ENGINEERING
TOMORROW

Safety Guide

LLS 4000/4000U

Contents

Introduction

Scope of the document

This document supplies functional safety data about the device. This data agrees with the IEC 61508 standard.

General hint

This level detector is a functionally-safe level detector. It may be deployed within safety critical systems requiring the safety function (for more data, refer to Specification of the safety function on page 7) at a safety integrity level 2.

In case of a detected potentially hazardous failure, the system performs a safety reaction to bring the device to a safe state, which is indicated by a safe position on the output relay. Depending on the failure class, the device will resume the detection mode as soon as the cause of the failure disappears (application dependent failure) or remains in failure mode (internal system failure). In the latter case, operator's interaction is required to restart the detection mode.

For safe operation, the operator / integrator must fulfil some conditions. These conditions are defined as Safety Application Conditions (SAC). For more data, refer to Safety application conditions (SAC) on page 7.

INFORMATION!

*The data in this supplement only contains the data applicable to the SIL approval. The technical data for the standard version in the Datasheet (document **[N1]**) shall be valid, provided that it is not rendered invalid or replaced by this supplement. If necessary, parts of document [N1] are referenced herein.*

INFORMATION!

Installation, commissioning and maintenance may only be carried out by approved personnel.

Device description

Detections are given through 1 output options:

- one switch output - relay

Detections can also be displayed via an application on a smart device with Bluetooth connection. The switch output - relay is the safety function.

When the device detects a measurement error, it switches the output relay to "safe" position. The "safe" position is the OPEN state.

Refer also to "Device description" in the Datasheet (document **[N1]**).

Device variants

The model name for the level transmitter and its options are identified by the VF type code on the device nameplate.

The SIL variant of the device shows a SIL2 logo on the device nameplate. When this logo appears on the device nameplate, the device is delivered for safety applications If this logo does not appear on the device nameplate, the device shall not be used for safety applications.

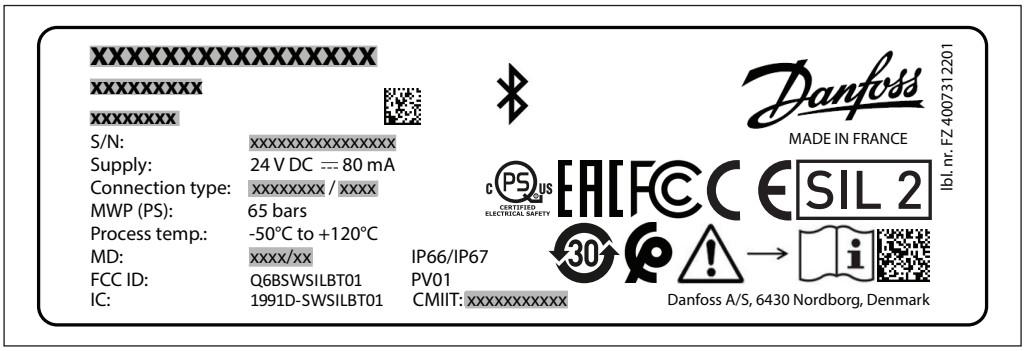


Figure 1-1: Location of the SIL logo on the device nameplate is in the middle right

Related documentation

[N1] LLS 4000 Datasheet **AI323832972563**

[N2] IEC 61508-1 to 7: 2010 Functional safety of electrical / electronic / programmable electronic safety-related systems

