mA
Number of devices per AS-interface branch	In a fully configured AS-interface network with 31 used standard addresses, it is possible to additionally install a maximum of four safety monitors without address. If fewer than 31 standard addresses are used, an additional monitor can be installed for each standard address that is not used. If additional subscribers are installed without address (e.g. earth-fault monitoring modules), the number of installable safety monitors is reduced accordingly. If repeaters are used, this applies for each segment.

Configuration interface

RS 232	9600 baud, no parity, 1 start bit, 1 stop bit, 8 data bits

Edition: 10/2006

Inputs and outputs

"Start" input	Optical coupling input (high active), input current approx. 10mA at 24V DC
"External device monitoring circuit" input	Optical coupling input (high active), input current approx. 10mA at 24V DC
Message output "safety on" [1]	PNP transistor output, 200mA, short-circuit and polarity-reversal protection
Safety output	Voltage-free make contact, max. contact load: 1A DC-13 at 24V DC 3A AC-15 at 230V AC
Continuous thermal current (max.)	ASISAFEMON1 and ASISAFEMON1B: max. total current for all output switching elements: 6A i.e. output circuit 1: 3A per output switching element ASISAFEMON2 and ASISAFEMON2B: max. total current for all output switching elements: 8A i.e. output circuit 1: 3A per output switching element output circuit 2: 1A per output switching element or output circuit 1: 2A per output switching element output circuit 2: 2A per output switching element
Safeguarding	External with max. 4A slow blow
Overvoltage category	3, for rated operating voltage 300V AC acc. to VDE 0110 part 1

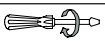
1) The "Safety on" message output is not relevant to safety!

Environmental data

Operating temperature	-20 … +60°C (-4°F to +140°F)
Storage temperature	-30 … +70°C (-22°F to +158°F)
Protection class	IP 20 (only suitable for use in electrical operating rooms / switching cabinets with minimum protection class IP 54)

Mechanical data

Dimensions (WxHxD)	45mm x 105,9mm x 120mm (1.77in x 4.17in x 4.73in)
Housing material	Polyamide PA 66
Weight	ASISAFEMON1 and ASISAFEMON1B: approx. 350g (12.35oz); ASISAFEMON2 and ASISAFEMON2B: approx. 450g (15.87oz)
Mounting	Snap-on mounting on top-hat rail acc. to EN 50022
Connection	

 ∅ 5 ... 6 mm / PZ2	0,8 ... 1,2 Nm 7 ... 10.3 LB.IN
	1 x (0,5 ... 4,0) mm² 2 x (0,5 ... 2,5) mm²
	1 x (0,5 ... 2,5) mm² 2 x (0,5 ... 1,5) mm²
AWG	2 x 20 ... 14

Edition: 10/2006

⚠ WARNING

INADEQUATE POWER SUPPLY

The AS-interface power supply unit for supplying the AS-interface components must demonstrate safe mains separation according to IEC 70742 and the ability to bridge brief mains failures up to 20ms.
The power supply unit for 24V supply must also demonstrate safe mains separation according to 60742 and the ability to bridge brief mains failures up to 20ms.

Failure to follow these instructions can result in death, serious injury, or equipment damage.

⚠ CAUTION

STATIC SENSITIVE COMPONENTS

The ASI-Safe Safety Monitor can be damaged by static electricity. Observe the electrostatic precautions below when handling, programming, and installing the monitor.

Failure to follow this instruction can result in equipment damage.

Note: The safety monitor has been tested for interference-free operation acc. to EN 61000-4-2 with 8kV air discharging. The air discharging value of 15 kV stipulated by EN 61496-1 is not relevant for the safety monitor as the safety monitor is installed in a system which is contained either in a protective housing or a switching cabinet and the monitor can be accessed only by trained personnel. Nevertheless, we recommend that before the user inserts the configuration cable into the safety monitor he perform a discharge (earthing) at a suitable location.

Edition: 10/2006

3.2 Consideration of failure probability according to IEC 61508

To allow calculation of failure probability for the entire system, the AS-interface safety monitor returns a component which depends on the maximum uninterrupted switch-on time of the output circuit(s).

This results in the following table:

Switch-on time	Total operating time	PFD
3 months	10 years	$< 4 \times 10^{-5}$
6 months	10 years	$< 6 \times 10^{-5}$
12 months	10 years	$< 9 \times 10^{-5}$

Table 3.1: Failure probability on request depending on switch-on time

The switch-on time describes the period of time until the safety function was requested, or the maximum period of time between two executed safety checks. During this check, safe shutdown is tested by actuating every safe sensor.

The total operating time describes the safety system's service life from commissioning to disassembly; it is used as the basis for calculating the failure probability.

Together with the failure probabilities of the other components used in the safety system (e.g. AS-interface slaves) it is then possible to determine the overall failure probability. The resulting value can be used for categorising the safety system under the respective safety level in accordance with IEC 61508.

Switch-on time	Total operating time	PFH
12 months	10 years	$< 9 \times 10^{-9}$

Table 3.2: Probability of failure per hour

Edition: 10/2006

3.3 Dimensioned drawings

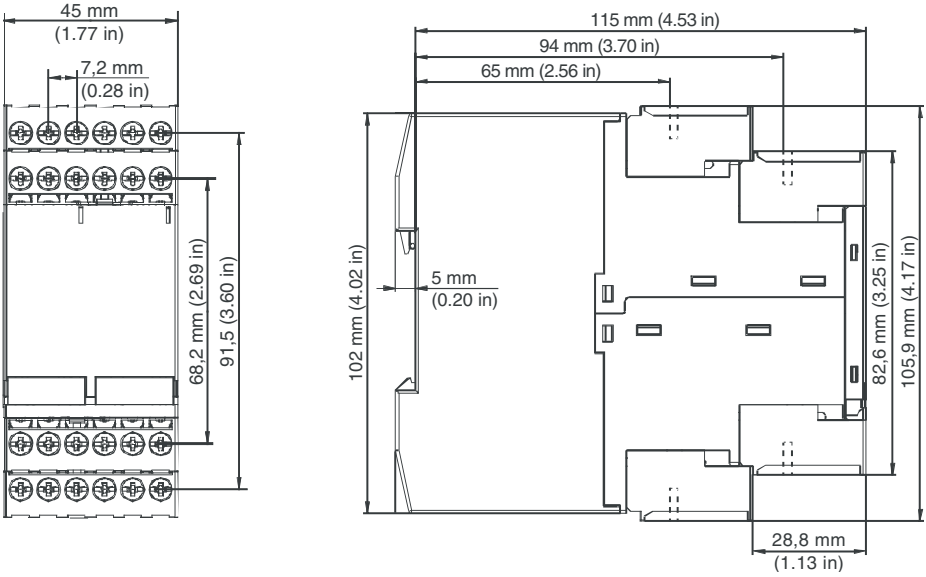


Figure 3.1: Dimensions

3.4 Scope of delivery

The **basic unit** consists of:

- AS-interface safety monitor ASISAFEMON1, ASISAFEMON2, ASISAFEMON1B or ASISAFEMON2B

The following **accessories** are available:

- Configuration interface cable (RJ45/SubD 9 pin) for the PC/safety monitor connection
- Software CD with
  - **ASISWIN2** communication software for Microsoft® Windows 9x/Me/NT/2000/XP®
  - Operating manual in PDF format
    (Adobe® Acrobat Reader® Version 4.x or newer is required for viewing the files)
- Operating manual
- Download cable (RJ45/RJ45) for the safety monitor/safety monitor connection
- Device front cover for protection and sealing

Edition: 10/2006

Edition: 10/2006

4 Mounting

4.1 Mounting in the switching cabinet

The AS-interface safety monitor is mounted on 35mm standard rails acc. to DIN EN 50022 in the switching cabinet.

⚠ WARNING

EQUIPMENT DAMAGE

The housing of the AS-interface safety monitor is not suitable for open wall mounting. Provide a protective housing in all cases when the device is not protected by an appropriately rated enclosure.

Failure to follow these instructions can result in death, serious injury, or equipment damage.

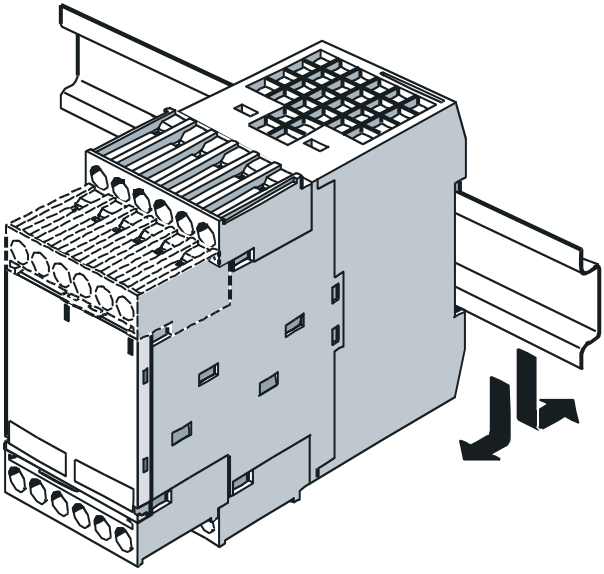


Figure 4.1: Mounting

To mount, position the device on the upper edge of the standard rail and then snap it onto the bottom edge. To remove, firmly press the device against the upper rail guide and lift out.

Note: When drilling above the device, cover the AS-interface safety monitor. No particles, no metal shavings in particular, should be allowed to penetrate into the housing through ventilation openings as they may cause a short-circuit.

Edition: 10/2006

Removable connection terminals

The AS-interface safety monitor contains keyed, removable connection terminals (**A**, **B**, **C**, **D** in Figure 4.2).

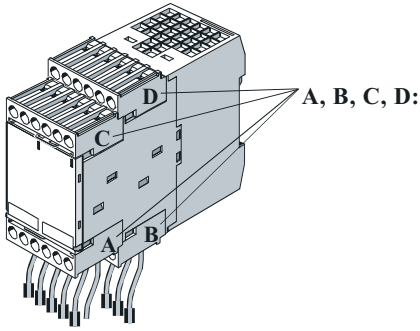


Figure 4.2: Removable connection terminals

To remove the keyed connection terminals, push back the safety spring **a** and pull the terminals out towards the front (Figure 4.3). When mounting, the connection terminals must audibly lock into place.

⚠ DANGER

ELECTRIC SHOCK HAZARD

Disconnect all power before servicing equipment.

Failure to follow this instruction will result in death or serious injury.

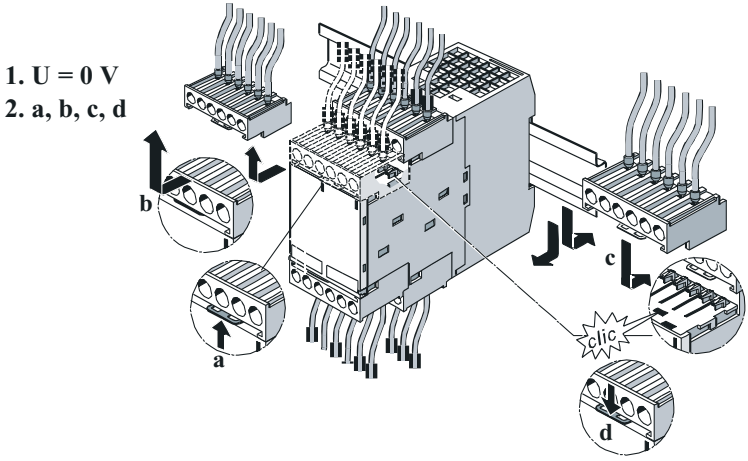


Figure 4.3: Removing and mounting keyed connection terminals

Edition: 10/2006

Mounting accessories

As the AS-interface safety monitor is a safety component, it is possible to protect the device from unauthorised access by sealing the **CONFIG** configuration interface and the **Service** button. Included in the delivery contents for the device is a transparent cover with safety hook through which you can pass a lead sealing wire or thread when the device is in its mounted state (see figure 4.4). You must break the safety hook off the cover before using.

