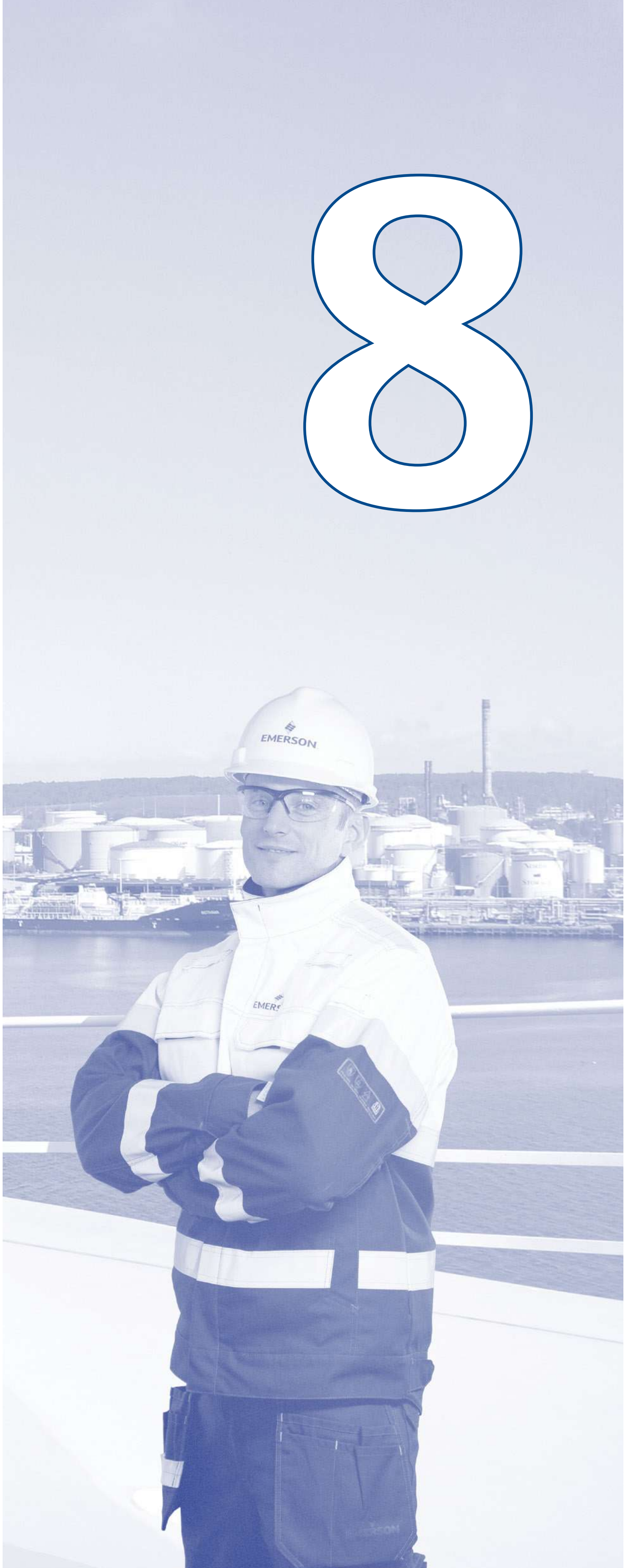


Overfill Prevention System

Topic Page

8. Overfill Prevention System

A multitude of protection layers are required to prevent an overfill from occurring. However, the protection layer most commonly associated with overfill prevention is the safety layer that is usually denoted overfill prevention system (OPS).

OPSs should always be separate and independent of BPCSs, but are present in the following two types: manual overfill prevention system (MOPS) and automatic overfill prevention system (AOPS).

8.1 Manual Overfill Prevention System

MOPS is dependent upon human actions. It usually consists of a level sensor that through an audiovisual alarm notifies an operator, who is expected to take appropriate actions to prevent an overfill, e.g. manually closing a valve, as depicted in figure 8.1.

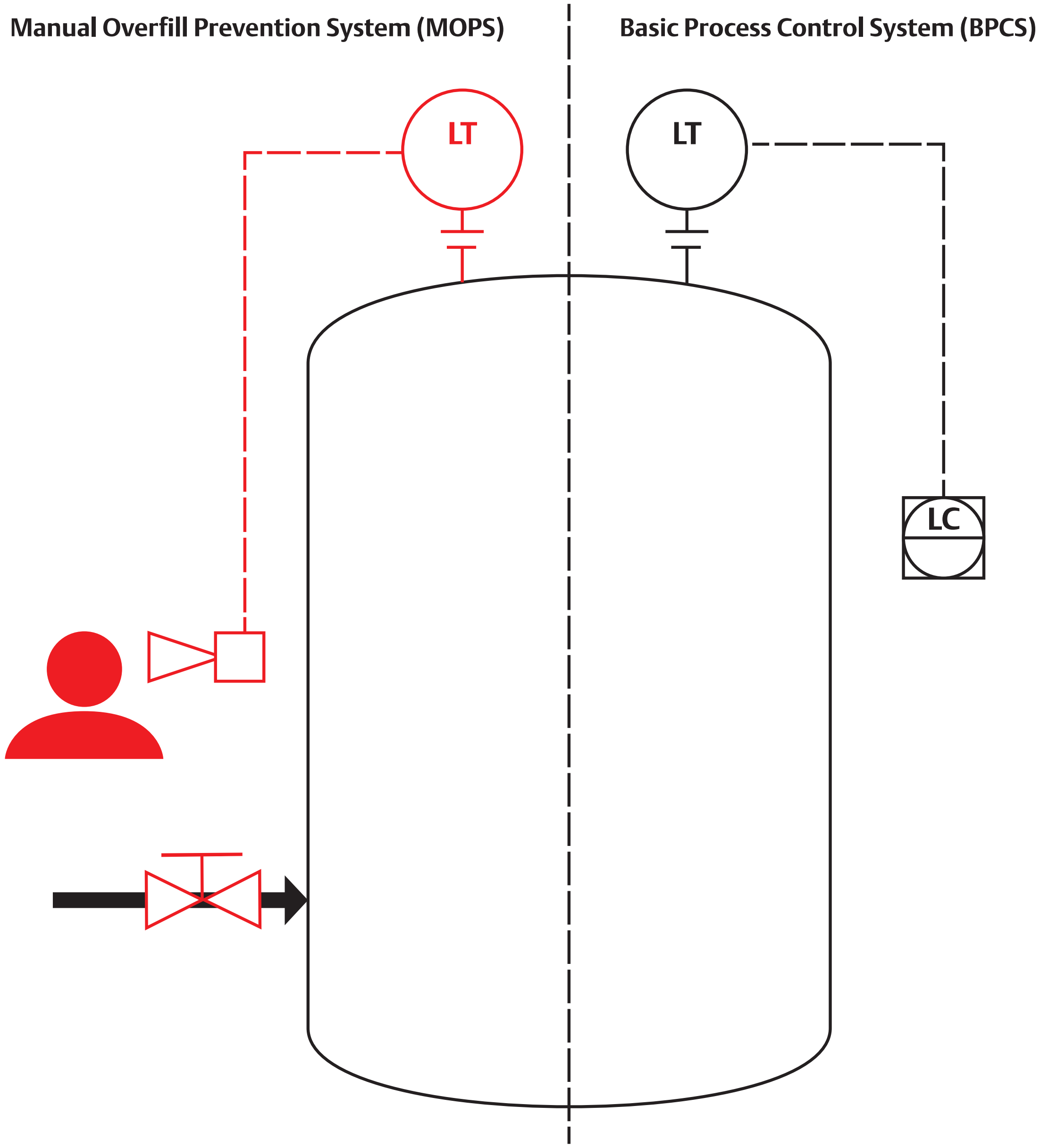


Figure 8.1: MOPS usually consists of a level transmitter (LT) connected to an audiovisual alarm that notifies an operator to take the appropriate action, e.g. closing a valve. API 2350 classification: category #3

8.2 Automatic Overfill Prevention System

AOPS is a safety instrumented function (SIF) and table 8.1 describes when conformance to IEC 61511 is a requirement.

An typical AOPS consists of the principal components illustrated in figure 8.2. It is also common that the AOPS consists of the following non-safety critical functions:

- Notification to operators through both audiovisual and screen alerts
- Actions to protect plant assets such as stopping pumps

Risk Reduction Factor	SIL	Conformance to IEC 61511
>10	1,2,3,4	Required

Table 8.1: AOPS conformance requirements to IEC 61511 according to IEC 61511

Similarly the upgrade of existing OPS is often a gradual process over several years where the sensors, logic-solver and actuators are upgraded in different projects. The existing system may be a MOPS or an AOPS that was designed before the first edition of IEC 61511 was released in 2003. Often the requirements

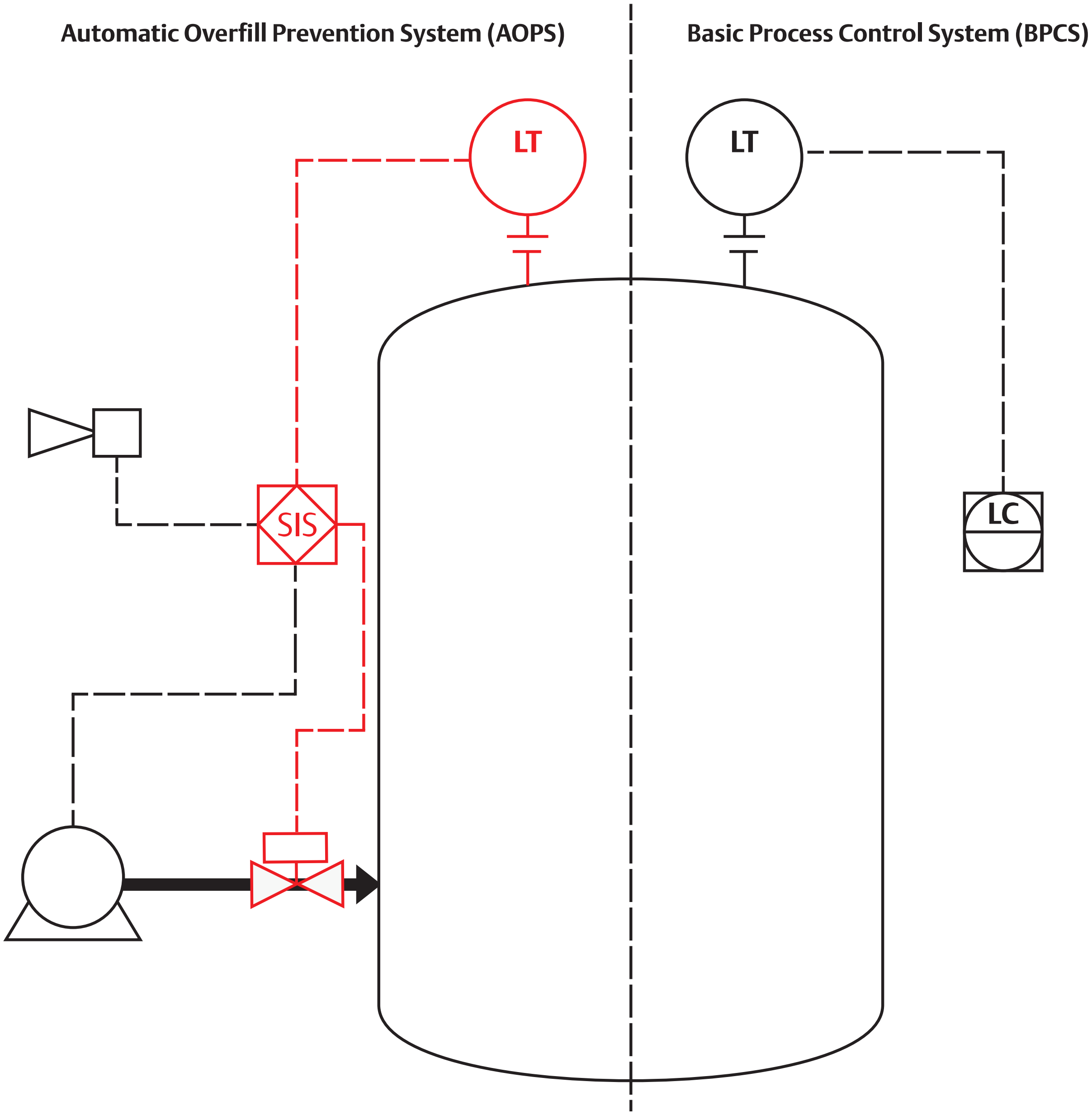


Figure 8.2: AOPS usually consists of a level transmitter (LT), logic and actuator which automatically closes a valve to prevent overfills from occurring. The logic may also execute non-safety critical tasks such as shutting down a pump and notifying the operators through audiovisual alerts. API 2350 classification: category #3

are uncertain. Maybe originally the goal is a risk reduction factor of 10 to 100 (SIL 1) but later evolves to 100 to 1,000 (SIL 2). The future-proof approach to the inherent uncertainty in many OPS projects is to select equipment from the beginning that:

1. Can be used in AOPS conforming to IEC 61511 as described in section “Equipment selection” chapter 5
2. Can be used, or easily upgraded, to meet a higher SIL than currently expected (target = SIL requirement + 1)

Input to the selection of individual components in an OPS can be found in chapter 10 “Equipment selection”.

8.3 AOPS vs. MOPS

MOPS has traditionally been used in some applications because it is easier to implement, has lower initial capital expenditure and less complexity.

However, modern overfill prevention takes preference to AOPS in conformance with IEC 61511 rather than MOPS because:

- Humans are inherently unreliable, and therefore MOPS is limited to a risk reduction factor of 10 according to IEC 61511. AOPS in conformance with IEC 61511 can offer risk reduction factors also above 10
- AOPS can considerably shorten response times compared to MOPS. It is not unusual that a MOPS has a 15 minute response time, whereas an AOPS has below 1 minute
- MOPS requires personnel in the field in potentially unsafe working conditions
- AOPS reduces workload for operators
- IEC 61511 / 61508 offers equipment with accreditation by third party assessors with standardize failure-rate data and safety manuals

8.4 Hardware Fault Tolerance

An AOPS needs to consist of a sensor, a logic solver, and an actuator. However, it is a common practice to add more than one of certain elements within the same AOPS. This is referred to as a system’s Hardware Fault Tolerance (HFT) and can be employed to increase both reliability and availability of an OPS. Hardware Fault Tolerance (HFT) can be employed to both increase the reliability and availability of an OPS as described in the following examples. Figure 8.3 illustrates the most basic setup. A single sensor is connected to a single logic solver that communicates with a single actuator. There are no redundant elements, hence HFT=0. This system is referred to as 1oo1 (1-out-of-1) since each element single-handedly determines the action of the system.

An alternative approach is to add a second actuator as illustrated in figure 8.4. There is 1 redundant actuator, which makes HFT=1 for this setup. It is referred to as 1oo2 (1-out-of-2) since only 1 of the 2 actuators needs to successfully close in order to prevent an overfill. This setup will increase reliability, but decrease the availability.

A third, and increasingly common alternative is to use a configuration of 2oo3 (2-out-of-3) sensors. The MOPS will close the valve when 2 of the 3 sensors agree that it is the proper action to take. With 2 redundant sensors, HFT increases to HFT=2, and in comparison to a 1oo1 configuration, this provides both increased reliability and availability.

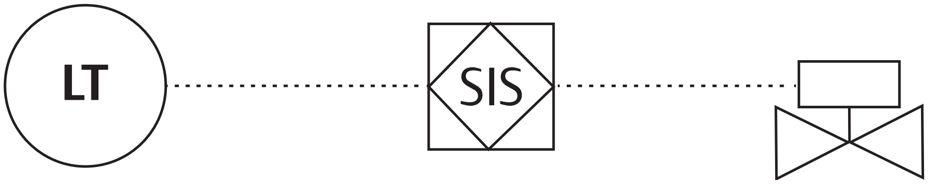


Figure 8.3: OPS consisting of 1oo1 sub-systems (HFT = 0)

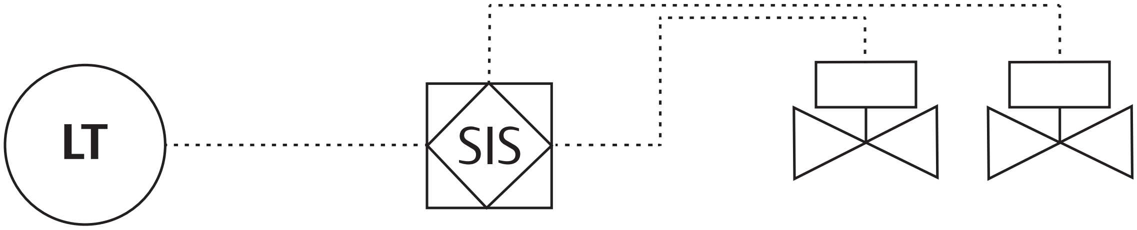


Figure 8.4: OPS consisting of 1oo2 actuators (HFT = 1). This configuration increases the reliability, but decreases the availability, compared to a 1oo1 configuration

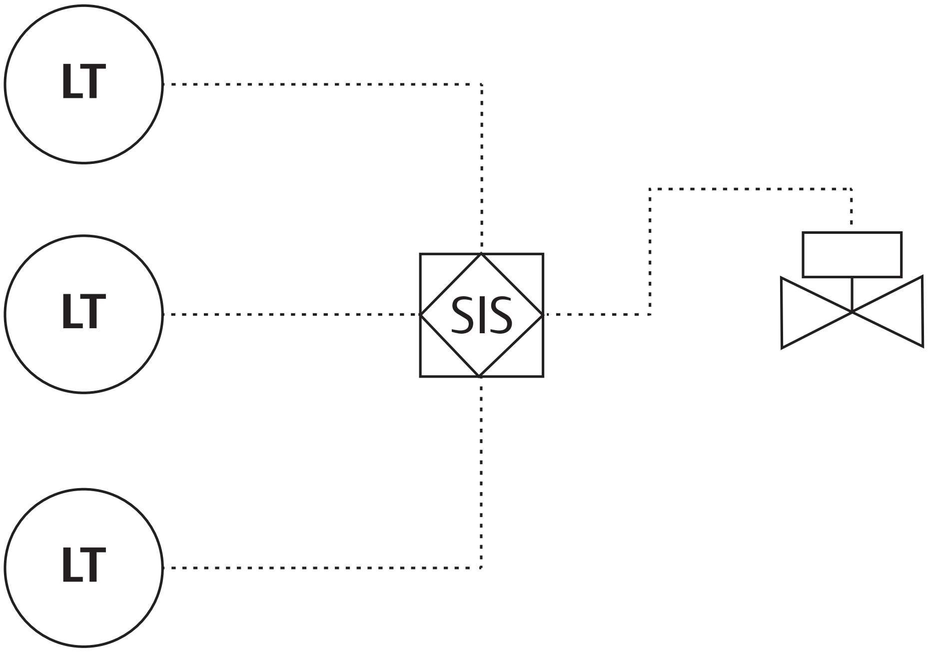


Figure 8.5: OPS consisting of 2oo3 sensors (HFT = 2). This configuration increases both the reliability and availability, compared to a 1oo1 configuration

8.5 Levels of Concern

A critical aspect of overfill prevention is to correctly define the levels of concern (LOC) which include Critical High (CH), Level Alarm High High (LAHH or simply HiHi) and Maximum Working Level (MWL) as depicted in figure 8.6 and described in table 8.2.

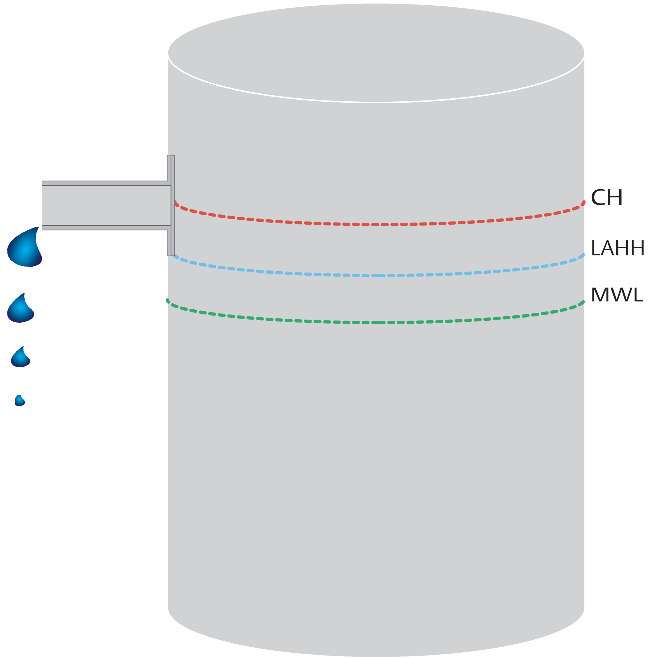


Figure 8.6: The Levels Of Concern (LOC) for tank overfill prevention

According to API 2350 the level alert high (LAH) is not included as a LOC but it may optionally be used for operational purposes. Note the difference in terminology: LAHH is an alarm whereas LAH is an alert. According to API 2350 an alarm is safety critical and requires immediate action whereas alerts are optional non-safety critical notifications.

Determining the LOC is a rigorous process where both internal and external requirements (chapter 5 "Industry standards" and chapter 4 "Regulatory requirements") should be taken into account as well as the performance of the OPS and BPCS.

CH – LAHH = Max level rate x Response time + Safety margin

The location of the LAHH is commonly determined by the following steps:

- The maximum level rate is calculated. Typically based on the maximum flow-rate and the diameter of the tank. Note that the diameter in the tank may vary and this must be taken into consideration
- The response time is determined. This must take the entire OPS into account. More specifically:
  - AOPS: the sum of the worst case response times of the sensor, logic and actuator
  - MOPS: the sum of the worst case response times of the level sensor, notification system and subsequent manual actions. The response time of the manual actions may include the time for the operator to observe the alarm, the time it takes to communicate the alarm to a field operator, time for a field operator to travel to the actuator, and the time it takes to activate the actuator
- The safety margin to be used is defined, which is ultimately a corporate decision
- Finally, LAHH is calculated by the following formula: LAHH = CH - Max level rate x Response time - Safety margin

Changes of the LOC should undergo a management of change process, which is a part of the overfill management system (OMS) described in chapter 7. Consequently, the LOC should not be changed frequently or temporarily due to, for example, operational inconveniences.

Level of Concern (LOC)	Abbreviations	Definition
Critical High Level	CH	The highest level in the tank that product can reach without detrimental impacts (i.e. product overflow or tank damage)
Level Alarm High-High	LAHH	An alarm is generated when the product level reaches the high-high tank level. Note that an alarm is safety critical and requires immediate action (whereas alerts are optional non-safety critical notifications)
Maximum Working Level	MWL	An operational level that is the highest product level to which the tank may routinely be filled during normal operations

Table 8.2: API 2350 definition of The Levels Of Concern (LOC) for tank overfill prevention

9

Proof-Testing

9. Proof-Testing

Safety must always be the top priority for the owners and operators of process plants and tank terminals. To minimize the risk of safety incidents occurring, it is essential for tanks to have in place a robust safety instrumented system (SIS) to prevent overfilling, designed and implemented in compliance with the relevant industry safety standards that will follow the safety life cycle SLC.

The cost to perform proof-tests can be considerable and often exceeds the initial cost of the equipment. It is important to understand the time taken and cost to perform a test, and how frequently tests are required. The device manufacturer should provide a description of the proof-test procedure and the proof-test coverage factor. This enables you to estimate the cost to perform a single proof-test. The proof-test interval, determined either by local regulation or calculated based on the required probabilistic failure rate, will determine the total proof-test cost over the lifecycle of the device.

The purpose of proof-testing is to detect random hardware failures to verify that commissioned equipment already in operation functions correctly. It is executed periodically and thereby differs from the site acceptance test (SAT) which is executed as a part of the commissioning or management of change process to detect systematic (human) errors.

