



Proof-testing

A guide to proof-testing level devices used in safety instrumented systems

2021 EDITION



This guide provides an overview to proof-testing level devices used in safety instrumented systems

For further information on proof-testing go to:
[Emerson.com/proof-testing](https://www.emerson.com/proof-testing)

Legal disclaimer

This Proof-test Guide (“Guide”) is designed to provide information on proof-testing level devices only based on [International Electrotechnical Commission’s IEC 61511 standard](#) and the [American Petroleum Institute’s API 2350 standard](#).

The contents of this Guide are presented for information purposes only, and while effort has been made to ensure their accuracy, they are not to be construed as warranties or guarantees, expressed or implied, regarding the products or services described herein or their use or applicability. This information is provided with the knowledge that the author is offering generic advice based which may not be applicable in every situation. You should therefore ensure you seek advice from an appropriate professional.

This Guide does not contain all information available on the subject. This Guide has not been created to be specific to any individual’s or organizations’ situation or needs. Every effort has been made to make this Guide as accurate as possible. However, there may be typographical and or content errors. This Guide contains information that might be dated. While we work to keep the information up-to-date and correct, we make no representations or warranties of any kind, express or implied, about the completeness, accuracy, reliability, suitability or availability with respect to the Guide or the information, products, services, or related graphics contained in the Guide for any purpose. Any reliance you place on such information is therefore strictly at your own risk. Therefore, this Guide should serve only as a general guide and not as the ultimate source of subject information. In no event will Emerson and/or any of its affiliates be liable for any loss or damage including without limitation, indirect or consequential loss or damage, arising out of or in connection with the use of the information contained in this Proof-test Guide. You hereby agree to be bound by this disclaimer or you may return this Guide.

All rights reserved. No part of this Guide may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying, recording or by any information storage and retrieval system, without written permission from the author.

Table of Contents

Introduction	7
Proof-test definition	7
Considerations when selecting level devices for a safety instrumented system	8
Is the measurement device compliant with the relevant industry safety standards?	8
How does a measurement device obtain a SIL rating?	8
Does the measurement device have the required SIL rating?	8
<i>Benefits of digital protocols</i>	8
Does the device provide a high level of diagnostic coverage?	9
Does the device provide the necessary reporting functionality to be compliant?	9
How can I reduce risk, increase safety and perform remote proof-testing?	9
<i>Risk reduction factor and PFD</i>	9
<i>Low and high demand modes of operation</i>	10
What are undetected failures?	10
What is the probability of failure on demand for the device?	10
What is the safe failure fraction?	10
Proof-testing	11
Proof-testing cost considerations	11
What is proof-test coverage?	11
Does diagnostic coverage affect the proof-test coverage?	11
What is the effect of the PTC on the PFD?	11
What is a comprehensive proof-test?	11
How is a comprehensive test performed?	11
Comprehensive proof-testing considerations	12
Performing a simulated test	12
What is a partial proof-test?	12
How does this differ from a comprehensive proof-test?	12
Do I still need to perform a comprehensive proof-test?	12
How regularly must proof-tests be performed?	12
What is remote proof-testing?	13
What are the advantages of remote proof-testing?	14
How are remote proof-tests performed for different device types?	14
Summary	14

Glossary	15
Reference section - contents	17
IEC 61508/IEC 61511 standards	18
Certification	18
SIF designs	18
PFDavg for low, high and continuous modes of operation	19
Systematic and random capability	19
Safe failure fraction and FMEDA	20
SIL and reliability	20
Site acceptance test	21
Factory acceptance test	21
FAT recommendations	21
FAT documentation	21
Guidance on SIS response time requirements	22
Proof-tests – comprehensive and partial	23
Does a partial test impact device reliability?	23
Calculating the PFD of a 1oo1-system without partial testing	24
Calculating the PFD for a 1oo1-system with partial testing	24
Conclusion	25
What is the effect of PTC on PFDavg when partial proof-testing is performed?	25
Conclusion	27
SIS IEC 61508 certificate quality evaluation	27
Step 1 - Collect information	27
Step 2 - Assess certification process	27
Step 3 - Review completeness of product certificate information	28
Summary	28
Application example	29

Introduction

The overfilling of tanks and vessels has long been a leading cause of serious incidents in the process and bulk liquid storage industries. The materials involved can be hazardous, flammable or even explosive, which means a spill can have catastrophic consequences – possibly causing injuries or fatalities, inflicting significant damage to assets, and harming the environment. The cost of such an incident can sometimes be measured in billions of dollars, while the ensuing adverse publicity can seriously blight a company’s reputation.

Safety must therefore 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 a robust safety instrumented system (SIS) to prevent overfilling, designed and implemented in compliance with the relevant industry safety standards. These are:

- The International Electrotechnical Commission’s IEC 61511 standard, which outlines best safety practices for implementing a modern SIS within the process industry. IEC 61511 is an industry-specific adaptation of IEC 61508, which is an industry-independent standard for functional safety.
- The American Petroleum Institute’s API 2350 standard, which provides minimum requirements to comply with modern best practices in the specific application of large non-pressurized above-ground petroleum storage tanks.

An SIS for overspill prevention includes the level devices, logic solvers and final control elements (in the form of actuated valve technology) for each of its safety instrumented functions (SIF), also known as safety loops. The purposes of an SIF are to permit a process to move forward in a safe manner when specified conditions allow, to automatically take a process to a safe state when specified conditions are violated, and to take action to mitigate the consequences of a hazard.

To ensure it will work correctly when there is a safety demand, and to verify it is operating at the required safety integrity level (SIL), each SIF must undergo regular proof-testing. This involves testing each of its components individually as well as the complete safety loop.

In this guide, we provide an overview of the factors that should be considered in selecting and proof-testing the level measurement and monitoring devices used within an SIS. This includes vibrating fork level detectors, differential pressure transmitters, guided wave radar level transmitters, and non-contacting radar level transmitters and gauges. The information throughout this guide is based on relevant standards including, but not limited to, International Electrotechnical Commission’s IEC 61511 standard and the American Petroleum Institute’s API 2350 standard. If you have any questions regarding matters not covered within this guide, please contact your local Emerson level measurement expert for assistance.

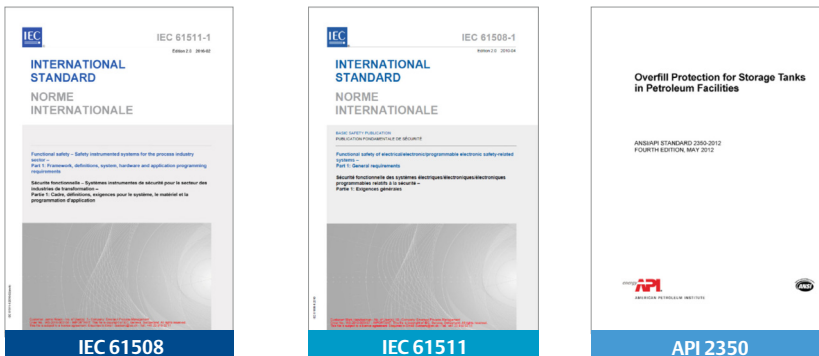


Figure 1: Industry safety standards

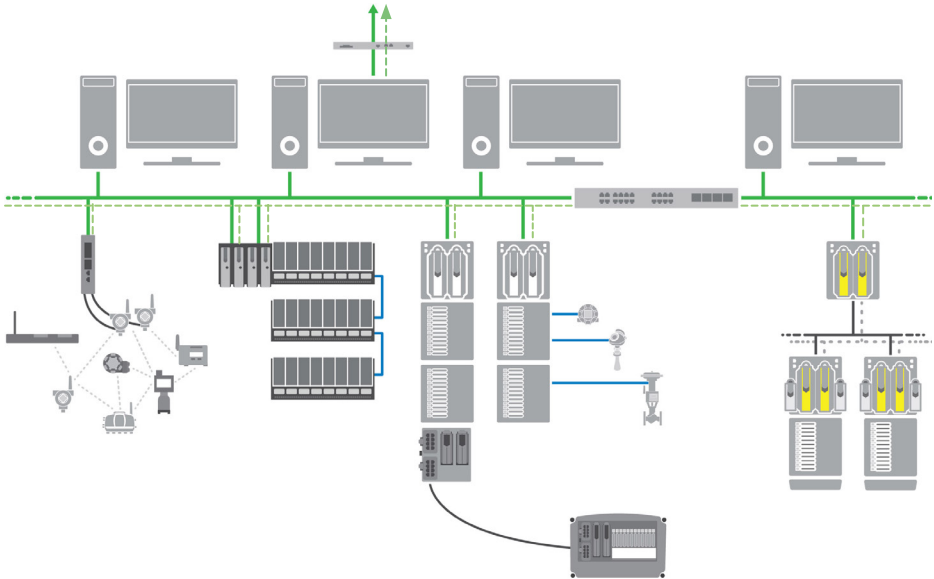


Figure 2: Safety instrumented system architecture

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 the device may be harboring unbeknown to anyone.

Testing of safety system components to detect any failures not detected by automatic online 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 an important part of the safety lifecycle and is critical to helping ensure a system achieves its required SIL throughout the safety lifecycle.

