ABB MEASUREMENT & ANALYTICS | SAFETY INSTRUCTION | SI/AZ20/AZ30-EN REV. A

Endura AZ20 and Endura AZ30

Oxygen analyzer

Endura AZ20 & Endura AZ30 oxygen analyzer

Measurement made easy

Introduction

This manual provides information and instructions that will be needed in order to use the AZ20 or AZ30 in safety related applications. It is aimed at those responsible for planning, designing, installing, commissioning and maintaining safety related systems.

To avoid duplication, many of the standard procedures are not explained in this document. However, references are made to user guides, installation procedures and maintenance procedures with links to the source material.

Contents

1 Overview – versions with SIL available

AZ20 safe area oxygen analyzer

Figure 1 AZ20 remote version

Figure 2 AZ20 integral version

Identifier:
AZ20/xxxxxxxxxxxxx0xx/STD

AZ30 hazardous area oxygen analyzer

Figure 3 AZ30 remote version

Figure 4 AZ30 integral version

Identifier:
AZ30/xxxxxxxxxxxxxxx/STD

2 Acronyms and abbreviations

Safety Function

A defined function executed by a safety related system which is intended to achieve or maintain a safe state in respect of a specific hazardous event.

“Safe” Failure

A failure which forces the safety instrumented system into a spurious annunciation state. This is usually synonymous with the term “spurious trip”.

Dangerous Failure

A failure which has the potential to put the safety instrumented system in a dangerous or non-functioning state. This is usually synonymous with the term “failure to trip”

Type A Subsystems

A subsystem is Type A if all of the following are true:-
The failure modes of all components are well defined
The behaviour of the subsystem under fault conditions can be completely determined
There is sufficient dependable field failure data to show that the claimed failure rates for detected and undetected dangerous failures are met.

Hardware Fault Tolerance (HFT)

The ability to continue to provide a safety function in the presence of faults and errors. A hardware fault tolerance of N means that N+1 faults could cause the loss of a safety function.

Safe Failure Fraction (SFF)

The fraction of failures that does not have the potential to put the safety instrumented system in a dangerous or non-functioning state. This figure is sometimes expressed as a percentage.

PFD The probability of failure on demand

This is intended to apply to systems operating in a low demand mode where the safety function is required on average a maximum of once per year.

Proof Test

Periodic tests that are performed to detect failures so that, if necessary, the system can be restored to a fully working state.

Safety Integrity Level (SIL)

IEC 61508 defines four Safety Integrity Levels from SIL1 to SIL4. Each of these corresponds to a range of probabilities that the safety function will fail. The higher the SIL the lower the probability of failure and the greater the probability that the safety function will work when required to do so.
Table 1 on page 4 shows the dependency of the SIL on the probability of failure on demand (PFD for low demand mode of operation.

…2 Acronyms and abbreviations

…Safety Integrity Level (SIL)

Table 1 Safety Integrity Levels

Safety Integrity Level	Low demand mode of operation
4	≥ 10^{-5} to 10^{-4}
3	≥ 10^{-4} to 10^{-3}
2	≥ 10^{-3} to 10^{-2}
1	≥ 10^{-2} to 10^{-1}

3 Standards and definitions of terms

Standard IEC 61508 (2010), Part 1 and 2

Functional safety of electrical/electronic/programmable electronic safety-related systems (target group: manufacturers and suppliers of devices).

Dangerous failure

A failure that has the potential to place the safety-related system in a dangerous state or render the system inoperative.

Safety-related system

A safety-related system performs the safety functions that are required to achieve or maintain a safe condition, e.g., in a plant.

Example:
Pressure meter, logics unit (e.g., limit signal generator) and valve form a safety-related system.

Safety function

A specified function that is performed by a safety-related system with the goal, under consideration of a defined hazardous incident, of achieving or maintaining a safe condition for the plant.

Example:
Limit pressure monitoring.