[N3] Liquid Level Switch Installation guide/Quick start **AN317523977313**

Terms and definitions

DC_D	Diagnostic Coverage of dangerous failures
Firmware	Software embedded in the device
FIT	Failure In Time (1×10^{-9} failures per hour)
FMEDA	Failure Modes, Effects and Diagnostics Analysis
FRT	Fault Response Time (diagnostic test interval + Fault Reaction Time)
HFT	Hardware Fault Tolerance
High demand or continuous mode	Where the frequency of demands for operation made on a safety-related system is greater than one time per year
λ_{DD}	Rate for dangerous detected failure
λ_{DU}	Rate for dangerous undetected failure
λ_{SD}	Rate for safe detected failure
λ_{SU}	Rate for safe undetected failure
Low demand mode	Where the frequency of demands for operation made on a safety-related system is no greater than one time per year
MTBF	Mean Time Between Failures
MTTF	Mean Time To Failure
MTTR	Mean Time To Recovery
PFD_{AVG}	Average Probability of Failure on Demand
PFH	Probability of a dangerous Failure per Hour
Process safety time	The time interval between a potentially dangerous failure and an error value from the current output
Safety Application Conditions	Conditions that are demands to be observed when using a safety related system or sub-system
SFF	Safe Failure Fraction
SIL	Safety Integrity Level
SIS	Safety Instrumented System
Systematic Capability	Measure (expressed on a scale of SC 1 to SC 3) of the confidence that the systematic safety integrity of an element meets the requirements of the specified SIL, in respect of the specified element safety function, when the element is applied in accordance with the instructions
Type A system	"Non-complex" system (all failure modes are well defined). For more data, refer to subsection 7.4.3.1.2 of IEC 61508-2
Type B system	"Complex" system (all failure modes are not well defined). For more data, refer to subsection 7.4.3.1.2 of IEC 61508-2
T[Proof]	Proof Test Interval
T[Repair]	Time to Repair
T[Test]	Internal Diagnostics Test Interval
2oo2	2 out of 2 channels architecture

Specification of safety function

Preliminary requirements

The device must be operated within the process and ambient conditions specified in the Datasheet (document **[N1]**) of the device.

The following chapter defines additional conditions, which have to be obeyed for safety applications

Definition of the safety function

General notes

The device contains a safety function that agrees with International Standard IEC 61508 (document **[N2]**). This safety function operates if the device detects a liquid in front of it.

Definition of the safety function

Within a maximum fault response time of 10s, the device sets its output relay to its fundamental state (open) if the level of a specified liquid in a tank has reached the middle of the sensing interface ±5 mm tolerance.

The safety integrity level of this safety function is SIL2.

Fault response time

The fault response time is the time that is necessary for the device to go into safe state after an error occurred in the safety function.

The maximum time is 10 seconds, as it is the time for the device to run all its internal diagnostics.

Safety function characteristics

The safety function uses only digital binary output signal to indicates the presence of the product and give the device status.

WARNING!

The device must have the applicable options and settings for the application. The ambient and process conditions must agree with the technical data given in the Datasheet (document [N1]) and this document (safety guide). You must obey the installation instructions given in the Datasheet (document [N1]).

Function input	None
Function output	Switch output - relay

If the device finds a fault:

Output relay, safe state	Open (**Remark:** The relay is considered as Open even in case of the output oscillates between close and open)

If a logic solver is used, it must use the output relay safe state to set itself to a fail-safe condition.

Safety application conditions (SAC)

Installation (refer to Installation guide - AN317523977313)

- The device must be installed with a minimum distance to any object (e.g. TDR probe) in front of the sensing part. The minimum distance is 25 mm
- The device must be installed with a maximum angle relative to horizontal in order to avoid liquid reservoirs. The maximum angle is 10°
- The device must be installed to avoid overflow due to a potential thicker layer of foreign liquid on top of the media in focus (like oil on refrigerant). Foreign liquid might not be detected and could potentially provoke an overflow
- The mechanical part of the device must not be disconnected from the electronic part of the device. The change of the electronic part is not allowed as it would lead to a significant loss of accuracy and the device would not be able to sense the product correctly

Operation

- The device must not be used for products with a viscosity above 5000 cps
- The device must not be used with foreign particles in the medium. Foreign particles can cause the device to detect the medium incorrectly
- The device must be tested after installation to ensure correct functionality. See chapter §5.3 for proof tests definition
- The device won't detect the presence of gas or the bubbles of a liquid medium. The device is parametrized to detect only a liquid phase of a product
- When the device reset in case of error detection, the relay stays in a safe position for at least 100 milliseconds

Functionally-safe configuration

- The device must be configured accordingly with the real product in the tank. This setting is in the parameter "Product Type". By default, this parameter is set to Ammonia
- It is only possible to use the safety function with:
  - The safe state relay is set to "OPEN". The normally open relay setting is not able to guarantee the safety function of the devices
  - Device protects from product overfill. The device is not able to protect safely enough the emptiness state of a tank
- If you use the device in a continuous mode or high demand mode of operation, the process safety time must be more than 10 seconds. This minimum time agrees with International Standard IEC 61508 Part 2 (document **[N2]**), section 7.4.4.1.4
- If you use the device in a high demand mode of position, the maximum frequency of demands is 1 demand every 17 minutes. This frequency agrees with International Standard IEC 61508 Part 2 (document **[N2]**), section 7.4.4.1.4

Functionally-safe use of the Bluetooth communication

The communication with the device is authorized using the Bluetooth communication and the dedicated application with the following restrictions.