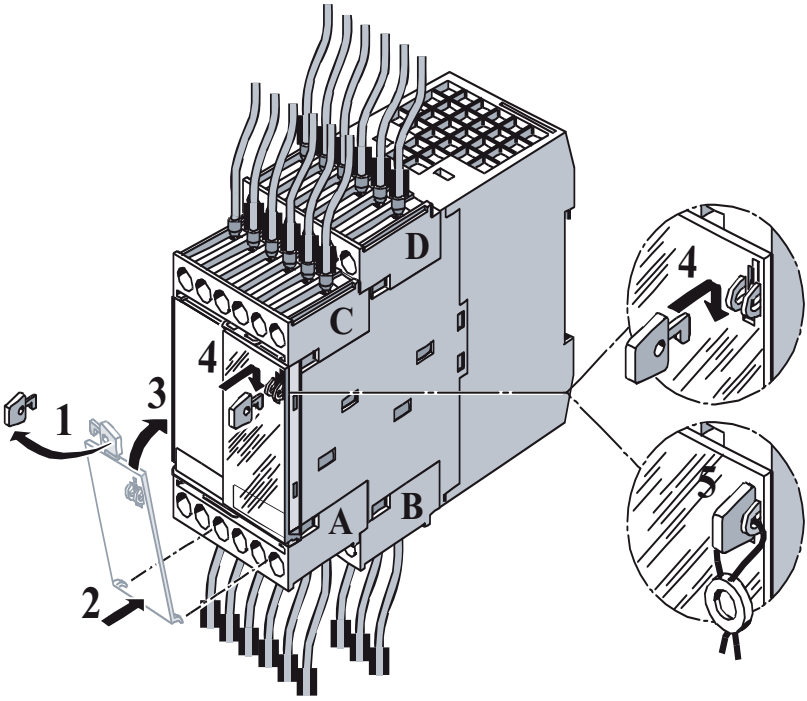


Figure 4.4: Mounting accessories for sealing the device

⚠ WARNING

ELECTROSTATIC DISCHARGES

The transparent cover with safety hook should always be used as they provide protection against electrostatic discharges (ESD) and the penetration of foreign bodies into the CONFIG socket of the AS-interface safety monitor configuration interface.

Failure to follow these instructions can result in death, serious injury, or equipment damage.

The sealing wire is not included in the carton.

Edition: 10/2006

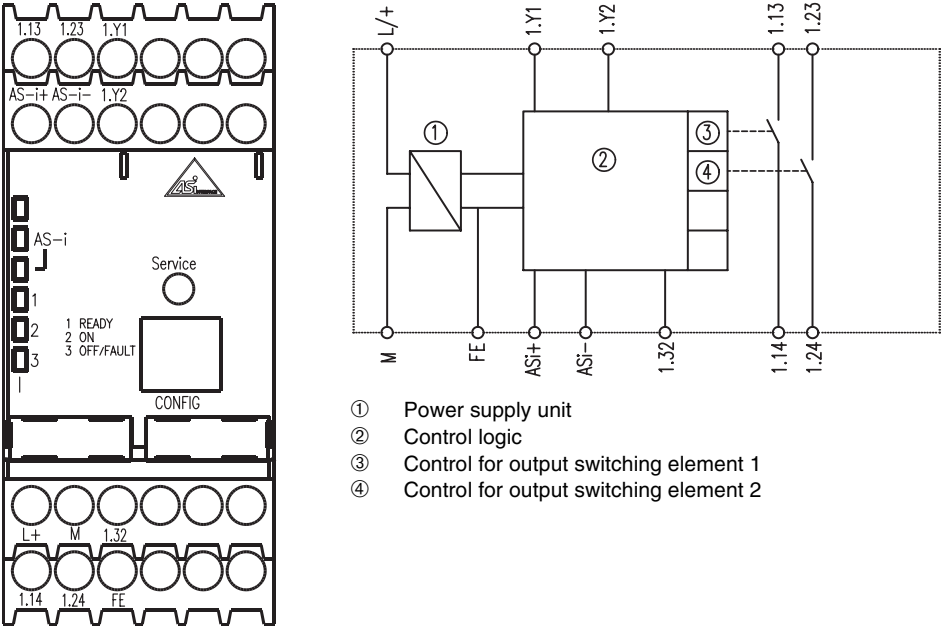
Edition: 10/2006

5 Electrical connection ASISAFEMON1 and ASISAFEMON1B

Note: Work on electrical installations may only be carried out by qualified personnel.

5.1 Terminal assignment

Terminal arrangement / block diagram



① Power supply unit
② Control logic
③ Control for output switching element 1
④ Control for output switching element 2

Figure 5.1: Terminal arrangement / block diagram of AS-interface safety monitor ASISAFEMON1 and ASISAFEMON1B

Edition: 10/2006

Terminal assignment

Terminal	Signal / description
AS-i+	Connection at the AS-interface bus
AS-i–	
L+	+24 V DC / supply voltage
M	COM/ return for the +24V DC supply
FE	Protective earth
1.Y1	EDM 1 / input of external device monitoring circuit
1.Y2	Start 1 / start input
1.13	Output switching element 1
1.14	
1.23	Output switching element 2
1.24	
1.32	Message output "safety on"

Table 5.1: Terminal assignment of AS-interface safety monitor ASISAFEMON1 and ASISAFEMON1B

Note: The connection of the earth lead to terminal FE is not necessary if terminal M is connected to earth in the direct vicinity of the device.

⚠ WARNING

INADEQUATE POWER SUPPLY

The AS-interface power supply unit for supplying the AS-interface components must demonstrate safe mains separation according to IEC 60742 and the ability to bridge brief mains failures up to 20ms.

The power supply unit for 24V supply must also demonstrate safe mains separation according to IEC 60742 and the ability to bridge brief mains failures up to 20ms.

Failure to follow these instructions can result in death, serious injury, or equipment damage.

Edition: 10/2006

5.2 Connection overview

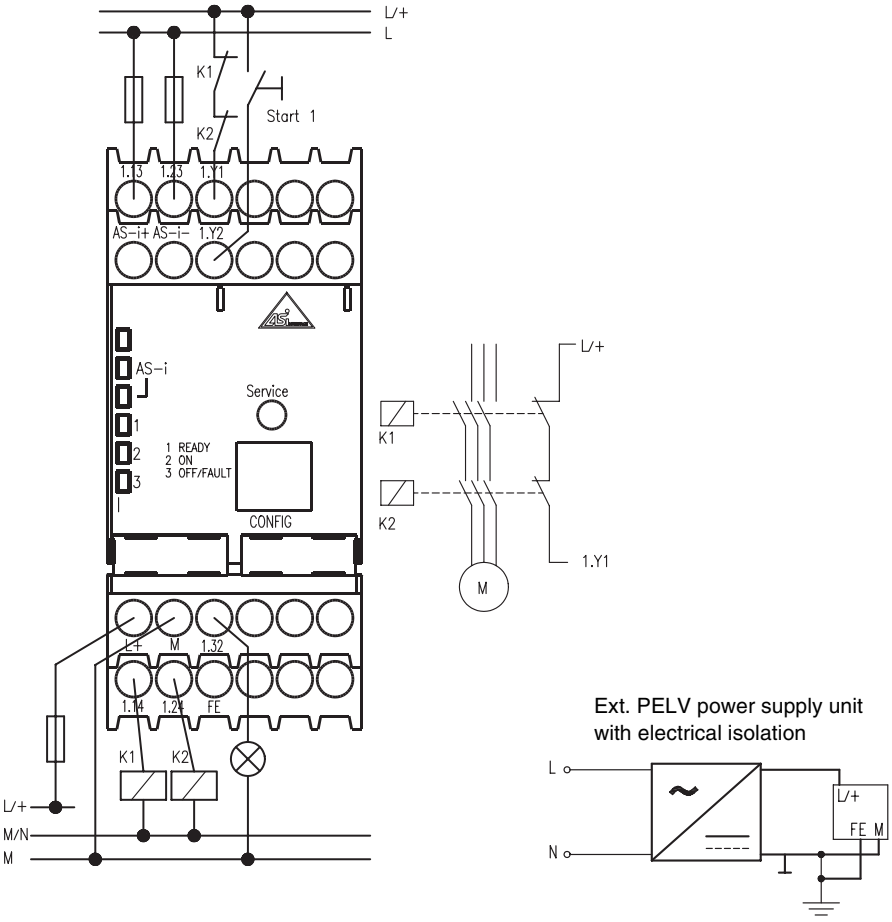


Figure 5.2: Connection overview of AS-interface safety monitor ASISAFEMON1 and ASISAFEMON1B

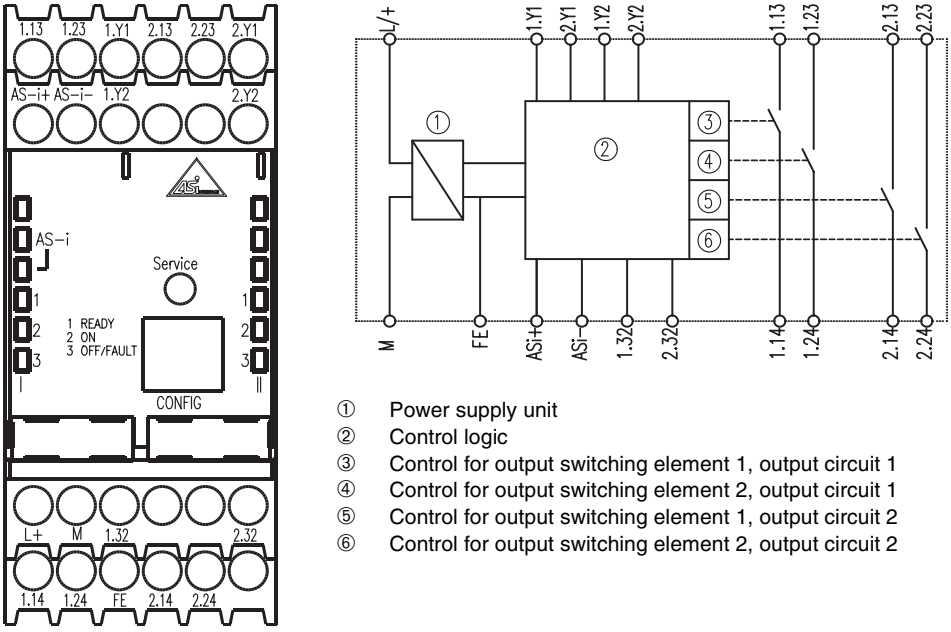
Edition: 10/2006

6 Electrical connection ASISAFEMON2 and ASISAFEMON2B

Note: Work on electrical installations may only be carried out by qualified personnel.

6.1 Terminal assignment

Terminal arrangement



① Power supply unit
② Control logic
③ Control for output switching element 1, output circuit 1
④ Control for output switching element 2, output circuit 1
⑤ Control for output switching element 1, output circuit 2
⑥ Control for output switching element 2, output circuit 2

Figure 6.1: Terminal arrangement / block diagram of AS-interface safety monitor ASISAFEMON2 and ASISAFEMON2B

Edition: 10/2006

Terminal assignment

Terminal	Signal / description
AS-i+	Connection at the AS-interface bus
AS-i–	
L+	+24V DC / supply voltage
M	COM/ return for the +24V DC supply
FE	Protective earth
1.Y1	EDM 1 / input of external device monitoring circuit, output circuit 1
1.Y2	Start 1 / start input, output circuit 1
1.13	Output switching element 1, output circuit 1
1.14	
1.23	Output switching element 2, output circuit 1
1.24	
1.32	Message output 1 "Safety on", output circuit 1
2.Y1	EDM 2 / input of external device monitoring circuit, output circuit 2
2.Y2	Start 2 / start input, output circuit 2
2.13	Output switching element 1, output circuit 2
2.14	
2.23	Output switching element 2, output circuit 2
2.24	
2.32	Message output 2 "Safety on", output circuit 2

Table 6.1: Terminal assignment of AS-interface safety monitor ASISAFEMON2 and ASISAFEMON2B

Note: The connection of the earth lead to terminal FE is not necessary if terminal M is connected to earth in the direct vicinity of the device.

⚠ WARNING

INADEQUATE POWER SUPPLY

The AS-interface power supply unit for supplying the AS-interface components must demonstrate safe mains separation according to IEC 60742 and the ability to bridge brief mains failures up to 20ms.
The power supply unit for 24V supply must also demonstrate safe mains separation according to IEC 60742 and the ability to bridge brief mains failures up to 20ms.

Failure to follow these instructions can result in death, serious injury, or equipment damage.

