



The Engineer's Guide to Level Safety Instrumentation and Overfill Prevention

2020 EDITION



Introduction

Why Invest?

Key Elements

Regulatory Requirements

Industry Standards

Risk Assessment

Overfill Management System

Overfill Prevention System

Proof-Testing

Available Technologies

Rosemount™ Products

**Overfill Prevention
System Examples**

References

ISBN 9789198277906



57599 >



9 789198 277906



“The quality of this book makes it the primary educational tool for the global process and bulk liquid storage industry to reduce the number of tank overfills”

Phil Myers,

Co-author and former API 2350 Committee Chairman

“If multiple layers of protection such as an independent high level alarm or automatic overflow prevention system had been present, this massive release [Puerto Rico, 2009] most likely would have been prevented.”

Vidisha Parasram,

Investigator at US Chemical Safety and Hazard Investigation Board (CSB)

Legal disclaimer

This book is designed to provide information on overfill prevention only.

This information is provided with the knowledge that the publisher and author are offering generic advice which may not be applicable in every situation. You should therefore ensure you seek advice from an appropriate professional.

This book does not contain all information available on the subject. This book has not been created to be specific to any individual's or organizations' situation or needs. Every effort has been made to make this book as accurate as possible. However, there may be typographical and or content errors. This book 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 book or the information, products, services, or related graphics contained in the book or report for any purpose. Any reliance you place on such information is therefore strictly at your own risk. Therefore, this book should serve only as a general guide and not as the ultimate source of subject information. In no event will we 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 this information. You hereby agree to be bound by this disclaimer or you may return this book.

All rights reserved. No part of this book 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 authors.

Table of contents

| | | |
|-----|-------------------------------------|-----|
| 1. | Introduction | 11 |
| 2. | Why invest? | 15 |
| 3. | Key elements | 29 |
| 4. | Regulatory requirements | 37 |
| 5. | Industry standards | 43 |
| 6. | Risk assessment | 49 |
| 7. | Overfill management system | 57 |
| 8. | Overfill prevention system | 61 |
| 9. | Proof-testing | 67 |
| 10. | Available technologies | 81 |
| 11. | Rosemount products | 85 |
| 12. | Overfill prevention system examples | 93 |
| 13. | References | 113 |

Abbreviations

| | |
|--------------------------|--|
| 1oo1 | One out of one |
| 1oo2 | One out of two |
| 2oo3 | Two out of three |
| AOPS | Automatic overfill prevention system |
| BPCS | Basic process control system |
| CH | Critical high |
| ESD | Emergency shutdown system |
| FIT | Failures in time; number of failures that can be expected in one billion (10^9) device-hours of operation |
| FMEDA | Failure modes, effects and diagnostic analysis |
| HFT | Hardware fault tolerance |
| in situ | In place; in the context of overfill prevention this implies that the equipment (usually the level sensor) does not need to be unmounted |
| IPL | Independent protection layer |
| LAHH | Level alarm high-high |
| LOC | Levels of concern |
| MOPS | Manual overfill prevention system |
| MTBF | Mean time between failures |
| MTTF | Mean time to fail |
| MTTR | Mean time to repair |
| MWL | Maximum working level |
| OPS | Overfill prevention system |
| PFD | Probability of failure on demand |
| PFD_{AVG} | Average probability of failure on demand |
| RRF | Risk reduction factor |
| SIF | Safety instrumented function |
| SIL | Safety integrity level |
| SIS | Safety instrumented system |

1

Introduction

| Topic | Page |
|---------------------|------|
| 1.1 Purpose_____ | 12 |
| 1.2 Background_____ | 12 |
| 1.3 Scope_____ | 13 |
| 1.4 Structure _____ | 13 |



1. Introduction

What is a tank overflow? In this book it is defined as the point when the product inside a tank rises to the critical high level. This is the highest level in the tank that product can reach without detrimental impact (e.g. product overflow or tank damage) (API 2350,2012).



1.1 Purpose

Does the risk of tank overflow worry you? Then this is the right book for you!

This book provides an objective overview of modern tank overflow prevention techniques based on relevant standards (IEC 61511, API 2350) and current Recognized and Generally Accepted Good Engineering Practice (RAGAGEP).

Robust overflow prevention is not just about fulfilling regulatory requirements and minimizing risk. This book also describes how to increase profits by increasing plant efficiency and reducing labour cost.