- The default PIN code of a device is 0000. This code must be changed at start. To change this code please check the installation guide (document **[N3]**)
- The dedicated application permits to change the settings of the device. For safety reason, it is only possible to change the parameter "Product Type" within the first 15 minutes after the starting up of the device
  After the change of parameter(s), the device proceeds to a warm reset and restart with new parameters. The relay set its state to a safe state for 2 seconds.
  If a device is connected to logic solver, the logic solver should implement a diagnostic when this case happens
- The dedicated application can be used with a specific mode to test the entire safety loop (proof tests). For this test, the relay must be set OPEN or CLOSE.
  This means that the safety information of the device is not guarantee during this part of proof test
- The Bluetooth communication is only used for set-up, calibration and diagnostic purposes. It is not used during safety operation mode

Operation

Conditions of use

WARNING!

Only approved personnel can change device settings. Keep a report of changes to the device settings. These reports must include the date, the menu item, the old parameter and the new parameter.

The configuration is protected with a password. For more data on password protection and device configuration, refer to the "Configuration" chapter in the installation guide (document **[N3]**).

Failure state

Switch output - relay

Output relay state	Description
CLOSED	Information of safe measurement, the device does not detect product
OPEN	The safety function changes the value to the "safe state", when the device detects a product, or the internal diagnostics detect a safe or dangerous detected failure.

Error conditions

The device can sense the error conditions in the table that follows. When the device detects a measurement error, it supplies the "safe" position on the output relay.

Error condition	Cause
Device does not start immediately	This error occurs if more than 5 seconds are necessary to start the device
Component hardware errors	Memory failure internal to the device
	Voltage failure internal to the device
	No signal for product detection
	Microcontroller failure internal error
	Antenna resonance is not correct
Ambient temperature is too high	The ambient temperature is more than 80 °C (176 °F)
Ambient temperature is too low	The ambient temperature is less than -40 °C (-40 °F)
Incorrect detection signal	The device is not able to sense correctly the product

User parameters

INFORMATION!

If you change a parameter in one or more of the menu items that follow, this will have an effect on the safety function.

Limits for change of parameters

CAUTION!

If you change the values of one or more of the parameters given in the "User parameters" section, this can have an unwanted effect on the safety function. Do a check of the safety function after you change a parameter.

LEGAL NOTICE!

The manufacturer declines all responsibility for the correct operation of the safety function if these parameters are changed by the customer with the supervisor access.

Parameter name	Function description	Selection list	Default value and comments
Media Type	Selection of the type of media the device measure.	Ammonia, Freon	Ammonia
Switch State	State of the relay when the device does not detect the presence of the media	Normally Close, Normally Open	Normally Close It is not possible to change this value for SIL devices

Service

Periodic maintenance

You must follow the maintenance instructions given in the Datasheet (document **[N1]**).

Operation modes and proof tests

Continuous and high demand mode

If you operate the level transmitter in a continuous or high-demand mode in the specified environmental limits, calculate the frequency to perform the necessary proof tests during its useful lifetime (for more data, refer to Characteristics for the device safety functions on page 15). Obey safety application conditions (SAC) that relate to useful lifetime and constant failure rates.

Low demand mode

The level transmitter includes a comprehensive set of online diagnostic tests which are executed fast and frequently, resulting in a very low mean down time. Assuming reasonable low repair and restoration times as well, the device fulfils SIL2-compatible PFD values.

Proof tests

It is necessary to do proof tests to make sure that the safety function is applicable to the product detection.

- The device settings must be correct. If a parameter is incorrect, the device will not detect correctly
- The electronic components must not be defective
- The software programs (firmware etc.) must operate correctly
- The mechanical installation of the device must not have an effect on the performance of the sensing part

We recommend that you do a proof test:

- Immediately after you install and start the device
- Immediately after you change the parameters of the device

WARNING!

SIS engineers must calculate the interval of proof tests. This interval must agree with the specified PFD_{AVG}. The minimum time between proof tests must be less than 5 years, but the interval between proof tests must also agree with the safety system used on site.