Considerations when selecting level devices for a safety instrumented system

<p>IEC 61508 3rd party assessed equipment</p>	<p>IEC 61511 Prior use, self certification requirements</p>	<p>IEC 61508 "Proven in use by the manufacturer"</p>
<p>3rd party certification of devices used in SIS applications is not requirement of type B programmable devices.</p>	<p>Essentially an owner/ operator's decision to use 'proven in prior use' components and subsystems from their preferred lists in an SIS application.</p>	<p>A proven in use claim relies on the availability of historical data for both random hardware and systematic failures.</p>

Figure 3: IEC Safety standards

Is the measurement device compliant with the relevant industry safety standards?

The IEC 61511 standard requires that manufacturers of measurement devices used in an SIS must comply with the requirements of IEC 61508. The measurement devices selected for an SIS must also comply with IEC 61508, with testing and certification performed by a third party or the vendor being able to demonstrate the safety level, capabilities and limitations of the device based on historical, proven in use data. Alternatively, the end user can meet the IEC 61511 requirements for the selection of devices based on prior use.

How does a measurement device obtain a SIL rating?

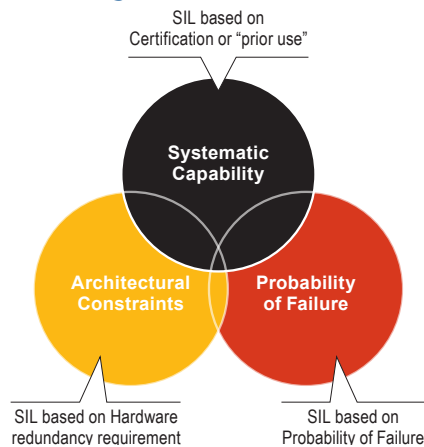


Figure 4: SIL ratings

SIL indicates the level of risk-reduction provided by a SIF safety. IEC 61508 defines four SILs, with SIL 4 being the most dependable. The required SIL for a given application is determined by quantitative and qualitative factors including a risk matrix, risk graphs and layers of protection analysis.

IEC 61508 indicates that Systematic Capability, Architectural Constraints and Probability of Failure of a product must be evaluated, with all three parts required to achieve the target SIL level. Systematic Capability requires the device manufacturer's quality management system to be assessed to ensure procedures are followed to prevent systematic design errors. A Failure Mode Effects and Diagnostic Analysis (FMEDA) (see Safe failure fraction and FMEDA section on page 20 for more details) is performed to evaluate the Architectural Constraints, while the Probability of Failure is assessed by calculating the average random probability of a failure. Independent third-party test companies such as Exida can determine the rate of failure, the fraction of safe failures and the likelihood of demand failure and provide FMEDA certification.

Does the measurement device have the required SIL rating?

In the process industry, instruments used in an SIS are required to be approved for use in SIL applications. For example, for a device to be certified for use in SIL 2 applications, the safe failure fraction (see page 10) of that device should be greater than 90%.

Benefits of digital protocols

Although analog devices can be applied to SIS, modern level devices feature digital protocols such as HART® or FOUNDATION™ Fieldbus, which in addition to measurement data, also provides access to diagnostic features and supports remote proof-testing. The diagnostic functionality enables dangerous failures to be identified in real time and then takes the device to a safe state.

Does the device provide a high level of diagnostic coverage?

Diagnostic coverage (DC) describes the ability of a device's diagnostics to detect dangerous failures. This diagnostic functionality will vary, with the latest devices being able to diagnose a wider range of issues. The DC is the fraction of dangerous failures detected out of the total number of dangerous failures. Devices with better diagnostic ability have a higher DC. DC does not indicate the number of undetected failures. A device with a high total number of dangerous failures, but almost all of which are discovered by the diagnostic ability, will have a high DC. However, if the device has very few dangerous failures and the same percentage of those are discovered, the device will have the same DC, but there will be a lower number of remaining undetected failures.

DC	Denotation
< 60%	None
60 to < 90%	Low
90 to < 99%	Medium
≥ 99%	High




Figure 5: Diagnostic coverage

Does the device provide the necessary reporting functionality to be compliant?

Safety Integrity Level	Probability of failure on Demand per year (or low demand)	Risk Reduction Factor	Probability of Dangerous failure per hour (Continuous mode or high demand)
SIL-4	$\geq 10^{-5}$ to $< 10^{-4}$	from 100 000 to 10 000	$\geq 10^{-9}$ to $< 10^{-8}$
SIL-3	$\geq 10^{-4}$ to $< 10^{-3}$	from 10 000 to 1 000	$\geq 10^{-8}$ to $< 10^{-7}$
SIL-2	$\geq 10^{-3}$ to $< 10^{-2}$	from 1 000 to 100	$\geq 10^{-7}$ to $< 10^{-6}$
SIL-1	$\geq 10^{-2}$ to $< 10^{-1}$	from 100 to 10	$\geq 10^{-6}$ to $< 10^{-5}$

Figure 6: Risk reduction factor

An important consideration when selecting level devices for an SIS is whether they can provide the reporting functionality needed to comply with the requirements of API 2350 and IEC 61511. Typically a level device would provide proof-testing data to a distributed control system, which in turn would generate a proof-test report. Organizations must provide written documentation of proof-testing procedures and schedules, and the criteria for equipment verification. This documentation must include instructions for maintaining safety during the proof-test and actions to be taken upon detection of a fault. Proof-testing intervals must be calculated and documented, and records certifying that tests were completed must be maintained. These should include descriptions of tests performed, names of the people performing them, the dates of the tests, and their results. API 2350 requires records to be maintained for at least three years. By providing the reporting functionality to support this requirement, modern advanced devices and their supporting software ensure compliance, while simplifying the documentation and auditing process.

How can I reduce risk, increase safety and perform remote proof-testing?

Risk reduction factor and PFD

Risk reduction factor (RRF) can be used to indicate the probability of failure on demand (see below) for an instrumented function, when the SIL mode is low demand (see below). The RRF is the inverse of the required probability of failure, which is represented in years. For example, a required probability of failure value of 0.001 would equal an RRF of 1000, meaning that the instrumented function would fail during a dangerous scenario about once every 1,000 years .

Low and high demand modes of operation

Low demand mode, is where the frequency of demands for operation made on a safety-related system is no greater than one per year. High demand or continuous mode, is where the frequency of demands for operation made on a safety-related system is greater than one per year. Continuous is regarded as very high demand.

What are undetected failures?

The dangerous failures that are not identified by the device diagnostics are known as dangerous undetected failures (DUs). DUs are measured as failures in time (FITs) and are the number of DUs per 10^9 hours of operation. Ideally, the DU rate should be extremely low, and selecting an instrument that provides a high level of diagnostic coverage will minimize DUs.

What is the probability of failure on demand for the device?

Another important consideration when selecting devices for an SIS is their probability of failure on demand (PFD). The PFD of an SIF relates to the risk of it failing to perform its safety function when required, and IEC 61511 states that the interval between proof-tests shall be calculated based on the average PFD (PFDavg) of the SIF during the time that it is in operation. The individual failure rates, diagnostic coverage and safe failure fraction are used to calculate the PFD avg. An SIF with a low PFDavg is more reliable than one with a high PFDavg and to help achieve this, the PFDavg of each component within the SIF needs to be as low as possible.

What is the safe failure fraction?

IEC 61508 defines the safe failure fraction (SFF) as the ratio of the potentially dangerous failures (that could lead to a hazardous situation such as an overflow) detected by built-in device diagnostics, and those failures which result in the device moving to a safe state, to the total number of failures. SFF is a measure of the effectiveness of a device's built-in diagnostics.

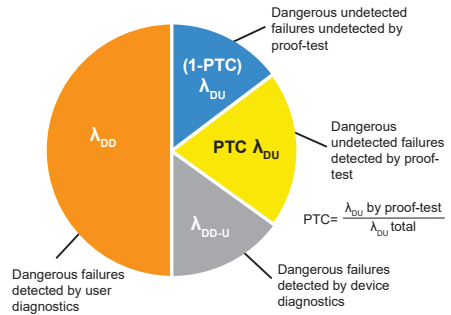


Figure 7: Safe failure fraction

The SFF is used to define the hardware fault tolerance (HFT), i.e. the required hardware redundancy, which can be seen in the table below.

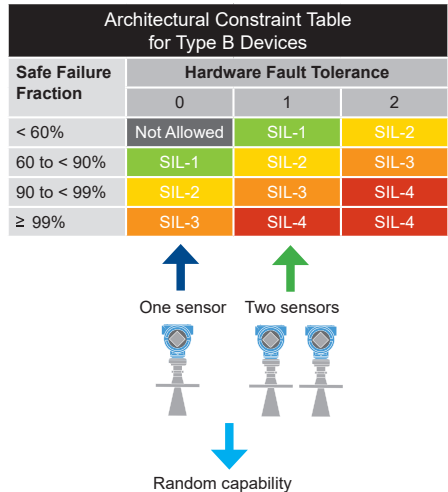


Figure 8: Architectural constraint table for type B devices

$$SFF = \frac{\lambda^{SD} + \lambda^{SU} + \lambda^{DD}}{\lambda^{SD} + \lambda^{SU} + \lambda^{DD} + \lambda^{DU}}$$

Failure rate types

λ^{SD} = Safe Detected failure rate

λ^{SU} = Safe Undetected failure rate

λ^{DD} = Dangerous Detected failure rate

λ^{DU} = Dangerous Undetected failure rate

Hardware fault tolerance (HFT) is the ability of a component or subsystem to continue to be able to undertake the required safety instrumented function in the presence of one or more dangerous faults in the hardware.

