

116-BS-1386 Safety Manual
AutroSafe System

AutroSafe 4 Integrated Fire and Gas Detection System IEC61508 SIL2 certified

AUTRONICA

COPYRIGHT ©

This publication, or parts thereof, may not be reproduced in any form, by any method, for any purpose.

Autronica Fire and Security AS and its subsidiaries assume no responsibility for any errors that may appear in the publication, or for damages arising from the information in it. No information in this publication should be regarded as a warranty made by Autronica Fire and Security AS. The information in this publication may be updated without notice.

Product names mentioned in this publication may be trademarks. They are used only for identification.

CE

1 Contents

1 Contents 3
2 Definitions and references 4
2.1 Definitions and abbreviations used in this document 4
2.2 References 5
3 Introduction 6
3.1 Scope of this document 6
3.2 AutroSafe System overview 6
3.2.1 AutroSafe SIL2 system (non-Dual Safety) 7
3.2.2 AutroSafe Dual Safety SIL2 system 8
3.3 Mode of operation 8
3.3.1 Operation modes 8
4 General Safety instructions 9
4.1 AutroSafe System design 9
4.2 Safety Instrumented Function and System 9
4.2.1 AutroSafe SIL2 9
4.2.2 AutroSafe Dual Safety SIL2 9
4.2.2.1 AutroKeeper 10
4.2.3 AutroGuard V-Series fire detector SIL2 10
4.2.3.1 AutroGuard Safe state 10
4.3 Safety function diagnostics 10
4.4 AutroSafe site specific design 11
4.5 Installation 11
4.6 Commissioning 11
4.7 Operation, Maintenance, Inspection & Service 11
4.7.1 AutroSafe Dual Safety SIL2 Configuration 12
4.8 Repair & Restore 12
4.8.1 Diagnostic 13
4.8.2 AutroGuard Repair and Restore 14
4.9 Modifications (planning) 15
5 Reliability data 16
5.1 Part Reliability Data AutroSafe SIL2 16
5.2 Common Cause failures 17
5.2.1 Redundancy 17
5.2.2 β - factor 18
5.2.3 Other Common Cause failures 18
5.3 Case calculations 18
6 Timing information 19
6.1 Regulatory requirements 19
6.2 Theoretical calculation 19
6.3 Measured delay on actual system 19
7 Appendices 20
7.1 Equipment list 20
7.2 AutroSafe Maintenance Schedule 22

2 Definitions and references

2.1 Definitions and abbreviations used in this document

Term / Abbreviation	Explanation / Description / Definition
AL_Com	Autronica Loop Communication (Protocol & physical implementation) – the detector loop network
AutroCom	AutroSafe Communication. Protocol used for communication with external systems
AutroNet	AutroSafe System network. TCP/IP network for panel to panel communication and connection to external equipment (AutroCom)
DC	Diagnostic Coverage
Dual Safety	AutroSafe 4 system with redundancy on panels and I/O modules
EUC	Equipment Under Control
FAD	Fire Alarm Devices
FAT	Factory Acceptance Test
FARE	Fire Alarm Routing Equipment
FMEA	Failure Modes and Effects Analysis
FMECA	Failure Modes, Effects and Criticality Analysis
FMEDA	Failure Modes, Effects and Diagnostic Analysis
FPE	Fire Protection Equipment
FWRE	Fault Warning Routing Equipment
HFT	Hardware Fault Tolerance – “ability of a functional unit to continue to perform a required function in the presence of faults or errors”
IO	Input & Output
MTTR	Mean Time To Restore from detection of fault to operation.
OZ	Operation Zone. Scope of control & indication in AutroSafe system
PFD_{AVG}	Average Probability of Failure on Demand
PDS	A method for quantifying the reliability/availability of safety instrumented systems (SIS). See http://www.sintef.no/Projectweb/PDS-Main-Page/The-PDS-Method/
RAMS	Reliability, Availability, Maintainability and Safety
SAR	Safety Analysis Report
SAT	Site Acceptance Test. Formal verification of system installed
SIF	Safety Instrumented Function, in this context according to IEC-61508
SIL	Safety Integrity Level, in this context according to IEC-61508
SIS	Safety Instrumented System, in this context according to IEC-61508

2.2 References

Ref no	Document Identification	Document Name
1.	asafesystemd_egb	System Description
2.	asafeinstall_dgb	Installation Handbook
3.	asafecommiss_egb	Commissioning Handbook
4.	asafeoperate_fgb	Operator's Handbook
5.	sysdeenginifg_xgb	System Design and Engineering
6.	asafeconfig_egb	Configuration Handbook
7.	EN-54 part 2	Fire detection and fire alarm systems - Part 2: Control and indicating equipment
8.	IEC 61508 2010 Part 1 – 7	Functional safety of electrical/electronic/programmable electronic safety-related systems
9.	TÜV Nord Report no 12 207 555929-002	TÜV Technical report dated 5/3-2012
10.	TÜV Nord Certificate 44 207 11 555929-001	TÜV Certificate AutroSafe 4 Oil & Gas Sil2
11.	AutroCom	AutroCom descriptions:
11.1.	116-BS-1387	AutroCom Protocol Specification
11.2.	116-BS-1388	AutroCom Sliding Window
11.3.	116-BS-1389	AutroCom High Integrity
12.	OLF-070 Edition 2	APPLICATION OF IEC 61508 AND IEC 61511 IN THE NORWEGIAN PETROLEUM INDUSTRY
13.	http://www.sintef.no/Projectweb/PDS-Main-Page/The-PDS-Method	PDS
14.	TÜV Nord Report no 35152659	TÜV Technical report dated 4/9-2015 "Dual Safety"
15.	BS5839-1, DPC: DC01/540647	Fire detection and alarm systems for buildings - Part 1

3 Introduction

3.1 Scope of this document

This Safety Manual defines the requirements and recommendations on how to use the AutroSafe System where requirements for safe operation according to IEC-61508 SIL2 are applicable. Failure to complete the actions described in this document would contravene the certification requirements.