Proof-testing is a useful tool to reduce the probability of failure of infrequently used safety systems. It is associated with the safety layer and not the Basic Process Control System (BPCS) which is always in use and is therefore (at least theoretically) assumed to be continuously verified. The BPCS may need periodic verification but this is typically not denoted proof-testing since the purpose is different (e.g. accuracy verification rather than detecting random hardware failures). In this guide, proof-testing is synonymous with verification of the overfill prevention system (OPS).

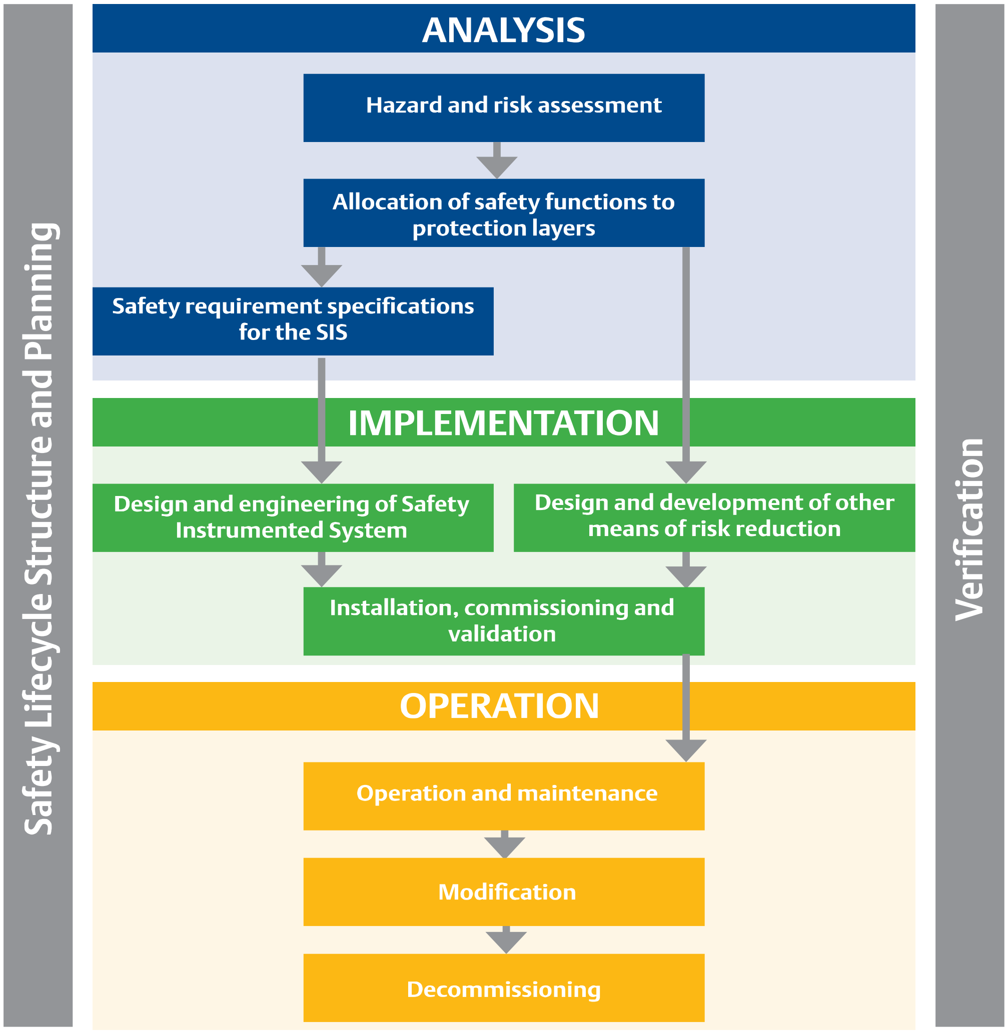


Figure 9.1.1: Management of functional safety

Proof-testing is generic and applies to any type of equipment. It is critical that the entire safety function and associated equipment are included.

At a minimum, there will be a sensor, actuator and a logic solver, but for an OPS, this could be interpreted as level sensors, a PLC, valves, emergency stop buttons, and audiovisual alarms. See figure 9.1.2.

The industry's focus on this particular subject has increased in recent times, mainly due to:

- Ever-increasing need for safety and efficiency improvements
- The introduction of IEC 61511 which emphasizes the safety life-cycle approach (figure 5.4) along with providing a theoretical framework for proof-testing and a quality metric (the coverage factor)
- A number of high profile accidents where lack of proper proof-testing was suspected to be one of the root-causes (e.g. the Buncefield accident)

The trend in the industry is to include proof-testing as a key selection criterion when purchasing equipment, since the cost to execute once the equipment has been commissioned can be considerable. Other important aspects involve personnel and process safety.

9.1 Proof-Testing Requirements

9.1.1 IEC 61511

Proof-testing is an integral part of IEC 61511 with numerous requirements presented throughout the safety life-cycle. The most important ones are listed below. Note that even if the scope of IEC 61511 is the safety critical components of an AOPS, most requirements are equally applicable to a MOPS or non-safety critical equipment used in an AOPS.

According to IEC 61511, basic proof-testing requirements shall already be included in the safety requirements specification (SRS) in the safety life-cycle step "safety requirements specifications for the safety instrumented system" (figure 5.4):

- Internal and external (e.g. functional, regulatory, insurance, company, site specific) requirements and relevant industry standards shall be documented
- It is recommended that the requirements for the desired proof-testing interval are specified. For example, if proof-testing is to be performed only during planned shutdowns (e.g. every 5 years), the design might require additional redundancy compared to where annual proof-

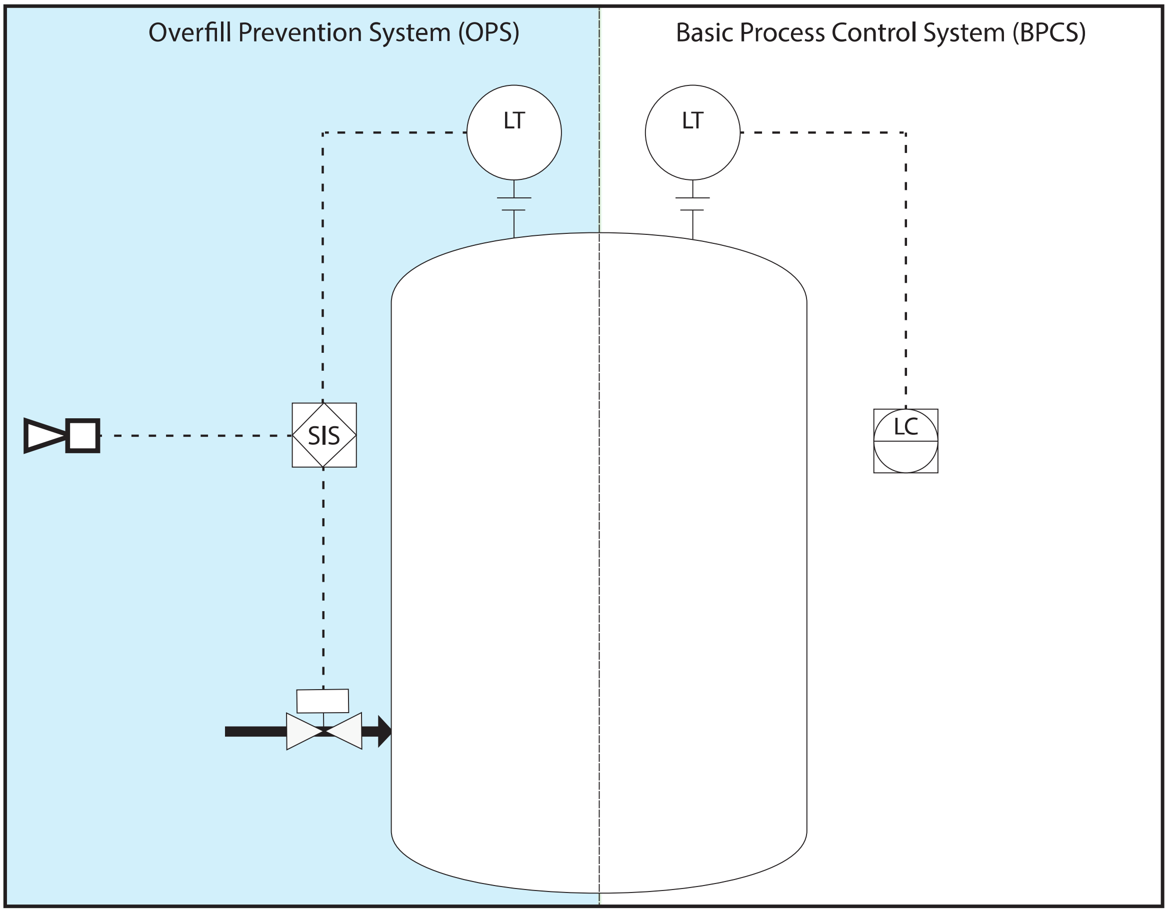


Figure 9.1.2: Proof-testing applies to all components of an overfill prevention system (OPS)

testing is implemented. As a result, the necessary parameters to calculate the proof-test interval also need to be specified

- Any requirements on overrides/inhibits/bypasses shall be documented

Furthermore, the IEC 61511 states that developing the proof-test procedure is an integral part of the design of the safety function. Consequently, the design of the proof-test procedure is not something that should be conducted “after the fact”. The following requirements are applicable for the safety life-cycle step “design and engineering of safety instrumented system” (figure 5.4):

- The proof-test may be carried out either end-to-end or by one element at a time (i.e. sensor, logic-solver, actuator)
- The proof-test procedure shall include overrides/inhibits/bypasses and how they will be cleared and how operators are notified
- Incorrectly performed testing can be dangerous. It is therefore important that the procedures are realistic to prevent deviations during execution, and that both process and personal safety concerns are taken into consideration. Testing personnel often have valuable experience and it is recommended that they are included during the development of the procedures and ultimately approve them. This additionally ensures compliance with current facility specific practices
- Care should be taken with human factors while designing proof-test procedures. For example, change of sensor configuration shall not be required as a part of the procedures and bypass switches shall be protected by key locks or passwords to prevent unauthorized use
- The proof-test procedures shall be properly documented and templates with pass/fail criteria for equipment verification shall be developed. The documentation shall also include instructions for maintaining process safety during the proof-test and behavior on detection of a fault
- Proof-test interval shall be calculated and documented

IEC 61511 also specifies proof-test requirements for the safety life-cycle step “operation and maintenance” (figure 5.4):

- Proof-testing can be dangerous. Immediate safety concerns can arise, or the safety function may be forgotten in an inoperable state. It is therefore critical that the proof-test is performed by qualified personnel who are properly trained and execute the procedure exactly according to the instructions, without any deviations
- The user shall maintain records that certify that proof-tests and inspections were completed as required. These records shall include the following information as a minimum:
    - o Description of the tests and inspections performed
    - o Dates of the tests and inspections
    - o Name of the person(s) who performed the tests and inspections
    - o Serial number or other unique identifier of the system tested
    - o Results of the tests and inspection

9.1.2 API 2350

API 2350 provides requirements for testing of overfill prevention systems which are equally applicable to both MOPS and AOPS. The requirements are similar to those found in IEC 61511, although targeted specifically towards the bulk liquid industry. The most important requirements are:

- Proof-test procedures shall be documented and schedules for periodic proof-testing shall be established
- Proof-test records shall be maintained for at least three years
- The personnel executing the proof-testing shall be competent. The facility is responsible for assigning dedicated personnel and providing appropriate training

9. 2 Proof-Test Interval

There are two basic methods for the determination of a proof-test interval:

- Prescriptive method with predetermined interval
- Analytical method based on equipment reliability and required risk reduction

The traditional approach is to use a predetermined interval which may result in an over or under engineered solution. The modern approach therefore uses the analytical method to calculate an interval appropriate for the specific safety function.

In practice, a number of factors based on internal and external requirements must be taken into account when determining the proof-test interval. The remainder of this section describes the requirements according to IEC 61511 and API 2350.

9.2.1 IEC 61511

According to the IEC 61511 methodology, the most important factors affecting the proof-test interval are:

- The safety functions risk reduction factor (RRF)
- The reliability of the device (λ_{DU})
- Proof-test effectiveness (coverage factor) and existence of partial proof-testing
- Mission time, i.e. the time from a system's start-up until its replacement or refurbishment to as-new condition

9.2.1.1 The Bathtub Curve

IEC 61511 provides a theoretical framework for the calculation of the proof-test interval. An important fundamental assumption for that framework is that the random hardware failure rate of a level sensor is constant during its useful lifetime. This is often referenced as the middle section of a so-called bathtub curve. The bathtub curve is a widely used model in reliability engineering and a more detailed explanation is provided in figure 9.2.

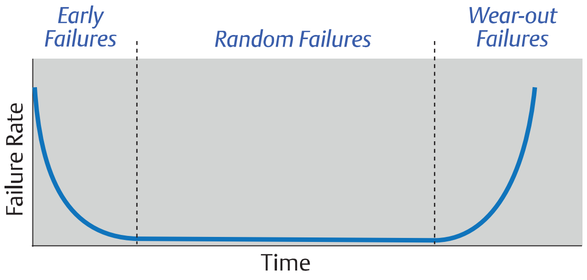


Figure 9.2: The bathtub curve

9.2.1.2 What is the Proof-test definition?

Proof-testing is defined in IEC 61508 as a 'Periodic test performed to detect dangerous hidden failures in a safety-related system so that, if necessary, a repair can restore the system to an "as new" condition or as close as practical to this condition'. In simple terms, a proof test is designed to reveal all the 'undetected/unrevealed' failures which the device may be harbouring unbeknown to anyone.

9.2.1.3 Why do proof-testing?

Testing of safety system components to detect any failures not detected by automatic on-line diagnostics i.e. dangerous failures, diagnostic failures, parametric failures is followed by repair of those failures to an equivalent as- new state. Proof-testing is a vital part of the safety lifecycle and is critical to ensuring that a system achieves its required SIL throughout the safety lifecycle.

The FMEDA analysis considers the failure rate of individual components. Failures that must be detected, depending on what SFF The ratio of safe failures and dangerous detected failures to total failures must be achieved by testing to find safe detected, safe undetected, dangerous detected, dangerous undetected failures for each component. Built-in diagnostics which can change dangerous undetected failures to dangerous detected failures.

9.2.1.4 Probability of Failure on Demand

According to IEC 61511, the proof-test interval shall be calculated based on the average probability of failure on demand, denoted PFD_{avg}, during the time that the safety function is in operation (mission time). For instance, an overfill prevention system with a high PFDavg runs a high risk of failing to close a shutdown valve in an event of excessive tank levels, whereas an overfill prevention system with low PFDavg is more reliable. The PFD_{avg} value needs to match the required risk reduction factor as described in table 9.1.

SIL	RRF	PFD_{avg}
1	10-100	0.1-0.01
2	100-1,000	0.01-0.001
3	1,000-10,000	0.001-0.0001
4	10,000-100,000	0.0001-0.00001

Table 9.1: Risk reduction factors (RRF) and average probability of failure on demand (PFD_{avg}) segmented by safety integrity levels(SIL)

Calculating PFD_{avg} involves a multitude of factors. Software packages exist with complex models but IEC 61508-6 provides approximate simplified formulas. Assuming non-redundant configurations (1oo1) where λ_{DU} is the safety function's dangerous undetected failure rate and T is the time interval:

$$PFD \approx \lambda_{DU} * T$$

$$PFD_{avg} \approx \lambda_{DU} * T / 2$$

The risk reduction factor (RRF) can be calculated in the following way:

$$RRF = 1/PFD_{avg}$$

Example: Calculation of PFD and PFD$_{avg}$ Using IEC 61508-6 Simplified Formulas

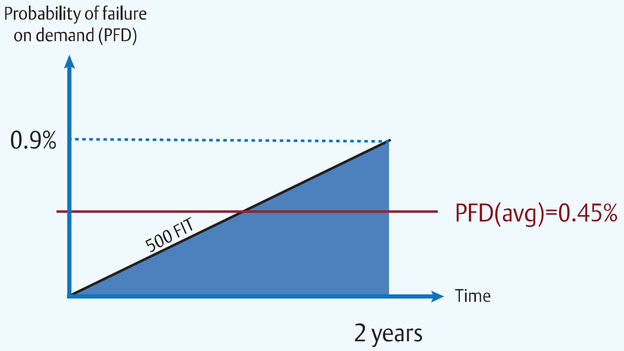
An automatic overfill prevention system has a total failure rate of λ_{DU}= 500 FIT = 500 [1/10^9 hours]. The probability of failure on demand at T=2 years approximately equals:

$$PFD \approx (500/10^9) \times (2 \times 365 \times 24) = 0.9\ \%.$$

The average probability of failure on demand during this period was:

$$PFD_{avg} \approx 0.9\% / 2 = 0.45\%.$$

This corresponds to a risk reduction factor of RRF=1/0.45%=220 which lies in the SIL 2 range.



Example 9.1: Calculation of PFD and PFD$_{avg}$ using IEC 61508-6 simplified formulas

9.2.1.5 How is Proof-Testing Performed?

Proof-testing is performed to check the functionality of devices implemented within a safety loop and is mandatory to be compliant with international safety standards. Dangerous undetected failures (DU), which are those failures not identified by device diagnostics, must be considered when designing the safety loop. The regularity of proof-tests is based on the safety integrity level of the safety loop and probability of a device failure (PFD). To ensure a device continues to achieve its required SIL, the PFD, which increases over time, can be reduced to almost its original level by performing comprehensive proof-testing. For devices with a low DU, this can be achieved with partial proof tests, which can be performed remotely and are far less time-consuming than comprehensive testing.

9.2.1.6 What is Proof-Test Coverage?

The diagnostic coverage combined with proof-testing determines the percentage of dangerous failures that can be detected for a device. Proof-test coverage is a measure of how many undetected dangerous failures, not identified by a device's diagnostics, that can be detected by the proof test.

9.2.1.7 Does Diagnostic Coverage Affect the Proof-Test Coverage?

The effectiveness of a proof-test in finding the DUs is known as the proof-test coverage (PTC) factor, and this should be as high as possible. PTC can be defined as the fraction of dangerous, undetected failures that can be detected by a user proof-test and is normally expressed as a percentage. In the past, it was commonly assumed that proof-test coverage was 100%. However, not all proof-tests are comprehensive, and approval agencies often indicate that the recommended proof-test does not have a 100% PTC.

9.2.1.8 Do I Still Need to Perform a Comprehensive Proof-Test?

Partial proof-tests do not replace comprehensive tests – they complement them. As a partial test only detects a percentage of potential failures, a comprehensive test must eventually be carried out after a given time interval to return the instrument close to its original PFD.

9.2.1.9 Proof-Test Coverage Factor

In practice, proof-tests are not 100% effective. The effectiveness of a proof-test is described using the coverage factor which specifies the share of detected dangerous undetected failures (λ_{DU}). The effect of an imperfect proof-test procedure (coverage less than 100%) is visualized in figure 9.3.

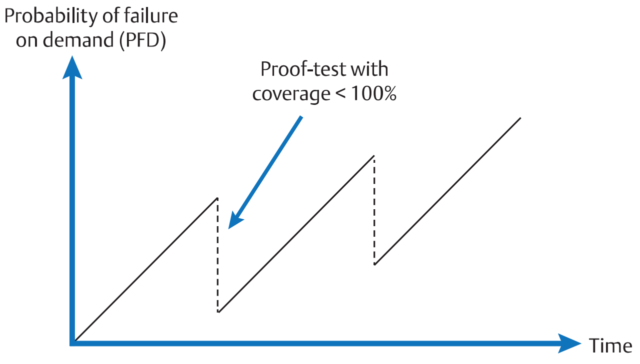


Figure 9.3: The repetitive effect on the probability of failure on demand caused by an imperfect proof-test procedure

In case the proof-test interval is an even multiplier of the mission time, the following simplified formula can be used to calculate the approximate average probability of failure:

$$PFD_{avg} \approx \lambda_{DU} * (1\text{-coverage factor}) * T_{\text{mission time}} / 2 + \lambda_{DU} * (\text{coverage factor}) * T_{\text{proof-test interval}} / 2$$

Considering that the coverage factor is an indication of a proof-test's effectiveness to detect dangerous undetected faults, it is a useful metric for a qualitative assessment of proof test quality.

There are three common SIF designs: simplex, duplex or triplex. Simplex or 1oo1 (1 out of 1) voting principle involves a single safety loop, and is normally designed for low level safety applications. The main disadvantage of a system with only a single safety loop, and no redundancy, is that should a safety loop fail, this immediately leads to a trip, resulting in the loss of the safety function or shutdown of the process.

Probability of Failure on Demand (PFD) is the risk of a device or SIF failing to perform its safety function when required. PFD_{avg} for low, high and continuous modes of operation are used to describe the functions performed by safety systems. The modes are relevant when relating the target failure measure of a safety function to be implemented by a safety system to the SIL.

9.2.1.10 Combining a Safety Function's Sub-Systems

Assuming that a safety function's components are independent, its total failure rate may simply be calculated as the sum of each component.

$$\lambda_{DU}=\lambda_{DU}^{Sensor}+\lambda_{DU}^{Logic}+\lambda_{DU}^{Actuator}$$

Consequently, the total average probability of failure on demand can be calculated by adding the PFD_{avg} values for each component.

$$PFD_{avg}=PFD_{avg}^{Sensor}+PFD_{avg}^{Logic}+PFD_{avg}^{Actuator}$$

This is critical as it is the total safety function's PFD_{avg} that determines the actual proof testing interval. It is however still useful to obtain an indicative figure of the requirements on the different components. One reason is that each component may be proof-tested at different intervals. Another is that the system's requirement can be broken down by suggested guidelines for each component. A commonly used model that provides guidelines on the suitable split of a system's PFD_{avg} between its components is shown in figure 9.5.

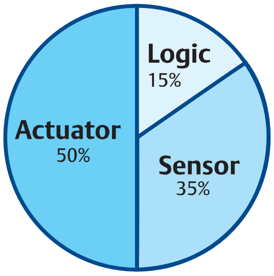


Figure 9.4: Commonly used model to estimate the approximate PFD_{avg} requirements for the different sub-systems in a safety function

Example Calculation: Estimating the Proof-Test Interval for a Level Sensor

A level sensor is evaluated for usage in a safety function that is required to provide a risk reduction of 200 (SIL 2). The mission time is 9 years and the specified minimum test interval is 3 years. According to the data sheet, the level sensor has a failure rate λ_{DU}= 80 FIT the proof-test coverage is 80%. Should this level sensor be considered as a potential candidate for this safety function?

According to the formulas provided in this section, the sensor's $PFD_{avg} \approx (80/10^9)x(1-80\%)x(9 \times 365 \times 24) / 2 + (80/10^9)x(80\%)x(3 \times 365 \times 24) / 2 = 0.15\%$.

According to the standard model, the sensor is allowed to contribute PFDavg = 35% x PFDavg = 35%x 1/200 = 0.18%.

Since the approximate average probability of failure on demand is lower than what can typically be assumed for a level sensor in this application (0.15% < 0.18%) the answer is yes, this sensor is a potential candidate for this safety function.