1.2 Background

Worrying about tank overfills is logical because there are hundreds of tank spills of hazardous materials every day (United States Environmental Protection Agency, 2014). The stored materials may be hazardous, flammable, explosive, and/or reactive with each other. The spill may affect the drinking water, or if exposed to an ignition source, there is potential for an explosion, which may result in injury to operations personnel, serious property damage, environmental issues, and evacuation of nearby communities. The cost is measured in thousands, millions or even billions of dollars. Previous accidents have proven that this can affect the company's survival.

Another reason to worry about tank overfills is that for a long time overfills have been a leading cause of serious incidents in the process and bulk liquid industries. But overfills do not occur randomly. They are predictable and thereby preventable. This book uses current knowledge and expertise to provide a holistic view of tank overflow prevention and describes how modern equipment can be used to reach closer to the goal of zero tank overfills.

There is no doubt that safety expectations are increasing. One reason is that legislators are becoming more aware due to accidents, and as a result, regulations and permitting are becoming increasingly stringent with larger consequences. It is difficult for the industry to maintain compliance because solutions that were considered acceptable in the past may not conform to current requirements. This book describes the latest advancements in overflow prevention and how to implement future-proof solutions.



Picture 1.1 and 1.2: The Buncefield tank overflow accident in 2005 resulted in costs of billions of dollars (this accident is further described in chapter 2.4)

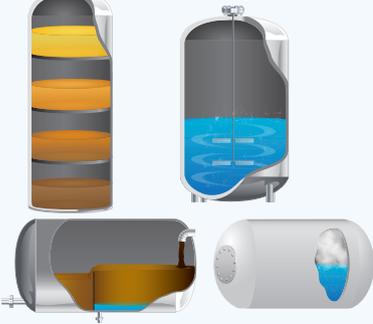
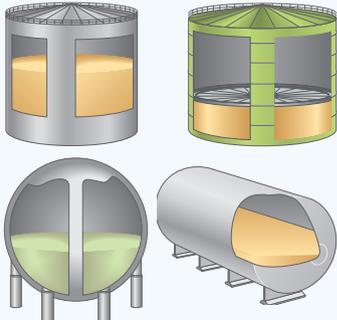
1 - Introduction

1.3 Scope

Although this book is intended for its defined scope (see below), many of the principles are generic and may therefore be used elsewhere.

1.4 Structure

This guide is structured to provide impartial information. The structure is based on the IEC 61511 safety life-cycle. The appendix contains vendor specific information.

| | | |
|----------------------------------|--|---|
| <p>Industry Overview</p> | <p>Process Industry</p>  | <p>Bulk Liquid Storage</p>  |
| <p>Specific Industries</p> | <p>The primary target of this book is the following industries:</p> <ul style="list-style-type: none"> • Petroleum • Chemical / Petrochemical • Power • Food and beverage • Pharmaceutical • Metals and mining • Airports | |
| <p>Spill Causes</p> | <p>This book focuses on overfilling. There are a number of other possible causes for tank spills such as leakage or tank rupture due to corrosion, incorrect couplings or simply that tank openings have been left open during maintenance. The most prominent problem, however, is tank overfills.</p> | |
| <p>Tanks and Stored Products</p> | <p>The material presented in this book is applicable to most tank types and applications containing liquid hazardous substances (e.g. oil and chemicals), but due to the generic approach it is impossible to cover every possible application and there are exceptions such as LNG tanks (Liquid Natural Gas) which are not covered by this book.</p> | |
| <p>Measurement Variables</p> | <p>When filling a tank it is important to be aware of all relevant measurement variables such as pressure, temperature and level. The scope of this book is limited to aspects relating to level measurement and associated systems.</p> | |



2



Why Invest?

| Topic | Page |
|---|------|
| 2.1 Risks Related to Tank Overfills | 16 |
| 2.2 Probability | 16 |
| 2.3 Consequence | 18 |
| 2.3.1 Life and Health | 18 |
| 2.3.2 Environmental Pollution | 18 |
| 2.3.3 Property Damages | 18 |
| 2.3.4 Corporate Social Responsibility | 18 |
| 2.3.5 Public Relations | 18 |
| 2.3.6 Industry Damage | 18 |
| 2.3.7 Legal Consequences | 18 |
| 2.4 Case Examples | 19 |
| 2.5 Additional Risks Associated With Tanks | 27 |
| 2.6 Financial Returns of Modern Overfill Prevention | 28 |
| 2.6.1 Efficiency Increase | 28 |
| 2.6.2 Reduced Cost of Risk | 28 |

2. Why Invest?

This chapter explains why investment in modern overflow prevention is good business because it not only reduces the statistically high risk of a tank overflow but also because it has an immediate positive financial impact.

