XTP/XTC 601
SIL Safety Manual

Note: Supplement to instruction manual

97587 Issue 1.1
August 2020

For Michell Instruments' contact information please go to
www.michell.com

Contents

NOTE: This product must not be modified or altered in any way. Unauthorised change is not permitted and to do so would cause the Functional Safety, as confirmed by the IEC61508 assessment, to be null-and-void. This products design is strictly controlled and to do so would invalidate all approvals, certification and warranties this product holds. Please consultant Michell Instruments Ltd directly for any functionality or service quries you may have.

Safety Guidelines

This manual relates only to the SIL aspects of this product.

For all other operation, installation & maintenance information refer to the product manual. The user must not use this equipment for any other purpose than that stated. Do not apply values greater than the maximum value stated.

This manual contains information relating to the SIL aspects of operating this product. Use competent personnel using good engineering practice for all procedures in this manual.

Qualified Personnel

This product should only be set up and used in conjunction with this documentation. Commissioning and operation of this product should only be performed by qualified personnel.

Abbreviations

The following abbreviations are used in this manual:

λ	Failure Rate
λD	Dangerous Failure Rate
λDD	Dangerous Detected Failure Rate
λDU	Dangerous Undetected Failure Rate
λs	Safe Failure Rate
/hr	Per Hour
ADC	Analogue-To-Digital Converter
DAC	Digital-To-Analogue Converter
DC	Diagnostic Coverage
E/E/PE	Electrical/Electronic/Programmable Electronic
EMF	Electromotive Force
ESC	Engineering Safety Consultants
EUC	Equipment Under Control
FIT	Failure in time
FMEDA	Failure Mode Effect and Diagnostics Analysis
FMR	Failure Mode Ratio
FS	Functional Safety
FSM	Functional Safety Management
HFT	Hardware Fault Tolerance
MDT	Mean Down Time
MTTR	Mean Time To Restoration
NPRD	Non-Electronic Parts Reliability Data
O_2	Oxygen
O/C	Open Circuit
PFD	Probability of Failure on Demand
PFH	Average Frequency of a Dangerous Failure per Hour
PLC	Programmable Logic Controller
PTI	Proof Test Interval
QA	Quality Assurance
RBD	Reliability Block Diagram
S/C	Short Circuit
SFF	Safe Failure Fraction
SIF	Safety Instrumented Function
SIL	Safety Integrity Level
SR	Safety Related
Tp	Proof Test Interval

This page has been left blank intentionally.

1 INTRODUCTION

1.1 General

This manual refers only to:

XTP601 Oxygen Transmitter.
XTP601 Oxygen Analyser.
XTC601 Binary Gas Analyser.
XTC601 Binary Gas Transmitter.

There are derivatives of each model as shown in the below table:

Analyzer Name	Type	
XTP601-GP1	General purpose analyser with display	
XTP601-GP2	General purpose analyser with flame arrestors	
XTP601-EX1	Hazardous area analyser with display	
XTP601-EX3	Hazardous area transmitter	
XTC601-GP1	General purpose analyser with display	
XTC601-GP2	General purpose analyser with flame arrestors	
XTC601-EX1	Hazardous area analyser with display	
XTC601-EX3	Hazardous area transmitter	

1.2 Required documentation

This document only applies in conjunction with the following documentation:

Analyzer Name	Type	Document No.
XTP601	Process Oxygen Analyzer User's Manual (UK)	97313
XTC601	Binary Gas Analyzer User's Manual (UK)	97400

NOTE: For each type, there are manuals with the same content translated into other languages.

This document contains SIL-related data that will be required when using the XTP601 & XTC601 products in safety-instrumented systems.

It is aimed at system planners, constructors, service and maintenance engineers and personnel who will commission the device.

2 SAFETY INSTRUCTIONS

These products are intended for use in safety applications.
All safety instructions relate exclusively to the analogue output signal (4–20mA). The products are certified to SIL2 (IEC 61508). The products software is certified SIL2 (IEC61508). The use of these products integrated in to safety-related systems is therefore possible.

Definition: **Safety-instrumented system**
A safety-instrumented system executes the safety functions that are required to achieve or maintain a safe status in a system. It consists of a sensor, logic unit/control system and final controlling element.

A Safety Instrumented System (SIS) could be made of an analyser (e.g. XTP 02 Concentration), a Safety rated logic Solver (e.g. safety relay or safety rated PLC) and a final element (e.g. valve, or alarm with defined response).

Definition: **Safety function**
Defined function executed by a safety-instrumented system with the objective of achieving or maintaining a safe system considering a defined dangerous occurrence.

Example: XTP O_2 concentration above or below a defined threshold.

