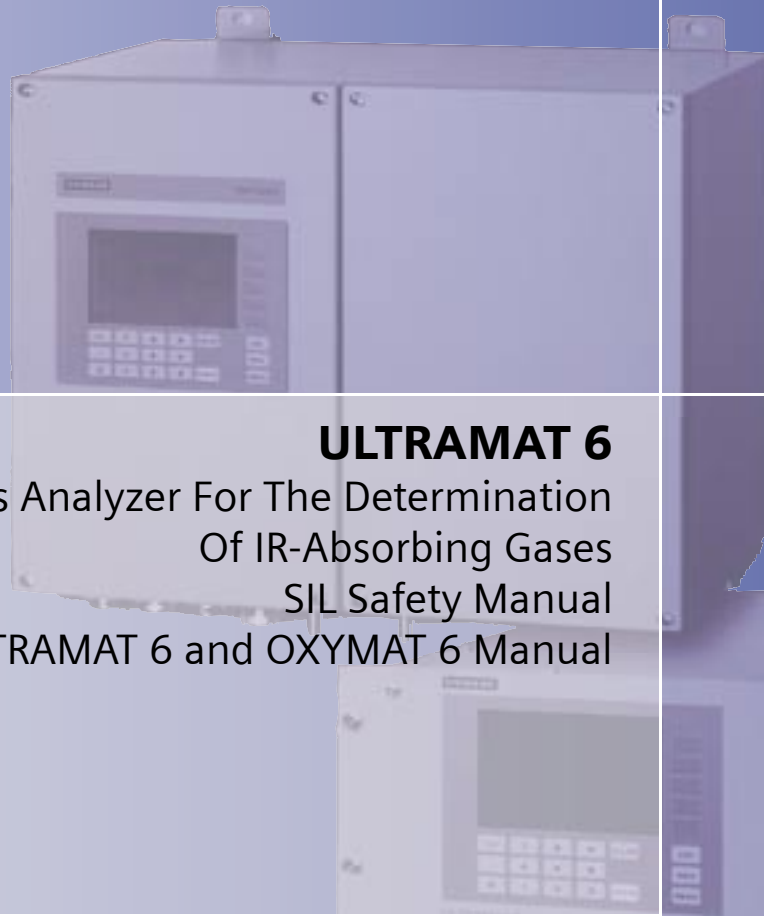**ULTRAMAT 6**

Gas Analyzer For The Determination
Of IR-Absorbing Gases
SIL Safety Manual
Supplement to ULTRAMAT 6 and OXYMAT 6 Manual

gas analysis

SIEMENS

SIEMENS

ULTRAMAT 6
Gas Analyzer for the
Determination of IR-Absorbing
Gases

SIL Safety Manual

Introduction	**1**
General safety instructions	**2**
Device-specific safety instructions	**3**
Appendix	**A**
List of Abbreviations/Acronyms	**B**

**Supplement to instruction manual
ULTRAMAT 6 and OXYMAT 6**

ULTRAMAT 6F
7MB2111, 7MB2117, 7MB2112, 7MB2118

ULTRAMAT 6E
7MB2121, 7MB2127, 7MB2123, 7MB2128, 7MB2124, 7MB2126

ULTRAMAT/OXYMAT 6E
7MB2023, 7MB2028, 7MB2024, 7MB2026

Siemens AG

Safety Guidelines

This manual contains notices you have to observe in order to ensure your personal safety, as well as to prevent damage to property. The notices referring to your personal safety are highlighted in the manual by a safety alert symbol, notices referring only to property damage have no safety alert symbol. These notices shown below are graded according to the degree of danger.

Danger

indicates that death or severe personal injury **will** result if proper precautions are not taken.

Warning

indicates that death or severe personal injury **may** result if proper precautions are not taken.

Caution

with a safety alert symbol, indicates that minor personal injury can result if proper precautions are not taken.

Caution

without a safety alert symbol, indicates that property damage can result if proper precautions are not taken.

Notice

indicates that an unintended result or situation can occur if the corresponding information is not taken into account.

If more than one degree of danger is present, the warning notice representing the highest degree of danger will be used. A notice warning of injury to persons with a safety alert symbol may also include a warning relating to property damage.

Qualified Personnel

The device/system may only be set up and used in conjunction with this documentation. Commissioning and operation of a device/system may only be performed by **qualified personnel**. Within the context of the safety notes in this documentation qualified persons are defined as persons who are authorized to commission, ground and label devices, systems and circuits in accordance with established safety practices and standards.