The Safety Manual is approved by TÜV as part of the AutroSafe System approval.

Further, it is the responsibility of the owner to ensure that the AutroSafe System is suitable for the chosen application and complies with the appropriate application standards.

OLF 070 [12] defines requirements for the use of IEC 61508 on the Norwegian Continental Shelf, including implementation of functions to a pre-defined SIL and requirements for management and evaluations related to maintenance, operations, and modifications. Our recommendation is to use this as a general guideline for SIL certified applications.

The typical user of this document is the responsible for engineering / installation / commissioning and/or operational planning.

This Safety Manual is not complete (as a standalone document), the referenced documents are also necessary.

3.2 AutroSafe System overview

The AutroSafe fire and gas detection system is certified to satisfy IEC 61508, SIL 1 and SIL 2 (Ref [8]). A short description of the system and its components is given in this report.

The AutroSafe 4.x system covers different types of fire and gas panels, connected through a network of panels. (See Figure 1 AutroSafe Integrated fire and gas detection System). A data channel (AutroCom) to third-party equipment may be connected to one or more of the panels. The data channel may also be connected to communication protocol converters for industry standard communication protocols. (These protocol converters are not prepared for SIL2 approval.)

Various field buses dedicated to applications connect field equipment to the panels. Field buses are AL_Com (Smoke & Heat Detectors and I/O units), PowerLoop (Power-demanding detectors) and AutroFieldBus for the distribution of PowerLoop and AL_Com loop drivers.

Multiple I/O modules (Loop drivers and input/output modules) can be connected to some panel-types. BSD-type loop modules are used as interfaces between a panel and a detector loop.

Detectors and I/O loop units are connected through the AL_Com detector loop. Detectors may also be connected via distributed Loop Drivers, on AutroFieldBus or PowerLoop.

Note that not all parts will be present in all applications. For example, the alarm output of the fire- and gas detection system may be connected to the general control system and the I/O units may be omitted. The number and types of panels are also application dependent. The requirements for integration of the AutroSafe system into a site-specific installation are described in the User manuals. See System Description [1] for more information.

3.2.1 AutroSafe SIL2 system (non-Dual Safety)

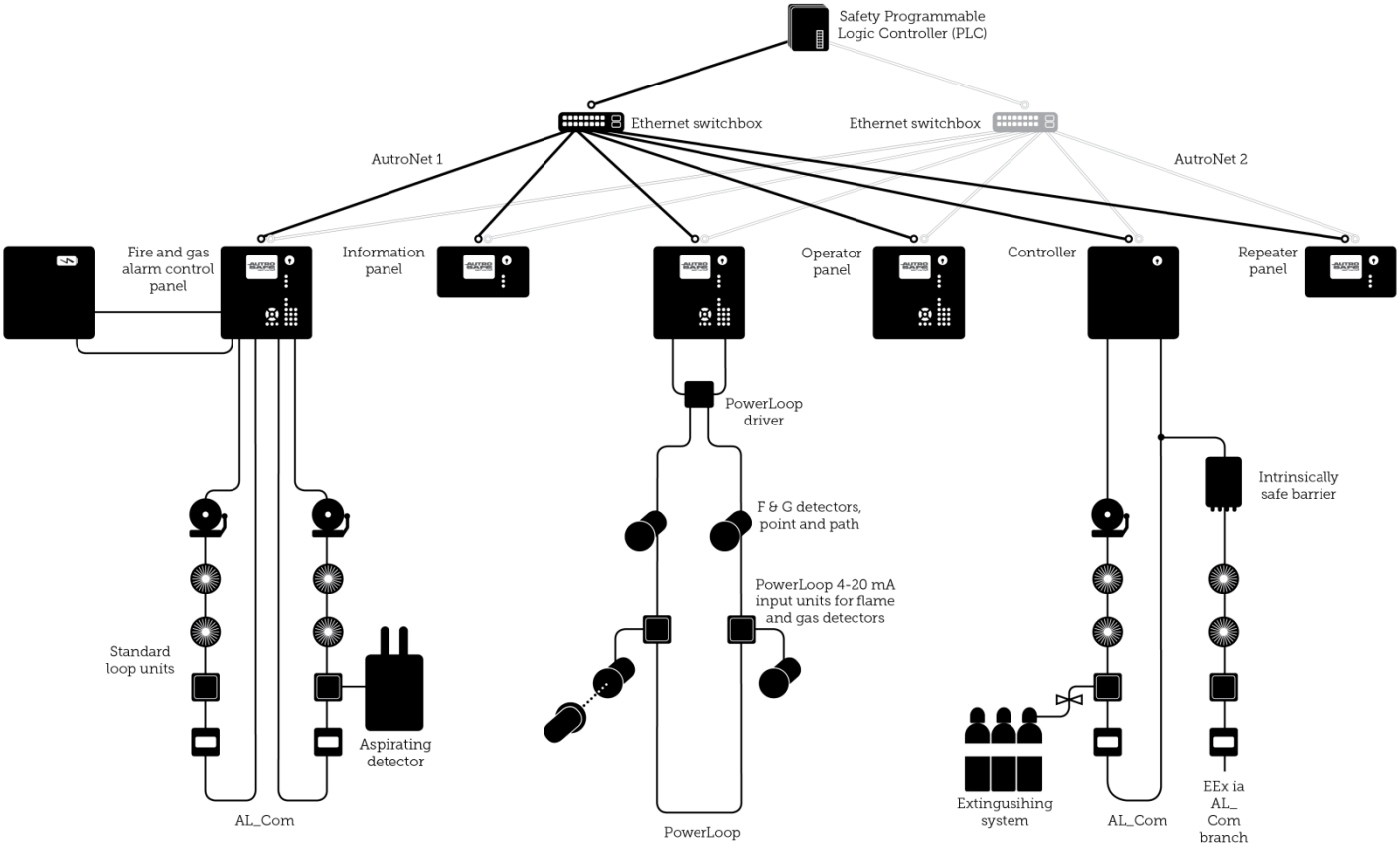


Figure 1 AutroSafe Integrated fire and gas detection System – Typical system topology

This is an example of a typical AutroSafe System. (Note that not all parts of this system are included in the IEC-61508 TÜV approval of AutroSafe. Section 7.1 Equipment list shows these).

