ABB MEASUREMENT & ANALYTICS | SIL-SAFETY MANUAL

EasyLine EL3000 / EL3060

Paramagnetic oxygen analyzer Magnos28

Additional instructions for
IEC / EN 61508 compliant devices

Measurement made easy

EL3000
EL3040
EL3060

Introduction

EasyLine is both a powerful and affordable line of instruments for the monitoring of gas concentrations in numerous applications. EasyLine is based on the proven and reliable analyzer technology of ABB for extractive continuous gas analysis. EasyLine is available in two versions, which are optimized for the various installation requirements of the respective location.

Additional information

Additional documentation on EasyLine EL3000 / EL3060 is available for download free of charge at www.abb.com/analytical.
Alternatively simply scan this code:

EL3000

EL3060

Table of contents

1 Application area 3
Application area 3
Purpose 3
Scope of application 3

2 Acronyms and abbreviations 4

3 Standards and definitions of terms 5
Standard IEC 61508 2000 (Edition 1), Part 1 to 7 5
Dangerous failure 5
Safety related system 5
Safety function 5

4 Determining the safety integrity level (SIL) 5

5 Applicable device documentation 6

6 Device specific safety instructions 6
Function 6
Applications 6
Safety function 7
Pressure correction 7
Settings 7
Protection against configuration changes 7
Checking the safety function after installation 7
Maintenance and proof test 8
Checking function 8
Proof test 8
Safety characteristics 10

7 SIL-Declaration of Conformity 11

8 Management summary 13

1 Application area

Application area

Monitoring oxygen concentrations in a safety-related system, that shall meet the safety requirements according to IEC / EN 61508.

Purpose

This safety manual/document contains information and safety instructions intended for system planners, constructors, service and maintenance engineers and personnel who will commission the ABB EasyLine EL3000 series Oxygen Analyzer Magnos28 (Models EL3020, EL3040) or EasyLine EL3060 Series Oxygen Analyzer Magnos28 (EL3060-Magnos28) for the purpose of integration in a safety instrumented system.

Scope of application

The Oxygen Analyzer Magnos28 is a paramagnetic magneto-mechanical oxygen analyzer.
The analyzer is available as a standalone unit:

- For general purpose (GP) in the EasyLine EL3000 series (Models EL3020, EL3040), referred to in this document as EL3000-Magnos28.
- For hazardous areas (Zone 2, EPL Gc) in the EasyLine EL3000 series (Model EL3040), referred to in this document as EL3000-Magnos28.
- For hazardous areas (Zone 1, EPL Gb) in the EasyLine EL3060 series (Model EL3060), referred to in this document as EL3060-Magnos28.

The Oxygen Analyzer Magnos28 can be used as a single channel (1oo1) or in redundant operation (1oo2) within a safety function.

The Catalog number are recorded in the Analyzer Data Sheet:

EL3020-Magnos28 IP 20, GP, twofold analog output (2× AO), without flow or pressure sensor	
System	24042 – 111011000000
Housing	24342 – 111011000001
Electronic module	24442 – 1100110000N1
Module	24644 – 1110110500H1

EL3040-Magnos28 IP 65, GP, twofold analog output (2× AO), without flow or pressure sensor	
System	24042 – 121031x00000
Housing	24342 – 121031x00001
Electronic module	24442 – 120031x000N1
Module	24644 – 121031x500L1

EL3040-Magnos28 IP 65, EPL GC, twofold analog output (2× AO), without flow or pressure sensor	
System	24042 – 121231x00000
Housing	24342 – 121231x00001
Electronic module	24442 – 120231x000N1
Module	24644 – 121231x500L1