Proof-testing

The purpose of proof-testing is to verify that commissioned equipment functions correctly. To ensure a device will work correctly when there is a safety demand, and to verify it is operating at the required SIL, each SIF must undergo regular proof-testing. This involves testing each of its components individually as well as the complete safety loop.

Proof-testing cost considerations

The cost to perform proof-tests can be considerable and may often exceed 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.

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.

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.

What is the effect of the PTC on the PFD?

The simplified equations below show the effect of PTC on the PFDavg. Without PTC, the PFDavg can be modelled using the following equation:

$$TI = \text{Test interval}$$

$$PFD_{avg} = \lambda DU * TI/2$$

When we factor in PTC, we can model the PFDavg using the following equation:

Failure modes covered by proof-test	Failure modes not covered by proof-test
[<----->]	[<----->]
$PFD_{avg} = PTC \times 1/2 \times \lambda DU$	$TI + (1-PTC) \times 1/2 \times \lambda DU \times MT$

Mission time (MT) is the time interval where the dangerous failure modes that are not detected by the proof-test, can exist as latent, dangerous failures. PFDavg accumulates over the MT period, which can be many multiples of the proof-test interval. Mission time increases the PFDavg in the part of the PFDavg equation that is due to lack of proof-test coverage. In some cases, it can significantly affect the PFDavg and negatively affect the achieved SIL. Mission time is loosely related to the useful life of the device.

What is a comprehensive proof-test?

Two types of proof-test – comprehensive and partial – may be performed in compliance with both IEC 61511 and API 2350. Comprehensive tests achieve the highest proof-test coverage and involve testing the entire SIF in a single procedure, to ensure all its parts are functioning correctly. This will return the PFD of the SIF back to, or very close to, its original level.

How is a comprehensive test performed?

Comprehensive proof-testing is traditionally carried out manually by technicians in the field, with another worker stationed in the control room to verify the reaction of the system. The level in the tank is raised manually to the activation point of the level device being tested. This provides proof that the instrument is functioning correctly.

Comprehensive proof-testing considerations

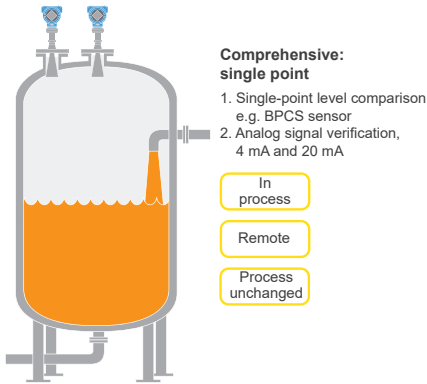


Figure 9: Comprehensive single point proof-testing

If the level device is a high-level sensor and fails to activate during the test, this could lead to a spill that could potentially present a safety risk. As a result, the latest version of API 2350 does not recommend the tank level be raised above the maximum working level. Performing proof-tests this way consumes a significant amount of time and labor and can lead to the process being offline for an extended period, affecting process availability during the outage and therefore having significant cost implications.

Performing a simulated test

Another approach is to remove the instrument from the tank and perform a simulated test in an alternative environment, such as a bucket. If the instrument is removed from a tank that would normally contain a hazardous or unpleasant product, water would be used instead. However, doing this would fail to prove that the device would work in the specific application, resulting in the proof-test coverage factor being reduced. This method also involves tanks being taken out of service for an extended period thus affecting profitability, exposing workers to greater safety risk, and is prone to human error when restoring equipment after testing.

What is a partial proof-test?

A partial proof-test has a reduced scope compared to a comprehensive test and is

performed to ensure that a device has no internal problems. Partial proof-testing will bring the PFD of a device back to a percentage of the original level and ensure that it fulfils its specified SIL requirement.

How does this differ from a comprehensive proof-test?

Whereas a comprehensive proof-test verifies all three functional elements of the device – output circuitry, measurement electronics and sensing element – a partial proof-test verifies one or two of them. A combination of partial proof-tests that covers all three functional elements is considered as a comprehensive proof-test and will reach a similar proof-test coverage.

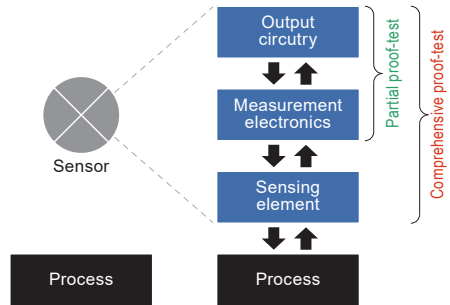


Figure 10: Comprehensive vs partial proof-testing

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 to its original PFD.

How regularly must proof-tests be performed?

API 2350 states that all components of an SIS required to be tested annually, with continuous level sensors to be tested once a year, and point level sensors semi-annually. IEC 61511 specifies that the proof-test interval depends on the SIL level that must be maintained of the complete

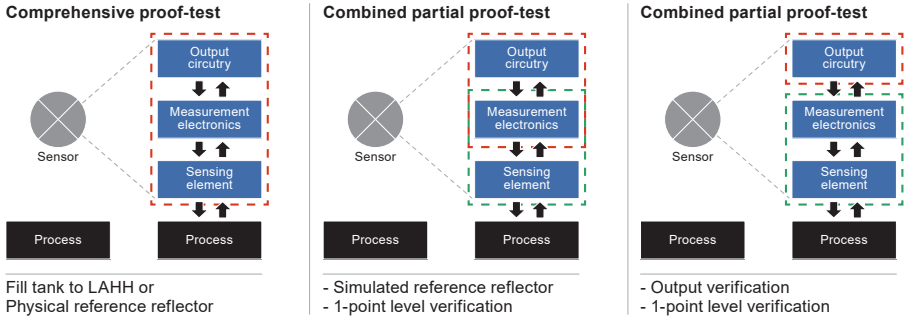


Figure 11: An example of how a combination of different partial proof-tests can be performed to cover all three functional elements

SIF. It also specifies that the entire SIS must be proof-tested periodically, and the frequency of testing is determined by the PFD average of the SIF. Performing a partial proof-test can, however, provide a technical justification for extending the time interval between comprehensive tests, while remaining within these regulatory requirements (see figure 12 below).

What is remote proof-testing?

The digital technology available in modern level instruments enables partial proof-testing to be performed remotely rather than through the traditional on-location approach. Remote proof-testing can be initiated via a command from the control room. Using this functionality, the instrument remains installed and does not need to be immersed during the proof-test. This is beneficial because performing tests during normal operation minimizes tank downtime and reduces worker exposure to hazardous environments without sacrificing SIL capability and functional safety.

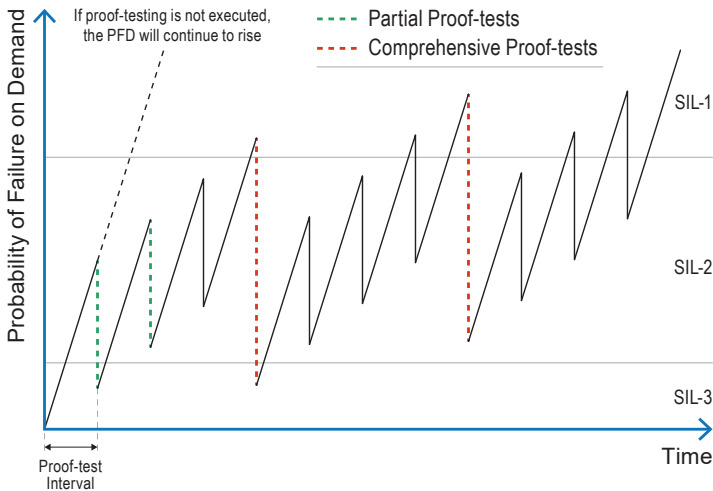


Figure 12: Partial proof-testing, while not comprehensive, does partially reduce the PFD, thereby extending the time period between more onerous comprehensive proof-tests.

What are the advantages of remote proof-testing?

Remote proof-testing is quick and easy, and multiple devices can be tested simultaneously, thereby increasing speed and safety, and reducing operational cost. Consequently, the ability to perform partial proof-testing remotely has become a key selection criterion when implementing level technology as part of an SIS.

How are remote proof-tests performed for different device types?

While the latest level measurement and monitoring devices used within an SIS have remote proof-testing capability, the means of performing the test differs for each technology. In the latest vibrating fork level detectors, remote partial proof-testing is performed by issuing a HART® command from the control room. Upon receiving the command, the device enters test mode, cycling the output through wet, dry and fault states, then returning to normal operation. Since the test can be performed in-process, it can take less than one minute to complete.

With advanced guided wave radar transmitters, an adjustable verification reflector fitted to the probe is used to simulate a high level in a tank. This avoids the need to fill the tank just to test the instrument and eliminates the risk of a spill happening if a device fails to activate during testing.