3.2.2 AutroSafe Dual Safety SIL2 system

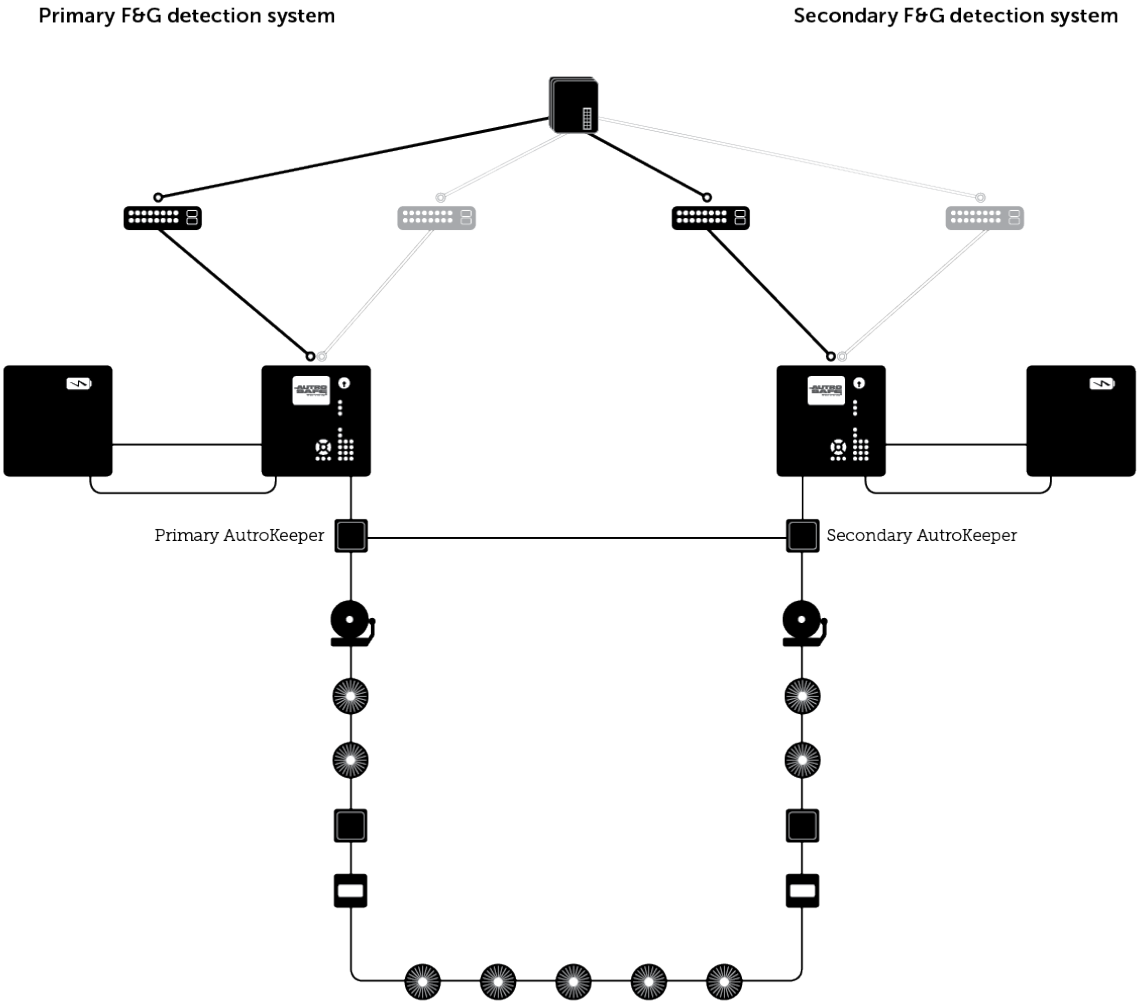


Figure 2 AutroSafe Dual Safety SIL2 – Example of redundant panel

This is an example of a simple SIL2 system (Note that not all parts of this system are included in the IEC-61508 TÜV approval of AutroSafe. Section 7.1 Equipment list shows these).

Panels, Power and I/O modules are duplicated physically in a Dual Safety installation.

3.3 Mode of operation

The AutroSafe system is approved for Low demand operation (ref [8] IEC-61508-4 sect 3.5.16).

The Operator's Handbook [4] describes Access levels to the panel operation. Methods or guidelines should be defined to ensure that unintended reduction of safety is not introduced by unauthorised personnel.

More information is provided by the AutroSafe user manuals [1-6].

3.3.1 Operation modes

During commissioning and start-up or re-initialisation of the AutroSafe system, it is not fully operational. A detailed description is found in the Commissioning handbook [3].

4 General Safety instructions

4.1 AutroSafe System design

The Safety Integrated function of any AutroSafe System is to detect alarms by fire or gas detectors, and signal them to configured outputs, by discrete signals or AutroCom data.

If the AutroSafe System is not capable of this, a fault describing the origin of the problem as closely as possible shall be signalled.

Information about the system's state is shown on the AutroSafe panel display by dedicated indicators and a buzzer which alerts personnel in the vicinity. This way of signalling via the panel operator interface is neither included in the safety function nor in the safety analysis for approval.

4.2 Safety Instrumented Function and System

The AutroSafe System is an E/E/PE system intended both as a mitigating and a proactive barrier for protecting an Equipment Under Control (EUC). Such a system may be considered as a Safety Instrumented System (SIS), which consists of at least 3 subsystems:

a) Input elements (IE) – AutroSafe Detectors that detect potentially dangerous conditions
b) Logic solver (LS) – AutroSafe Panels that analyse the input from IEs and control final elements as an effect of causes
c) Final elements (FE) – Outputs or AutroCom performing a safety function on the Equipment Under Control (EUC)

A Safety-Instrumented Function (SIF) is a function that is designed to protect the EUC against a specific demand. The IE is a subsystem of the safety-related system that performs the SIF and that is implemented by a SIS.

