SIL O_2 Analyser

Safety Manual

Manual Part Number: 06-265

Rev. 0.1

EXCELLENCE
THROUGH DIVERSITY

INTRODUCTION **5**
FUNCTIONAL SPECIFICATION **6**
SYSTEM CONFIGURATION **6**
PRINCIPLE OF OPERATION **9**
SAFETY FUNCTIONS **10**
CONSTRAINTS OF USE **10**
METHODOLOGY **12**
SYSTEM FAILURE MODES **12**
ENVIRONMENTAL PROFILE **14**
FAILURE RATE DATA **15**
ASSUMPTIONS **15**
RESULTS **16**
APPLYING THE FMEDA RESULTS **18**
1oo1D Architecture 19
1oo1D Safe Failure Fraction 19
1oo1D Calculation of Average Probability of Dangerous Failures 19
Proof Test Philosophy 20
Calculation of PFH 21
Diagnostics 22
ALTERNATIVE ARCHITECTURES 23
Using alternative architectures to improve PFH or PFD_{avg} 23
Using alternative architectures to improve plant availability 23
Limitations of alternative architectures due to systematic capability constraints 23
SYSTEMATIC CAPABILITY **24**
QUALITY DOCUMENTATION **25**
PROOF-TESTING **26**
REFERENCES AND SUPPORTING DOCUMENTATION **28**
RELEASE NOTES **29**

CLASSIFICATION OF THE SAFETY INSTRUCTIONS

This manual contains instructions that you have to observe for your personal safety as well as to avoid material damage. These instructions are highlighted using a triangular warning sign and shown as follows, depending on the degree of risk.

HAZARD

means that death or severe physical injury will occur if the appropriate precautionary measures are not taken.

WARNING

means that death or severe physical injury may occur if the appropriate precautionary measures are not taken.

CAUTION

with a warning triangle means that a slight injury may occur if the appropriate precautions are not taken.

CAUTION

without a warning triangle means that a material damage may occur if the appropriate precautions are not taken.

ATTENTION

means that an undesired result or state may ensue if the corresponding instruction is not followed.

NOTE

denotes important information about the product, handling of the product or the respective part of the documentation, is aimed at drawing special attention to the latter and should be complied with.

In addition to the instructions in this manual, the generally applicable safety and accident prevention regulations must be observed. If the information contained in this document should not be sufficient in any specific case, you can obtain more detailed information from our telephone service.

Please read this manual carefully prior to installation and commissioning.

CE mark

This product meets the specifications according to the EMC standard EN 61326-3-2 and the Low Voltage Directive 2006/95/EC.

General Instructions

WARNING

Devices with the type of protection designated as "intrinsic safety" lose their conformity certification as soon as they have been operated in circuits that do not meet the values specified in the test certificate. Flawless and safe operation of this device requires proper transport, proper storage, installation and assembly as well as careful operation and maintenance. The device may only be used for the purposes specified in this operating manual.

Note: Programming of all Alarm levels and other necessary functionality is not a user enabled function and is undertaken by Ntron prior to delivery of the device. Should any changes be necessary to the programming, please contact Ntron.

DISCLAIMER

All modifications to the device fall within the responsibility of the user unless expressly specified otherwise in the operating manual.

Qualified PERSONNEL

are persons who are familiar with installation, assembly, repair and operation of the product and have the qualifications necessary for their work, such as:

- Training, instruction and/or authorization to operate and maintain equipment/systems in accordance with the standards of safety technology for electrical circuits, high pressures and corrosive as well as hazardous media.

- In the case of equipment with explosion protection: training, instruction and/or authorization to perform work on electrical circuits for potentially explosive equipment.

- Training or instruction in accordance with the standards of safety technology regarding care and use of appropriate safety equipment.

CAUTION

- Potentially electrostatic components may be destroyed by voltage that is far below the limits of human perception. Such voltage occurs even when you touch a component or electrical connections of a component and are not electrostatically discharged. The damage that occurs to a component because of overvoltage usually cannot be detected immediately and does not become noticeable until after a longer operating period.

- No software development is possible. The required competence is limited to understanding and following the procedures documented in the Safety Manual.

INTRODUCTION

Intended use of this manual

This manual details the safety related data required to implement this product into a Safety Instrumented System.
This Manual does not contain the technical specifications or operating instructions for this product. Consult the SIL O2 User Operation and maintenance Manual for that information. Basic system outline and connectivity information is given in this Manual as an aid to system design and implementation.

FUNCTIONAL SPECIFICATION

SYSTEM CONFIGURATION

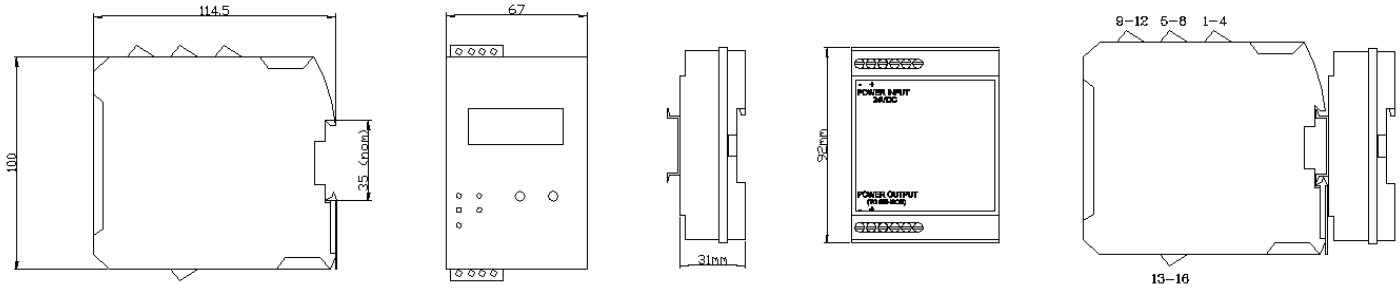
Hardware

The complete SIL2 Analyser system comprises of the following components.