EL3060-Magnos28 IP 65, EPL Gb, fourfold analog output (4× AO), without flow or pressure sensor	
System	24042 – 151121x00000
Housing	24342 – 151121x20001
Electronic module	24442 – 150121x000X1
Module	24644 – 151121x200X1

x random character

2 Acronyms and abbreviations

Abbreviation	English	Description
HFT	Hardware Fault Tolerance	The hardware fault tolerance of the device. This is the capability of a functional unit to continue the execution of the demanded function in case of faults or deviations. HFT = 0 refers to single channel operation (1oo1) and HFT = 1 for dual channel, redundant operation (1oo2).
MTBF	Mean Time Between Failures	This is the mean time period between two failures.
MTTR	Mean Time To Restoration	This is the mean time period between the occurrence of a failure in a device or system and its repair.
PFD	Probability of Failure on Demand	This is the likelihood of dangerous failures of the safety function occurring on demand.
PFDAVG	Average Probability of Failure on Demand	This is the average likelihood of dangerous failures of the safety function occurring on demand.
PFH	Probability of Dangerous Failure Occurring per Hour	This is the probability of dangerous failure occurring per hour (PFH) for a high demand/continuous mode safety-related system.
SIL	Safety Integrity Level	The international standard IEC/EN 61508 specifies four discrete safety integrity levels (SIL 1 to SIL 4). Each level corresponds to a specific probability range regarding the failure of a safety function. The higher the safety integrity level of the safety-related systems, the lower likelihood of non-execution of the demanded safety functions.
SFF	Safe Failure Fraction	The fraction of non-hazardous failures, i.e. the fraction of failures without the potential to set the safety-related system to a dangerous or impermissible state.
Low demand mode	Low demand mode of operation	Measuring mode with low demand rate. Measuring mode, in which the demand rate for the safety-related system is not more than once a year and is not greater than double the frequency of the periodic test. Typically low demand mode initiates an actuator or shutdown.
High demand mode	High demand or continuous mode of operation	High demand or continuous mode is where the frequency of demands for operation made on a safety-related system is greater than once per year or greater than twice the proof test frequency.
PLC	Programmable logic controller	A programmable logic controller is a digital computer used for automation of electromechanical processes.
HMI	Human Machine Interface	Here, the HMI is the combined module consisting of LCD and local keypad.
FIT	Failure in Time	1×10^{-9} Failures per hour.
TI	Test Interval	Test interval between live testing of the safety function.
T1	Time between proof test	Test interval between live testing of the entire safety function.
λs	Failure rate for all safe failures	Overall rate for all safe failures.
λdd	Failure rate for all dangerous detected failures	Overall rate for all dangerous detected failures.
λdu	Failure rate for all dangerous undetected failures	Overall rate for all dangerous undetected failures.

3 Standards and definitions of terms

Standard IEC 61508 2000 (Edition 1), Part 1 to 7

- English:
  Functional safety of electrical / electronic / programmable electronic safety-related systems (Target group: Manufacturers and Suppliers of Devices).
- German:
  Funktionale Sicherheit sicherheitsbezogener elektrischer / elektronischer / programmierbarer elektronischer Systeme (Zielgruppe: Hersteller und Lieferanten von Geräten).

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 Determining the safety integrity level (SIL)

The term safety integrity level (SIL) is a used in functional safety and is designated in accordance with International Electrotechnical Commission (IEC) standard 61508. Four discrete levels are defined for the specification of the requirements for the safety integrity of the safety functions, whereby the safety integrity level 4 represents the highest level of safety integrity and the level 1 the lowest.

The achievable Safety Integrity Level is determined by the following safety-related parameters:

- Average Probability of Failure on Demand (PFDAVG)
- Probability of Dangerous Failure Occurring per Hour (PFH)
- Hardware Fault Tolerance (HFT)
- Safe Failure Fraction (SFF)
- Systematic safety integrity

The following table shows the dependency of the SIL on the average probability of dangerous failures of a safety function of the entire safety instrumented system (PFDAVG). The table deals with “Low demand mode”, i. e. the safety function is required a maximum of once per year on average and “high demand mode”, i. e. the demand made on a safety function is greater than once per year or greater than twice the proof test frequency

Safety Integrity Level (SIL)	PFD_{AVG} (low demand mode)	PFD_{AVG} (high demand mode)
4	$\geq 10^{-5}$ to $< 10^{-4}$	$\geq 10^{-9}$ to $< 10^{-8}$
3	$\geq 10^{-4}$ to $< 10^{-3}$	$\geq 10^{-8}$ to $< 10^{-7}$
2	$\geq 10^{-3}$ to $< 10^{-2}$	$\geq 10^{-7}$ to $< 10^{-6}$
1	$\geq 10^{-2}$ to $< 10^{-1}$	$\geq 10^{-6}$ to $< 10^{-5}$