A Safety Integrity Level (SIL) is always related and calculated to a specific SIF and not to a SIS or individual components.

4.2.1 AutroSafe SIL2

In an AutroSafe SIL2 system, the safety function is described as follows:

a) An alarm event from a loop unit, i.e., a manual call point, smoke, fire or gas detector, shall be detected and the alarm event shall activate outputs i.e. FPE, FAD, FARE according to the site specific configuration data.
b) An alarm event shall be sent to the external systems via AutroCom according to the site-specific configuration data.
c) Fault events shall activate FWRE and any other configured outputs according to its site-specific configuration data. A fault event shall cause a corresponding fault message to be sent to external systems via AutroCom.

4.2.2 AutroSafe Dual Safety SIL2

A Dual Safety SIL2 system adds the following components and roles to an AutroSafe SIL2 system:

a) AutroKeepers that initiates and controls a loop "hot-swap".
b) Secondary panels with loop drivers. This system is "Hot-Standby" which means a running system not connected to the loop, but ready to communicate with loop units after a "hot-swap".

The secondary system (b) is a copy of the primary system with, seen in isolation, the same safety functions as the system described in 4.2.1.

The Dual Safety structure adds the following safety functions:

- "Hot-swap" the loop control from the active system to the standby system in case the active system fails to operate the loop in the following conditions:

a) Loss of power in the active system
b) Missing ping from the active system

The standby system shall monitor itself and signal faults also when the system is in standby mode. These safety functions increase the availability and fault tolerance of the total system and the availability of the loop units.

4.2.2.1 AutroKeeper

The AutroKeepers safety function is to monitor that the loop has power and communication with the active system.

On loss of power or missing ping: the AutroKeepers will automatically switch power and communication to the standby side without dropping the power on the loop. Communication will automatically be handled by the standby system which is now having control over the loop.

4.2.3 AutroGuard V-Series fire detector SIL2

The AutroGuard V-Series fire detector is the latest generation smoke and heat detectors in the AutroSafe system. It is a loop unit, functioning as input element (IE) to the AutroSafe Logic solver. As such, the IE is a subsystem of the safety-related system that performs the Safety Integrated Function (SIF), with the following safety function:

- Report fire according to EN54-5 and EN54-7 standard
    - The performance of the smoke and heat detector is defined by EN54-5 for heat detection and EN54-7 for smoke detection.
- Let the system know if a fire cannot be detected (DD-failure)

The AutroGuard is monitoring its internal state and will fail in a safe manner if the device detects an unrecoverable fault causing it to not be able to perform the primary safety function.

- If the fault does not limit the device's ability to run the application in degraded mode, the fault is communicated to the panel.
- AutroGuard Safe state: If the runtime environment of the device is compromised it will stop communicating with the AutroSafe panel, leaving the panel to assume the device is missing or dead. No output on the device will be activated.

In either case, when a fault is detected and reported to the panel and operating in degraded mode it will need to be replaced. See section AutroGuard Repair and Restore [4.8.2].

4.2.3.1 AutroGuard Safe state

The safe state of a SIS is defined as «state of the EUC when safety is achieved» The safe state of a typical fire detection system (SIS) is:

- Do not alter state of final elements
- Give audible and visible alerts that a safe state is reached

For the IE subsystem, a safe state may be defined as

- Do not answer to messages
- Do not impact loop communications

4.3 Safety function diagnostics

The requirements of EN-54 part 2 define periodic verification of safety critical functions. A description of diagnostics and reports are shown in section Repair, Diagnostic [4.8.1].

4.4 AutroSafe site specific design

There are some constraints that must be observed to obtain safe operation:

Operation Zones (OZ) should be used carefully in SIL approved applications to make sure that the system is kept simple and manageable. The OZs define a hierarchic partitioning of the system. Alarms, Faults etc. are propagated upward in the OZ hierarchy. Commands such as Reset and Silence are propagated downwards. Activation of Fire Alarm Devices and Fire Protection Equipment can in principle be configured across the OZ hierarchy. This should be avoided to ensure that alarms always can be silenced, and the system can be reset in a logical and straightforward way. This is ensured by not using more than two levels in the OZ hierarchy and to not cross connect Cause & Effect relations between adjacent OZs.

The only exception for using a third level of OZs is that these OZs are used to collect outputs that shall be activated as a group.

If a new installation reuses a configuration from another installation, care shall be taken to ensure that parts or the whole of it is not integrated into a different setting unless risks and / or consequences are evaluated.

The specified time of reaction is defined for the first event; if multiple events appear in a short timeframe, it may require longer processing and action time.

Data or signals from equipment not listed in the List of approved products must not be used in logic that interferes with the safety function(s). For example: input units or IO Modules that are not approved, or non-compliant items using standard AutroCom communication like Modbus/Espa etc. should not inhibit, disable or in other ways prevent a potential activation of a safe function.

The network used for AutroNet shall only be utilised for the AutroNet and AutroCom data traffic. Modbus may be used for transmission of information to an external system but shall not have any influence on the safety functions.

The outputs from the AutroSafe System are AutroCom High Integrity only or by outputs from the list of certified equipment only (See TÜV Certification Report [9]).

Power sourced to the system shall be redundant to ensure reliability and avoid common factors of failure over the system. Likewise, power sourced from the AutroSafe system to vital parts distributed in the system that is engineered for the safety application shall be redundant and have separated physical paths.

In AutroSafe the communication by AutroNet or field buses are designed for redundancy by duality or ring structures. It is required to install the cable and wiring so that this redundancy is maintained and also robust to cabling trouble.

4.5 Installation

Requirements to mechanical fitting / electrical connection/ EMC/ shielding & grounding/ heat dissipation / environment etc. are described in the Installation Handbook [2].