To remotely proof-test the latest non-contacting radar level transmitters and gauges, a high-level alarm can be verified using a simulated reference reflector. The proof-testing procedure is simplified through the use of dedicated software, which leads the operator through the various procedures step by step, and only requires them to input a straightforward sequence of settings and commands.

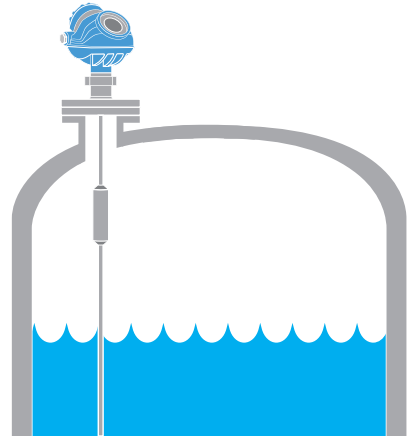


Figure 13: Adjustable verification reflector fitted to a guided wave radar probe.

Summary

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.

Glossary

Accreditation

Formal recognition by an authoritative body of the competence to work to specified standards.

Basic Process Control System (BPCS)

System that handles process control and monitoring.

Certification

Represents a written assurance by a third party of the conformity of a product, process or service to specified requirements.

Comprehensive Proof-test

Manual user proof-test that verifies all three functional elements of a device.

Dangerous Failure

A failure of a component in a safety instrumented function that prevents that function from achieving a safe state when it is needed (for example to shut down a pump and prevent an overflow).

Dangerous Undetected Failure (DU)

A dangerous failure not detected by the device's inbuilt diagnostics.

Diagnostics Coverage (DC)

A measure of a system's ability to detect failures. This is a ratio between the failure rates for detected failures to the failure rate for all failures in the system.

Equipment Under Control (EUC)

Equipment, machinery or plant used for manufacturing, processing or other activities.

Failure Mode Effect and Diagnostic Analysis (FMEDA)

Systematic analysis to obtain device failure rates, failure modes and diagnostic capability.

Failure in Time (FIT)

Device failure rate per billion hours.

Functional Safety

A methodology to achieve freedom from unacceptable risk achieved through the safety lifecycle. See IEC 61511.

Hardware Fault Tolerance (HFT)

The required hardware redundancy in an SIS.

IEC 61508

Industry-independent standard for safety instrumented systems.

IEC 61511

Standard for use of electrical/electronic/programmable electronic safety-related systems in the process industry. Unlike IEC 61508, this standard is targeted toward the process industry users of safety instrumented systems.

In-situ Proof-testing

Proof-testing of instrumentation performed at the point of interest and in contact with the subject of interest.

Partial Proof-test

Proof-test that verifies one or two functional elements of a device.

Probability of Dangerous Failures per Hour (PFH)

Probability that a system will fail dangerously, and not be able to perform its safety function when required.

Probability of Failure on Demand (PFD)

Risk of a device or SIF failing to perform its safety function when required.

Proof-testing Coverage (PTC or Cpt)

Measure of how many DUs are detected by the proof-test.

Risk Reduction Factor (RRF)

Used to indicate the probability of failure on demand for an instrumented function.

Safe Failure Fraction (SFF)

A measure of the effectiveness of a device's built-in diagnostics.

Safety Instrumented Function (SIF)

Function performed by the SIS to take a process to a safe state, when specified conditions are violated, to mitigate a hazard.

Safety Instrumented System (SIS)

One or more SIFs. An SIS is composed of any combination of sensor(s), logic solver(s), and final element(s).

Safety Integrity Level (SIL)

Quantitative target for measuring the level of performance needed for a safety function to achieve a tolerable risk for a process hazard.

User Diagnostics

A method of identify a problem through systematic analysis of the history, examination of the signs or symptoms, evaluation of the research or testing, and investigation of probable causes.

Reference Section - Contents

IEC 61508/IEC 61511 standards	18
Certification	18
SIF designs	18
PFDavg for low, high and continuous modes of operation	19
Systematic and random capability	19
Architectural Constraints, Probability of Failure, Systematic Capability	19
Safe failure fraction and FMEDA	20
SIL and reliability	20
Site acceptance test	21
Factory acceptance test	21
FAT recommendations	21
FAT documentation	21
Guidance on SIS response time requirements	22
Proof-tests – comprehensive and partial	23
Does a partial test impact device reliability?	23
Calculating the PFD of a 1oo1-system without partial testing	24
Calculating the PFD for a 1oo1-system with partial testing	24
Conclusion	25
What is the effect of PTC on PFDavg when partial proof-testing is performed?	25
Conclusion	27
SIS IEC 61508 certificate quality evaluation	27
Step 1 - Collect information	27
Step 2 - Assess certification process	27
Step 3 - Review completeness of product certificate information	28
Summary	28
Application example	29

IEC 61508/IEC 61511 standards

IEC 61508 and IEC 61511 are commonly confused. IEC 61508 is an industry-independent standard for safety instrumented systems (SIS), whereas IEC 61511 is one of several industry specific versions of IEC 61508. IEC 61511 is intended specifically for users in the process industry.

An SIS can be designed to conform to IEC 61511, but the individual components (e.g. sensor, logic solver and actuator) should be designed according to IEC 61508, since equipment manufacturers are not considered to be users in the process industry. IEC 61511 requires a comprehensive life-cycle approach.

Certification

Equipment conformance to IEC 61508 is a rigorous process for the manufacturer. It involves not only the hardware and software design of the product, but also the associated processes to maintain the quality of product. There are stringent requirements as to the necessary documentation provided with the product. Consequently, IEC 61508 certification is both a quality stamp and an indication of the equipment's performance with respect to safety applications.

Ideally, conformance to IEC 61508 is audited by an independent third party. These assessors usually issue a compliance report and a certificate. The value of these certificates is dependent on the specific assessor. It is therefore important to ensure that the assessor is accredited by a recognized third-party in the field of functional safety.

It is important to understand that certification is also a business and certification agencies are not all the same. It is therefore recommended to carefully review each individual certificate.

A typical concern is lack of necessary information. For example, if the basic parameters presented in this document are not readily available in an understandable format, the value of the certificate is probably questionable. See section "SIS IEC 61508 certificate quality evaluation" on page 27 for additional details.

SIF designs

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.

Duplex or 2oo2 voting principle improves the integrity of safety systems. If a safety loop failure occurs, the other is still capable of performing the safety function. The duplication of safety loops in a 2oo2 architecture significantly reduces the probability of a false trip, as both safety loops have to fail before the system is shutdown. The key disadvantage is that the probability of failure on demand is twice as high as that of a single safety loop system.

Triplex or voting 2oo3 principle has three safety loops and requires two of these to be functioning correctly. The 2oo3 voting principle requires complete physical separation of the microprocessors. Although the latest systems offer greater diagnostic capability, safety systems based on 2oo3 voting have a probability of failure on demand that is approximately three times higher than 1oo1-based systems.

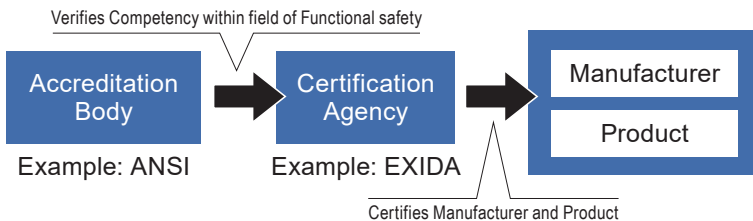


Figure R1: Independent third party auditing

PFDavg for low, high and continuous modes of operation

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.

When the allocation has sufficiently progressed, the safety integrity requirements, for each safety function allocated to the safety system, shall be specified in terms of the SIL in accordance with Table 1 or Table 2 and shall indicate whether the target failure measure is either low demand mode or high demand mode.

Low demand mode is where the frequency of demands for operation made on a safety system is no greater than one per year. Table 1 shows the average probability of dangerous failure on demand of the safety function, (PFDavg), for a low demand mode of operation.

High demand or continuous mode is where the frequency of demands for operation made on a safety-related system is greater than one per year. Continuous mode is regarded as very high demand. Table 2 shows the average frequency of a dangerous failure of the safety function [h-1], (PFH), for a high or continuous demand mode of operation.

Safety integrity levels – target failure measures for a safety function operating in low demand mode of operation

Safety Integrity Level	Probability of failure on Demand per year (or low demand)
SIL-4	$\geq 10^{-5}$ to $< 10^{-4}$
SIL-3	$\geq 10^{-4}$ to $< 10^{-3}$
SIL-2	$\geq 10^{-3}$ to $< 10^{-2}$
SIL-1	$\geq 10^{-2}$ to $< 10^{-1}$

Figure R2: Safety integrity level (SIL) Average probability of a dangerous failure on demand of the safety function

Safety integrity levels – target failure measures for a safety function operating in high demand mode of operation or continuous mode of operation

Safety Integrity Level	Probability of Dangerous failure per hour (Continuous mode or high demand)
SIL-4	$\geq 10^{-9}$ to $< 10^{-8}$
SIL-3	$\geq 10^{-8}$ to $< 10^{-7}$
SIL-2	$\geq 10^{-7}$ to $< 10^{-6}$
SIL-1	$\geq 10^{-6}$ to $< 10^{-5}$

Figure R3: Safety integrity level (SIL) Average frequency of a dangerous failure of the safety function [h-1]

Systematic and Random Capability

Safety integrity level (SIL) is separated between systematic (human) errors and random hardware failures. Systematic capability indicates human-related factors involving processes, whereas random capability indicates product specific safety performance with respect to random hardware failures.