Why invest in modern overflow prevention?

- **Protect life & health**
- **Protect environment**
- **Protect plant assets**
- **Comply with regulations**
- **Improve public relations**
- **Corporate social responsibility**
- **Increase plant efficiency**
- **Minimize financial & legal risks**

exceeds 100,000 spills of hazardous products per year globally. All of these spills do not necessarily arise from a tank overflow, but the data provides an interesting perspective.

The insurance company Marsh provides an alternative approach focused only on tank overfills, by collecting actual data from the bulk liquid storage industry. According to their research on atmospheric storage tanks, one overflow occurs statistically every 3,300 filling operations (Marsh and McLennan Companies, 2001). This equals one overflow every 10 years for a group of 10 tanks where each tank is filled 3 times per month. Using the same assumptions for a group of 100 tanks, the rate of overflow equals one every year.

Historical industry data indicates:

One overflow every 3,300 fillings

2.1 Risks Related to Tank Overfills

Risk consists of two components: Probability x Consequence. This section exemplifies these two components from a general perspective to establish why there is considerable risk of tank overflow if improper overflow prevention is used. Chapter 6 “Risk assessment” discusses how an assessment of the risk can be estimated for specific tanks and what tools to use.

Risk = Probability x Consequence

2.2 Probability

The probability of a tank overflow can be estimated using historical data. Although individuals and companies may try to conceal spills, the United States environmental agency has been able to report around 14,000 oil spills annually in the United States alone (United States Environmental Protection Agency, 2014). Since the US currently consumes approximately 20% of the world’s oil demand (Central Intelligence Agency, 2015), this equates to 70,000 oil spills globally. Considering there are hazardous substances other than oil, and original data is conservative due to spill concealment and the fact that some countries are less focused on spill prevention than others, the true number probably

2 - Why Invest?

As an alternative to referencing historical data, the probability of failure of overflow prevention equipment can be examined.

Basic Tank Example with Mechanical Level and Independent Switch: What is the Probability of a Tank Overflow?

Assumptions

Tank Operations:

- Two fillings per month

Mechanical Float and Tape Level Measurement:

- Randomly fails dangerously undetected once every five years (e.g. by getting stuck)
- Failure is detected during every transfer
- Repaired when the transfer has been completed

Mechanical Level Switch:

- Randomly fails dangerously undetected once every 10 years
- Proof-tested annually (12 months) and repaired if a failure is detected

Calculation

During 10 years or 120 months of operation, two fillings each month will add up to 240 fillings in total.

Mechanical float and tape level measurement is stated to fail dangerously undetected once every five years. This means two failures during 240 fillings. Since repair is expected to occur directly upon transfer completion, the overall probability of filling with a failed float and tape level measurement is $2/240 = 0.8\%$.

Similarly, the mechanical level switch is expected to fail dangerously undetected only once during the 240 fillings over 10 years. However, with an annual proof-testing, one must expect that each failure remains unnoticed for an average of six months, which translates to 12 fillings assuming two fillings per month. Hence, the probability of filling with a failed mechanical switch is $12/240 = 5\%$.

Altogether, the probability of filling a tank with float and tape level measurement AND the mechanical switch is $0.8\% \times 5\% = 0.04\%$. Alternatively, once every $1/0.04\% = 2,400$ fillings.

Interpreting the Calculations

The result of these calculations can easily be understood by applying them to a tank group consisting of 10 tanks equipped with the above specified equipment. During 10 years, such a tank group would experience 2,400 fillings. Under the given assumptions, there is consequently a 100 percent probability that the mechanical level switch and the mechanical float and tape will simultaneously be non-functional during a tank filling. The operators will be unaware that the level sensors are non-functional and consequently there is a probability that a tank overflow will occur.

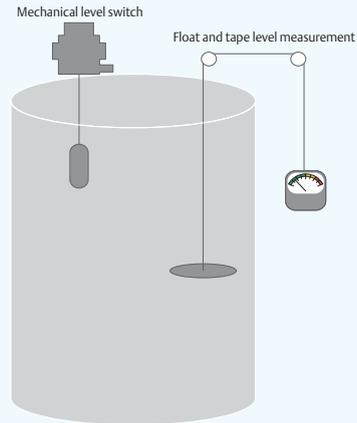


Figure 2.1: Generic tank example with a mechanical level transmitter and an independent switch

Fact box 2.1: Basic tank example with mechanical level and independent switch: What is the probability of a tank overflow? Once every 2400 fillings.