4.6 Commissioning

The AutroSafe system shall be engineered and commissioned by certified personnel trained in and having knowledge of the product and the safety requirements it is intended for.

Recommendations and guidelines for configuration & commissioning are described in commissioning handbook [3].

Prior to the operational use of the system, a full SAT or FAT shall be made to verify all causes and effects completely to ensure that all safety functions are correct. (These tests are normally dictated by the end user). See also the list of periodic verification, Appendix 7.2 AutroSafe Maintenance Schedule.

4.7 Operation, Maintenance, Inspection & Service

During the life cycle of the product, personnel with sufficient competence shall be responsible for performing the defined tasks.

A periodic maintenance scheme is described in Appendix 7.2 AutroSafe Maintenance Schedule. The PFD_{AVG} calculations (later in this document) are based on either 12 months or 18 months periods. Thus, the calculated figures according to test period of AutroSafe may be adapted to the integration's requirements.

The AutroSafe System shall be in Access level 1 (or 2) in operation. Entering access level 3 shall only be allowed for competent personnel and with care, as parts of the system may be set out of function.

If 3rd party equipment is interfaced to AutroSafe the corresponding user manuals and Safety manuals of these shall be used during the lifecycle of the installation.

4.7.1 AutroSafe Dual Safety SIL2 Configuration

It is possible to configure Dual Safety systems to either only transfer the loops that are lost from the Active system, or to select that all loops shall be transferred if the criteria for transferring one loop is satisfied. This is done by choosing "Swap loop control for all loops" in Site Configuration System Settings in the configuration tool.

A Dual Safety system will by default not initialise automatically. However, it is possible to configure the primary system to automatically initialise by choosing "Dual Safety automatic initialisation" in the configuration tool.

4.8 Repair & Restore

AutroSafe will diagnostic itself and report faults if they occur. A textual description of the fault is presented on the display of the panel. It will also be reported on AutroCom.

4.8.1 Diagnostic

Diagnostic intervals	Diagnostic	Result of failure
< 100s	HW Watchdog & System Monitoring of SW tasks	Restart or System Fault
	Fault in communication lines; AutroNet, AutroFieldBus, Powerloop; Al_Com, AutroCom	Fault condition & indication
	Fault in or/ missing units (no answer on polling)	Fault condition & indication
	Power supply; voltage or temperature outside spec	Fault condition & indication
< 15 min	Missing battery	Fault condition & indication (report)
< 30 min	Missing power supply	Fault condition & indication
< 1hour	Site specific configuration data, SD flash	Fault condition & indication
	Site specific configuration data, RAM	Restart or System Fault
< 4 hours	Battery high resistance	Fault condition & indication
< 24 hours	SD memory file check (Program & site-specific configuration data)	Fault condition & indication
	SV of all detectors (of SV type)	Fault condition & indication Or log only (depends on Config setting)
Restart of system	All of the above, plus:	
	Deep Memory check	Halted start-up / System Fault
	File system check & file check	Try to repair or Halted start-up
	Compatibility Program version vs site Specific configuration data	Halted start-up / Commission mode
	Panel switch settings consistency	Halted start-up / Commission mode

The fault report indicates the source of the problem, and the responsible for responding to a fault can use this to isolate the problem. The log should also be examined, especially after a reboot or System Fault.

The Main CPU controls the Panel Operational State relay per panel. The relay is in the activated state if the application software is running. It is switched to the deactivated state in the following situations:

- Power off
- Panel is in the Safe State / System Fault
- The Application SW is not initialised, i.e., not able to react on any type of input from field devices.

Outputs and indications like Fault, Disablements, Point Inhibit, FWRE / Common Trouble are invalid unless the Panel Operational State output signal is activated.

The scope and consequence of the fault shall be evaluated to ensure that the required safety level is maintained.

Availability of Spare parts should be planned to maintain a certain MTTR, based on the requirements

at the site. The FMEDA calculations of AutroSafe assume MTTR=8 hours.

Once the parts have been replaced and system set into operation, functional verification shall be performed to verify that the system is fully operational after the repair. It should be noted that it is the customer's responsibility to obtain a proper MTTR when planning the operation of the site.

A restart in a Dual Safety system will require manual interaction to get the system in a fully functional state. Automatic start-up of the primary system is configurable.

4.8.2 AutroGuard Repair and Restore

AutroGuard will diagnostic itself and report faults if they occur. A textual description of fault reports is presented on the display of the AutroSafe panel. Faults will also be reported on AutroCom. The detector can also stop responding (either deliberately or due to HW failures) in which case AutroSafe will detect this and report the detector missing.

Diagnostic intervals	**Diagnostic**	**Result of failure**
< 24h	SelfVerify™	Reported, no action taken
< 45s (reported after 90s)	Ping from AutroSafe	Detector reported as missing
< 10s (reported after 2h)	CPU temperature	AutroGuard Safe state
< 10s (reported after 100s)	Internal voltage	For minor discrepancies: Reported, no action taken For large discrepancies: Detector reported as missing
< 10s	Verification of chamber sensors	Compensate for dust ingress Report fault when compensation limit reached
< 2s	HW Watchdog & System Monitoring of SW tasks	Attempt to fix with restart: AutroGuard Safe state after 8 failed restarts within a time limit
< 2s (reported after 20s)	Poll on internal interface	Attempt to fix with restart: Detector reported missing
< 1s (reported after 30s)	NTC temperature	Report short circuit or missing sensor
continuous (reported after 10m)	Verify DAC to ADC	Report sensor failure
continuous (reported after 24h)	Verify program memory	AutroGuard Safe state
continuous (reported after 7m)	Verify EEPROM (config data)	Reported, no action taken
continuous (reported after 4h)	Check of RAM	AutroGuard Safe state
continuous (reported after 4h)	Check of CPU core	AutroGuard Safe state
continuous (reported after 4h)	Check peripherals	AutroGuard Safe state

Table of AutroGuard diagnostics intervals

In a AutroSafe system, the loop units are configured from the panel. Repairing a faulty AutroGuard always means replacing it with a new device of the same type. Autronica recommends having spare parts available on-site. For some persistent faults, the AutroGuard will continue working in degraded mode. However, all persistent faults will require a replacement of the unit. Persistent faults arising in the AutroGuard base (as reported on the AutroSafe panel), means that base must be replaced. When replacing a unit, it will be automatically configured by AutroSafe.