4 Other applicable documents and papers

Table 2 AZ20 reference documents

Data Sheet Endura AZ20 oxygen analyser Combustion Gas Analysis	DS/AZ20-EN
Maintenance Guide Endura AZ20 oxygen analyser Combustion Gas Analysis	IM/AZ20M-EN
User Guide Endura AZ20 oxygen analyser Combustion Gas Analysis	IM/AZ20P-EN
Manual Endura AZ20 oxygen analyser Combustion Gas Analysis	IM/AZ20E-EN

Table 3 AZ30 reference documents

Data Sheet Endura AZ30 oxygen analyser Combustion Gas Analysis	DS/AZ30-EN
Maintenance Guide Endura AZ30 oxygen analyser Combustion Gas Analysis	MI/AZ30M-EN
User Guide Endura AZ30 oxygen analyser Combustion Gas Analysis	OI/AZ30P-EN
Programming Guide Endura AZ30 oxygen analyser Combustion Gas Analysis	COI/AZ30E-EN

5 Zirconia probe as part of the safety function system

The AZ20 or AZ30 transmitter generates an analog signal (4 to 20 mA) proportional to the oxygen % content. The analog signal is fed to a downstream logics unit such as a PLC or a limit signal generator, and is monitored for exceeding a specified maximum or minimum value.

The following elements of the detector are considered to be within the boundary of the safety system covered in this manual:

- AZ20 or AZ30 probe
- AZ20 or AZ30 transmitter
- Interconnecting cable (only applicable to remote transmitter versions)

The safe operation of anything else beyond the above components falls outside the scope of this document.

Note:
HART is not considered part of the SIL output

Device-specific data related to functional safety

Table 4 Device-specific data

Device type	**AZ20 oxygen analyzer AZ30 oxygen analyzer**
Type of assessment	IEC61508
Hardware type tolerance	0
Component type	B

Failure rates

Table 5 Failure rates

	High demand	**Low demand**
Safety integrity	SIL 1	SIL 2
“hazardous” failure (revealed)	0.28 10^{-2} per annum	3.11 10^{-6} per hour
“hazardous” failure (unrevealed)	2.72 10^{-2} per annum	3.22 10^{-7} per hour
“safe” failure (revealed)	0	0.54 10^{-6} per hour
“safe” failure (unrevealed)	0	0
Diagnostic coverage	>91 %	90.6 %
Safe failure fraction		>91 %
Probability of failure on demand		1.6 10^{-3}

…5 Zirconia Probe as part of the safety function system

…Failure rates

Notes:

1. Auto-diagnosed failures are assumed to be dealt within 48 hours. Undiagnosed failures are assumed to be revealed subject to a proof-test interval of one year.
2. The equipment is in virtually continuous use such that failure rates (based on 8760 hours per year) are applicable.

6 Functional safety compliance - prerequisites to operate the device

- The analog signal of the transmitter can be considered safe after 2 hours (warm up time), or after the heater output stabilizes (see signal view).
- A dangerous error is an error during which the output of the transmitter no longer responds to the input signal or deviates by more than 2 %.
- The maximum reaction time of the device on error is less than 10 minutes.
- Use of the device in a safety-related system is only permitted within the first 20 years after production of the device. This is a basis for the calculated failure rates.
- The ambient temperature for use in a safety-related system must be above –40 °C. The information according to the operating instructions applies to the upper limit of the ambient temperature.
- When using the device for the measurement of corrosive media, keep in mind the limitations referred to in the operating instructions or data sheet.
- Selection of the correct version of probe or transmitter is the operator’s responsibility.

7 Configuration

This document does not replace the standard installation manuals for the AZ20 or AZ30. For full details on how to safely install and configure AZ20 and AZ30 probes, please refer to the documentation listed in section 4 on page 5.
However, in this section are listed some areas that are not absolutely necessary for operation, but can affect the safety function.

Locking/unlocking the configuration level

SAFETY NOTE

Unauthorized changes of the parameter settings may affect the safety function.

Once configuration is completed, the device must be protected against unauthorized access.

Passwords can be set in **Device Menu > Security setup**.

Users with standard access can change the password for standard users and users with advanced access can set passwords for both standard and advanced users.