Edition: 10/2006

6.2 Connection overview

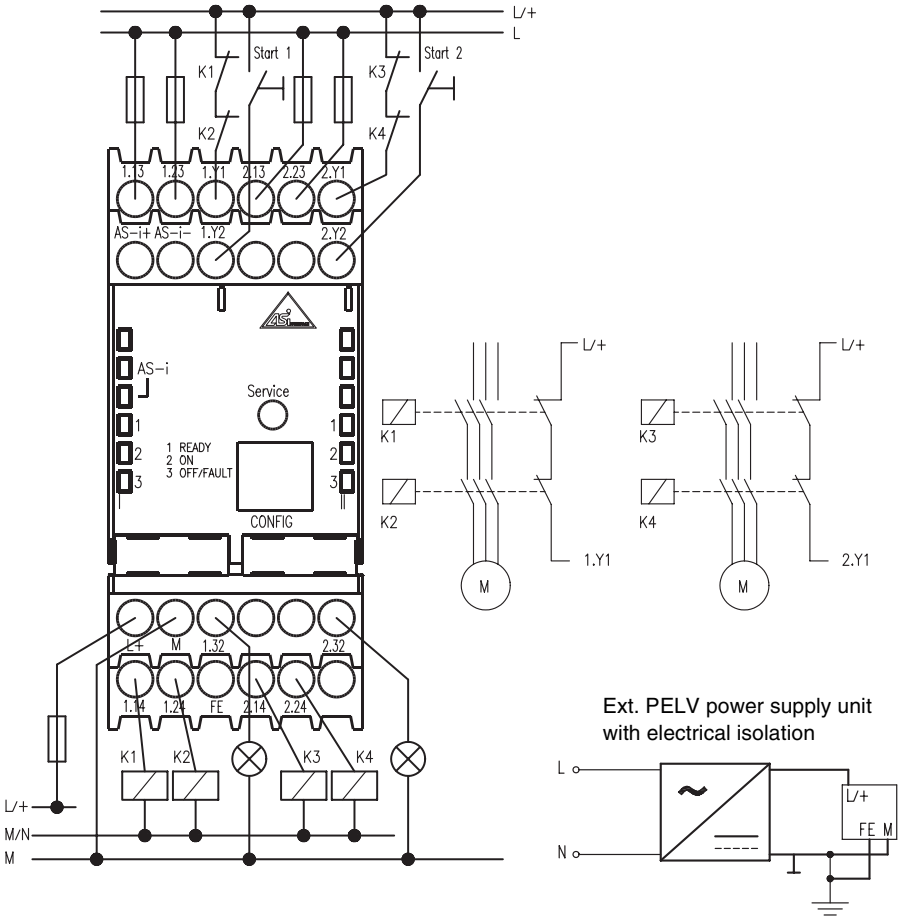


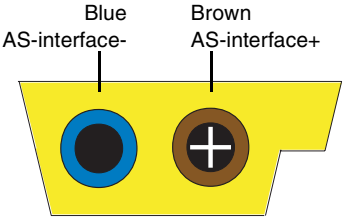
Figure 6.2: Connection overview of AS-interface safety monitor ASISAFEMON2 and ASISAFEMON2B

Edition: 10/2006

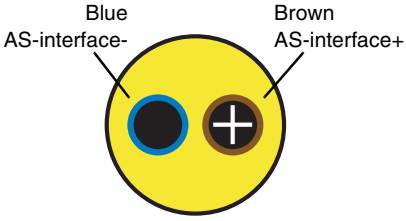
7 Electrical Connection of All Types

Note: Work on electrical installations may only be carried out by qualified personnel.

7.1 AS-interface bus connection



Yellow AS-interface ribbon cable



Two-conductor AS-interface round cable (recommended: flexible power cable H05VV-F2x1.5 acc. to DIN VDE 0281)

Figure 7.1: AS-interface cable variants

Edition: 10/2006

7.2 Serial interface

The serial RS 232C interface **CONFIG** is used for communication between PC and device and is permanently set to a baud rate of 9600 baud.

The interface is provided on the AS-interface safety monitor as an RJ45 socket. A matching interface cable with 9-pin subD connector is available as an accessory.

Note: Use only the optional interface cable. The use of other cables may lead to functional disturbances or damage to the connected AS-interface safety monitor.

Configuration interface RS 232C

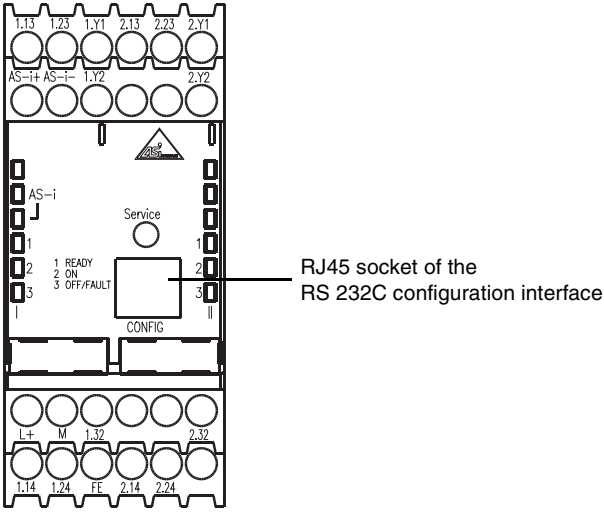


Figure 7.2: Location of the RS 232C configuration interface

Edition: 10/2006

8 Function and Commissioning

The configuration and commissioning of the AS-interface safety monitor is performed using a PC/ notebook with the **ASISWIN2** configuration software.

Note: The description of the **ASISWIN2** software and the commissioning of the AS-interface safety monitor can be found in the "ASISWIN2 - AS-interface safety monitor configuration software for Microsoft®-Windows®" manual.

The software manual is an important part of the operating manual for the AS-interface safety monitor. Configuration and commissioning of the AS-interface safety monitor is not possible without the **ASISWIN2** software.

Configuration may be performed only by a qualified personnel. All commands relevant to safety are protected by a password.

8.1 Function and operating modes

With the AS-interface safety monitor, a distinction is made between 3 operating modes:

- Start-up operation
- Configuration operation
- Protective operation

8.1.1 Start-up operation

After switching on, the microcontrollers in the AS-interface safety monitor first perform a system test of the hardware and internal software. If an internal device error is detected, the other device initialisation processes are stopped and the output switching elements remain switched off.

If all internal tests are completed successfully, the AS-interface safety monitor checks whether a valid, validated configuration is stored in the internal configuration memory.

If yes, this configuration is loaded, the necessary data structures assembled and the device switches to protective operation. Depending on the configuration, the output switching elements are then switched on or remain switched off.

If either no configuration or a faulty configuration is detected in the configuration memory, the device switches to configuration operation. The output switching elements remain switched off.

Edition: 10/2006

8.1.2 Configuration operation

In configuration operation of the AS-interface safety monitor, a command processing module is activated which communicates via the serial configuration interface with the **ASISWIN2** software installed on the PC/notebook (see the "ASISWIN2 - AS-interface safety monitor configuration software for Microsoft®-Windows®" manual). Data transmission is monitored for transmission errors and, if necessary, repeated.

It is possible to switch to configuration operation by

- sending the password-protected command **stop** while in protective operation from the **ASISWIN2** software. Configured shutdown delay times are to be taken into account here.
- sending the command **stop** while in protective operation from the **ASISWIN2** software without entering a password. This is only possible if there is no communication on the AS-interface line. You can ensure that this is the case by, for example, directly disconnecting the AS-interface line from the monitor.
- detecting a missing or faulty configuration in start-up operation.
- pressing the **Service** button for the first time when replacing a malfunctioning safe AS-interface slave (see chapter 10.4 "Replacing malfunctioning safe AS-interface slaves").

8.1.3 Protective operation

Protective operation is the normal operating mode of the AS-interface safety monitor. In this mode the output switching elements are activated and deactivated depending on the operating state of the monitored safe AS-interface slaves and configured functional components.

In protective operation, the AS-interface safety monitor continuously transmits diagnostic data via the serial configuration interface. This data is processed by the **ASISWIN2** software.

If an internal error function is detected during protective operation of the AS-interface safety monitor, the output switching elements are switched off immediately and without regard to any set delay times. The AS-interface safety monitor then performs a self test again. If the error no longer exists, the AS-interface safety monitor returns to protective operation. If the error still exists, this state is error-locked and can be exited only by switching the AS-interface safety monitor back on.

It is possible to switch to protective operation by

- sending the command **start** while in configuration operation from the **ASISWIN2** software.
- detecting a valid, validated configuration in start-up operation.
- pressing the **Service** button for the second time when replacing a malfunctioning safe AS-interface slave (see chapter 10.4 "Replacing malfunctioning safe AS-interface slaves").

Edition: 10/2006

8.2 Display and operating elements

The LED indicators on the front side of the AS-interface safety monitor provide information about the operating mode and the device state.

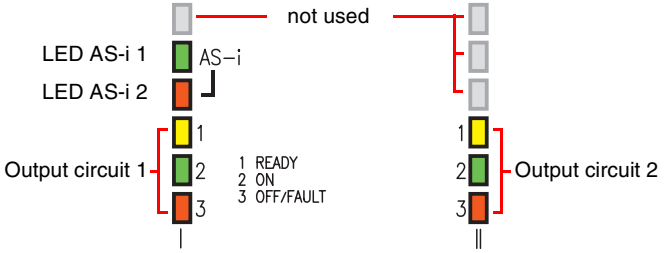


Figure 8.1: Overview of device LEDs

Meanings of the LED indicators in protective operation

LED	Colour		Meaning
AS-i 1		off	no supply
		green, continuous	AS-interface supply present
AS-i 2		off	normal operation
		red, continuous	communication error
1 READY (per output circuit)		off	–
		yellow, continuous	start-up/restart-disable active
		yellow, flashing	external test necessary / acknowledgement / delay before start-up active
2 ON (per output circuit)		off	contacts of the output switching element open
		green, continuous	contacts of the output switching element closed
		green, flashing	delay time runs in event of Stop Category 1
3 OFF/FAULT (per output circuit)		off	contacts of the output switching element closed
		red, continuous	contacts of the output switching element open
		red, flashing	error on level of the monitored AS-interface components

Edition: 10/2006

LED	Colour		Meaning
1 READY 2 ON 3 OFF/FAULT (per output circuit)		simultaneously flashing rapidly	internal device error, error message can be queried by means of **ASISWIN2** software

Note: Pressing the Service button is acknowledged by a one-time, brief illumination of all device LEDs.

⚠ CAUTION

EQUIPMENT DAMAGE

Do not exert more than 1Nm (8.85 lb-in) of actuation force on the Service button.

Failure to follow this instruction can result in injury or equipment damage.

8.3 Switching on the device

As soon as the supply voltage is present at the device, the internal system test begins. This operating status is indicated by the switching on of all LEDs installed in the device (see chapter 8.1.1 "Start-up operation").

8.4 Device configuration and parameterisation

For the device configuration and parameterisation, you require the software program **ASISWIN2**.

The **ASISWIN2** software is responsible for the following tasks:

- Configuring the AS-interface safety monitor
- Documentation of the device configuration
- Commissioning the AS-interface safety monitor
- Diagnosis of the AS-interface safety monitor

Note: The description of the ASISWIN2 program can be found in the separate software manual (Reference Number 9547118-GB / Edition 2GB/154/02).

Configuration operation (chapter 8.1.2) is indicated by sequential illumination of LEDs 1 … 3 of the output circuit 1.

Edition: 10/2006

Proceed as follows:

- Install the program on your PC.
- Apply the supply voltage to the AS-interface safety monitor.

⚠ CAUTION

STATIC SENSITIVE COMPONENTS

The ASI-Safe Safety Monitor can be damaged by static electricity. Observe the electrostatic precautions below when handling, programming, and installing the monitor.

Failure to follow this instruction can result in equipment damage.

- Use the interface cable (RJ45/SubD 9-pin) to connect the PC to the AS-interface safety monitor (see chapter 2.1.2 "Connection between the AS-interface safety monitor and the PC" of the software manual).
- Configure the AS-interface safety monitor and put it into operation as described in the software manual *(Reference Number 9547118-GB / Edition 2GB/154/02)*.
- The AS-interface safety monitor is ready for operation following commissioning.

