Special considerations when using Rosemount 5300 and 5400 Series as the level sensor in Safety Instrumented Systems (SIS)
Section 1: Introduction

Section 2: Recommendations grouped according to IEC 61511 safety life-cycle

2.1 Process Hazard and Risk Analysis (Clause 8), Allocate Safety Function to Protection (Clause 9)

2.2 SIS Safety Requirements Specification (clauses 10 & 12) ................................. 8

2.3 SIS design and engineering (clauses 11 & 12) .................................................... 12

2.3.1 Design Overview ....................................................... 12

2.3.2 Auxiliary Components ................................................ 13

2.3.3 Power Supply .......................................................... 14

2.3.4 Application ............................................................. 15

2.3.5 Measurement Accuracy ................................................ 15

2.3.6 Mechanical Considerations ............................................ 15

2.3.7 Electrical and Mechanical installation ................................................. 19

2.3.8 Transmitter communication ................................................ 20

2.3.9 SIL validation .......................................................... 27

2.3.10 Failure Rates .......................................................... 31

2.3.11 Diversification ......................................................... 32

2.3.12 Demand-mode ......................................................... 32

2.3.13 Response Time ......................................................... 32

2.3.14 SAT ................................................................. 33

2.3.15 Proof-test .............................................................. 33

2.4 FAT: Factory acceptance testing (clause 13) .................................................... 35

2.5 SIS installation and commissioning (clause 14) ................................................. 35

2.6 SIS safety validation (clause 15) ..................................................................... 36

2.7 SIS operation and maintenance (clause 16) ..................................................... 37

2.8 SIS modification (clause 17) ................................................................. 37

Appendix A: IEC 61511 safety life-cycle overview
Section 1 Introduction

The intention of this document is to provide guidance for the special considerations that are unique, unusual or commonly overlooked when applying Rosemount 5300 and 5400 process radar transmitters as level sensors in safety instrumented systems (SIS). Consequently this document is a complement, rather than a replacement, to other available product documentation such as data sheets, manuals and drawings. The document may be viewed as an informal version of IEC 61511-2 “Guidelines for the application of IEC 61511-1“ with a limited and very specific scope.

There is no guarantee that this document is complete; if in doubt, turn to the original sources (IEC 61511, IEC 61508, Manuals, Product Data Sheets).

Safety Instrumented Systems (SIS) is a generic term usually referring to functional safety systems based on IEC 61508 or one of its descendants (Figure 1-1). These include a number of different types of systems such as Emergency Shutdown Systems (ESD), Burner Management Systems (BMS), Fire and Gas Systems (F&G), Critical Turbomachinery Control, Railway Switching, Semiconductor Life Safety Systems (SEMI S2), Nuclear Safety Systems and High Integrity Pressure Protection System (HIPPS). This document is however limited to ESDs used in the process industry, and thereby the scope is limited to IEC 61511. Parts of this document may however also be relevant for ESDs that are partially, or not at all, designed per IEC 61511.

Figure 1-1. Relation between the generic standard for safety instrumented systems, IEC 61508, and industry-specific descendants

A SIS is built-up of one or more safety instrumented functions (SIF). Figure 1-2 depicts a generic SIF which principally consists of three elements: sensor, logic and actuator. It is the behavior of the complete SIF that is relevant, rather than the specific sub-elements. And although the view of IEC 61511 is the complete SIF this document will only address the sensor sub-element due to the limitation in scope to process radar level transmitters. To ensure the distinction and avoid
confusion this text will therefore use the prefix ‘Sensor’ wherever relevant, e.g. ‘Sensor-Response Time’ and ‘Sensor-PFD$_{avg}$’.

**Figure 1-2. Generic Safety Instrumented Function (SIF) per IEC 61511. The scope of this document is the sensor specifically.**

![Diagram of Sensor-Logic-Actuator](image)

Level sensors can be applied in different use-cases such as roof-tilt measurement, dike fluid monitoring, leak detection and open channel flow measurement. The scope of this document is however limited to the following level sensor ESD use-cases:

- **Overfill prevention**: Level Alarm High High (LAHH), and optionally Level Alarm High (LAH)
- **Dry-run prevention**: Level Alarm Low Low (LALL), and optionally Level Alarm Low (LAL)

Thereby the document also indirectly covers level deviation monitoring applications commonly used in continuous processes to maintain a narrow interval of level (since these consists of overfill and dry-run prevention alarms combined). The scope is also limited to liquids.

A typical example design of a SIF for these ESD use-cases is exemplified in **Figure 1-3**. When the level is too high and/or too low depending on the use-case, the logic solver will take the process to a safe state by communicating with the actuator. In this example the actuator consists of one (or multiple) valves that shutdowns or diverts the flow of incoming or outgoing product. Other types of ESDs may consist of different types of actuators that for example stop a chemical reaction or prevent over/under-pressure.

**Figure 1-3. Overview typical ESD for overfill prevention and/or dry-run protection using Emerson equipment**

![Diagram of ESD setup](image)
Although there exist safety-rated digital and wireless communication protocols this document will assume the usage of wired 4-20mA communication since this is what the overwhelming majority of functional safety installations today use (1).

**IEC 61511 Safety Life-cycle**

According to IEC 61511, SIFs shall be planned, designed, commissioned, operated, maintained, and decommissioned according to the safety life-cycle depicted in Figure 1-4. This process consists of a number of individual steps. To ensure simplicity and completeness the remainder of this document has been structured accordingly (similarly to IEC 61511-2). The document does however not cover the life-cycle phases 'Management of Functional Safety and Functional Safety Assessment', 'Safety Lifecycle Structure and Planning' and 'Verification' due to their generic nature and tight connection to a proper functional safety management system (rather than the equipment in the SIF).

**Figure 1-4. The Safety lifecycle according to IEC 61511-1 (the clauses refer to the specific chapters in the standard). A brief description of the individual steps is available in Appendix A.**

The correct operation of a functional safety system is dependent upon all the phases in the life-cycle, which a study of a number of accidents in the process industry by the HSE(UK) clearly shows in Figure 1-5.

Figure 1-5. Causes for accidents according to government investigation "Out of control" by the HSE (UK)
Section 2: Recommendations grouped according to IEC 61511 safety life-cycle

Each chapter in this section corresponds to one or more steps in the IEC 61511 safety life-cycle which is depicted in Figure 1-4. A description of the individual steps is available in Appendix A.

2.1 Process Hazard and Risk Analysis (Clause 8), Allocate Safety Function to Protection (Clause 9)

The owner/operator is ultimately responsible for the creation of a risk assessment, deciding the tolerable risk, safety function allocation, safety margins and the selection of a safety integrity level (SIL).

Emerson does however have a wide experience in the field of functional safety and can for example upon request provide input data to the risk assessment concerning product failure rates, see Table 2-1. Alternatively, if the radar level transmitter is equipped with an IEC 61508 certificate, refer to the corresponding FMEDA-data.

Table 2-1. Field demonstrated mean time between failures (MTBF)
Source: Rosemount MTBF-documents (February 2013)

<table>
<thead>
<tr>
<th>Product</th>
<th>Sensor-MTBF</th>
<th>Sensor - λ</th>
</tr>
</thead>
<tbody>
<tr>
<td>3300</td>
<td>760 years</td>
<td>150 FIT</td>
</tr>
<tr>
<td>5300</td>
<td>186 years</td>
<td>613 FIT</td>
</tr>
<tr>
<td>5400</td>
<td>226 years</td>
<td>505 FIT</td>
</tr>
</tbody>
</table>

Contact your local Emerson representative to obtain the most recent MTBF-document exemplified in Figure 2-1.
Sometimes the question arises how many of the field-demonstrated failures (denoted Sensor-\(\lambda\) in Table 2-1) can be qualified as dangerous undetected failures (\(\lambda_{DU}\)) and thereby contribute to the probability of failure on demand (PFD). This data is not available, and therefore it has to be estimated. Exactly what method to use is the responsibility of the owner/operator, but below are some examples:

1. **Max conservative method**: Assume that all failures are dangerous, which corresponds to a Safe Failure Fraction (SFF) = 0, and consequently Sensor-\(\lambda_{DU}\) = Sensor-\(\lambda\).