Prescribed Usage

Note the following:

Warning

This device may only be used for the applications described in the catalog or the technical description and only in connection with devices or components from other manufacturers which have been approved or recommended by Siemens. Correct, reliable operation of the product requires proper transport, storage, positioning and assembly as well as careful operation and maintenance.

Trademarks

All names identified by ® are registered trademarks of the Siemens AG. The remaining trademarks in this publication may be trademarks whose use by third parties for their own purposes could violate the rights of the owner.

Disclaimer of liability

While we have verified the contents of this manual for agreement with the hardware and software described, variations remain possible. Thus we cannot guarantee full agreement. The contents of this manual are regularly reviewed and corrections are included in subsequent editions. We welcome all suggestions for improvement.

Siemens AG

Table of contents

1

Introduction

1.1 General

There are two types of analyzers: Stand alone ULTRAMAT 6 analyzers and units with two analyzers: OXYMAT 6 and ULTRAMAT 6. The synonym **ULTRAMAT 6** is used for both types of devices.

The following table lists all available types:

Analyzer name	Design	Standard analyzer	Special analyzer
ULTRAMAT 6F	1 channel (1 x IR)	7MB2111	7MB2117
ULTRAMAT 6F	2 channels (2 x IR)	7MB2112	7MB2118
ULTRAMAT 6E	1 channel (1 x IR)	7MB2121	7MB2127
ULTRAMAT 6E	2 channels (2 x IR)	7MB2123	7MB2128
ULTRAMAT 6E	1 channel (2 x IR) or 2 channels (3 x IR)	7MB2124	7MB2126
ULTRAMAT/ OXYMAT 6E	2 channels (1 O_2, 1 IR)	7MB2023	7MB2028
ULTRAMAT/ OXYMAT 6E	2 channels (1 O_2, 1 IR)	7MB2024	7MB2026

1.2 Purpose of this document

This document contains information and safety instructions that you will require when using the ULTRAMAT 6 in safety-instrumented systems.

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

1.3 Required documentation

This document deals with the ULTRAMAT 6 gas analyzer exclusively as part of a safety function. This document only applies in conjunction with the following documentation:

No.	Name	Order No.
/1/	INSTRUCTION MANUAL ULTRAMAT 6E/F, OXYMAT 6E/F	C79000-G5200-C143 (German) C79000-G5276-C143 (English) C79000-G5278-C143 (Spain) C79000-G5272-C143 (Italian) C79000-G5277-C143 (French)

1.4 Change history

Currently released versions of this documentation:

Edition	Comment
10/2005	First edition (A5E00695577-01)
08/2006	Second edition: Declaration of conformity updated

1.5 Further information

Information

The contents of these instructions shall not become part of or modify any prior or existing agreement, commitment or legal relationship. All obligations on the part of Siemens AG are contained in the respective sales contract which also contains the complete and solely applicable warranty conditions. Any statements contained herein do not create new warranties or modify the existing warranty.

The content reflects the technical status at the time of printing. We reserve the right to make technical changes in the course of further development.

References

If there are references to further information on an aspect described here, these will always be found at the end of a chapter under "See also".

2

General Safety Instructions

2.1   Safety-instrumented system

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.

Example:
A safety instrumented system is made up of an analyzer (for example CO concentration), a PLC and a control valve (Figure 2-1).

Definition: Safety function

Defined function executed by a safety instrumented system with the objective of achieving or maintaining a safe system taking into account a defined dangerous occurrence.

Example:
CO concentration

Definition: Dangerous failure

Failure with the potential to bring the safety instrumented system into a dangerous or non-functional status.

Description

The analyzer logic unit/control system is a final controlling element combine to form a safety-instrumented system, which executes a safety function.