2.3 Consequence

Potential consequences of a tank overfill are detailed below, along with case examples in section 2.4.

2.3.1 Life and Health

A work environment where there is a probability of severe consequences such as personal injuries or even fatalities must be avoided at all costs. The slightest rumor about an unsafe work place or part of a facility will affect reputation, even if an accident has not occurred.

In cases where an accident occurs that involves injuries or fatalities, in addition to personal suffering, claims for the company responsible can be expected.

A case example of fatalities, injuries and evacuation is presented in case 7 “Fatalities, injuries and evacuation”.

2.3.2 Environmental Pollution

Potential environmental pollution from a tank overfill includes many aspects of the local surroundings. Drinking water, air pollution, wildlife and the ecosystems are just a few examples. The local community’s trust is often closely connected to environmental aspects.

When an accident occurs that results in environmental pollution, considerable fines for the responsible company may be expected. Additionally the cost of removing or treating contaminated soil or water (“clean-up”) can be considerable.

Case examples of spill clean-up and clean-water contamination are presented in cases 1 “Spill clean up” and 4 “Clean water contamination”.

2.3.3 Property Damages

Tank overfills may result in both fires and explosions which can cause considerable damage both on and off-site.

A case example of property damages is presented in case 2 “Property damages”.

2.3.4 Corporate Social Responsibility

The process industry operates on the foundation of the public’s acceptance. Tank overfills may considerably impact not only the facility and its personnel, but also the surrounding communities, as described in previous sections of this chapter.

For companies to be viable in the long run they need to be perceived by the public as operating ethically and correctly according to societal values. Fines, additional regulations and inspections, operational changes, ownership adjustments and ultimately

closure are all possible results that can occur if the public’s trust is lost. Implementing modern overfill prevention is one of many required actions to fulfil the public’s expectation on corporate social responsibility.

2.3.5 Public Relations

The news of an accident spreads quickly. Written statements, photos and videos are often made available to the public. This can influence regulators to tighten legislation and increase governmental involvement through additional requirements on safety and more frequent and thorough inspections.

2.3.6 Industry Damage

An accident does not only affect the responsible facility, but also the entire industry. The entire industry is at stake when it comes to incidents.

There are numerous examples where a single tank overfill has affected the entire industry, and a specific case example is presented in case 5 “Corporate fines”.

2.3.7 Legal Consequences

Tank overfills frequently end up in court or with settlements involving both criminal and civil charges. Not only may the responsible company be accused, but also its staff, and there are cases where employees, executives and owners have been imprisoned. Here are a few examples:

- Buncefield, 2005 accident (Case 2 “Property damage”): five companies accused of causing the accident faced criminal prosecution.
- Puerto Rico, 2009 (Case 3 “Bankruptcy”): A joint lawsuit against the responsible company by 1,000 defendants seeking \$500 million in damages. The company went bankrupt.
- Elk River, 2014 (Case 4 “Clean water contamination”): The company went bankrupt due to clean-up costs and lawsuits. The company’s president was indicted on charges of negligent discharge of a pollutant among other alleged violations. Three former owners were indicted on charges of negligent discharge of a pollutant and negligent discharge of refuse matter.
- Jaipur, 2009 (Case 7 “Fatalities, injuries and evacuation”): 20 people were accused of one or more of the following charges: causing death by negligence; public servant disobeying law with intent to cause injury to any person; punishment of criminal conspiracy; and punishment for attempting to commit offences punishable with imprisonment for life or other imprisonment.

2.4 Case Examples

This section provides information about the actual consequences that can occur from a tank overflow using specific case examples.

All the examples included relate to spills, but some of them are not a direct result of a tank overflow. However, these examples are included to show the potential consequences of a tank overflow; the result is similar independently of how the spill occurred.

Deflagration and Vapor Cloud Explosions

If an organic, volatile and flammable compound's air mixture exists in an open space - as might be caused by a tank overflow of propane, natural gas, or gasoline, then an ignition source may result in an explosion. Safety engineers distinguish the explosion by considering a few key characteristics of the explosion.

Deflagration

In a deflagration, the combustion process of the burning wave front initiated at the ignition source propagates through the flammable mixture at subsonic speeds. The hazard is the flame or flash fire that at high temperature has the potential to burn equipment, people, and ignite other flammable liquid sources, creating the potential for fire escalation and other safety hazards.