2. **Medium conservative method**: Assume SFF = 60% which corresponds to the SIL 0 / SIL 1 limit according to IEC 61508-2 table 3, and consequently Sensor-\(\lambda_{DU}\) = Sensor-\(\lambda\) * (100-60)% = Sensor-\(\lambda\) * 40%

3. **Least conservative method**: Both the hardware and diagnostic coverage is approximately the same for Rosemount 5300 and 5400 units purchased with and without the ‘SIL-option’ (QT/QS model-code), therefore a reasonable approximation is to assume that the SFFs equal the FMEDA-reports, and consequently Sensor-\(\lambda_{DU}\) = Sensor-\(\lambda\) * (100% - SFFFMEDA)

Radar Level Transmitters have relatively low failure rates which result in large risk reduction factors (RRF). It is however important to note the limitation in IEC 61511 of max RRF=10 for a non-IEC 61511 compliant independent protection layer (IPL) such as a non-SIS BPCS-layer.

Although not unique to process radar level gauges, please note that IEC 61511 contains requirements for preventing common cause, common mode and dependent failures. If this assumption is made during the risk assessment (which almost always is the case), associated requirements shall be reflected in the Safety Requirement Specification (SRS).

What methodology and information to include in the risk assessment is ultimately the responsibility of the owner/operator. In this context it is however relevant to mention the minimum likelihood and consequence factors that shall be taken into account according to API 2350, which are listed in Table 2-2. Although the scope of API 2350 is limited to overfill..
protection in atmospheric bulk liquid storage tanks containing petroleum products and therefore often not applicable to process level applications, these factors can often still serve as valuable input when assessing the risk for tank overfills.

Table 2-2. Minimum likelihood and consequence factors to include in a risk assessment for tank overfills according to API 2350

<table>
<thead>
<tr>
<th>Probability</th>
<th>Consequence</th>
</tr>
</thead>
<tbody>
<tr>
<td>Frequency, rate and duration of filling</td>
<td>Hazard characteristics of material (product) in tank</td>
</tr>
<tr>
<td>Systems used to properly measure and size receipts to tanks</td>
<td>Volatility, flammability, dispersion, VCE potential</td>
</tr>
<tr>
<td>Accurate tank calibration (both strapping and verified critical high)</td>
<td>Number of people onsite who may be affected by a tank overflowing</td>
</tr>
<tr>
<td>Systems used to monitor receipts</td>
<td>Number of people offsite who may be affected by a tank overflowing</td>
</tr>
<tr>
<td>Extent of monitoring and supervision of manual and automatic tank gauging</td>
<td>Possibility of a tank overflowing resulting in (escalation) of hazardous events onsite or offsite</td>
</tr>
<tr>
<td>Impact of complexity and operating environment on the ability of operating personnel to execute overfill prevention tasks</td>
<td>Possibility of impact to nearby sensitive environmental receptors</td>
</tr>
<tr>
<td>Filling multiple tanks simultaneously</td>
<td>Physical and chemical properties of product released during overflowing</td>
</tr>
<tr>
<td>Switching tanks during receipt</td>
<td>Maximum potential overfill flow rates and duration</td>
</tr>
</tbody>
</table>

When allocating the safety function, diversity needs to be taken into consideration, but it is not a requirement according to IEC 61511. In practice this means that the same type of sensor can be used for both the SIS- and BPCS-layers (e.g. 2x5300 or 2x5400) or SIFs with HFT (e.g. 1oo2, 2oo3) - if proper precautions that fulfill the required SIL have been taken to avoid systematic failures. This property is denoted ‘systematic capability’ and shall be presented by manufacturers in the specific product’s IEC 61508 certificate. Further details are presented in section SIS design and engineering (clauses 11 & 12).

Theoretically, the SIF does not have to be designed according to IEC 61511 in case the required RRF is below 10. The tolerable risk levels may however change over time, e.g. due to new owner/operator or the risk may increase e.g. due to liquid product change, upgraded pumps which increase max flow-rates, etc. To future proof the investment, it is therefore advisable to use IEC 61511-compliant equipment in all functional safety applications, independently of whether they are SIL 0, 1, 2, 3 or 4. Additionally, the available data when purchasing equipment designed for safety applications usually simplifies the implementation and thereby immediately returns the additional initial capital expenditure (CAPEX).
2.2 SIS Safety Requirements Specification (clauses 10 & 12)

Emerson has in-depth knowledge and experience in overfill prevention systems (OPS), dry-run prevention systems and level deviation monitoring systems and can provide valuable guidance and input during the creation of a Safety Requirement Specification (SRS) for these use-cases. Upon request, Emerson Process Management’s system division has a team of functional safety consultants that offers the service to write the entire SRS. Additional information is available in Figure 2-2.

The SRS shall define the SIF’s minimum acceptable SIL. Most SIFs in the process industry are designed to fulfill SIL 0, 1 or 2, corresponding to a minimum risk reduction factor (RRF) of 1-10, 10-100 and 100-1,000 respectively. If the risk assessment indicates higher need for risk reduction then commonly the inherent process is re-designed because the risk levels are considered unacceptable.

Although not explicitly required by IEC 61511, it is indirectly required to specify the SIF’s minimum required mission time (replacement interval) to fulfill the life-cycle requirements. While doing this, it is also important to take the useful life-time of the equipment into account. Specific values for the Rosemount 5300 and 5400 Series are presented in the section SIS design and engineering (clauses 11 & 12).
Intuitively the safe state may be believed to be obvious but according to IEC 61511 it needs to be strictly defined and documented in the SRS. Often it is advisable with a narrow and limited definition of the safe state to limit the complexity and cost of the SIF. For an AOPS this typically means that the SIF’s functionality is limited to stopping or diverting the flow of incoming product into the tank, but not to actively pump product to empty/fill the tank, to reach the safe state.

Another requirement in the SRS is to forecast the source and rate of demands. This information can usually be retrieved from the risk assessment. If an appropriate BPCS is in use, the result in level applications is virtually always low demand mode (less than once per year).

Since the SIF is activated infrequently in the low demand mode, proof-testing is commonly employed to ensure that the SIF is functioning correctly and thereby lower the average probability of failure on demand (PFD\text{avg}) to reach the required SIL. Maximum allowable proof-test interval for the entire SIF, which depends on a number of factors, is a requirement that needs to be included in the SRS (if demand mode application) and it is ultimately the responsibility of the owner/operator. Specific values for the Rosemount 5300 and 5400 Series are presented in the section SIS design and engineering (clauses 11 & 12) and can be used as a guideline. In addition to IEC 61511, also other sources of requirements may exist that shall be taken into account. Sometimes local regulations and/or company standards dictate the proof-test intervals with fixed requirements such as once per annum or once per tank/process/facility/site turnaround.

Although not required by IEC 61511, it is highly advisable to include other properties related to the proof-test in the SRS such as minimum allowable coverage factor (‘quality of the proof-test’), influence on the process and personal safety requirements during the test. Examples of such requirements are presented below in the paragraph with the listing of recommended but non-mandatory requirements to be included in the SRS.

Another mandatory SRS requirement is to define the entire SIF’s maximum acceptable response-time and to describe the ESD’s trip-point(s). In this context, the ultimate SIF trip-point where the process shall be brought into a safe state is usually denoted ‘Level Alarm High High’ (LAHH) or ‘Level Alarm Low Low’ (LALL) according to common industry practice. ‘Hi-Alert’ and/or ‘Low-Alert’ may be used as complementary indications, but are optional, and usually tied primarily to the BPCS.