Note   This document deals with the ULTRAMAT 6 exclusively as part of a safety function.
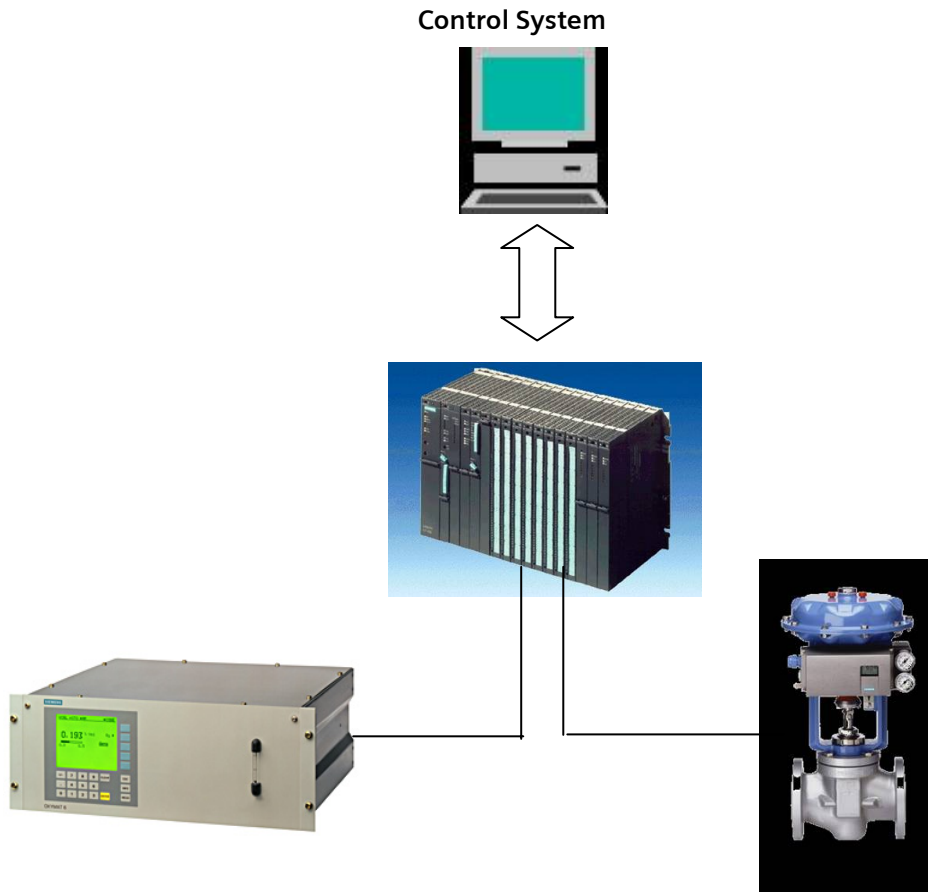

Control System

Figure 2-1   Example of a safety-instrumented system

Function

The measuring principle of the ULTRAMAT 6 gas analyzer operates on the specific absorption of molecules in the middle infrared range(2 – 10 μm) and is used to measure the concentration of ir active gases.

Special characteristics
-    Four freely-programmable measuring ranges per component, also with suppressed zero
-    All measuring ranges are inear!
-    The isolated analog output is set to 4 to 20 mA (NAMUR)

For safety instrumented systems the relay output is used for diagnostics only.

2.2 Safety Integrity Level (SIL)

Definition: 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 (PFD_{AVG})
- 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 (PFD_{AVG}). The table deals with "Low demand mode", i.e. the safety function is required a maximum of once per year on average.

SIL	PFD_{AVG}
4	$\geq 10^{-5} \ldots < 10^{-4}$
3	$\geq 10^{-4} \ldots < 10^{-3}$
2	$\geq 10^{-3} \ldots < 10^{-2}$
1	$\geq 10^{-2} \ldots < 10^{-1}$

Table 2-1 Safety Integrity Level

The "average probability of dangerous failures of the entire safety instrumented system" (PFD_{AVG}) is normally spilt between the three subsystems in the following figure.
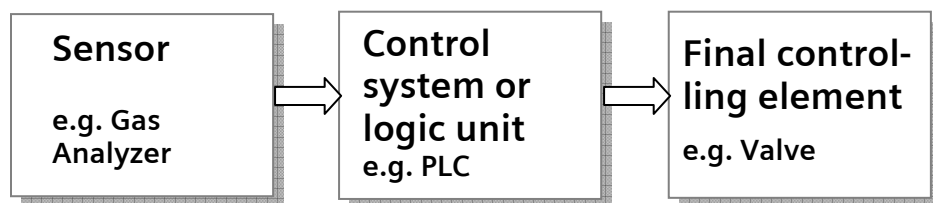

Figure 2-2 PFD distribution

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). Type B systems 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

3

Device-specific safety instructions

3.1 Applications

The Hardware assessment of the ULTRAMAT 6 shall provide the safety instrumentation engineer with the required failure data as per IEC 61508 / IEC 61511 and **does not include an assessment of software.**

The hardware of ULTRAMAT 6 satisfies the special requirements in terms of functional safety to SIL 1 in accordance with IEC 61508 or IEC 61511-1.
The ULTRAMAT 6 is usable in safety applications to monitor limits.