4.9 Modifications (planning)

Modifications of an existing AutroSafe application should go through all relevant steps of the initial installation procedure. To this end, the documentation of the initial installation process and the SAT checklist should be used as a basis to generate simplified modification checklists.

These checklists must then be followed to ensure that the resulting modified AutroSafe system is still working as intended. Special consideration should be given to the modification of the AutroSafe configuration, because of its safety relevance.

5 Reliability data

The calculation of the reliability data is shown in Appendix, [5.1]. Engineering judgement based on IEC-61508-2010 [7] together with PDS-data [Ref 13] has been performed during the first approval of AutroSafe to IEC-61508. All units are Type B according to the definition in IEC 61508 part 2 (Ref [8])

5.1 Part Reliability Data AutroSafe SIL2

Data of each product is extracted from the respective RAMS / Diagnostic coverage or FMEDA documents. The data will be sufficient to integrate AutroSafe in an installation.

Component	SFF [%]	λ_D	DC	Single channel (Technical Report No. 12 799 416000-002)		Dual Safety – HFT1 struture (1oo2D)	
				PFD_{AVG} T1 = 12 months	PFD_{AVG} T1 = 18 months	PFD_{AVG} T1 = 12 months	PFD_{AVG} T1 = 18 months
BSD-31x	96,0 %	8,00E-08	0,90	3,57E-05	5,32E-05	1,84E-06	2,74E-06
BSB-310	96,0 %	8,00E-08	0,90	3,57E-05	5,32E-05	1,84E-06	2,74E-06
BSJ-310	86,0 %	3,00E-08	0,30	9,22E-05	1,38E-04	3,53E-06	5,29E-06
BSE-310	95,3 %	7,00E-08	0,90	3,12E-05	4,66E-05	1,99E-06	2,97E-06
BSE-320	84,0 %	8,00E-08	0,60	1,41E-04	2,11E-04	1,69E-05	2,54E-05
BSD-340	96,0 %	8,00E-08	0,90	3,57E-05	5,32E-05	1,84E-06	2,74E-06
BD(H)-***/**	96,3 %	1,00E-06	0,91	4,02E-04	5,99E-04	2,05E-05	3,07E-05
BHH-***	95,6 %	3,84E-07	0,94	1,02E-04	1,51E-04	7,37E-06	1,09E-05
BHH-320&520	95,7 %	6,65E-07	0,93	2,16E-04	3,21E-04	1,52E-05	2,27E-05
BF-***	81,8 %	3,00E-07	0,33	8,75E-04	1,31E-03	5,52E-05	8,35E-05
BN-221/01	91,5 %	1,43E-06	0,85	9,44E-04	1,41E-03	8,94E-05	1,34E-04
BN-221/02	91,4 %	6,42E-07	0,86	4,04E-04	6,04E-04	4,93E-05	7,37E-05
BN-300&500	91,0 %	9,00E-08	0,90	4,01E-05	5,99E-05	6,56E-06	9,79E-06
BN-310	90,1 %	4,30E-08	0,84	3,06E-05	4,57E-05	4,17E-06	6,22E-06
BN-320	90,1 %	4,30E-08	0,84	3,06E-05	4,57E-05	4,17E-06	6,22E-06
BZ-500	98,0 %	2,00E-08	0,90	8,92E-06	1,33E-05	1,99E-07	2,95E-07
BN-300M	91,0 %	9,00E-08	0,90	4,01E-05	5,99E-05	6,56E-06	9,79E-06
BSD-321	96,0 %	8,00E-08	0,90	3,57E-05	5,32E-05	1,84E-06	2,74E-06
BN-342	91,0 %	9,00E-08	0,90	4,01E-05	5,99E-05	6,56E-06	9,79E-06
V-530, all variants	99,910 %	1,18E-07	0,9988	2,02E-06	2,32E-06	6,77E-08	8,73E-08
V-110, V-120, all variants	99,707 %	8,60E-08	0,9956	2,69E-06	3,53E-06	1,26E-07	1,79E-07
V-530 and V-110, V-110/RETRO or V-120	99,816 %	2,04E-07	0,9975	4,71E-06	5,84E-06	1,95E-07	2,68E-07
AutroPoint HC300PL	97,1 %	3,04E-06	0,95	6,68E-04	9,90E-04	4,44E-05	6,63E-05
AutroFlame X33AF PL	98,3 %	1,60E-06	0,97	2,54E-04	3,74E-04	1,09E-05	1,62E-05
BN-180	86,6 %	8,00E-08	0,73	9,42E-05	1,41E-04	1,16E-05	1,74E-05
(BS-420)							
BSA-400 Std alone	93,7 %	1,13E-06	0,93	3,43E-04	5,10E-04	4,15E-05	6,19E-05
BSA-400 Ethernet & Multifunct	96,2 %	2,69E-06	0,96	5,44E-04	8,05E-04	4,03E-05	5,99E-05
BSA-400A All functions	91,1 %	3,71E-06	0,90	1,65E-03	2,46E-03	2,61E-04	3,91E-04

The interpretation of these data (by each column in the table) is defined in IEC 61508-4 (Ref [8])

NOTE 1: For AutroGuard (V-530, V-110/*, V-120) the MTTR is set to 12 hours in the calculations above. For all other devices the MTTR is assumed to be 8 hours.

