LLT SIL FUNCTIONAL SAFETY GUIDE

LLT100

Laser level transmitter

Disclaimer

This document contains product specifications and performance statements that may be in conflict with other ABB published literature, such as product fliers and catalogs. All specifications, product characteristics, and performance statements included in this document are given as indications only. In case of discrepancies between specifications given in this document and specifications given in the official ABB product catalogs, the latter takes precedence.

ABB reserves the right to make changes to the specifications of all equipment and software, and contents of this document, without obligation to notify any person or organization of such changes. Every effort has been made to ensure that the information contained in this document is current and accurate. However, no guarantee is given or implied that the document is error-free or that the information is accurate.

ABB makes no representations or warranties with regard to the product and instructional and reference materials, including, but not limited to, all implied warranties of merchantability and fitness for a particular purpose.

ABB does not warrant, guarantee, or make any representations regarding the use, or the results of the use, of any software or written materials in terms of correctness, accuracy, reliability, currentness, or otherwise. ABB shall not be liable for errors or omissions contained in its software or manuals, any interruptions of service, loss of business or anticipatory profits and/or for incidental or consequential damages in connection with the furnishing, performance or use of these materials, even if ABB has been advised of the possibility of such damages.

All equipment, software, and manuals are sold as is. The entire risk as to the results and performance of the equipment and software is assumed by the user.

The software or hardware described in this document is distributed under a license and may be used, copied, or disclosed only in accordance with the terms of such license.

Table of Contents

Page intentionally left blank

CHAPTER 1

Introduction

The purpose of this safety manual is to provide information necessary to design, install, verify, and maintain a Safety Instrumented Function (SIF) utilizing the LLT100. This manual provides the necessary requirements for meeting the IEC 61508 functional safety standards.

This chapter defines terms, abbreviations and acronyms used in this document. It also exposes reference documents and how to get product support.

Terms and abbreviations

Term	Meaning
Basic Safety	The equipment must be designed and manufactured such that it protects against risk of damage to persons by electrical shock and other hazards and against resulting fire and explosion. The protection must be effective under all conditions of the nominal operation and under single fault condition.
Continuous Mode	Mode where the safety function retains the EUC in a safe state as part of normal operation.
Fail Annunciation Detected	Failure that does not cause a false trip or prevent safety function but does cause loss of an automatic diagnostic or false diagnostic indication.
Fail Annunciation Undetected	Failure that does not cause a false trip or prevent the safety function but does cause loss of an automatic diagnostic and is not detected by another diagnostic.
Fail Dangerous	Failure that does not respond to a demand from the process (i.e. being unable to go to the defined fail-safe state).
Fail Dangerous Detected	Failure that is dangerous but is detected by automatic stroke testing.
Fail Dangerous Undetected	Failure that is dangerous and that is not being diagnosed by automatic stroke testing.
Fail No Effect	Failure of a component that is part of the safety function but that has no effect on the safety function.
Fail-Safe State	State where the output current is ≤3.6 mA (fail low) or ≥21 mA (fail high)
Fail Safe	Failure that causes the current output to go to the defined fail-safe state without a demand from the process.
Functional Safety	The ability of a system to carry out the actions necessary to achieve or to maintain a defined safe state for the equipment under control of the system.
High Demand Mode	Mode, where the frequency of demands for operation made on a safety related system is more than one per year.
Low Demand Mode	Mode, where the frequency of demands for operation made on a safety related system is not more than one per year.
Multidrop	Multidrop Mode. In Multidrop Mode, multiple devices are connected in parallel to a single wire pair. The analog current signal simply serves to supply power to the devices in two-wire technology with a fixed current.

Term	Meaning
Safety	Freedom from unacceptable risk of harm.
Safety Function	A specified function that is performed by a safety-related system with the goal, under consideration of a defined hazardous incident, of achieving or maintaining a safe condition for the plant.
Safety related system	A safety related system performs the safety functions that are required to achieve or maintain a safe condition.
Ullage	The distance by which a container falls short of being full.