3.2 Safety function

The ULTRAMAT 6 is mainly used for user defined threshold monitoring. Only the analog output 4...20 mA (NAMUR) was calculated as safety function. The dangerous failure is a deviation of the output current of ±5% full span.

Warning

The binding settings and conditions are listed in the "Settings" and "Safety characteristics" sections. These conditions must be met in order 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 8 hours.

The calculated Mean Time Between Failure (MTBF) for ULTRAMAT 6 is 50 years.

Reference

Instruction manual ULTRAMAT 6 E/F, OXYMAT 6E/F (Order number see chapter 1.3)

See also

Settings (Chapter 3-3)
Safety characteristics (Chapter 3-6)

Siemens AG

3.3   Settings

After assembly and commissioning in line with the device manual, the following parameter settings should be made for the safety function:

Safety parameters

Please enter following parameter via ULTRAMAT 6 menu:

Function Number	Function	
70	Analog Output	Select NAMUR/ 4-20 mA

Reference
Instruction Manual ULTRAMAT 6E/F, OXYMAT 6E/F

Protection against configuration changes
After configuration, the ULTRAMAT 6 access codes (function number 79) shall be changed so that the device is protected against unwanted and unauthorized changes/operation.

Checking the safety function after installation
After installation of the ULTRAMAT 6 a safety function test has to be carried out (see chapter 4 "Maintenance" and 5 "Operation" of the instruction manual ULTRAMAT 6E/F, OXYMAT 6E/F).

Using zero 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 the component to be measured. The results of the measurement must be within a range of ±5% (full span) of the expected result.

3.4 Behavior in case of faults

Fault

The procedure in case of faults is described in the device operating manual /1/.

Repairs

Defective devices should be sent to the Repair Department with details of the fault and the cause. When ordering replacement devices, please specify the serial number of the original device. The serial number can be found on the nameplate.

Reference

The address of the responsible repair enter, contact, spare parts lists etc. can be found in the Instruction Manual ULTRAMNAT 6E/F, OXYMAT 6E/F at chapter 8.2 ("return delivery").

Or look at following web addresses:

www.siemens.com/automation/services&support
www.automation.siemens.com/partner

3.5 Maintenance / Checking

Checking function

We recommend that the functioning of the ULTRAMAT 6 is checked at regular intervals of one year.

Check at least the following:
Test the basic functionality of the ULTRAMAT 6 as described in the Instruction Manual /1/.

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 circulation of each individual safety circuit in a system (PFD$_{AVG}$). Recommended prove interval depends on application but max within one year. We recommend a prove test interval of once per moth.

To detect dangerous undetected faults the ULTRAMAT 6 analog output shall be checked with 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 table 3-1.

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 Gas Analyzer ULTRAMAT 6 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 Gas Analyzer ULTRAMAT 6 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

Table 3-1 Steps for Proof Test 1

Proof test 2 consists of the following steps, as described in Table 3-2.

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 two-point calibration of the Gas Analyzer ULTRAMAT 6
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

Table 3-2 Steps for Proof Test 2

3.6   Safety characteristics

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

- The ULTRAMAT 6 is 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 ULTRAMAT 6 is blocked against unwanted and unauthorized changes/ operation.
- The average temperature viewed over a long period is 40°C.
- All used materials are compatible with process conditions.
- The MTTR after a device fault is 8 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 (>21mA) and under range (<3.6mA) failure of the ULTRAMAT 6 (Fail High and Fail Low) and will recognize these as internal failure of the devices and not cause a spurious trip.

See also

Settings (Chapter 3-3)
SIL Declaration of Conformity (Chapter A.1)

Siemens AG

A

Appendix

A.1 SIL Declaration of Conformity

SIEMENS

SIL Declaration of Conformity

Functional Safety according to IEC 61508 and IEC 61511

Siemens AG
Automation & Drives
Process Instrumentation and Analytics
Östliche Rheinbrückenstr. 50
76187 Karlsruhe, Germany

Product:	ULTRAMAT 6
Ordering Nr. :	7MB2111, 7MB2117, 7MB2112, 7MB2118
	7MB2121, 7MB2127, 7MB2123, 7MB2128, 7MB2124, 7MB2126
	7MB2023, 7MB2028, 7MB2024, 7MB2026

We as manufacturer declare that the hardware of the above gas analyzer ULTRAMAT 6 is suitable for use in safety instrumented systems according to IEC 61508 / 61511. The usable safety functionality is the monitoring of user defined threshold values with a tolerance of ±5%. The appropriate SIL safety instructions shall be observed.