Component	λ_{TOT}	MTTF [hours]	Average availability *)
BSD-31x	2,00E-07	5 000 000	99,99984 %
BSB-310	2,00E-07	5 000 000	99,99984 %
BSJ-310	1,50E-07	6 666 667	99,99988 %
BSE-310	1,50E-07	6 666 667	99,99988 %
BSE-320	2,00E-07	5 000 000	99,99984 %
BSD-340	2,00E-07	5 000 000	99,99984 %
BD(H)-***/**	2,40E-06	416 667	99,99808 %
BHH-***	5,12E-07	1 955 034	99,99959 %
BHH-320&520	1,11E-06	900 901	99,99911 %
BF-***	1,10E-06	909 091	99,99912 %
BN-221/01	2,50E-06	400 160	99,99800 %
BN-221/02	1,06E-06	946 074	99,99915 %
BN-300&500	1,00E-07	10 000 000	99,99992 %
BN-310	7,00E-08	14 285 714	99,99994 %
BN-320	7,00E-08	14 285 714	99,99994 %
BZ-500	1,00E-07	10 000 000	99,99992 %
BN-300M	1,00E-07	10 000 000	99,99992 %
BSD-321	2,00E-07	5 000 000	99,99984 %
BN-342	1,00E-07	10 000 000	99,99992 %
V-530, all variants	1,52E-07	6 577 217	99,99982 %
V-110, V-120, all variants	1,30E-07	7 717 121	99,99984 %
V-530 and V-110, V-110/RETRO or V-120	2,82E-07	3 550 859	99,99966 %
AutroPoint HC300PL	5,00E-06	199 840	99,99600 %
AutroFlame X33AF PL	3,21E-06	311 429	99,99743 %
BN-180	1,60E-07	6 249 266	99,99987 %
(BS-420)			
BSA-400 Std alone	1,21E-06	829 119	99,99904 %
BSA-400 Ethernet & Multifunct	3,13E-06	319 622	99,99750 %
BSA-400A All functions	4,14E-06	241 784	99,99669 %

NOTE 2: HFT is the Hardware Fault Tolerance of a unit to achieve the defined SIL level. A hardware fault tolerance of N means that N + 1 fault is the minimum number of faults that could cause a loss of the safety function, ref [8-2].

NOTE 3: For AutroGuard (V-530, V-110/*, V-120) the MTTR is set to 12 hours in the calculations above. For all other devices the MTTR is assumed to be 8 hours.

In a SIL2 system BSJ-310, BSE-320, BF-xxx and AutroCom & AutroNet all have a HFT = 1.

5.2 Common Cause failures

5.2.1 Redundancy

There are few parallel dependency paths where common cause failures apply. It is most visible when considering redundancy, as any common failure mechanism will affect both. The AutroSafe System is mostly singular, however the field equipment is cabled as loop cabling. In addition, there are two diverse power sources. This applies to the AutroNet, AutroFieldBus, PowerLoop and AL_Com loops.

The loop structure creates redundancy, and the strength is that there is a higher probability of

physical distance between the two paths at installation (compared to dual redundant buses). Common cause failures here may be:

- Distributed weak connection or short (not a certain defined point of break or short, which then makes it difficult to detect).
- Design weaknesses (systematic failure) that lead to a failure to operate the isolation in each device.
- Power supply failure.
- Environmental problems (humidity / water flow, electrical (noise), temperature).
- User errors leading to overload at certain events.

The use of a loop structure for cabling and isolation in each device is robust against single faults in the cabling itself. Multiple faults will of course have more drastic effects (two breaks on the same loop will make multiple devices lost). Single faults on field equipment are considered to be isolated.

A Dual Safety configuration will reduce the effect of common cause failures on network and panels as long as the Primary and Secondary systems are completely separated.

5.2.2 β - factor

When applying this at a plant, plant specific β- factors should be adopted. Note that the engineering of the site influences this factor; separation of equipment and cables, common power supplies, temperature control of equipment ambient etc.

5.2.3 Other Common Cause failures

Activators sharing the same equipment as the detector that is intended to trigger them. Examples:

- Outputs on the same loop as the detector. Loop driver or cable problems etc. affect both.
- Outputs on the same panel as detector. Panel failure will prevent activation.

Stress

If components are stressed more than expected, caused by electrical, temperature or humidity outside specified range, this will probably affect several products.

Power supply failure

Overload at certain events, reduced capability etc.

Other situations

Excessive stress and Abnormal situations that may occur, like water flow / ingress, natural events like earthquake, hurricanes, fire in the installed system area, physical damage from vehicles, animals and falling trees etc.

5.3 Case calculations

A set of typical cases of installations is described in the TÜV certification report [9], with calculations of PFD_{AVG}.

6 Timing information

This section describes the timing information of critical events in the system. We want to look at the time from a decision about a hazard (fire detected) has been made in an input element (smoke detector) until that information is communicated, processed by the logic solver and results in an activation of an output element (digital output signal).

We provide theoretical numbers based on design review and compare this with measure results. We also refer to regulatory requirements.

6.1 Regulatory requirements

According to EN 54-2 [7] a delay between fire detection and response can be 10s. BS5839-1 [15] has a further recommendation for manual call-points that the delay should not exceed 3s. The AutroSafe system is therefor designed and tested according to a maximum delay of 3s.

6.2 Theoretical calculation

The AutroSafe system guarantees that in a situation of multiple alarms at the same time, the first alarm will arrive in a predictable manner and that all alarms will be received eventually. We assume therefor that the system is idle and calculate the delay for the first alarm to be processed and an output activated. Even in an idle system there are traffic being transmitted on communication paths, so we add the time to wait for the bus to become available for high priority messages.

Initiating device	Receiving device	Transmission / Processing	Best case	Worst case
116-V-530	116-V-100	LU-bus	50ms	55ms
116-V-100	116-BSD-310	AL_Com	150ms	250ms
116-BSD-310	116-BS-420G2	AL_Com+	100ms	200ms
116-BS-420G2	116-BS-420G2	C&E	30ms	35ms
116-BS-420G2	116-BSB-310A	AL_Com+	100ms	200ms
116-BSB-310A	External output	Output pin	30ms	35ms
		Total time	**460ms**	**775ms**

Table: Communication time delay, split into time for each transmission.