The entire SIF’s accumulated max response-time shall be defined in the SRS but there is no requirement to specify each sub-element’s response time. Since the SIF contains of primarily sensor(s), logic solver(s) and actuator(s) these need to be understood to have reasonable expectations on the entire SIF’s realistic response-time. To ensure that the SIF can be implemented in practice, typical (but fairly conservative) figures for level sensor response-time is around 20 - 30 seconds to achieve stated accuracy upon a step change at max level-rates including filtering factors in the logic solver. Additionally, depending on the safety logic solver’s capability to discriminate sensor-alarms from normal measurements, the alarm delays to mask transmitter restarts may have to be taken into account. Further details are found in the section Transmitter communication.

As a comparison: the overfill prevention standard for large petroleum atmospheric storage tanks, API 2350, prescribes a default response time of 15 minutes for tanks with level measurement and independent OPS (category 3 per API 2350 classification).

When documenting the startup requirements for the SIF, it shall be taken into account that the Rosemount 5300 and 5400 Series typically have 40 seconds startup-time, refer to Figure 2-15 and Figure 2-16.
It is also relevant to mention the importance of properly specifying the environmental extremes as defined and required by IEC 61511 since these may have implications on the selection of the transmitter, probe/antenna and accessories such as isolators, barriers and power-supplies. These extremes include (but are not limited to) “ambient temperature, humidity, contaminants, grounding, electromagnetic interference/radiofrequency interference (EMI/RFI), shock/vibration, electrostatic discharge, electrical area classification, flooding, lightning, and other related factors” (IEC 61511-1 10.3.1).

The SRS shall include all the requirements for the SIF. This also includes requirements not originating from IEC 61511, such as company standards and local regulations. The local Emerson representative has a wide experience in this field and can provide local support upon request.

Although not required, the following non-mandatory SRS requirements may also be relevant:

- Sensor communication shall be fail-safe analog 4-20mA signal
- Sensor shall have no moving parts to avoid the potential for wear-out failures and application related systematic failures such as ‘getting stuck’
- The measurement technology shall measure the liquid’s product surface directly to reduce the number of potential error sources (e.g. incorrect density-setting when pressure used to measure level)
- The SRS shall specify the level sensor’s required measuring range
- To future proof the investment, the alarm (and optional alerts) shall be adjustable within the specified measuring range. Additionally, correct operation of the sensor shall be possible to validate ‘on-line’, ‘in-situ’ and remotely. This requires a sensor with continuous level measurement and digital communication
- Sensor shall be equipped with an externally visible integral display to allow for local read-out
- In the event of sensor failure, the following criteria need to be fulfilled to ensure an efficient exchange procedure that minimizes the risk
  - Written sensor exchange instructions authored by the manufacturer
  - Sensor electronics (e.g. sensor head) and wetted parts (e.g. antenna/probe) shall be separate, and individually replaceable. Matching between individual electronics and individual wetted parts shall not be required.
  - It shall be possible to download and backup a sensor’s configuration data, and then upload this data to a replacement sensor to restore the original sensor’s configuration
  - The facility shall maintain an adequate inventory of spare-parts. Manufacturer shall provide a proposed spare-parts list. The required spare-parts inventory and associated cost shall be taken under consideration when selecting sensor
- To detect systematic failures, the sensor shall have a written site-acceptance test (SAT) procedure authored by the manufacturer
- To detect random hardware failures, the sensor shall have written proof-test procedures authored by the manufacturer that fulfill the following requirements:
  - multiple proof-test procedures shall be available where
  - at least one procedure has a coverage factor above 90%
* at least one procedure is a 'partial proof-test' that does not affect the process nor the sensor communication output during the test

* each proof-test shall be documented in the safety manual describing test-instruction and coverage factor (percentage of Sensor-$\lambda_{\text{DU}}$ detected).

° proof-test procedure shall not require personnel to physically visit the tank (due to the associated risks)

° proof-test procedure shall not expose the facility/tank to a dangerous state (e.g. moving liquid surface above LAHH)

It shall be possible to continuously perform a 'partial proof-testing' by comparing the BPCS and SIS level sensors' deviation between each other, 'level delta measurement':

° this functionality shall be implemented in the BPCS to avoid the risk of impacting the SIF

° The partial-test coverage factor (percentage of Sensor-$\lambda_{\text{DU}}$ detected) shall be specified in the safety manual

The physical sensor location shall allow for visual inspection
2.3 SIS design and engineering (clauses 11 & 12)

2.3.1 Design Overview

The most common SIF involving level sensors is designed with a valve as the actuator and without redundancy to fulfill SIL 0, 1 or 2 as presented in Figure 2-3.

![Figure 2-3. Principal Overview typical SIL 0, 1 or 2 Automatic Overfill Prevention System (AOPS). Logic condition for dry-run prevention systems: <
Logic condition for level deviation prevention systems: <>](image)

There exist however many examples where SIFs are designed with hardware fault tolerance. Typically the primary target for hardware fault tolerance is the actuator since this is the statistically most likely component to fail, but this design-technique is becoming increasingly popular also for the sensor, as depicted in Figure 2-4. The key reasons behind this trend are:

1. Spurious trips reduction by using 2oo3 voting
2. Proof-test frequency reduction by using 1oo2 or 2oo3 configurations that reduce the SIF’s PFD
3. Fulfilling SIL 3 requirements by using multiple sensors in 1oo2 or 2oo3 configurations (relatively uncommon in today’s process industry)

![Figure 2-4. Example Automatic Overfill Prevention System (AOPS) with 2oo3 sensor voting.](image)

Often it is useful and convenient to tie additional functionality to the SIF. Frequently used functionality is to for example shutting down pumps or alerting operators/maintenance personnel thru audiovisual alerts. Components not required to bring the process to a safe state is usually not considered as a part of the SIF and consequently do not have to be designed according to IEC 61511 - if proven that they cannot deteriorate the functionality of the SIF.
typical example is presented in Figure 2-5. According to IEC 61511-1 10.3.1: “Non-safety instrumented functions may be carried out by the SIS to ensure orderly shutdown or faster start-up. These should be separated from the safety instrumented functions”. An additional consequence of this is that the High-Alert (LAH) and Low-Alert (LAL) set-points usually are not safety rated.

Figure 2-5. Example AOPS where the SIF consists of a sensor, logic solver and actuator, which are marked red to indicate their need for compliance with IEC 61511. The pump and the audiovisual alarm are not required to reach the safe state and thereby do not have to be designed according to IEC 61511.

2.3.2 Auxiliary Components

SIFs are traditionally, and previously in this document, separated into Sensor, Logic-Solver and Actuator. In practice each of these functional blocks may consist of sub-components that all have to be taken into consideration when implementing the SIF. In level measurement applications the sensor functional block often consists of a level transmitter and auxiliary components such as power-supply (with or without backup-power), barriers (e.g. for intrinsic safety, surge, lightning or short circuit protection) and/or isolators (e.g. for ground voltage protection) as depicted in Figure 2-6. The scope of this document is limited to the level transmitter, but where relevant other relevant components will be discussed at a non-product specific overview perspective.
Section 2: Recommendations grouped according to IEC 61511 safety life-cycle

Figure 2-6. When implementing a SIF in practice each functional block usually consists of multiple components. In this specific example, the sensor consists of a level transmitter, power-supply and optional barriers and/or isolators.