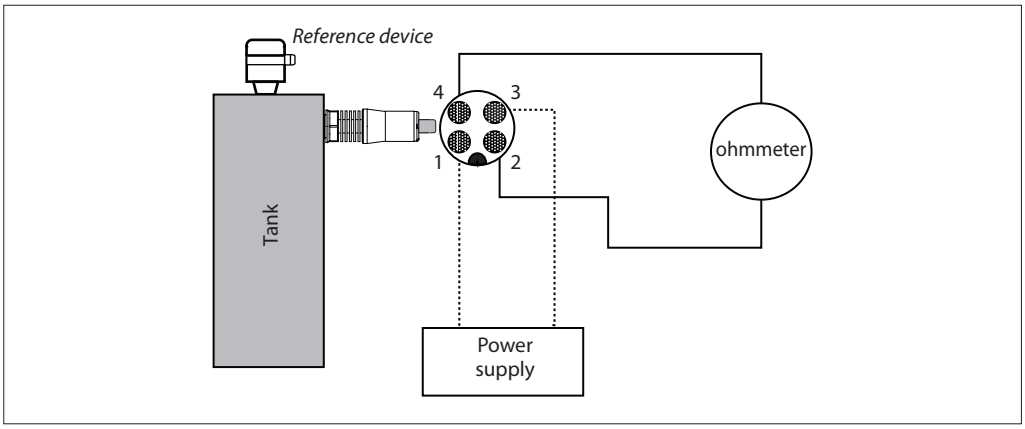
Prepare the device for the proof tests.

CAUTION !

- *Proof tests done by the customer must be equivalent or more difficult than the tests given in this section*
- *Keep a report of each proof test. These reports must include the date, the tests results (performance of the safety function or faults found), a list of approved personnel who did the test and the report revision number. These reports must be put into storage and made easily available. A proof test report form (for copying) is available on page 18*
- *If the proof test results are not correct because the device is not set correctly or it does not detect the product, speak or write to the manufacturer*
- *The location of the device and how it is installed on the tank can have an effect on the performance. Make sure that you obey the installation instructions given in the **installation guide** (document **[N3]**)*
- *Disconnect the device from the safety system PLC when you do proof tests because this system configuration can open the circuit breaker*

Equipment needed

- Device installed on the process
- Smartphone application connected to the device
- ohmmeter
- Reference device: an approved level meter or indicator



How to make sure that the device installation is correct

Do a visual check of the device position

- Check that the device is set on the tank to prevent for overfilling

Do a visual check of the device

- Check on the device nameplate if the following SIL logo appears

SIL 2

Do a check of the Product Type

- Power the device
- Power the smartphone and launch the application
- Connect the device with the smartphone application
- Go into section CONFIGURATION
- Check the Product Type parameter is correctly set according to the product in the tank
- If the Product Type parameter is not set correctly then the test is a failure

Do a check of the Relay State configuration

- Connect the device with the smartphone application
- Go into section CONFIGURATION
- Check the "Switch State" parameter is set to "Normally Closed". If the parameter is not "Normally Closed" then the test is a failure

How to make sure of the relay output capability

Do a check of the output relay "safe" position

- Power the device
- Power the smartphone and launch the application
- Connect the device with the smartphone application
- Go into section Additional info
- Click on the button "OPEN RELAY"
- Check the output relay for more than 10 seconds:
  - if the value of the ohmmeter is greater than 50 ohms during the 10 seconds, the output relay is considered as open. This test is successful
  - If the value of the ohmmeter is spuriously lower or equal than 50 ohms during the 10 seconds, the output relay must be considered as close. This test is a failure

Click on "EXIT TEST" to end the checking of the open state of the relay.

WARNING: If there is no action on "EXIT TEST", the relay will stay open independently of the product detection.

Do a check of the output relay normal position

- Power the device
- Power the smartphone and launch the application
- Connect the device with the smartphone application
- In the settings, enter the device service login
- Go into section Additional info
- Click on the button "CLOSE RELAY"
- Check that the output relay is close: if the value of the ohmmeter is lower than 50 ohms, the relay of the device is close. This test is successful

Click on "EXIT TEST" to end the checking of the close state of the relay.

WARNING: If there is no action on "EXIT TEST", the relay will stay close independently of the product detection, and can hide a dangerous state.