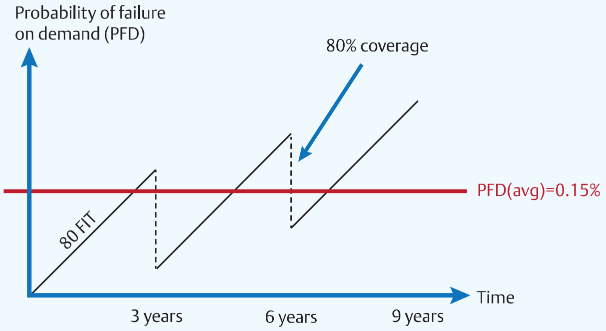


Figure 9.5: Visualization of example PFD and PFD_{avg} calculation

Example 9.2: Estimating the proof-test interval for a safety function's sensor

9.2.1.11 Comprehensive and Partial Proof-Testing

Proof-testing has traditionally affected tank operations and thereby caused down-time. This problem has been especially prominent in continuous processes, where it may not have been possible to close a valve and thereby shut down the flow of incoming or outgoing product. The solution in this case has been bypass pipes as depicted in figure 9.6, but the proof-test procedure becomes very

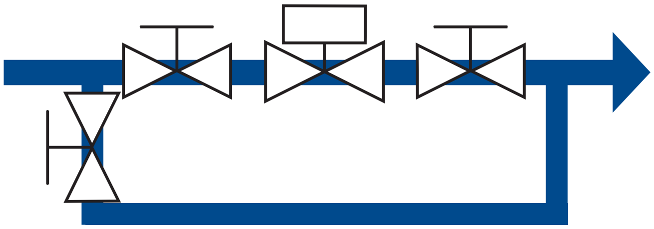


Figure 9.6: Principal overview bypass pipe used for actuator and valve testing

cumbersome with the risk of forgetting manual valves. Based on this background, actuator and valve manufacturers developed methodologies that only close valves partially, thereby minimizing the effect on the process. The rationale is that one of the most frequent failure modes of a valve is that it gets completely stuck, e.g. due to rust. This type of test also, to some extent, verifies the actuator and its connections. Although there is no definition for partial testing, this has been the industry terminology for this type of testing. The opposite is usually denoted comprehensive testing, in this case implying that the valve is entirely closed during the proof-test.

More recently a similar principle has been applied to sensors. The rationale can be understood by segmenting the sensor into functional elements as depicted in figure 9.7; Output circuitry, Measurement electronics, and Sensing element.

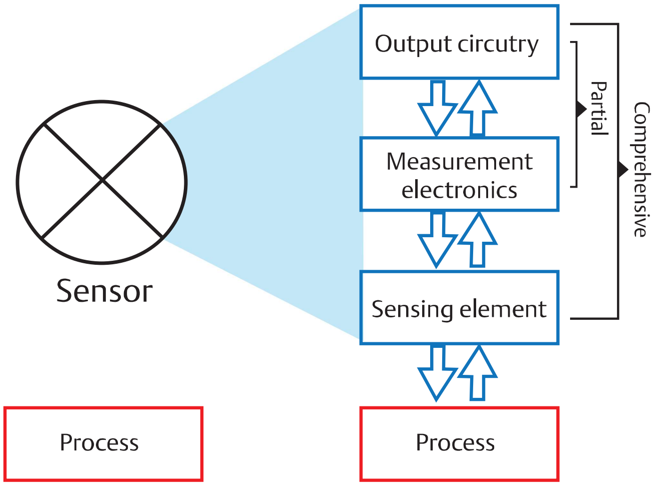


Figure 9.7: Sensor segmented into the functional elements Output circuitry, Measurement electronics, and Sensing element

For sensors, the scope of comprehensive proof-testing includes all of the elements described in figure 9.7, whereas the scope of partial proof-testing is limited to only one or a few elements (but not all). This could be exemplified with testing the analog output signal of a pressure transmitter. This would be partial proof-testing as it does not verify the integrity of the process seal.

Usually, partial proof-tests are used to extend the time interval of the comprehensive proof-test. Mathematically, the partial proof-test has a lower coverage factor than the comprehensive proof-test. The principal effect on the probability of failure on demand is depicted in figure 9.8.

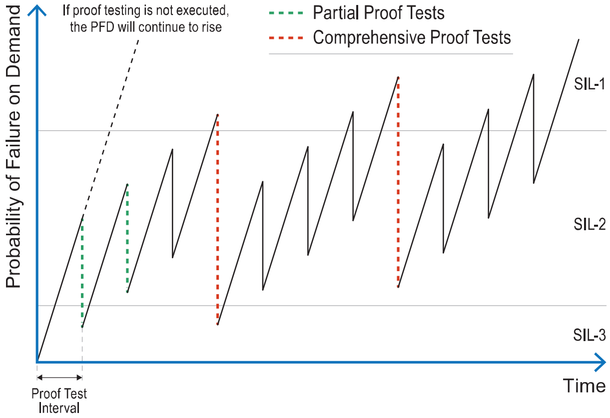


Figure 9.8: Test coverage of partial and comprehensive proof-testing

Although partial proof-test, which is usually performed remotely, is useful to extend the time interval of the comprehensive proof-test, it is important not to forget the need for visual inspection.

9.2.2 API 2350

API 2350 contains a mixed approach to proof-testing interval with a prescriptive number specified in conjunction with the alternative of using a performance based approach (in practice this means according to the IEC 61511 approach described above).

For the prescriptive numbers, API 2350 specifies that:

- Point-level sensors shall be proof-tested every six months
- All other equipment in the overfill prevention system shall be proof-tested every 12 months

The type of testing (i.e. partial or comprehensive) that should be conducted at these time intervals is not specified.

9.3 The Traditional Approach to Overfill Prevention

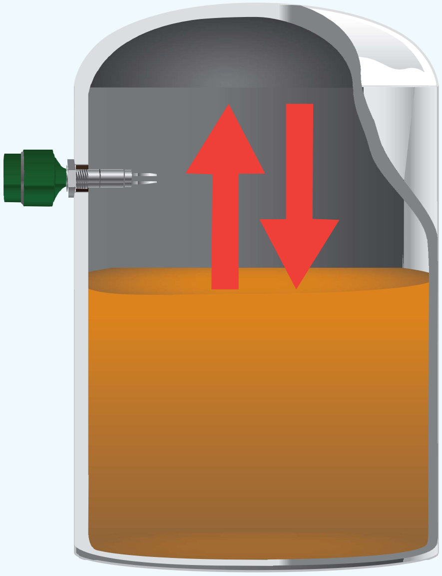
Proof-testing has attracted little attention in the traditional approach to overfill prevention (described in chapter 3 “Key Elements”). Test effectiveness has often been low and the test intervals have often not been determined analytically. The personnel’s trust in the tests has been low and execution has therefore not been stringent and often close to random. The often non-documented procedures have been cumbersome and in some cases dangerous and resulted in considerable downtime. Documented evidence that the proof-test has been executed correctly is often incomplete or non-existing.

9.3.1 Traditional Proof-Testing Procedures Exemplified with Point Level Sensors

Although the trend is towards using continuous level sensors for safety critical measurements, point-level sensors have been traditionally used for these types of applications. Over the years, equipment manufacturers, system integrators and users have developed several different proof-testing procedures, which can broadly be separated into the categories listed below and overleaf.

Live Simulation of Alarm Condition

An intuitive proof-testing method is to raise and lower the actual product level to verify that the level sensor's output signal functions as expected. Although this may appear to be straightforward, in practice this method is time-consuming and, more importantly, it exposes the tank to a dangerous condition. According to API 2350 this type of proof-testing method should be avoided.



Test Buttons and Remote Proof-Testing

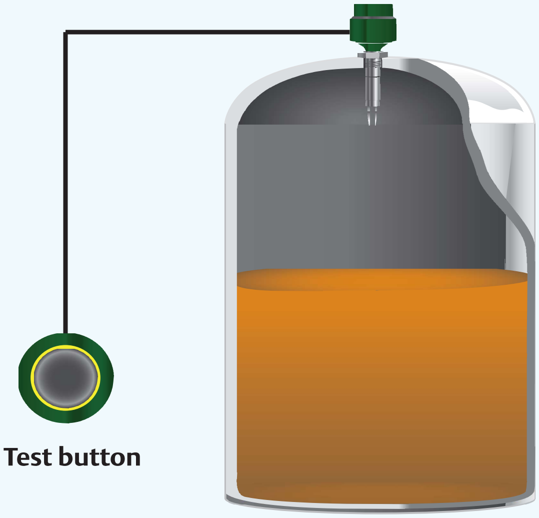
Versions of the test lever principle have also been designed for electronic point level sensors, often implemented as a local test button inside the level sensor's enclosure. This can be performed in-situ but requires an enclosure cover to be removed, which is a potential risk. Therefore, some designs feature a magnet, which do not require the cover to be removed.

Designs also exist that incorporate remote test buttons. These, however, add components with additional failure modes that reduce the overall equipment reliability. Additionally, the transmitter is not visually inspected.

Some of the newest generation of electronic point level sensors incorporate an integrated remote proof test which reduces system complexity and potential failure modes. The proof test is activated by sending a command from the control room host to the device.

Due to their nature, remote proof tests only perform a partial proof-test (e.g. they may test the output relay only or certain parts of the electronics). The primary usage is, therefore, as a complement to the comprehensive proof-test procedures that verify all parts of the level sensor including the sensing element (e.g. through a bucket test).

In order to assess the value, relevance and effectiveness of test buttons, it is critical to have both a qualitative understanding of what failure modes are covered, as well as a quantitative coverage factor.

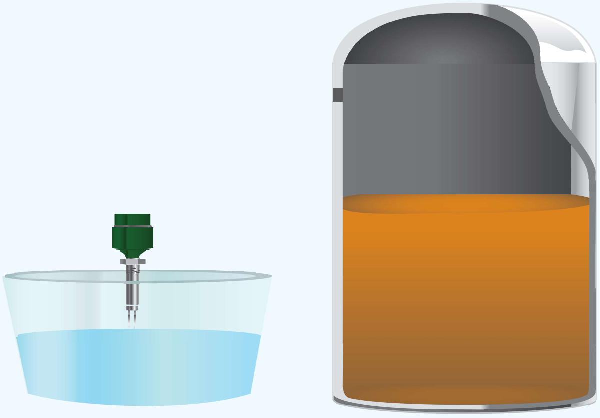


Bucket Testing

Another traditional proof-testing method is to dismount the point level sensor and expose it to the alarm condition. In practice, this is often performed by inserting the device into a bucket filled with product. This method requires a visit to the tank and access to the level sensor while the tank is temporarily taken out of operation. The procedure may be a direct safety concern to the personnel executing the test since it both exposes the tank to the atmosphere and the bucket contents may be hazardous. Additional precautions must be taken if it is a pressurized tank or an explosive environment. Ideally, the product in the bucket should be the same as in the tank, but for safety reasons, water is often used.

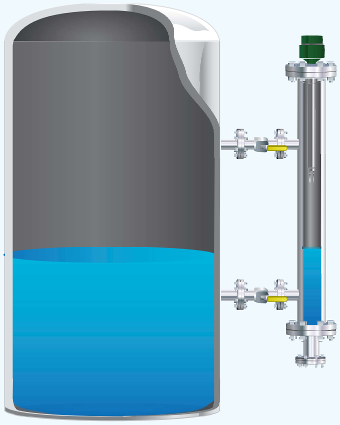
When the test is not performed with the media to be measured, there is an obvious risk that test results become irrelevant for the true process conditions. Furthermore, when sensors are dismounted, there is no guarantee that re-commissioning is correctly executed. There may be cable glitches, gaskets missing, loose bolts or even damage imposed to the sensor itself.

One advantage with this type of testing however, is that it allows for visual inspection of the sensor's wetted parts. For example indications of corrosion or material incompatibility may be used as input for predictive maintenance.



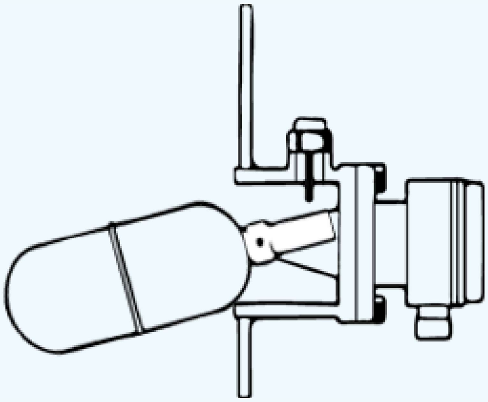
Test Chambers

An alternative to live simulation is to mount the level sensor inside a chamber that can be mechanically isolated from the tank. By the usage of external connections, the chamber can be filled and drained with product (ideally the same as in the tank), thereby simulating an alarm condition. This method shares many of the drawbacks of bucket testing since it exposes atmosphere and personnel to the product inside the tank. Additionally, these chambers are often inaccessible and there is a risk that the mechanical by-pass is not restored correctly, rendering the measurement inoperable.



Test Levers

To eliminate problems relating to dismounting and isolation of the level sensor, various types of in-situ ("in place") proof-testing methods have been developed. The most frequent principle is the usage of test levers that mechanically simulate the alarm condition. Although the levers may be spring loaded and originally designed to fail safe, empirical evidence has shown this is often not the case. Leaks, corrosion, intermediate positions, or improper handling by personnel may result in dangerous failure modes. This was believed to be one of the root-causes of the Buncefield accident.



9.4 The Modern Approach to Proof-Testing

9.4.1. Benefits

Modern equipment provides benefits when compared to the traditional solutions from both a safety and an efficiency perspective.

The benefits of a modern approach also include safety improvements:

- Higher test effectiveness (coverage factor) results in increased reliability of the safety function
- Increased safety for the personnel executing the tests
- Minimal impact on process safety during the tests
- Reduced risk of leaving the tested device inoperable
- Simultaneous verification of the level sensor used in the basic process control system (BPCS)

Efficiency Improvements

- Labor savings through more efficient procedures and longer test intervals
- Reduction in tank down-time and minimized process impact
- Simplified documentation and auditing
- Reduced engineering time to develop the bypass, test and restoration procedures

As an example, a proof-test procedure for a traditional point level measurement is likely to require approximately four hours to complete and should, according to API 2350, be completed twice a year. Over a safety function's lifetime of 10 years, direct labor costs would accumulate to approximately $8,000. In comparison, proof-test completion of the modern approach utilizing a continuous level measurement may be reduced to 30 minutes and is only required once every year. That corresponds to labour costs of only $500. This simplified and conservative estimation shows potential savings of $7,500, which easily provides financial justification to invest in equipment with modern proof-testing capabilities. Note that this does not include additional improvements in terms of safety and reduced downtime. See detailed calculation steps below.

Proof-testing point level measurement: 4 hours x 2 tests/year x 10 years x $100/hour = $8000

Proof-testing continuous level measurement: 0.5 hours x 1 tests/year x 10 years x $100/hour = $500

Proof-Testing Case: LA Refinery

This Latin American refinery has a tank farm consisting of 300 tanks. Currently, there is a work force of 15 employees assigned full time for monthly testing of each tank's manual overfill prevention system, which mainly consists of a mechanical level switch. Hence, each employee proof-tests 20 tanks each month, which corresponds to 8 man-hours per tank and month.

With modern proof-testing procedures, the completion time may be reduced to 30 minutes once every year, corresponding to only 150 man-hours required for a full year's proof-testing of the entire tank farm. Consequently, the potential efficiency improvement is almost 15 full-time jobs.

Picture 9.1: Refinery

Case 9.1: Proof-testing case: LA Refinery

9.5 Implications

Proof-testing has become an increasingly important feature and is now one of the key selection criteria when selecting equipment for modern overfill prevention systems. Some of the relevant features are:

- Is the proof-test procedure properly described?
- Are both comprehensive and partial proof-tests available?
- Has the proof-test been assessed by an accredited 3rd party?
- Is the proof-test IEC 61508 certified?
- Quantitative justification:
    - Is the effectiveness (coverage factor) specified?
    - Is the failure-rate (λ) specified?
    - Is the equipment's useful life-time specified?
- Qualitative justification: Is there an acceptable description of why the equipment is adequately tested using the proposed procedure?
- Man-hours to complete the test?
- Safety concerns for the personnel executing the test?
- Requirements for process alterations (e.g. tank level movement)?
- Expected downtime?
- Templates for proof-testing records?
- What overrides/inhibits/bypasses are required?
- Tools required to execute the proof-test?
- Is there a possibility to forget the proof-test in an unsafe state?

Detailed selection criteria is provided in chapter 10 "Equipment selection".

Proof-Testing Radar Level Sensors: Latest Advancements

Selected radar level sensors designed specifically for SIS and certified according to IEC 61508 offer comprehensive proof-testing functionality such as:

- Documented procedure with coverage factor above 90%
- The proof-test can be completed remotely within a few minutes without altering the level
- Software package with wizards that guide the user and upon completion generate a proof-test record compliant with IEC 61511 and API 2350
- Theoretical proof-test intervals exceeding 10 years (SIL 2)

Qualitatively, the principal proof-test procedure is described in table 11.2.

Sensor Elements	Proof-Test Procedure
Output circuitry	Relay or analog signal altered
Measurement electronics	Comparison of level reading with secondary measurement (i.e. BPCS level sensor)
Antenna	Verification that measurement signal has not degraded significantly and that it is acceptable

Table 9.2: Description of selected radar level sensors' proof-test procedure segmented by its major components

A radar level sensor functions principally as a laser pointer; an electromagnetic wave is transmitted and received. Therefore, there is no need to test the sensor at the specific set-point (LAHH) as long as the product in the tank is further away (lower level) since it does not provide any additional coverage of dangerous undetected failures.

The measurement electronics can be continuously proof-tested by implementing level deviation checks between the BPCS- and OPS level sensors.

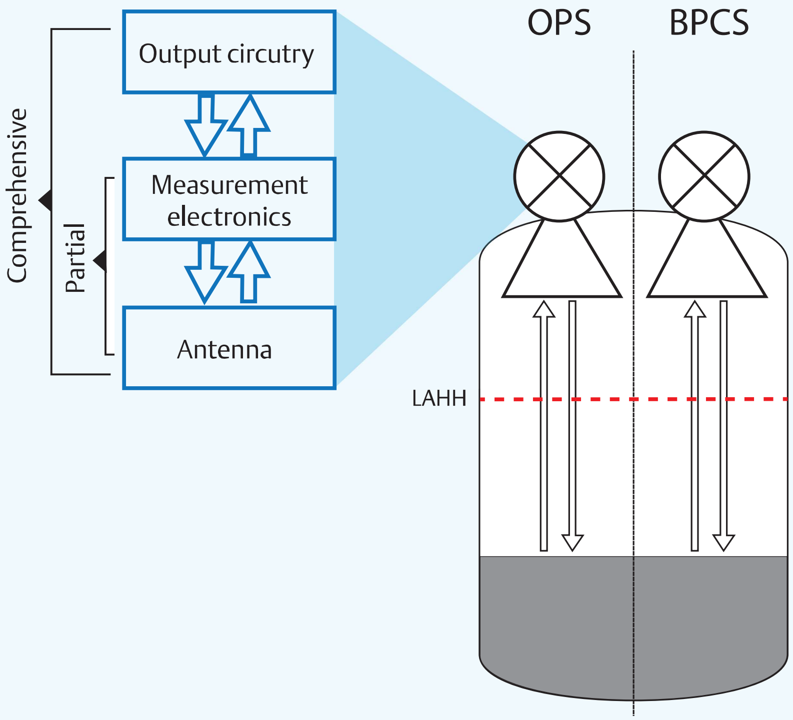


Figure 9.10: Example of better proof-testing methods with modern overfill prevention equipment

Outlook box 9.1: Proof-testing radar level sensors: Latest advancements

Proof-Testing in Rosemount TankMaster™

TankMaster has a built in proof test wizard which allows operators to perform proof test of Rosemount Tank Gauging overfill prevention systems safely, and remotely from the control room.

You may combine continuous product level monitoring with proof testing at regular intervals.

A step-by-step guide helps you to perform one or several comprehensive or partial proof tests. A detailed proof test report is automatically generated for each proof test and stored. The software also offers proof test history records, scheduling, customized checklists and more.

Comprehensive Proof Test

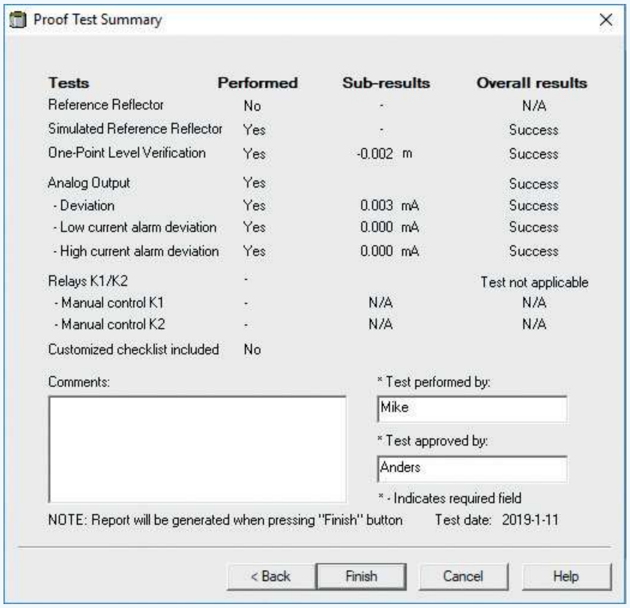
- High level alarm verification using a reference reflector

Partial Proof Test

- High level alarm verification with simulated reference reflector
- One-point level verification by comparing with a secondary level measurement
- Analog output verification
- Relay output verification

Multiple tests can be performed in a sequence in order to achieve required proof test coverage. You may for example do a High-Level Alarm test with a reference reflector, followed by a test of the analog outputs of a connected tank hub.

A detailed proof test summary and proof test report is automatically generated for each proof test performed. The proof test report includes device specific information for identification of which devices that has been tested, detailed results of each proof test as well as who performed and approved the tests.