SFF	HFT		
	0	1	2
< 60 %	Not allowed	SIL1	SIL2
60 to 90 %	SIL1	SIL2	SIL3
90 to 99 %	SIL2	SIL3	SIL4
> 99 %	SIL3	SIL4	SIL4

5 Applicable device documentation

For the EL3000-Magnos28 and EL3060-Magnos28 analyzers the following documentation must be present:

Document	EL3000-Magnos28	EL3060-Magnos28
Commissioning instruction	CI/EL3000	CI/EL3060
Operating instruction	OI/EL3000	OI/EL3060
Data sheet	DS/EL3000	DS/EL3060

For devices in explosion-proof design, the relevant EC type examination certificate must be available. Outside the EU, the local operating rules and guidelines apply. The technical data for storage and operating conditions are given in the Installation Guide.

6 Device specific safety instructions

Function

The EL3000-Magnos28 and EL3060-Magnos28 are paramagnetic magneto-mechanical oxygen analyzers and are available as standalone units.

Features:

- Two freely-programmable measuring ranges per component, without suppressed zero
- The analog output of the measuring range is set to 4 to 20 mA

Applications

The Hardware assessment (electronics and sensor physics) of The EL3000-Magnos28 and EL3060-Magnos28 shall provide the safety instrumentation engineer with the required failure data as per IEC / EN 61508 and does not include an assessment of software.

The hardware of EL3000-Magnos28 and EL3060-Magnos28 satisfy the special requirements in terms of functional safety to SIL 2 in accordance with IEC / EN 61508. The EL3000-Magnos28 and EL3060-Magnos28 are usable in safety applications to monitor oxygen concentration.

Safety function

For the EL3000-Magnos28 and EL3060-Magnos28 analyzers the following measuring ranges for the measurement of oxygen were considered for the SIL compliance:

Smallest range*:	0 to 0,5 Vol.-%
Standard range* **:	0 to 25 Vol.-%
Largest range**:	0 to 100 Vol.-%

* The EL3000-Magnos28 is set ex-factory 0 to 100 Vol.-%; 0 to 1 Vol.-% and 0 to 25 Vol.-% must be set by operator.

** The maximum oxygen content of the sample gas mixture in the EL3060-Magnos28 must be 21 Vol.-%, corresponding to atmospheric conditions.

The safety function of the device is the oxygen measuring value as a linear 4 to 20 mA analogue current signal. A signal deviation of more than ±5 % full scale without pressure correction was considered within the FMEDA as a dangerous failure. For changes in pressure of ±50 hPa, a ±10 % deviation will be considered as a dangerous failure.

Current signals ≤ 2.5 mA and ≥ 21.5 mA need to be interpreted as an analyzer failure by the control unit (e. g. a PLC) which must be connected in series. The fault relay (collective status) in normally energized mode is included as part of the safety function because several internal faults will be signaled by de-energizing the relay and not via current output.

Note
In order for an optimal operation of the EL3000-Magnos28 or EL3060-Magnos28 analyzers, the flow and pressure in the sample gas needs to be monitored.
A pressure signal can be used to correct the measurement signal of the EL3000-Magnos28 or EL3060-Magnos28 via an external PLC.
For details see the user's manual or the section below. The user is responsible for the pressure sensor employed and its functional safety.

Pressure correction

The EL3000-Magnos28 and EL3060-Magnos28 analyzer performance is altitude dependent. For this reason the typical atmospheric pressure at the installation site needs to be set in the device (see user's manual).

The measured value (MV) can be corrected for pressure fluctuations in the sample gas externally, for example by the PLC, by using a separately supplied pressure signal from the sample gas and employing the following formula in the PLC:

$$MV_{corr} = MV_{current} \times \frac{p_{constant}}{p_{sample}}$$

MV_{corr}	Corrected measured value
$MV_{current}$	Current measured value
$p_{constant}$	Reference pressure ex-factory (1013 hPa)
p_{sample}	Pressure in the sample gas

Settings

Any changes made to the original configuration of the EL3000-Magnos28 or EL3060-Magnos28 analyzers will lead to a change in the Safety Function.