How to make sure of the correct behavior of the device

Do a functional check of the device

- Power the device
- Use the reference level indicator for setting the level below the device position
- Check the output relay is close: if the value of the ohmmeter is lower than 50 ohms, the relay of the device is close
- Use the reference level indicator for filling the tank until the level gets higher than the device position
- Check the output relay is open: if the value of the ohmmeter is greater than 50 ohms, the relay of the device is open
- Use the reference level indicator for emptying the tank until the level gets lower than the device position
- Check the output relay is close: if the value of the ohmmeter is lower than 50 ohms, the relay of the device is close
- If the relay of the device is not set properly in the previous checks, then the test is a failure

CAUTION!

Do a visual inspection of the housing, seals and electrical wires to make sure that they are serviceable.

If you do the tests in this section, it is possible to get this proof test coverage:

Device information	Proof test coverage (PTC)
Output relay	95%

Troubleshooting

INFORMATION!

Modifications to the device are not permitted.
Only approved personnel can repair the device.

If you find a problem, please contact your local representative. If the device must go back to the manufacturer.

Send a report to the manufacturer if there is a failure that is related to functional safety. If you find a problem, please contact your local representative.

Technical Data

Characteristics for the device safety function

Version	LLS 4000
Product Version	PV01
Device type	Type B system
Systematic capability	2
Safety integrity level	
Dual channel	SIL2
Architecture	2oo2
HFT	1
PFH	7.37×10^{-9}
SFF	98%
λ_{SD}	5.1×10^{-9}
λ_{SU}	160×10^{-9}
λ_{DD}	165×10^{-9}
λ_{DU}	5.65×10^{-9}
PFD_{AVG} (T[Proof] = 1 year)	2.48×10^{-5}
PFD_{AVG} (T[Proof] = 3 years)	7.43×10^{-5}
PFD_{AVG} (T[Proof] = 5 years)	1.24×10^{-4}
Proof test coverage	95%
Diagnostic test interval	10 s
Fault reaction time	< 1 s
MTBF	304 years

Assumptions

FMEDA is applicable for the conditions that follow:

- Use of the device agrees with its design and performance characteristics. This includes ambient and process conditions
- Installation of the device must agree with the instructions and the requirements of the application
- We can ignore wear of mechanical parts. Failure rates are constant
- Failures that follow one after the other are put in the same group as the failure that is the source of the problem
- The Bluetooth protocol is only used for set-up, calibration and diagnostic purposes. It is not used during safety operation mode
- All components that are not part of the safety function and cannot influence the safety function (feedback immune) are not included
- The output relay is used for safety applications
- The Mean Time to Recovery after safe failure is 72 hours (MTTR = 72 h)
- External power failure rates are not included

INFORMATION!

The FMEDA of the device was calculated with the exida tool FMEDA v7.1.17, with the configuration that follows:
Database SN 29500
Ambient temperature is 40 °C
T[Proof] is from 1 to 10 years (87600 hours)
T[Repair] is 72 hours
T[Test] is 10 seconds (all internal test functions are done a minimum of one time during this period)

Support for SIL-approved devices

If the manufacturer makes a modification that has an effect on the safety function of the device, the manufacturer will tell you about the modification immediately.

Appendix

Proof test report form (for copying)

CAUTION !

Complete the report form that follows when you do a proof test.

For more data, refer to Proof tests on page 11.

Recorded by:	**Date:**
Unique device ID (e.g. serial number):	

Parameter value check				
	Proof tests results			
	Recorded value	**Correct value**	**Approved**	
Device mounting position		Device protects overfilling.	[Yes]	[No]
Visual check of the SIL logo		There is the logo **SIL 2** on the nameplate	[Yes]	[No]
Product Type parameter value		Value according to the product in the tank	[Yes]	[No]
Relay Init State parameter value		Value set to 0 (zero)	[Yes]	[No]

Functional check				
	Proof tests results			
	Recorded value	**Correct value**	**Approved**	
Check output relay in "safe" position		output relay is open (ohmmeter gives an error or >50 ohms)	[Yes]	[No]
Check output relay in normal position		output relay is closed (ohmmeter gives an error or <50 ohms)	[Yes]	[No]
With a level below the device position, output relay is in normal position		output relay is closed (ohmmeter gives an error or <50 ohms)	[Yes]	[No]
With a level increasing above the device position, output relay is in "safe" position		output relay is open (ohmmeter gives an error or >50 ohms)	[Yes]	[No]
With a level decreasing below the device position, output relay is in normal position		output relay is closed (ohmmeter gives an error or <50 ohms)	[Yes]	[No]

Conclusion		
Does the device operate satisfactorily in safety-related systems?	[Yes]	[No]
Signature:		