2.1 Safety Integrity Level (SIL)

The international standard IEC 61508 defines four discrete Safety Integrity Levels (SIL) from SIL 1 to SIL 4. Each level corresponds to the probability range for the failure in a safety function. The higher the SIL of the safety-instrumented system, the higher the probability that the required safety function will work.

The achievable SIL is determined by the following safety characteristics:

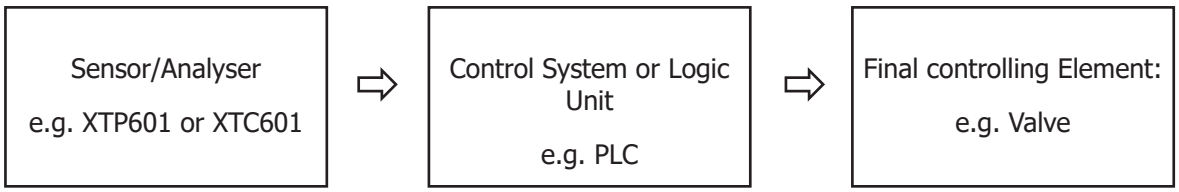
- Average probability of dangerous failure of a safety function in case of demand (PFDAvG)
- Hardware fault tolerance (HFT)
- Safe failure fraction (SFF)

Description:
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.

SIL level	PFDavg
SIL 4	10–4 > PFDavg ≧ 10–5
SIL 3	10–3 > PFDavg ≧ 10–4
SIL 2	10–2 > PFDavg ≧ 10–3
SIL 1	10–1 > PFDavg ≧ 10–2

Table 1 Safety Integrity Level

The "average probability of dangerous failures of the entire safety-instrumented system" (PFDAvG) is normally spilt between the entire SIL system.



The following table shows the achievable Safety Integrity Level (SIL) for the entire safety-instrumented system for type B systems depending on the proportion of safe failures (SFF) and the hardware fault tolerance (HFT). XTP and XTC units are considered Type B due to their complexity. Type B systems also include sensors and positioners actuators with complex components, e.g. microprocessors (see also IEC 61508, Section 2).

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

Table 2 Safety Integrity Level

3 DEVICE-SPECIFIC SAFETY INSTRUCTIONS

3.1 Applications

The Hardware assessment of the XTP601 & XTC601 shall provide the safety instrumentation engineer with the required failure data as per IEC 61508.

The hardware of XTP601 & XTC601 satisfies the requirements in terms of functional safety to SIL 2 in accordance with IEC 61508. The XTP601 & XTC601 is usable in safety applications to monitor limits.

3.2 Safety Function

The XTP601 & XTC601 are mainly used for user-defined threshold monitoring.

The XTP601 Process Oxygen Analyser was assessed against the following safety function:

- Ability to detect oxygen presence within another gas stream and generate a 4–20mA output.

The XTC601 Binary Gas Analyser was assessed against the following safety function:

- Ability to detect target gas in another gas stream and generate a 4–20mA output.

Warning
See the "Settings" and "Safety characteristics" sections for the binding settings and conditions. These conditions must be met to fulfil the safety function.

When the safety function has been executed, safety-instrumented systems with no self-locking function should be brought to a monitored or otherwise safe status within the Mean Time To Repair (MTTR). The MTTR is 168 hours.

For full product information refer to User Manuals 97313 & 97400.

3.3 Settings

After installation and commissioning (refer to User Manuals), the following parameter settings should be made for the safety function:

Safety parameters

Function	
Analog Output	Select 4–20mA (NAMUR)

Protection against configuration changes

After configuration, the menu access codes of XTP601 & XTC601 shall be changed so that the device is protected against unauthorized changes and operation.

Checking the safety function after installation

After installation a safety function test must be carried out.

Using reference gas, i.e. N_2, 4mA 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.

3.4 In case of faults

Fault

The procedure in case of faults is described in the User Manuals.

Repair

The defective product should be sent to a Michell Instruments Service Department with details of the fault and the cause. When ordering a replacement product, please specify the serial number of the original product. The serial number can be found on the nameplate.

Information regarding the location of Michell Instruments Service centres can be found at the following web address: www.michell.com

3.5 Maintenance/Calibration

We recommend that the functioning of the XTP601 & XTC601 is checked at regular intervals of one year.

Check at least the following:

Test the basic functionality of the XTP601 & XTC601 as described in the User Manual.

Checking safety

You should regularly check the safety function of the entire safety circuit in line with IEC 61508/61511.

The testing intervals are determined during the circulation of each individual safety circuit in a system. The recommended prove interval depends on the application but it should be at least once a year.