After assembly and commissioning in line with the device manual, the following steps should be undertaken.

Protection against configuration changes
After configuration, the EL3000-Magnos28 or EL3060-Magnos28 access codes (password) shall be changed and activated so that the device is protected against unwanted and unauthorized changes/operation. Please note that once the password has been activated, no changes can be made to the device at any level. It is important and imperative that only authorized personal know the password.

Checking the safety function after installation
After installation of the EL3000-Magnos28 or EL3060-Magnos28, a safety function test has to be carried out (see section below). Using reference gas, i. e. N_2, 4 mA must be measured at the analog output. For the test of the safety function it is fundamental to use a second reference gas with a defined proportion of oxygen. The results of the measurement must be within a range of ±5 (full span) of the expected result. If the tolerance value is exceeded, a calibration and adjustment of the device is required.

… 6 Device specific safety instructions

Maintenance and proof test

Minimum once per year a proof test has to be carried out for the overall / entire safety function according to / in line with IEC / EN 61508. For the analyzer the proof test comprises the regular calibration / adjustment, the manual testing of the relays and the checking of all parameter settings and the stored calibration data.

Checking function

We recommend that the functioning of the EL3000-Magnos28 or EL3060-Magnos28 are checked in regular intervals of at least once a year, by testing the basic functionality of the analyzers as described in the respective User's Manual.

Proof test

Recommended proof interval depends on the application, but max within one year. Before performing the proof test, bypass the safety PLC or take other appropriate action to avoid a false trip. Remember also to remove the bypass once the proof test has been concluded.

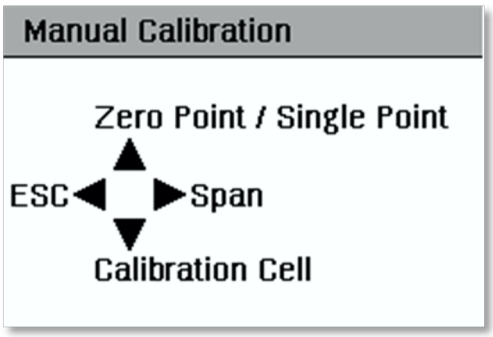
The proof test involves three steps:

1. Check the measured value by performing a calibration and verifying that the reported value of the analog signal is within specification
2. Generating a failure mode by setting the analog output to lower than ≤2.5 mA and higher than ≥21.5 mA
3. Testing the overall status digital output (ex-factory = X20 DO1)*

* Without Modbus or PROFIBUS

The logic solver (PLC) which monitors the analyzer needs to respond appropriately to the respective proof test steps: i.e. detect over range (≥21.5 mA), under range (≤2.5 mA) and de-energizing of the relay, and should recognize these as failure of the device and initiate the appropriate action.

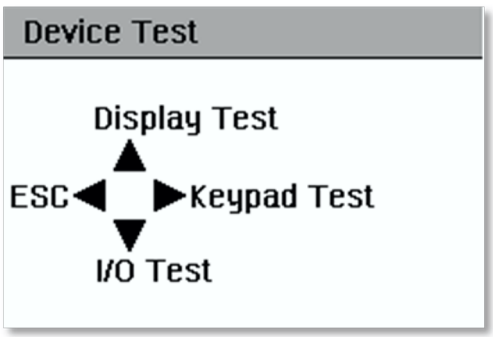
The proof test point 1 can be performed via the HMI under the Manual Calibration Menu



Menu path: Operation / Calibration / Manual Calibration

Figure 1: Manual calibration menu

The proof test points 2 and 3 can be performed via the HMI under the Device Test Menu / Device Test.



Menu path: Maintenance / Diagnosis / Test Functions / Device Test / I/O Test

Figure 2: Device test menu

The analog and digital outputs of the EL3000-Magnos28 are positioned in following slots depending on the configuration ordered.