Tests	Performed	Sub-results	Overall results
Reference Reflector	No	-	N/A
Simulated Reference Reflector	Yes	-	Success
One-Point Level Verification	Yes	-0.002 m	Success
Analog Output	Yes		Success
- Deviation	Yes	0.003 mA	Success
- Low current alarm deviation	Yes	0.000 mA	Success
- High current alarm deviation	Yes	0.000 mA	Success
Relays K1/K2	-		Test not applicable
- Manual control K1	-	N/A	N/A
- Manual control K2	-	N/A	N/A
Customized checklist included	No		

Comments:

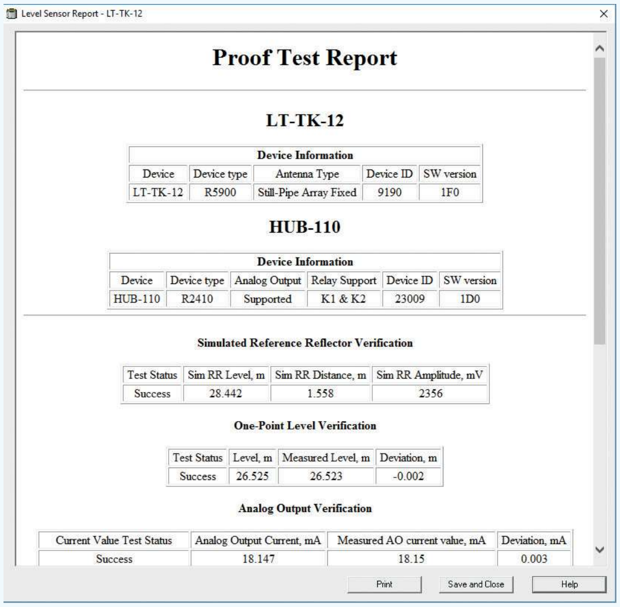
* Test performed by: Mike

* Test approved by: Anders

* - Indicates required field

NOTE: Report will be generated when pressing "Finish" button

Test date: 2019-1-11



Proof Test Report

LT-TK-12

Device Information				
Device	Device type	Antenna Type	Device ID	SW version
LT-TK-12	R5900	Still-Pipe Array Fixed	9190	1F0

HUB-110

Device Information					
Device	Device type	Analog Output	Relay Support	Device ID	SW version
HUB-110	R2410	Supported	K1 & K2	23009	1D0

Simulated Reference Reflector Verification

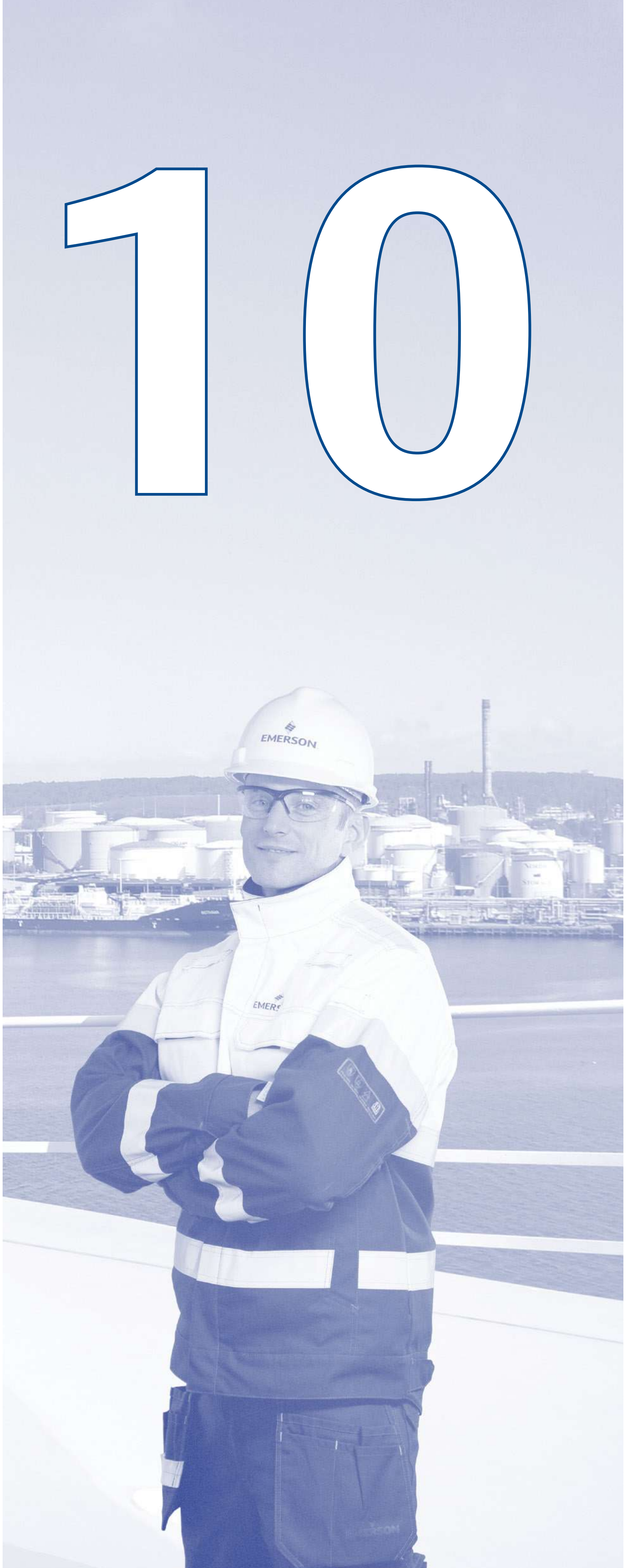
Test Status	Sim RR Level, m	Sim RR Distance, m	Sim RR Amplitude, mV
Success	28.442	1.558	2356

One-Point Level Verification

Test Status	Level, m	Measured Level, m	Deviation, m
Success	26.525	26.523	-0.002

Analog Output Verification

Current Value Test Status	Analog Output Current, mA	Measured AO current value, mA	Deviation, mA
Success	18.147	18.15	0.003



10

Available Technologies

Topic Page

10. Available Technologies

With overfill prevention solutions, there is no one size fits all technology and system. Different applications have their own specific challenges and it is important to select the appropriate technologies to meet these. The level sensor is the specific element of the OPS and offers several alternatives. A range of level monitoring and measurement technologies can be applied, from simple electro-mechanical float and displacer switches through to advanced modern solutions, including vibrating fork switches, guided wave radar and non-contacting radar. Finding the technology that best fits a specific application requires good knowledge of the technology itself as well as the application, and it is important to choose the most suitable technology that will result in the highest possible safety for your plant. Below is brief description of the basic principles, together with some of the advantages and limitations regarding common modern technologies.

10.1 Vibrating Forks

Vibrating fork switches (figure 10.1) are used for point level detection and operate using the concept of a tuning fork. Two tines are immersed into the process vessel and an internal piezo-electric crystal oscillates these tines at their natural frequency. This frequency varies as the tines are immersed in the medium. Any changes are detected by the electronics, providing an effective means of detecting the presence or absence of liquids.

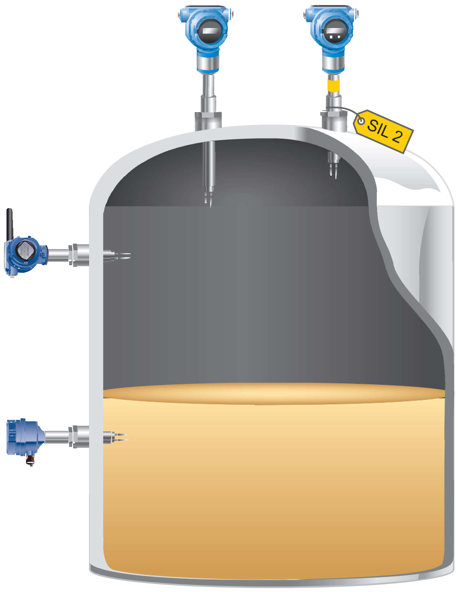


Figure 10.1: Vibrating forks

10.1.1 Advantages

With no moving parts to wear or stick, vibrating fork technology is less prone to failure compared with other technologies and requires less on-site maintenance. Vibrating fork switches are virtually unaffected by flow, bubbles, turbulence, foam, vibration, solids content, coating, properties of the liquid, and product variations, making them highly reliable for overfill prevention applications. There is also no need for calibration and they require minimum installation procedures. The latest technology on the market incorporates diagnostics and electronic proof testing capabilities enabling operators to verify the health and functionality of their overfill prevention device.

10.1.2 Limitations

Vibrating fork switches are not suitable for very viscous media. Build up between the forks, creating bridging of the forks, may cause false switching.

10.2 Guided Wave Radar

Guided wave radar (GWR) is based on microwave technology (figure 10.2). GWR uses low power, nano-second microwave pulses which are guided down a probe submerged in the process media. When the microwave pulse reaches a medium with a different dielectric constant, part of the energy is reflected back to the transmitter. The time difference between the transmitted and the reflected pulse is converted into a distance, and the total level or interface level is then calculated. The transmitter uses the residual wave of the first reflection to measure the interface level. Part of the wave, which was not reflected at the upper product surface, continues until it is reflected at the lower product surface, making it possible to calculate the amount of several different substances at the same time.

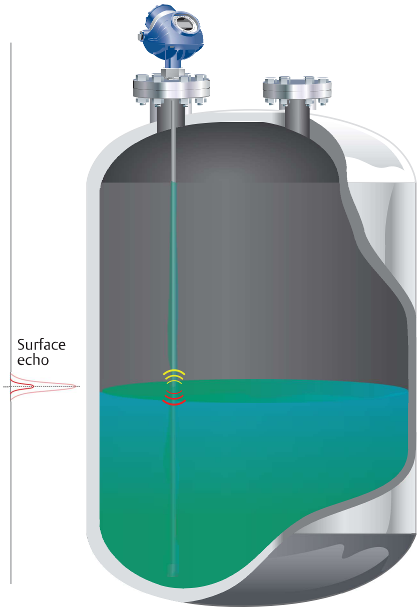


Figure 10.2: Guided wave radar technology

10.2.1 Advantages

GWR provides an accurate and reliable measurement for both level and interface, and can be used in a wide variety of applications. It is a top-down, direct measurement that measures the distance to the surface. GWR can be used with liquids, sludges, slurries, and some solids. A key advantage of radar is that no compensation is necessary for changes in the density, dielectric, or conductivity of the fluid. Changes in pressure, temperature, and most vapor space conditions have no impact on the accuracy of radar measurements. In addition, radar devices have no moving parts so maintenance is minimal. GWR is easy to install and can easily replace other technologies, such as displacer and capacitance, even if there is liquid in the tank.

With the large coaxial probe the null zone requirement is totally removed, which means that the transmitter is able to register level down the whole probe making optimal for overfill prevention applications.

The latest technology on the market incorporates diagnostics and electronic proof-testing capabilities enabling operators to verify the health and functionallity of their GWR overfill prevention device.

10.2.2 Limitations

While GWR works in many conditions, some precautions need to be taken with respect to probe choice. Several probe styles are available and application, length, and mounting restrictions influence the choice. Unless a coaxial probe is used, probes should not be in direct contact with a metallic object, because that will impact the signal. If the application tends to be sticky or coat, then only single lead probes should be used. Some of the latest GWRs on the market have advanced diagnostics, with the ability to detect build-up on the probe. Chambers with a diameter less than 3 in. (75 mm) may cause problems with build-up and may make it difficult to avoid contact between chamber wall and probe.

10.3 Non-Contacting Radar

Non-contacting radar (NCR) level transmitters (figure 10.3) also provide continuous level measurement, but without making contact with the media being measured. The transmitters are virtually unaffected by changing density, temperature, pressure, media dielectric, pH, and viscosity. Furthermore, NCR transmitters are ideal when internal tank obstructions are a limiting factor.

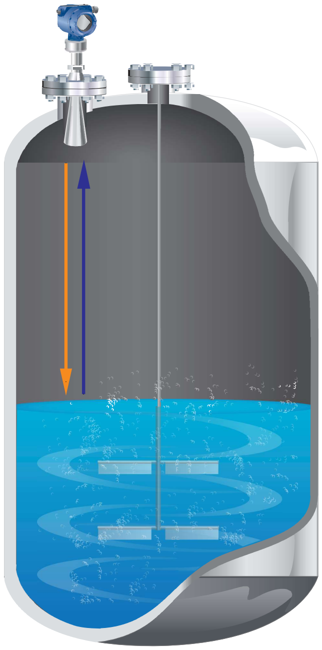


Figure 10.3: Non-contacting radar technology

10.3.1 Advantages

NCR provides a top-down, direct measurement as it measures the distance to the surface. It can be used with liquids, sludges, slurries, and some solids. A key advantage of radar is that no compensation is necessary for changes in density, dielectric, or conductivity of the fluid. Changes in pressure, temperature, and most vapor space conditions have no impact on the accuracy of radar measurements. In addition, radar devices have no moving parts so maintenance is minimal. NCR devices can be isolated from the process by using barriers such as PTFE seals or valves. Since it is not in contact with the measured media it is also good for corrosive and dirty applications.

The latest NCR devices use powerful diagnostics to ensure that the transmitters are operating safely and efficiently. Remote proof-testing functionality is also incorporated in newer devices.

10.3.2 Limitations

For NCR, good installation is the key to success. The gauge needs a clear view of the surface with a smooth, unobstructed, unrestricted mounting nozzle. Obstructions in the tank, such as pipes, strengthening bars and agitators can cause false echoes, but most transmitters have sophisticated software algorithms to allow masking or ignoring of these echoes.

NCR gauges can handle agitation, but their success will depend on a combination of the fluid properties and the amount of turbulence. Dielectric constant (DK) of the medium and the surface conditions will impact the measurement. With low dielectric process fluids, much of the radiated energy is lost to the fluid, leaving very little energy to be reflected back to the gauge. Water and most chemical solutions have a high DK; fuel oil, lube oil and some solids, such as lime, have a low DK.

The measurement may be influenced by the presence of foam. Energy tends to not be reflected by light and airy foam while a dense and heavy foam typically reflects the energy.

If the surface is turbulent, whether from agitation, product blending, or splashing, more of the signal is lost. A combination of a low dielectric fluid and turbulence can limit the return signal to a non-contacting radar gauge. To get around this, bypass pipes or stilling wells can be used to isolate the surface from the turbulence.

11

Rosemount™ Products

11. Rosemount Products

Picture 11.1: SIL-certified Rosemount products for Process Level and Tank Gauging

Rosemount instrumentation for overfill prevention has been assessed per the relevant requirements of IEC 61508 including a FMEDA (Failure Mode, Effects and Diagnostic Analysis) report by the third party Exida. The different technologies have characteristics and capabilities that differentiate them from each other making them suitable for differing environments and systems, including Safety Integrity Level, SFF, operating ranges, accuracy and functionality.

11.1 Rosemount 2120 Vibrating Fork

Picture 11.2: Rosemount 2120

11.1.1 Operating Environment

Standard model. The Rosemount 2120 Level Switch (picture 11.2) is a popular choice for high and low level alarm and pump control duties for its simplicity, ease of use and reliability.

Temperature Range	Operating pressure
Standard: –40 to 302 °F (–40 to 150 °C)	1450 psig (100 barg)

11.1.2 Certificates and Approvals

Output Type	Level of Integrity	SFF
Namur (K)	SIL 2 @ HFT=0, Route 1_H SIL 3 @ HFT=1, Route 1_H	91.1%*
8/16mA (H)	SIL 2 @ HFT=0, Route 1_H SIL 3 @ HFT=1, Route 1_H	90.9%*
PNP/PLC (G)	SIL 2 @ HFT=0, Route 1_H SIL 3 @ HFT=1, Route 1_H	90%*
Relay (V)	SIL 1 @ HFT=0, Route 1_H SIL 2 @ HFT=1, Route 1_H	72%*

* DRY=ON configuration

11.1.3 Product Features

- “Fast drip” fork design gives a quicker response time, especially with viscous liquids
- No moving parts or crevices for virtually no maintenance
- Wide choice of materials, process connections and output options configurable for different applications
- General area, explosion-proof/flameproof. and intrinsically safe options
- Adjustable switching delay for turbulent or splashing applications
- Magnetic test point for quick and simple partial proof test
- General area, explosion-proof/flameproof, and intrinsically safe options
- Visable heartbeat LED for device status
- DiBt/WHG overfill protection certification
- 3-A and EHEDG certificates available for hygenic applications

11.2 Rosemount 2130 Vibrating Fork

Picture 11.3: Rosemount 2130

11.2.1 Operating Environment

Enhanced performance model. The Rosemount 2130 Level Switch (picture 11.3) is developed for challenging applications, tough operating conditions and safety critical environments.

Temperature Range		Operating Pressure
Standard:	Optional:	1450 psig
–40 to 356 °F	–94 to 500 °F	(100 barg)
(–40 to 180 °C)	(–70 to 260 °C)	

11.2.2 Certificates and Approvals

Output Type	Level of Integrity	SFF
Namur (N)	SIL 2 @ HFT=0	95.2%*
PNP/PLC (P)		92.1%*
Load Switching (L)		92.2%*
8/16mA (M)		94.8%*
Relay (D)	SIL1 @ HFT=0	79.6%*
	SIL 2 @ HFT=1	

* DRY=ON configuration

11.2.3 Product Features

- Flexibility of Rosemount 2120 options and features with extended capabilities for challenging process conditions
- Extended operating temperature range
- Advanced built-in diagnostics continuously check electronic and mechanical health
- Visible Heartbeat led for device status and health
- Adjustable switching delay for turbulent or splashing applications
- Magnetic test point for quick and simple partial proof test
- DiBt/WHG overfill protection certification

11.3 Rosemount 2140:SIS Vibrating Fork

Picture 11.4: Rosemount 2140:SIS

11.3.1 Operating Environment

Wired HART® safety certified model. Utilizing the wired HART protocol, the Rosemount 2140:SIS (picture 11.4) can be easily integrated into systems without the need for additional point to point wiring. Switch easily between HART 5 and HART 7 to meet requirements. The Rosemount 2140:SIS features capability for both local and remote proof-testing. This unique remote proof-testing functionality can be performed from the control room, and provides the capability for multiple devices to be tested simultaneously on the bus, maximizing both safety and efficiency.

Temperature Range		Operating Pressure
Standard: –40 to 302 °F (–40 to 150 °C)	Optional: –94 to 500 °F (–70 to 260 °C)	1450 psig (100 barg)

11.3.2 Certificates and Approvals

Device/ Configuration	Level of Integrity	SFF
T0 terminal block WET=ON	SIL 2 @ HFT=0, Route 1_H	97.6%
T0 terminal block DRY=ON		96.7%
T1 terminal block WET=ON		97.7%
T1 terminal block DRY=ON		96.8%

11.3.3 Product Features

- World's only wired HART vibrating fork level detector
- Designed specifically for functional safety, critical control and overfill prevention applications
- Excellent diagnostics coverage, with an industry-leading low number of dangerous undetected failures
- Remote configuration, diagnostics and proof-testing capabilities keep workers off the tank
- Fully integrated remote proof test simplifies testing and eliminates safety risks from human error
- Plan predictive maintenance with Advanced Diagnostics and Smart Diagnostics Suite
- Media Learn function ensures reliable switching even if media characteristics are unknown

11.4 Rosemount 5300 Guided Wave Radar

Picture 11.5: Rosemount 5300

11.4.1 Operating Environments

The Rosemount 5300 (picture 11.5) is highly accurate and reliable direct level measurement with no compensation needed for changing process conditions (such as density, conductivity, viscosity, pH, temperature, and pressure) and is suitable for most liquid and solids level applications and liquid interface applications.

Temperature Range	Operating Pressure	Range & Accuracy
–320 to 752 °F (–196 to 400 °C)	5000 psi (Full vacuum) (345 bar)	Up to 164 ft (50m) ±0.12 in (±3 mm)

11.4.2 Certificates and Approvals

Level of Integrity	SFF
SIL3 @ HFT=1, Route 1_H	91.5%
SIL2 @ HFT=0, Route 1_H	
SIL3 @ HFT=1, Route 2_H	N/A
SIL2 @ HFT=0, Route 2_H	

11.4.3 Product Features

- Top down installation minimizes risk for leakages
- Highly accurate and reliable direct level measurement with no compensation needed for changing process conditions
- EchoLogics and smart software functions provide enhanced ability to keep track of the surface and detect a full vessel situation
- No moving parts and no re-calibration result in minimized maintenance
- Heavy-duty unique hardware for extreme temperature and pressures with multiple layers of protection
- Online device verification and reliable detection of high level conditions with the verification reflector
- Signal Quality Metrics diagnostics detect product build-up on probe to monitor turbulence, boiling, foam, and emulsions
- DiBt/WHG overfill protection certification

11.5 Rosemount 5408:SIS Non-Contacting Radar

Picture 11.6: Rosemount 5408:SIS

11.5.1 Operating Environments

Rosemount 5408:SIS (picture 11.6) is ideal for safety applications and level measurements over a broad range of liquid applications such as storage- and buffer tanks, reactors, open atmospheric applications, still pipe and chamber installations, blenders and mixers.

Temperature Range	Operating Pressure	Range & Accuracy
−76 to 482 °F (−60 to 250 °C)	1450 psi (100 bar)	Up to 131ft (40m) ±0.08 in (±2 mm)

11.5.2 Certificates and Approvals

Level of Integrity	SFF
SIL3 @ HFT=1, Route 1_H SIL2 @ HFT=0, Route 1_H	92.7%

11.5.3 Product Features

- Unique energy-efficient two-wire FMCW radar technology for optimal performance
- Engineered and user tested for best in class safety, reliability, and ease-of-use
- A Smart Diagnostics Suite provides operators with early alerts in case of antenna build-up, weak power supply, or abnormal surface conditions
- A local memory enables full insight into the last seven days of measurements, alerts, and echo profiles
- Safe, easy, and remote proof testing without process interruptions
- Hazardous area approvals: ATEX, IECEx, FM, CSA
- DiBt/WHG overfill protection certification
- Immune to intermittent power loss

11.6 Rosemount 5900S Radar Level Gauge

Picture 11.7: Rosemount 5900S

11.6.1 Operating Environments

The Rosemount 5900S is a state of the art non-contacting FMCW radar optimized for bulk liquid storage tanks. It offers highest stability, reliability and accuracy for virtually any tank type and liquid product.

Temperature Range	Accuracy
−40 to 158 °F (−40 to 70 °C) (min. start up temp. -58 °F/-50 °C)	± 0.020 in (0.5 mm)

11.6.2 Certificates and Approvals

Output Type	Level of Integrity	SFF
4-20mA	SIL2 @ HFT=0, Route 1_H	91.9%
Relay		91.6%
4-20mA & Relay combined		90.9%
4-20mA Relay 4-20mA & Relay combined	SIL2 @ HFT=0, Route 2_H	N/A

11.6.3 Product Features

- Continuous surveillance – radar level gauges are always in operation
- 2-wire intrinsically safe cabling on tanks
- Analog 4-20 mA and/or relay output
- Suitable for a wide range of media – from light products to heavy fuel oil or asphalt
- Installation normally with tank in service
- DiBt/WHG overfill protection certification

11.7 Rosemount 5900S 2-in-1 Radar Level Gauge

Picture 11.8: Rosemount 5900S 2-in-1

11.7.1 Operating Environments

The Rosemount 5900S 2-in-1 is a unique, patented solution that features one primary and one backup radar level gauge installed in one single housing. As such, a single 5900S 2-in-1 unit can serve as a safety certified level device in two independent protection layers (i.e. BPCS and OPS).

Temperature Range	Accuracy
–40 to 158 °F (–40 to 70 °C) (min. start up temp. -58 °F/-50 °C)	± 0.020 in (0.5 mm)

11.7.2 Certificates and Approvals

Output Type	Level of Integrity	SFF
Relay	SIL3 @ HFT=0, Route 1_H	99%
4-20mA	SIL2 @ HFT=0, Route 1_H	91.9%
Relay		91.6%
4-20mA & Relay combined		90.9%
4-20mA	SIL2 @ HFT=0, Route 2_H	N/A
Relay		
4-20mA & Relay combined		

11.7.3 Product Features

- The two radar units are galvanically separated and completely independent from each other
- Needs only one tank opening for BPCS and OPS – reduces installation cost
- Enables real time measurement verification by comparing signals on primary and secondary radar unit
- Level output of safety sensor is available as redundant level measurement data
- DiBt/WHG overfill protection certification

11.8 Rosemount 5900C Radar Level Gauge

Picture 11.9: Rosemount 5900C

11.8.1 Operating Environments

The Rosemount 5900C offers reliable performance for level measurement in bulk liquid storage tanks. It is suitable for virtually any tank type and liquid product.

Temperature Range	Accuracy
–40 to 158 °F (–40 to 70 °C) (min. start up temp. -58 °F/-50 °C)	± 0.12 in (3 mm)

11.8.2 Certificates and Approvals

Output Type	Level of Integrity	SFF
4-20mA	SIL2 @ HFT=0, Route 1_H	91.9%
Relay		91.6%
4-20mA & Relay combined		90.9%
4-20mA	SIL2 @ HFT=0, Route 2_H	N/A
Relay		
4-20mA & Relay combined		

11.8.3 Product Features

- Continuous surveillance – radar level gauges are always in operation
- 2-wire intrinsically safe cabling on tanks
- Analog 4-20 mA and/or relay output
- Suitable for a wide range of media – from light products to heavy fuel oil or asphalt
- Installation normally with tank in service
- DiBt/WHG overfill protection certification

11.9 MTBF (Mean Time Between Failure)

Reliability of a product can be quantified as Mean Time Between Failure (MTBF). MTBF is the statistical average (mean) period of time between failures in a group of complete units, caused by "random" failures in one of the unit's components. Failures due to mistakes (so called systematic failures) are not included in MTBF.

MTBF can be divided into two groups: Theoretical MTBF and Field Experienced MTBF. While Theoretical MTBF is a result of anlaysis of a unit tested under strict conditions (e.g. in a lab), the Field Experienced MTBF is a result of data gathered from units installed on site. Following is an estimation and presentation of Field Experienced MTBP.

The estimated MTBF does not advise product life time. Rather, it aims to statistically determine how many units are needed to support a certain number of units in operation. To provide a describing example: if MTBF for a specific type of radar level gauge is 100 years, then one spare-unit is needed to support a group of 100 units during one year. Conversely, in a group of 200 radar level gauges with MTBF equals to 100 years, then during 10 years, the number of units that statistically will fail is 20 units (2000 unit-years / 100 years).

11.9.1 Random Failures

It is generally accepted that a component's failure will go through three phases during its life cycle: Infant Mortality, Imaginable Constant, and Wear-Out. This life cycle when plotted is visualized in what is commonly referred to as a bathtub curve (figure 11.9.1).