Although the scope of this document is the level transmitter specifically, it is worthwhile mentioning the following general remarks for the sensor’s auxiliary components:

- All components in the SIF need to be evaluated against IEC 61511
- The ‘SIL-calculations’ shall include all components in the SIF. Consequently, each component needs to have failure data available
- Also the auxiliary components need to be included when evaluating common cause, common mode and dependent failures
- All components shall be taken into consideration during all steps of the safety life-cycle such as proof-testing, site acceptance testing (SAT) and response time determination
- The different components may be assigned different proof-test intervals

In practice the auxiliary components are often not included in the ‘SIL calculations’ due to their low impact on the overall dangerous undetected failure rates. This is ultimately the responsibility of the owner/operator, but it is important to emphasize the correct operation of also these and to properly understand their failure modes to end up with a sensor-subsystem functioning as expected.

2.3.3 Power Supply

It is recommendable, but not a requirement, to use a separate UPS-backed power-supply for the SIS level sensor independent from the BPCS level sensor. The exact power supply requirements are listed in the respective product manual. The requirements for the UPS are dependent upon the specific transmitter power-supply used but in principle the Rosemount 5300 and 5400 have the same requirements as any other analog 4-20mA transmitter in this respect.

Often UPSs cause small power variations (‘glitches’) when switching over from on-line to battery backed power. This may cause the Rosemount 5300 and 5400 to restart which ultimately may result in spurious trips. The exact behavior of the UPS in conjunction with the level sensor is difficult to predict and it is therefore recommendable to test this behavior during the SAT and if required, configure the safety logic solver as described in section Transmitter communication to avoid spurious trips.
2.3.4 Application

One of the most critical aspects for a correctly functioning level sensor is to select the correct measurement technology and product for the specific application. In principle, there is no difference between selecting a Rosemount 5300 and 5400 Series for use in the BPCS- or Safety-layers. Consequently the same recommendations apply, and existing literature on this topic can be used. The Rosemount 5300 and 5400 SIS-models do however have some limitations in the available product options offering that may limit the application range compared to non-SIS transmitters. Consequently, it is recommended to specifically verify that the selected model-code is available with the SIS model-code options in the product data sheet (PDS).

Specific for safety applications is that the SRS may provide additional application information and requirements that have to be taken into consideration. These may for example include:

- Information about the demand. This may for example include the source of the demand and how it affects the measurement conditions, or concurrent events that impact measurement conditions (e.g. boiling surface due to chemical reactions or clogging due to changes in product temperature).
- Information about the ESD set-point(s) and factors that may affect the measurement conditions in this part of the tank. This may for example include the internal tank structure, location of agitator blades and liquid product inlets or outlets.
- Information about max flow rates must be converted into max level rates and verified against the sensor specification. It is also important to ensure that the max level rate is valid throughout the intended measuring range and especially at and in the vicinity of the ESD set-point(s). This is especially important in case of tanks with varying circumferences (e.g. a bullet tank or a tank with cone-shaped bottom).

Finally, IEC 61511-1 provides some additional guidance for the selection of sensors in the clause 11.6.1: “Conditions that should be considered include corrosion, freezing of materials in pipes, suspended solids, polymerization, cooking, temperature and pressure extremes, condensation in dry-leg impulse lines, and insufficient condensation in wet-leg impulse lines.”

2.3.5 Measurement Accuracy

The accuracy of the safety-rated 4-20mA signal is 2% of the configured 4-20 mA range (‘safety accuracy’). HART™ communication can be used to obtain non-safety rated measurements with accuracy per the specification in the product data sheets.

2.3.6 Mechanical Considerations

At a minimum the level transmitter’s effective measuring range needs to include the ESD set-point(s) and fulfill any additional requirements in the SRS. For operational purposes such as early alerts, it is however advisable to use a level transmitter with as large measuring range as possible preferably encompassing the entire tank. All devices do however have limitations in the measuring range, and these are discussed in detail below for the Rosemount 5300 and 5400 Series. Also note that the effective measuring range is limited by the transmitter’s configuration and the scaling of the 4-20mA signal, which is described in subsequent section Transmitter communication.
Although not ideal, it is possible to use Rosemount 5300 in chambers that normally are fully immersed in dry-prevention applications (Figure 2-7). The transmitter may need installation specific configuration and in the case that the High Temperature High Pressure (HTHP) seal is used it is recommended that a Rosemount certified service engineer conducts the transmitter configuration.

**Rosemount 5300 Series**

The measuring range is dependent on a number of application factors such as the liquid product being measured, measurement conditions and the type and length of the selected probe. Consequently, the measuring range for the specific application and model selection needs to be verified against the product data sheet (PDS).

Additionally, the measuring range is limited by the blind zones at the very top and bottom of the probe. In the Blind Zones, the accuracy exceeds ±30 mm (1.18 in.), and measurements may not be possible. Measurements close to the blind zones will have reduced accuracy Figure 2-8 illustrates how the measuring range is related to the blind zones and the areas with reduced accuracy. Values for different probe types and dielectric constants are presented in the product’s manual.
As a result of these limitations:

- the ESD set-point must be located outside the blind zones
- It is not recommended to locate the ESD set-point inside the upper reduced accuracy zone. If this is the case, usage of a spool-piece to move the ESD set-point(s) outside this zone is recommended, refer to Figure 2-9
- in case the ESD set-point is located within, or close to, the lower reduced accuracy zone then the reduced accuracy needs to be taken into account when determining for example the ESD set-point and alarm dead-band settings
Rosemount 5400 Series

The measuring range is dependent on a number of application factors such as the liquid product being measured, measurement conditions and the type of antenna. Consequently, the measuring range for the specific application and model selection needs to be verified against the product data sheet (PDS).

Additionally, the measuring range is limited by the transition zone and near zone as depicted in Figure 2-10. Transition zones are areas where measurements are not recommended. Near zones are areas where the accuracy is reduced. Values for different antenna types presented in the product’s manual.

Figure 2-10. Rosemount 5400 Series transition- and near zones

As a result of these limitations:

- the ESD set-point needs to be outside the transition zone, and preferably also outside the near zone where the accuracy is reduced
- in case the ESD set-point is within, or close to, the near zone then the reduced accuracy needs to be taken into account when determining e.g. the ESD set-point(s) and alarm dead-band settings

Also measurements close to the tank bottom may have reduced accuracy depending on the tank type and other installation specific limitations. Contact your local Emerson representative with application specific data for more information.
Mechanical Considerations

When determining the effective measurement range mechanical factors shall also be taken into consideration:

- The limitations in the Rosemount 5300 and 5400’s measuring range close to the probe/antenna are referenced from the transmitter’s flange. What is the vertical position of the transmitter’s process connection and if needed, can it be elevated using a spool-piece (Figure 2-9)?

- In case a pipe is used, the effective measurement range may also be limited by the length of the pipe.

- In case a chamber (bridle) is used, the effective measuring range is limited by the location of the upper and lower process connections as depicted in Figure 2-11. It is advisable to design the chamber’s top-side sufficiently large to include the Rosemount 5300’s upper blind- and reduced accuracy zones to maximize the effective measuring range. In case of existing installations, a spool-piece can be used to achieve this purpose (Figure 2-9).

![Figure 2-11. The effective measuring range in a chamber is limited by the upper and lower process connections.](image)

2.3.7 Electrical and Mechanical installation

In principle, the mechanical and electrical installation of the Rosemount 5300 and 5400 Series are identical independently of whether they are used in the BPCS- or Safety layers. Consequently the same recommendations apply, and existing literature and drawings on this topic can be used.
There are however some generic requirements related to IEC 61511 that may be relevant to also take into considerations:

- Dedicated electrical wiring that is separate (e.g. use different cable trays) from the BPCS-sensor is a requirement if the SIF is to be considered as an IPL
- IEC 61511 requires sensors to be periodically visually inspected. Consequently the physical location of the transmitter needs to take this requirement into account
- The selected SAT or proof-test procedures may have implications on the electrical and mechanical installation. For example, it may be a requirement to have the possibility to
  - connect a multimeter to the electrical loop (in-case the safety logic solver is not used for this functionality)
  - drain capabilities in the chamber to alter the liquid surface location

Rosemount 5300 and 5400 series with explosion- and flame-proof hazardous location approvals have a built-in intrinsically safe barrier which is referenced to the ground. Therefore the following considerations need to be taken into account when using transmitters with these specific approvals:

- Common-mode voltages shall be avoided. For example, certain earth leak detectors which are based on this principle cannot be used together with the Rosemount 5300 and 5400 Series.
- Ground-potential differences shall be avoided. In case this is a problem, it is recommended to install an isolator as described in Figure 2-12. Upon temporary problems, e.g. due to lightning, ground-potentials may cause the transmitter to restart which may cause spurious trips. This problem can be resolved by either installing an isolator, or alternatively by configuring the safety logic solver to avoid tripping the SIF during transmitter restarts, see section Transmitter communication.