Architectural Constraints, Probability of Failure, Systematic Capability

Architectural Constraints, Systematic Capability and Probability of Failure are three parameters, evaluated to determine the SIL of a product used in a SIF. Architectural Constraints are evaluated by FMEDA through the rules of Route 1H or Route 2H. The Probability of Failure requires the random probability of a failure to be calculated (PFDavg) for low demand mode of operation or PFH for high or continuous demand modes. Systematic Capability requires equipment to be designed using procedures intended to prevent systematic design errors and is evaluated through an assessment of the quality management system.

Route 1_H uses SFF (calculated by lab testing or FMEDA) to determine the minimum HFT for a given SIL. Route 2_H uses failures rates from historical data from a device.



Systematic Capability: SC 3 (SIL 3 Capable)
Random Capability: Type B Element
SIL 2 @ HFT=0; Route 1_H
PFH/PFD_{avg} and Architecture Constraints
must be verified for each application

Figure R3: Example excerpt from an IEC 61508 Certificate

End users need to know both the systematic and random capability to ensure they are meeting the required risk reduction for the system. Consequently, it is important that the IEC 61508 certificate specifies the attained SIL for both systematic and random failures separately.

Safe failure fraction and FMEDA

In order to calculate the SFF, a vendor or third-party assessor provides a FMEDA report. The FMEDA analysis considers:

- The failure rate of individual components
- Failures that must be detected, depending on what SFF must be achieved
- Safe detected, safe undetected, dangerous detected, dangerous undetected failures for each component
- The ratio of safe failures and dangerous detected failures to total failures
- Built-in diagnostics which can change dangerous undetected failures to dangerous detected failures

The SFF describes the fraction of safe failures and detected dangerous failures related to the total failure rate. IEC 61508 standard defines the SFF as the “fraction of the overall failure rate of a subsystem that does not result in a dangerous failure.” Failures are considered as non-hazardous if they cannot put the system in a dangerous state. The higher the SFF value, the lower the probability of a dangerous system failure. A value of 91% signifies that 91 out of 100 failures do not have an impact on the safety system function. By increasing product quality and reducing the number of Dangerous Undetected failures, this will lead to an increase in the SFF.

$$SFF = \frac{\lambda^{SD} + \lambda^{SU} + \lambda^{DD}}{\lambda^{SD} + \lambda^{SU} + \lambda^{DD} + \lambda^{DU}}$$

Failure rate types

- λ^{SD} = Safe Detected failure rate
- λ^{SU} = Safe Undetected failure rate
- λ^{DD} = Dangerous Detected failure rate
- λ^{DU} = Dangerous Undetected failure rate

SIL and reliability

Reliability engineering involves theoretical concepts and calculations and may appear complex and difficult. For example, few people have a comprehensive understanding of a lambda (λ) value and its use. One way of visualizing these numbers is a pie-chart of the PFDavg value. The size of the pie-chart represents the assigned “SIL loop contribution”, and the individual segments represent the contribution from the various sub-systems. Since the risk reduction factor is the inverse of the PFDavg value (RRF=1/PFDavg):

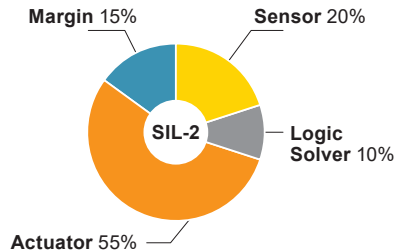


Figure R4: Example #1: SIL 2 Overfill PFDavg = 0.00125
 RRF = 800

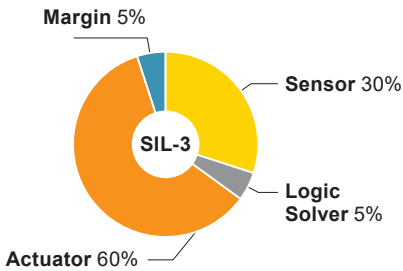


Figure R5: Example #2: SIL 3 Overfill PFDavg = 0.0008
RRF = 1250

- A large segment represents a large probability of failure (and low risk reduction factor)
- A small segment represents a small probability of failure (and high risk reduction factor)

Calculating a sub-system's contribution to the total PFD_{avg} requires multiple inputs, such as

- λ_{DU}
- Common cause β (if redundancy used)
- Mission time (MT)
- Proof-test intervals (TI)
- Proof-test coverage (PTC)
- Redundancy/hardware fault tolerance (HFT)
- SIS assigned RRF (or PFD_{avg})

The PFD_{avg} calculation for a sensor is often performed using a software package. An equipment manufacturer competent in functional safety will be able to calculate this number if adequate data is provided. Visualizing the RRF is useful for a comprehensive understanding of the various numbers associated with an SIS. A lower PFDavg is better and the number is usually below 30%.

$$\lambda_{DU} \left[\left(PTC \times \frac{TI}{2} \right) + (1 - PTC) \frac{MT}{2} \right]$$

Site Acceptance Test (SAT)

A SAT is performed to verify that the equipment has been commissioned correctly. The purpose is to detect systematic (human) failures, such as incorrectly configured set-points. Consequently it is an important procedure to ensure the SIS will function correctly. Depending on methodology,

the cost to execute a SAT can be significant and therefore an important consideration and selection parameter. The equipment manufacturer will provide a generic SAT procedure that often needs to be customized for the specific installation.

Factory Acceptance Test (FAT)

A FAT is performed to verify the system and its components function properly, all manufacturing assembly software generation and configuration have been completed correctly and the system performance is in compliance with the agreed procurement specification. The objective of a FAT is to test the logic solver and associated software together, to ensure that it satisfies the requirements defined in the Safety Requirement Specification. By testing the logic solver and associated software prior to installation, errors can be readily identified and corrected.

FAT Recommendations

The need for a FAT should be specified during the design phase of a project. The planning of a FAT should specify the following:

- Types of test to be performed
- Test cases, test description and test data
- Dependence on other systems/interfaces
- Test environment and tools
- Logic solver configuration
- Criteria for when the test is considered complete
- Procedures for corrective action in case of failure of the test
- Test personnel competencies
- Location of test

For each FAT, the following should be addressed:

- The version of the test plan being used
- What is actually being tested
- A chronological record of the test activities
- The tools, equipment and interfaces used

FAT Documentation

FAT documentation forms part of the overall safety system documentation and according to IEC 61511-1 should contain: (1) the test cases, (2) the test results, and (3) whether the objectives and the test criteria have been met. If there is a failure during the test, the reason should be documented and analyzed and corrective actions implemented.

Guidance on SIS response time requirements

The response time of an SIS begins when the process is at the trip condition and ends when the final control elements reach their safe state. The maximum permitted response time for the SIF must be less than the time to prevent a hazard.

Requirements to manually bring the process to a safe state should be defined. For example, if there is a requirement for the operator to be able to manually shutdown a piece of equipment from either the control room or a field location, then this should be specified. Any requirement for independence of manual shutdown procedures from the SIS logic solver should also be defined, as must the response time requirements for each SIF to bring the process to a safe state within the process safety time.

The response time requirement of a typical emergency shut down (ESD) system - from detecting a fault or alarm to completion of an action by an output device - will vary considerably, according to the nature of the process under control. For example, a safety function with an input transmitter or switch as a sensor and a valve as a final element, would normally give a response time better than 10 seconds – with the operating time of the valve being the dominant factor. The response time of the functional safety system – in the range 50 to 200 ms – is significantly faster

than that of a typical valve, enabling much lower response times when combined with faster acting final elements.

The response time of a safety function is calculated when preparing the safety requirements specification. The response time is the sum of the sensing element's scan time, execution time of the logic, and actuation time for the final element. When determining the response time, the first thing to consider is the process safety time or the time for the process to move from the safety function trip point to the harmful accident. The SIF response time must be considerably faster than this to prevent the accident. One accepted rule of thumb is that the response time should generally be less than half of the process safety time. This helps ensure that even if the hazardous condition presents itself at the end of a scan cycle, the SIF will still have enough time to react.