Security setup	Used to set Standard and Advanced level passwords of up to 6 alphanumeric characters. **Note**. Standard and Advanced passwords are not set at the factory and must be set by the end-user(s).	None
Standard	Set by Standard and Advanced users	
Advanced	Set by Advanced users	

Reset password

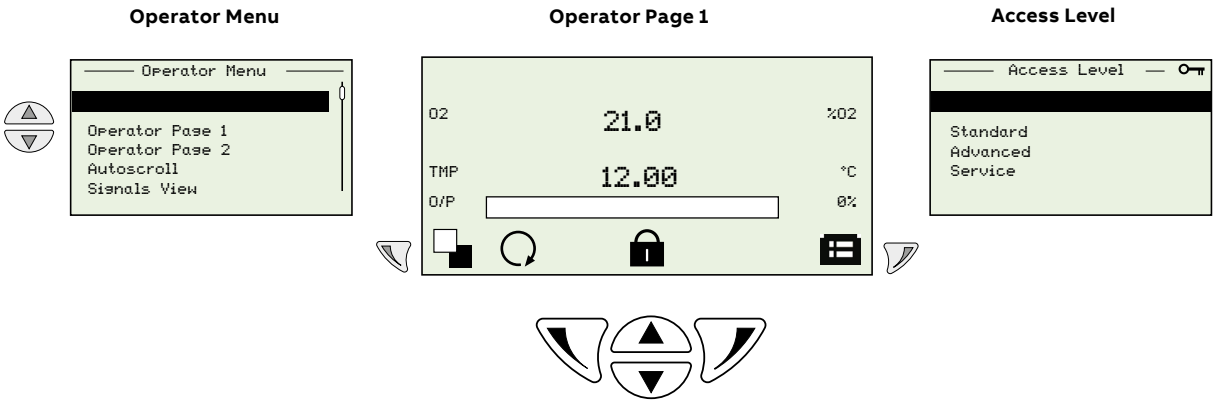
If the password has been forgotten, there is an option to reset it. Please refer to ABB to have your password reset.