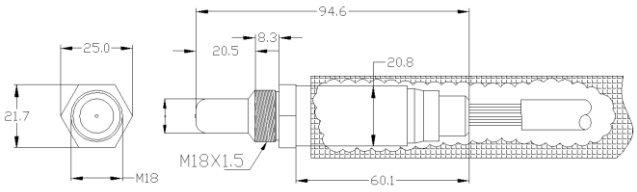
1. SILO2 ZR Analyser Part No.: 05-015
2. Power Supply Base Unit. Part No. 04-607
3. Zirconia Oxygen Sensor type 'LT' or 'LP' with electrical connector*
4. Extension cable with electrical connector(to mate with Sensor connector)*

*Available with options of connector types, extension cable lengths and process fittings so part numbers will vary accordingly and are available on request from Ntron.

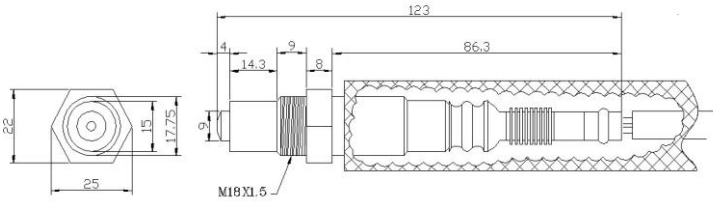
System Components Drawing



SILO2 ZR Analyser with Power Supply Base unit



'LT' Model Sensor



'LP' Model Sensor

Sensor fitted with integral 500mm long cable and connector.
Extension cable with mating is also supplied with the Sensor.
Standard length is 3000mm with option of bespoke length made to customer's requirements.

System Software

SILO2 ZR Firmware

The SILO2 ZR Analyser has integral operational Firmware which contains variable settings to allow the configuration of specified to input and output elements meet the required application. Such settings have a bearing on the internal signal processing and hardware interfaces.
The variable settings can only be accessed and changed by means of a PC running dedicated interface software. Both the device Firmware and Interface software are revision controlled.

Current Version:
Firmware Version No.: 5.03

Interface Software

This Interface software is used for the factory configuration of each SILO2 ZR analyser but is also available to end users allowing onsite setting and adjustment of certain operational settings. This software allows configuration of both electronic and hardware input and output interface elements to the required application specific settings. Once a given configuration is downloaded to the SILO2 ZR Analyser, the interface software is disconnected from the Analyser and shut down.
Current Version:
Software Version No.: Version 8 Release 0.8

Interface Software Communications

The PC based interface software communicates with the SILO2 ZR Analyser by means of a dedicated RS232 connection cable assembly. See the Technical Data section of this manual for the RS232 communication settings.

Security

Without connection to the Interface Software and hardware, no configuration changes can be made to the SIL O2 ZR analyser.
The Interface software has two level password protection which can be set and changed by the user.
Password level 1: Allows access to all variable parameter settings except 'Calibration'.
Password level 2: Allows access to 'Calibration' only.

The SILO2 Analyser is designed for mounting within Enclosures or control panels. Such Enclosures or control panels should have restricted user entry to specified key holders. This can prevent unauthorised calibration adjustment to the SILO2 ZR Analyser via the manual calibration buttons on the device.

Recommended Configuration

The only configurable parameters that should be adjusted by the customer/user are those involving the operation of the user interface relay outputs. These are as follows.
1 Relay Alarm Levels; 2 Relay Hysteresis; 3 Relay operation delay time, 4 Rising or falling Oxygen level operation,5 Energised(fail safe) or de-enegised state when healthy.
The foregoing settings values are typically determined by the customer/user and transmitted to Ntron for configuring during the production process.

Software development
The software element of the SILO2 analyser is a fixed program language (FPL) with no user access for coding development. User access is limited to entering data as instructed by operation and maintenance procedures.

Compatibility

- Backwards compatibility

The SILO2 ZR Firmware version 5.03 is backward compatible with Firmware version 5.02 models. This model is only suitable for use with Sensors with wire break functionality.

- Compatibility with other systems

The SILO2 ZR analyser System is a Stand alone solution and no compatibility concerns with other systems are relevant.

Change control
Should any changes to the programming be necessary, please contact Ntron.

Factory defaults
No automatic device restore to a design safe state is supported. A Configuration Reload would be required.

User interface
User access is limited to entering data as instructed by operation and maintenance procedures.

PRINCIPLE OF OPERATION

The oxygen sensor [3] measures the volumetric oxygen concentration in gas-phase. The oxygen sensor is a galvanic cell with solid electrolyte sandwiched between two electrodes. At temperatures above a threshold temperature, the solid electrolyte permits the passage of oxygen; producing a net flux of oxygen across the solid electrolyte from one side to the other when there is a difference in oxygen concentration in the atmospheres on either side of the solid electrolyte. This flow of oxygen generates an electrical potential between the two electrodes that is proportional to the oxygen gradient.

A reference gas (ambient air) is maintained on one side of the solid electrolyte and the process gas is presented to the opposite side of the solid electrolyte. The electrical potential generated by the ionic conductance of oxygen across the electrolyte when above the threshold temperature is proportional to the difference in oxygen concentration between the process gas and the reference gas. When the oxygen concentration in the process gas is low compared to the reference gas, the electrical potential is negative. As the process gas oxygen concentration increases, the electrical potential decreases (becomes less negative) until the electrical potential eventually falls to 0 mV when the process gas oxygen concentration is approximately 15%, or greater and air is used as the reference gas. Increasing the process gas oxygen concentration further causes the electrical potential to become positive and increase with increasing process gas oxygen concentration. This means that for applications where the process oxygen concentration must be maintained at a level that generates a negative electrical potential across the electrolyte (i.e. below 15% oxygen), any failure resulting in a signal voltage output from the sensor of 0 mV would be falsely interpreted as a high oxygen concentration and trigger whatever action is required to put the equipment under control into a safe state, or maintain a safe state. A safe failure.