Acronyms

Acronym	Definition
DC	Diagnostic Coverage
DCS	Distributed Control System. Control system used in industrial applications to monitor and control decentralized units.
DTM	Device Type Manager. A DTM is a software module that supports specific functions for accessing device parameters, the setup and the operation of devices, and diagnostics. The DTM is not executable software. It requires a FDT container program to be activated.
DUT	Device Under Test
EDD	Electronic Device Description
EUC	Equipment Under Control
FDT	Field Device Tool
FMEDA	Failure Modes, Effects and Diagnostic Analysis
HART	Highway Addressable Remote Transducer
HFT	Hardware Fault Tolerance. Ability of a functional unit (hardware) to continue to perform a required function when faults or errors are prevailing.
HMI	Human Machine Interface. In this case, the HMI is a combined module consisting of an LCD display with 4 buttons keypad.
LRV	Lower Range Value. Device Configuration, LRV of the measurement range
MTBF	Mean Time Between Failures
MTTR	Mean Time To Restoration. Mean time between the occurrence of an error in a unit or in a system and its repair.
PFD	Probability of Failure on Demand
PFD_{AVG}	Average Probability of Failure on Demand
SFF	Safe Failure Fraction. Proportion of non-hazardous failures; in other words, the proportion of failures without the potential to put the safety-related system in a hazardous or impermissible state.
SIF	Safety Instrumented Function. A set of equipment intended to reduce the risk due to a specific hazard.
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 the failure of a safety function. The higher the Safety Integrity Level of the safety-related systems, the lower the probability that they will not perform the required safety function.
URV	Upper Range Value. Device Configuration, URV of the measurement range.

Support

The user should regularly refer to the ABB website for the latest documentation updates.

Additional documentation on LLT100 is available for download free of charge at http://www.abb.com/laserlevel.

Product support can be obtained by contacting ABB by one of the means indicated on the back cover of this manual.

Applicable documents

The following documentation must be available with the LLT100 and shall be read in addition to this safety manual.

AD1	OI_LLT-EN	Operating Instruction	http://new.abb.com/products/measurement-products/level/laser-level-transmitters/llt100
AD2	DS_LLT100-EN	Datasheet	http://new.abb.com/products/measurement-products/level/laser-level-transmitters/llt100

These documents include details about functional specifications of the analog output and how to operate and configure the device.

Reference documents

RD1	IEC 61508 (2010) (Edition 2), Part 1 to 7	Functional safety of electrical/electronic/programmable electronic safety-related systems. International standard published by International Electro-technical Commission (IEC).

Page intentionally left blank

CHAPTER 2

Description

The LLT100 is specifically made for industrial applications and harsh environments. It provides continuous, non-contact level measurement capabilities for process automation and inventory management in industries. It provides precise measurement of any solid or liquid independently from the material properties. It also has dust and fog penetration capabilities with a class 1 laser.

Using a pulsed laser to perform time-of-flight measurements, the LLT100 provides accurate distance measurements using a LIDAR sensor as input and a 4–20 mA loop as output. The unit is powered thought the 4–20 mA loop on two wires. A HART 7 communication interface (not used as safety function) is available on the same two wires.

Depending on the type of accessory, it can meet the demands of hazardous area locations, and high pressure and high temperature applications. Ordering specifications are described in the LLT100 data sheet (AD2). Refer to this data sheet to get exact measuring range, operating temperature and accuracy specifications. The LLT100 is explosion-proof class 1, division 1 (zone 1).

For dusty applications, the dust tube prevents dust deposition on the window, significantly decreasing the need for preventive maintenance. For very high dust levels, a purge ring can be added to the dust tube to provide an air flow to enhance the dust protection. High temperature applications are made possible by the addition of a cooling tube. Cooling tubes with different process interfaces and different pressure ratings are available.

Additional documentation on LLT100 is available for download at http://www.abb.com/laserlevel.

Instrument version

This safety manual applies to LIDAR sensor LLT100, with the most up-to-date revision in this table:

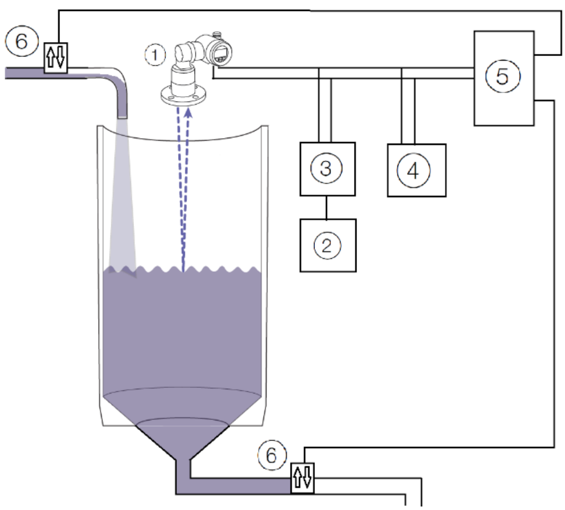
Safety Release Number	Release Date	Software Version	FPGA Version	Hardware Version	Release Notes
1	15 June 2018	1.01.03	1.01.03		Initial safety version Restriction for combination of vessel height value ≤1.0 m, drain rate enabled and clear liquids mode described in “Restriction 1” on page 14.
2	August 2020	1.01.31		2.0.0	Changed FPGA version field to Hardware version field in CB software.