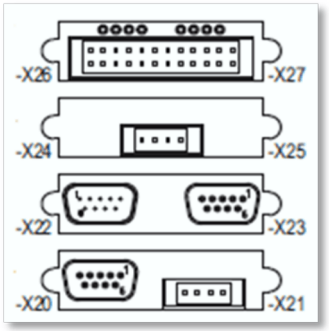


Figure 3: Position of analog and digital outputs

When Modbus or PROFIBUS has been configured, the slot no. changes to a higher slot. For a detailed description see the Analyzer Data Sheet provided with the analyzer.
The analog and digital outputs of the EL3060-Magnos28 are fixed as illustrated in the data sheet.
The EasyLine Configuration Tool (ECT) Software can be used to assign a different order to the digital output signals.
If changes have been made to the digital outputs, the respective DO needs to be tested during the proof test.

Proof Test 1 - Calibration
Procedure is as described in the user's manual for calibration.

Proof Test 2 – Test of the Analog Inputs

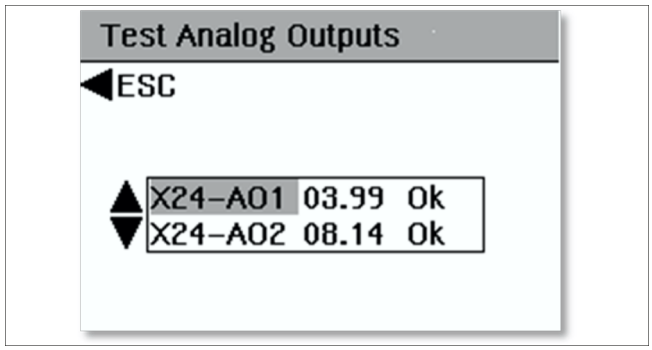


Figure 4: Test oft h analog outputs

The analog outputs (AO) available in the Analog output modules installed in the instrument are shown in the list. They are named according to the installation locations of the analog output modules (X20, X22, X24, X26).
Test:

1. Select the analog output to be tested with ▼ or ▲
2. Call up the value change with ▶
3. Change the displayed value digit by digit with ▼ or ▲ and confirm the change with OK

Result: the current signal at the analog output changes its value, the status display changes from **"OK"** to **"Test"**, and the status signal **"Function Check"** is output.

4. Either test another analog output in the same way or reset the tested analog output.

The test of the analog outputs is ended by pressing the ◀ key or after approx. 5 minutes through the time-out function; all analog outputs are thereby reset to the status **"OK"** and the status signal **"Function check"** is canceled.

… 6 Device specific safety instructions

… Maintenance and proof test

Proof Test 3 – Test of the Digital Outputs (overall status ex-factory = X20-D013)

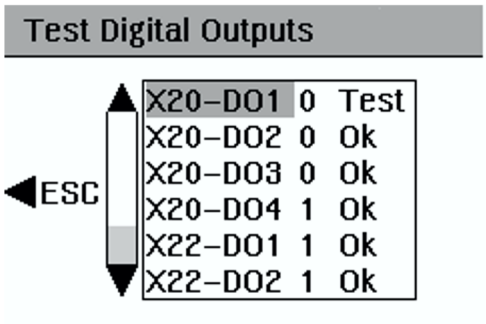


Figure 5: Test of the digital outputs

The digital outputs (DO) available in the Digital I/O modules installed in the instrument are shown in the list. They are named according to the installation locations of the digital I/O modules (X20, X22, X24, X26).
Test:

1. Select the digital output to be tested with ▼ or ▲
2. Call up the value change with ▶.
3. Change the displayed value with ▼ or ▲ and confirm the change with OK.
4. Result: the relay at the digital output is actuated, the status display changes from **"OK"** to **"Test"**, and the status signal **"Function Check"** is output.

Either test another digital output in the same way or reset the tested digital output.
The test of the digital outputs is ended by pressing the ◀ key or after approx. 5 minutes through the time-out function; all digital outputs are thereby reset to the status **"OK"** and the status signal **"Function check"** is canceled.