The following equation is used to calculate the safety response time:

$$\text{SRT} = \text{PST} - \text{TTT} - (\text{PRT} + \text{SMT})$$

SRT = Safety response time
 PST = Process safety time
 TTT = Time to trip
 PRT = Process response time
 SMT = Safety margin time

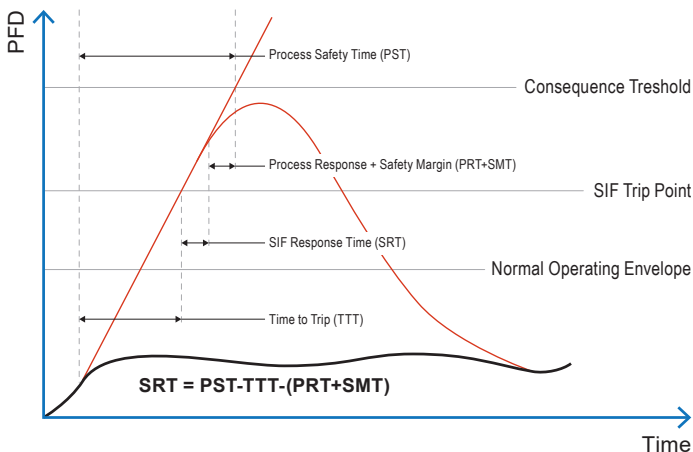


Figure R6: Response time calculation example

Transmitter	Safety analog input module	Safety controller	Safety DI/DO digital I/O module	Pilot and control valve
Response time				
50 ms	30 ms	100 ms	10 ms	4 s

Figure R7: Process response time calculation example

The typical response time for the system outlined above is:
 $0.05 + 0.03 + 0.1 + 0.01 + 4 = 4.19$ seconds (i.e. within the 10 second process safety time)

The ‘worst-case’ response time for the system outlined above (which would occur when the transmitter input cycles and analog input module become un-synchronized, causing their individual contribution to the response time to double) is:
 $0.05 * 2 + 0.03 * 2 + 0.1 + 0.01 + 4 = 4.27$ seconds (i.e. still within the process safety time)

Proof-tests – comprehensive and partial

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

Some equipment manufacturers offer multiple proof-test procedures, with different coverage factors, sometimes denoted “partial” and “comprehensive” proof-testing. The advantage with partial proof-testing is quicker completion and less interference with operations.

The disadvantage is that only parts of the equipment

are tested, and consequently provide a lower test coverage factor. Sometimes a combination of the two types of procedure is advantageous.

Depending on the methodology, the implications of executing a proof-test can be considerable:

- Requires many man-hours to perform the test
- Interferes with daily operations
- Creates a safety risk to both process and personnel

It is not uncommon that the operational expenditure (OPEX) to conduct proof-testing during the life-time of the SIS exceeds the initial capital expenditure (CAPEX). Consequently, proof-testing needs to be carefully reviewed and included as one of the key parameters when selecting a level sensor.

Does a partial test impact device reliability?

Device reliability cannot be increased by performing a partial test, but it will reduce the level of undetected failures. The purpose of the partial test is to cover as much of the remaining undetected failures to increase the reliability of the SIF. Dangerous undetected failures can exist in a device until the SIF is required to prevent a hazard.

Failure mode	λDU Failure Rate (per year)	Detected by partial stroke testing?
(PST) Solenoid fails to vent	0,005	Yes
(PST) Valve sticks open	0,004	Yes
(NT) Valves do not fully close or pass	0,001	No
(NT) Other unknown failures	0,006	No
Total	0,016	

Figure R8: Calculating the PFD of a 1oo1-system without partial testing

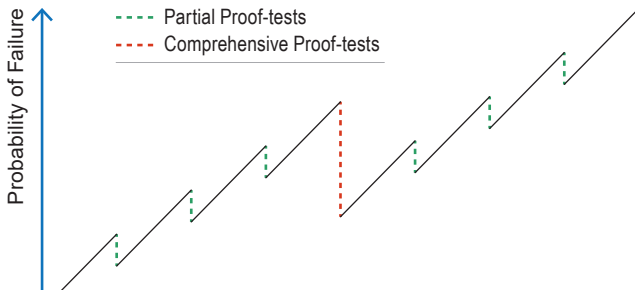


Figure R9: Test coverage of partial and comprehensive proof-testing

Calculating the PFD of a 1001-system without partial testing

The following equation explains how to calculate PFD:

$$\text{PFD avg} = \lambda \text{DU} * \text{TI} / 2$$

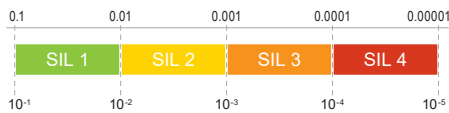
Where:

- λDU = Dangerous undetectable failure rate
- TI1 = Time interval between manual functional tests of the component (hours)
- TI2 = Mission in time corresponding to the end of life or the process equipment or a period of time between each major shutdown and overhaul/replacement of all equipment (years, hours)
- Risk reduction factor = $1/\text{PFDavg}$

For example, if the final element is a valve that is required to close to achieve the safety function, and we assume that there is no partial stroke testing and the plant is shut down every four years, then the PFD for this valve would be:

$$\text{PFD avg} = \lambda \text{DU} * \text{TI} / 2 =$$

$$0,016 * 4 (\text{yr}) / 2 = 0,032 = 3,2\text{E-}2 = \text{SIL 1 RRF 31,25}$$



Calculating the PFD for a 1001 system with partial testing

However, with partial stroke proof-testing every three months (0.25 years):

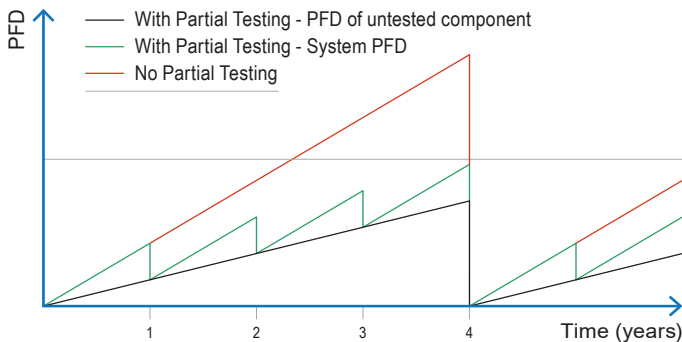


Figure R10: How PFD changes over time with partial testing

$$\text{PFDavg} = \lambda \text{DU} * \text{TI1} / 2$$

Covered by proof-test

$$+ \lambda \text{DU} * \text{TI2} / 2 =$$

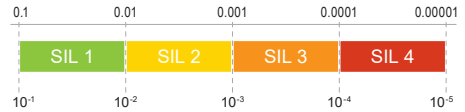
not covered by the proof-test

$$(0,005 + 0,004) * 0,25 / 2$$

$$+ (0,001 + 0,006) * 4 / 2$$

$$= 0,001125 + 0,014 = 0,015 = 1,5\text{E-}2 = \text{SIL 1} =$$

RRF = 66 Higher SIL 1 (Lower PFDavg)



This means the instrumented function would fail during a dangerous scenario about once every 1,000 years. In this example, the PFDavg of the valve is more than halved as a result of the partial stroke proof-testing.

This partial valve test is assumed to be a proof-test, not a diagnostic test, since it does not detect and action failures found within the specified mean time to repair (which has been assumed to be very small in this case).

In the above equation, note that the first term on the right-hand side refers to failures of the system detected during partial stroke testing and the second term refers to the remaining failures that are only tested every four years during a shutdown. Therefore, even if the partial stroke testing was performed almost constantly (e.g. every hour = 0.0001 years), such that the first term became almost zero, the minimum PFDavg value would be 0.014. With partial stroke testing, the SIF is only as strong as the weakest link (i.e. device with the highest PFDavg value).

This shows the effect of partial testing (i.e. it does not matter if you test part of the system very well), the failure rate will eventually be dominated by the parts of the system that are not tested.

Note that in the graph the PFD varies over time, and PFD is the probability of failure for a simplex non-redundant system, not PFDavg.

PFDavg is the preferred measure when:

- SIF operates in the low-demand mode, with demands occurring less than once per year.
- SIF operates independently of the EUC control system (and if relevant, any other SIS installed).
- The red line represents the scenario where no partial testing is performed. Only a full test is done every four years.
- The blue line represents the PFD of the system with partial testing. Note that the PFD of the untested part of the system (black line) increases until four years when a full test is carried out. By the end of the four years, the PFD is dominated by the untested part of the system.
- The purple line represents the required performance.

Conclusion

When a proof-test is executed it will only find a portion of the λ DU, indicated by the PTC (also known as Cpt). In a low demand system, the object is to discover dangerous failures through proof-testing before they are discovered by real demand. For this reason, the demand frequency should be considerably lower than the proof-testing frequency.

PFDavg is the average probability of failure on demand, which is the correct measure to use since the probability changes over time. The probability of the system failing will depend on how long ago it was tested. A safety-related product is designed to have a particularly low failure rate.

With partial proof-testing, the demand frequency should be considerably lower than the worst-case proof-test frequency (in the above example it would be considerably lower than every four years). The higher the probability of the system failing, the lower the risk of a hazardous situation.

What is the effect of PTC on PFDavg when partial proof-testing is performed?

The effectiveness of proof-testing is not negligible and has a significant influence on the final PFDavg. The effectiveness of a proof-test is measured by its PTC. The proof-test coverage factor is the fraction of dangerous undetected failures which can be detected by proof-testing. PTC is the term given to the percentage of dangerous undetected failures exposed by a defined proof-test procedure.