Vapor Cloud Explosion

In a vapor cloud explosion or (VCE) the burning flame front travels above the speed of sound and a compression wave is set up. The high pressure shock wave or blast wave by itself (even if there were no heat) is sufficient to cause fatalities and to create major damage to facilities and structures.



Picture 2.1: Refinery explosion

Fact box 2.2: Deflagration and vapor cloud explosion

Spill Clean-up

Western Massachusetts, United States, 2005

Sequence of Events

Small facility with a single operator present while a bulk liquid storage tank was filled through a pipeline. The operator thought that he would have time to go to the bar across the street for a quick beer. Suddenly the bartender points out that diesel is shooting out from a tank vent. The operator runs back to the terminal to close a valve in order to shut down the flow of incoming product. As a result of this tank overfill, 23,000 gallons of diesel was released to the secondary containment which consisted of soil bottom and steel sides. 14,000 gallons of the released product was recovered using vacuum trucks and 9,000 gallons were lost to the subsurface which contaminated the groundwater. Light non-aqueous phase liquid was found in 14 wells during two weeks. More than 300,000 gallons of liquids were extracted and reinjected to recover the soil in the vicinity of the tank. Total cost exceeded \$350,000.



Picture 2.2: Spill clean up

Root Causes

- Failure to adhere to written instructions
- Incorrect manual calculation of flow-rates
- Overfill prevention system existed but was not automatic

Lessons Learned

- Although the personnel were qualified, there was a lack of safety culture that made personnel deviate from instructions
- An automatic overfill prevention system could have prevented this accident

Source: Felten, 2015

Case 1: Spill clean up

Property Damages

Buncefield fuel depot, United Kingdom, 2005

Sequence of Events

A floating-roof tank overfilled at a tank terminal which resulted in the release of large quantities of gasoline near London. A vapor cloud formed which ignited and caused a massive explosion and a fire that lasted five days.

The terminal was at the time the fifth largest in the United Kingdom. The terminal supplied both Heathrow and Gatwick airports with aviation fuel as well as distribution of motor fuels and gasoline throughout the region.

Root Causes

The primary root cause was that the electromechanical servo level gauge failed intermittently and the mechanical level switch used in the independent overfill prevention system was inoperable.

The mechanical level switch required a padlock to retain its check lever in a working position. However, the switch supplier did not communicate this critical point to the installer and maintenance contractor or the site operator. Because of this lack of understanding, the padlock was not fitted and as a consequence the mechanical level switch was inoperable.

The electromechanical servo level gauge had stuck 14 times in the three months prior to this major failure. The root-cause of the "sticking" was never properly investigated or determined. The lack of a proper "lessons-learned" procedure indicates that there was an obvious problem with the overfill management system.

Consequences

- 40 people injured but no fatalities
- Major property damages including destruction of tanks and nearby office buildings
- Largest fire in Europe since World War II
- Disruption of nearby transportation routes and businesses
- Groundwater pollution
- Settlements exceeding £700 million (approximately \$1 billion)
- Civil and criminal charges against the company and individual employees

Lessons Learned

The accident received considerable attention from the public and the government. As a result stringent regulations were created based on a holistic perspective and the functional safety standard IEC 61511. The government now inspects to ensure these types of facilities have implemented proper management systems, risk assessments of all tanks and lessons learned procedures.

More specifically, the Buncefield Major Incident Investigation Board* issued a recommendation to install an independent automatic overfill prevention system conforming to IEC 61511 on all bulk liquid storage tanks

Source: Marsh, 2007



Picture 2.3: Property damage caused by the accident in Buncefield

Bankruptcy

Puerto Rico, United States, 2009

Sequence of Events

During the off-loading of gasoline from a tanker ship to the tank farm, a five million gallon above ground storage tank overfilled into a secondary containment dike, resulting in the formation of a large vapor cloud which ignited after reaching an ignition source in the wastewater treatment area of the facility. In addition to causing an extensive vapor cloud fire, the blast created a pressure wave registering 2.9 on the Richter scale. For more than two days, dark clouds of particulates and smoke polluted the air, and petroleum products leaked into the soil and navigable waterways in the surrounding area. The smoke cloud was large enough to be visible by NASA's Terra satellite.



Picture 2.4: Puerto Rico accident in 2009

On the days after the explosion, more than 60 agents from both the FBI and the Bureau of Alcohol, Tobacco, Firearms and Explosives were dispatched to the site.