The sensor is fitted with an internal heater element to maintain the temperature above approximately 350°C. This temperature is above the threshold temperature at which ionic conductance across the solid electrolyte can occur. Any failure of the heater that caused the temperature of the sensor to fall below the threshold temperature would stop the flow of oxygen and remove the electrical potential across the electrodes, generating a sensor signal output of 0 mV, which would be falsely interpreted as a high oxygen concentration and trigger whatever action is required to put the equipment under control into a safe state, or maintain a safe state. A safe failure.

Any failure of the heater element that caused the temperature of the sensor to rise much above the temperature at which the sensor was calibrated would decrease the resistance to the flux of oxygen across the solid electrolyte and creating a marginal increase in the electrical potential. This has an effect on the sensor calibration, causing the analyser to underestimate the concentration of oxygen in the process gas by a small degree and potentially allow the Equipment Under Control to operate at an oxygen concentration that is not safe. However, provided the set point chosen for the allowable oxygen concentration in the process gas is sufficiently low to allow for this small amount of sensor drift, the safety function will not be affected.

Electrical power is supplied to the sensor heater element via a power supply unit (the PSU), this is a DC/DC converter circuit that converts a 24 V DC supply received from the Oxygen Analyser into a 14 VDC output.

SAFETY FUNCTIONS

1. **De-energise alarm relay(s) R1 and R2 on detection of high oxygen level**
   The OC85 generates a mV output that is proportional to the oxygen concentration in a process gas. The SILO2 interprets the mV input signal from the OC85 and calculates the oxygen concentration using a calibration function. The analyser then compares the calculated oxygen concentration with a pre-determined threshold value that is defined by the user. When the calculated oxygen concentration exceeds the threshold value, the SILO2 de-energises two alarm relays (R1 and R2), which may be used either singly or together as part of a SIS to actuate the Final Element(s) and put the equipment under control into a safe state or maintain a safe state.

2. **De-energise fault relay R3 on detection of fault by SILO2 internal diagnostics**
   The SILO2 has an automatic on-line diagnostic monitoring system that will de-energise a fault relay (R3) on detection of faults within the OC85, or SILO2, itself.

3. **De-energise alarm relay(s) R1 and R2 when certain faults occur in OC85**
   Certain faults that occur in OC85 cause the signal voltage to a fixed value of 0 mV, which drives the output of the SILO2 above the pre-determined threshold oxygen concentration value, causing the alarm relay(s) R1 and R2 to de-energise.

4. **Provide an analogue 4-20 mA output proportional to the measured oxygen concentration of the process gas**
   The SILO2 provides a 4-20 mA output that is proportional to the oxygen concentration derived from the mV input signal from the OC85. The 4-20 mA output signal may be used as part of a SIS.

CONSTRAINTS OF USE

Functional safety can only be achieved if the following constraints are observed:

- Functional safety is only valid for applications where the safe state is an oxygen concentration that is below a pre-determined threshold, i.e. a low oxygen concentration is safe.
- The system can only be used where the safe state is below a pre-determined oxygen concentration threshold that generates a mV signal from the OC85 that is negative in value. Oxygen concentrations that are ≥15% generate 0mV or positive mV output signals. The SILO2 must be configured so that the alarm relay(s) R1 and/or R2 used in the safety circuit are de-energised when the output signal from the OC85 equal 0 mV or is positive in value. This is because a 0 mV output from the

OC85 also indicates dangerous fault conditions and must be used to put the equipment under control into a safe state or maintain a safe state.

- For functional safety to be achieved, the fault relay R3 must be used as part of the SIS in event of a fault detected by internal diagnostics to actuate the Final Element(s) and put the equipment under control into a safe state or maintain a safe state.
- One or both of alarm relays R1 and R2 must be designated to de-energise to trip when the measured oxygen concentration is above a pre-determined user-defined set-point programmed into the analyser and selected to ensure process safety. De-energising the relay(s) must result in an action that puts the Equipment Under Control into a safe state, or maintain a safe state.
- All of the supplier's installation, commissioning, operation & maintenance and conditions of use must be followed.
- Low oxygen safety level (Explosion protection)
    - any output of 0 mV or -mV is treated as a potential fault, and the relay would de-energise. Effectively, this means that the control set point can be any value below 15% oxygen, or more accurately the control set point oxygen concentration must be below whatever oxygen concentration results in a 0 mV output.
    - High Oxygen safety level (Personnel Entry Protection)
    - the relays de-energise whenever the mV output is 0 mV or a +mV value, treating this as a potential fault. This means that the control set point can be any value above 15% oxygen concentration, or more accurately the control set point oxygen concentration must be above whatever oxygen concentration results in a 0mV output.

FAILURE MODE, EFFECTS AND DIAGNOSTICS ANALYSIS (FMEDA)

METHODOLOGY

Failure Mode, Effect and Diagnostics analysis is a systematic procedure for the analysis of a system to identify the potential failure modes, their causes and effects on system performance and functionality, including the immediate assembly and the entire system or process. The term system is used as a representation of the hardware, software (with their interaction), or a process. There are wide variations in the manner in which an FMEDA may be conducted and presented. The FMEDA conducted here follows guidelines presented in IEC 60812 (2nd Ed) Analysis Techniques for System Reliability- procedure for Failure Mode and Effect Analysis (FMEA). In addition to the formal guidelines, faults revealed by both on-line automatic diagnostics and periodic proof testing are also identified.

SYSTEM FAILURE MODES

The failure modes of the OXYGEN ANALSER SYSTEM due to random hardware failures and the behaviour of the system following failure of the function are described in the following tables.

Table 1 describes the failure modes when the safety instrumented system is being used where a safe state is maintained when the oxygen concentration is above a predetermined threshold that must be greater than 16% .

Table 2 describes the failure modes when the safety instrumented system is being used where a safe state is maintained when the oxygen concentration is below a predetermined threshold that must be lower than 14%.