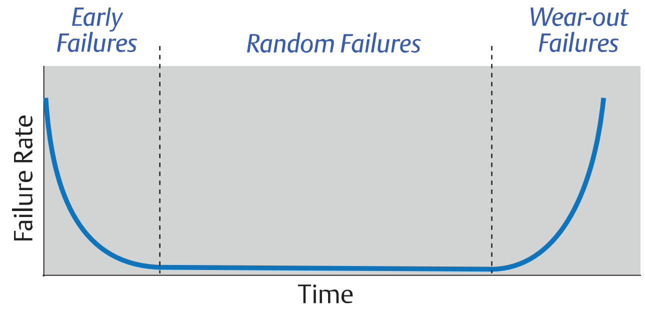


Figure 11.1: The Bathtub Curve showing hypothetical failure rate over time

11.9.2 The Model

MTBF has been estimated by taking the accumulated time-in-operation of all gauges delivered, divided by the accumulated random and verified failures reported on these units. MTBF is usually expressed in "years", but theoretically the unit is "unit-years per failure".

$$\text{MTBF} = \frac{\text{Accumulated Time in-Operation}}{\text{Accumulated No. of Random Failures}} = \frac{1}{\lambda}$$

Alternatively, MTBF can be expressed as a failure rate (lambda). The failure rate of electronic devices is usually expressed in FiT (Failures in Time), where one FiT equals one failure per billion hours (or one FiT = 10^{-9} failures per hour).

11.9.3 The Calculation

The data used in the calculations is based on all 5900´s shipped from the original product launch date (September, 2010) to the creation date of this document (December, 2018). Units with the two-in-one feature have been excluded from the data.

The accumulated time-in-operation has been estimated as the time interval between shipment date to the creation date of this document subtracted by six months. Here, five months represent the average time between shipment of a unit and the time of commissioning. Additionally one month is used to represent the average time it takes a user to notify the manufacturer of the device failure. (5+1 = 6 months)

For Rosemount 5900 (1-in-1) in the given time period:

Accumulated Time-In-Operation = 48900 years

Accumulated No. of Random and Verified Failures = 66

Field Experienced MTBF = 48900 / 66 years

Field Experienced MTBF Rosemount 5900
741 years

An MTBF-result of 741 years equals a failure rate of 154 FIT (or 154 failures per billion of hours).

11. 10 Product Overview Specification

Below is a selection of Rosemount overfill prevention products and specifications.

Rosemount level Sensors for Overfill Prevention

Device	Safety Instrumented Systems	AOPS	MOPS	Proof-testing
5300	IEC 61508 certified. Single device up to SIL 2	+	+	Remote
5408:SIS	IEC 61508 certified. Single device up to SIL 2	+	+	Remote
3300	N/A	-	+	N/A
3308	N/A	+	+	N/A
2140:SIS	IEC 61508 certified. Single device up to SIL 2	+	+	Local and Remote
2160	N/A	-	+	N/A
2120/2130	IEC 61508 certified. Single device up to SIL 2	+	+	Local (in situ option)
5900S 2-in-1 SIL 3	IEC 61508 certified. Single device up to SIL 3	+	+	Remote
5900S 2-in-1 SIL 2	IEC 61508 certified. Single device up to SIL 2	+	+	Remote
5900S 1-in-1 SIL 2	IEC 61508 certified. Single device up to SIL 2	+	+	Remote
5900C 1-in-1 SIL 2	IEC 61508 certified. Single device up to SIL 2	+	+	Remote

Overfill Prevention System Examples

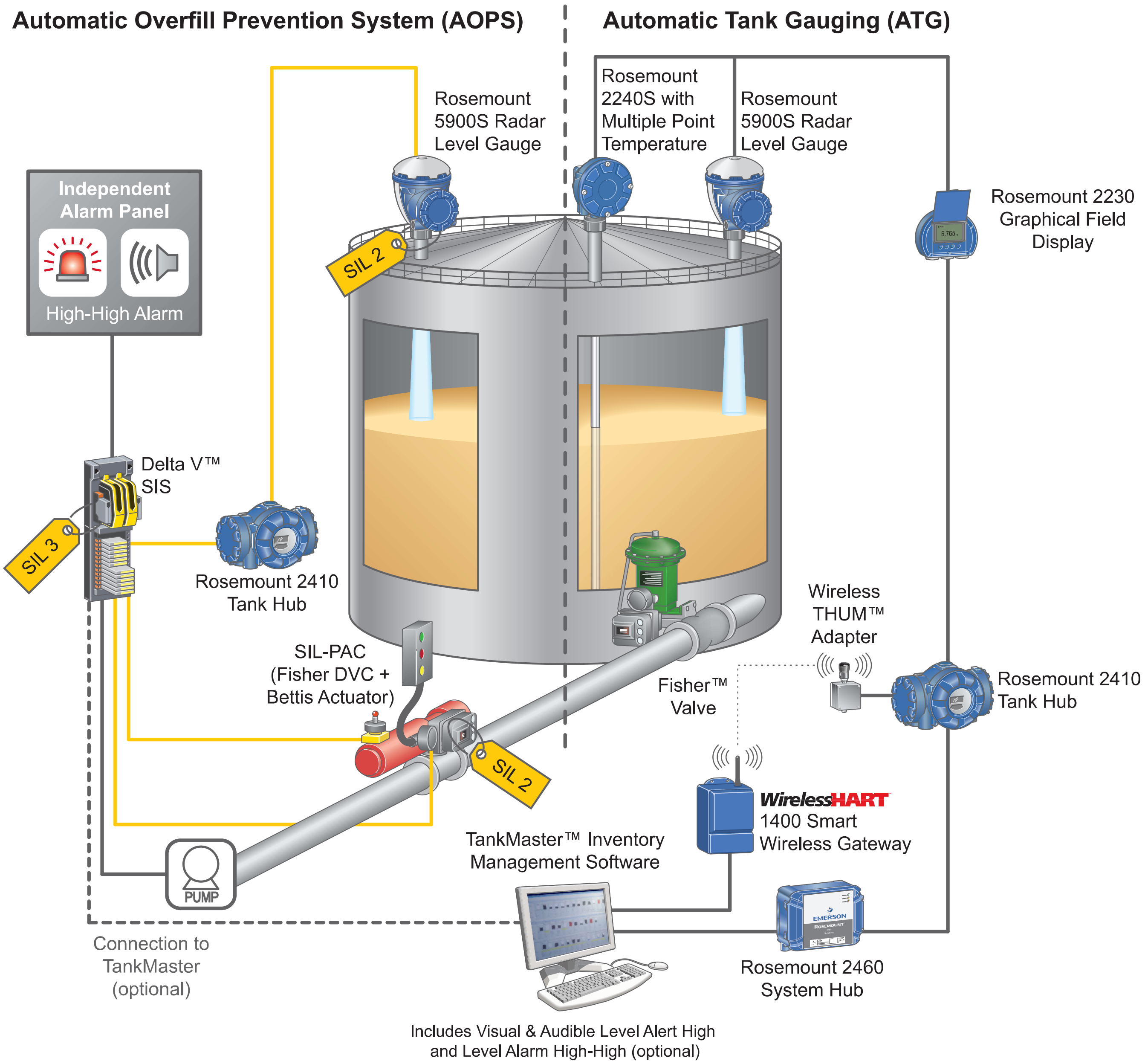
Topic Page

12. Overfill Prevention System Examples

12.1 Bulk Liquid Storage

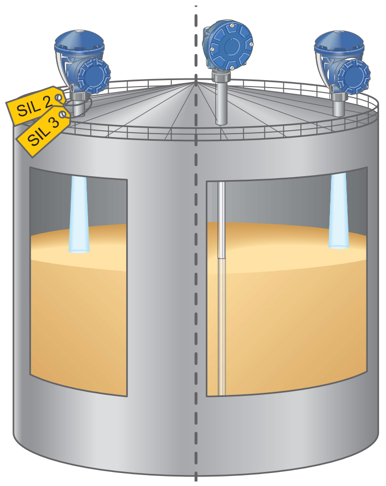
12.1.1 Fixed Roof Tanks

Illustration shows a fixed roof tank equipped with Automatic Tank Gauging based on the Rosemount™ 5900S and a SIL 3 AOPS based on the Rosemount 5900S, DeltaV SIS and a Bettis actuator.



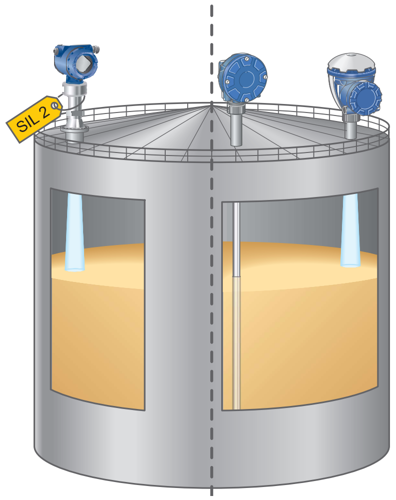
12 - Overfill Prevention Systems Examples

Below are alternatives of recommended Rosemount level sensors for fixed roof tanks:



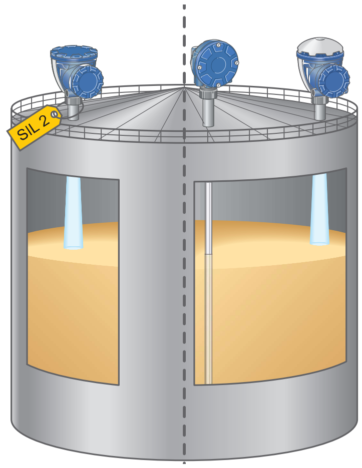
Rosemount
5900S (AOPS, MOPS)

Rosemount
5900S



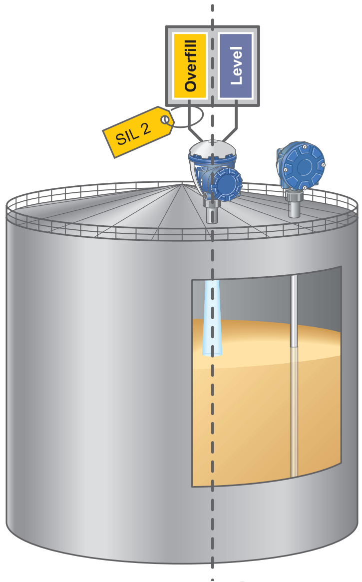
Rosemount
5408 (AOPS, MOPS)

Rosemount
5900S

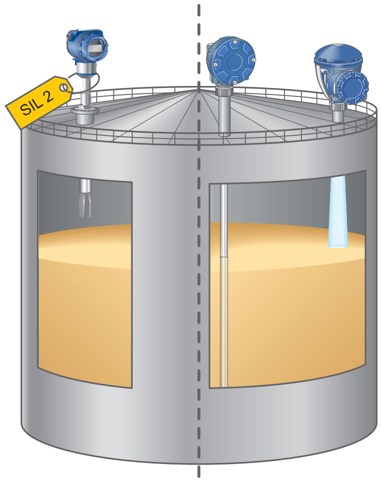


Rosemount
5900C (AOPS, MOPS)

Rosemount
5900S



Rosemount
5900S 2-in-1 (AOPS)

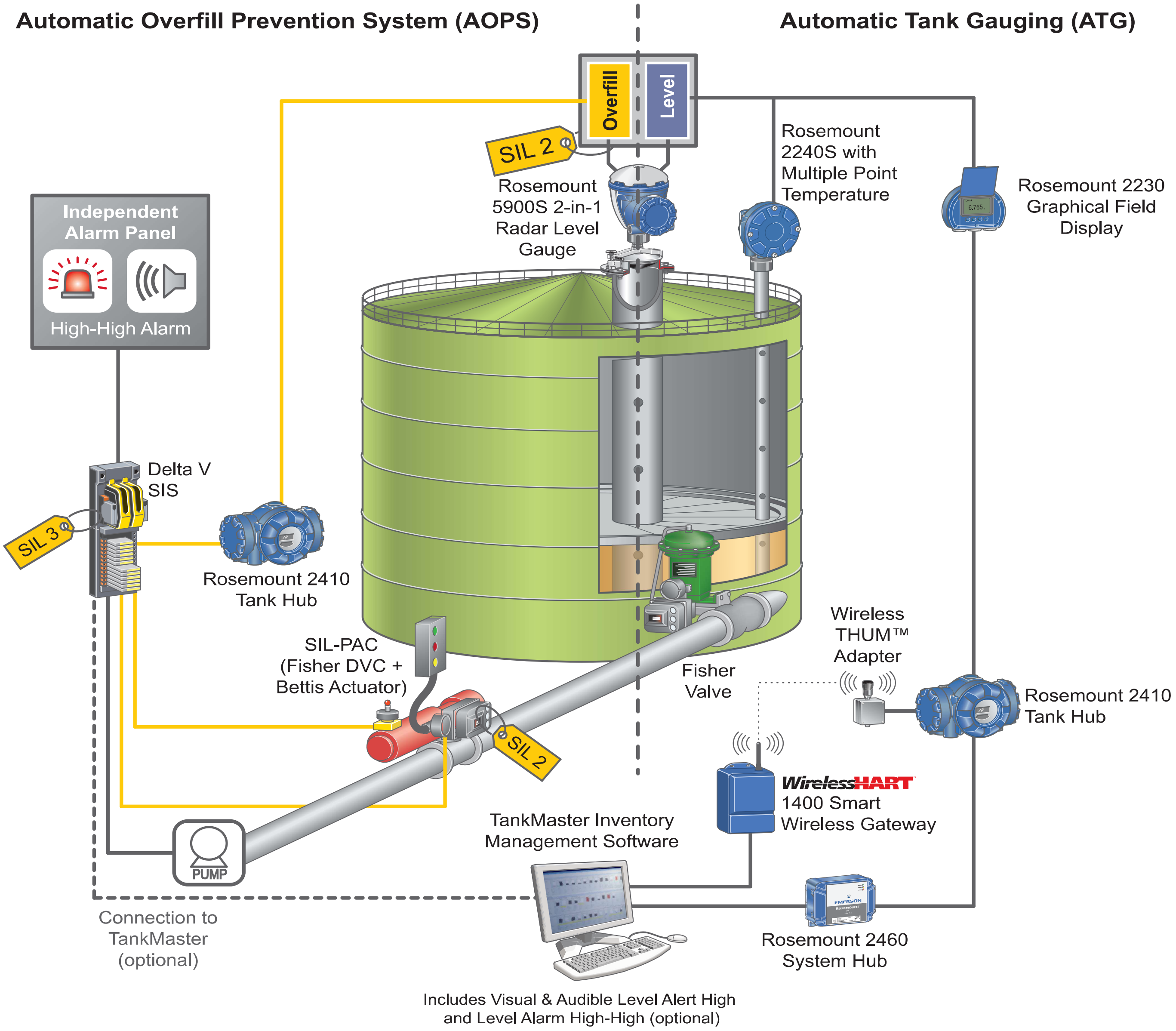


Rosemount
2140 (AOPS, MOPS)

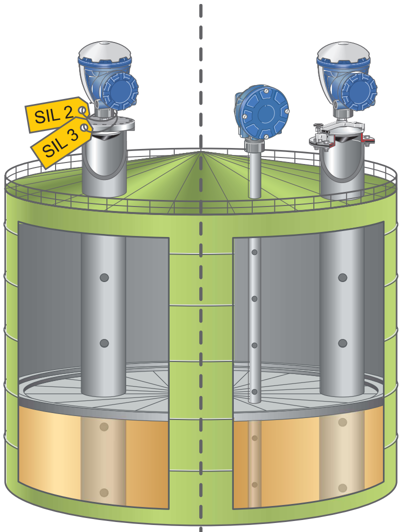
Rosemount
5900S

12.1.2 Floating Roof Tanks

Illustration shows a floating roof tank equipped with Automatic Tank Gauging based on the Rosemount 5900S and a SIL 2 AOPS based on the Rosemount 5900S, DeltaV SIS and a Bettis™ actuator.

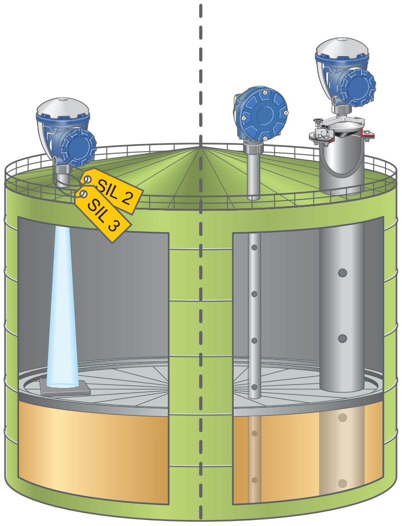


Below are alternative Rosemount level sensors for floating roof tanks:



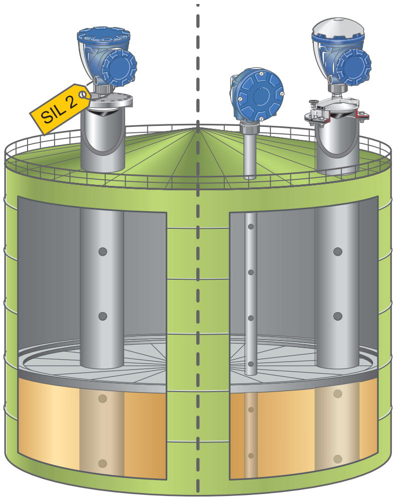
*Rosemount
5900S (AOPS, MOPS)
(pipe)*

*Rosemount
5900C*



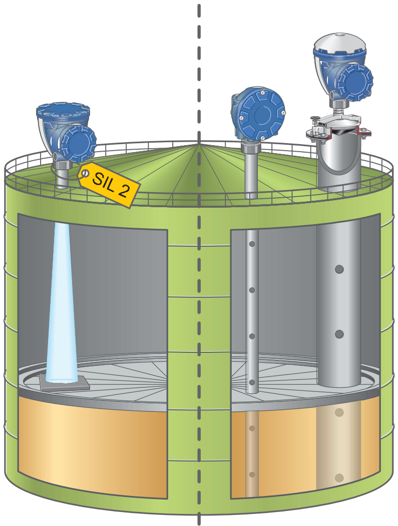
*Rosemount
5900S (AOPS, MOPS)
(roof-plate)*

*Rosemount
5900C*



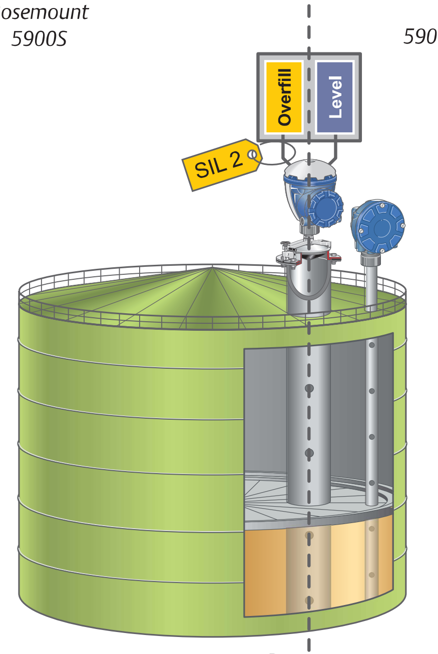
*Rosemount
5900S (AOPS, MOPS)
(pipe)*

*Rosemount
5900S*



*Rosemount
5900S (AOPS, MOPS)
(roof-plate)*

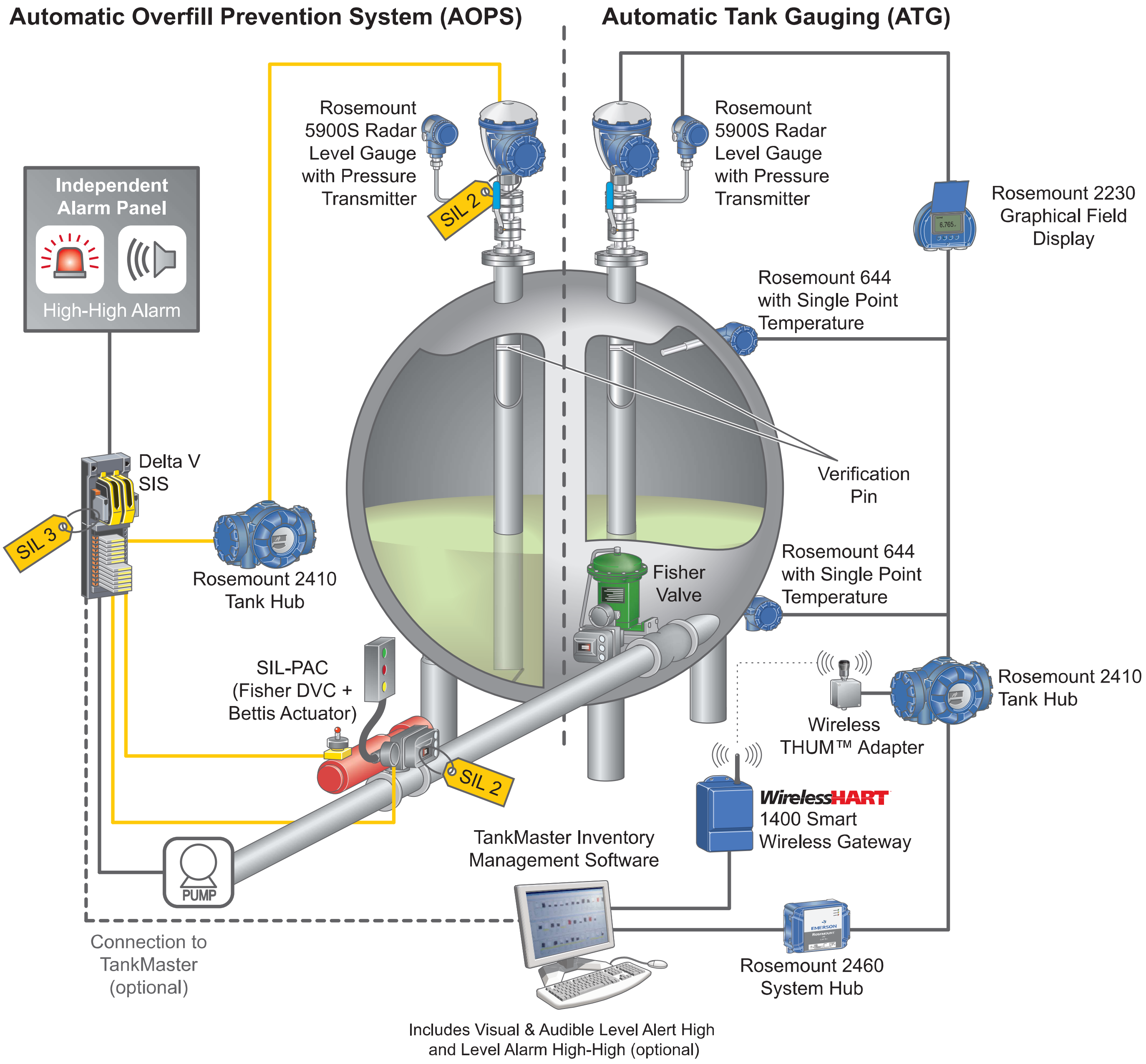
*Rosemount
5900S*



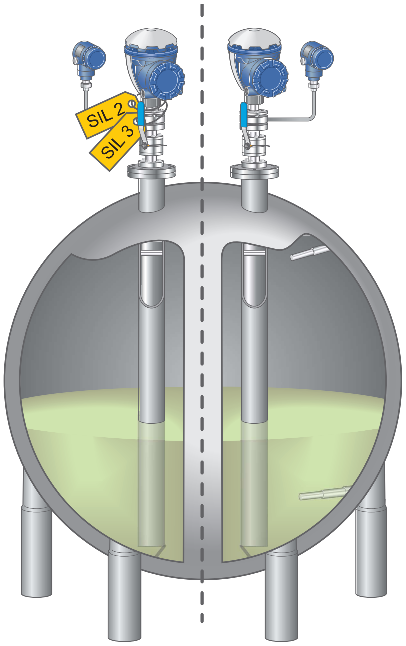
*Rosemount
5900S 2-in-1 (AOPS, MOPS)*

12.1.3 Spherical Tanks

Illustration shows a spherical tank equipped with Automatic Tank Gauging based on the Rosemount 5900S and a SIL 2 AOPS based on the Rosemount 5900S, DeltaV SIS and a Bettis actuator.