**Figure 2-12. Installation of an isolator can be used to prevent ground potential differences.**

**2.3.8 Transmitter communication**

It is essential to correctly understand the transmitter's output-behavior to be able to configure the safety logic solver for a correct interpretation compliant to IEC 61511. Incorrect behavior
can for example result in spurious trips or malfunction of the SIF. In functional safety applications, the Rosemount 5300 and 5400 series shall be equipped with 4-20mA/HART communication.

**Table 2-3. Basic properties of Rosemount 5300- and 5400 Series 4-20mA/HART communication**

<table>
<thead>
<tr>
<th>Transmitter Communication</th>
<th>Safety-rated</th>
<th>Primary Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Analog 4-20mA signal</td>
<td>Yes</td>
<td>Continuous communication of primary measurement value and transmitter failure indication</td>
</tr>
<tr>
<td>Superimposed HART digital signal</td>
<td>No</td>
<td>Configuration, proof-testing, diagnostics</td>
</tr>
</tbody>
</table>

During this phase in the safety-life cycle it is important to clearly specify the parameters required for the communication interface between the transmitter and safety logic solver to function correctly. These parameters include (but may not be limited to):

- **Primary Variable**
- **Lower range value**
- **Upper range value**
- **ESD trip-point(s)**
- **Operator alert trip-point(s) (in mA or percent of configured 4-20mA range)**
- **Saturation and alarm limits**
- **Transmitter alarm behavior**
- **Alarm-delay parameters**

**Analog 4-20mA signal**

**Superimposed HART digital signal**

The behavior of the 4-20mA signal is thoroughly described in Rosemount 5300 and 5400’s safety-manuals.

When defining the parameters for the communication interface between the transmitter and safety logic solver, the following considerations shall also be taken into account:

- **Primary Variable**: The transmitter measurement variable that will control the 4-20mA output. Usually specified as level, or in some instances distance.
- **Lower/Upper range value**: Controls the scaling of the 4-20mA output. At a minimum, the interval specified must include the ESD set-point(s), but preferable the entire transmitter’s effective measuring range (see section *Mechanical Considerations*) as depicted in Figure 2-13.
Figure 2-13. Typical configuration of upper/lower range value in bridle (chamber) applications.
Section 2: Recommendations grouped according to IEC 61511 safety life-cycle

Trip-point(s): Shall be specified in mA or percent of configured 4-20mA range. For example, 16.8 mA corresponds to 80% of the configured 4-20mA range. Note the difference between the 4-20mA range and the actual tank and the configured scaling in the safety logic solver, which may or may not be the same.

Alarm and saturation limits: Rosemount standard alarm and saturation limits are used as default; refer to the product manual for exact details. NAMUR NE43 compliant limits are also available and can be specified using the model-code. Although configurable, the default behavior of the transmitter output is to park the signal at the saturation limits when the actual measurement is outside the configured analog range.

Transmitter alarm behavior: Transmitter default is high-alarm, but can be changed to low-alarm either by using a model-code option or by transmitter configuration. Note that the Rosemount 5400 is not available with the combination NAMUR NE43 alarm and saturation limits and low-alarm.

Alarm-delay parameters: The intention with this functionality is to avoid spurious trips due to temporary variations in the 4-20mA signal. Note that increased delays may increase the entire SIF’s response-time. The exact delay functionality varies between different transmitters and safety logic solvers and has to be adapted accordingly. Refer to Figure 2-15 and Figure 2-16 for typical startup behavior of the Rosemount 5300 and 5400. To avoid spurious trips due to for example power-glitches and lightning it is advisable to configure the different alarm delays in such a way that transmitter restarts are ignored. Modern safety logic solvers usually incorporate multiple different types of alarm delay capabilities, which broadly can be separated into the following two categories:

° ‘Good sensor status’ (4-20mA signal is within the specified saturation limits): Safety logic solver accepts the input as a valid measurement. Minimum recommendable SIF alarm-delay to mask transmitter restarts is 8 seconds (which equals the Rosemount 5300 and 5400 response-time, refer to subsequent section Response time). This type of delay impacts the SIF’s overall response-time.
° ‘Bad sensor status’ (4-20mA signal is outside the 4-20mA saturation limits): Minimum recommendable alarm-delay to mask transmitter restarts is 30 seconds. In addition, a time that takes the down-time into account shall be added, refer to Figure 2-15 and Figure 2-16. This type of delay may or may not (usually the case) be considered to impact the SIF’s overall response-time depending on the frequency of occurrence in relation to the demand frequency.

° Simpler logic solvers may not have the capability to distinguish between these two types of basic alarm delays. If that’s the case, then the two shall be added to a combined transmitter alarm-delay of 38 seconds. In addition, a time that takes the down-time into account shall be added, refer to Figure 2-15 and Figure 2-16. This type of delay impacts the SIF’s overall response-time.

Figure 2-15. Rosemount 5300 and 5400 typical startup behavior, Rosemount standard alarm and saturation limits, high alarm (default setting). Recommended minimum alarm delays to avoid tripping during restarts:

- ‘Bad sensor status’ alarm delay = 30 seconds + Power down time
- ‘Good measurement status’ alarm delay = 8 seconds
Figure 2-16. Rosemount 5300 and 5400 typical startup behavior, Rosemount standard alarm and saturation limits, low alarm. Recommended minimum alarm delays to avoid tripping during restarts:
- ‘Bad sensor status’ alarm delay = 30 seconds + Power down time
- ‘Good measurement status’ alarm delay = 8 seconds

The action that shall be taken upon 'bad sensor status' also needs to be specified. The exact requirements are addressed in IEC 61511-1 11.3.1 (redundant configurations) and 11.3.2 (non-redundant configurations) but can be summarized as the SIF shall trip and bring the process to a safe state (option a), or alternative measures shall be taken to ensure the process safety (option b). Consequently it is not necessarily a requirement to activate the SIF upon 'bad sensor status', which can be used to reduce the rate of spurious trips.
The behavior of the Rosemount 5300 and 5400 4-20mA analog output is summarized in Table 2-4 and Table 2-5.

**Table 2-4. Typical interpretation of the Rosemount 5300 and 5400 Series 4-20mA signal in overfill prevention applications**

<table>
<thead>
<tr>
<th>Analog signal (1)</th>
<th>Interpretation</th>
<th>SIF Action</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>≥ 21.75 mA</td>
<td>Sensor failure, sensor restarting, wire failure, I/O failure</td>
<td>a) or b) per IEC 61511-1 11.3.1/11.3.2</td>
<td>Usage of ‘bad sensor status’ alarm-delay is recommendable.</td>
</tr>
<tr>
<td>20.8 mA to ESD set-point</td>
<td>Acceptable measurement but level at or above ESD Set-point.</td>
<td>Activate ESD</td>
<td>Consider the usage of measurement alarm delay and appropriate alarm dead-band settings.</td>
</tr>
<tr>
<td>ESD set-point to 3.9 mA</td>
<td>Normal measurement</td>
<td>N/A</td>
<td>May contain set-points to e.g. control non-SIS equipment such as pumps or Hi-alerts to notify the operators.</td>
</tr>
<tr>
<td>≤ 3.75 mA</td>
<td>Sensor failure, sensor restarting, wire-cut, auxiliary component failure, I/O failure</td>
<td>a) or b) per IEC 61511-1 11.3.1/11.3.2</td>
<td>Usage of ‘bad sensor status’ alarm-delay is recommendable.</td>
</tr>
</tbody>
</table>

(1) Rosemount standard alarm and saturation limits assumed. For NAMUR NE43 alarm and saturation limits refer to the product manual.
Table 2-5. Typical interpretation of the Rosemount 5300 and 5400 Series 4-20mA signal in dry-run prevention applications.