⚠ WARNING

LOSS OF CONTROL

• The designer of any control scheme must consider the potential failure modes of control paths and, for certain critical control functions, provide a means to achieve a safe state during and after a path failure. Examples of critical control functions are emergency stop and overtravel stop.
• Separate or redundant control paths must be provided for critical control functions.
• System control paths may include communication links. Consideration must be given to the implications of unanticipated transmission delays or failures of the link. [a]
• Each implementation of an ASi Safe Safety Monitor and its associated components must be individually and thoroughly tested for proper operation before being placed into service.

Failure to follow these instructions can result in death, serious injury, or equipment damage.

[a] For additional information, refer to NEMA ICS 1.1 (latest edition), “Safety Guidelines for the Application, Installation, and Maintenance of Solid State Control” and to NEMA ICS 7.1 (latest edition), “Safety Standards for Construction and Guide for Selection, Installation and Operation of Adjustable-Speed Drive Systems”.

Edition: 10/2006

8.5 Technical safety documentation for the application

Note: The detailed description of the technical safety documentation for the configuration of your application can be found in the separate software manual (Reference Number 9547118-GB / Edition 2GB/154/02).

Proceed as follows:

- Create the AS-interface safety monitor configuration for your application.
- Validate the configuration (to be performed by the qualified personnel).
- Print out the final configuration log and, optionally, the configuration overview (see chapter 5.8 "Configuration documentation" of the software manual).
- Sign the final configuration log (to be performed by the qualified personnel).
- File the log together with the other technical safety documentation for your application (machine documentation) and store in a safe location.

Edition: 10/2006

Edition: 10/2006

9 Maintenance

9.1 Checking for safe shutdown

The proper function of the AS-interface safety monitor within the system to be secured, i.e. the safe shutdown following the triggering of an assigned safe sensor or switch, is to be checked at least annually by the qualified personnel.

⚠ WARNING

LOSS OF CONTROL

- Qualified personnel must perform maintenance at least once a year on the system by activating each AS-interface slave and visually inspecting the switching behavior of the output circuits of the AS-interface safety monitor.
- The maximum switch-on time and total operating time depends on the PFD value selected for the overall failure probability. When the maximum switch-on time has been reached (three, six, or twelve months), the safety system must be checked to ensure that it is functioning correctly by prompting the shutdown function.
- When the total operating time has been reached (10 years), the device must be checked at the manufacturer's factory to insure that it is functioning correctly.

Failure to follow these instructions can result in death, serious injury, or equipment damage.

Edition: 10/2006

10 Status Display, Errors and Error Rectification

10.1 Status display on the device / error diagnosis on the PC

An internal or external error is indicated by the red flashing LED **OFF/FAULT** on the AS-interface safety monitor (see chapter 8.2 "Display and operating elements").

Note: A more exact diagnosis of the error is possible via the configuration interface using the ASISWIN2 software (see software manual).

10.2 Troubleshooting tips

Error	Possible cause	Remedy
LED AS-i 1 is off	No AS-interface supply	• Check line connections • Check AS-interface power supply unit
LED AS-i 2 illuminates red	Communication on the AS-interface bus is faulty	• Check line connections • Check AS-interface master
LED 3 OFF/FAULT flashes red	Error on level of the monitored AS-interface components	• Perform diagnostics with **ASISWIN2** • If necessary, replace malfunctioning AS-interface components
LEDs 1 … 3 simultaneously flashing rapidly	Internal device error	• Note down the error numbers displayed by **ASISWIN2** in the error message window and contact the manufacturer

10.3 Error release with the "Service" button

An error-locked safety monitor (red LED **3 OFF/FAULT** flashes) can be released by pressing the "Service" button. The device with the error is reset when the button is pressed. A start test must be performed on this device after the reset.

Note: Pressing the Service button is acknowledged by a one-time, brief illumination of all device LEDs.

Edition: 10/2006

10.4 Replacing malfunctioning safe AS-interface slaves

⚠ DANGER

ELECTRIC SHOCK HAZARD

Disconnect all power before servicing equipment.

Failure to follow this instruction will result in death or serious injury.

10.4.1 Replacing a malfunctioning safe AS-interface slave

If a safe AS-interface slave is malfunctioning, it is possible to replace it without a PC and without reconfiguring the AS-interface safety monitor by using the **Service** button on the AS-interface safety monitor.

⚠ CAUTION

EQUIPMENT DAMAGE

Do not exert more than 1Nm (8.85 lb-in) of actuation force on the Service button.

Failure to follow this instruction can result in injury or equipment damage.

Note: When the Service button is pressed, the safety monitor switches from protective operation to configuration operation. The output circuits are therefore deactivated in all cases.

Pressing the Service button is acknowledged by a one-time, brief illumination of all device LEDs.

Proceed as follows:

1. Disconnect the malfunctioning AS-interface slave from the AS-interface line.
2. Press the **Service** button for approx. 1 second on all AS-interface safety monitors which use the malfunctioning safe AS-interface slave.
3. Connect the new safe AS-interface slave to the AS-interface line.
4. Press the **Service** button again for approx. 1 second on all AS-interface safety monitors which use the replaced safe AS-interface slave.

The first time the **Service** button is pressed, the monitor determines whether exactly one slave is missing. This is noted in the error memory of the AS-interface safety monitor. The AS-interface safety monitor switches to configuration operation. The second time the **Service** button is pressed, the code sequence of the new slave is read in and checked for correctness. If the code sequence is OK, the AS-interface safety monitor returns to protective operation.

Edition: 10/2006

⚠ WARNING

LOSS OF CONTROL

- The designer of any control scheme must consider the potential failure modes of control paths and, for certain critical control functions, provide a means to achieve a safe state during and after a path failure. Examples of critical control functions are emergency stop and overtravel stop.
- Separate or redundant control paths must be provided for critical control functions.
- System control paths may include communication links. Consideration must be given to the implications of unanticipated transmission delays or failures of the link. [a]
- Each implementation of an ASi Safe Safety Monitor and its associated components must be individually and thoroughly tested for proper operation before being placed into service.

Failure to follow these instructions can result in death, serious injury, or equipment damage.

[a] For additional information, refer to NEMA ICS 1.1 (latest edition), “Safety Guidelines for the Application, Installation, and Maintenance of Solid State Control” and to NEMA ICS 7.1 (latest edition), “Safety Standards for Construction and Guide for Selection, Installation and Operation of Adjustable-Speed Drive Systems”.

10.4.2 Replacing several malfunctioning safe AS-interface slaves

If more than one safe AS-interface slave on an AS-interface branch is malfunctioning, the devices must be replaced in the following way:

Note: When the Service button is pressed, the safety monitor switches from protective operation to configuration operation. The output circuits are therefore deactivated in all cases.

Pressing the Service button is acknowledged by a one-time, brief illumination of all device LEDs.

⚠ CAUTION

EQUIPMENT DAMAGE

Do not exert more than 1Nm (8.85 lb-in) of actuation force on the Service button.

Failure to follow this instruction can result in injury or equipment damage.

1. Disconnect all malfunctioning AS-interface slaves from the AS-interface line. Connect all new, **already addressed** safe AS-interface slaves **except one** to the AS-interface line (Auto_Address does not function in this case).
2. Activate all newly connected slaves so that no code sequences are sent by the slave (actuate emergency shutdown, open door, break light barrier, etc.).

Note: The error detection function integrated in the monitor only accepts a new slave if point 2 is fully observed.

Edition: 10/2006

3. Press the **Service** button for approx. one second on all AS-interface safety monitors which used the malfunctioning safe AS-interface slaves.
4. Connect the last missing and already addressed slave to the AS-interface line.
5. Press the **Service** button for approx. one second on all AS-interface safety monitors which used the malfunctioning safe AS-interface slaves.
6. Disconnect one of the replaced and not yet taught AS-interface slaves from the AS-interface line.
7. Press the **Service** button for approx. one second on all AS-interface safety monitors which used the malfunctioning safe AS-interface slaves.
8. Reconnect the previously disconnected AS-interface slave to the AS-interface line.
9. Activate the newly connected slave. The code sequence is now transmitted to the AS-interface safety monitor and stored there.
10. Press the **Service** button for approx. one second on all AS-interface safety monitors which used the malfunctioning safe AS-interface slaves.
11. Repeat the procedure from step 6 onwards until all replaced AS-interface slaves have been taught.

The first time the **Service** button is pressed, the monitor determines whether exactly one slave is missing. This is noted in the error memory of the AS-interface safety monitor. The AS-interface safety monitor switches to configuration operation. The second time the **Service** button is pressed, the code sequence of the new slave is read in and checked for correctness. If the code sequence is OK, the AS-interface safety monitor returns to protective operation.

⚠ WARNING

LOSS OF CONTROL

• The designer of any control scheme must consider the potential failure modes of control paths and, for certain critical control functions, provide a means to achieve a safe state during and after a path failure. Examples of critical control functions are emergency stop and overtravel stop.

• Separate or redundant control paths must be provided for critical control functions.

• System control paths may include communication links. Consideration must be given to the implications of unanticipated transmission delays or failures of the link. [a]

• Each implementation of an ASi Safe Safety Monitor and its associated components must be individually and thoroughly tested for proper operation before being placed into service.

Failure to follow these instructions can result in death, serious injury, or equipment damage.

[a] For additional information, refer to NEMA ICS 1.1 (latest edition), “Safety Guidelines for the Application, Installation, and Maintenance of Solid State Control” and to NEMA ICS 7.1 (latest edition), “Safety Standards for Construction and Guide for Selection, Installation and Operation of Adjustable-Speed Drive Systems”.

Edition: 10/2006

10.5 Replacing a malfunctioning AS-interface safety monitor

⚠ DANGER

ELECTRIC SHOCK HAZARD

Disconnect all power before servicing equipment.

Failure to follow this instruction will result in death or serious injury.

If an AS-interface safety monitor is malfunctioning and must be replaced, the replacement device does not necessarily need to be reconfigured using the **ASISWIN2** software. It is possible instead to transfer the configuration from the malfunctioning device to the replacement device using the download cable (optional accessory).

Requirements:

- A download cable must be available (see accessories in chapter 3.4).
- The replacement device must not have a valid configuration stored in its configuration memory.

Note: If an AS-interface safety monitor which was previously used somewhere else is now to be used as a replacement device, you must replace the existing old configuration with a new configuration which, however, you should not validate.

AS-interface safety monitor version < V2.12:

Proceed as follows:

- Disconnect the malfunctioning AS-interface safety monitor from the supply.
- Use the download cable (RJ45/RJ45) to connect the malfunctioning device to the replacement device.
- Apply the supply voltage to the replacement device.
- The configuration of the malfunctioning device is now automatically transferred to the replacement device.
  Active transmission is indicated by the continuous illumination of the yellow **READY** LED. Conclusion of a successful transmission is indicated by the continuous illumination of the yellow **READY** LED and the green **ON** LED.
- Disconnect the new AS-interface safety monitor from the supply and disconnect the download cable from both devices. The replacement device can now directly be used in the place of the malfunctioning device.

AS-interface safety monitors version ≥ V2.12:

Proceed as follows:

- Disconnect the malfunctioning AS-interface safety monitor from the supply and uninstall it.
- Install the new AS-interface safety monitor and connect it (connections L+, M and FE as well as AS-i+ and AS-i- as well as additional connections as necessary).
- Switch on the supply voltage for the new AS-interface safety monitor. The AS-interface safety monitor enters configuration operation.

Edition: 10/2006

- Connect the malfunctioning AS-interface safety monitor, which is not connected to voltage, to the new AS-interface safety monitor via the download cable (RJ45/RJ45) and press the **Service** button.
- The AS-interface safety monitor restarts (LED test) and the configuration is transferred. During transfer, the **1 READY** yellow LED illuminates.
- When the **1 READY** yellow LED goes out, transfer has concluded. Disconnect the two AS-interface safety monitors from one another and press the **Service** button again.
- The AS-interface safety monitor restarts and now operates with the transferred configuration.

⚠ WARNING

LOSS OF CONTROL

• The designer of any control scheme must consider the potential failure modes of control paths and, for certain critical control functions, provide a means to achieve a safe state during and after a path failure. Examples of critical control functions are emergency stop and overtravel stop.

• Separate or redundant control paths must be provided for critical control functions.