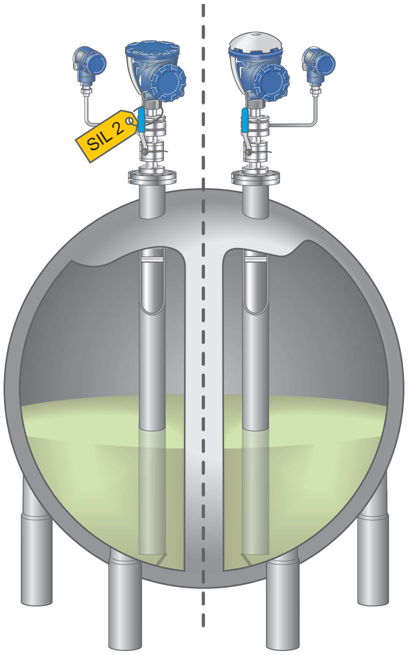


Below are alternative Rosemount level sensors for spherical tanks:



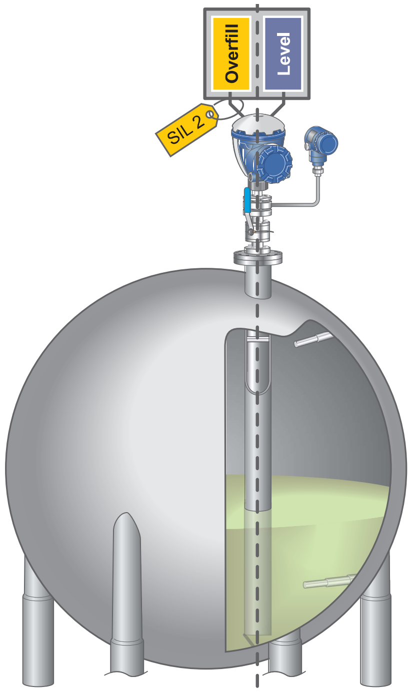
Rosemount
5900S (AOPS, MOPS)

Rosemount
5900S



Rosemount
5900S (AOPS, MOPS)

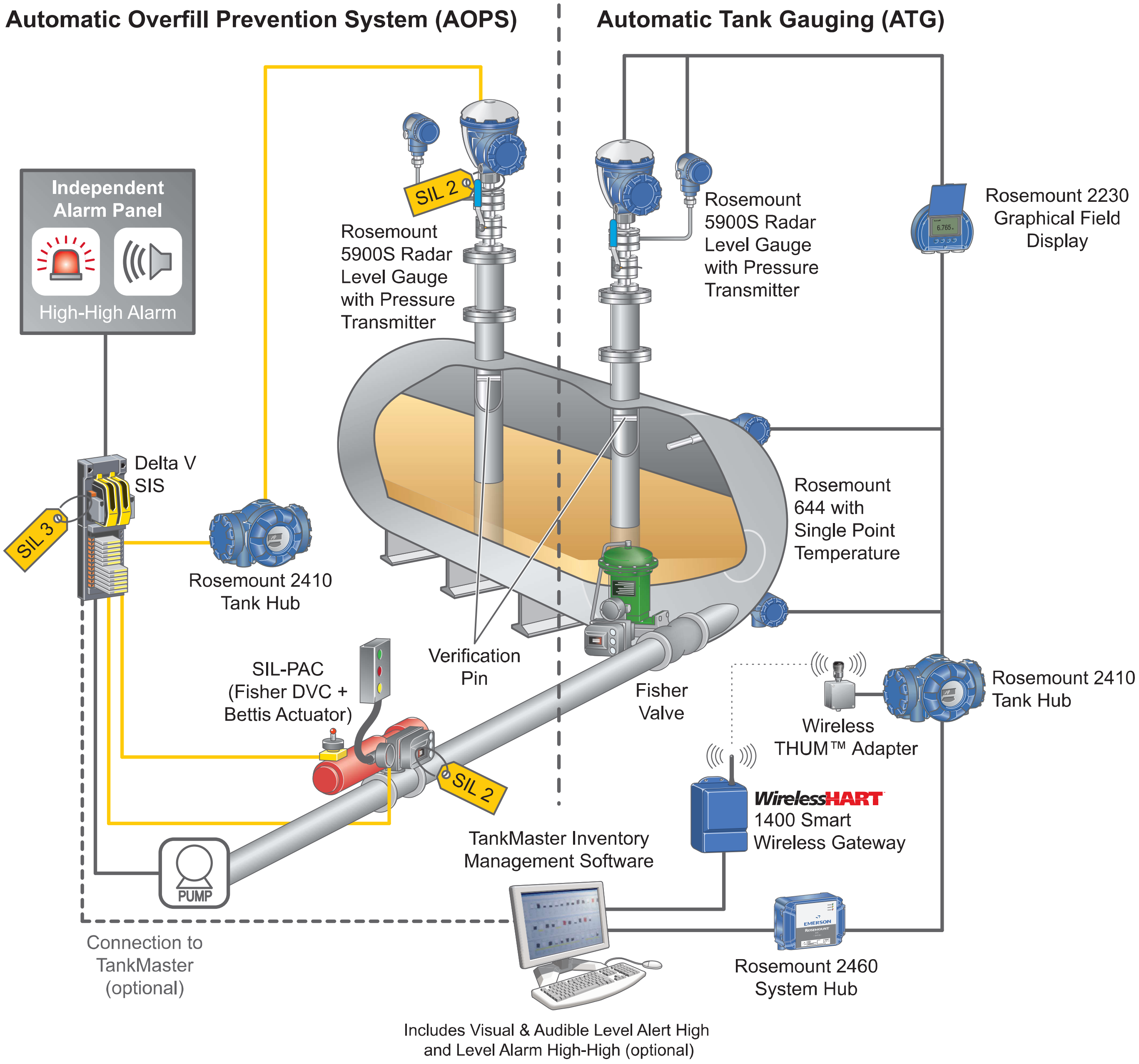
Rosemount
5900C



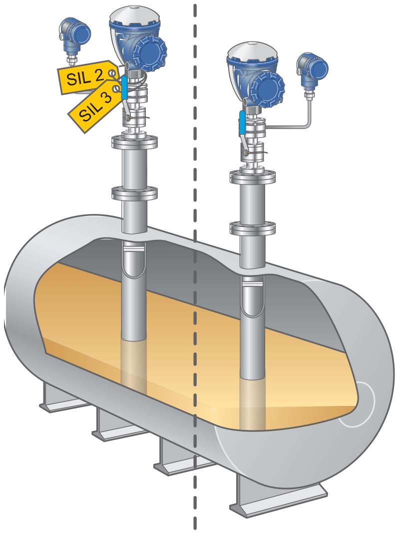
Rosemount
5900S 2-in-1 (AOPS, MOPS)

12.1.4 Bullet Tanks

Illustration shows a bullet tank equipped with Automatic Tank Gauging based on the Rosemount 5900S and a SIL 2 AOPS based on the Rosemount 5900S, DeltaV SIS and a Bettis actuator.

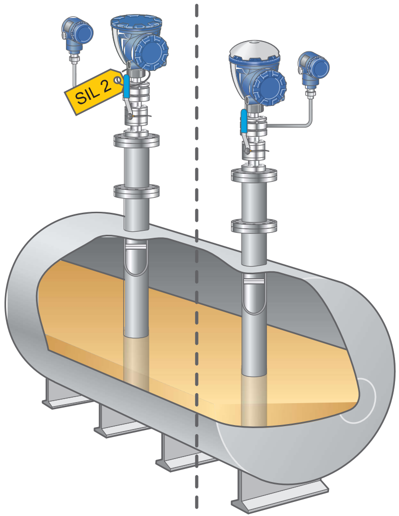


Below are alternative Rosemount level sensors for bullet tanks:



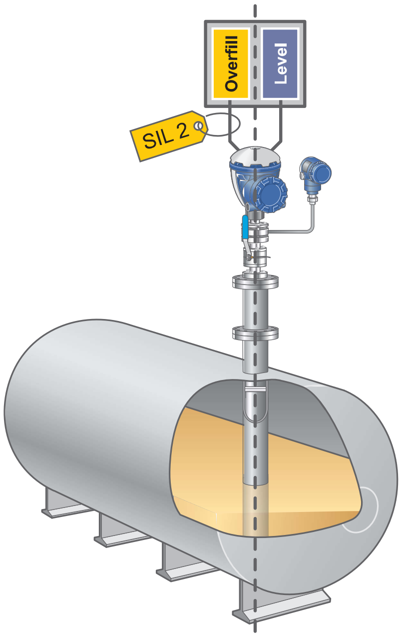
*Rosemount
5900S (AOPS, MOPS)*

*Rosemount
5900S*

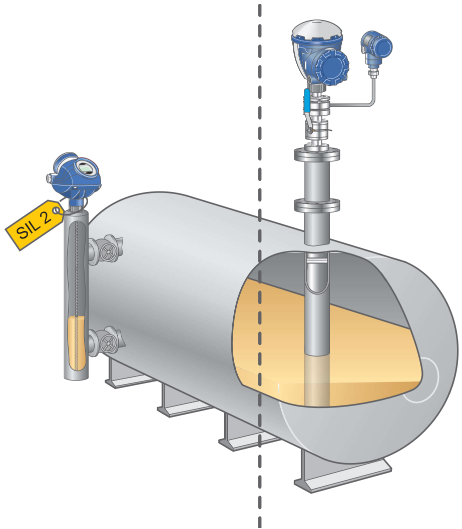


*Rosemount
5900C (AOPS, MOPS)*

*Rosemount
5900S*



*Rosemount
5900S 2-in-1 (AOPS, MOPS)*



*Rosemount
5300 (AOPS, MOPS)*

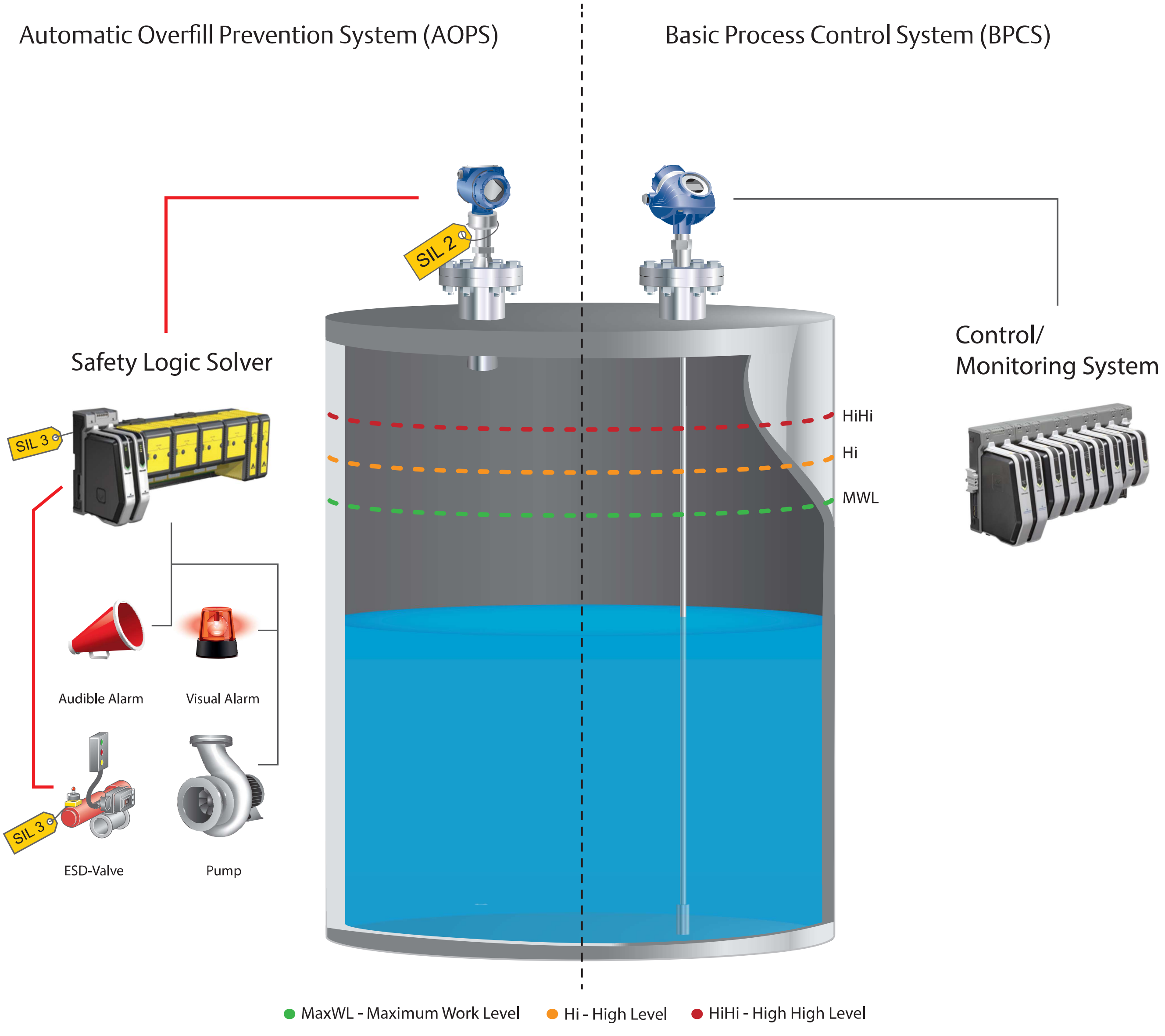
*Rosemount
5900S*

Additional bulk liquid storage tank examples is available in "The Complete Guide to API 2350" (Ref.No. 901030)

12.2 Process Vessels

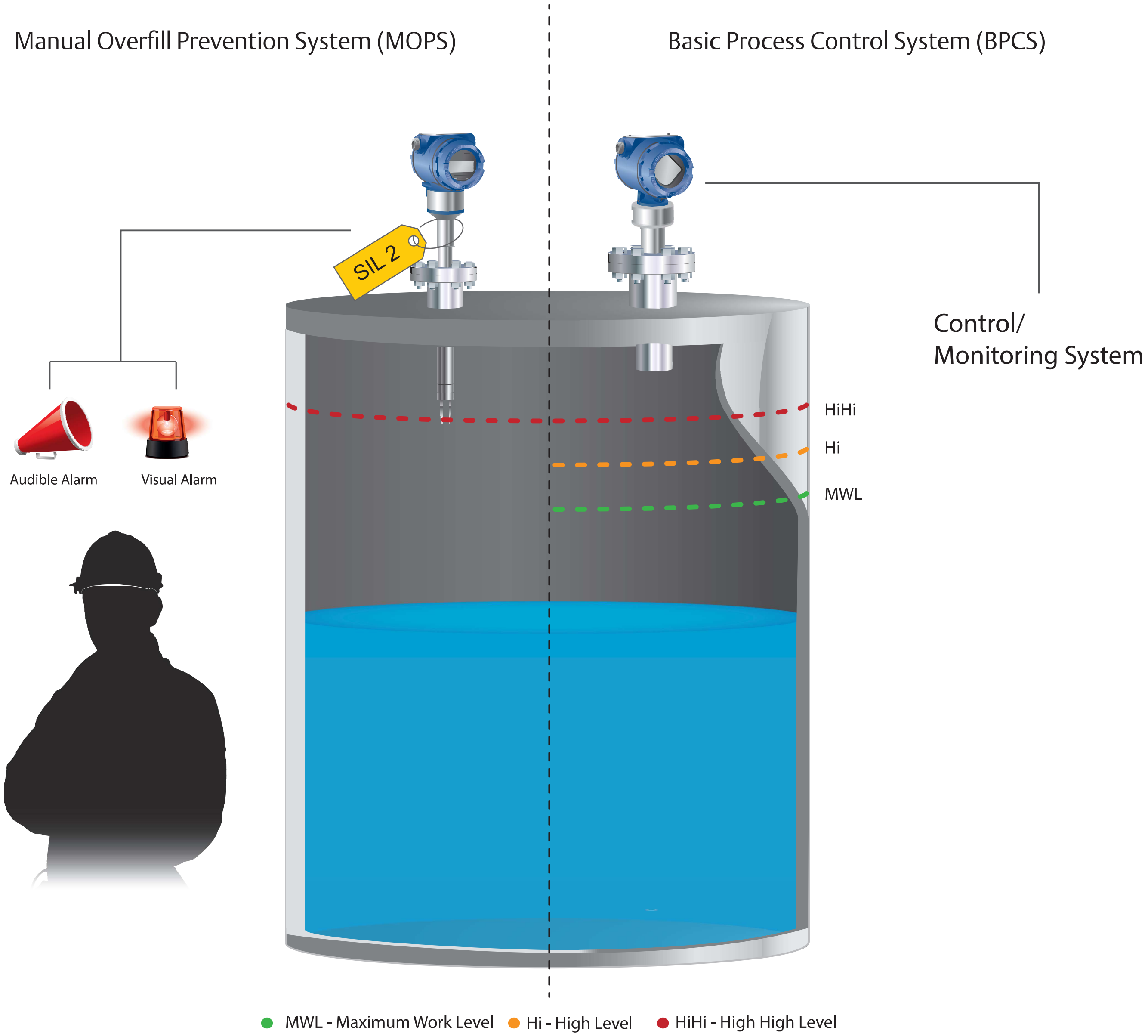
12.2.1 Top Mounted OPS Level Sensor

Illustration shows a cone tank equipped with a Rosemount 5300 for BPCS and SIL 2 AOPS based on Rosemount 5408:SIS, DeltaV SIS and Bettis actuator.

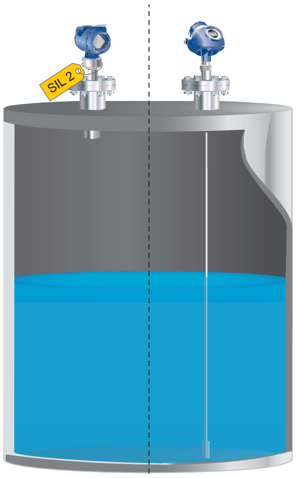


12 - Overfill Prevention Systems Examples

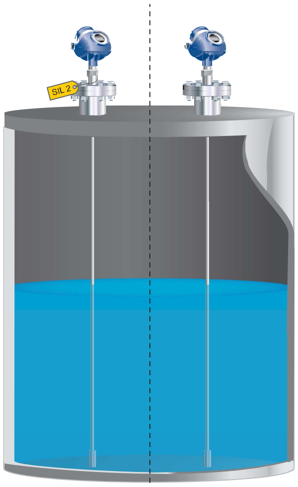
Illustration shows a cone tank equipped with a Rosemount 5408 for BPCS and MOPS based on a Rosemount 2140:SIS.



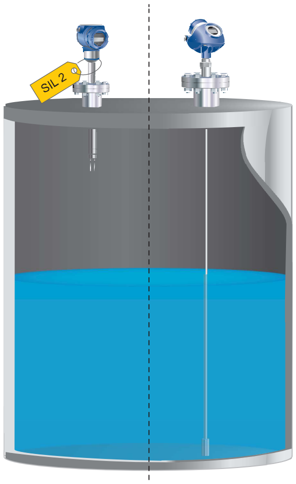
Below are alternative Rosemount level sensors top mounting:



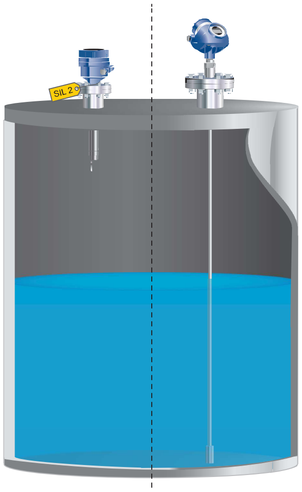
Rosemount 5408 SIS (AOPS) — *Rosemount 5300*



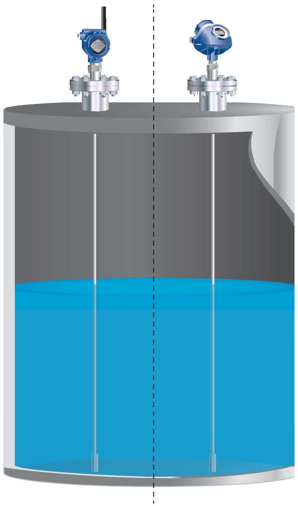
Rosemount 5300 (AOPS) — *Rosemount 5300*



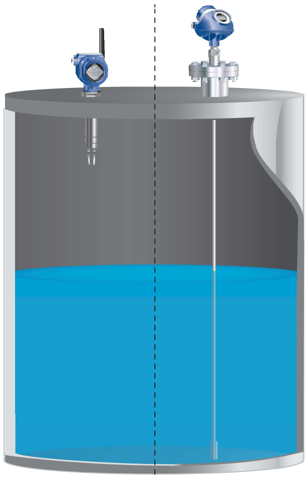
Rosemount 2140:SIS (AOPS) — *Rosemount 5300*



Rosemount 2100 (AOPS) — *Rosemount 5300*



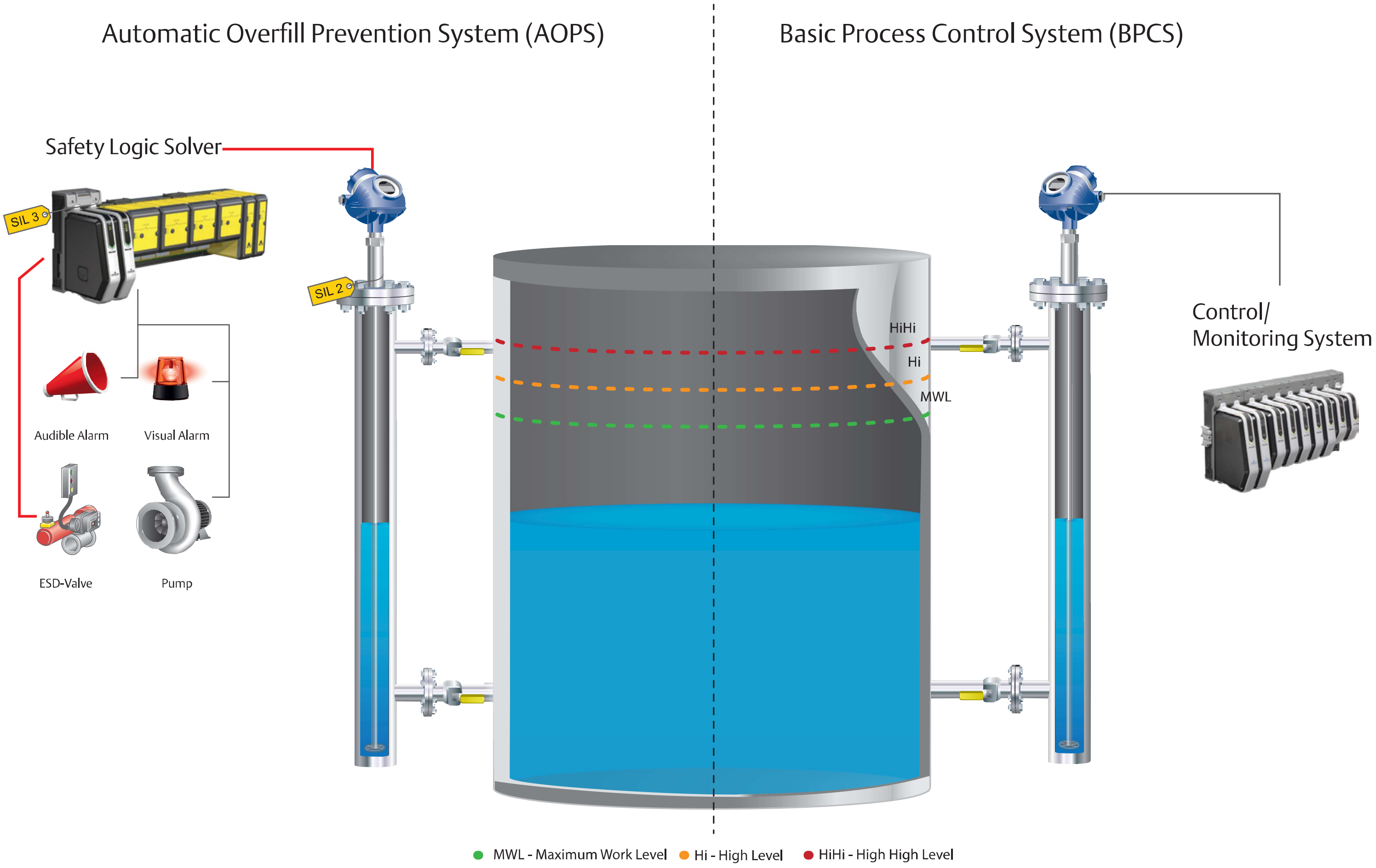
Rosemount Wireless 3308 (MOPS) — *Rosemount 5300*



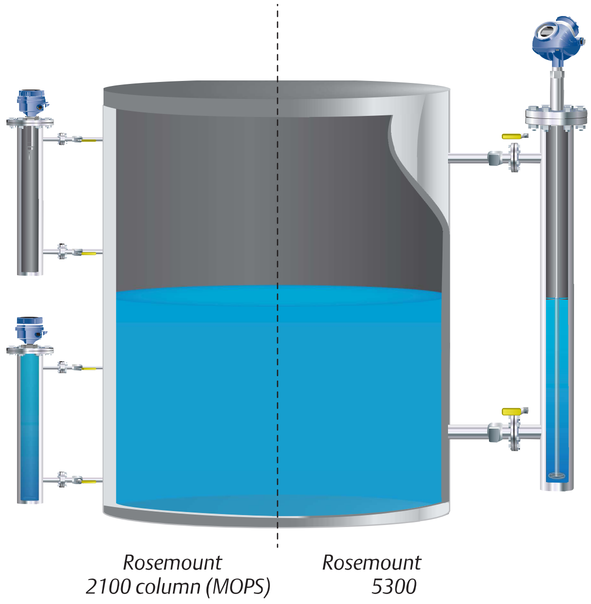
Rosemount Wireless 2160 (MOPS) — *Rosemount 5300*

12.2.2 Chamber Mounted OPS Level Sensor

Illustration shows chamber installations. Rosemount 5300 is used for BPCS and SIL 2 AOPS are based on Rosemount 5300, DeltaV SIS and Bettis actuator.