The failure rates were calculated via an FMEDA (Failure Modes, Effects and Diagnostics Analysis) according to IEC 61508. The FMEDA was carried out by exida.com.

Safety Related Characteristics

Device Type		B
SIL	Safety Integrity Level	1
HFT		0
PFD_{AVG}		$3,03*10^{-3}$
λ_{SD}	Safe detected Failure Rate	0 FIT
λ_{SU}	Safe undetected Failure Rate	344 FIT
λ_{DD}	Dangerous detected Failure Rate	1129 FIT
λ_{DU}	Dangerous undetected Failure Rate	691 FIT
SFF	Safe Failure Fraction	68 %

These characteristics are valid for low demand mode of operation within an 1oo1 architecture. (Guidance to calculation see IEC 61508-6, annex B). The PFD_{AVG} value is valid under the assumption of Mean Time To Repair MTTR = 8h and Proof Test Interval T1 = 8760h.

Karlsruhe, 2006, August 15th

Siemens AG

Peter Berghäuser, Project Manager

Martin Michler, A&D PI Functional Safety Manager

Siemens AG

A.2 *exida* Test Report (extract)

Management summary

This report summarizes the results of the hardware assessment carried out on the Gas Analyzer ULTRAMAT 6 with software version V4.6.1.

The hardware assessment consists of a Failure Modes, Effects and Diagnostics Analysis (FMEDA). A FMEDA is one of the steps taken to achieve functional safety assessment of a device per IEC 61508. From the FMEDA, failure rates are determined and consequently the Safe Failure Fraction (SFF) is calculated for the device. For full assessment purposes all requirements of IEC 61508 must be considered.

The failure rates of the electronic components used in this analysis are the basic failure rates from the Siemens standard SN 29500.

SIEMENS and *exida* together did a quantitative analysis of the mechanical parts of the Gas Analyzer ULTRAMAT 6 to calculate the mechanical failure rates using different failure rate databases ([N5], [N6], [N7] and *exida*'s experienced-based data compilation) for the different mechanical components (see [R1]). The results of the quantitative analysis are included in the calculations described in section 5.2.

According to table 2 of IEC 61508-1 the average PFD for systems operating in low demand mode has to be $\geq 10^{-2}$ to $< 10^{-1}$ for SIL 1 safety functions. A generally accepted distribution of PFD_{AVG} values of a SIF over the sensor part, logic solver part, and final element part assumes that 35% of the total SIF PFD_{AVG} value is caused by the sensor part. For a SIL 1 application the total PFD_{AVG} value of the SIF should be smaller than 1,00E-01, hence the maximum allowable PFD_{AVG} value for the Gas Analyzer ULTRAMAT 6 would then be 3,50E-02.

The Gas Analyzer ULTRAMAT 6 is considered to be a Type B[1] component with a hardware fault tolerance of 0.

For a Type B component the SFF has to be between 60% and 90% for SIL 1 (sub-) systems with a hardware fault tolerance of 0 according to table 3 of IEC 61508-2.

The following tables show how the above stated requirements are fulfilled.

Table 1: Summary – Failure rates

Failure category	Failure rates (in FIT)
Fail Dangerous Detected	**1129**
Fail detected (int. diag.)	810
Fail low (detected by the logic solver)	260
Fail High (detected by the logic solver)	59
Fail Dangerous Undetected	**691**
No Effect	**325**
Annunciation Undetected	**19**
Not part	**100**

---

[1] Type B component: "Complex" component (using micro controllers or programmable logic); for details see 7.4.3.1.3 of IEC 61508-2.

Siemens AG

Table 2: Summary – IEC 61508 failure rates

λ_{sd}	λ_{su} [2]	λ_{dd}	λ_{du}	SFF	DC_S [3]	DC_D [3]
0 FIT	344 FIT	1129 FIT	691 FIT	68%	0%	62%

Table 3: Summary – PFD$_{AVG}$ values

T[Proof] = 1 month	T[Proof] = 6 months	T[Proof] = 12 months
PFD$_{AVG}$ = 2,65E-04	PFD$_{AVG}$ = 1,52E-03	PFD$_{AVG}$ = 3,03E-03

The boxes marked in green (▩) mean that the calculated PFD$_{AVG}$ values are within the allowed range for SIL 1 according to table 2 of IEC 61508-1 and table 3.1 of ANSI/ISA–84.01–1996 and do fulfill the requirement to not claim more than 35% of this range, i.e. to be better than or equal to 3,50E-02.