6.3 Measured delay on actual system

Manual testing using calibrated equipment shows: **510ms**.

7 Appendices

7.1 Equipment list

List of Products approved for use with AutroSafe 4.x

Product no.: System Units	**Description:**
BS-420G2	BS-420G2 is a complete fire alarm control panel with full operation capabilities. Ref. datasheet bs420_cgb.pdf
BC-420G2	The Controller, BC-420G2, serves as a connection unit for the detection loop, alarm sounders, controls and inputs. Ref. datasheet bc420_cgb.pdf
BC-440G2	Same as BC-420G2 but for rack mounting
BU-420G2	The fire brigade panel BU-420G2 displays alarms and allows you to operate alarms and receive additional information related to the relevant operation zone. To operate alarms, a fireman's key must be used. Ref. datasheet bubv420_cgb.pdf
BV-420G2	The Information Panel BV-420G2 serves as an indication device only. It provides information related to the defined operation zone(s). Ref. datasheet bubv420_cgb.pdf
BS-430G2	BS-430G2 serves as an operating panel for one or several defined operation zones. Ref. datasheet bs430_cgb.pdf
IO Modules in System Products	
BSD-310, 311	Detector Loop driver module
BSB-310	4 Monitored outputs module
BSJ-310	8 Open collector outputs module
BSE-310	4 Monitored inputs module
BSE-320	8 Galvanic isolated inputs module
BSS-310A	Power supply for IO Modules
BSL-310	Communication Module
BSS-311	Dual Power Monitoring unit
AutroFieldBus & PowerLoop Units	
BSD-340	PowerLoop driver module
BSD-321	AutroFieldBus to serial Interface
Detector Loop Units	
BDH-200, 300, 500	Heat detector
BHH-200, 300, 500	Smoke detector
BHH-320, 520	Multi sensor

BF-XXX	Call point
BN-221/01	State machine unit
BN-221/02	Monitored Output unit
BN-300, 500	Input unit
BN-310	Relay output unit
BN-320	I/O unit
BZ-500	Ex-barrier
BN-300M	Modular input unit
AutroGuard V-Series	
V-530	Smoke, heat and multi sensor
V-110	Standard socket (also includes retro variant)
V-120	Certified explosion proof (also includes retro variant)
AutroGuard Retro spare part detector	
BHH-5XX/X/SPARE	AutroGuard Retro spare part detectors, replaces 116-BHH-5XX/X
BDH-5XX/X/SPARE	AutroGuard Retro spare part detectors, replaces 116-BDH-5XX/X
PowerLoop	
BN-342	4-20 mA Input unit
AutroPoint HC-300 PL	Gas detector
AutroFlame X33AF PL	Flame detector
Other parts	
BSL-332	Profisafe protocol converter
BN-180	AutroKeeper (Dual Safety)

7.2 AutroSafe Maintenance Schedule

There are many factors to consider when setting up a maintenance schedule. Among important factors to consider are classification, National / Government regulations, SIL requirements, etc. From our experience with various oil and gas installations, we recommend reviewing the contents of the table below when defining your site's maintenance schedule:

Autronica supplies quality products, of which most possess a built-in self-checking functionality. The detectors can detect errors as they occur. The self-test ensures that the detector can initiate an alarm when it should, and at the right level (it is a calibrated alarm test). In environments such as a production platform, FPSO (Floating Production Storage & Offloading) and refinery, etc., there is always a risk that a sensor or detection chamber can be physically covered. It is therefore very important that a visual inspection is done regularly.

Note that the latest series of detectors (AutroGuard) comes with built in cover-detection.

Detector/Equipment:	**Type:**	**Polluted or Loaded areas: [Yes/No]**	**Schedule:**	**Notes:**
Smoke/Heat – detectors	BH-50x [/S,/EX,/N], BD-50x, V-530 [HS/UL/EX]		12-24 months	Depending on area classification, it is possible to make a schedule where you test, for example, 20% random detectors. Every detector does a SelfVerify check every day, where the detector tests itself for errors/pollution.
Smoke/Heat – detectors	BH-50x [/S,/EX,/N], BD-50x, V-530 [HS/UL/EX]	Yes	6-12 months	SelfVerify will do a calibrated check on each detector every day, but in heavy polluted areas it is recommended to make a visual inspection more often.
Manual Call Points	BF-50x [/EX]		3 months	Visual Inspection
Manual Call Points	BF-50x [/EX]		6 months	Function test
Flame Detectors	X33AF		6 months	Visual Inspection -- A calibrated optical integrity test is done every 60 seconds and it is therefore not necessary to perform manual functional testing.
Flame Detectors	X33AF	Yes	3 months	Visual Inspection
Flame Detectors	X33AF		12 months	Function test
Gas Detectors	HC-200, HC-300PL		3 months	Visual inspection
Gas Detectors	HC-200, HC-300PL		12 months	Function test
Gas Detectors	Toxic (Electro Chemical), Catalytic Gas sensors		3 months	Visual inspection and calibration have to be done on a regular basis. These detectors are not self-checking, and the sensors will inherently degrade over time.
Field mounted Input/Output modules			12 – 24 months	Visual inspection

AutroSafe, controllers, repeater panels, modules etc. placed in equipment/instrument rooms etc.	See List of Equipment [sect 7.1]		1 month	Functional test of Alarm from a point Fault report from a loop unit NOTE: Monthly tests unless actual events have taken place, then these will be valid as a test (check event log)".
AutroSafe, controllers, repeater panels, modules etc. placed in equipment/instrument rooms etc.	See List of Equipment [sect 7.1]		1 year (or interval defined by the site-specific T1 = Test Interval)	Full service. Visual inspection of all parts. Verify cause / effects, batteries, pollution of detectors, check events in logs and reports. Perform a Power On restart of the system.

1) Recommendations for the periodic service of the overall system is described in “AFS-02508 Sjekkliste ved periodisk kontroll” (Norwegian only)