Below are alternative Rosemount level sensors for chamber installations:



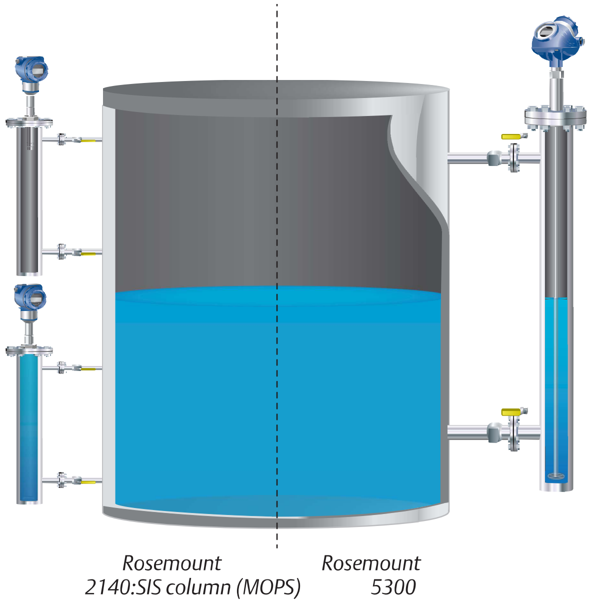
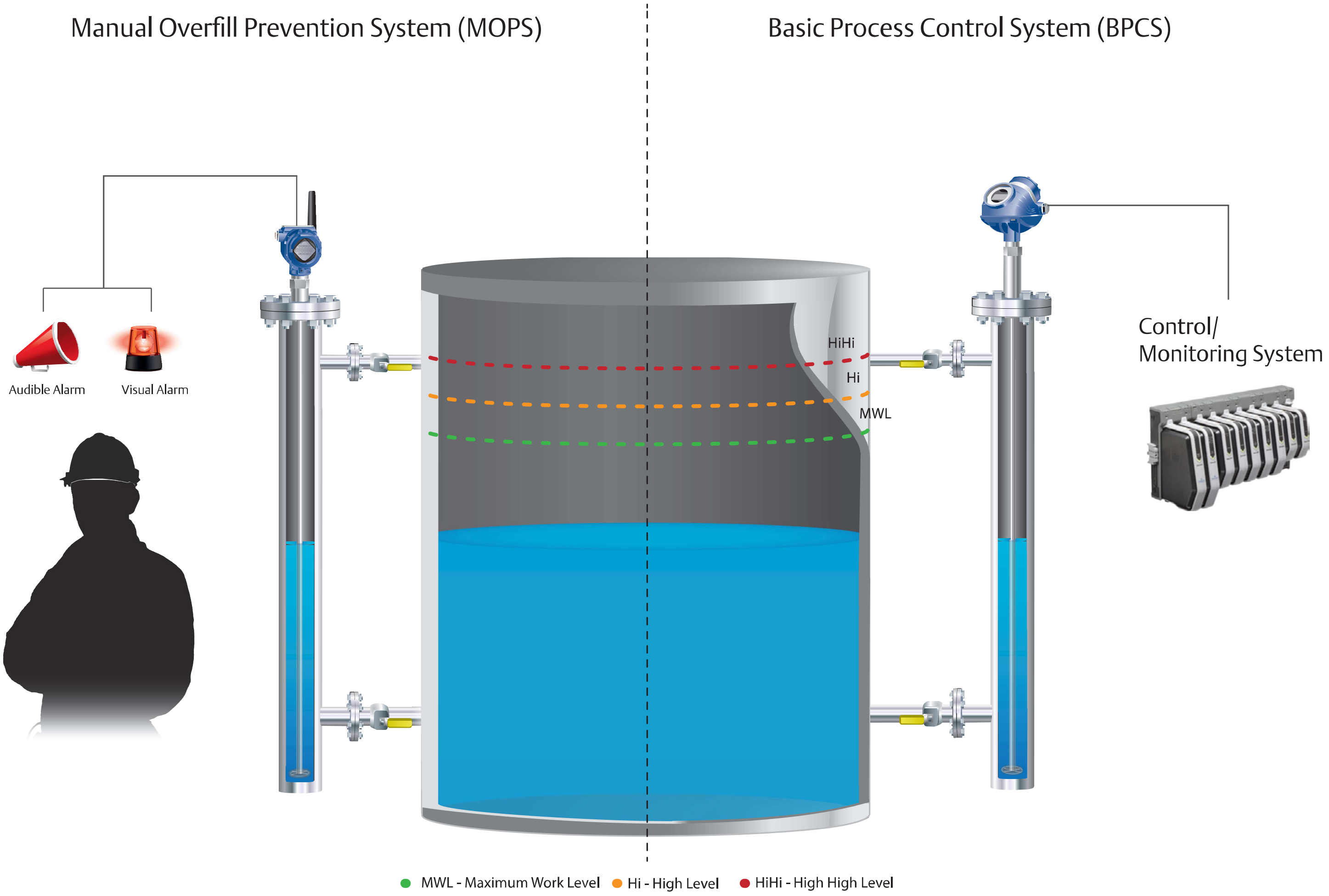
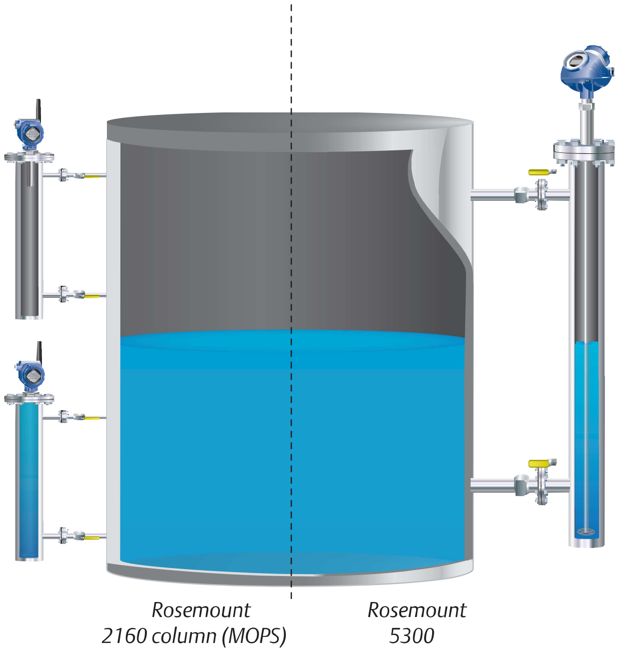


Illustration shows a cone tank equipped with a Rosemount 5300 for BPCS and MOPS based on a Rosemount 3308.

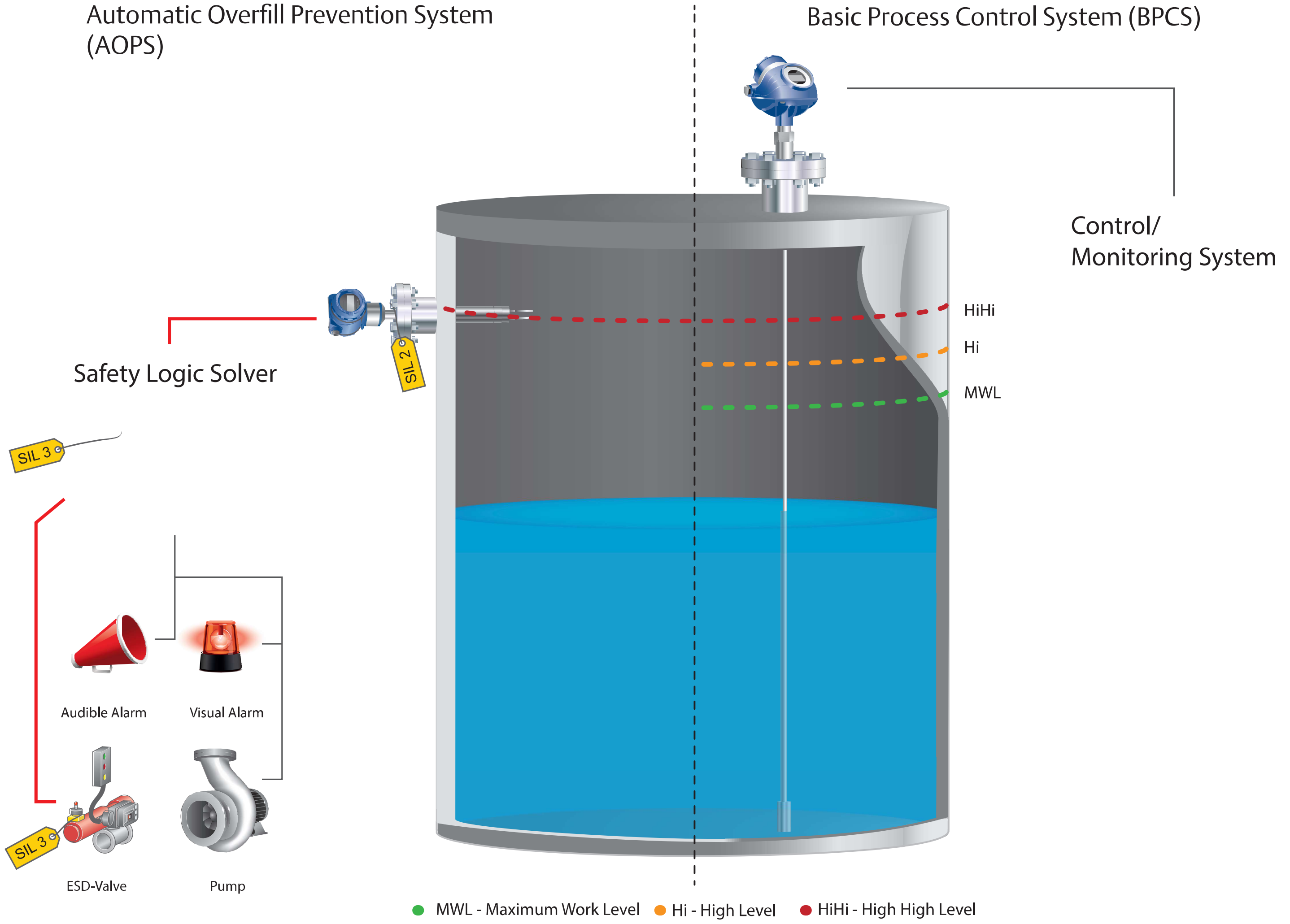


Below are alternative Rosemount level sensors for chamber installations:

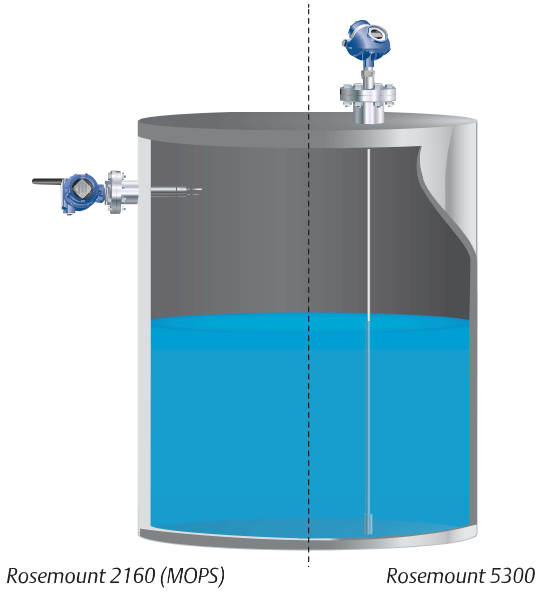


12.2.3 Side Mounted OPS Level Sensor

Illustration shows a tank side installation. Rosemount 5300 is used for BPCS and SIL 2 AOPS is based on Rosemount 2140:SIS, DeltaV SIS and Bettis actuator.

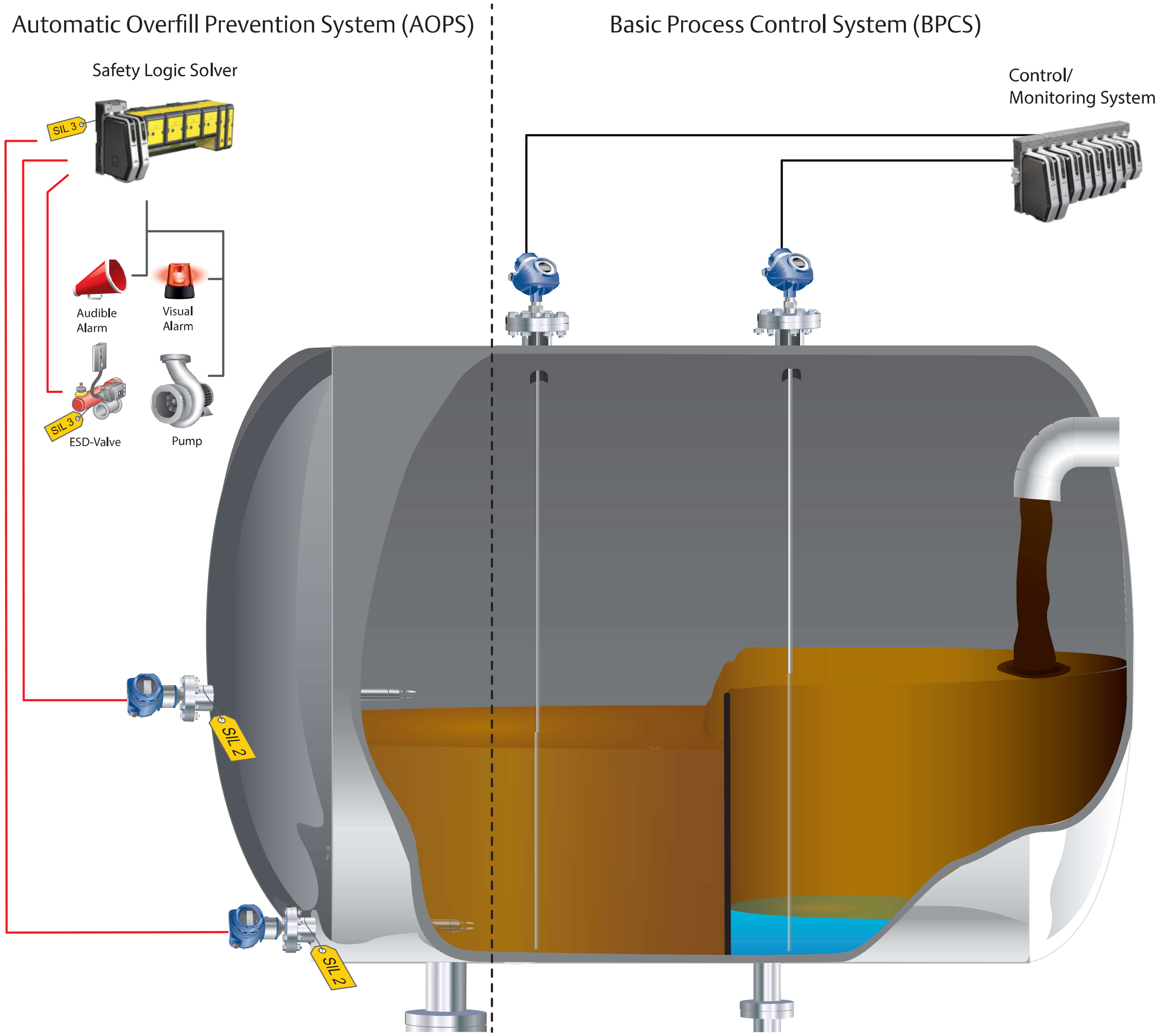


Below is an alternative Rosemount level sensor for side mounting:



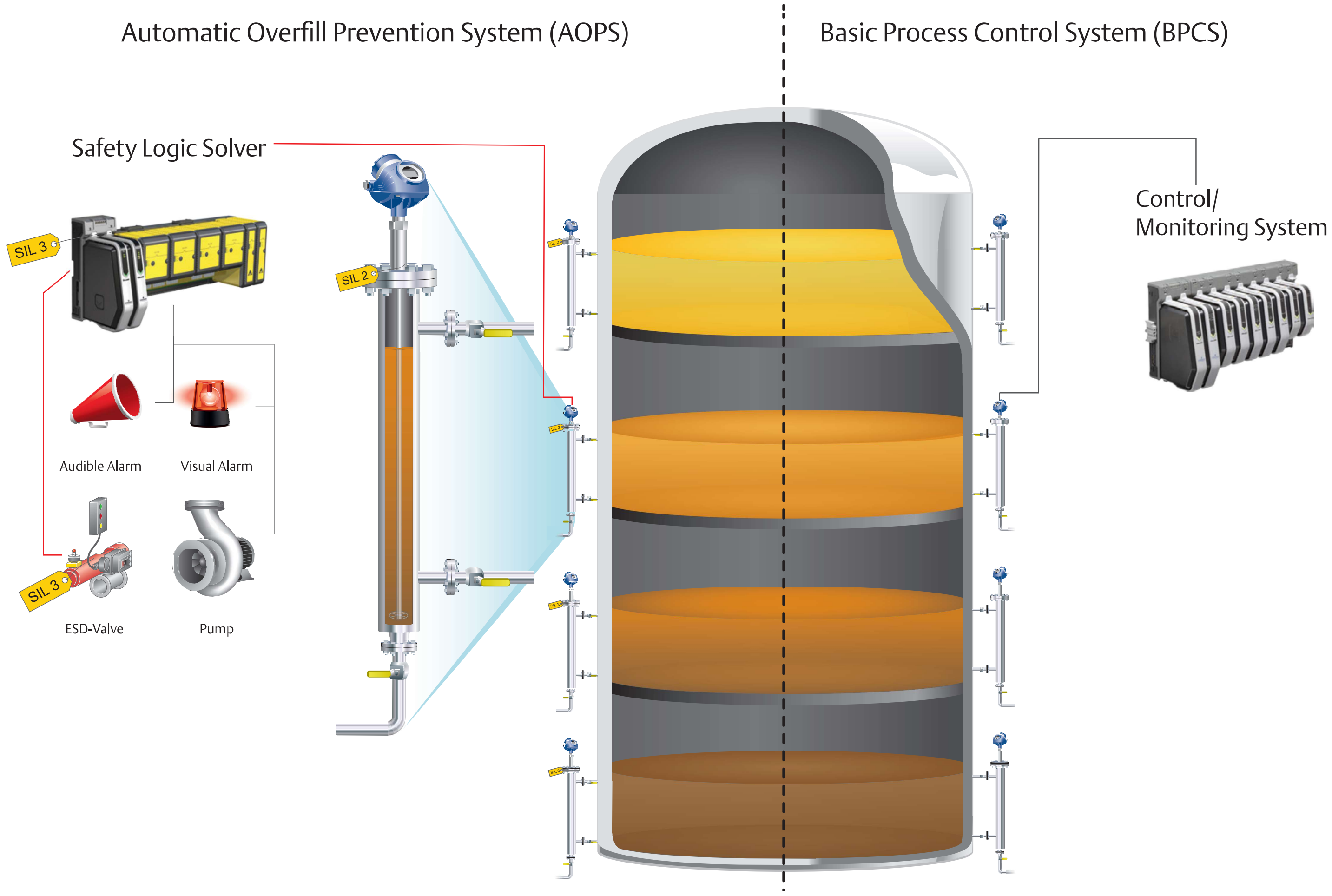
12.2.4 Separator Tank

The separator tank is a vessel that allows fluids to separate into different components. Illustration shows a separator tank equipped BPCS with two Rosemount 5300 for level and interface measurement and SIL2 AOPS and SIL2 dry-run protection based on Rosemount 2100, DeltaV SIS and Bettis actuator.



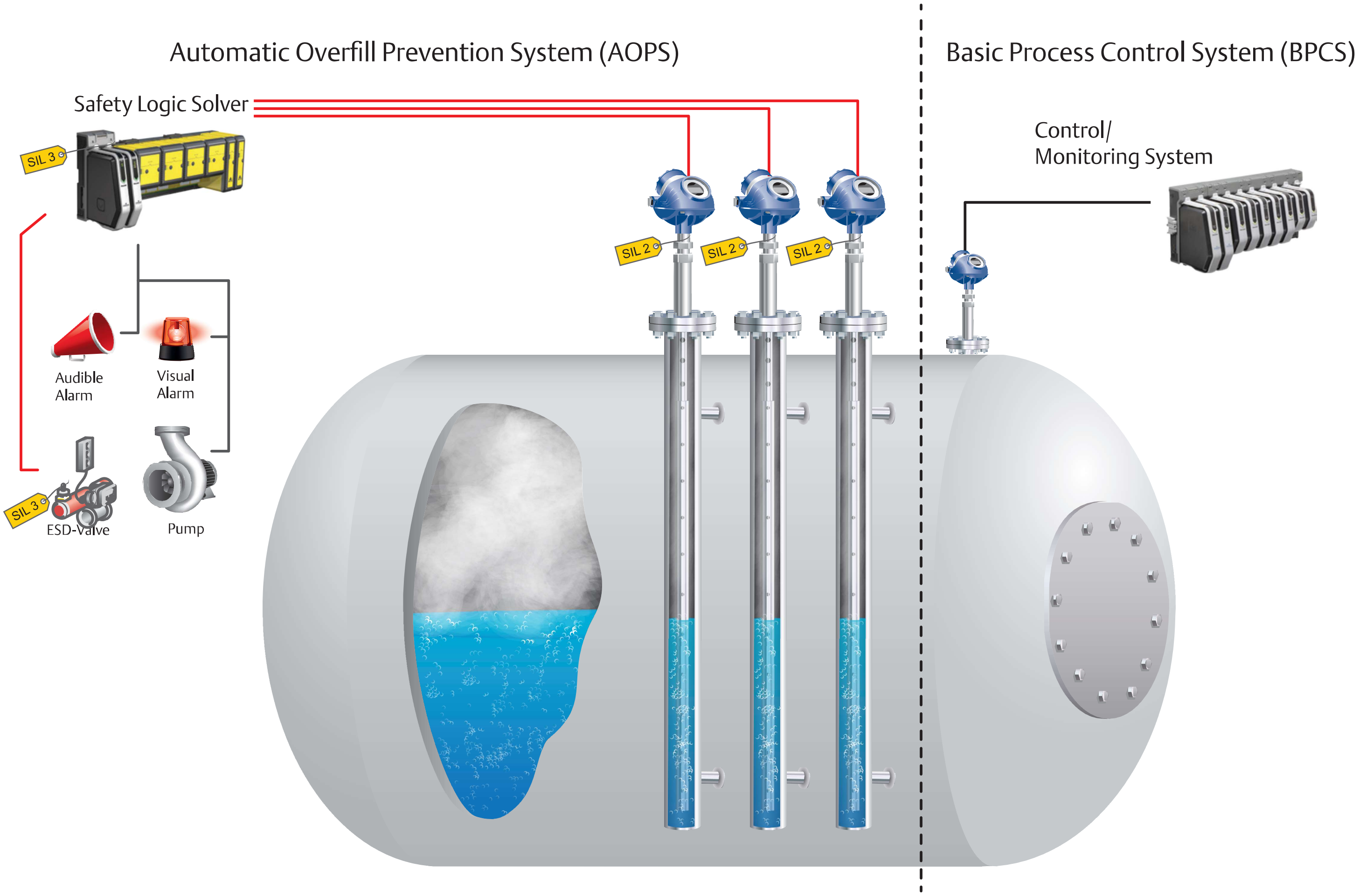
12.2.5 Distillation Column

Distillation columns allow separation of fluid mixtures based upon their boiling points. As vapors rise through the column, different components will condense at different temperatures and accumulate for withdrawal. Illustration shows a distillation column equipped with a BPCS with a Rosemount 5300 for level measurement and SIL2 AOPS based on Rosemount 5300, DeltaV SIS and Bettis actuator.