Safety characteristics

The safety characteristics necessary for use of the system are listed in the SIL declaration of conformity (see chapter “Declaration of conformity”). These values apply under the following conditions:

- The EL3000-Magnos28 or EL3060-Magnos28 analyzers are normally used in safety-related systems with a low demand mode for the safety function.
- The safety-related parameters/settings (see “Settings” section) have been entered by local operation and checked before commencing safety instrumented operation.
- The EL3000-Magnos28 or EL3060-Magnos28 analyzers are blocked against unwanted and unauthorized changes/operation.
- All used materials are compatible with process conditions.
- The MTTR after a device fault is 24 hours.
- The best time to react on a dangerous detected failure is 1 hour.
- The logic solver (PLC) has to be configured to detect over range (≥ 21.5 mA) and under range (≤ 2.5 mA) failure of the EL3000-Magnos28 and EL3060-Magnos28 (Fail High and Fail Low) and will recognize these as internal failure of the devices and not cause a spurious trip.

7 SIL-Declaration of Conformity

SIL Declaration of conformity

ABB Automation GmbH
60488 Frankfurt am Main
Germany

declares that the products

Continuous Gas Analyzers EasyLine EL3000 series Oxygen Analyzer Magnos28 (Models EL3020, EL3040) or EasyLine EL3060 Series Oxygen Analyzer Magnos28 (EL3060-Magnos28), without flow or pressure sensor,

comply with the requirements of the European Standards for Functional Safety :

EN 61508 (2010) part 2 [identical with IEC 61508 (2010)]

The catalog numbers are recorded in the analyzer data sheet:

Analyzer	System	Housing	Electronic Module	Module
EL3020-Magnos28* *IP20, twofold analog output*	24042-111011000000	24342-111011000001	24442-1100110000N1	24644-1110110500H1
EL3040-Magnos28* *IP65, twofold analog output*	24042-121031x00000	24342-121031x00001	24442-120031x000N1	24644-121031x500L1
EL3040-Magnos28* *IP65, twofold analog output*	24042-121231x00000	24342-121231x00001	24442-120231x000N1	24644-121231x500L1
EL3060-Magnos28* *IP65, fourfold analog output*	24042-151131x00000	24342-151131x20001	24442-150131x000X1	24644-151131x200X1

x random character
* without flow or pressure sensor

The assessment of hardware failure rates was carried out for single channel and redundant operation of Magnos28 by the company embeX (see compliance statement) as independent consultant confirming the correctness of this declaration. The conditions of safety related operation specified overleaf have to be obeyed by the user to achieve the claimed SIL compliance.

	Single channel use (one out of one)	Redundant use (one out of two)
Safety function	Oxygen measurement with 4–20 mA output The fault relay in normal energized mode is part of the safety function because several internal faults will be signaled by de-energizing the relay and not via current output.	
Measuring ranges - Standard	0–25 Vol.% / 0–100 Vol.% Oxygen	
Smallest measuring range	0–0,5 Vol.% Oxygen	
SIL capability hardware	2	3
Type of Device	B	
Proof test interval	1 year	
MTTR	24 h	
SFF	90,80 %	
HFT	0	1
β Factor	—	5 %
PFD_{avg}	$7{,}05 \times 10^{-4}$	$3{,}51 \times 10^{-5}$
PFH	$1{,}53 \times 10^{-7}$	$8{,}01 \times 10^{-9}$
λ_{du}	$1{,}53 \times 10^{-7}$ (per h)	
λ_{dd}	$1{,}28 \times 10^{-6}$ (per h)	
λ_{su}	$1{,}07 \times 10^{-7}$ (per h)	
λ_{sd}	$1{,}21 \times 10^{-7}$ (per h)	

Frankfurt, 14.06.2019

i.V. Dr. Carsten Rathke
IMS & OPEX Manager
IMS & OPEX Manager

i.V. Dr. Jürgen Kappler
Head of R&D
Leiter Entwicklung

ABB Automation GmbH
DC/EL3000/EL3060/MAGNOS28/SIL-XA Rev. B Page / *Seite* 1 / 2

... 7 SIL-Declaration of Conformity

Annex / *Anhang*

Annexes are part of this declaration. This declaration certifies conformance with the above mentioned Standards. Affirmation of attributes in a legal sense is not included. Security declarations given in the product documentation have to be considered.

Conditions for use

The values for the SIL-Capability of the analyzer and the determined failure rates are valid only if the following conditions for use are observed:

- Output signals of the analyzer of ≤ 2,5 mA (fail low) and ≥ 21,5 mA (fail high) have to be recognized by the control unit (e.g. PLC) as analyzer failure.
- De-energizing of the fault relay has to be recognized by the control unit (e.g. PLC) as analyzer failure.
- The analyzer has to be maintained regularly following the manufacturer's instructions and to be calibrated using a certified calibration gas mixture.
- The Safety Reference Manual/Instructions has to be followed.