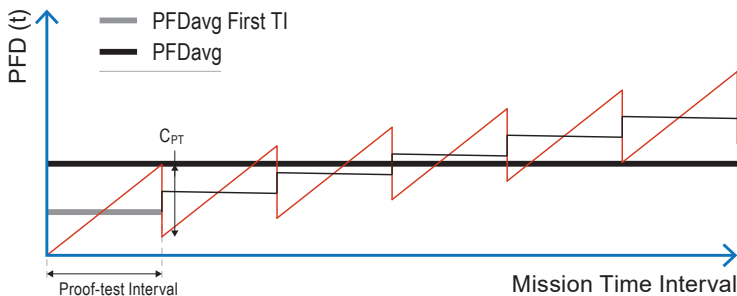


Figure R11: The effect of PTC on PFDavg when partial proof-testing is performed

Cpt (PTC)= λDU (identified by PT) / λDU (total)

- Cpt = Proof-test coverage
- λDU (identified by PT) = Dangerous undetected failure rate identified by the proof-test
- λDU (total) = Total dangerous undetected failure rate
- MT (or T12) = Mission in time corresponding to the end of life or the process equipment or a period of time between each major shutdown and overhaul/replacement of all equipment
- Risk reduction factor = 1/PFDavg

Using the above calculation and adding the Cpt:

$$PFD_{avg} = \lambda DU * T1 * Cpt / 2 + \lambda DU * MT * (1 - Cpt) / 2 = MT \gg T1$$

Mission time (MT) is the period of time over which the SIF has to function, without requiring a major overhaul and/or replacement of its equipment. MT is not the same as Useful Life (the time specified by the manufacturer for its product to function before requiring replacement). Since an SIF has different equipment, with each piece of equipment having a different Useful Life, choosing the MT is very important, especially with regards to the target SIL. With imperfect proof-testing, MT plays a crucial role in determining the effective SIL of the SIF.

With a PTC of 80%:

$$PFD_{avg} = \lambda DU * T1 * Cpt / 2 + \lambda DU * MT * (1 - Cpt) / 2 =$$

$$(0,005 + 0,004) * 0,25 * 0,8 / 2 + (0,001 + 0,006) * 4 * (1 - 0,8) / 2$$

$$= 0,001125 * (0,8) + 0,014 * (1 - 0,8) = 0,0009 + 0,0028 = 0,0037 = 3,7E - 3 = SIL 2 RRF = 270$$

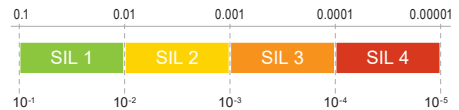
With a PTC of 94%:

$$PFD_{avg} = \lambda DU * T1$$

$$* Cpt / 2 + \lambda DU * MT * (1 - Cpt) / 2 =$$

$$(0,005 + 0,004) (PT) * 0,25 * 0,94 / 2 + (0,001 + 0,006) * 4 * (1 - 0,94) / 2$$

$$= 0,001125 * (0,94) + 0,014 * (1 - 0,94) = 0,0010575 + 0,00084 = 0,002175 = 2,175E - 4 = SIL 3 RRF = 4597$$



Safety Integrity Level	Probability of failure on Demand per year (or low demand)	Risk Reduction Factor	Probability of Dangerous failure per hour (Continuous mode or high demand)
SIL-4	≥ 10 ⁻⁵ to < 10 ⁻⁴	from 100 000 to 10 000	≥ 10 ⁻⁹ to < 10 ⁻⁸
SIL-3	≥ 10 ⁻⁴ to < 10 ⁻³	from 10 000 to 1 000	≥ 10 ⁻⁸ to < 10 ⁻⁷
SIL-2	≥ 10 ⁻³ to < 10 ⁻²	from 1 000 to 100	≥ 10 ⁻⁷ to < 10 ⁻⁶
SIL-1	≥ 10 ⁻² to < 10 ⁻¹	from 100 to 10	≥ 10 ⁻⁶ to < 10 ⁻⁵

Figure R12: Failure probabilities

Conclusion

Will the PFDavg be affected by a higher proof-test coverage? Yes and no. A high SFF means the built-in device diagnostics has typically identified most of the dangerous undetected failures or the most serious of the dangerous undetected failures.

SIS IEC 61508 certificate quality evaluation

All level sensors in an SIS are a critical component of safety. It is therefore highly recommended, for quality assurance, that this type of equipment is certified to IEC 61508. However, it is important to realize that certification is a big business in itself. Consequently, all “certificates” are not equal. This section will provide guidance on assessing the quality of an individual certificate, and distinguishing the “good” from the “bad”.

Step 1 - Collect information

Different vendors and certification bodies use slightly different terminology and document structures, but typically the relevant information is available from two different sources:

Product specific information from the equipment manufacturer

- IEC 61508 Certificate
- Safety Manual
- Data Sheet

Certification body

- Proof of 3rd party accreditation of the certification body with respect to functional safety and IEC 61508

- Description of certification body’s IEC 61508 certification process

Step 2 - Assess certification process

Who gives the certification body the right to issue a certificate? The generally accepted industry practice involves an independent accreditation body that ensures the certification body is competent and consistently delivers high quality work.

Especially with safety critical devices and information, self-declarations from equipment manufacturers or self-proclaimed certification bodies without independent accreditation shall not be accepted. To assess the quality of the certification process:

1. Determine who has accredited the certification body that has issued the product’s IEC 61508 certificate. Make sure the accreditation is within the field of functional safety and IEC 61508 specifically (generic accreditation has little or no value in this context). Only accept internationally accepted accreditation bodies.
2. Ensure the certification body has a thorough description of their IEC 61508 certification process.

This will ensure the certification body is competent and has a solid process to produce high quality safety certificates consistently.

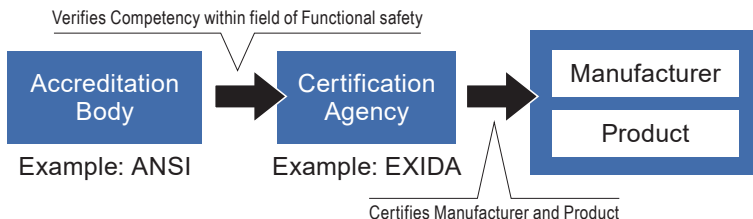


Figure R13: Independent third party auditing

Step 3: Review completeness of product certificate information

Review the IEC 61508 certificate for completeness by ensuring the following information is available:

1. Documentation: Safety manual
2. Documentation: IEC 61508 certificate
3. Documentation: IEC 61508 certification process
4. Certification: Standard (shall state IEC 61508:2010 or IEC 61508 Edition 2)
5. Certification: Parts (shall state Part 1 to 7)
6. Certification: Body
7. Certification: Body's IEC 61508 accreditation
8. Systematic Capability (SIL1-3)
9. Random Capability (SIL1-3)
10. Failure Rates: λ_{safe}
11. Failure Rates: λ_{DD}
12. Failure Rates: λ_{DU}
13. Proof-test: Documented procedure
14. Proof-test: Documented coverage factor
15. Site Acceptance Test (SAT): Documented procedure
16. Response Time

Summary

This chapter provides a methodology for assessing the quality of a product's IEC 61508 SIS Certificate in three simple steps, as depicted in figure R14. The methodology evaluates the completeness of basic safety information. The methodology does not assess the safety performance, which needs to be addressed separately (i.e. what SIL is required).

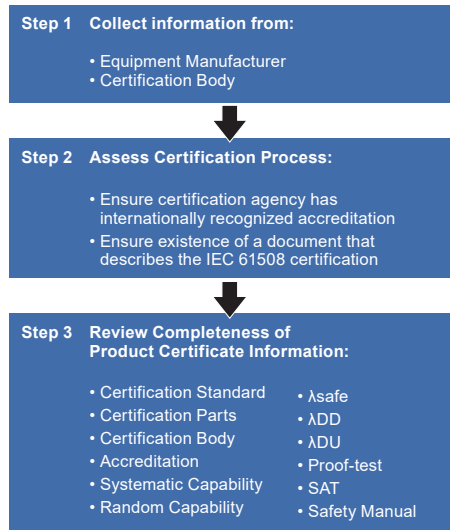


Figure R14:: Methodology for assessing the quality of a product's IEC 61508 SIS certificate

Application example: Floating roof tank SIL 2 SIS with a Rosemount 5900S 2-in-1 Non-Contacting Radar Gauge