CHAPTER 3

Designing an SIF using the LLT100

Figure 1 shows a safety function example with the LLT100. The vessel level is monitored by the laser level transmitter. The LLT100 4–20 mA output loop is proportional to the level, ullage or volume of the vessel. Configuration of the LLT100 can be performed directly on its HMI or with HART communication protocol through a computer or handheld terminal. The LLT100 connects to the user logic device to control one or multiple actuators for process control and SIF.

Figure 1 Safety function with LLT100 monitoring a vessel and user logic controlling it



Number	Description
①	LLT100
②	Computer with FDT and LLT100 DTM
③	HART FSK modem
④	Handheld terminal
⑤	Automation system, Logic-unit, PLC or other logic device
⑥	Actuator

Safety function

The laser level transmitter produces an analog signal, between 4 mA and 20 mA, proportional to the level, volume or ullage, as defined by the operator. The analog signal is fed to a downstream logics unit such as a PLC or a limit signal generator, and is monitored for exceeding a specified maximum or minimum value. All safety functions refer exclusively to this analog output. The total valid range of the output signal shall be configured to a minimum of 3.8 mA and a maximum of 20.5 mA (factory defaults).

The LLT100 provides the following Type-B safety functions:

- Computes a distance/level measurement.
- Outputs a 4–20 mA signal of the transformed measurement.
- Measurement transformations are user-defined (math functions). These functions can be either on or off. Multiple parameters can be set related to:
  - Damping
  - Linearization function
  - Filtering

The safety related function of the transmitter is the safe monitoring of the level within an accuracy of 2% of span (2% of 16 mA). The safe state output current can be configured to be ≤3.6 mA (low alarm) or ≥21.0 mA (high alarm), with the exception of CPU faults where the current output is in low alarm mode (≤3.6 mA).

There are other functionalities of the LLT100 that are not considered as part of the safety function:

- Digital input (optional, external)
- HART communication
- HMI (optional)
- Remote display (optional accessory)
- Other accessories: lens heater, dust tube

Alarm response and current output

In case of detected critical faults, the configured alarm current will be produced and fed to a subsequent logic unit, e.g., a DCS, and monitored for violation of a defined maximum value.

Selectable alarm current modes

There are two selectable modes for this alarm current:

- HIGH (max alarm current) which is the factory default setting;
  or
- LOW (min alarm current).

Configurable alarm currents

The low alarm current is configurable from 3.5 to 3.6 mA with a factory default setting of 3.6 mA. The high alarm current is configurable from 21.0 to 21.6 mA with a factory default setting of 21.0 mA. The reaction time after the occurrence of a critical error until the output of the alarm current amounts to ≤1 min.

DCS Configuration

For safe fault monitoring, the following conditions must be fulfilled:

- The LOW ALARM must be configured with a value of ≤3.6 mA;
  or
- The HIGH ALARM must be configured with a value ≥21.0 mA.
- The DCS must be capable of recognizing the selected configured high alarms or low alarms as a malfunction detection.
- For safe current output operation, the terminal voltage at the device must be between 15.5 V and 42 V, with a minimum of 21 V for HART functionality.

The DCS loop must provide the required voltage level even if the current output operates on the configured HIGH alarm.

The DCS shall be able to latch a detected High or Low Alarm, as the LLT100 alarm state may not be maintained after the alarm-triggering condition is not met anymore. The DCS shall be configured with a sampling interval smaller or equal to 500 ms to have the capability to sample all 4-20 mA loop current fault-indicating values.

Power On Behavior

On startup, the LLT 100 current output will follow the following sequence:

1. Low alarm mode (≤ 3.6 mA) for approximately 0.6 s;
2. High alarm mode (≥ 21.0 mA) for a duration between 10 s and 20 s due to internal power management constraints.

If a CPU fault occurs at startup during the instrument self-test, the current output will stay in low alarm mode (≤3.6 mA).

Power Failure Alarm Behavior

As demonstrated through fault insertion testing, some internal hardware failures may cause the LLT100 to undergo a perpetual reset loop behavior which will be similar to its power on behavior as described above:

1. Low alarm mode (≤ 3.6 mA) for approximately 0.6 s;
2. High alarm mode (≥ 21.0 mA) for approximately 4 s.

Behavior of Transition to Alarm Current

The 4–20 mA output transition from nominal measurement to alarm current is performed in the following manner:

1. Nominal current output (e.g.; 9.8 mA)
2. Transition to intermediate value for one measurement cycle, thus approximately 1.5 s:
   - 4.0 mA if primary value (PV) is set to Ullage
   - 20.0 mA if primary value (PV) is set to Level or Volume
3. Alarm current; high or low as described in “Selectable alarm current modes” and “Configurable alarm currents” on page 12.

Conditions when device is not safety compliant

The device is not safety-compliant during the following conditions:

- During configuration
- Whenever HART is used to carry an output of the device that is used for safety instead of the 4–20 mA output
- During simulation
- During proof test of the safety function.

The fraction of failures without the potential to put the device into a dangerous function status is given by the SFF value shown in “Safety parameters (FPGA and software versions up to 1.1.3)” on page 16.

Overall safety accuracy

The defined value for the safety threshold of the safety function of this device is: 2% of 4–20 mA span (2% of 16 mA).

Restricted modes and parameters

Restriction 1

The combination of the following instrument configuration parameters **shall not** be used for a Safety Instrumented Function:

Configuration Parameter	Value
Measurement mode	Clear Liquids
Drain Rate	Enabled
Vessel Height	≤1 m

This restriction is only related to the combination of clear liquids measurement mode, vessel height smaller or equal to 1 m and drain rate enabled. In this situation, the 4–20 mA output will remain at a constant value between 4 mA and 20 mA, regardless of actual level variations.

All other instrument configurations can be used for a Safety Instrumented Function.

Behavior for undetected faults

If a LLT100 fault occurs and is not detected through its internal diagnostics, the safety function may output a current between 4 and 20 mA, which exceeds its specified safety accuracy or is not proportional to the level, volume or ullage as defined by the operator.

Environmental limits

The designer of a SIF must check that the product is rated for use within the expected environmental limits. Refer to the Operating Manual (AD1) or data sheet AD2, for accurate information about environmental limits. Some limits depend on the model and accessories installed on it. Additional accessories can be used to help reduce the impact of dust or fog environment on the LLT100 measurement.

The LLT100 measurements can be affected by dust or fog between the instrument and the surface to be measured. Dust and fog between the instrument and the surface to be measured should be kept to a minimum. The user shall perform verifications to ensure that proper measurements can be made in the target application environment.

Applications limits

The LLT100 can have flanges in aluminum or stainless steel. It is important for the designer to check for material compatibility considering on-site chemical contaminants and air supply conditions. If the LLT100 is used outside of the application limits or with incompatible materials, the reliability data provided could become invalid.

The laser used for measuring distance is a class 1 laser (IEC60825-1 Ed 2, 2007).

Measuring laser safety

A class 1 laser is safe for all conditions of use.

Design verification

A Failure Mode, Effects and Diagnostics Analysis (FMEDA) summary report is available from ABB Inc. This report details all the failure rates and failure modes as well as the expected lifetime of the LLT100.

The achieved SIL of an entire SIF design must be verified by the designer via a calculation of PFD_{AVG} considering architecture, proof test interval, proof test effectiveness, any automatic diagnostics, average repair time and the specific failure rates of all products included in the SIF. Each subsystem must be checked to ensure compliance with minimum hardware fault tolerance requirements.

The safety parameters used for SIL calculation of the SIF are shown in “Safety parameters (FPGA and software versions up to 1.1.3)” below.

SIL capabilities

Systematic integrity

The product meets proven-in-use requirements for SIL 2. A SIF designed with this product must not be used at a SIL level higher than the statement without prior-use justification by the end user or diverse technology redundancy in the design.

Random integrity

The LLT100 is a type B device. Therefore, based on the SFF ≥ 90%, when the LLT100 is used as the only component in a final element subassembly, a design can meet SIL 2 @ HFT=0. When the final element assembly consists of many components, the SIL must be verified for the entire assembly using failure rates from all components. This analysis must account for any hardware fault tolerance and architecture constraints.

Safety parameters (FPGA and software versions up to 1.1.3)

The table below shows the failure rate information obtained from the FMEDA and other useful information.

Table 1 Characteristics as per IEC 61508 (FPGA and software versions up to 1.1.3)

Parameter	Value
Type of assessment	Proven in use
Safety Integrity Level	2
Systematic capability	2
HFT	0
Component type	B
Measuring mode	Low demand mode, High demand mode
SFF	97%
MTTR	24 h
MTBF	31 years
Diagnostic coverage	$\lambda_{dd} / (\lambda_{dd} + \lambda_{du}) \approx 94\%$
Diagnostic test interval	<15 min
Reaction time after detection of a critical error	≤1 min
Reaction time to process change	<1.5 s (with no damping or filtering)
Measurement time interval	<1.5 s
Proof test effectiveness	73%

Table 2 Failure rates (FPGA and software versions up to 1.1.3)

λ_s	λ_{dd}	λ_{du}	PFH
1,559 FIT	2,852 FIT	124 FIT	0.124×10^{-6} failures/h

Table 3 PFD_{AVG} (FPGA and software versions up to 1.1.3)

TI (years)	1	2	3	4	5
PFD_{AVG}	2.0×10^{-3}	2.4×10^{-3}	2.8×10^{-3}	3.2×10^{-3}	3.5×10^{-3}
TI (years)	**6**	**7**	**8**	**9**	**10**
PFD_{AVG}	3.9×10^{-3}	4.3×10^{-3}	4.7×10^{-3}	5.1×10^{-3}	5.5×10^{-3}

All safety related parameters are calculated using the *Exida* Electrical and Mechanical Component Reliability Handbooks, 4th edition. The *Exida* environmental profile chosen for this FMEDA was *Exida* Profile 2: Low Power Field Product. This environmental profile information is summarized in the table below.

Table 4 Environmental profile summary (FPGA and software versions up to 1.1.3)

Profile according to IEC 60654-1	Mean external temperature (°C)	Mean internal temperature (°C)	Temperature cycle (°C/365 days)
C3	25	30	25

Safety parameters (Hardware version 2.0.0, software version 1.1.31 and later)

The table below shows the failure rate information obtained from the FMEDA and other useful information.

Table 5 Characteristics as per IEC 61508 (Harware version 2.0.0, software version 1.1.31 and later)

Parameter	Value
Type of assessment	Proven in use
Safety Integrity Level	2
Systematic capability	2
HFT	0
Component type	B
Measuring mode	Low demand mode, High demand mode
SFF	90%
MTTR	24 h
MTBF	70 years
Diagnostic coverage	$\lambda_{dd} / (\lambda_{dd} + \lambda_{du}) \approx 86\%$
Diagnostic test interval	<15 min
Reaction time after detection of a critical error	≤1 min
Reaction time to process change	<1.5 s (with no damping or filtering)
Measurement time interval	<1.5 s
Proof test effectiveness	71%

Table 6 Failure rates (Harware version 2.0.0, software version 1.1.31 and later)

λ_s	λ_{dd}	λ_{du}	PFH
356 FIT	717 FIT	118 FIT	0.118×10^{-6} failures/h

Table 7 PFD_{AVG} (Harware version 2.0.0, software version 1.1.31 and later)

TI (years)	1	2	3	4	5
PFD_{AVG}	1.8×10^{-3}	2.2×10^{-3}	2.6×10^{-3}	3.0×10^{-3}	3.3×10^{-3}
TI (years)	**6**	**7**	**8**	**9**	**10**
PFD_{AVG}	3.7×10^{-3}	4.1×10^{-3}	4.4×10^{-3}	4.8×10^{-3}	5.2×10^{-3}

All safety-related parameters are calculated using the *Exida* Electrical and Mechanical Component Reliability Handbooks, 4th edition. The *Exida* environmental profile chosen for this FMEDA was *Exida* Profile 2: Low Power Field Product. This environmental profile information is summarized in the table below.

Table 8 Environmental profile summary (Harware version 2.0.0, software version 1.1.31 and later)

Profile according to IEC 60654-1	Mean external temperature (°C)	Mean internal temperature (°C)	Temperature cycle (°C/365 days)
C3	25	30	25

Considerations for High Demand Mode

In high demand mode, the end user shall comply with IEC61508-2 sections 7.4.5.3 and 7.4.5.4 for the failure rates to be applicable.

If compliance to these specified sections is not met, the end user shall contact ABB (see back cover ot this document) to calculate failure rates that are appropriate.

General requirements

The user shall verify that the LLT100 is suitable for use in safety applications by confirming that the LLT100 nameplate contains the **CS** label as part of the model identification code. An example of such a valid identification code is shown below:

LLT100.AIAH10L5-E03.CS.P901

Personnel performing maintenance and testing on the LLT100 shall be competent to do so.

Results from proof tests shall be recorded and reviewed periodically.

CHAPTER 4

Installation and commissioning

Only qualified and authorized specialists should be charged with the installation, electrical connection, commissioning, operation, and maintenance of LLT100 instruments.

Installation

The level laser transmitter must be installed with standard practices outlined in the Operating Instructions manual. Environmental parameters, such as temperature, pressure and dust level to name a few, must be checked to verify that they do not exceed the LLT100 ratings . As far as possible, the measuring setup should be free from critical ambient conditions such as large variations in temperature, vibrations, or shocks.

Physical location and placement

The LLT100 shall be accessible with sufficient room for electrical connection and shall allow manual proof testing, as described in “Proof test without automatic testing” on page 23.

In liquid applications, the laser beam must be as perpendicular as possible to the liquid surface. Alignment of the beam shall be within ±5 degrees from vertical.

In solid applications, if the laser is installed with an angle, the setting level calibration points in AD1 shall be executed to calibrate the actual depth of the monitored vessel with the measured depth.

Electrical connection

See the Operating Instructions manual for electrical connection instructions. Connection details like wires gauge and maximum length of cable are described in this manual. Make sure that the LLT100 is grounded according to the national and local electrical code. Outside installations or installations exposed directly or indirectly to lightning discharges should have a secondary lightning protection module.

Do NOT make electrical connections unless the electrical code designation stamped on the LLT100 name plate matches the classification of the area in which you want to install the LLT100.

Commissioning

The LLT100 needs to be configured before first use, since it comes with a factory default configuration. This instrument can be configured with the local HMI, with the DTM via the HART interface or with a handheld terminal. Configuring the device with the local HMI is documented in the Operating Instructions. During configuration, safe operation of the device shall not be assumed.

Checklist before safety operation

The following items must be checked before safety operation:

- Before the first startup of the device, as a part of a safety function, check that the device configuration fulfills the safety function of the system.
- Check that the right device is installed on the right measuring point.
- Make sure that the vessel empty (LRV) and vessel full (URV) parameters correspond to real values with appropriate units.
- After every change to the device, as a part of a safety function, such as a change to the installation position of the device, process type change or configuration of safety parameters, the safety function of the device shall be verified (see “Verify safety function” on page 21).
- After the safety function has been checked, device operation must be locked because a change to the measuring system or parameters can compromise the safety function. The **write protection shall be enabled** before powering up when it is desired to go into safe operation.

Adding password protection

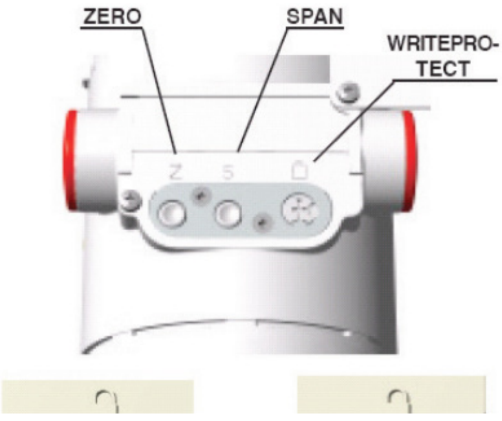
To allow only authorized personnel to modify the LLT100 configuration, and therefore the safety function behavior, password protection must be added.

1. From the **Device Setup** menu, select **Access Control > Advanced Password**.
2. In the password edit screen, edit each password character.
3. Press **OK**.
4. Repeat steps 1 to 3 for Standard Password instead of Advanced Password.

Enabling/Disabling the write protection

The device shall be write-protected for the safety operation. This could be performed through the following steps:

1. Remove the nameplate by releasing the holding screw lying on the bottom left corner.
2. Use a suitable screwdriver to press the switch down fully.
3. Turn the switch clockwise by 90°.



To deactivate the switch and remove the write protection, push it down slightly and turn counterclockwise by 90°.

High/Low alarm configuration

The LLT100 alarm state must be configured to ensure corresponding current value between the device and the DCS. The low alarm limit can be set from 3.5 to 3.6 mA and the high alarm limit between 21.0 and 21.6 mA.

1. From the **Process Alarm** menu, select **Process Alarm Limits > Current Out > Low Alarm** or **High Alarm**.
2. From there, edit the value as necessary, based on the information above.
3. Press **OK**.

Verify safety function

1. Verify and record the conditions as they are found prior to checking the safety function: write protection is on/off, instrument parameters.
2. Disable write protection before power up.
3. Check the current out precision by simulating current out and measure it with a multimeter. This could be performed by using an EDD/DTM interface or the HMI. The current out test shall test 4 mA and 20 mA at least.
4. Verify the alarm state configuration and alarm value configuration (3.5–3.6 mA and 21.0–21.6 mA). Simulate an alarm to check whether the alarm current is what was set via multi-meter.
5. Enable write protection and power down. If no alarm is issued after system startup, then the safety function is ensured during run-time.

Page intentionally left blank

CHAPTER 5

Operation and maintenance

Proof test without automatic testing

In accordance with IEC 61508, the safety function of the measuring device must be checked at appropriate time intervals. The operator must determine the proof test interval and take this into account when determining the PFD_{AVG} value of the laser level transmitter. The test must be carried out in such a way that it verifies correct operation of the device.

Testing of fixed output current, HIGH and LOW alarm output current and measuring accuracy are covered in the proof test. Testing the device can be performed by following the steps described below.

Testing the instrument

To check the safety function of the device, proceed as follows:

1 Verify and record the conditions as they are found prior to checking the safety function: write protection is on/off, instrument parameters.

NOTE: The process must be put into a safe state during proof testing.

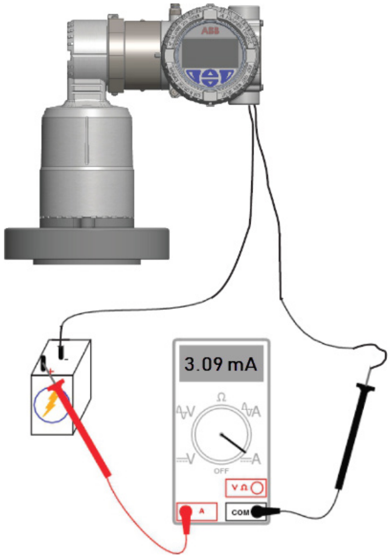
2 Perform a visual inspection and record any visible defects or wear outs. In case of low signal, instrument optical interface (glass) may be inspected and cleaned.

3 Bridge the safety DCS or take other appropriate measures to prevent inadvertent triggering of alarms.

4 Deactivate write protection (see “Commissioning” on page 19).

5 Performing the proof test requires the specified voltage input (see “Alarm response and current output” on page 12) in series with an ammeter (see Figure 2).

Figure 2 LLT100 current measurement



6 Set the transmitter output to a HIGH ALARM value by means of the HMI push buttons, HART communication by using a DTM in combination with HART software, or with the Field Information Manager (FIM-Tool) using simulation function (Menu: Diagnostics>Simulation Mode>Current Out).
7 Check whether the current output signal reaches the value set for high alarm value.
8 Set the output of the transmitter to a LOW-ALARM value by means of the push buttons of the HMI, HART communication by using the LLT100 DTM or with the Field Information Manager tool (FIM-Tool) using simulation function (menu: **Diagnostics>Simulation Mode>Current Out**).
9 Check whether the current output signal reaches this value.
10 Terminate the simulation mode after finishing the output simulation.
11 Activate the write lock (see section 4.4 Configuration) and wait for 10 seconds.
12 Restart the device by powering it down.
13 Check the measured distance or ullage against a secondary standard on an installed device which could be a calibrated reference device, a mobile calibration rig or on a factory calibration rig. The measured values of the secondary standard and the device under test (DUT) must be compared. The amount of deviation between the measured distance, ullage and the set point must not exceed the measured error specified for the safety function (±0.32 mA).
14 Remove the bridging of the safety DCS or restore normal operation in another way.
15 After the test has been performed, the results must be documented and stored in a suitable manner.

By using this test method at least 72 % (PTC = 0.72) of dangerous, undetected failures are detected. The influence of systematic errors like e.g., medium properties, operating conditions, build-up or corrosion on the safety function is not fully covered by the test.

If one of the test criteria from the test procedure described above is not fulfilled, the device may no longer be used as part of a safety instrumented system.

Possible error messages

If the LLT100 is malfunctioning in any way, the LCD displays specific error messages destined to help you identify and solve the problem. The chapter “Troubleshooting and service” of the Operating Instructions guide explain where the error summary appears and how to access the full details of the error.

CPU internal faults will result in the LOW alarm independent from the configured alarm current. Other failures will be immediately signaled within the LOW or HIGH alarm range in line with the configured alarm current.

Maintenance

The LLT100 should have its optical interface (glass) inspected and cleaned when the proof test is performed (as described in “Testing the instrument” on page 23).

Repair

To maintain safety operation, repairs must be performed by ABB after the instrument is taken out of service. Replacing modular components by original ABB spare parts is permitted if personnel was trained by ABB for this purpose.

Before sending the unit to ABB, it must be cleaned and decontaminated. ABB must be contacted to obtain the Contamination Data Sheet. After filling and sending the contamination data sheet to ABB, an RMA number will be attributed and after those steps the unit can be sent to ABB for repair.

Refer to Operating Instruction manual for further details.