To detect dangerous undetected faults, the XTP601 & XTC601 analog output shall be checked with the following test:

To execute the safety proof test both tests (1 and 2) must be performed.

Proof test 1 consists of the steps described in the table below.

Step	Action
1	Bypass the safety PLC or take other appropriate action to avoid a false trip.
2	Generate or simulate an alarm condition to force the product to go to the high alarm current output and verify that the analog current reaches that value.
3	Generate or simulate an alarm condition to force the product to go to the low alarm current output and verify that the analog current reaches that value.
4	Restore the loop to full operation.
5	Remove the bypass from the safety PLC or otherwise restore normal operation.

Proof test 2 consists of the steps described in the table below.

Step	Action
1	Bypass the safety PLC or take other appropriate action to avoid a false trip.
2	Perform Proof Test 1.
3	Perform a 2-point calibration of the product.
4	Perform a reference measuring with at least one measuring point between min and max concentration. You must use a calibration gas with a well-known gas concentration. The expected result must have a tolerance of not more than 5%.
5	Restore the loop to full operation.
6	Remove the bypass from the safety PLC or otherwise restore normal operation.

This test will detect more than 90% of possible "du" failures in the product.

Should faults be detected, the product should not be used until completely rectified.

3.6 Safety Characteristics

The safety characteristics necessary for use of the system are listed in the SIL declaration of conformity (see Appendix A.1). These values apply under the following conditions:

- The XTP601 & XTC601 are only 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 XTP601 & XTC601 is blocked against unwanted and unauthorized changes/ operation.
- The maximum operating temperature is +40°C for the XTC601 and +55°C for the XTP601.
- All used materials are compatible with process conditions.
- The MTTR after a device fault is 168 hours.
- The logic solver (PLC) must be configured to detect over range (>21mA) and under range (<3.6mA) failure of the XTP601 & XTC601 (Fail High and Fail Low) and will recognize these as internal failures of the products and not cause a spurious trip.

Also see the Settings section of this manual and Appendix below.

Appendix A

A.1 SIL Declaration of Conformity

ENGINEERING SAFETY CONSULTANTS
The Global Provider of Functional Safety Expertise and Technical Consultancy

Certificate of Conformity to IEC 61508 Safety Integrity Level (SIL) 2

Functional Safety of Safety-Related Programmable Electronic Systems

The **Michell Instruments UK Ltd, XTP601 Process Oxygen Analyser & XTC601 Binary Gas Analyser** have been assessed and are considered capable for use in a low demand Safety Function up to SIL 2 capability with regards to systematic, random failure rates and architectural constraints.

The assessment was based on the assumptions, data provided, and recommendations given in:

- **ESC Ltd Report: H215_FM001 rev. 3.**

The products were assessed against the following failure modes:

- XTP601: Ability to detect oxygen presence within another gas stream and generate a 4-20mA output;
- XTC601: Ability to detect target gas in another gas stream and generate a 4-20mA output.

The assessment was carried out to determine compliance with IEC 61508 (2010 Edition) with regards to:

- Random Hardware Failures (20% of SIL 2 range) (refer to Table below) with a Mean Down Time (MDT) of 168 hours, a Proof Test Interval (PTI) of one year (8760 hours) and capable of revealing 100% of undetected failures;
- Architectural Constraint (Type B, SFF >90%, <99%), HFT = 0;
- Systematic SIL 2 capability against IEC 61508 (2010 Edition) Parts 1, 2 and 3.

Device	λ NSR (/hr)	λs (/hr)	λDU (/hr)	λDD (/hr)	SFF	Achieved PFD
XTP601	1.3E-07	1.6E-07	5.4E-08	7.4E-07	94%	3.6E-04
XTC601	1.3E-07	1.6E-07	3.9E-08	7.0E-07	96%	2.9E-04

IMPORTANT: It should be noted that this assessment does not include confirmation of the response time of the device. For response times (along with any relevant assumptions) reference should be made to the Safety Manual of each device and the total SIF response time **MUST** be compared against the process safety time for the specific application.