Note: it is not possible to use the OXYGEN ANALYSER SYSTEM where the threshold oxygen concentration that defines a safe state is between 14% and 16%. The sensor signal mV output that would result in a measured oxygen concentration of between 14% and 16% is reserved by automatic online diagnostic functions.

Table 1

Mode	Description
Safe State	The oxygen concentration of the Equipment Under Control is above a pre-determined safe threshold greater than 16% that is defined by the user. The threshold must be sufficiently high that the output signal of the sensor has a positive electrical potential.
Dangerous State	The oxygen concentration of the Equipment Under Control is below a pre-determined safe threshold greater than 16% that is defined by the user. The threshold must be sufficiently high that the output signal of the sensor has a positive electrical potential.
Safe Failure	A failure that causes the safety instrumented system to cause the equipment under control to go into a safe state or maintain a safe state without a demand from the process to do so.
Safe Failure (Detected)	A safe failure that is detected by automatic internal diagnostics.

Dangerous Failure	A failure that prevents the safety instrumented system from operating as designed and causing the equipment under control to go into a safe state or maintain a safe state when there is a demand from the process to do so.
Dangerous Failure (Detected)	A dangerous failure that is detected by automatic internal diagnostics and causes either: the output signal from the analyser to be driven above a pre-determined safe threshold defined by the user, or de-energises fault relay (R3).
Fail High	A failure that causes the output signal from the analyser to go above 20 mA.
Fail Low	A failure that causes the output signal from the analyser to go below 4 mA.
No Effect Failure	A failure of part of the system that has no effect on the safety function and is neither a safe failure, nor a dangerous failure. It is not included in the SFF calculation.
No Part Failure	A failure that is not part of the system and does not affect the safety function.

Table 2

Mode	**Description**
Safe State	The oxygen concentration of the Equipment Under Control is below a pre-determined safe threshold less than 14% that is defined by the user. The threshold must be sufficiently low that the output signal of the sensor has a negative electrical potential.
Dangerous State	The oxygen concentration of the Equipment Under Control is above a pre-determined safe threshold less than 14% that is defined by the user. The threshold must be sufficiently low that the output signal of the sensor has a negative electrical potential.
Safe Failure	A failure that causes the safety instrumented system to cause the equipment under control to go into a safe state or maintain a safe state without a demand from the process to do so.
Safe Failure (Detected)	A safe failure that is detected by automatic internal diagnostics.
Dangerous Failure	A failure that prevents the safety instrumented system from operating as designed and causing the equipment under control to go into a safe state or maintain a safe state when there is a demand from the process to do so.
Dangerous Failure (Detected)	A dangerous failure that is detected by automatic internal diagnostics and causes either: the output signal from the analyser to be driven above a pre-determined safe threshold defined by the user, or de-energises fault relay (R3).
Fail High	A failure that causes the output signal from the analyser to go above 20 mA.
Fail Low	A failure that causes the output signal from the analyser to go below 4 mA.
No Effect Failure	A failure of part of the system that has no effect on the safety function and is neither a safe failure, nor a dangerous failure. It is not included in the SFF calculation.
No Part Failure	A failure that is not part of the system and does not affect the safety function.

ENVIRONMENTAL PROFILE

For the purposes of the FMEDA, environmental profiles were chosen to represent the more severe characteristics of typical locations for the products, of which these components are part. The profiles are not intended to represent average conditions, but rather conditions estimated such that 90% of installations will be in environments that are less severe than the profile. It is assumed that process-wetted components are compatible with the physical and chemical surroundings. A list of physical and chemical compatibilities of the process-wetted components is presented in appendix XX.

These profiles provide component-level environmental conditions inside the product. It must be noted that the component environmental conditions -mounted on a circuit board, inside an enclosure, inside a cabinet- will be different to the product's external environment.

The environmental profiles of the system are shown in the following table:

Sub assembly:	SILO2 PSU	OC85 electrical (non-process wetted)	OC85 mechanical (process wetted)
Profile no.	1	3	6
Profile description	Cabinet mounted/climate controlled	General field mounting (self-heating)	Process wetted
IEC 60654-1 profile designation	B2	C3 / D1	NA
Average ambient temperature °C	30	25	See appendix XX
Average internal temperature °C	60	45	NA
Daily temperature excursion (pk-pk) °C	5	25	NA
Seasonal temperature excursion °C	5	40	NA
Exposed to elements/weather?	No	Yes	Exposed to process conditions
Humidity[1]	0-95% non-condensing	0-100% Condensing	See appendix XX
Shock[2]	10g	15g	See appendix XX
Vibration[3]	2g	3g	See appendix XX
Chemical corrosion[4]	G2	G3	See appendix XX

Surge[5]			
Line-Line	0.5 kV	0.5 kV	NA
Line-Ground	1 kV	1 kV	
EMI Susceptibility[6]			
80MHz-1.4GHz	10 V/m	10 V/m	NA
1.4GHz-2.0GHz	3 V/m	3 V/m	
2.0GHz-2.7GHz	1 V/m	1 V/m	
Electrostatic Discharge (air)[7]	6 kV	6 kV	NA

FAILURE RATE DATA

The failure rate data used in the FMEDA assumes a constant failure rate, independent of wear-in (infant mortality) effects and wear-out (end of life) effects. It is important therefore to ensure that commissioning checks are completed on installation and components are replaced within the suppliers recommended lifetime figures.

Component-level failure rate data was obtained from Exida Electrical & Mechanical Component Reliability Handbook, 3rd Edition. The data was derived using field data from various sources and failure data from various databases. The rates were chosen in a way that is appropriate for safety integrity level verification calculations. It is anticipated that the actual number of field failures due to random hardware failures will be less than the number predicted by the failure rates used in this study.