Annual Proof Test

Minimum once per year a proof test has to be carried out for the overall safety function. For the analyzer the proof test is a regular calibration /adjustment, the manual testing of the relays and the checking of all parameters and the calibration data. The proof test is described in detail in the Safety Reference Manual/Instructions.

8 Management summary

Note
The full FMEDA report and calculation sheets are available upon request for auditing purposes.
embeX GmbH Test Report (extract)

embeX GmbH
Heinrich-v.-Stephan-Straße 23
D-79100 Freiburg

Date: 13.06.2019

Result of the Determination of Safety Parameters for EL3020 / 3040 / 3060 with Magnos28

The safety parameters of the oxygen analyzer „EL3020 / 3040 / 3060 with Magnos28" including the elements SSI, AMC, AO2 or AO4, IO and sensor have been determined. (The safety parameters of AO2 and AO4 are similar. AO4 is used, because its PFD_{avg} und PFH are higher.) The analysis of embeX comprises the changed parts of SSI; the parameters of the unchanged parts have been taken from the existing reports.

The safety function is defined as follows:

„For the analyzer Magnos28 for oxygen measurement the follwoing measurement ranges have been considered: smallest range 0 to 0.5 vol. %, standard range 0 to 25 vol. %, largest range 0 to 100 vol. %. The safety function of the device is the measured oxygen concentration as linear 4 …20 mA analogue current signal. A signal deviation of more than ±5% full scale is considered as a dangerous failure. Current signals ≤ 2.5 mA and ≥ 21.5 mA shall be interpreted by the control unit (e.g. PLC), which shall be connected in series, as analyzer failure. The fault relay, working in normally energized mode, is part of the safety function, because several internal faults are signaled by de-energizing the relay and not via the current output."

Single Channel Operation

The following safety parameters of the safety function are reached in single channel operation:

$PFD_{avg}=7.05 \times 10^{-4}$; PFH=$1.53 \times 10^{-7}$ 1/h; SFF=90.8%

Failure rates [in 1/h]: $\lambda SD=1.21 \times 10^{-7}$; $\lambda SU=1.07 \times 10^{-7}$; $\lambda DD=1.28 \times 10^{-6}$; $\lambda DU= 1.53 \times 10^{-7}$

PFD_{avg} consumes 7.0% of the permitted failure rate of the complete system in low demand mode for SIL2. PFH consumes 15.3% of the permitted failure rate of the complete system in high demand mode for SIL2. The required value >90% for the safe failure fraction SFF for SIL2 has been exceeded.

Result:

The calculated characteristic values correspond to the values required by IEC61508 for SIL2.

Redundant Operation

For the rate of faults leading to a common cause failure of both channels the value of β=5% has been assumend (from [EN50402]).

The following safety parameters of the safety function are reached in dual channel operation of two EL3020 / 3040 / 3060 with Magnos28:

$PFD_{avg}=3.51 \times 10^{-5}$; PFH=$8.01 \times 10^{-9}$ 1/h ; HFT=1

Failure rates of one channel [in 1/h]:
$\lambda SD=1.21 \times 10^{-7}$; $\lambda SU=1.07 \times 10^{-7}$; $\lambda DD=1.28 \times 10^{-6}$; $\lambda DU= 1.53 \times 10^{-7}$

PFD_{avg} consumes 3.5%, PFH 8.0% of the permitted failure rate of the complete system for SIL3.

The SFF of 90.8%, which has been determined for single channel use, is sufficient for SIL3 in redundant operation (HFT1).

Result:

The calculated characteristic values correspond to the values required by IEC61508 for SIL3.

Notes

Notes

ABB Automation GmbH
Measurement & Analytics
Stierstädter Str. 5
60488 Frankfurt am Main
Germany
Tel: +49 69 7930-4666
Email: cga@de.abb.com

abb.com/analytical

3KXG112002R4801

SM/EL3000/EL3060/Magnos28/SIL-EN Rev. A 08.2019