<table>
<thead>
<tr>
<th>Analog signal(^{1})</th>
<th>Interpretation</th>
<th>SIF Action</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>≥ 21.75 mA</td>
<td>Sensor failure, sensor restarting, wire failure, I/O failure</td>
<td>a) or b) per IEC 61511-1 11.3.1/11.3.2</td>
<td>Usage of 'bad sensor status' alarm-delay is recommendable.</td>
</tr>
<tr>
<td>20.8 mA to ESD set-point</td>
<td>Normal measurement</td>
<td>N/A</td>
<td>May contain set-points to e.g. control non-SIS equipment such as pumps or Lo-alerts to notify the operators.</td>
</tr>
<tr>
<td>ESD set-point to 3.9 mA</td>
<td>Acceptable measurement but level at or above ESD Set-point.</td>
<td>Activate ESD</td>
<td>Consider the usage of measurement alarm delay and appropriate alarm dead-band settings.</td>
</tr>
<tr>
<td>≤ 3.75 mA</td>
<td>Sensor failure, sensor restarting, wire-cut, auxiliary component failure, I/O failure</td>
<td>a) or b) per IEC 61511-1 11.3.1/11.3.2</td>
<td>Usage of 'bad sensor status' alarm-delay is recommendable.</td>
</tr>
</tbody>
</table>

\(^{1}\) Rosemount standard alarm and saturation limits assumed. For NAMUR NE43 alarm and saturation limits refer to the product manual.

**Superimposed HART digital signal**

The transmitter’s HART digital signal is not safety rated. It can be used for e.g. configuration, advisory diagnostics and proof-testing but shall not be used for any safety critical communication such as activation of the SIF.

### 2.3.9 SIL validation

According to IEC 61511, sensors shall be certified according to IEC 61508 or alternatively “be in accordance with IEC 61511 11.4 and 11.5.3 to 11.5.6 as appropriate” (‘prior-use’/‘proven-in-use’).

To validate that a SIF meets the expected SIL the following properties need to be evaluated (SIF overall SIL is determined by the lowest individual score)

1. Systematic Capability or Prior-Use Justification
2. Architecture Constraints (redundancy)
3. Random Hardware Failures
Rosemount 5300 Series

The Rosemount 5300 Series has been certified to IEC 61508:2010 Parts 1-7 by the accredited third part Exida as described in Figure 2-17. The basic SIL requirements are evaluated in Table 2-6 and the result is depicted in Figure 2-18 and Figure 2-19.

Figure 2-17. Rosemount 5300 Series IEC 61508 Certificate. Issuer: Exida.
Section 2: Recommendations grouped according to IEC 61511 safety life-cycle

March 2015

Table 2-6. Rosemount 5300 Series SIL requirements evaluation

<table>
<thead>
<tr>
<th>SIL Requirement</th>
<th>Fulfillment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Systematic Capability (or Prior-Use Justification)</td>
<td>Rosemount 5300 Series has a systematic capability of SIL 3 according to IEC 61508 certificate</td>
</tr>
<tr>
<td>Architecture Constraints (redundancy)</td>
<td>Rosemount 5300 is a type B element with a Safe Failure Fraction (SFF) in the 90-99% range, and consequently according to IEC 61508-2:2010 7.4.4.2.2:</td>
</tr>
<tr>
<td></td>
<td>- SIL 2 @ HFT=0 (no redundancy)</td>
</tr>
<tr>
<td></td>
<td>- SIL 3 @ HFT=1 (redundancy)</td>
</tr>
<tr>
<td>Random Hardware Failures</td>
<td>The PFD_{avg} has to be calculated individually for the entire SIF but Rosemount 5300 typically fulfills requirements up to SIL 3 depending on proof-test interval. Refer to Table 2-10 for specific examples.</td>
</tr>
</tbody>
</table>

Figure 2-18. Rosemount 5300 Series can be used in SIL 2 SIFs in non-redundant configuration

Figure 2-19. Rosemount 5300 Series can be used in SIL 3 SIFs in homogenous redundant configurations such as 1oo2 and 2oo3

Rosemount 5400 Series

IEC 61511 allows the owner/operator to self-qualify sensors that already have a proven track record in similar applications. The basic requirements that the owner/operator needs to fulfill when self-qualifying sensors per the IEC 61511 prior-use path is listed in Table 2-7, accompanied with Emerson’s proposal on how to fulfill the requirements and information about data that may be relevant. The basic SIL requirements are evaluated in Table 2-8 and the result is depicted in Figure 2-20.
Table 2-7. Prior-use requirements per IEC 61511-1 11.5.3.2

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Rosemount 5400 proposed fulfillment procedure</th>
</tr>
</thead>
<tbody>
<tr>
<td>Consideration of the manufacturer’s quality, management and configuration</td>
<td>Review ISO 9001 and ISO 14001 certificates. Contact your local Emerson representative to obtain a copy.</td>
</tr>
<tr>
<td>management systems</td>
<td></td>
</tr>
<tr>
<td>Adequate identification and specification of the components or subsystems</td>
<td>Rosemount 5400 is specified thru the use of model-codes which are thoroughly defined in the product data sheet (PDS). Model-code, Serial-number, manufacturer, tag printed on enclosure label, refer to product manual for further details.</td>
</tr>
<tr>
<td>Demonstration of the performance of the components or subsystems in similar</td>
<td>Option 1) Rosemount 5400 FMEDA-report Option 2) Rosemount 5400 field demonstrated MTBF (Figure 2-1). Contact your local Emerson representative to obtain a copy.</td>
</tr>
<tr>
<td>operating profiles and physical environments(1)</td>
<td></td>
</tr>
<tr>
<td>The volume of the operating experience(1)</td>
<td>Review Rosemount 5400 field demonstrated MTBF (Figure 2-1). Contact your local Emerson representative to obtain a copy.</td>
</tr>
</tbody>
</table>

(1) According to IEC 61511 11.5.3.1 Note 1: “In the case of field elements, there may be extensive operating experience either in safety or non-safety applications. This can be used as a basis for the evidence.”

Table 2-8. Rosemount 5400 Series SIL requirements evaluation

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Fulfillment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Systematic Capability or Prior-Use Justification</td>
<td>Rosemount 5400 Series can be qualified per IEC 61511 prior-use clause, refer to Table 2-7.</td>
</tr>
</tbody>
</table>
| Architecture Constraints (redundancy)            | The Rosemount 5400 Series fulfills the following requirements:  
  - the device allows adjustment of process-related parameters only, for example, measuring range, upscale or downside failure direction  
  - the adjustment of the process-related parameters of the device is protected, for example, jumper, password; Consequently according to IEC 61511-1 11.4.4 the Rosemount 5400 when qualified per the prior-use clause can be used in up to SIL 2 @ HFT=0 (no redundancy). |
| Random Hardware Failures                         | The PFD avg has to be calculated individually for the entire SIF but Rosemount 5400 typically fulfills requirements up to SIL 2 depending on proof-test interval. Refer to Table 2-10 for specific examples. |
2.3.10 Failure Rates

The primary source of failure rate data for the Rosemount 5300 and 5400 is their corresponding FMEDA-reports and safety manuals. Alternatively, documentation with field demonstrated MTBF data is available, refer to Table 2-1.