• System control paths may include communication links. Consideration must be given to the implications of unanticipated transmission delays or failures of the link. [a]

• Each implementation of an ASi Safe Safety Monitor and its associated components must be individually and thoroughly tested for proper operation before being placed into service.

Failure to follow these instructions can result in death, serious injury, or equipment damage.

[a] For additional information, refer to NEMA ICS 1.1 (latest edition), “Safety Guidelines for the Application, Installation, and Maintenance of Solid State Control” and to NEMA ICS 7.1 (latest edition), “Safety Standards for Construction and Guide for Selection, Installation and Operation of Adjustable-Speed Drive Systems”.

Edition: 10/2006

10.6 What to do if you forget the password

⚠ WARNING

LOSS OF VALID CONFIGURATION

-Only the responsible safety officer is permitted to retrieve a lost password in the way described below.

-Accessing the configuration stored in the AS-interface safety monitor can affect the reliability of the system. Changes to validated configurations should only be made by authorized personnel. All changes must be made in accordance with the instructions given in the user manual supplied with the ASISWIN2 configuration software.

Failure to follow these instructions can result in death, serious injury, or equipment damage.

If you have lost the password for your configuration, proceed as follows:

1. Find the valid configuration log (printout or file) of the AS-interface safety monitor for which you no longer have a password. In the configuration log, find a four-digit code in line 10 (Monitor Section, Validated).
   - If the configuration log is unavailable and the AS-interface safety monitor is not to be switched to configuration operation, connect the AS-interface safety monitor for which you no longer have a password to the PC and start the **ASISWIN2** software.
   - Select a neutral configuration and start the diagnostic function in **ASISWIN2** with **Monitor -> Diagnose**. Now wait until the current configuration appears on the screen. This can take up to five minutes.
   - Open the **Information about monitor and bus** window (menu item **Edit -> Information about monitor and bus …**). In the **Title** tab you will again find the four-digit code in the **Download time** window area.
2. Contact the technical support department of your supplier and state the four-digit code.
3. A **master password** can be generated from this code. This password allows you to access to the stored configuration again.
4. Use the master password to stop the AS-interface safety monitor and to enter a new user password. To do so, select **Change password…** in the **Monitor** menu of the **ASISWIN2** configuration software.

Edition: 10/2006

⚠ WARNING

LOSS OF VALID CONFIGURATION

-Only the responsible safety officer is permitted to retrieve a lost password in the way described below.

-Accessing the configuration stored in the AS-interface safety monitor can affect the reliability of the system. Changes to validated configurations should only be made by authorized personnel. All changes must be made in accordance with the instructions given in the user manual supplied with the ASISWIN2 configuration software.

Failure to follow these instructions can result in death, serious injury, or equipment damage.

Note: If no valid configuration has yet been stored in the AS-interface safety monitor, the default password "SIMON" is valid.

Edition: 10/2006

Edition: 10/2006

11 Diagnostics via AS-interface

11.1 General procedure

Note: The assignment of an AS-interface slave address for the AS-interface safety monitor is a prerequisite for diagnosing the AS-interface safety monitor on the AS-interface master.

Using the AS-interface bus, diagnosis of the AS-interface safety monitor and configured devices is possible from the AS-interface master, normally a PLC with master module.

However, to ensure reliable transmission and efficient evaluation of the diagnostic data, a series of requirements must be satisfied:

- Relatively long code sequence propagation times may occur, particularly when using an additional bus system between PLC and AS-interface. Owing to the asynchronous transmission in the master in the case of two successive, identical data calls, the PLC may not necessarily know when the AS-interface safety monitor is responding to the new call. Thus, the answers to two successive, different data calls should differ by at least one bit.
- The diagnostic data must be consistent, i.e. the status information sent by the AS-interface safety monitor must match the actual device states, especially if the propagation time to the PLC is longer than the updating time in the AS-interface safety monitor (approx. 30 … 150ms).
- Whether a deactivated relay of an output circuit represents the normal state depends on the operating mode of the AS-interface safety monitor. The diagnostics in the PLC should only be called in the event of a deviation from the normal state.

The diagnostic procedure described below satisfies these requirements and should therefore always be followed.

Diagnostic procedure

The PLC always queries the AS-interface safety monitor alternately with two data calls (0) and (1). These data calls return the basic information (state of the output circuits, protective/configuration operation) to allow a diagnosis. The AS-interface safety monitor answers the two calls with the same user data (3 bit, D2 … D0). Bit D3 is a control bit, similar (but not identical) to a toggle bit. D3 is 0 for all even data calls (0); D3 is 1 for all odd data calls (1). This enables the PLC to detect whether the answer has changed.

Data calls (0) and (1) return the answer X000 if the normal state exists (protective operation, everything OK). For devices with only one output circuit and with two dependent output circuits, output circuit 2 is always marked as OK. With two independent output circuits, an unconfigured circuit is also marked as OK. In order to be able to interpret what is OK and what is not OK, the user must be familiar with his configuration.

If the data call changes from (0) to (1), the data set is stored in the AS-interface safety monitor. Bit D3 in the answer, however, remains reset until the process is concluded. As a result, the PLC thinks it has received answers to data call (0). If D3 is set, a consistent data set exists.

If, with the bit D3 set, the answer from the AS-interface safety monitor signals deactivation of an output circuit, detailed diagnostic information can now be queried in the stored state with the specific data calls (2) … (B). Depending on the setting in the configuration of the AS-interface safety monitor, data

Edition: 10/2006

calls (4) … (B) return device diagnostic information sorted according to output circuit (see section 11.2.2) or unsorted (see section 11.2.3).

Note: If the AS-interface safety monitor is in configuration operation, it is not possible to query the detailed diagnostic information using the data calls (2) … (B).

A fresh data call (0) cancels the stored state again.

11.2 Code sequence

11.2.1 Diagnosis of AS-interface safety monitor

State of output circuits, operating mode

Note: The alternate sending of data calls (0) and (1) is essential for consistent data transmission. See “Diagnostic procedure” on page 49.

The **binary values of the data calls relate to the AS-interface level** and may possibly be inverted at PLC level.

Data call / Value	Answer D3 … D0	Meaning
(0) / 1111 State of monitor	0000	Protective operation, everything OK (unavailable, unconfigured or dependent output circuits are displayed as OK).
	0001	Protective operation, output circuit 1 off.
	0010	Protective operation, output circuit 2 off.
	0011	Protective operation, both output circuits off.
	0100	Configuration operation: Power On.
	0101	Configuration operation
	0110	Reserved / not defined
	0111	Configuration operation, fatal device error, RESET or device exchange required.
	1XXX	No up-to-date diagnostic information available, please wait.

Edition: 10/2006

Data call / Value	Answer D3 … D0	Meaning
(1) / 1110 Store diagnostic information (state of monitor)	1000	Protective operation, everything OK (unavailable, unconfigured or dependent output circuits are displayed as OK).
	1001	Protective operation, output circuit 1 off.
	1010	Protective operation, output circuit 2 off.
	1011	Protective operation, both output circuits off.
	1100	Configuration operation: Power On.
	1101	Configuration operation
	1110	Reserved / not defined
	1111	Configuration operation, fatal device error, RESET or device exchange required.

State of device LEDs

Data calls (2) and (3) return a simplified indication of the output circuit LEDs (see chapter 8.2) on the AS-interface safety monitor.

If answer to data call (1) = 10XX:

Data call / Value	Answer D3 … D0	Meaning
(2) / 1101 State of LEDs of output circuit 1	0000	Green = contacts of output circuit closed
	0001	Yellow = startup/restart-disable active
	0010	Yellow flashing or red = contacts of output circuit open
	0011	Red flashing = error on level of the monitored AS-interface components
	01XX	Reserved

Data call / Value	Answer D3 … D0	Meaning
(3) / 1100 State of LEDs of output circuit 2	1000	Green = contacts of output circuit closed
	1001	Yellow = startup/restart-disable active
	1010	Yellow flashing or red = contacts of output circuit open
	1011	Red flashing = error on level of the monitored AS-interface components
	11XX	Reserved

Edition: 10/2006

Colour coding

Note: The colour of a device corresponds to the colour of the virtual LEDs in the diagnostic view of the **ASISWIN2** configuration software. A device which is not assigned to any output circuit is always shown in green.

Code CCC (D2 … D0)	Colour	Meaning
000	green, continuous	Device is in the ON state (switched on)
001	green, flashing	Device is in the ON state (switched on), but already in the process of being switched to the OFF state, e.g. switch-off delay
010	yellow, continuous	Device is ready, but is still waiting for another condition, e.g. local acknowledgement or start button
011	yellow, flashing	Time condition exceeded, action must be repeated, e.g. synchronisation time exceeded
100	red, continuous	Device is in the OFF state (switched off)
101	red, flashing	The error lock is active, release by means of one of the following actions: • Acknowledge with the service button • Power OFF/ON • AS-interface bus OFF/ON
110	grey, off	No communication with the AS-interface slave

Table 11.1: Colour coding

Note: During proper protective operation, there are also devices which are not in the green state. When searching for the cause of a shutdown, the device with the lowest device index is the most important. Others may just be subsequent effects (example: when the emergency shutdown button is pressed, the start device and timer are also in the OFF state).

By appropriately programming the functional component in the PLC, the user can be guided to the primary cause of the error. Detailed knowledge of the configuration and the function of the AS-interface safety monitor are necessary for the interpretation of additional information.

Because the device numbers can be shifted if the configuration is changed, we recommend using the diagnosis index assignment.

Edition: 10/2006

11.2.2 Diagnosis of devices, sorted according to OSSD

With the appropriate configuration setting, data calls (4) … (B) return device diagnostic information sorted according to output circuit.

Note: Make sure that the correct diagnosis type is set for the AS-interface safety monitor in the **Information about monitor and bus** window of the **ASISWIN2** configuration software.

The values returned in calls (5) and (6) as well as (9) and (A) refer to the device diagnosis index in the configuration program and not to an AS-interface address.

Always execute data calls (4) … (7) and (8) … (B) together in sequence for each device.

Sorted device diagnosis, output circuit 1

If answer to data call (1) = 10X1:

Data call / Value	Answer D3 … D0	Meaning	
(4) / 1011 Number of devices not green, output circuit 1	0XXX	XXX = 0: XXX = 1 … 6: XXX = 7:	no devices, answers to data calls (5) … (7) not relevant. number of devices in output circuit 1 number of devices is > 6 in output circuit 1

Data call / Value	Answer D3 … D0	Meaning	
(5) / 1010 Device address HIGH, output circuit 1	1HHH	HHH = I5,I4,I3:	diagnosis index of device in output circuit 1 of configuration (HHHLLL = diagnosis index)

Data call / Value	Answer D3 … D0	Meaning	
(6) / 1001 Device address LOW, output circuit 1	0LLL	LLL = I2,I1,I0:	diagnosis index of device in output circuit 1 of configuration (HHHLLL = diagnosis index)

Data call / Value	Answer D3 … D0	Meaning
(7) / 1000 Colour of device, output circuit 1	1CCC	CCC = colour (see table 11.1 on page 52)

Edition: 10/2006

Sorted device diagnosis, output circuit 2

If answer to data call (1) = 101X:

Data call / Value	Answer D3 … D0	Meaning	
(8) / 0111 Number of devices not green, output circuit 2	0XXX	XXX = 0: XXX = 1 … 6: XXX = 7:	no devices, answers to data calls (5) … (7) not relevant. number of devices in output circuit 2 number of devices is > 6 in output circuit 2

Data call / Value	Answer D3 … D0	Meaning	
(9) / 0110 Device address HIGH, output circuit 2	1HHH	HHH = I5,I4,I3:	diagnosis index of device in output circuit 2 of configuration (HHHLLL = diagnosis index)

Data call / Value	Answer D3 … D0	Meaning	
(A) / 0101 Device address LOW, output circuit 2	0LLL	LLL = I2,I1,I0:	diagnosis index of device in output circuit 2 of configuration (HHHLLL = diagnosis index)

Data call / Value	Answer D3 … D0	Meaning
(B) / 0100 Colour of device, output circuit 2	1CCC	CCC = colour (see table 11.1 on page 52)

Note: Data calls (C) 0011 to (F) 0000 are reserved.

Edition: 10/2006

11.2.3 Diagnosis of devices, unsorted

With the appropriate configuration setting, data calls (4) … (B) return unsorted device diagnostic information for all devices.