ASSUMPTIONS

The following assumptions have been made during the Failure Mode, Effects and diagnostics Analysis of the OC85, SILO2 assembly:

- There is zero fault tolerance; a single component failure will result in loss of the safety function of the OC85 and the SILO2.
- Constant failure rates are assumed. Wear-in and wear-out mechanisms are excluded.
- Propagation of errors by the device in the system are not taken into consideration
- Components that are not part of the safety function, or which have no effect on the safety function have been recognised during the analysis but are excluded from reliability calculations.
- Component stress levels are considered 'average' for industrial applications. The OC85 'process-wetted parts' environment is comparable to Exida Profile 3, whereas the non-process-wetted parts of OC85 environment is comparable to Exida Profile 6 and. The SILO2 is intended to be cabinet mounted in an environment comparable with Exida Profile 1.

- De-energising either alarm relays or fault relays will cause the SIF to put the equipment under control into a safe state, or maintain a safe state.
- All 'process-wetted' parts are compatible with the process conditions in terms of materials, erosion, corrosion and function.
- The system is installed and operated in accordance with the supplier's instructions.
- Maintenance schedules are observed, including replacement parts, calibrations and proof-testing.
- The system is not subject to abuse or sabotage.
- The time required to detect a fault by internal automatic diagnostics is no longer than 5 minutes.

RESULTS

Annex D of IEC61508-2 requires that all failure modes of the compliant item due to random hardware failures are identified and made available to the user in a safety manual, including:

- the failure rates for each failure mode,
- the effects of each failure mode and the associated outputs,
- whether each failure mode is detected by either internal or external on-line diagnostics,

The user of these numbers is responsible for determining their applicability to any particular installation or environment. Accurate plant specific data may be used for this purpose. If a user has data collected from a good proof test reporting system that indicates higher failure rates, the higher numbers must be used. Some industrial plant sites may have higher levels of stress than those assumed in this analysis. Under such conditions, the failure rate data should be adjusted to reflect the specific conditions of the installation.

Failure data obtained from the FMEDA is presented in the following tables:

OC85 (+PSU)		
Failure Mode	**Failure rate (failures per 10^9 hours)**	**Output of failure mode**
Fail safe undetected	1807	De-energises alarm relay(s) R1 and/or R2
Fail safe detected	75	De-energises alarm relay(s) R1 and/or R2 and fault relay, R3
Fail dangerous detected	154	De-energises fault relay, R3
Fail dangerous undetected	912	Unable to de-energise alarm relay(s) R1 and/or R2 and fault relay, R3 when required to do so by a process demand.
No effect / No part	188	No effect on safety function

Combined system SILO2 and OC85(+PSU)		
Failure Mode	**Failure rate (failures per 10^9 hours)**	**Output of failure mode**
Fail safe undetected	2111	De-energises alarm relay(s) R1 and/or R2
Fail safe detected	177	De-energises alarm relay(s) R1 and/or R2 and fault relay, R3
Fail dangerous detected	535	De-energises fault relay, R3
Fail dangerous undetected	931	Unable to de-energise alarm relay(s) R1 and/or R2 and fault relay, R3 when required to do so by a process demand.
No effect / No part	1164	No effect on safety function

SILO2		
Failure Mode	**Failure rate (failures per 10^9 hours)**	**Output of failure mode**
Fail safe undetected	304	De-energises alarm relay(s) R1 and/or R2
Fail safe detected	102	De-energises alarm relay(s) R1 and/or R2 and fault relay, R3
Fail dangerous detected	381	De-energises fault relay, R3
Fail dangerous undetected	19	Unable to de-energise alarm relay(s) R1 and/or R2 and fault relay, R3 when required to do so by a process demand.
No effect / No part	976	No effect on safety function

APPLYING THE FMEDA RESULTS

In IEC 61508-2 2010 Clause 7.4.4: in the context of hardware safety integrity, the highest safety integrity level that can be claimed for a safety function is limited by hardware safety integrity constraints which shall be achieved by implementing one of two possible routes (to be implemented at system or subsystem level). These are:

Route 1_H based on hardware fault tolerance and safe failure fraction concepts; or, Route 2_H based on component reliability data from feedback from end users, increased confidence levels and hardware fault tolerance for specified safety integrity levels (Proven in Use).

In the absence of reliability data feedback from end users, Route 1_H will be used to determine the hardware safety integrity architectural constraints.

Under the requirements of IEC61508 and prior to loop calculations (PFD) it is necessary to determine the absolute minimum architecture that is required. This is determined by the 'safe failure fraction' (SFF) which can be expressed by the formula:

Equation 1 SFF

$$SFF = \frac{\lambda_{SD}+\lambda_{SU}+\lambda_{DD}}{\lambda_{SD}+\lambda_{SU}+\lambda_{DD}+\lambda_{DU}}$$

This equation can only be used if dangerous detected failures (λ_{DD}) are detected by automatic online diagnostics for low-demand mode applications and where detection of the dangerous failure causes the Equipment Under Control to go into a safe state, or maintain a safe state.

The safe failure fraction is component specific and is completely independent of maintenance criteria such as Proof Test Interval (PTI) and MTTR. Failure to meet the required SFF for a given SIL level can only be resolved by adding redundancy and not by changing the maintenance variables.

Under the safe failure fraction there are two defined types of components/devices: type 'A' where full Failure Mode and Effect Analysis (FMEA) is available and where fault behaviour can be determined and where field data is available or type 'B' where either one or more of these criteria is missing.