The assessment has shown that the Gas Analyzer ULTRAMAT 6 has a PFD$_{AVG}$ within the allowed range for SIL 1 according to table 2 of IEC 61508-1 and table 3.1 of ANSI/ISA–84.01–1996 and a Safe Failure Fraction (SFF) of more than 68%.

The failure rates listed above do not include failures resulting from incorrect use of the Gas Analyzer ULTRAMAT 6.

The listed failure rates are valid for operating stress conditions typical of an industrial field environment similar to IEC 60654-1 class C (sheltered location) with an average temperature over a long period of time of 40°C. For a higher average temperature of 60°C, the failure rates should be multiplied with an experience based factor of 2,5. A similar multiplier should be used if frequent temperature fluctuation must be assumed.

A user of the Gas Analyzer ULTRAMAT 6 can utilize these failure rates in a probabilistic model of a safety instrumented function (SIF) to determine suitability in part for safety instrumented system (SIS) usage in a particular safety integrity level (SIL). A full table of failure rates is presented in section 5.2 along with all assumptions.

It is important to realize that the "no effect" failures and the "annunciation" failures are included in the "safe undetected" failure category according to IEC 61508. Note that these failures on its own will not affect system reliability or safety, and should not be included in spurious trip calculations.

The failure rates are valid for the useful life of the Gas Analyzer ULTRAMAT 6, which is estimated to be 10 years (see Appendix 3).

---

[2] Note that the SU category includes failures that do not cause a spurious trip
[3] DC means the diagnostic coverage (safe or dangerous).

B

List of Abbreviations/Acronyms

B.1   Abbreviations

Abbreviation	Full term in English	Meaning
FIT	Failure in Time	Frequency of failure of the protective function
HFT	Hardware Fault Tolerance	Hardware fault tolerance: Capability of a function unit to continue executing a required function in the presence of faults or deviations.
MTBF	Mean Time Between Failures	Average period between two failures
MTTR	Mean Time To Repair	Average period between the occurrence of a fault on a device or system and the repair
PFD	Probability of Failure on Demand	Probability of dangerous failures of a safety function on demand
PFD_{AVG}	Average Probability of Failure on Demand	Average probability of dangerous failures of a safety function on demand
PLC	Programmable Logic Controller	
SIL	Safety Integrity Level	The international standard IEC 61508 defines four discrete Safety Integrity Levels (SIL 1 to SIL 4). Each level corresponds to a range of probability for failure of a safety function. The higher the Safety Integrity Level of the safety-instrumented system, the lower the probability that it will not execute the required safety functions.
SFF	Safe Failure Function	Proportion of safe failures: Proportion of failures without the potential to bring the safety instrumented system into a dangerous on no permissible functional status.
TI	Test Interval	Testing interval of the protective function
XooY	"X out of Y" voting	Classification and description of the safety-instrumented system in terms of redundancy and the selection procedures used.
		"Y" -Specifies how often the safety function is executed (redundancy).
		"X" -Determines how many channels have to work correctly.
		Example: Pressure measurement: 1oo2 architecture. A safety instrumented system decides that a specified pressure limit has been exceeded if one out of two pressure sensors reaches this limit. In a 1oo1 architecture, there is only one pressure sensor.

Glossary

Dangerous failure

Failure with the potential to bring the safety-instrumented system into a dangerous or non-functional status

Low Demand Mode

The frequency of demands for operation made on a safety related system is no greater than one per year and no greater than twice the proof-test frequency;

Safety function

Defined function executed by a safety-instrumented system with the objective of achieving or maintaining a safe system status taking into account a defined dangerous occurrence.

Example:
Monitoring of user defined threshold values.

Safety Integrity Level

SIL

Safety-instrumented system

A safety-instrumented system excludes 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.

Example:
A safety-instrumented system is made up of a pressure transmitter, a limit signal sensor and a control valve.

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 of 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 (PFD_{AVG})
- Hardware fault tolerance (HFT)
- Safe failure fraction (SFF)