Note: Make sure that the correct diagnosis type is set for the AS-interface safety monitor in the **Information about monitor and bus** window of the **ASISWIN2** configuration software.

The values returned in calls (5) and (6) as well as (9) and (A) refer to the device diagnosis index in the configuration program and not to an AS-interface address.

Always execute data calls (4) … (7) and (8) … (B) together in sequence for each device.

Unsorted device diagnosis, all devices

If answer to data call (1) = 1001, 1010 or 1011:

Data call / Value	Answer D3 … D0	Meaning	
(4) / 1011 Number of devices not green, continuous	0XXX	XXX = 0: XXX = 1 … 6: XXX = 7:	no devices, answers to data calls (5) … (7) not relevant. number of devices not green. number of devices not green is > 6 (for colours, see table 11.1 on page 52).

Data call / Value	Answer D3 … D0	Meaning	
(5) / 1010 Device address HIGH	1HHH	HHH = I5,I4,I3:	diagnosis index of device of configuration (HHHLLL = diagnosis index).

Data call / Value	Answer D3 … D0	Meaning	
(6) / 1001 Device address LOW	0LLL	LLL = I2,I1,I0:	diagnosis index of device of configuration (HHHLLL = diagnosis index).

Data call / Value	Answer D3 … D0	Meaning
(7) / 1000 Colour of device	1CCC	CCC = colour (see table 11.1 on page 52).

Data call / Value	Answer D3 … D0	Meaning
(8) / 0111	0XXX	not used

Edition: 10/2006

Data call / Value	Answer D3 … D0	Meaning
(9) / 0110 Device address HIGH	1HHH	HHH = I5,I4,I3: diagnosis index of device of configuration (HHHLLL = diagnosis index).

Data call / Value	Answer D3 … D0	Meaning
(A) / 0101 Device address LOW	0LLL	LLL = I2,I1,I0: diagnosis index of device of configuration (HHHLLL = diagnosis index).

Data call / Value	Answer D3 … D0	Meaning
(B) / 0100 Assignment to output circuit	10XX	XX = 00: device from pre-processing XX = 01: device from output circuit 1 XX = 10: device from output circuit 2 XX = 11: device from both output circuits

Note: Data calls (C) 0011 to (F) 0000 are reserved.

Edition: 10/2006

11.3 Example: Querying with diagnosis sorted according to OSSD

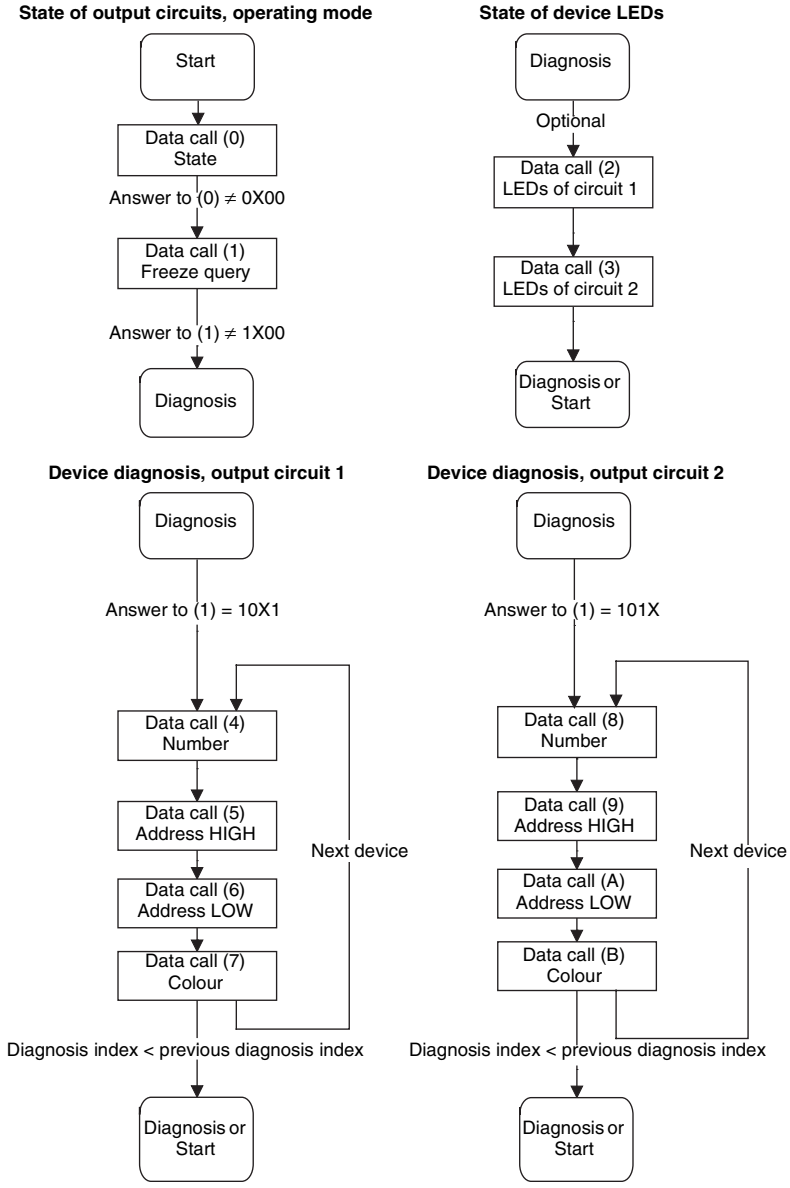


Figure 11.1: Querying with diagnosis sorted according to output circuit

Edition: 10/2006

12 Safe Bus Systems with AS-Interface

The expansion of AS-interface for safe functions is based on the EN 50295 standardised system which takes into consideration the networking of binary-switching sensors and actuators.

No changes or expansions to the standard transmission system were necessary, instead, additional safe components can be integrated into an existing system. Mixed operation of operational and safe functions is possible within one system.

AS-interface is also designed for binary-switching components in safety applications. Instead of the 8 bits of I/O data available in the system, now only 1 bit of safe user data is transmitted for each slave. For example, in the case of an emergency shutdown switch the information "switch activated" or "switch not activated" is transmitted.

Applications of up to controller category 4 acc. to EN 954-1 [2] are possible.

12.1 General description

The safe functions are described in detail below. The description of the standard system goes only into as much detail as is necessary for the understanding of the corresponding measures which regard safety.

For detailed information on the standard AS-interface system, refer to the AS-interface manual [3] and the corresponding standard EN 50295 [1][1].

New expansions, such as the operation of 62 slaves in one system, have also been included in Version 2.1 of the AS-interface specification [4].

With AS-interface, up to 31 or 62 slaves communicate via a 2-conductor line with one master. This master controls the exchange of information and exchanges all relevant data of the system with the so-called host. The primary system component is referred to as the host. This is most often a PLC, an industrial PC or a coupler to a primary fieldbus such as INTERBUS or PROFIBUS. The master is generally realised as one of the components of the host system, e.g. as a plug-in card in a PLC.

1. Information is also available in the Internet under **http://www.as-interface.net**.

Edition: 10/2006

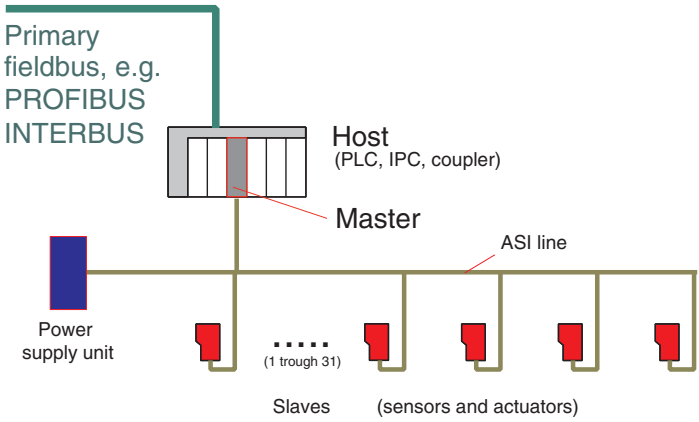


Figure 12.1: AS-interface system overview

The system, as shown in figure 12.1, is supplied via a specific power supply unit, which also contains the required data coupling. Information and power are both transmitted via a shared two-wire line with a minimum cross section of 1.5mm^2, whereby the sum of all line sections may have a maximum length of 100m (328.08 ft) and the cycle time for the information exchange is 5ms when the system is fully expanded.

The primary advantage is a considerable reduction in the installation work required for the binary sensors and actuators on the process level, i.e. in the general scope of industrial automation. The AS-interface electromechanics make it possible to wire using a special two-wire ribbon cable on the basis of clamping technology (here, the connections of the subscriber clamp onto the ribbon cable). This also leads to improved and simplified diagnosis of the participating sensors and actuators as well as simplified expansion, thanks to the fact that the topology of the constructed network can be freely selected.

Since it was introduced to the market in 1994, when used with one of the over 2 million slave ICs sold in the past years the system has proven itself through actual operation, in particular with regard to the EMC requirements for components and systems used in the field of industrial automation.

With expanded safety functionality, the user now also has available the aforementioned advantages with the same system design for safe components in one continuous technology. The second wiring system, which was previously required for the diagnosis of the switching state of safe components, is no longer necessary as the AS-interface system makes the diagnostic information available in the host, usually a non-safe PLC, at no additional cost.

Thus, it is possible to integrate up to 31 safe slaves into one system, whereby applications of up to controller category 4 acc. to EN 954-1 with a maximum system reaction time of 40ms are possible.

Edition: 10/2006

12.2 Transmission-specific hardware structure of the bus subscribers

We begin with a system having the structure of the standard system acc. to figure 12.1, consisting of one master with up to 31 slaves.

Note that according to [4], Version 2.1 of the AS-interface specifications, up to 62 so-called A/B slaves can also be operated in a system. This does not affect the expansion of safety functionality as the maximum number of safe slaves remains limited to 31 when expanded to its maximum. For example, in a system with 5 safe slaves, either an additional 26 standard slaves or 52 A/B slaves acc. to [4] can be operated.

In so-called normal operation of the master with data exchange and management phases, 4 bits of output data (4O) are passed to all slaves in addition to the slave address during the data exchange phase by means of a master call. The affected slave responds with a slave answer as shown in figure 12.2 after receiving a call from the master, transmitting 4 bits of input data (4I) in the process. Thus, each slave exchanges a total of 8 bits of user data with the master.

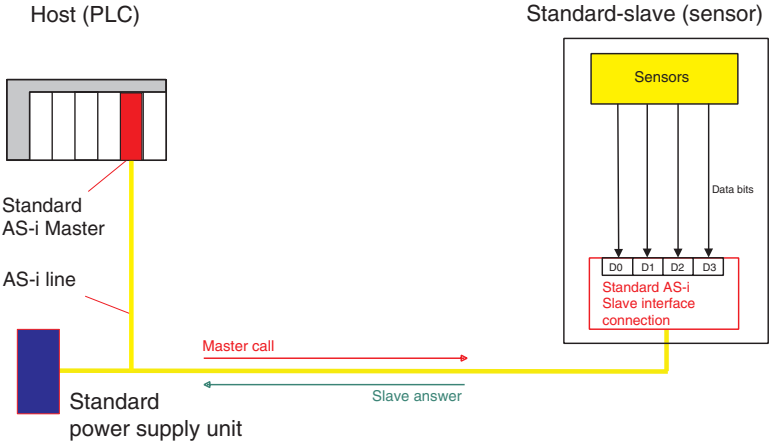


Figure 12.2: Data exchange in standard operation

The master itself determines the sequence of the calls. During the data exchange phase, all slaves are queried in ascending address order.

This process, also known as master-slave polling, is continuously repeated during so-called cyclical normal operation of the master. A message from the management phase follows the up to 31 messages of the data exchange phase before the next data exchange phase begins.

If the master detects an error in a message during the data exchange phase, this message is repeated immediately.

All of the mentioned mechanisms also apply unchanged to the expansion of the safety functionality. Thus, each specification-conformant AS-interface master can also be used unchanged with safe components in the system seeing as the master itself does not count as one of the safe components: in addition to the safe slaves, the only additional component required in the system is a safety monitor.

Edition: 10/2006

As the name implies, this component does not interfere in the data traffic between the master and slaves. As shown in figure 12.3, it only monitors the traffic and uses it to determine the switching state of each individual safe slave.