Software updates

Software updates, if applicable and recommended by ABB, must be performed by ABB trained personnel after the instrument is taken out of service.

Useful life

The applied failure rates of the components are valid within the usable service life (8 to 12 years) according to IEC 61508-2 section 7.4.9.5, note 3, and start increasing after this period.

ABB notification

All detected failures that compromise functional safety shall be reported to ABB. Contact ABB customer service as described in “Support” on page 7.

Page intentionally left blank

CHAPTER 6

Double IEC-61508 certificates

The initial LLT100 product was launched in 2016. Based on field return data analysis, ABB implemented a hardware modification which improves product reliability.

Consequently, two IEC-61508 certificates are issued:

- Legacy product: FPGA version (up to 1.1.3)
- Current product: Hardware version 2.0.0

Page intentionally left blank

CHAPTER 7

Document status

Change record

Version	Date	Change Description
A	18 June 2018	Initial release
B	August 2020	Updated Safety Parameters values. Updated proof test without automatic testing section. Corrected typos. Changed FPGA version for Hardware version in the HMI menu. Now includes product (hardware) version 2.0.0.

IEC-61508 certificate

The manufacturer
may use the mark:

Revision 2.0 August 11, 2020
Surveillance Audit Due
June 1, 2022

ISO/IEC 17065
PRODUCT CERTIFICATION BODY
1004

Certificate / Certificat

Zertifikat / 合格証

ABB 1704094 C001

exida hereby confirms that the:

LLT100 Lidar Sensor

ABB
Quebec, QC - Canada

has been assessed per the relevant requirements of:

IEC 61508 : 2010 Parts 1-7

and meets requirements providing a level of integrity to:

Systematic Capability: SC 2 (SIL 2 Capable)

Random Capability: Type B Element

SIL 2 @ HFT=0; Route 1_H

PFH/PFD_{avg} and Architecture Constraints must be verified for each application

Safety Function:
The 4 to 20 mA current output will reflect the calibrated range in level, volume or ullage, as selected by the user, within the specified safety accuracy and safety time; and will change to 3.6 or 21 mA within the specified time upon detection of a failure.

Application Restrictions:
The unit must be properly designed into a Safety Instrumented Function per the Safety Manual requirements.

Evaluating Assessor

Certifying Assessor

Page 1 of 2

Series LLT100

Lidar Sensors

Certificate / Certificat / Zertifikat / 合格証

ABB 1704094 C001

Systematic Capability: SC 2 (SIL 2 Capable)

Random Capability: Type B Element

SIL 2 @ HFT=0; Route 1_H

PFH/PFD$_{avg}$ and Architecture Constraints must be verified for each application

Systematic Capability:

The product has met manufacturer design process requirements of Safety Integrity Level (SIL) 2. These are intended to achieve sufficient integrity against systematic errors of design by the manufacturer.

A Safety Instrumented Function (SIF) designed with this product must not be used at a SIL level higher than stated.

Random Capability:

The SIL limit imposed by the Architectural Constraints must be met for each element.

IEC 61508 Failure Rates in FIT*

FPGA version up to 1.1.3 | Software version up to 1.1.3

Device	λ_{SD}	λ_{SU}	λ_{DD}	λ_{DU}
ABB LLT100	0	1559	2852	124

Hardware version 2.0.0 | Software version 1.1.31 and later

Device	λ_{SD}	λ_{SU}	λ_{DD}	λ_{DU}
ABB LLT100	0	356	717	118

* FIT = 1 failure / 10^9 hours

SIL Verification:

The Safety Integrity Level (SIL) of an entire Safety Instrumented Function (SIF) must be verified via a calculation of PFH/PFD$_{avg}$ considering redundant architectures, proof test interval, proof test effectiveness, any automatic diagnostics, average repair time and the specific failure rates of all products included in the SIF. Each element must be checked to assure compliance with minimum hardware fault tolerance (HFT) requirements.

The following documents are a mandatory part of certification:

Assessment Report: ABB 17-04-094 R001 V2R1

Safety Manual: AA019031-01 Rev B LLT100 SIL Safety Manual

exida®

80 N Main St
Sellersville, PA 18960

T-013, V6R1

Page 2 of 2

Page intentionally left blank

ABB Inc.
Measurement & Analytics

3400, rue Pierre-Ardouin
Québec (Québec) G1P 0B2
Canada

Phone:
North America: 1 800 858 3847
Worldwide: +1 418 877 8111

Fax:
+1 418 877-2834

E-mail:
laserscanner.support@ca.abb.com

Web:
www.abb.com/laserlevel

P/N AA019031-01 Rev B