...7 Configuration

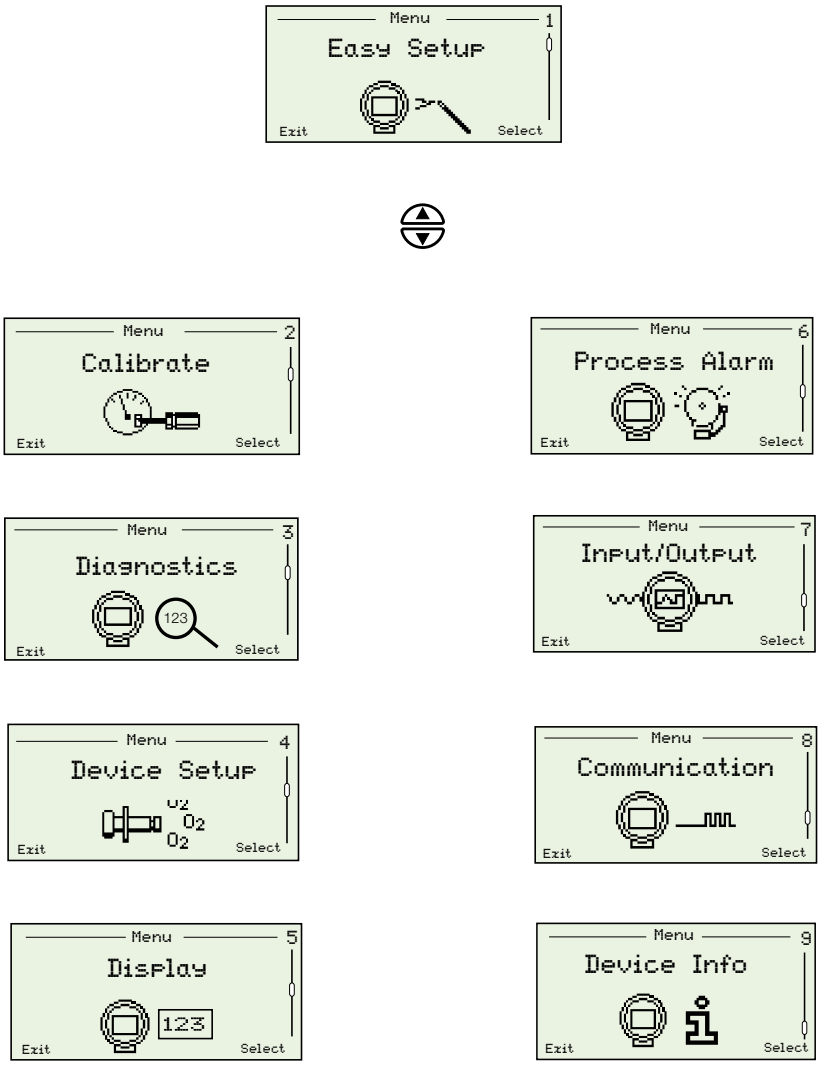
Configuration of the transmitter

At power-up, Operator Page 1 is displayed – this is the normal operating state of the transmitter. The Operator Menu is accessed by pressing for Operator Menu details. The

Access Level is accessed by pressing .



Overview of top level menus



...7 Configuration

Process display

Operator Page 1 shows the current process values and is the default page at start-up or during operation.
There are two main levels accessible from this page

Information level (Operator Menu)

The information level contains the parameters and information that are relevant for the operator.
The device configuration cannot be altered on this level.

Configuration Level (Menu)

SAFETY INSTRUCTIONS

The following parameters may affect the safety function, some of which must be set during installation so that an application as part of a safety function is possible.

To exclude interim changes and to ensure the suitability for the intended use, the following parameters need to be checked after activation of the write protection and before taking the safety function into operation.

For AZ20, the instructions for settings and installation can be found in the User Guide and Manual.

For AZ30, the instructions for settings and installation can found in the User Guide and Programming Guide.

The configuration level contains all the parameters required for device commissioning and configuration. The device configuration can be changed in this level.

Parameter descriptions

Table 6 Parameter descriptions

Menu/Parameter	Description	Additional notes/restrictions
Device Setup... Security Setup		
Standard Password	Set by Standard and Advanced Users	Passwords do not affect the safety function, but should be set and recorded by the user to prevent unauthorized changes after the initial installation
Advanced Password	Set by Advanced Users	
Easy Setup		
Probe Type	Selects the probe type to be used with the transmitter	
Cable length	The length in metres of the cable between the probe and the remote transmitter. This length is used in the cold junction measurement for the impedance pf the cable	0 to 100 m, applicable only to remote transmitter type systems
Mains voltage	Selects the mains type voltage	115 V or 230 V or autodetect (default)
Autocal hardware	Selects the type of automatic calibration hardware to be used	None, Internal or Remote
%O2 Range Hi	Sets the maximum oxygen concentration	Default 25.00 % O2
%O2 Range Lo	Sets the minimum oxygen concentration	Default 0.01 % O2
Thermocouple type	Selects the thermocouple type used for cell temperature measurement	Fixed as K from factory for all AZ20 and AZ30. Should not be changed
Factory Cal. Offset	Used to enter the calibration offset value supplied with a new probe or cell.	Default 0 mV Should be changed to match the supplied factory calibration value upon first use
Factory Cal. Factor	Used to enter the calibration factor value supplied with a new probe or cell	Default 1.00 Should be changed to match the supplied factory calibration value upon first use
Calibrate... Tests Gases		**Only relevant to the safety function on initial setup if using autocal hardware and calibration are scheduled**
Test gas 1 type	Gas Air (default) Process air	
Test gas 1 value	0.01 to 100 % O2 Default 1.00 %	Only enabled if test gas 1 type is set to 'Gas'
Test gas 2 type	Gas (default) Air Process air	
Test gas 2 value	0.01 to 100 % O2 Default 1.00 %	Only enabled if test gas 2 type is set to 'Gas'

8 Proof test

In accordance with IEC61508, the safety function of the measuring device must be checked at appropriate time intervals. The operator must determine the checking interval and take this into account when determining the probability of failure of the device.

The test must be carried out in such a way that it verifies correct operation of the device.