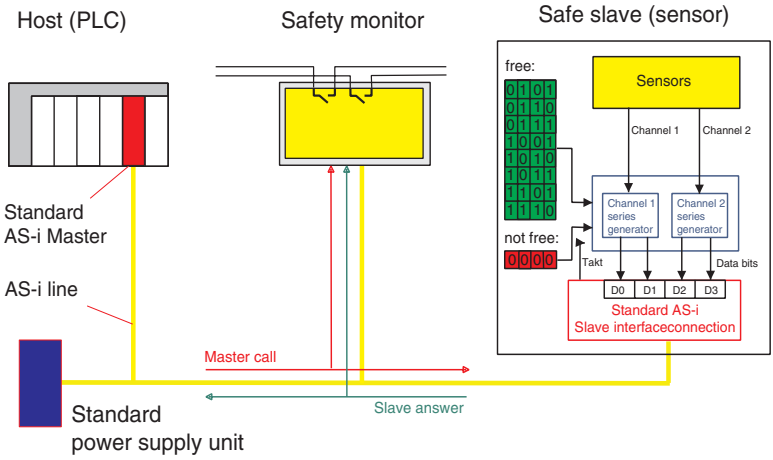


Figure 12.3: Safe data exchange

The switching state of all safe slaves is included in the safe process image of the safety monitor and is made available in a safety-oriented manner to units connected downstream.

The first realisation of a safety monitor is designed as an independent device and contains one unit as a downstream element. This unit performs a corresponding linking of the information of the process image and engages via relays with the conventionally structured, safe control circuit (e.g. an emergency shutdown circuit).

Edition: 10/2006

figure 12.4 shows the block diagram of the safety monitor, figure 12.5 the structure of a system with operational and safe components.

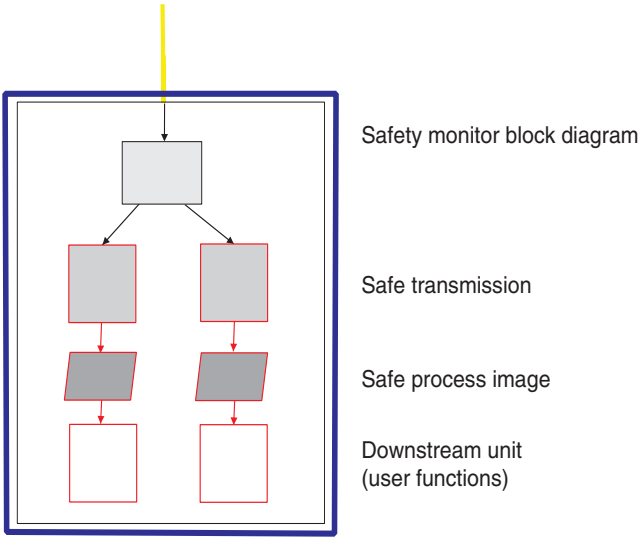


Figure 12.4: Safety monitor block diagram

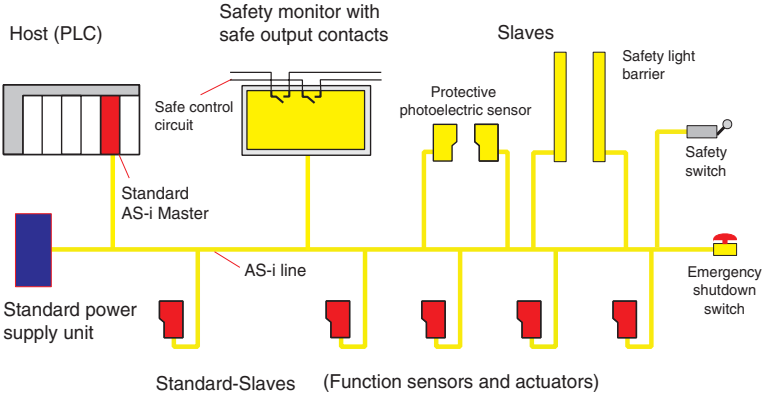


Figure 12.5: System design with safety monitor

The downstream unit can, acc. to figure 12.6, also be realised as an interface to a primary, safe field-bus system such as PROFISAFE or SafetyBus p. In this case, the safe process image of a primary safe controller is made available.

Edition: 10/2006

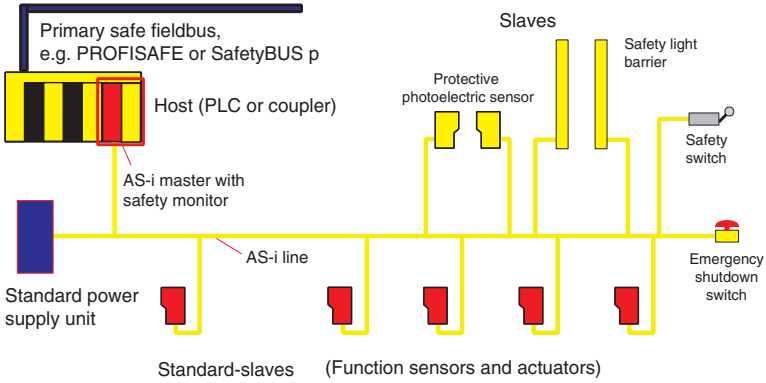


Figure 12.6: System design with safe host

If the master and safety monitor are arranged together in one unit as shown in figure 12.6, it is also possible to operate safe binary-switching actuators via the AS-interface line. A safe controller must then make available as a safe source the switching information for the actuators. The safe controller is higher in the hierarchy than the master as well as the safety monitor.

This design is based on architecture model D acc. to [5]. Here, the AS-interface transmission system is not used as a safe transmission channel. The required safety is achieved through the mechanisms in the higher-order elements of the safe slaves and in the safety monitor.

Here, the safety is based on the dynamics and special coding of the transmitted information.

To achieve the required safety, special requirements are also placed on the following components:

1. Safe slave
   When setting up a safe slave, the separation of the code generator from the AS-interface IC described in chapter 12.3 must be ensured.

2. Safety monitor
   The safety monitor can pre-process the dynamic messages in a single channel. All other functions are relevant to safety and are to be designed accordingly.

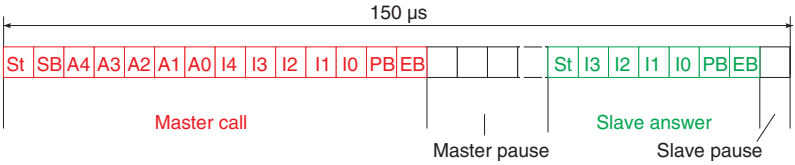
All other components of the system, such as master, power supply unit and operational slaves, are not classified as safety relevant.

Edition: 10/2006

12.3 Safe code sequence structure

The safe information is transferred via the non-safe transmission channel of the standard AS-interface. This is explained in chapter 12.2 and described in detail in [3].

A 14-bit-wide master call follows a 7-bit-wide slave answer after a slave pause. The meanings of the individual bits can be found in figure 12.7. The digital signals pending at the inputs are then cyclically read in and transmitted. If a signal is pending statically, it is read back in on each cycle and the constant value transmitted again on every cycle.



St	= Start bit (= 0)		
SB	= Control bit		
A4 ... A0	= Slave address (5 bits)	St	= Start bit (= 0)
I4 ... I0	= Information (5 bits)	I3 ... I0	= Information (4 bits)
PB	= Parity bit	PB	= Parity bit
EB	= End bit (= 1)	EB	= End bit (= 1)

Figure 12.7: Meanings of the bits in the master call and slave answer

For the safe transmission, the same transmission mechanism applies, i.e. the 4-bits of information pending at the AS-interface IC of the slave are transmitted. From a transmission perspective, information is transmitted from the master to the slave and back. The flow of information relevant to safety, however, occurs from the slave to the safety monitor which "listens" and monitors all information exchange. The safe user data are defined as follows here:

- Only 1 bit of user information is transmitted. The two possible states have the meanings **free** (=1) and **not free** (=0).
  Example:
  emergency shutdown not activated == **free** ("unsafe motion enabled")
  emergency shutdown activated == **not free** ("unsafe motion disabled")
- In the state **not free**, the value (0,0,0,0) is statically applied to the 4 input bits of the slave-IC.
- In the state **free**, a different value is applied to the 4 input bits with each cycle. The values represent a series of 8 pairs of different 4-bit values, where each slave in the system has its own unique series.
  The series is stored in a slave's code table and is to be generated according to defined rules. It is assigned by the manufacturer, whereby several series may be stored for each slave. The user can then select one of the predefined series prior to commissioning.
  An example of a valid series can be seen in figure 12.3.

Edition: 10/2006

- In its safe process image, the monitor sets for each slave one of the three states **free**, **not free** or **error**.

  not free .... In this state, the slave is passed over upon reception of a value (0,0,0,0).

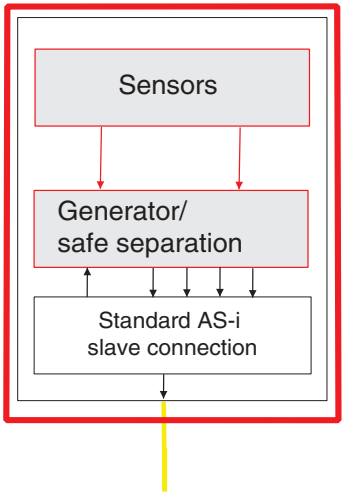
  free .... In this state, the slave is passed over when the value (0,0,0,0) has been received at least 8x in sequence and then the correct value of the series is received 9 times in sequence.

  error .... After detecting a violation in the rules for safe transmission, e.g. after receiving an impermissible 4-bit value or when no correct series value has been received for an impermissibly long time.

As a result of a reduction of the user data, it is from a safety standpoint only necessary to differentiate between the states **free** and **not free**.

The state **free**, which enables the unsafe movement, is represented by the dynamically changed information in such a way that a possible error in the transmission channel can be reliably detected, preventing the unsafe motion from being enabled.

While the value (0,0,0,0) is statically transmitted in the state **not free**, a different value must be transmitted with each cycle in the state **free**. According to figure 12.8, the code generator makes available the appropriate value of a series at the AS-interface IC for take-over. With each cycle that is detected via the data strobe signal of the AS-interface IC (DSTB, see. [3]), the code generator first determines the next value of the series and makes it available for take-over. The transmitted value is then compared with the expected value in the safety monitor. If the values deviate from one another, a safe shutdown is performed.



Safe slave
block diagram

Figure 12.8: Block diagram of safe slave with two-channel safety component

The monitor knows what value to expect following the teach-in to be performed during commissioning. The teach-in is described in chapter 12.6.

Edition: 10/2006

The process is continuously repeated. If, however, the safe component switches to the state **not free**, the value (0,0,0,0) is then immediately transmitted statically, resulting in an immediate shutdown.

The structure of a safe slave must ensure that when in the state **not free** the output of the code generator be safely separated from the input of the AS-interface slave ICs and that if the value is not (0,0,0,0), the value pending at the AS-interface IC input at least be a static value.

A peculiarity is taken into account for the case when safe coupler modules are used to couple conventionally designed safe components to the AS-interface. In this case, the safe slave is located in the coupler module. As the conventional component with the appropriate safety category is to be coupled using two-channels, the static errors of a channel, such as contact welding or short-circuits between contacts, must be detected reliably.

If, as shown in Block diagram of safe slave with two-channel safety component, two bits per channel are now separated during the safe separation of the code generator from the AS-interface IC, the shutdown occurs only via two of the four used bits in the case of contact welding. The safety monitor detects the situation using the transmitted values, switches off safely and blocks restarting of the system.

Moreover, in addition to the requirements on the design, the safe slaves must meet the required residual error rate for the following described errors:

1. Faulty start:
   Transmission errors and other disturbances must not at any time result in the switching from the state **not free** to the state **free**.

2. Failed shutdown:
   The transition from the state **free** to the state **not free** must occur within the maximum reaction time, even when transmission errors, disturbances and other external influences arise during the switching process.

12.4 Measures against transmission errors

The transmission of the safe user data is, as explained, based on the transmission of the standard system. For this reason, the mechanisms against transmission errors contained in the standard system should be considered in the first step. A distinction is made here between measures for the suppression of disturbing influences and those for the detection of errors caused by disturbances.