When calculating the SIF’s mission time also the individual components’ useful life times need to be taken into account, refer to Table 2-9.

<table>
<thead>
<tr>
<th>Product</th>
<th>Useful lifetime</th>
</tr>
</thead>
<tbody>
<tr>
<td>5300(^{(1)})</td>
<td>50 years</td>
</tr>
<tr>
<td>5400(^{(2)})</td>
<td>8-12 years</td>
</tr>
</tbody>
</table>

\(^{(1)}\) Based on Exida Rosemount 5300 FMEDA-report revision 4
\(^{(2)}\) Based on Rosemount 5400 SP FMEDA-report revision 2. No specific investigation has been conducted, but according to IEC 61508-2, 7.4.7.4, note 3, the useful lifetime often lies within a range of 8 to 12 years for transmitters. Based on Emerson’s experience with Radar Level Gauges, this number is believed to be a very conservative estimate for this type of device.

The mean time to repair/restoration (MTTR) is site and tank specific and depends on a number of factors such as the availability of spare-parts, distance and availability of the tank, maintenance department work-load and paperwork procedures. For the Rosemount 5300 and 5400 the replaceable parts are the transmitter head and the antenna/probe. Reasonable assumptions for the typical effective time for replacing these parts in non-pressurized tanks are:

- Transmitter head: 1 hour
- Antenna/Probe: 2 hours
2.3.11 Diversification

The purpose of technology or product diversification is to avoid systematic failures.

The Rosemount 5300 has a systematic capability of SIL 3 (RRF=1,000-10,000) which implies that two units of the same sensor type can be used for both BPCS (RRF=1-10) and a SIF up to SIL2 (RRF=100-1000) since the total risk reduction equals SIL3. This configuration is exemplified in Figure 2-21.

In case of Rosemount 5400, its suitability for usage in both the BPCS and SIS layer must be determined based on the prior-use data.

Figure 2-21. Rosemount 5300 fulfills the systematic requirements to be used as 1xBPCS-sensor and 1xSIF-sensor up to SIL2.

2.3.12 Demand-mode

Rosemount 5300 and 5400 Series can support the demand mode but not the continuous mode as specified in IEC 61511.

2.3.13 Response Time

The entire SIF’s response time is dependent upon the combined behavior of the sensor, logic-solver and actuator. The SIF’s overall response time combined with the tank’s maximum level-rate usually serves as an important input when determining the ESD set-point(s).
Rosemount 5300 and 5400, which constitute a sensor functional block, have a default response time of 8 seconds for the measurement variables level and distance. Additionally the transmitters contain an adjustable damping (first order filter) which default is set to 2 seconds.

2.3.14 SAT

Site acceptance test (SAT) is an integrated part of the safety life-cycle that needs to be planned, design and documented during this phase of the project. The proposed procedures for Rosemount 5300 and 5400 Series are described in their respective safety manuals. Refer to section SIS safety validation (clause 15) for further details.

2.3.15 Proof-test

The purpose of proof-testing is to detect random dangerous undetected hardware failures ($\lambda_{DU}$), unlike the SAT which purpose is to detect systematic failures such as incorrect transmitter settings.

During this phase of the project, a test-plan with the exact procedures and test acceptance criteria shall be created. The procedures for Rosemount 5300 and 5400 Series are described in their respective safety manuals. For the test acceptance criteria, the procedures need to be evaluated against the current process and available equipment/data to determine the specific tolerances.

When evaluating and selecting between the different proof-test procedures available for the Rosemount 5300 and 5400 at a minimum the following factors shall be taken into account:

- **SIF impact**: is it acceptable (and sometimes even requested) that the proof-test procedure affects other parts of the SIF (i.e. tripping the safety logic solver and the actuator)? If not, a partial proof-testing may be preferable or alternatively appropriate by-pass measures need to be implemented to avoid the entire SIF from tripping.
- **Process impact**: is it acceptable that the proof-test affects the process (e.g. 2-point level verification test) or does this need to be avoided?
- **Rosemount 5300 and 5400 proof-tests can be performed in-situ (i.e. without removing the transmitter)**
- **Is it acceptable to physically have to visit the transmitter during the test?** If not, the Rosemount 5300 and 5400 offer proof-tests that can be performed remotely from the control or maintenance room. If a tank visit will be required, appropriate measures for personal safety need to be documented in the test-plan.

The test-plan shall also contain:

- **A description of what actions to take during the proof-test to ensure process safety**
- **An estimation of the time to completion. Typically, the effective proof-test time for the Rosemount 5300 and 5400 is in the range of 5 - 20 minutes**
- **The tools required to perform the proof-test. Depending on the selected proof-test procedure, typically the following tools are needed:**
  - HART-capable configuration tool (e.g. AMS® Device Manager, Rosemount Radar Master, 475)
Current-meter (e.g. the safety logic solver or a multimeter)

° Liquid level surface locator (e.g. BPCS level sensor or hand-gauging)

The proof-test interval shall be calculated individually for the specific SIF. It shall be verified at a minimum against legislative requirements, the SRS and any company specific requirements. The exact proof test interval will depend on a number of factors, but indicative numbers are provided in Table 2-10.

Table 2-10. Proof-test interval

<table>
<thead>
<tr>
<th>Product</th>
<th>Sensor-λDU</th>
<th>Sensor Proof-test Interval @</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>SIL 1</td>
</tr>
<tr>
<td>5300</td>
<td>96 FIT(2)</td>
<td>15+ years</td>
</tr>
<tr>
<td>5400</td>
<td>276 FIT(3)</td>
<td>15+ years</td>
</tr>
</tbody>
</table>

(1) Approx max statistical proof-test interval based on failure rates according to IEC 61508-6 formulas and the assumption that the level sensor is used in a 1oo1 configuration and uses 35% of the SIF’s total dangerous failure rate: PFDavg = Sensor-IDUT/2 =35%/1/10SIL. In this simplified calculation, the mission-time assumed equal to proof-test interval

(2) Based on Rosemount 5300 Exida FMEDA-report revision 4

(3) Based on Rosemount 5400 SP FMEDA-report revision 2

It is a requirement to maintain records that certify that the proof tests were completed as required. During this phase of the safety life-cycle, it is recommended to develop a template for this purpose. Refer to the product safety manual or contact your local Emerson representative for suggestions on how to design this template.

According to IEC 61511-1 11.2.4 it is acceptable to exchange information between the BPCS and SIS layers if the integrity of the SIS is not compromised. As a result, it is becoming increasingly popular to implement a deviation alarm between the BPCS and SIS level measurements. Effectively this is an online ‘partial proof-testing’ that reduces the Sensor-PFD_{avg}. The following considerations are recommended to take into account:

- The coverage factor is stated in the product safety manual and reduces the Sensor-λDU to Sensor-λDU * (100% - Coverage factor partial proof test). This number can be used in the PFD_{avg} calculation to reduce the frequency of proof testing.
- The exact alarm-limit to use is dependent on the specific installation. Often it is advantageous to employ a relatively wide limit based on historical data to minimize the number of spurious alerts.
- To take credit for the deviation alarm it is required to ensure that proper action is taken when it arises and hence it cannot be an informative alert that may be ignored or overlooked.

According to IEC 61511-1 16.3.2 “each SIS shall be periodically visually inspected”. There is however no requirement on the time-interval and it does not increase the theoretical proof-test coverage factor specified in the safety manuals. Therefore this requirement is usually fulfilled during plant turn-arounds and during normal operation the Rosemount 5300 and 5400 proof-test procedures are performed remotely.
2.4 FAT: Factory acceptance testing (clause 13)

FAT is optional according to IEC 61511 and the standard only covers logic solvers in detail, and hence no guidance is offered for sensors. Emerson does however offer customizable FATs as a service. Contact your local Emerson representative to obtain a copy of the standard FAT procedure.