Root Causes

- Malfunctioning automatic tank gauge (float and tape)
- Lack of independent overfill prevention system
- Incorrect manual calculation of flow rate
- Inadequate overfill management system
- Lack of formal procedures for operations

Consequences

- Bankruptcy
- The blast and fire from multiple secondary explosions resulted in significant damage to the petroleum storage tanks and other equipment on site and in hundreds of homes and businesses up to 1.25 miles from the site
- Groundwater pollution
- Calls for additional regulation
- Involvement of the United States Department of Homeland Security (which adds complexity to the industry)

Lessons Learned

One of the aspects that the United States Chemical Safety and Hazard Investigation Board (CSB) emphasizes is the importance of an independent and automatic overfill prevention system. Additionally, this incident shows the importance of correctly measuring the actual flow-rate into the tank and an automatic calculation of the estimated completion time of the transfer. This can be achieved by using a level transmitter and an automatic calculation of the level rate combined with a calculation of the tank's volume

Source: U.S. Chemical Safety and Hazard Investigation Board (2015) and Puerto Rico Seismic Network (2009)

Clean Water Contamination

Elk River, United States, 2014

Sequence of Events

Approximately 7,500 gallons of chemicals used to process coal spilled into the Elk River in West Virginia from an above ground storage tank at a small tank depot. The Elk River is a municipal water source that serves approximately 300,000 people in the surrounding area.

Root Causes

- Corroded tank
- Malfunctioning secondary containment

Consequences

- Officials issued a “do-not-use” the drinking water advisory for five days
- The company went bankrupt and the facility was razed to the ground
- Criminal charges against six individuals associated to the company (owners, managers and employees) who pleaded guilty

Lessons Learned

Local regulators realized the risk associated with tank overfill and have implemented legislation (United States Environmental Protection Agency’s “Spill Prevention, Control, and Countermeasure Plan”; SPCC Plan) for above ground storage tanks. The legislation contains requirements for tank and secondary containment inspections.



Picture 2.5: Water inspection

Case 4: Clean water contamination

Corporate Fines

Monongahela River, United States, 1988

Sequence of Events

A four-million gallon tank catastrophically failed. The tank was used for the first time after being reconstructed at a new site. One million gallons of the diesel oil spilled into a storm sewer that flowed into the Monongahela River.

Consequences

- Federal Government issued a fine of \$2.25 million, the largest for a petroleum company at the time
- Lawsuits: one for violating the Clean Water Act and another for violating the Federal Refuse Act
- \$18 million in cleanup fees and civil lawsuits from those distressed by the experience.
- The potable water supplies for about one million people were disrupted. Water shortages were common after the incident. Wildlife, fish and mussels were harmed or killed
- Over 1,200 residents had to evacuate for approximately a week

Lessons Learned

Tank overfills do not only concern the owner of the tank, but also the public. Governments may issue considerable fines which, including other associated costs with a spill, may result in bankruptcy.

Incidents do not only affect the specific company but also the entire industry. For example this incident is one of the reasons why the industry, through API, garnered a task group to publish the standard API 653 "Above Ground Storage Tanks Inspector Program".



Picture 2.6: Refinery next to river

Case 5: Corporate fines

Condemnation of Executives

Texas City refinery, United States, 2005

Sequence of Events

The incident occurred during the startup of the raffinate splitter section of the isomerization unit, when the raffinate splitter tower was overfilled. The excess gas flowed into a back-up unit, which then also overflowed and sent a geyser of gasoline into the air. Flammable liquid was released, vaporized, and ignited, resulting in an explosion and fire.



Picture 2.7: Texas City refinery accident

Root Causes

- Malfunctioning level transmitters and alarms
- The level transmitters measurement ranges were insufficient
- Lack of safety culture made the operators regularly deviate from written startup procedures

Consequences

- 15 contract employees were killed
- A total of 180 workers at the refinery were injured, 66 seriously
- Considerable property damages on-site, and off-site windows were shattered in homes and businesses located, up to three-quarters of a mile (1.2 km) away from the isomerization unit
- The company was charged with criminal violations of federal environmental laws, and has been named in lawsuits by the victims' families. In a quarterly report the company revealed that it had reserved \$700 million for fatality and personal injury claims, although some cases had not yet been settled
- Government recommended the company appoint an independent panel to investigate the safety culture and management systems. The investigation was headed by former United States Secretary of State James Baker III and the resulting report is known as the "Baker Panel report"
- