Functional Safety Manual
M310/FSM, Rev BA
April 2017

Mobrey™ Magnetic Level Switches

Functional Safety Manual

EMERSON™

Contents

Section 1 Introduction

1.1 Scope and purpose of the safety manual

This safety manual contains the information to design, install, verify and maintain a Safety Instrumented Function (SIF) utilizing the Mobrey Magnetic Level Switch.

The manual provides the necessary requirements to enable the integration of the horizontal point-level float switch when showing compliance with the IEC 61508 or IEC 61511 functional safety standards. It indicates all assumptions that have been made on the usage of the level switch. If these assumptions cannot be met by the application, the Safety Integrity Level (SIL) capability of the product may be adversely affected.

Note
For product support, use the contact details on the back page.

1.2 Skill Level Requirement

System design, installation and commissioning, and repair and maintenance shall be carried out by suitably qualified personnel.

1.3 Safety messages

Procedures and instructions in this section may require special precautions to ensure the safety of the personnel performing the operation. Information that raises potential safety issues is indicated by a warning symbol (⚠). Refer to the following safety messages before performing an operation preceded by this symbol.

⚠ WARNING

Failure to follow these guidelines could result in death or serious injury.

- Make sure only qualified personnel perform the installation.

Explosions could result in death or serious injury.

- Verify that the operating environment of the level switch is consistent with the appropriate hazardous locations certifications.
- Do not remove the level switch covers in explosive atmospheres when the circuit is alive.

Electrical shock can result in death or serious injury.

- Avoid contact with the leads and terminals. High voltage that may be present on leads can cause electrical shock.
- Make sure the main power to the level switch is off, and the lines to any other external power source are disconnected or not powered while wiring the level switch.

1.4 Terms, abbreviations, and acronyms

Table 1-1. Terms, Abbreviations, and Acronyms

Term	Definition
Basic safety	Freedom from unacceptable risk of harm
BPCS	Basic Process Control System – a system which responds to input signals from the process, its associated equipment, other programmable systems and/or an operator and generates output signals causing the process and its associated equipment to operate in the desired manner but which does not perform any safety instrumented functions with a claimed SIL greater than or equal to 1.
Fail Safe State	State where the switch output is in the state corresponding to an alarm condition. In this condition, the switch contacts will normally be open.
Fail Dangerous	Failure that does not respond to an input from the process (i.e. not switching to the fail-safe state).
Fail Dangerous Detected	Failure that is dangerous but is detected.
Fail Dangerous Undetected	Failure that is dangerous and that is not detected.
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	Failure that causes the switch to go to the defined fail-safe state without an input from the process.
FIT	FIT is the abbreviation for Failure In Time. One FIT is $1x10^{-9}$ failure per hour
FMEDA	Failure Modes, Effects and Diagnostic Analysis
Functional Safety	Part of the overall safety relating to the process and the BPCS which depends on the correct functioning of the Safety Instrumented System (SIS) and other protection layers.
HFT	Hardware Fault Tolerance
Low demand	Mode of operation, where the frequency of demands for operation made on a safety-related system is no greater than twice the proof test frequency.
PFD_{AVG}	Average Probability of Failure on Demand
SFF	Safe Failure Fraction – a fraction of the overall random failure rate of a device that results in either a safe failure or a detected dangerous failure.
SIF	Safety Instrumented Function – a safety function with a specified SIL which is necessary to achieve functional safety. Typically a set of equipment intended to reduce the risk due to a specified hazard (a safety loop).
SIL	Safety Integrity Level - a discrete level (one out of four) for specifying the safety integrity requirements of the safety instrumented functions to be allocated to the safety instrumented systems. SIL 4 has the highest level of safety integrity, and SIL 1 has the lowest level.
SIS	Safety Instrumented System (SIS) – an instrumented system used to implement one or more safety instrumented functions. An SIS is composed of any combination of sensors, logic solvers, and final elements.

1.5 Documentation and standards

This section lists the documentation and standards referred to by this safety manual

Table 1-2. Associated Documentation

Documents	Purpose of documents
IEC 61508-2: ed2, 2010	Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems
Exida EM 10/08-36 R001	FMEDA Report Version V1, Revision R2 for the Mobrey magnetic level switch with a F84 Float
IP101	Mobrey magnetic level switch Product Data Sheet
M310	Mobrey magnetic level switch Instruction leaflet

Table 1-3. Associated Standards

Standards	Purpose of standards
IEC 61508: ed2, 2010	Functional Safety of electrical/electronic/programmable electronic safety-related systems
IEC 61511 (ANSI/ISA 84.00.01-2004)	Functional safety - Safety instrumented systems for the process industry sector

Section 2 Product Description

Note
For all product information and documentation downloads, see the on-line Mobrey Magnetic Level Switch web page at Emerson.com/Mobrey.

2.1 Operation principle

The level switch is designed to open or close a circuit ("switch") as a changing liquid level within a vessel passes the level of the float (the Switch Point).

When the process fluid level is below the Switch Point, contacts B-B are made and contacts A-A are open (Figure 2-1 on page 5).

When the process fluid level is above the Switch Point, contacts A-A are made and contacts B-B are open (Figure 2-2 on page 5).

Figure 2-1. Level Decreases – Float Pivots Downwards

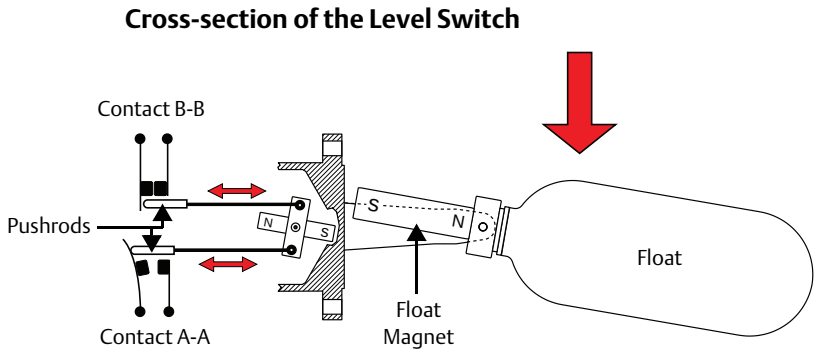
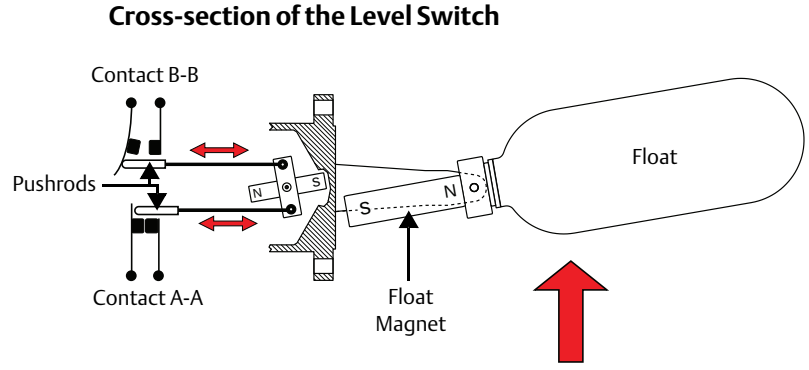


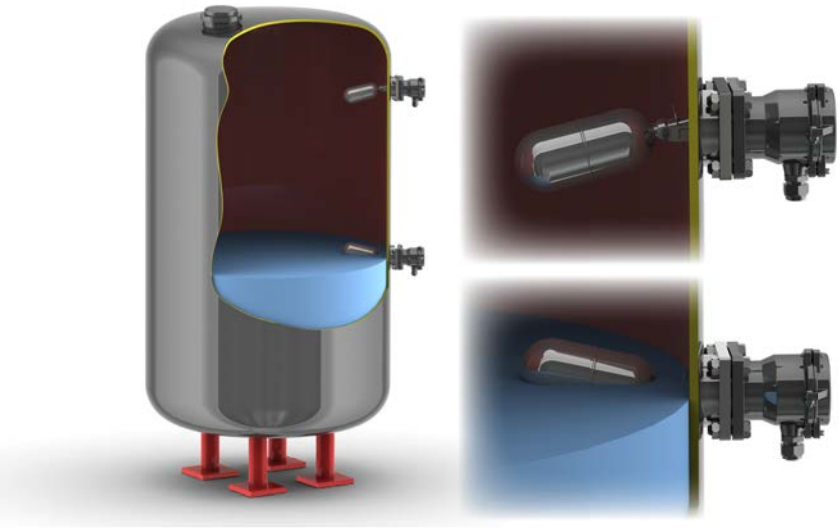
Figure 2-2. Level Increases –Float Pivots Upwards



2.2 Level switch purpose

Mobrey magnetic level switches are ideal for high and low liquid level alarm, overfill alarm, and pump control duties.

Figure 2-3. Application Example: High and Low Level Alarm



2.3 Ordering information

Level switch models fitted with options listed Appendix B: Level Switches Certified to IEC 61508 of this manual have been externally assessed and certified to IEC 61508.

A copy of the third party SIL certificate can be ordered using the part number MBY-CERT-SIL-L2049.

Note
For all product information and documentation downloads, see the on-line Mobrey Magnetic Level Switch web page at Emerson.com/Mobrey.

Section 3 Designing a Safety Function Using the Level Switch

Note
For all product information and documentation downloads, see the on-line Mobrey Magnetic Level Switch web page at Emerson.com/Mobrey.

3.1 Safety function

A change in liquid level through the operating range of the float causes the switch to operate. It may be used in high level or low level safety related applications. In either case, it is recommended to use the set of contacts (A-A or B-B) which are Open in the Fail Safe State.

3.2 Environmental limits

The designer of the SIF (Safety Instrumented Function) must check that the level switch is rated for use within the expected environmental limits. See the Mobrey Magnetic Level Switch Product Data Sheet for environmental limits.

3.3 Application limits

It is very important that the SIF designer checks for material compatibility by considering process liquids and on-site chemical contaminants. If the level switch is used outside the application limits or with incompatible materials, the reliability data and predicted SIL capability becomes invalid.

The construction materials of a level switch are specified in the product data sheet and the product reference manual (see Table 1-2 on page 3). Use the model code on the product label, and the ordering information table and specification in these product documents, to find out the construction materials.

3.4 Design verification

A detailed Failure Modes, Effects and Diagnostics Analysis (FMEDA) report for the Mobrey Magnetic Level Switch is available from Emerson. This report details all failure rates and failure modes as well as expected lifetime.

Note
The FMEDA report is available from the Mobrey Magnetic Horizontal Float Switches web site page at Emerson.com/Mobrey. In the Documents section, there are SIL documents including the FMEDA report and this safety manual.

The achieved Safety Integrity Level (SIL) of an entire Safety Instrumented Function (SIF) design must be verified by the designer using a PFD_{AVG} calculation considering the architecture, proof-test interval, proof-test effectiveness, any automatic diagnostics, average repair time, and the specific failures rates of all equipment included in the SIF.

Each subsystem must be checked to assure compliance with minimum Hardware Fault Tolerance (HFT) requirements. When using the level switch in a redundant configuration, a common cause factor of at least 5% should be included in the safety integrity calculations.

The failure rate data listed in the FMEDA report is only valid for the useful lifetime of the level switch. Failure rates increase after this useful lifetime period has expired. Reliability calculations based on the data listed in the FMEDA report for mission times beyond the lifetime may yield results that are too optimistic, i.e. the calculated SIL will not be achieved.

3.5 SIL capability

3.5.1 Systematic integrity

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

A Safety Instrumented Function (SIF) designed with the Mobrey level switch must not be used at a SIL higher than the statement without “prior use” justification by the end-user, or verification of diverse technology in the design.

3.5.2 Random integrity

The Mobrey level switch is a type A device according to Table 2 of the standard IEC 61508-2. Using Route 2H assessment criteria, the device Random Capability has been determined as SIL 2.

3.5.3 Safety parameters

The failure rates given here are valid for the useful lifetime of the product, as described in the section “Useful lifetime” on page 13.

Note
The FMEDA report is available from the Mobrey Magnetic Horizontal Float Switches web site page at Emerson.com/Mobrey. In the Documents section, there are SIL documents including the FMEDA report and this safety manual.

Table 3-1. Failure Rates for Level Switch, 4-contact Versions – Types D and P

Failure category	Failure rate (FIT)[1]	
	Maximum detection	Minimum detection
Fail Safe Detected	0	0
Fail Safe Undetected	88	117
Fail Dangerous Detected	0	0
Fail Dangerous Undetected	243	214
No Effect	34	34

1. FIT is the abbreviation for Failure In Time. One FIT is $1x10^{-9}$ failure per hour.

Table 3-2. Failure Rates for Level Switch, 6-contact Versions – Types D6, P6, H6, and B6

Failure category	Failure rate (FIT)[1]	
	Maximum detection	Minimum detection
Fail Safe Detected	0	0
Fail Safe Undetected	168	197
Fail Dangerous Detected	0	0
Fail Dangerous Undetected	327	298
No Effect	34	34

1. FIT is the abbreviation for Failure In Time. One FIT is $1x10^{-9}$ failure per hour.

Table 3-3. Failure Rates according to IEC 61508, 4-contact Versions – Types D and P (FIT)

Device	δ_{SD}[1]	δ_{SU}	δ_{DD}	δ_{DU}
Level switch, maximum detection	0	88	0	243
Level switch, minimum detection	0	117	0	214

1. FIT is the abbreviation for Failure In Time. One FIT is $1x10^{-9}$ failure per hour.

Table 3-4. Failure Rates according to IEC 61508, 6-contact Versions – Types D6, P6, H6, and B6 (FIT)

Device	δ_{SD}[1]	δ_{SU}	δ_{DD}	δ_{DU}
Level switch, maximum detection	0	168	0	327
Level switch, minimum detection	0	197	0	298

1. FIT is the abbreviation for Failure In Time. One FIT is $1x10^{-9}$ failure per hour.

3.6 Connection of the level switch to the SIS logic solver

The Mobrey level switch should be connected to the safety-rated logic solver which is actively performing the safety function as well as automatic diagnostics (if any) designed to diagnose potentially dangerous failures within the level switch. The Mobrey Magnetic Level Switch Reference Manual gives installation details for the level switch.

3.7 General requirements

- The system and function response time shall be less than the process safety time. The Mobrey level switch will change to its defined safe state in less than this time with relation to the specific hazard scenario.
- All SIS components, including the Mobrey level switch must be operational before process start-up.
- The user shall verify that the Mobrey level switch is suitable for use in safety applications by confirming the level switch nameplate and model number are properly marked.
- Personnel performing maintenance and testing on the Mobrey level switch shall first be assessed as being competent to do so.
- Results from periodic proof tests shall be recorded and periodically reviewed.
- The Mobrey level switch shall not be operated beyond the useful lifetime as listed in the section "Useful lifetime" on page 13 without undergoing overhaul or replacement.

Section 4 Installation and Commissioning

Note
For all product information and documentation downloads, see the on-line Mobrey Magnetic Level Switch web page at Emerson.com/Mobrey.

4.1 Installation

The Mobrey Magnetic Level Switch (“level switch”) must be installed as described in the installation section of the product manual M310. Check that environmental conditions do not exceed the ratings in the specification section.

The Mobrey level switch must be accessible for physical inspection.

4.2 Physical location and placement

The Mobrey level switch shall be accessible with sufficient room for cover removal and electrical connections, and allow for manual proof-testing to take place.

The switch point is determined by the location of the level switch, and consideration must be given to allow the safe proof-testing of the level switch by forcing liquid to put the switch into its Fail Safe State.

4.3 Electrical connections

Wiring should be adequately rated and not be susceptible to mechanical damage. Electrical conduit is commonly used to protect wiring.

Section 5 Operation and Maintenance

5.1 Proof-test requirement

During operation, a low-demand mode SIF must be proof-tested. The objective of proof-testing is to detect failures within the equipment in the SIF that are not detected by any automatic diagnostics of the system. Undetected failures that prevent the SIF from performing its function are the main concern.

Periodic proof-tests shall take place at the frequency (or interval) defined by the SIL verification calculation. The proof-tests must be performed more frequently than or as frequently as specified in the SIL verification calculation in order to maintain the required safety integrity of the overall SIF.

A sample procedure is provided in Appendix A: Proposed Proof-test Procedure.

Results from periodic proof tests shall be recorded and periodically reviewed.

5.2 Repair and replacement

Repair procedures in the product manual M310 must be followed.

5.3 Notification of failures

In case of malfunction of the system or SIF, the Mobrey Magnetic Level Switch (“level switch”) shall be put out of operation and the process shall be kept in a safe state by other measures.

Emerson must be informed when the level switch is required to be replaced due to failure. The occurred failure shall be documented and reported to Emerson using the contact details on the back page of this functional safety manual. This is an important part of Emerson’s SIS management process.

5.4 Useful lifetime

According to the 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 the probabilistic estimation method (see FMEDA report), this only applies provided that the useful lifetime[(1)] 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.

This assumption of a constant failure rate is based on the bath-tub 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.

Based on general field failure data and manufacturer component data, a useful life period of approximately 10 to 15 years is expected for the Mobrey level switch. When plant experience indicates a shorter useful lifetime than indicated here, the number based on plant experience should be used.

1. *Useful lifetime is a reliability engineering term that describes the operational time interval where the failure rate of a device is relatively constant. It is not a term which covers product obsolescence, warranty, or other commercial issues.*

Appendix A Proposed Proof-test Procedure

A.1 Suggested proof-test

According to Section 7.4.3.2.2 (f) of the standard IEC 61508-2, proof-tests shall be undertaken to reveal dangerous faults which are undetected by diagnostic tests. This means that it is necessary to specify how dangerous undetected faults which have been noted during the Failure Modes, Effects, and Diagnostic Analysis can be detected during proof-testing.

The suggested proof-tests (Table A-1 and Table A-2) consist of switch operation tests in-situ.

Table A-1. Suggested Proof-test (Low Level Alarm)

Step	Action
1	Inspect the accessible parts of the level switch for any leaks or damage
2	Bypass the safety function and take appropriate action to avoid a false trip
3	Disable any **filling** mechanism and drain the vessel to force the switch to the fail-safe state and confirm that the Safe State was achieved and within the correct time. **INDEPENDENT PRECAUTIONS MUST BE TAKEN TO ENSURE THAT NO HAZARD CAN RESULT FROM THIS OPERATION**.
4	Reinstate the **filling** mechanism so that the vessel refills and confirm that the normal operating state of the switch was achieved.
5	Remove the safety function bypass and otherwise restore normal operation

Table A-2. Suggested Proof-test (High Level Alarm)

Step	Action
1	Inspect the accessible parts of the level switch for any leaks or damage
2	Bypass the safety function and take appropriate action to avoid a false trip
3	Disable any **drain** mechanism and fill the vessel to force the switch to the fail-safe state and confirm that the Safe State was achieved and within the correct time. **INDEPENDENT PRECAUTIONS MUST BE TAKEN TO ENSURE THAT NO HAZARD CAN RESULT FROM THIS OPERATION**.
4	Reinstate the **drain** mechanism so that the vessel refills and confirm that the normal operating state of the switch was achieved
5	Remove the safety function bypass and otherwise restore normal operation

A.2 Proof-test coverage

The proof-test coverage for the tests listed in the section "Suggested proof-test " are in Table A-3.

Table A-3. Proof-test Coverage

Safety function	Proof-test coverage
4-contact versions – types D and P	84%
6-contact versions – types D6, P6, H6, and B6	88%

Appendix B Level Switches Certified to IEC 61508

B.1 List of Level Switches Certified to IEC 61508

Tables B-1, B-2, and B-3 list all Mobrey Magnetic Level Switch options that are certified to IEC 61508. In general, this is the entire range with the exception of the marine versions, pneumatic switch mechanisms, and some floats. Refer to product data sheet IP101 for the full specifications.

Table B-1. Level Switches for General Purpose Applications (Stainless Steel Wet-side)

Model	Product description		
S	Switch		
Flange (head)		**Flange (head)**	
36	Mobrey A	431	EN 1092-1 PN 16 (DN 125)
190	Mobrey A	417	EN 1092-1 DN 65 PN 40 (DN 65)
440	3 in. ASME B16.5 Class 150 RF	418	EN 1092-1 PN 40 (DN 80)
441	4 in. ASME B16.5 Class 150 RF	419	EN 1092-1 PN 40 (DN 100)
424	3 in. ASME B16.5 Class 300 RF	433	EN 1092-1 PN 40 (DN 125)
425	4 in. ASME B16.5 Class 300 RF	434	EN 1092-1 PN 40 (DN 150)
489	3 in. ASME B16.5 Class 600 RF	488	EN 1092-1 PN 63 (DN 80)
490	3 in. ASME B16.5 Class 900 RF	435	EN 1092-1 PN 63 (DN 100)
428	EN 1092-1 PN 16 (DN 65)	436	EN 1092-1 PN 63 (DN 125)
429	EN 1092-1 PN 16 (DN 80)	437	EN 1092-1 PN 63 (DN 150)
430	EN 1092-1 PN 16 (DN 100)		
Switch mechanism			
D	Electrical: 2 independent Single Pole Single Throw (SPST) contact sets		
P	As Type D but with gold plated contacts		
D6	Electrical: 2 independent circuits of double pole changeover contact sets		
P6	As Type D6 but with gold plated contacts		
H6	As Type D6 but with gold plated contacts and hermetically sealed moving parts		
B6	As Type H6 but approved for Zone 2 areas		
Enclosure/housing			
A	Aluminum alloy		
Float			
F84	General purpose e.g. high/low alarm, 316 SST		
F93	Shrouded for dirty liquids, 316 SST		
F96	General purpose e.g. high/low alarm, 316 SST		
F98	General purpose e.g. high/low alarm, 316 SST		
F185	General purpose e.g. high/low alarm, Alloy 400		
F104/+	Cranked arm: horizontal or vertical, 316 SST		
F106	General purpose e.g. high/low alarm, 316 SST		
F107	General purpose e.g. high/low alarm, 316 SST		
Typical Model Number: S 36 D A / F84			

Table B-2. Level Switches for General Purpose Applications (Aluminum Bronze Wet-side)

Model	Product description
S	Switch
Flange (head)	
01	Mobrey A flange
Switch mechanism	
DB	Electrical: 2 independent Single Pole Single Throw (SPST) contact sets
PB	As Type DB but with gold plated contacts
D6B	Electrical: 2 independent circuits of double pole changeover contact sets
P6B	As Type D6B but with gold plated contacts
Float	
F84	General purpose e.g. high/low alarm, 316 SST
F93	Shrouded for dirty liquids, 316 SST
F185	General purpose e.g. high/low alarm, Alloy 400
F104/+	Cranked arm: horizontal or vertical, 316 SST
Typical model number: S 01 DB / F84	

Table B-3. Level Switches for Hazardous Area Applications

Model	Product description
S	Switch
Flange (head)	
250	Mobrey G, 316 Stainless Steel
275	Mobrey G, Gunmetal
256	3 in. ASME B16.5 Class 150 RF
257	4 in. ASME B16.5 Class 150 RF
278	6 in. ASME B16.5 Class 150 RF
251	3 in. ASME B16.5 Class 300 RF
254	4 in. ASME B16.5 Class 300 RF
260	3 in. ASME B16.5 Class 600 RF
261	3 in. ASME B16.5 Class 900 RF
253	EN 1092-1 PN 40 (DN 80)
255	EN 1092-1 PN 40 (DN 100)
269	EN 1092-1 PN 40 (DN 125)
272	EN 1092-1 PN 63 (DN 80)
268	EN 1092-1 PN 63 (DN 100)
270	EN 1092-1 PN 63 (DN 125)
271	EN 1092-1 PN 63 (DN 150)

Switch Mechanism	
D	Electrical: 2 independent Single Pole Single Throw (SPST) contact sets
P	As Type D but with *gold plated contacts*
D6	Electrical: 2 independent circuits of double pole changeover contact sets
P6	As Type D6 but with *gold plated contacts*
H6	As Type D6 but with *gold plated contacts* and *hermetically sealed moving parts*
Enclosure / Housing	
A	Aluminum alloy
G	Gunmetal
X	Use 'AX' or 'GX' for applications with ambient temperatures –4 to –76 °F (–20 to –60 °C)
Float	
F84	General purpose e.g. high/low alarm, 316 SST
F185	General purpose e.g. high/low alarm, Alloy 400
F96	General purpose e.g. high/low alarm, 316 SST
F98	General purpose e.g. high/low alarm, 316 SST
F104/+	Cranked arm: horizontal or vertical, 316 SST
F106	General purpose e.g. high/low alarm, 316 SST
F107	General purpose e.g. high/low alarm, 316 SST
Typical model number: S 250 D A / F84	

Head Office

Rosemount Measurement Limited
158 Edinburgh Avenue
Slough, Berks., SL1 4UE, UK
+44 (0)1753 756600
+44 (0)1753 823589
Infocentral@Emerson.com

North America Office

Emerson Automation Solutions
6021 Innovation Blvd.
Shakopee, MN 55379, USA
+1 800 999 9307 or +1 952 906 8888
+1 952 949 7001
RFQ.RMD-RCC@Emerson.com

Linkedin.com/company/Emerson-Automation-Solutions

Twitter.com/Rosemount_News

Facebook.com/Rosemount

Youtube.com/user/RosemountMeasurement

Google.com/+RosemountMeasurement

MOBREY

EMERSON