The MTBF (unrevealed) figures assume that tests are conducted once per year minimum.

Testing the device can be performed in the following steps:

Calibration

AZ20 calibration
Refer to section 6 Calibration of the User Guide:
IM/AZ20E-EN.

AZ30 calibration
Refer to section 7 of the Programming Guide:
COI/AZ30E-EN.

Inspection

Visual Inspection should take place by ABB personnel or by personnel trained by ABB and is only necessary in the event of alarms or failed calibration.
On-site inspection includes:
- Manual calibration
- Visual inspection
- Component resistance checks

9 Repair

For testing and replacing key components, instructions can be found in the Maintenance Guide:
IM/AZ20M-EN.

To ensure the safety related function, repairs must be performed by ABB, or by suitably trained personnel. Replacing modular components with ABB spare parts is permitted if personnel have been trained by ABB for this purpose.

The “Declaration of contamination and cleaning” must be enclosed when returning the defective device. Refer to instruction manual or contact ABB for further details.

10 SIL certificate

26 ORCHARD DRIVE,
TONBRIDGE, KENT, TN10 4LG.
Tel: 01732 352532
david.smith@technis.org.uk
www.technis.org.uk

CERTIFICATE of RELIABILITY and FUNCTIONAL SAFETY

This is to certify that

The Endura AZ20 and AZ30 Oxygen Analyser, provided by **ABB Limited Oldends Lane, Stonehouse, GL10 3TA, Gloucestershire, UK** has been assessed and is considered suitable for use in low and high demand safety functions:

- **As a simplex item (ie hardware fault tolerance of 0) at SIL 2 (low demand)**
- **As a simplex item (ie hardware fault tolerance of 0) at SIL 1 (high demand)**

This claim is in respect of an FMEA and some data, addressing random hardware failures and architectural constraints (ie safe failure fraction). The assessment was based on the assumptions and recommendations given in Technis Report T740 (Issue 1.1). The product was assessed against the failure modes:

- **Fail to respond to a specific level change of oxygen with an appropriate 4-20ma output**
- **Spurious response despite no valid change**

The assessment was carried out having regard to the guidance in IEC 61508 [2010] and the related body of guidance in respect of Random Hardware Failures and Architectural Constraints [route 1_H]

	High Demand	**Low Demand**
Safety Integrity	SIL 1	SIL 2
"hazardous" failure rate (revealed)	0.28 10^{-2} per annum	3.11 10^{-6} per hr
"hazardous" failure rate (unrevealed)	2.72 10^{-2} per annum	3.22 10^{-7} per hr
"safe" failure rate (revealed)	0	0.54 10^{-6} per hr
"safe" failure rate (unrevealed)	0	0
Diagnostic Coverage	0	90.6%
System Type	B	B
Hardware Fault Tolerance	0	0
Safe Failure Fraction	>91%	>91%
Probability of failure on demand		1.6 10^{-3}

The validity of this certificate requires that the product is used in accordance with any assumptions, limitations or intervals stipulated in the underpinning reliability/integrity report. The product build state continues to conform to the drawings and issues quoted in the underpinning reliability/integrity report. The product is used having regard to the instructions, limitations of use, intervals etc as outlined in the manufacturer's Safety Manual. The manufacturer maintains a credible level of Functional Safety Management in respect of (for example) design configuration control, procurement, manufacturing and defect analysis. The certificate will not apply to any product variation/modification or to the use of functions not addressed in the original study. It is recommended that the design, defect records and the company FSM procedure are reviewed, at least every 2 years, and should any changes have occurred since the original certification then the manufacture should contact Technis to request re-certification.

Signed:.....(Certificate No T740-093.2) – 29 Jan 2018

Dr David J. Smith BSc,PhD,CEng,FIEE,FIQA,HonFSaRS,MIGasE
This certificate does not warrant fitness for any specific applications related purpose and is based on probabilistic and statistical assessment

Notes

Notes

ABB Measurement & Analytics

For your local ABB contact, visit:
www.abb.com/contacts

For more product information, visit:
www.abb.com/measurement

SI/AZ20/AZ30-EN Rev. A 03.2022