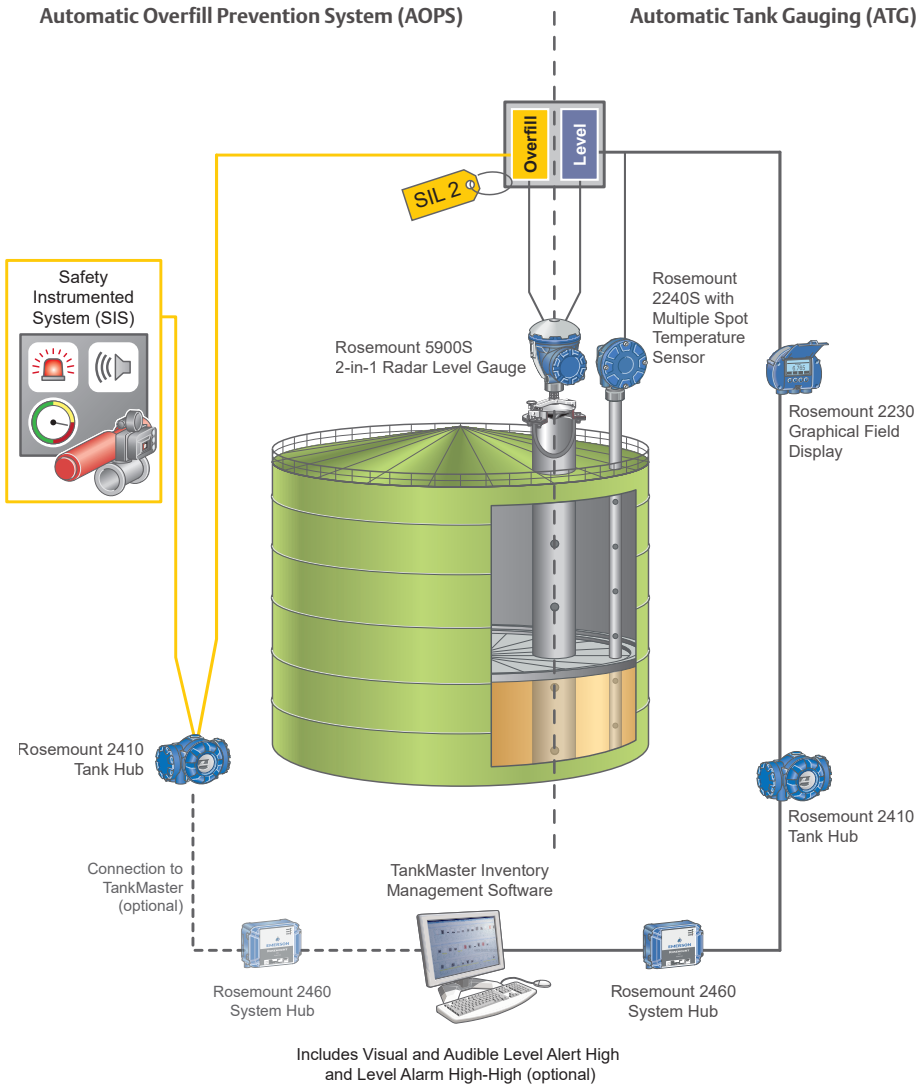


Figure R15: A Rosemount 5900S 2-in-1 Non-Contacting Radar Level Gauge is a frequently used solution for bulk liquid tanks with floating roofs due to the combination of custody transfer grade accuracy and easy installation with minimal tank modifications

The table below is the engineering specification for a tank equipped with Rosemount 5900S. This provides all the necessary data from to perform proof-testing calculations.

Engineering Specification Level sensor for usage in overfill prevention systems (OPS) TK102: Bulk liquid storage floating roof tank		
Section	Parameter	Value
1. Overfill Prevention System (OPS)	OPS Name	OPS-102
	OPS Description	Automatic overfill prevention system tank 102
	OPS Tag	TK102-AOPS
	Safety Certified (SIS/IEC 61511 Compliance)	N/A SIL 1 SIL 2 SIL 3
	Level Sensor Redundancy/Voting (Hardware Fault Tolerance)	Single level transmitter for OPS (HFT=0) Dual level transmitters for OPS with 1oo2 voting (HFT=1) Triple level transmitters for OPS with 2oo3 voting (HFT=1)
2. Basic Process Control System (BPCS) - Informative	BPCS LT Name	Rosemount 5900S 2-in-1
	BPCS LT Tag	TK102-LT
	BPCS LT Measurement Technology	10 GHz FMCW radar
	BPCS LT Accuracy	Custody transfer accuracy according to OIML R85:200. ± 0.020 in. (0.5 mm) instrument accuracy
	BPCS LT Measurement Range	0 to 66.601 ft (0 to 20.3 m)
	BPCS Alarms and Alerts	Level Alarm High High (LAHH) Level Alert High (LAH) Maximum working level (MWL)

3. General OPS Level Sensor Information	OPS LT Name	Rosemount 5900S 2-in-1
	OPS LT Tag	TK102-LAHH
	Manufacturer	Emerson
	Model	Rosemount 5900S
	Model-code	5900SPS2F1R1A21A8SHH8A0QT
	Measurement Type	Continuous level Point level
	Direct/Indirect Measurement	Direct measurement Indirect measurement
	Instrument's Primary Usage	Sensor for overfill prevention system Level Alarm High High (LAHH) Level Alert High (LAH) Maximum working level (MWL)
	Instrument Secondary Usage	Verify BPCS-LT measurement Backup if BPCS-LT fails N/A
	Mounting Position	8-in. still-pipe
	Measurement Technology	Non-contacting Radar
	Measurement Principle	FMCW 10 GHz
		OPS/BPCS Level Sensor 2-in-1
OPS/BPCS Measurement Technologies		Same technology acceptable for both OPS and BPCS Level Measurement (this is the normal case and compliant with international standards) Different technologies required for OPS and BPCS Level Measurement (technology diversification)
4. Alarms and Alerts	Instrument Response Time	Max 60 seconds
	Set-point: Level Alarm High High (LAHH)	0 to 60.532 ft (0 to 18.45 m)
	Set-point: Level Alert High (LAH)	0 to 59.383 ft (0 to 18.1 m) N/A
5. Tank Data	Tank Name	TK102
	Service	Storage tank
	Tank Type	Floating roof
	Tank Dimensions	Diameter: 100 ft (30 m) Height: 68.898 ft (21 m)
	Tank Connection(s)	8-in. Pipe, Flange, 8-in. ANSI 150#

6. Process Conditions	Product	Crude oil	
	State	Liquid Solid	
		Max	Min
	Pressure (barg)	Atmospheric	Atmospheric
	Temperature	95 °F (35 °C)	41°F (5 °C)
	Other	Foam Vapors Condensation/build-up Agitation Surface turbulence Dust Corrosive Other (please specify)	
7. Instrument Specification		Min	Max
	Range, Level	0	60.60 ft (20.3 m)
	Range, Distance	500	68.24 ft (20.8 m)
	Max Level Rate	0.2 in./s (5 mm/s)	
	Accuracy	Same as BPCS	
	Communication Signal	4-20 mA Discrete Modbus	
	Power Supply	230 Vac	
	Ambient Temperature	95 °F (35 °C)	
	Hazardous Location	ATEX Exd or ATEX Exia	
	Enclosure	Painted aluminum housing with M20 connections	
	Wetted Materials	316/316L SST	
	Transient/Lightning Protection	IEC 61000-4-4-5, IEEE 472, IEEE 587 Cat B	
	Field Proven Mean Time To Fail (MTTF/MTBF)	Minimum 150 years	
	Safety Marking	Yellow tag	
	Average Mean Time To Repair (MTTR)	4 to 8 hours	
Maintenance	Instrument shall be maintenance-free		

8. SIS/SIL (IEC 61508/ IEC61511)	Certification Standard	IEC 61508:2010		
	Certification Body	Exida		
	Certification Body's Accreditation	ANSI		
	Systematic Capability	SIL 3		
	Random Capability	SIL 2		
	Safety Manual	Required		
	Mission Time	8 years		
	Failure Rates	λ_{safe}	λ_{DD}	λ_{DU}
		719 FIT	1758 FIT	218 FIT
	SIL	OPS Reliability	OPS Risk Reduction	Sensor % of PFD _{avg}
PFD _{avg} = 0.005		RRF = 200	41%	
9. Site Acceptance Test (SAT)	SAT Document	Safety manual		
	Procedure	Local test acceptable (tank access required) Remote test acceptable (from control room) Tank out of service acceptable Tank out of service NOT acceptable Process alteration acceptable		
	Mean Time for Completion	Maximum 4 hours		
	Tools/Data Required	Digital multimeter; hand tape or verified BPCS-LT reading		
	Personnel Safety Concerns	Follow normal procedures for manual level measurement and 4-20 mA current measurement		
	10. Proof-test	Document	Safety manual	
Time Interval		12 months		
Coverage (% of λ_{DU})		84%		
Procedure		Local test acceptable (tank access required) Remote test acceptable (from control room) Tank out of service acceptable Tank out of service NOT acceptable Process alteration acceptable		
Mean Time for Completion		Maximum 30 minutes		
Tools/Data Required		Multimeter		
Personnel Safety Concerns		OPS shall be de-activated during proof-test and therefore no on-going emptying/filling operations		

The Emerson logo is a trademark and service mark of Emerson Electric Co.
Rosemount is a mark of one of the Emerson family of companies.
All other marks are the property of their respective owners.
© 2020 Emerson Electric Co. All rights reserved.



[Youtube.com/user/RosemountMeasurement/](https://www.youtube.com/user/RosemountMeasurement/)



[Facebook.com/Rosemount](https://www.facebook.com/Rosemount)







[LinkedIn.com/company/Emerson-Automation-Solutions](https://www.linkedin.com/company/Emerson-Automation-Solutions)



[Twitter.com/Rosemount_News](https://twitter.com/Rosemount_News)




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 Europe GmbH

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




Middle East & Africa Regional Office Emerson Automation Solutions

Emerson FZE P.O. Box 17033
Jebel Ali Free Zone - South 2
Dubai, United Arab Emirates

 +971 4 811 8100
 +971 4 886 5465
 RFQ.RMDMEA@Emerson.com

Asia Pacific Regional Office Emerson Automation Solutions

1 Pandan Crescent
Singapore 128461

 +65 6777 8211
 +65 6777 0947
 Enquiries@AP.Emerson.com