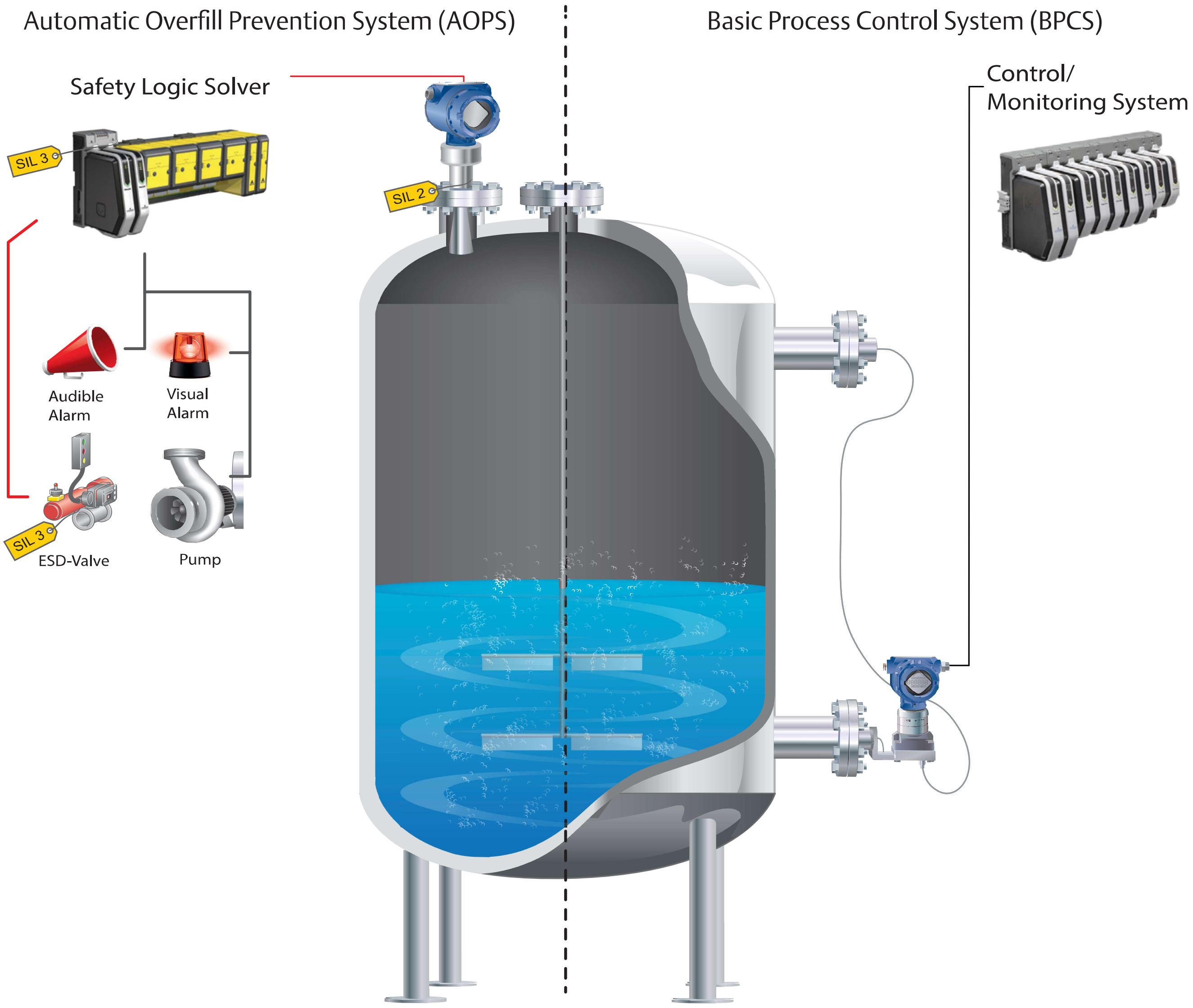
12.2.6 Boiler Drum

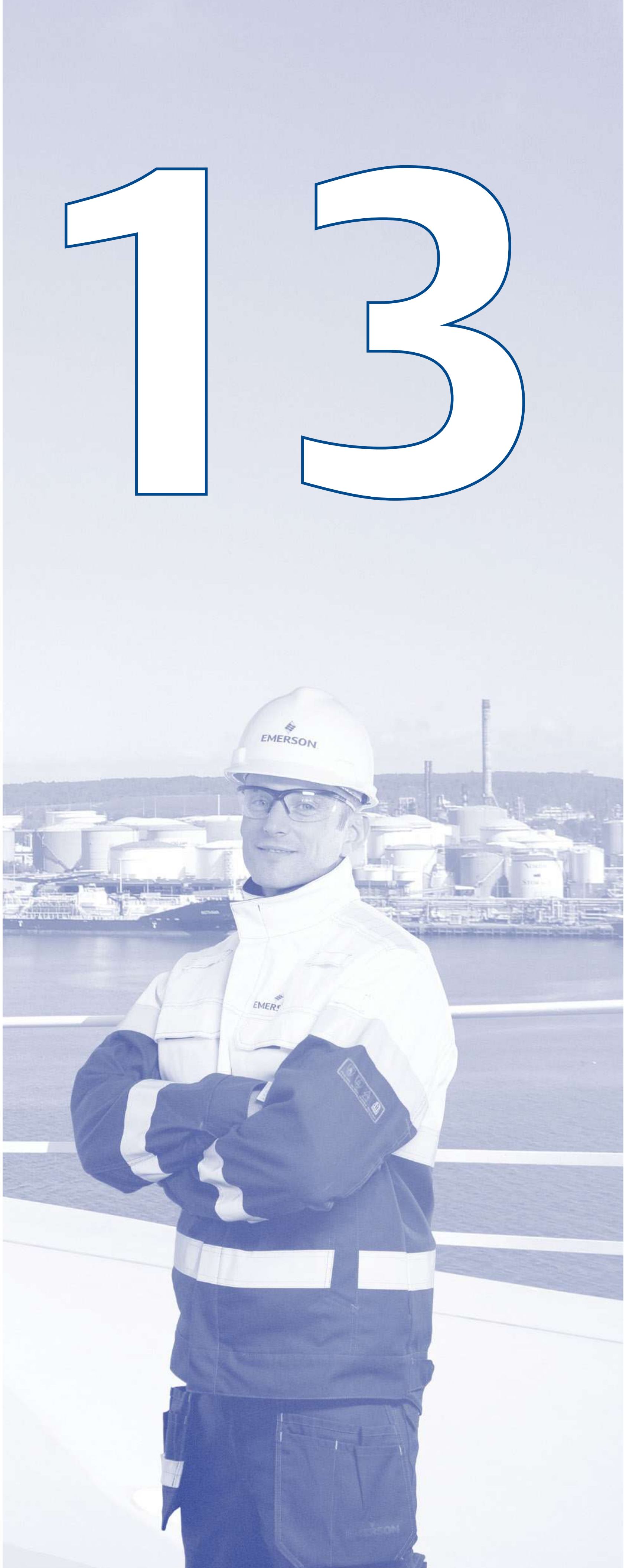
Illustration shows a boiler drum equipped with a BPCS with a Rosemount 5300 for level measurement and SIL3 AOPS based on three Rosemount 5300 (2oo3), DeltaV SIS and Bettis actuator.



12.2.7 Blending Tank

Blending tanks are used for mixing fluids or solids into fluids, usually at ambient conditions. Level measurements are to monitor fluid additions. Illustration shows a blending tank equipped with a BPCS of Rosemount differential pressure level measurement gauge and SIL2 AOPS based on the Rosemount 5408:SIS, DeltaV SIS and Bettis actuctor.





13

References

Topic Page

13. References

13.1 Literature References

American Petroleum Institute (2012) *API 2350. Overfill Protection for Storage Tanks in Petroleum Facilities*, Fourth edition

Central Intelligence Agency (2015) *The World Factbook*, https://www.cia.gov/library/publications/the-world-factbook/rankorder/2246rank.html 2015-09-04

Center for Chemical Process Safety (2007) *Guidelines for Risk Based Process Safety*, Wiley

Control of Major Accident Hazards (2011) *Buncefield: Why did it happened?* http://www.hse.gov.uk/comah/buncefield/buncefield-report.pdf 2015-09-03

Felten, D., (2015) *When Prevention Fails: Managing Your Spill Response*, NISTM 17th Annual International Aboveground Storage Tank Conference & Trade Show, Florida

Goble, W., (2013) *Make the IEC 61511 into a cookbook?* http://www.exida.com/Blog/Make-IEC-61511-into-a-Cookbook#sthash.oqiYamB1.dpuf 2015-07-21

International Electrotechnical Commission (2010) *IEC 61511 Functional safety - Safety instrumented systems for the process industry sector*

International Electrotechnical Commission (2010) *IEC 61508 Functional Safety of Electrical/Electronic/Programmable Electronic Safety-related Systems*

Loren (2005) *BP reveals costs of Texas City settlements*, http://blog.chron.com/lorensteffy/2005/07/bp-reveals-costs-of-texas-city-settlements/ 15-07-17

Marsh & McLennan Companies (2011) *Management of Atmospheric Storage Tank*, Rev 01, United Kingdom

Mars (2007) *Recommendations on the design and operation of fuel storage sites*, Buncefield Major Incident Investigation Board

M B Lal Committee Report (2009) *Independent Inquiry Committee Report on Indian Oil Terminal Fire at Jaipur* http://oisd.gov.in/ 2015-09-04

Puerto Rico Seismic Network (2009) *Informe Especial, Explosión de Caribbean Petroleum en Bayamón,* University of Puerto Rico Mayagüez Campus.

Sreenevasan, R., (2015) *The effect of regulations in improving process safety*, Tetra Tech Proteus, https://www.engineersaustralia.org.au/sites/default/files/shado/Learned%20Groups/Technical%20Societies/Risk%20Engineering%20Society/australian_regulations_res_wa_paper.pdf 2015-07-21

United States Environmental Protection Agency (2014) *Response to Oil Spills*, http://www.epa.gov/ceppo/web/content/learning/response.htm 2015-07-14

U.S. Chemical Safety and Hazard Investigation Board (2015) FINAL INVESTIGATION REPORT CARIBBEAN PETROLEUM TANK TERMINAL EXPLOSION AND MULTIPLE TANK FIRES http://www.csb.gov/assets/1/16/06.09.2015_FINAL_CAPECO_Draft_Report__for_Board_Vote.pdf 2015-09-03

13.2 Picture references

In order of appearance:

Picture 1.1: https://commons.wikimedia.org/wiki/File:Buncefield2.jpg 2015-07-20

Picture 1.2: By Andrea Booher https://commons.wikimedia.org/wiki/File:FEMA_-_7429_-_Photograph_by_

Andrea_Booher_taken_on_12-20-2002_in_Guam.jpg 2015-07-20

Picture 2.1: By Enriquillonyc https://commons.wikimedia.org/wiki/File:2009_Catano_refinery_explosion.jpg 2015-07-20

Picture 2.2: Copyright Emerson

Picture 2.3: https://commons.wikimedia.org/wiki/File:Buncefield.jpg 2015-07-20

Picture 2.4: https://commons.wikimedia.org/wiki/File:Caribbean_Petroleum_Corporation_Disaster.jpg 2015-07-20

Picture 2.5: https://commons.wikimedia.org/wiki/File:Va._Guard_personnel_assist_W.Va._water_collection_operations_140119-Z-BN267-003.jpg 2015-07-20

Picture 2.6: https://pixabay.com/sv/photos/water%20tank/ 2015-07-16

Picture 2.7: https://commons.wikimedia.org/wiki/File:BP_PLANT_EXPLOSION-1_lowres2.jpg 2015-07-20

Picture 2.8: By Jonas Jordan, United States Army Corps of Engineers [Public domain], via Wikimedia Commons http://www.hq.usace.army.mil/history/Kuwait_burn_oilfield.jpg

Picture 3.1: Copyright Emerson

Picture 3.2: Copyright Emerson

Picture 3.3: Copyright Emerson

Picture 3.4: Copyright Emerson

Picture 9.1: “Anacortes Refinery 32017” by Walter Siegmund (talk) - Own work. Licensed under CC BY 2.5 via Commons - https://commons.wikimedia.org/wiki/File:Anacortes_Refinery_32017.JPG#/media/File:Anacortes_Refinery_32017.JPG

About the authors

Author

Phil E. Myers

Phil E. Myers has chaired numerous task groups for the American Petroleum Institute, including API 2350. Currently, he is the director of PEMY Consulting. He has also worked at Chevron Corporation where he was a mechanical integrity specialist for tanks, piping and pressure vessels specializing in safety and risk. Myers holds a BSc in Chemical Engineering from UC Berkeley and an MSc in Theoretical and Applied Statistics from California State University.

Author

AnnCharlott Enberg

AnnCharlott "ACE" Enberg has worked as a Process Safety and Functional Manager for major petrochemical plants in Sweden and Europe for more than 20 years. Enberg says that working with hazards is sometimes about creating order in chaos and clearly defining and prioritizing potentially enormous needs. Safety, technical design, risk assessment, and management is what motivates Enberg. She uses her experience from the petrochemical-oil-energy market within these areas to share and develop new roads.

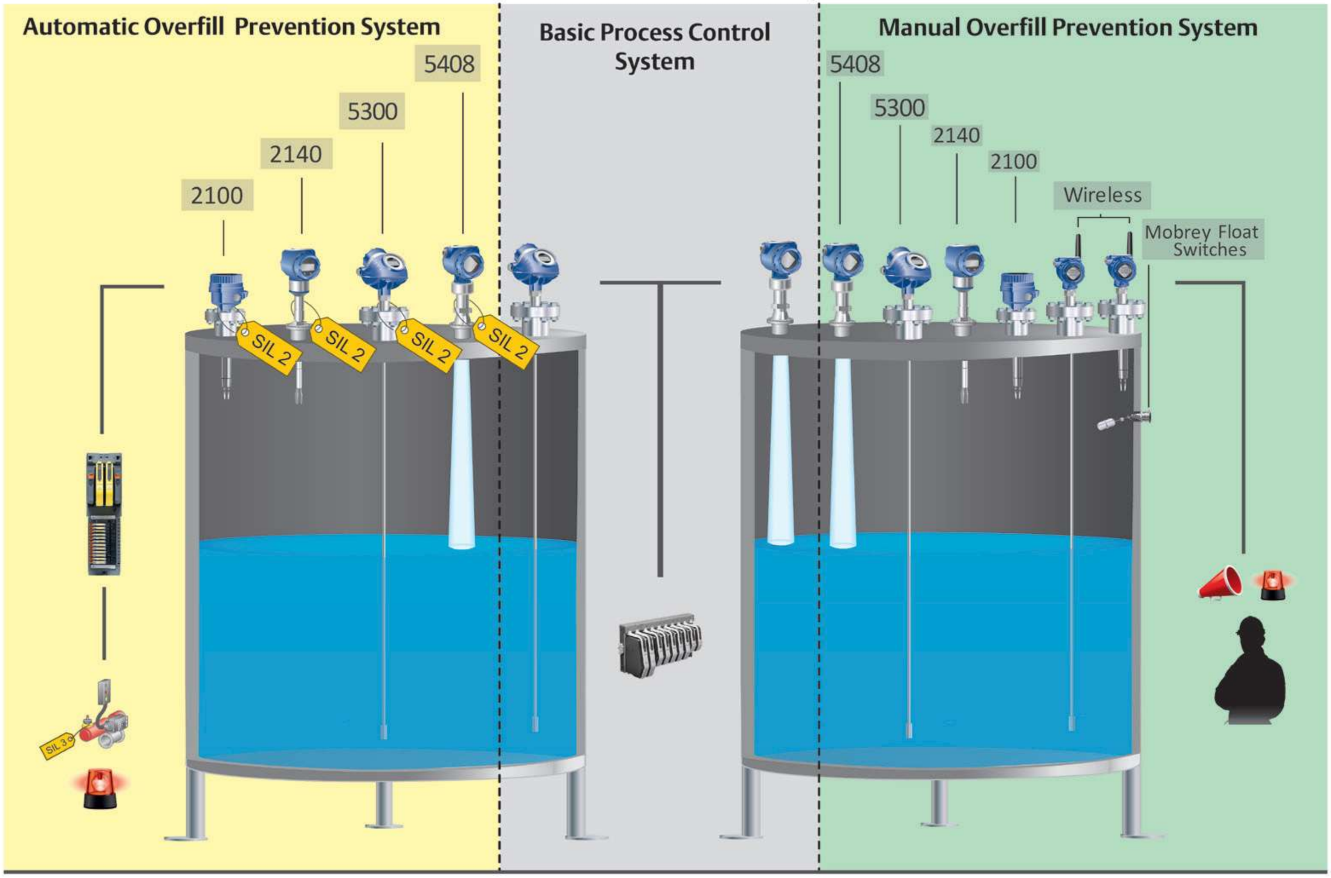
Author

Carl-Johan Roos

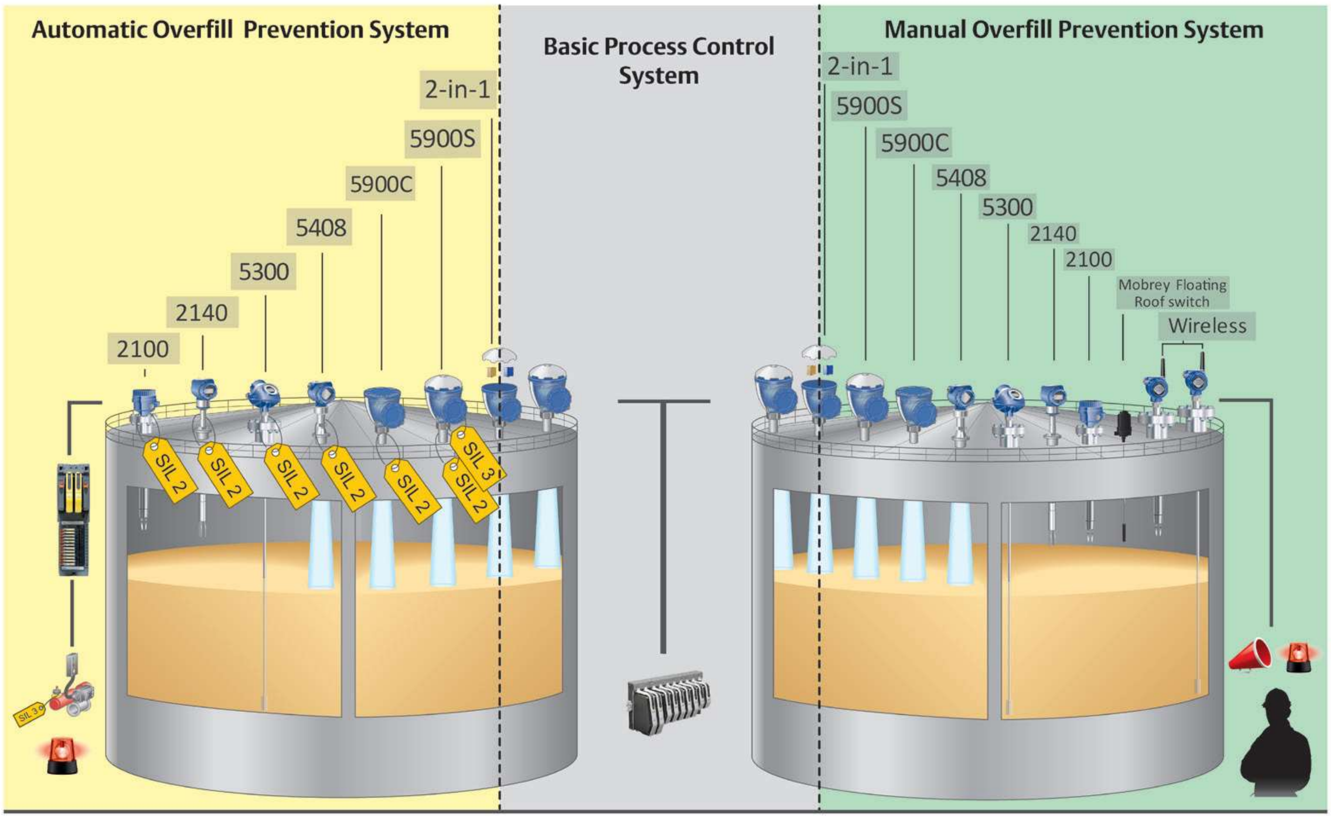
Carl-Johan “CJ” Roos was previously functional safety officer for Process Level and Tank Gauging at Emerson. Besides API2350, he has actively participated in numerous product specific IEC61508 certifications and site specific IEC61511 related projects. Roos has a Masters degree in Electrical and Computer Engineering from Georgia Tech and Chalmers University, and a Masters of Business Administration degree from the University of Gothenburg.

Rosemount products for overfill prevention

Process Industry



Bulk Liquid Industry



Introduction

Why Invest?

Key Elements

Regulatory Requirements

Industry Standards

Risk Assessment

Overfill Management System

Overfill Prevention System

Proof-Testing

Available Technologies

Rosemount Products

Overfill Prevention System Examples

References

Global capabilities

Global Headquarters

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

Europe Regional Office

Emerson Automation Solutions
Neuhofstrasse 19a P.O. Box 1046
CH 6340 Baar
Switzerland
☎ +41 (0) 41 768 6111
📠 +41 (0) 41 768 6300
✉ RFQ.RMD-RCC@Emerson.com

Asia Pacific Regional Office

Emerson Automation Solutions
1 Pandan Crescent
Singapore 128461
☎ +65 6777 8211
📠 +65 6777 0947
✉ Enquiries@AP.Emerson.com

Middle East and Africa Regional Office

Emerson Automation Solutions
Emerson FZE P.O. Box 17033,
Jebel Ali Free Zone - South 2
Dubai, United Arab Emirates
☎ +971 4 8118100
📠 +971 4 8865465
✉ RFQ.RMTMEA@Emerson.com

www.Emerson.com/OverfillPrevention

Recommended retail price $75.99

Youtube.com/user/RosemountMeasurement/
Facebook.com/Rosemount
LinkedIn.com/company/Emerson-Automation-Solutions
Twitter.com/Rosemount_News

ISBN 9789198277906
57599 >
9 789198 277906

Literature reference number: 00805-0100-1042 Rev. DA