

E3 Modulevel®

SIL Certified Safety Manual for E3 Modulevel® Model E3X-XXXX-SXX



Liquid Level Displacer Transmitter

This manual complements and is intended to be used with the Magnetrol® E3 Modulevel® Liquid Level Displacer Transmitter Installation and Operating manual (Bulletin 48-635).

Safety Function

The HART® version of the E3 Modulevel® transmitter will measure level and transmit a signal proportional to that level within the stated safety accuracy of $\pm 2\%$ of span (or the measured error published in I/O Manual 48-635, whichever is greater). In addition, when continuous, automatic diagnostics detect that the transmitter cannot perform this function, the output will be driven to the customer-specified out-of-range signal (i.e., 3.6 mA or 21 mA).

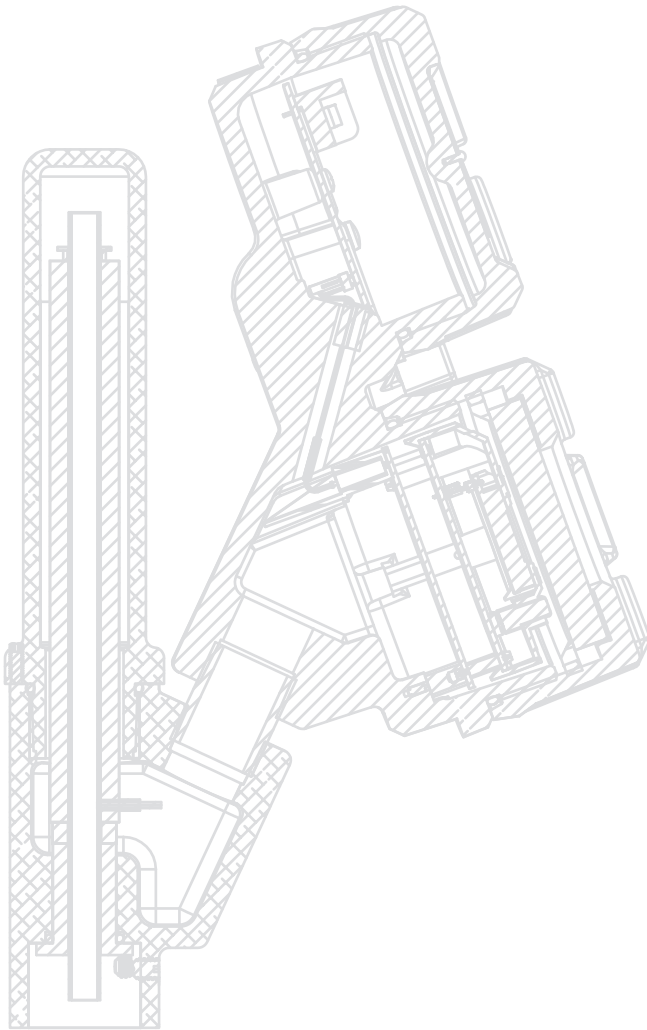
The E3 MODULEVEL is certified for use in low demand level measurement applications.

Application

The HART® version of the E3 MODULEVEL level transmitter can be applied in most process or storage vessels, bridles, and bypass chambers up to the transmitter's rated temperature and pressure. The E3 MODULEVEL can be used in liquids, clean or dirty, light hydrocarbons to heavy acids (SG=0.23 to 2.20) to meet the safety system requirements of IEC 61508 (Edition 2.0, 2010).

Benefits

- Level protection to SIL 3 as certified by exida Certification per IEC 61508.
- Level ranges from 14 to 120+ inches (356 to 3048+ mm).
- Process temperatures to +850 °F (+454 °C) for non-steam applications, +800 °F (+427 °C) for steam applications
- Process pressures to 5150 psi (355 bar).
- Continuous self-test with 22 mA or 3.6 mA fault indication fully compliant with NAMUR NE 43.
- IS, XP, and Non-Incendive approvals.
- Emission and immunity compliance to EN 61326.
- Two-wire, loop-powered transmitter for level, interface, or density measurement.





E3 Modulelevel® Displacer Level Transmitter

SIL Manual for E3 Modulelevel® E3X-XXXX-SXX

Table of Contents

| | | | |
|---|---|--|----|
| 1.0 Introduction..... | 3 | 6.6 Site Acceptance Testing..... | 8 |
| 1.1 Product Description..... | 3 | 6.7 Recording Results..... | 8 |
| 1.2 Theory of Operation..... | 3 | 6.8 Maintenance..... | 8 |
| 1.3 Determining Safety Integrity Level (SIL)..... | 4 | 6.8.1 Diagnostics and Response Times..... | 8 |
| 2.0 Applicable Models..... | 4 | 6.8.2 Troubleshooting..... | 9 |
| 3.0 Level Measuring System..... | 4 | 7.0 Recurrent Function Tests..... | 9 |
| 3.1 Miscellaneous Electrical Considerations..... | 5 | 7.1 Proof Testing..... | 9 |
| 3.1.1 Pollution Degree 2..... | 5 | 7.1.1 Introduction..... | 9 |
| 3.1.2 Overvoltage..... | 5 | 7.1.2 Interval..... | 9 |
| 3.1.3 Electromagnetic Compatibility..... | 5 | 7.1.3 Recording Results..... | 9 |
| 4.0 Mean Time To Repair (MTTR)..... | 5 | 7.1.4 Suggested Proof Test..... | 10 |
| 5.0 Supplementary Documentation..... | 6 | 7.1.5 Proof Test Coverage..... | 10 |
| 6.0 General Instructions..... | 6 | 8.0 Safety Requirements..... | 11 |
| 6.1 Systematic Limitations..... | 6 | 8.1 System Safety Assumptions..... | 11 |
| 6.1.1 Application..... | 6 | 8.2 Safety Function Requirements..... | 12 |
| 6.1.2 Environmental..... | 6 | 8.3 Safety User Programming and Configuration | |
| 6.1.2.1 Operating..... | 6 | Requirements..... | 12 |
| 6.1.2.2 Storage..... | 6 | 9.0 Appendices..... | 13 |
| 6.2 Installation..... | 7 | 9.1 SIL Certificate..... | 13 |
| 6.3 Skill Level of Personnel..... | 7 | 9.2 FMEDA Report: exida Management Summary..... | 14 |
| 6.4 Necessary Tools..... | 7 | 9.3 Specific E3 MODULELEVEL Values..... | 15 |
| 6.5 Configuration Information..... | 7 | 9.4 Report: Lifetime of Critical Components..... | 15 |
| 6.5.1 General..... | 7 | | |
| 6.5.2 Configuration..... | 7 | | |
| 6.5.3 Write Protecting/Locking..... | 8 | | |

1.0 Introduction

1.1 Product Description

Table 1
Enhanced E3 MODULELEVEL
Model Numbers

| | |
|----------|---|
| 1 | Transmitters: Model E3 MODULELEVEL, E3X-XXXX-SXX (HART) Hardware Version (or later) Analog Board 030-2475-001 + -003 Rev E Digital Board 030-9145-001 Rev AG Wiring Board 030-9151-001 Rev Q Software Version (or later) Model E3 HT 1.1cA.mot |
|----------|---|

The E3 MODULELEVEL is a loop-powered, two-wire, 24 VDC level transmitter that uses simple buoyancy principles in combination with a precision range spring and a highly accurate LVDT (linear variable differential transformer) to detect and convert liquid level changes into a stable 4–20 mA output signal.

NOTE: For Safety Instrumented Systems usage, it is assumed that the 4–20 mA output is used as the safety variable.

The analog output from the E3 MODULELEVEL meets the NAMUR NE 43 standard (3.8 mA to 20.5 mA usable). The transmitter contains self-diagnostics and is programmed to drive the output to a user-selected failure state, either low or high, upon internal detection of a diagnostic indicator. The device can be equipped with or without an optional non-interfering graphic liquid crystal display (LCD).

Table 1 indicates the version of the E3 MODULELEVEL transmitter that has been certified for SIL 2/3 applications.

1.2 Theory of Operation

The E3 MODULELEVEL Displacer Level Transmitter relies on the principles of buoyancy to convert mechanical movement to an electronic output.

The movement of the range spring, as it compresses or elongates based on the volume of displacer submerged in the liquid, causes movement of a special LVDT core attached to the spring. The LVDT technology converts the movement of the LVDT core within the LVDT to a stable 4–20 mA output signal. The position of the core, with respect to a primary and two secondary windings, induces voltage in each winding. The comparison of the induced voltages within the microprocessor of the E3 MODULELEVEL results in very accurate level or interface level output.

The E3 MODULELEVEL can, alternatively, be set up to track the changing density of a liquid over a known density range and convert that into a stable 4–20 mA output signal. As the density of the liquid changes, so does the mass of the liquid displaced by the displacer. This resulting change in buoyancy force on the displacer causes movement of the LVDT core needed to convert the density change to the 4–20 mA signal.

Table 2
SIL vs. PFDavg

| Safety Integrity Level (SIL) | Target Average probability of failure on demand (PFDavg) |
|------------------------------|--|
| 4 | $\geq 10^{-5}$ to $< 10^{-4}$ |
| 3 | $\geq 10^{-4}$ to $< 10^{-3}$ |
| 2 | $\geq 10^{-3}$ to $< 10^{-2}$ |
| 1 | $\geq 10^{-2}$ to $< 10^{-1}$ |

Table 3
Minimum hardware fault tolerance

Type B sensors, final elements and non-PE logic solvers

| SFF | Hardware Fault Tolerance (HFT) | | |
|---------------------|--------------------------------|-------|-------|
| | 0 | 1 | 2 |
| None: <60% | Not Allowed | SIL 1 | SIL 2 |
| Low: 60% to <90% | SIL 1 | SIL 2 | SIL 3 |
| Medium: 90% to <99% | SIL 2 | SIL 3 | |
| High: $\geq 99\%$ | SIL 3 | | |

1.3 Determining Safety Integrity Level (SIL)

Safety Instrumented System designers using the E3 MODULELEVEL must verify their design per applicable standards.

Three limits must be met to achieve a given SIL level:

1. The PFD_{AVG} numbers for the entire Safety Instrumented Function (SIF) must be calculated. Table 2 shows the relationship between the Safety Integrity Level (SIL) and the Probability of Failure on Demand Average (PFD_{AVG}).
2. Architecture constraints must be met for each subsystem. Table 3 can be used to determine the achievable SIL as a function of the Hardware Fault Tolerance (HFT) and the Safe Failure Fraction (SFF) for each subsystem in a safety system (Type B—complex components as per IEC 61508 Part 2) of which the level transmitter is just one component.
3. All products chosen for use in the SIF must meet the requirements of IEC 61508 for the given SIL Capability level or be justified based on proven in use data collected for each job.

The exSILentia tool from exida is recommended for design verification. This automatically checks all three limits and displays the results for any given design. The E3 MODULELEVEL is in the exSILentia database. This tool contains all needed failure rate, failure mode, SIL Capability and common cause data as well as suggested proof test methods.

2.0 Applicable Models

This manual is only applicable to the HART versions of the E3 MODULELEVEL transmitter shown in Table 1.

3.0 Level Measuring System

The diagram at left shows the structure of a typical measuring system incorporating the E3 MODULELEVEL transmitter. This SIL 2/3 Certified device is only available with an analog signal (4–20 mA) with HART communications; and, the measurement signal used by the logic solver can be the analog 4–20 mA signal proportional to the Level, Interface Level or Density.

- For fault monitoring, the logic unit must recognize both high alarms (≥ 21.5 mA) and low alarms (≤ 3.6 mA).
- If the logic solver loop uses intrinsic safety barriers, caution must be taken to ensure the loop continues to operate properly under the low alarm condition.

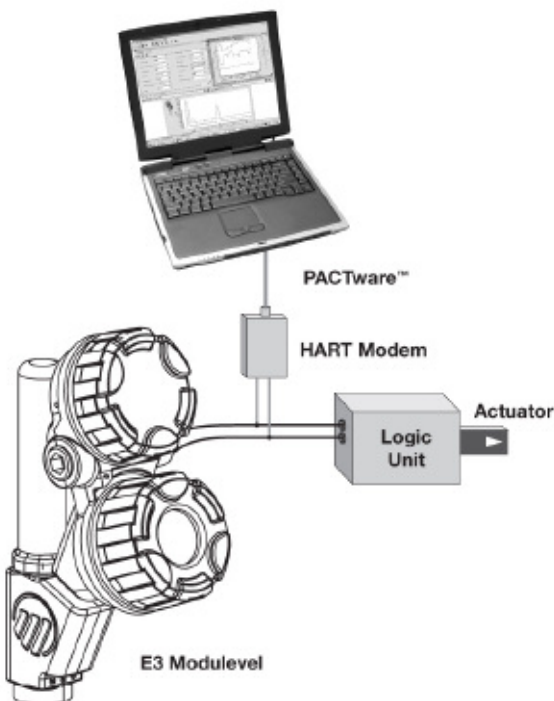


Figure 1
Typical System

-
- The only unsafe mode is when the unit is reading an incorrect level within the 4–20 mA range ($> \pm 2\%$ deviation).
 - MAGNETROL defines the faulted mode as one in which the 4–20 mA current is driven out of range (i.e., less than 3.8 mA or greater than 21.5 mA).
 - The 4–20 mA output signal can be configured for over-range per NAMUR NE43.

3.1 Miscellaneous Electrical Considerations

Following are miscellaneous electrical issues to be considered in a safety system.

3.1.1 Pollution Degree 2

The E3 MODULEVEL transmitter is designed for use in a Category II, Pollution Degree 2 installation, which is defined by a nonconductive pollution of the sort where occasionally a temporary conductivity caused by condensation must be expected.

This is the usual pollution degree used for equipment being evaluated to IEC/EN 61010.

3.1.2 Overvoltage

The E3 MODULEVEL has overvoltage protection per CE requirements; this protection is to 1000 volts when considering Hi-pot, Fast Transients, and Surge. Therefore, there should be no unsafe failure modes up to 1 KV.

Overvoltage Category II is a local level, covering appliances, portable equipment, etc., with smaller transient overvoltages than those characteristic of Overvoltage Category III. This category applies from the wall plug to the power supply isolation barrier (transformer). The typical plant environment is Overvoltage Category II, so most equipment evaluated to the requirements of IEC/EN 61010 are considered to belong in that classification.

3.1.3 Electromagnetic Compatibility

The E3 MODULEVEL is designed to meet the requirements of EN 61326 and NAMUR NE21.

4.0 Mean Time To Repair (MTTR)

SIL determinations are based on a number of factors including the Mean Time To Repair (MTTR). The analysis for the E3 MODULEVEL is based on a MTTR of 24 hours.

5.0 Supplementary Documentation

The E3 MODULEVEL Installation and Operating Manual (Bulletin 48-635) must be available for installation of the measuring system.

The following Electronic Device Description File is required if HART is used:

Manufacturer Code 0x56

**Model E3 MODULEVEL Device ID 0xE3, device revision 2
DD revision 1**

For device installations in a classified area, the relevant safety instructions and electrical codes must be followed.

6.0 General Instructions

6.1 Systematic Limitations

The following instructions must be observed to avoid systematic failures:

6.1.1 Application

The E3 MODULEVEL transmitter should be located for easy access for service, configuration, and monitoring. There should be sufficient headroom to allow installation and removal of the transmitter head, and, in cases of tank top configuration, the displacer. Special precautions should be made to prevent exposure to corrosive atmosphere, excessive vibration, shock, or physical damage. The E3 MODULEVEL should only be used for applications in which buildup of solid materials on the spring or in the enclosing tube is not an issue.

Caution: Operation of all buoyancy type level devices should be done in such a way as to minimize the action of dynamic forces on the float or displacer sensing element. Good practice for reducing the likelihood of damage to the control is to equalize pressure across the device very slowly.

6.1.2 Environmental

Refer to the E3 MODULEVEL Installation and Operating Manual (Bulletin 48-635) for Environmental limitations.

6.1.2.1 Operating

The operating temperature range is -40 to +175 °F (-40 to +80 °C).

6.1.2.2 Storage

The device should be stored in its original shipping box and not be subjected to temperatures outside the storage temperature range of -50 to +185 °F (-46 to +85 °C).

6.2 Installation

Refer to the E3 MODULELEVEL Installation and Operating Manual 48-635 manual for complete installation instructions.

- Contains information on the use, changing and resetting of the password-protection function.
- Provides menu selection items for configuration of the transmitter as a level sensing device.
- Offers configuration recommendations.
- Input voltage and loop resistance must be within the safe operating area of the device.

6.3 Skill Level of Personnel

Personnel following the procedures of this safety manual should have technical expertise equal to or greater than that of a qualified Instrument Technician.

6.4 Necessary Tools

No special equipment or tools are required to install E3 MODULELEVEL. The following items are recommended:

- **Wrenches, flange gaskets, and flange bolting appropriate for process connection(s)**
- Flat-blade screwdriver
- Level
- 1/8" Allen wrench
- 24 VDC power supply, 23 mA minimum
- Digital multimeter
- 250 to 450 ohm resistor for HART communication

6.5 Configuration Information

6.5.1 General

The E3 MODULELEVEL can be configured via the local display, the HART compatible handheld communicator, or a PC using *PACTware* and associated DTM.

6.5.2 Configuration

Ensure the E3 MODULELEVEL transmitter has been properly configured for the application. Special consideration should be given to the following configuration parameters:

User Password: Must be changed to a specific value other than Zero.

Failure Alarm: DO NOT choose HOLD for this parameter as a Fault will not be annunciated on the current loop.

Analog Output Mode: Ensure this is set to Enabled.

Interface Management: Ensure the displacer is completely immersed in liquid.

6.5.3 Write Protecting / Locking

The E3 MODULELEVEL transmitter is password protected with a numerical value between 0 and 255. After the password has been successfully entered, an exclamation mark (!) appears as the last character on the first line of the display.

Refer to the E3 MODULELEVEL Installation and Operating Manual (Bulletin 48-635) for information on password protection.

NOTE: Default Password = 0 = Password disabled.

For an SIS system, it is required that, after configuration of the system is complete, a password is utilized to prevent inadvertent changes to the device.

6.6 Site Acceptance Testing

To ensure proper operation after installation and configuration, a site acceptance test should be completed. This procedure is identical to the Proof Test Procedure described in Section 7.1.4.

6.7 Recording Results

Results of Site Acceptance Testing must be recorded for future reference.

6.8 Maintenance

The only maintenance required is the proof test.

- Report all failures to Magnetrol®.
- Firmware can be upgraded only by factory personnel.

6.8.1 Diagnostics and Response Times

Continuous internal diagnostics are present within the E3 MODULELEVEL transmitter. In the event a Fault is detected, a message will appear on the LCD and the output current will be driven to 3.6 mA or 22mA depending on how the FAULT parameter is configured.

A) Start-up Time:

- a. From application of power to normal operating mode: 5 seconds
- b. From application of power to Fault mode: 8 seconds or less (Assuming a Fault is present upon start-up)

-
- B) Diagnostic Test Interval: 3 seconds
 - a. This is defined as the time from the normal operating mode to the Fault mode upon the occurrence of a fault.
 - C) Safety Function Response Time:
3 seconds (with Damping=0)

6.8.2 Troubleshooting

Report all failures to the MAGNETROL Technical Support Department.

Refer to the E3 MODULELEVEL Installation and Operating Manual Bulletin 48-635 for troubleshooting device errors. To assist in finding errors should they occur, at start-up complete the Configuration Data Sheet found at the back of this manual, make a list of all device configuration parameters, including the password, and retain this information in a safe place.

- Firmware can be upgraded only by factory personnel.

7.0 Recurrent Function Tests

7.1 Proof Testing

7.1.1 Introduction

Following is the procedure utilized to detect Dangerous Undetected (DU) failures.

7.1.2 Interval

To maintain the appropriate Safety Integrity Level of a Safety Instrumented System, it is imperative that the entire system be tested at regular time intervals (shown as TI in the appropriate standards). The suitable SIL for the E3 MODULELEVEL transmitter is based on the assumption that the end user will carry out this test and inspection at least once per year.

NOTE: It is the responsibility of the owner/operator to select the type of inspection and the time period for these tests.

7.1.3 Recording Results

Results of the Proof Test should be recorded for future reference.

7.1.4 Suggested Proof Test

The suggested proof test for the E3 is described in the following table. The end user must use calibrated equipment to measure the output in steps 3, 4, and 6.

| Step | Action |
|------|--|
| 1 | Bypass the safety function and take appropriate action to avoid a false trip. |
| 2 | Use HART communications to retrieve any diagnostics and take appropriate action. |
| 3 | Send a HART command to the transmitter to go to the high alarm current output and verify that the analog current reaches that value. ① |
| 4 | Send a HART command to the transmitter to go to the low alarm current output and verify that the analog current reaches that value. ② |
| 5 | Inspect the transmitter for any leaks, visible damage or contamination. |
| 6 | Perform a two-point calibration ③ of the transmitter over the full working range. |
| 7 | Remove the bypass and otherwise restore normal operation. |

7.1.5 Proof Test Coverage

The Proof Test Coverage for the various product configurations is given in the following table.

Table 8 Proof Test Coverage – E3

| Device | λ_{DUPT} (FIT) | Proof Test Coverage |
|--------------------------|---------------------------|---------------------|
| E3, Single Solenoid, DTT | 14 | 76% |
| E3, Single Solenoid, ETT | 14 | 77% |

① This tests for compliance voltage problems such as a low loop power supply voltage or increased wiring resistance. This also tests for other possible failures.

② This tests for possible quiescent current related failures.

③ If the two-point calibration is performed with electrical instrumentation, this proof test will **not** detect any failures of the sensor.

8.0 Safety Requirements

This section specifies those safety characteristics allocated to the E3 MODULELEVEL that are conditions for its acceptance as a SIL certified device.

NOTE: This SIL evaluation has assumed that the customer will be able to acknowledge an over- or under-current condition via the Logic Solver.

8.1 System Safety Assumptions

The System Safety Assumptions provide a list of safety relevant assumptions made on the usage of the product over the safety life cycle of a user Safety Integrity Function, SIF. Magnetrol cannot directly control the user life cycle of a SIF using this product but needs to have assumptions on how the product will be used. It is important that users have full knowledge of these assumptions to ensure they are met when using the product as part of a SIF. This is to ensure the product is used in a manner consistent with the safety design.

This section only lists product specific assumptions and is not intended to specify measures required of the end user that are standard requirements for safety applications.

| Assumptions for Safety |
|---|
| The user SIF will detect and properly handle annunciation of detected fault conditions signaled by the alarm level output according to the specific requirements of the SIF. |
| Proper operation of the Model E3 MODULELEVEL is dependent on having 11 VDC or greater across the transmitter terminals during normal operation. |
| A user SIF integrating the Model E3 MODULELEVEL current loop output will detect faulted field wiring and other faults resulting in a current loop value signal outside of the specified range and take proper actions to maintain safety integrity according to the specific requirements of the SIF. |
| Local User Interface will not be relied upon by the end user SIF during normal operation and will be considered non-interfering to the safety function. |
| HART communications will not be relied upon by the end user for the SIF normal operation and will be considered non-interfering to the safety function. |
| The impact of end user configured damping values is not included in the published safety (function) response time. (The end user must consider this as part of overall time response of the SIF.) |
| The end user must take the E3 offline, independently verify all changes to end user configured parameters, and validate the safety function prior to putting the E3 back online and relying on the product for safety protection. |
| The end user will enable the User Password to lock out any end user modifiable configuration parameters available via the Local User Interface during normal operation. |
| The end user will enable the user password to lock out any end user modifiable configuration parameters available via the HART interface during normal operation. The end user will allow HART access only to qualified and trained personnel. |
| The end user will have proper procedures in place to ensure safe operation over the product life cycle. |
| The end user will ensure the device is properly installed per the product literature. The proper displacer will be used for the application with the transmitter properly connected. |
| The end user must not select HOLD for the alarm output. |
| Loop Current mode must be enabled. |

8.2 Safety Function Requirements

This section lists the Safety Function Requirements that specify what safety relevant functionality is to be performed for implementation of the safety integrity function and also to maintain the desired level of safety integrity. These requirements may also rule out particular functionality for SIF usage that could lead to designs that are difficult to validate for deterministic performance or safety integrity.

Safety Function Requirement

Upon application of power and successful initialization, the Model E3 MODULELEVEL **shall** enter the Normal Mode or Faulted Mode of operation.

Upon application of power and successful initialization, the Model E3 MODULELEVEL **shall** enter the Normal Mode operation within 5 seconds.

Upon application of power and successful initialization, the Model E3 MODULELEVEL **shall** enter the Faulted Mode of operation in less than 8 seconds.

The Model E3 MODULELEVEL **shall** transition to the Faulted Mode from the Normal Mode within the Diagnostic Test Interval after a diagnostic event occurs. The safety function will respond to a change from the user's process within the safety (function) response time.

The Model E3 MODULELEVEL **shall** transition to the Faulted Mode from the Normal Mode within the Diagnostic Test Interval of 3 seconds after a diagnostic event occurs.

The safety function output of the Model E3 MODULELEVEL **shall** respond to a change from the user's process within the safety (function) response time of 3 seconds assuming Damping is set to 0.

The Model E3 MODULELEVEL **may** leave the Faulted Mode when all diagnostics are clear.

8.3 Safety User Programming and Configuration Requirements

The Safety User Programming and Configuration Requirements provide the requirements for field configuration of the device required to create and maintain SIF configurations. These requirements should provide the necessary guidance to ensure that the engineering environment will meet both the intended market and safety certification requirements, along with guidance and user restrictions documented in the safety manual.






Safety User Programming Requirement

Setup, configuration, and maintenance functionality for the Model E3 MODULELEVEL **shall** be supported by the non-interfering HART communications interface.

Setup, configuration and maintenance functionality for the Model E3 MODULELEVEL **shall** be supported by the non-interfering Local User Interface.

9.0 Appendices

9.1 SIL Certificate

|  <p>The manufacturer may use this mark.</p>  <p>Revision 1.1 Sep 1, 2016 Surveillance Audit Due September 1, 2019</p>  <p>ANSI Accredited Program PRODUCT CERTIFICATION #1604</p> | <p>Certificate / Certificat / Zertifikat / 合格証 Zertifikat / 合格証 MAG 15-02-050 C001 <i>exida</i> hereby confirms that the:</p> <p>E3 Module Level Displacer Transmitter Magnetrol International, Inc. Aurora, IL - USA</p> <p>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 3 (SIL 3 Capable) Random Capability: Type B Element SIL 2 @ HFT=0; SIL 3 @ HFT = 1; Route 2_H PFD_{avg} and Architecture Constraints must be verified for each application</p> <p>Safety Function: The E3 Module Level Displacer Transmitter will measure a level, interface level or density measurement, and transmit a corresponding signal within the stated safety accuracy.</p> <p>Application Restrictions: The unit must be properly designed into a Safety Instrumented Function per the Safety Manual requirements.</p> <p> Evaluating Assessor <i>David S. Bell</i> Certifying Assessor <i>John C. Zippell</i></p> <p>Page 1 of 2</p> | <p>E3 Module Level Displacer Transmitter</p>  <p>80 N Main St Solersville, PA 19800 T-002, v04r30</p> | <p>Certificate / Certificat / Zertifikat / 合格証 MAG 15-02-050 C001 Systematic Capability: SC 3 (SIL 3 Capable) Random Capability: Type B Element SIL 2 @ HFT=0; SIL 3 @ HFT = 1; Route 2_H PFD_{avg} and Architecture Constraints must be verified for each application</p> <p>Systematic Capability : The product has met manufacturer design process requirements of Safety Integrity Level (SIL) 3. 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. This device meets exida criteria for Route 2_H.</p> <p>Random Capability: The SIL limit imposed by the Architectural Constraints must be met for each element.</p> <p>IEC 61508 Failure Rates in FIT*</p> <table border="1"><thead><tr><th>Device</th><th>Asd</th><th>Asu</th><th>Aoo</th><th>Aou</th></tr></thead><tbody><tr><td>E3 Local</td><td>0</td><td>13</td><td>579</td><td>61</td></tr><tr><td>E3 Remote</td><td>0</td><td>14</td><td>607</td><td>61</td></tr></tbody></table> <p>* FIT = 1 failure / 10⁹ hours</p> <p>SIL Verification: The Safety Integrity Level (SIL) of an entire Safety Instrumented Function (SIF) must be verified via a calculation of 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.</p> <p>The following documents are a mandatory part of certification: Assessment Report: MAG 15-02-050 R002 V1 R2 Safety Manual: E3 Module Level Safety Manual 48-651.0</p> <p>Page 2 of 2</p> | Device | Asd | Asu | Aoo | Aou | E3 Local | 0 | 13 | 579 | 61 | E3 Remote | 0 | 14 | 607 | 61 |
|--|--|--|---|--------|-----|-----|-----|-----|----------|---|----|-----|----|-----------|---|----|-----|----|
| Device | Asd | Asu | Aoo | Aou | | | | | | | | | | | | | | |
| E3 Local | 0 | 13 | 579 | 61 | | | | | | | | | | | | | | |
| E3 Remote | 0 | 14 | 607 | 61 | | | | | | | | | | | | | | |



Management Summary

The Functional Safety Assessment of the Magnetrol International, Inc.

E3 Modulevel® Liquid Level Displacer Transmitter

development project, performed by *exida* consisted of the following activities:

- *exida* assessed the development process used by Magnetrol International, Inc. through an audit and review of a detailed safety case against the *exida* certification scheme which includes the relevant requirements of IEC 61508. The assessment was executed using subsets of the IEC 61508 requirements tailored to the work scope of the development team.
- *exida* reviewed and assessed a detailed Failure Modes, Effects, and Diagnostic Analysis (FMEDA) of the devices to document the hardware architecture and failure behavior.
- *exida* reviewed the manufacturing quality system in use at Magnetrol International, Inc.

The functional safety assessment was performed to the SIL 3 requirements of IEC 61508:2010. A full IEC 61508 Safety Case was created using the *exida* Safety Case tool, which also was used as the primary audit tool. Hardware and Software process requirements and all associated documentation were reviewed. Environmental test reports were reviewed. The user documentation and safety manual also were reviewed.

The results of the Functional Safety Assessment can be summarized by the following statements:

The audited development process, as tailored and implemented by the Magnetrol International, Inc. E3 Modulevel® Level Transmitter development project, complies with the relevant safety management requirements of IEC 61508 SIL 3.

The assessment of the FMEDA also shows that the E3 Modulevel® Level Transmitter meets the requirements for architectural constraints of an element such that it can be used, with HFT=0, to implement a SIL 2 safety function, or with HFT = 1, to implement a SIL 3 safety function.

This means that the E3 Modulevel® Level Transmitter is capable for use in SIL 3 applications in Low demand mode when properly designed into a Safety Instrumented Function per the requirements in the Safety Manual, and when using the versions of the product specified in section 3.1 of this document. The PFD_{avg} of the Safety Instrumented Function must also be calculated and found to be in the SIL 3 range required by IEC 61508 for compliant use.

© *exida*
T-034 V4R8

MAG 15-02-050 R002 V1R2 IEC 61508 Assessment Report - E3.docx
64 N. Main St, Sellersville, PA 18960
Page 2 of 17



Results of the IEC 61508 Functional Safety Assessment

Project:
E3 Modulevel® Liquid Level Displacer Transmitter

Customer:
Magnetrol International, Inc.
Aurora, IL
USA

Contract No.: Q15/02-050
Report No.: MAG 15-02-050 R002
Version V1, Revision R2, 9/1/2016
Dave Butler

The document was prepared using best effort. The authors make no warranty of any kind and shall not be liable in any event for incidental or consequential damages in connection with the application of the document.
© All rights reserved.

9.3 Specific E3 MODULELEVEL Values

| Product | E3 MODULELEVEL Model E3X-XXXX-SXX |
|--------------------|--------------------------------------|
| SIL | SIL 2 |
| HFT | 0 |
| SFF | 90.6% |
| PFD _{avg} | Refer to FMEDA report |

9.4 Report: Lifetime of Critical Components

According to section 7.4.9.5 of IEC 61508-2, a useful lifetime, based on experience, should be assumed.

Although a constant failure rate is assumed by probabilistic estimation method, this only applies provided that the useful lifetime of components is not exceeded. Beyond their useful lifetime the result of the probabilistic calculation method is therefore meaningless, as the probability of failure significantly increases with time. The useful lifetime is highly dependent on the subsystem itself and its operating conditions.

The assumption of a constant failure rate is based on the bathtub curve. Therefore it is obvious that the PFD_{avg} calculation is only valid for components that have this constant domain and that the validity of the calculation is limited to the useful lifetime of each component.

The expected useful life of E3 MODULELEVEL Model E3X-XXXX-SXX is at least 50 years.

It is the responsibility of the end user to maintain and operate the Model E3X-XXXX-SXX per manufacturer's instructions. Furthermore, regular inspection should indicate that all components are clean and free from damage.

When plant experience indicates a shorter lifetime than indicated by the FMEDA report, the number based on plant experience should be used.

References

- IEC 61508 Edition 2.0,2010
“Functional Safety of Electrical/Electronic/
Programmable Electronic Safety Related Systems”
- ANSI/ISA-84.00.01-2004 Part 1 (IEC 61511-1Mod)
“Functional Safety: Safety Instrumented Systems for
the Process Industry Sector – Part 1 Hardware and
Software Requirements”
- ANSI/ISA-84.00.01-2004 Part 2 (IEC 61511-2Mod)
“Functional Safety: Safety Instrumented Systems for
the Process Industry Sector – Part 2 Guidelines for
the Application of ANSI/ISA84.00.01-2004 Part 1
(IEC 61511-1 Mod) – Informative”
- ANSI/ISA-84.00.01-2004 Part 3 (IEC 61511-3Mod)
“Functional Safety: Safety Instrumented Systems for
the Process Industry Sector – Part 3 Guidance for the
Determination of the Required Safety Integrity Levels
– Informative”
- ANSI/ISA-TR84.00.04 Part 1 (IEC 61511 Mod)
“Guideline on the Implementation of ANSI/ISA-
84.00.01-2004”

Disclaimer

The SIL values in this document are based on an FMEDA analysis using exida’s SILVER Tool. MAGNETROL accepts no liability whatsoever for the use of these numbers or for the correctness of the standards on which the general calculation methods are based.

ASSURED QUALITY & SERVICE COST LESS

Service Policy

Owners of MAGNETROL controls may request the return of a control or any part of a control for complete rebuilding or replacement. They will be rebuilt or replaced promptly. Controls returned under our service policy must be returned by prepaid transportation. MAGNETROL will repair or replace the control at no cost to the purchaser (or owner) other than transportation if:

1. Returned within the warranty period; and
2. The factory inspection finds the cause of the claim to be covered under the warranty.

If the trouble is the result of conditions beyond our control; or, is NOT covered by the warranty, there will be charges for labor and the parts required to rebuild or replace the equipment.

In some cases it may be expedient to ship replacement parts; or, in extreme cases a complete new control, to replace the original equipment before it is returned. If this is desired, notify the factory of both the model and serial numbers of the control to be replaced. In such cases, credit for the materials returned will be determined on the basis of the applicability of our warranty.

No claims for misapplication, labor, direct or consequential damage will be allowed.

Return Material Procedure

So that we may efficiently process any materials that are returned, it is essential that a “Return Material Authorization” (RMA) number be obtained from the factory prior to the material’s return. This is available through a MAGNETROL local representative or by contacting the factory. Please supply the following information:

1. Company Name
2. Description of Material
3. Serial Number
4. Reason for Return
5. Application

Any unit that was used in a process must be properly cleaned in accordance with OSHA standards, before it is returned to the factory.

A Material Safety Data Sheet (MSDS) must accompany material that was used in any media.

All shipments returned to the factory must be by prepaid transportation.

All replacements will be shipped F.O.B. factory.



705 Enterprise Street • Aurora, Illinois 60504-8149 • 630-969-4000 • Fax 630-969-9489
info@magnetrol.com • www.magnetrol.com

Copyright © 2016 Magnetrol International, Incorporated. All rights reserved. Printed in the USA.

Magnetrol, Magnetrol logotype and Eclipse are registered trademarks of Magnetrol International, Incorporated.
HART is a registered trademark of the HART Communication Foundation.
PACTware is trademark of PACTware Consortium.

BULLETIN: 48-651.0
EFFECTIVE: September 2016