AS-interface has been designed and developed for use in the process level of industrial automation. The appropriate environmental requirements have, thus, been taken into consideration in the system. The task to develop a system for the transmission of power and information via a two-wire, non-twisted-conductor ribbon cable in the very electromagnetically noisy industrial environment has been fulfilled with a logical, symmetrically structured system. It has been shown that the common-mode rejection resulting in the symmetrically structured system provides the required interference rejection. Thus, a properly designed network can achieve results which surpass the interference rejection achieved in conventionally designed systems.

A condition here is also a safe separation in the power supply unit acc. to PELV.

To avoid transmission errors, all relevant conditions regarding EMC have, moreover, been defined in the AS-interface specification based on IEC 61000 [6]. Detailed prototype tests, which are to be performed within the framework of product certification by the AS-International Association, ensure con-

Edition: 10/2006

formity with the specifications.

The information transfer shown in [3] uses a Manchester encoding which contains the primary features for detecting errors.

The primary mechanisms for detecting errors are:

- Parity check in master request and slave answer
- Alternating rule in the encoding
- code sequence-length monitoring
- Pause monitoring

Overall, the system has proven itself over years of operation and has generally been accepted due to its high availability. The rates of detected errors measured in test systems are, in proper operation, in the range of less than 10 errors/h based on past experiences. This corresponds to a bit error probability of $P_{bit} < 10^{-7}$ and shows that the selected error suppression contributes significantly to the high availability of the system.

The mechanisms implemented in the master for the repetition of messages in the event of detected errors have an added benefit. Namely, that, assuming uniform distribution of the errors, the system theoretically remains available up to a bit error probability of $P_{bit} = 4.7 \bullet 10^{-2}$ when all components in the system function properly.

As mixed operation is permitted on one line, the same conditions with regard to the transmission channel apply for operational and safe functions. As the information transmission is made dynamic, additional measures are, however, available for the safe transmission which ensure that the safety requirements are met even if all safety measures of the standard system should fail.

In particular, it is shown in chapter 12.5 that the resulting residual error rate lies below the threshold required for SIL 3 acc. to IEC 61508.

Moreover, it can easily be shown that the transmission system errors detailed in [5], such as message repetition, loss, insertion, reversal, falsification and delay, can be controlled with the dynamisation mechanisms.

12.5 Determining the residual error probability

The residual error probability is determined using methods based on those described in [5].

For certification acc. to SIL 3 in accordance with IEC 61508 [7] or controller category 4 acc. to EN 954-1 [2] this requires that a residual error rate Λ with $\Lambda < 10^{-9}$ /h be achieved, i.e. one single undetected error every 10^9 hours of operation.

For systems with strictly informational data integrity checks, such as CRC or similar measures, the scenario can be based on known procedures. For AS-interface, however, the entire system must be considered as a special case. The points listed in chapter 12.3 are to be considered as particularly safety-relevant, critical cases. The probability of their occurrences is to be determined:

Edition: 10/2006

Unsafe start-up

The safe slave statically transmits a series (0,0,0,0). As the result of an appropriate error on the transmission path, the receiver however receives the series for activation. The receiver then switches the slave to **free** in the process image and thus enables the unsafe motion.

Failed shutdown

At the moment that the safe slave initiates the shutdown process and statically transmits the series (0,0,0,0) instead of the dynamic series, the transmission is falsified in such a way that the dynamic series is correctly continued at the receiver. The state **free** is retained in the process image and the shutdown process thus does not occur.

Increased bit error rate

If the safety mechanisms of the standard system are not working, massive disturbances induced on the bus line increase the residual error rate through continuously occurring bit errors.

A detailed examination was able to prove that the mentioned error cases satisfy the requirements acc. to SIL 3. Below, the calculation is only briefly outlined and explained.

Regarding 1, unsafe start-up:

The errors possible during the start-up process are to be considered.

A safe slave is switched by the monitoring safety monitor to the state **free** when the following condition is fulfilled:

The entire series of the 8 pair-wise different values is cycled through correctly and the first received value is correctly received a second time, i.e. a total of 9 correct values of a series.

If, in a worst case scenario, only one set bit is required in order to achieve a correct value for a series, the probability that 9 correct values of a series, and thus residual error probability, can be estimated as

$P_{series} = P_{REP} < P_{bit}^{9}$.

Even with a bit error probability of 10^{-2}, the residual error rate Λ for unsafe start-up at a request rate of 1 Hz can be estimated with

$\Lambda < 10^{-13}$/h (per message).

(Comment: this scenario contradicts the rules for generating the code tables. Such a series cannot occur and is worse than any real series; "worse than worst case".)

Edition: 10/2006

Regarding 2, failed shutdown:

The errors possible during the shutdown process are to be considered.

If the dynamic series continues to be transmitted instead of the static series (0,0,0,0) required for shutdown, only one bit is to be falsified with the next element under worst-case conditions. According to the generation rules for the code table, however, at least two bits must be falsified in order for the next value to become a correct value. The falsification of an individual bit is again relevant to the third value of the series. In all, the probability that an error will result in the occurrence of a correct series can be approximated as follows:

$P_{series} = P_{REP} < 1/8 \bullet P_{bit}^4$.

With a bit error rate of $P_{bit} = 10^{-4}$ and a request rate of 1 Hz, the overall residual error rate is Λ according to [5]:

$\Lambda < 9 \bullet 10^{-10}/h$

Regarding 3, increased bit error rate:

According to [5] the bit error probability which is included in the calculation of the residual error rate is either to be proven or assumed to be $P_{bit} = 10^{-2}$.

An error counter may be used to estimate the expected residual error rate. If a certain error rate is exceed, a shutdown can thus be performed reliably.

The error monitoring used in the case of AS-interface is described in brief below:

As already explained, the bit error probabilities which correspond to the observed bit error rates, of correctly operated AS-interface systems are in the range of $P_{Bit} < 10^{-7}$. As a result, the bit error probability of 10^{-4} assumed for calculating the residual error rate exceeds the rate observed in correctly operated systems by a factor of 1000.

For the calculation of the residual error rate, it is assumed that all safety mechanisms of the standard system, in particular the Code Checker of the AS-interface slave ICs and of the master, are not functioning. Under these requirements, each error which occurs is passed on to the primary safety level of the safety monitor.

These errors are detected there with high probability as the majority of the transmitted bits are known in advance by the safety monitor. In this case, the received message would not match that which is expected. This applies to the values of the series transmitted by the slave as well as to the slave address passed by the master. This is because the safety monitor continuously monitors both the series as well as the increasing order of the addresses used in the master call.

Overall, it can be shown that the assumed bit rate errors used in the calculation of the residual error rate result in a detected error in the safety-monitor safe monitoring within a very short amount of time, resulting in a shutdown (see table 12.1):

Edition: 10/2006

P_{bit}	Shutdown time
10^{-4}	1s
10^{-2}	10ms

Table 12.1: Shutdown times and bit error probability

This means that for bit error rates of 10^{-4} or 10^{-2}, a shutdown occurs every second or every 10ms, respectively, values which are unacceptable on-site. It can, therefore, be assumed that the AS-interface is used only for bit error rates which are less than 10^{-7}. This corresponds to a shutdown every 1000s.

12.6 Commissioning/repair

In comparison to the commissioning of a standard AS-interface system described in [3], only a few additional steps are required. The following procedure is to be adhered to:

- Design the system with all components which are to be used.
- Optional: configure the master via the non-safe host (usually a PLC).
- Configure the safe portion by configuring the safety monitor.
- Assign the AS-interface slave addresses to operational and safe components.
- Switch on the voltage supply.
- Configure the master with the function "Configure actual configuration" (if not already configured via host).
- After entering AS-interface normal operation: teach the code tables of the safe components.
- Condition: all slaves must be in the **free** state.
  (e.g.: emergency shutdown must not be activated)
- Testing and documentation of all safety functions are to be completed by the responsible personnel.
- Validation of system operation.

If misoperation or failures occur in the system, primarily the following situations must be controlled in addition to the error cases known from the standard system:

1. Failure of a safe slave
   In this case, the affected component must usually be replaced. As duplicate code tables for the safe components are not permitted within a system, it must be assumed that the code table which happens to be contained in the replacement device is not the same as that of the malfunctioning slave. After replacing the device and assigning the AS-interface address, the code table of the slave must, therefore, be read back in by means of a teach process. If no other errors are present, the system can then be put back into operation.
2. Failure of the safety monitor
   If a safety monitor fails, it is absolutely necessary that the replacement component be configured exactly as the original component. This can be performed using two mechanisms:
   - Reloading the configuration into the new component from the configuration PC
   - Direct transmission of the configuration from the malfunctioning device if the specially protected configuration memory of the malfunctioning device has not been affected.

Edition: 10/2006

12.7 Availability

The availability of the safe functions of the bus system used in mixed operation is identical to the availability of the standard system.

As already shown, the majority of systems installed in the past years has proven that the high resistance of AS-interface against disturbances as determined in the laboratory provides an availability which is adequate for the requirements for use in industrial automation.

12.8 Manufacturers

The initial task was the development of a system concept for the safe expansion of the standard system by a working group of the AS-International Association. The concept includes all transmission mechanisms and represents the basis for all product developments. The system is, thus, open for a wide range of products from various manufacturers. The interoperability of all products can, therefore, be ensured.

The development of the first products was accelerated through the co-operative efforts of the interested companies. The safety monitor (the one additionally required component) was developed by a consortium of the following companies:

Bihl+Wiedemann, EJA, Euchner, Festo, Idec, ifm, Leuze, Omron, Pepperl+Fuchs, Pilz, Schmersal, Schneider electric, Sick, and Siemens

With regard to certification, two points are of particular importance for safe components on the AS-interface line:

- Certification with regard to interoperability with other AS-interface products by the AS-International Association.
- Certification with regard to the required controller category acc. to EN 954-1 by an accredited institute, for example TÜV or BIA.
- Certification acc. to IEC 61508 by an accredited institute, for example TÜV or BIA.

Edition: 10/2006

12.9 References

[1] DIN EN 50295,
Niederspannungsschaltgeräte - Steuerungs- und Geräte-Interface-Systeme - Aktuator Sensor Interface (AS-interface); Deutsche Fassung EN 50295: 1999-10
Low-voltage switchgear and controlgear - Controller and device interface systems - Actuator Sensor Interface (AS-interface); German version EN 50295: 1999-10

[2] DIN EN 954-1,
Sicherheit von Maschinen - Sicherheitsbezogene Teile von Steuerungen - Teil 1: Allgemeine Gestaltungsleitsätze; Deutsche Fassung EN 954-1: 1997-03
Safety of machinery - Safety-related parts of control systems - Part 1: General principles for design; German version EN 954-1: 1997-03

[3] Kriesel, Werner R.; Madelung, Otto W. (Hrsg.): AS-Interface. Das Aktuator-Sensor-Interface für die Automation. Auflage, Carl Hanser Verlag; München, Wien, 1999, ISBN 3-446-21064-4
The Actuator Sensor Interface for Automation. Published by Carl Hanser Verlag; Munich, Vienna, 1999, ISBN 3-446-21064-4

[4] Spezifikation des AS-Interface, ComSpec V2.1. AS-International Association (erhältlich bei AS-International Association, http://www.as-interface.net).
AS-Interface Specifications, ComSpec V2.1. AS-International Association (available from AS-International Association, http://www.as-interface.net).

[5] Vorschlag eines Grundsatzes für die Prüfung und Zertifizierung von "Bussystemen für die Übertragung sicherheitsrelevanter Nachrichten", Stand 29.2.2000.
Suggestion for fundamental testing and certification of "bus systems for the transmission of safety-relevant messages", 29.2.2000

[6] DIN EN 61000 in mehreren Teilen, Elektromagnetische Verträglichkeit (EMV)
DIN EN 61000 in several parts, electromagnetic compatability (EMC)

[7] IEC 61508 1-7, Functional safety of electrical/electronic/programmable electronic safety-related systems, 2000-05

[8] AS-Interface - Die Lösung in der Automation, Ein Kompendium über Technik, Funktion, Applikation (erhältlich, auch in englischer Sprache, bei AS-International Association, http://www.as-interface.net).
AS-Interface - The Automation Solution, A compilation of technology, functionality, applications (also available in English from AS-International Association, http://www.as-interface.net).

Edition: 10/2006

ASISMONDOC
10/2006

2GB/149/02
95471 12-GB

Printed in Germany