Table 3a and 3b

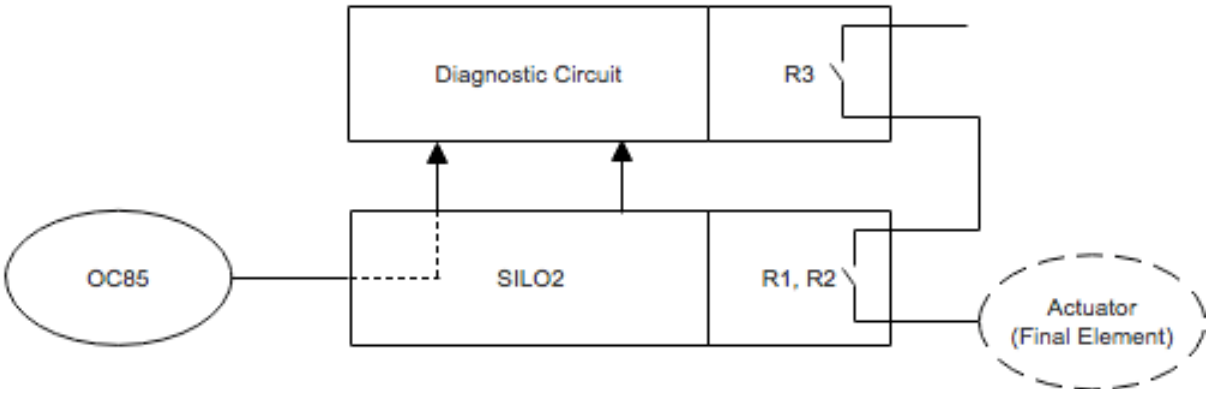
Type 'A' devices			
SFF	Hardware fault tolerance		
	0	1	2
<60%	SIL 1	SIL 2	SIL 3
60%<90%	SIL 2	SIL 3	SIL 4
90%<99%	SIL 3	SIL 4	SIL 4
≥99%	SIL 3	SIL 4	SIL 4

Type 'B' devices			
SFF	Hardware fault tolerance		
	0	1	2
<60%	-	SIL 1	SIL 2
60%<90%	SIL 1	SIL 2	SIL 3
90%<99%	SIL 2	SIL 3	SIL 4
≥99%	SIL 3	SIL 4	SIL 4

IEC61508:2010 Part 2 Tables 2 &3

1oo1D Architecture

1oo1D architecture uses a single controller channel with diagnostic capability and a second diagnostic channel wired in series to utilise the diagnostic signal to de-energise the output. Diagnostics allow a detected dangerous failure to be converted into a safe failure. 1oo1 architecture has a fault tolerance of zero.



1oo1D Safe Failure Fraction

The OC85 sensor element is defined as 'Type A', however the SILO2 analyser is a 'Type B' element. The maximum safety integrity level that can be claimed based on the hardware fault tolerance in a system with 1oo1D architecture is given in the following table:

Element	Fault Tolerance (1oo1D)	Element Type	Safe Failure Fraction (%)	Maximum allowable SIL
OC85	0	A	69	2
SILO2	0	B	97	2

1oo1D Calculation of Average Probability of Dangerous Failures

The 1oo1D architecture has a second diagnostic channel that will de-energise when failures are detected by automatic on-line diagnostics. Therefore, the only failures that cause system with outputs energised are dangerous undetected failures. The equation for PFD_{avg} for a 1oo1D architecture is:

$$PFD_{avg} = 1 - e^{-\lambda_{DU}\frac{T}{2}}$$

Where T = Proof test interval

Proof Test Philosophy

The greatest source of undetected dangerous failures is due to sensor drift or reduced sensitivity, which together account for a combined failure frequency of 900 failures per 109 hours. A convenient bump-test procedure may be used to reveal these faults as part of a partial proof test. The bump-test procedure is described in the Proof Test part of the Maintenance section in this document. Note that the bump-test will test the entirety of the function it is designed to examine, and thus is different to partial stroke testing.

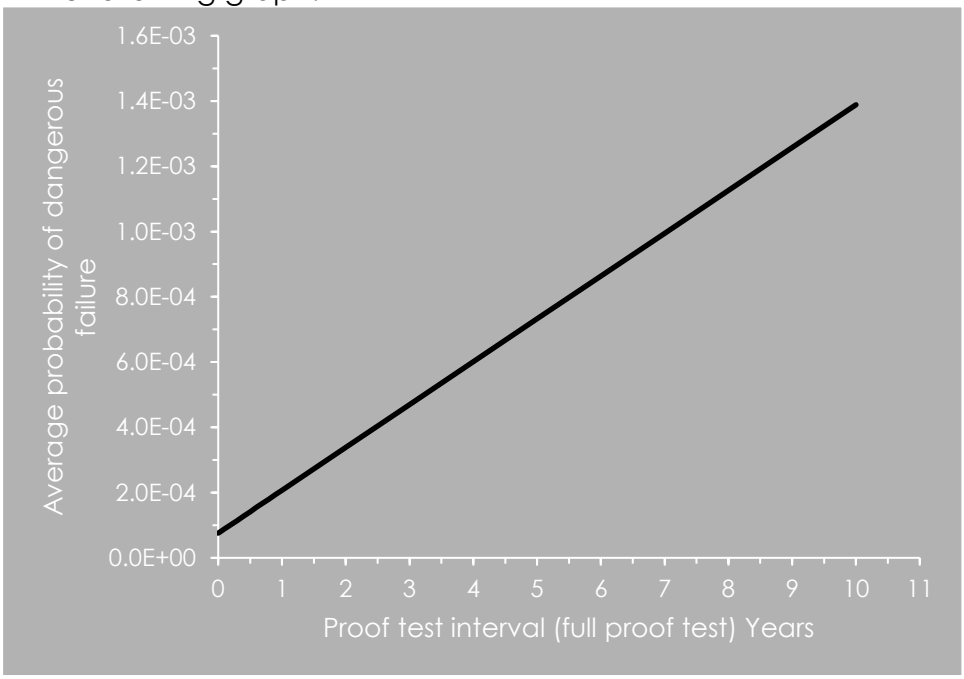
It is recommended that the bump-test partial proof test is done at weekly intervals and a full proof test of the entire system is done at a frequency determined by the user's target PFDavg using the following equation:

$$PFD_{avg} = 1 - e^{-\lambda_{Drift}\frac{T_B}{2} + (\lambda_{DU} - \lambda_{Drift})\frac{T}{2}}$$

Where:

T	= Full proof test interval	
T_B	= Bump test interval	= 1 week
λ_{Drift}	= Failure frequency due to sensor drift/ reduced sensitivity	900/10⁹ hours
λ_{DU}	= Total dangerous undetected failure rate	931/10⁹ hours
PFD_{avg}	=Average probability of dangerous failure	

The average probability of dangerous failures where a weekly bump test partial proof test is performed and a full proof test is performed at specified intervals is given in the following graph:



Allowance must be made for the contribution the user's logic solver and final element(s) will make towards the total PFD_{avg} of the entire SIS It is reasonable to consider the PFD_{avg} of the sensor element will comprise 35% of the available SIL range, the logic solver 15% and the final element 50%. Therefore, the target of the sensor will be restricted to 35% of the available SIL range to allow development of the remaining SIS elements:

Safety Integrity Level (SIL)	Average Probability of Dangerous Failure (PFD_{avg})
4	$\geq 1x10^{-5}$ to $<1x10^{-4}$
3	$\geq 1x10^{-4}$ to $<1x10^{-3}$
2	$\geq 1x10^{-3}$ to $<1x10^{-2}$
1	$\geq 1x10^{-2}$ to $<1x10^{-1}$

a) SIL 1 target PFD_{avg} = 0.35×10^{-1}
b) SIL 2 target PFD_{avg} = 0.35×10^{-2}
c) SIL >2 Not Applicable with 1oo1D architecture due to safe failure fraction requirements

Safety Integrity Level	Full Proof Test Interval (years)*		PFD_{avg}
SIL 1 Range	Maximum allowable[1]	35	0.35×10^{-1}
	Minimum practical[2]	3.5	0.35×10^{-2}
SIL 2 Range	Maximum allowable[1]	3.5	0.35×10^{-2}
	Minimum practical[2]	4 months	0.35×10^{-3}

Note: The calculated proof test intervals are for indication only, the system developer must calculate the required proof test interval for the complete system, including sensor, logic solver and final element. The actual proof test interval required may be higher or lower than those stated in this report.

Calculation of PFH

The average frequency of dangerous failure per hour (PFH) is used for situations where a safety instrumented system is operating in high demand, or continuous demand modes of operation. In this case, any dangerous failure has the potential create a hazard. With a 1oo1D architecture, dangerous detected failures may be assumed to be safe failures only if the detection is by automatic online diagnostics, detection of a fault results in an action to put the equipment under control in to a safe state, or maintain a safe state and the time taken to detect a fault and put the equipment under control into a safe state is less than the process safety time (the time between loss of process control and a hazardous event occurring).

The PFH is given by the dangerous failure rate per hour.

[1] Exceeding the maximum allowable proof test interval increases the PFD_{avg} beyond the limits of the safety integrity level.
[2] Decreasing the proof test interval below the minimum practical value reduces the PFD_{avg} below the allowable limits of the safety integrity level

Safety Integrity Level (SIL)	Average frequency of a dangerous failure of the safety function (h^{-1})
4	$\geq 1x10^{-9}$ to $<1x10^{-8}$
3	$\geq 1x10^{-8}$ to $<1x10^{-7}$
2	$\geq 1x10^{-7}$ to $<1x10^{-6}$
1	$\geq 1x10^{-6}$ to $<1x10^{-5}$

Allowance must be made for the contribution the user's logic solver and final element(s) will make towards the total PFD_{avg} of the entire SIS It is reasonable to consider the PFH of the sensor element will comprise 35% of the available SIL range, the logic solver 15% and the final element 50%. Therefore, the target of the sensor will be restricted to 35% of the available SIL range to allow development of the remaining SIS elements:

a) SIL 1 target PFH = 3.50×10^{-6}
b) SIL 2 target PFH = 0.35×10^{-6}

PFH (credit taken for failure detection) = 0.94×10^{-6}

Therefore, the system being studied is capable of use in a compliant safety instrumented system operating in continuous or high demand mode of operation without redundancy for SIL 1 applications only.

Note: care must be taken when using oxygen analysers in continuous demand mode as some standards, such as Directive 2014/34/EU (ATEX) prohibit the use of safety devices in this mode of operation.

Diagnostics
Diagnostic measures related to the monitoring of safety functions are provided via the SILO2 Analyser and also by the OC85 Sensor in combination with the SILO2 Analyser. The diagnostic test interval is dictated by the clock-speed of the SILO2 analyser.

The response time for the release of the Safety Function on detection of a fault is: <30 s.

Diagnostics provided by the SILO2 Analyser:

- Measurement of loop resistance
- Diagnostics of the output current (4-20 mA) by feedback measurement
- Diagnostics of the alarm relay output by feedback contact
- Supervision of supply voltages (under and overvoltage)
- Plausibility checks of parameters and measured values
- RAM-Test
- ROM and EEPROM consistency check by CRC
- Program sequence monitor combined with watchdog functionality
- CPU test

Output on detection of a fault is the de-energisation of relay R3

Additional automatic diagnostics are provided through the functionality of the OC85/86 Sensor. A voltage output signal from the OC85 of 0 mV is reserved for diagnostics functions. The measured oxygen concentration must be such as to generate a negative electrical potential in the sensor signal circuit, i.e. less than 15%, An input signal to the SILO2 Analyser of 0mV from the OC85 sensor generates a measured value that exceeds 15% oxygen, causing the SILO2 analyser to de-energise the selected alarm relay(s) used for functional safety, triggering the final element to put the equipment under control into a safe state or maintain a safe state. This diagnostic function detects:

- Faults with the sensor heater that cause the sensor temperature to fall below the ionic conductivity threshold of the solid electrolyte.
- A sensor signal wire-break.

ALTERNATIVE ARCHITECTURES

This report describes the use of the ANALYSER SYSTEM in 1oo1D architecture. The system may be used in alternative architectures, but these are outside the scope of the Safety Manual. The design of alternative architectures and assessment of the associated SIL must be completed by individuals competent in functional safety.