2.5 SIS installation and commissioning (clause 14)

According to IEC 61511, the purpose of this phase in the life-cycle is to

- install the safety instrumented system according to the specifications and drawings
- commission the safety instrumented system so that it is ready for final system validation (SAT)

The Rosemount 5300 and 5400 installation procedures are thoroughly described in the product manuals. According to experience, the following factors are especially important to avoid any potential problems:

- Correct configuration of the Rosemount 5300 and 5400 is critical to ensure a reliable level measurement with a minimum of spurious alarms. Consequently, the personnel executing this task needs be appropriately trained and qualified for the task and perform the configuration according to the product manuals
- Configuration shall be performed under actual operating conditions with the correct product in the tank. If possible, it is recommended to investigate the following measurement scenarios more closely by for example viewing the echo-curve when they occur and configure the gauge appropriately
  - Full tank
  - Measurements close to the ESD set-point
  - Situations that may affect the measurement such as boiling, foam, agitation
- Configuration of the 4-20 mA signal scaling and behavior shall be performed as specified during the SIS design and engineering (clauses 11 & 12) phase (rather than deciding the configuration ad-hoc during the installation)
- During the installation of the Rosemount 5300 and 5400, it is also advisable to configure the alarm delay settings in the safety logic solver in such a way that transmitter restarts do not generate a spurious trip. The exact configuration shall be specified during the SIS design and engineering (clauses 11 & 12) phase. Although a transmitter restart can be invoked through software it is recommendable to remove the transmitter power temporarily. It is also advisable to test the UPS switch-over functionality (if applicable)
- The most convenient way to generate a demand on the SIF is to use the level simulation capability in the Rosemount 5300 and 5400
- Note carefully that certain parameters such as the filtering (‘damping’) can affect the SIF’s response-time
- Upon completion of the installation, always store the transmitter’s configuration in case the transmitter needs to be replaced. Also the echo-curve shall be stored as a reference for future proof-tests.
2.6 **SIS safety validation (clause 15)**

This section is commonly referred to as site acceptance test (SAT) in the process industry. It is usually more extensive than a proof-test since the purpose is to detect systematic failures (e.g. incorrect calibration or sensor configuration).

It is recommended to conduct the Rosemount 5300 and 5400 SATs under actual operating conditions with the correct product in the tank. The selected test procedure is recommended to verify at a minimum the following potential systematic failures:

- Visual inspection to ensure
  - electrical and mechanical installation has been performed correctly
  - review transmitter label and printed model-code to ensure the correct device is being used
- SIS level sensor cabling is separate and independent from the BPCS level sensor
- Review transmitter specification meets the requirements in the SRS
- Scaling of the 4-20 mA signal has been done correctly. At a minimum, review the following configuration parameters
  - Primary Variable
  - Lower Range Value
  - Upper Range Value
- Transmitter configuration has been done correctly by reviewing
  - Threshold settings in relation to the product surface amplitude
  - Tank Height
  - Hold off
- Simulate power failure and ensure transmitter behavior is acceptable
- Simulate UPS switch-over and ensure transmitter behavior is acceptable (if applicable)
- Verify that the following procedures have been properly documented and can be executed in practice
  - Proof-test procedure and interval
  - Bypass
  - Manual shutdown
  - Reset
- Documentation is consistent with actual installation and operating procedures

In order to test the entire SIF end-to-end, the Rosemount 5300 and 5400 support simulation of the transmitter output signal.
2.7 **SIS operation and maintenance (clause 16)**

Rosemount 5300 and 5400 do not have any moving parts and consequently there are no general maintenance requirements. In applications where there is a risk for build-up or clogging of the wetted parts the proof-test is recommended to be designed to detect these types of problems. Information about diagnostic alerts can be found in the product manuals.

Proof-test shall be performed as specified in the test-plan, refer to section Proof-test for further details.

2.8 **SIS modification (clause 17)**

It is required to perform a SAT upon any modification of a Rosemount 5300 and 5400 such as device replacement or configuration change.

Upon device replacement, it is recommendable to re-use the configuration of the device being replaced which should have been stored during the original installation or last modification.
# Appendix A: IEC 61511safety life-cycle overview

**Note**  
Source: IEC 61511-1:2003 Table 2

<table>
<thead>
<tr>
<th>Phase</th>
<th>Objectives</th>
<th>Inputs</th>
<th>Outputs</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hazard and risk assessment</td>
<td>To determine the hazards and hazardous events of the process and associated equipment, the sequence of events leading to the hazardous event, the process risks associated with the hazardous event, the requirements for risk reduction and the safety functions required to achieve the necessary risk reduction</td>
<td>Process design, layout, manning arrangements, safety targets</td>
<td>A description of the hazards, of the required safety function(s) and of the associated risk reduction</td>
</tr>
<tr>
<td>Allocation of safety functions to protection layers</td>
<td>Allocation of safety functions to protection layers and for each safety instrumented function, the associated safety integrity level</td>
<td>A description of the required safety instrumented function(s) and associated safety integrity Requirements</td>
<td>Description of allocation of safety requirements (see Clause 9)</td>
</tr>
<tr>
<td>SIS Safety Requirements Specification</td>
<td>To specify the requirements for each SIS, in terms of the required safety instrumented functions and their associated safety integrity, in order to achieve the required functional safety</td>
<td>Description of allocation of safety requirements</td>
<td>SIS safety requirements; software safety requirements</td>
</tr>
<tr>
<td>SIS design and engineering</td>
<td>To design the SIS to meet the requirements for safety instrumented functions and safety integrity</td>
<td>SIS safety requirements; Software safety requirements</td>
<td>Design of the SIS in conformance with the SIS safety requirements; planning for the SIS integration test</td>
</tr>
<tr>
<td>SIS installation, commissioning and validation</td>
<td>To integrate and test the SIS. To validate that the SIS meets in all respects the requirements for safety in terms of the required safety instrumented functions and the required safety integrity</td>
<td>SIS design; SIS integration test plan; SIS safety requirements; Plan for the safety validation of the SIS</td>
<td>Fully functioning SIS in conformance with the SIS design results of SIS integration tests Results of the installation, commissioning and validation activities</td>
</tr>
<tr>
<td>SIS operation and maintenance</td>
<td>To ensure that the functional safety of the SIS is maintained during operation and maintenance</td>
<td>SIS requirements; SIS design; Plan for SIS operation and maintenance</td>
<td>Results of the operation and maintenance activities</td>
</tr>
</tbody>
</table>
## IEC 61511 safety life-cycle overview

<table>
<thead>
<tr>
<th>Phase</th>
<th>Objectives</th>
<th>Inputs</th>
<th>Outputs</th>
</tr>
</thead>
<tbody>
<tr>
<td>SIS modification</td>
<td>To make corrections, enhancements or adaptations to the SIS, ensuring that the required safety integrity level is achieved and maintained</td>
<td>Revised SIS safety requirements</td>
<td>Results of SIS modification</td>
</tr>
<tr>
<td>Decommissioning</td>
<td>To ensure proper review, sector organization, and ensure SIF remain appropriate</td>
<td>As built safety requirements and process information</td>
<td>SIF placed out of service</td>
</tr>
<tr>
<td>SIS verification</td>
<td>To test and evaluate the outputs of a given phase to ensure correctness and consistency with respect to the products and standards provided as input to that phase</td>
<td>Plan for the verification of the SIS for each phase</td>
<td>Results of the verification of the SIS for each phase</td>
</tr>
<tr>
<td>SIS functional safety assessment</td>
<td>To investigate and arrive at a judgment on the functional safety achieved by the SIS</td>
<td>Planning for SIS functional safety assessment SIS safety requirement</td>
<td>Results of SIS functional safety assessment</td>
</tr>
</tbody>
</table>