Managing Director: Kenneth G L Simpson
Member of the IEC 61508 committee
Assessment Date: February 2020, February 2022
Certificate: H215_CT001 rev. 2

ENGINEERING SAFETY CONSULTANTS LTD is ISO9001-certified by Global Group, itself a UKAS-accredited ISO9001 certification body

Reg: 12Q12086

ENGINEERING SAFETY CONSULTANTS LTD
Tuition House
27-37 St George's Road Wimbledon London SW19 4EU UK
Telephone/Fax: +44 (0)20 8542 2807
E-Mail: info@esc.uk.net Web: www.esc.uk.net
Registered in England and Wales: 7006868
Registered Office: 27-37 St George's Road Wimbledon London SW19 4EU

A.2 Engineering Safety Consultants Limited. London, UK Test Report extract

2.1 General

This report provides a Prior Use Assessment of the Michell Instruments UK Ltd, XTP601 Process Oxygen Analyser and XTC601 Binary Gas Analyser, as defined in the Prior Use requirements in IEC 61511 (2nd Edition) Clause 11.5.3 and 11.5.4 [2] including an estimation of Probability of Failure on Demand (PFD), Safe Failure Fraction (SFF) and a review of the systematic capability as supporting evidence for avoidance and minimisation of systematic failures.

A Failure Mode Effects and Diagnostics Analysis (FMEDA) was conducted on the XTP601 & XTC601 to estimate the random hardware failure rate in order to assess suitability for use in a safety function with regards to the PFD and the architectural requirements in terms of Hardware Fault Tolerance (HFT) and SFF, using the approach detailed in Route 1H in IEC 61508-2 [1].

2.2 Hardware Reliability Verification

These devices will form part of the sensor element sub-system of a Safety Instrumented Function (SIF) and thus an assessment was conducted to demonstrate its capabilities in terms of PFD. The remaining sensing, logic solver and final element sub-systems were excluded from the assessment, in order to allow for their PFD contributions, the devices were assessed against 20% of Safety Integrity Level (SIL) 2 PFD band (e.g. SIL 2 band modified to 2.0E-03).

The analysis was based on the assumption that repairs would be carried out with a Mean Down Time (MDT) of 168 hours, a Proof Test Interval (PTI) of one year (8760 hours) and capable of revealing 100% of undetected failures.

The XTP601 Process Oxygen Analyser was assessed against the following safety function:
• • Ability to detect oxygen presence within another gas stream and generate a 4–20mA output.

The XTC601 Binary Gas Analyser was assessed against the following safety function:
• • Ability to detect target gas in another gas stream and generate a 4–20mA output.

Table 3 shows a summary of the results of the XTP601 & XTC601 based on the data provided and the assumptions given in this report. The full set of results for the hardware reliability verification is presented in Table 4.

Device	PFD Target (20% of SIL2 band)	PFD achieved	PFD achieved (SIL)	SFF	Type	Achieved SIL (Architecture HFT =0)	Overall achieved SIL
XTP601	2.0E-03	3.6E-04	2	94%	B	2	2
XTC601	2.0E-03	2.9E-04	2	96%	B	2	2

Table 3 SIL Results Summary

Device Reference		XTP601 & XTC601
Function Specification		XTP601 Oxygen Transmitter XTC601 Binary Gas Analyser
Software Configuration/Settings		As per customer order
Software Version		Firmware for XTP601: 36217 V1.09 Firmware for XTC601: 37701 V1.06
Hardware Diagram version		XTP601: 80895/C V2.0 XTC601: 81003/C V1.0
Hardware Configuration/Settings		As per customer order
Failure Mode(s) Definition	Dangerous detected	dangerous detected failure rate per hour
	Dangerous undetected	dangerous undetected failure rate per hour
	Safe	safe (or spurious) failure rate per hour
Estimated failure rate		XTP601 **7.0E-07**, XTC601 **5.9E-07**
Dangerous Undetected Failures (λDU)		XTP601 **5.41E-08**, XTC601 **3.87E-08** (*FIT/hr*)
Dangerous Detected Failures (λDD)		XTP601 **7.39E-07**, XTC601 **7.00E-07** (*FIT/hr*)
Safe Failures (λS)		XTP601 & XTC601 **1.57E-07** (*FIT/hr*)
Probability of Failure on Demand (PFD)		XTP601 **3.6E-04**, XTC601 **2.9E-04**
Safe Failure Fraction (SFF)		XTP601 **94%** XTC601 **96%**
Hardware Fault Tolerance (HFT)		**0**
Classification (Type A or Type B)		**B**
Demand (Low demand or High Demand)		**Low**
Proof Testing Procedures		See section 3.5
Installation		Refer to User Manual 97313 (XTP) & 97400 (XTC)
Average lifetime of device (yrs)		**5**
Environmental Profile		Max +50°C. 80%rh>31°C/50%>+50°C
Systematic/Proven in Use Safety Integrity Level		**2**
Assumptions		Refer to User Manual
General Notes and applicable regulations		This product complies with applicable standards and clauses of EU ATEX, EMC, PED Directives. Refer to the EU Declaration supplied with each product for full details of the latest versions.
Testing requirements		See section 3.5

Table 4 Verification Results

http://www.michell.com