Using alternative architectures to improve PFH or PFD_{avg}

The PFD_{avg} or PFH may be reduced by combining the ANALYSER SYSTEM in redundant architectures, such as 1oo2D. This also allows the possibility of using the 4-20 mA analogue output signals from the SILO2 to be used to provide an additional diagnostic function to detect loss of calibration, or drift, of one sensor or the other.

Using alternative architectures to improve plant availability

The number of spurious trips may be reduced by using the ANALYSER SYSTEM in a 2oo2D architecture requiring both systems to respond to a demand before putting the equipment under control into a safe state, or maintain a safe state. However, such a configuration will have a significant detrimental effect on the PFD_{avg} and PFH.

Limitations of alternative architectures due to systematic capability constraints

The Systematic Capability of the ANALYSER SYSTEM is adjudged to be SC2 (see section xxx). The maximum SIL that can be claimed for a combination of elements each of systematic capability SC2 can be no more than SIL3. It is not permitted to achieve a higher SIL than SIL3 by successively building elements of Systematic Capability SC2.

SYSTEMATIC CAPABILITY

The systematic capability is a measure (expressed on a scale of SC1 to SC4) of the confidence that the systematic safety integrity of an element meets the requirement of the specified SIL. The systematic capability is determined with reference to the requirements for the avoidance and control of systematic faults. The requirements for systematic safety integrity (systematic capability), can be met by achieving one of the following compliance routes:

- Route 1_S: compliance with the requirements for the *avoidance* of systematic faults as detailed in IEC 61508-2, 7.4.6 (hardware) and IEC 61508-3 (Software) and the control of systematic faults as detailed in IEC 61508-2, 7.4.7 (hardware) and IEC 61508-3 (Software).
- Route 2_S: Compliance with the requirements for evidence that the equipment is proven in use as detailed in IEC 61508-2, 7.4.10 (hardware and software)
- Route 3_S for pre-existing software elements only: Compliance with IEC 61508-3, 7.4.2.12.

The relationship between SC and SIL are shown in the following table:

Systematic Capability (SC)	Safety Integrity Level (SIL)
4	4
3	3
2	2
1	1

In the absence of data to provide evidence for proven in use, the systematic capability was assessed using Route 1_S for the avoidance and control of systematic faults.

The systematic capability assessed for each phase of the design process are shown in the following table:

Phase	Systematic Capability (SC)	Assessment
Design Specification	2	Validation Assessment
Design & Development	2	
Integration	2	
Validation	2	
Hardware Design (control)	2	
Environmental Stress	2	
Operational	2	
Software	2	*Risknowlodgy assessment of Mutec transmitter*

QUALITY DOCUMENTATION

Each SILO2 ZR System will be supplied with the following Documentation.

Calibration Certificate
EU Certificate of Conformity
Process Fitting Material Certificate if applicable
SIL O2 user Operation and maintenance manual

PROOF-TESTING

(See also page 27 of this manual)

Periodic proof tests must be conducted at specified intervals to reveal undetected faults that would otherwise prevent the system operating in accordance with the user's Safety Requirement Specification. Different parts of the system may require different proof test intervals and the frequency of the proof test interval must be decided by the PFDavg calculation (see section "Applying FMEDA Results").The entire system must be tested, including sensor(s), logic solver and final element(s), either end-to-end or in parts. Where the interval between scheduled process downtime is greater than the proof test interval, then on-line testing facilities must be provided.

The user must maintain records that certify that proof tests were completed as required. These records must include the following information as a minimum:

- a description of the tests
- dates that the tests were done
- name of the person(s) who performed the tests
- serial number or other unique identifier of the system tested
- results of the test

BUMP TEST PROCEDURE

A regular check of the SIL O2 Analyser operation is a requirement, to confirm the correct operation and safety related functionality of the Sensor. The following partial proof-test procedure should be carried out at 6 monthly intervals or less.

Note: This procedure should be arranged so as not create a Hazardous condition for personnel or equipment. (This procedure may be able to be carried out whilst the system and host equipment is in operational mode or it may require putting the host equipment Into an offline mode and in some applications this may require removing the Sensor from the equipment or process)

1. Apply a Bump Check Gas of 20.9% O2 to the Sensor. (Certified gas preferred for accuracy)
2. Observe the display on the SIL O2 Analyser. It should read 20.9% or be within a tolerance band of 19.5% O2 to 21%
3. If the display reads below 19.5% O2 then the sensor is demonstrating excessive drift and must be replaced, or re-tested against a certified gas (if not done so already). If the sensor still reads below 19.5% when tested against a certified gas, it must be replaced.
4. Remove the Check gas and return the Analyser/Sensor and Host equipment to operational mode.

Warning!: It is not possible to correct a failure that causes excessive drift by re-calibrating the sensor! A sensor that has failed a bump test within the specified calibration interval must be replaced.

A comprehensive Proof Test and Compliance Document SILO2-001 is available from Ntron.

The following elements should be included in any proof test procedure to be undertaken.

- Power Supply Output Voltage (See the Technical data section of this manual)
- Disconnect the Sensor from analyser to initiate a fault alarm. Main Trip/Diagnostic Relay de-activates. (simulated wire-break) Analyser resets when Sensor is re-connected.
- Analyser measured oxygen concentration is within (X)% of a reference gas concentration (check for sensor drift). (See the Technical data section of this manual)
- Selected alarm relay goes into alarm state when supplied oxygen concentration rises above alarm set point (full functional check)

NOTE: All failures, whether revealed by diagnostics, maintenance tasks or proof testing must be documented and reported to Ntron for investigation.

REFERENCES AND SUPPORTING DOCUMENTATION

Supporting documentation reviewed in preparation of the safety manual.
System Specification
Design requirement specification
Validation plan
Validation assessment
FMEDA
Risknowlogy Report
Installation Manual
User O&M Manual
EMI Report

RELEASE NOTES

Reason for release
Known issues or problems with release
Changes from previous release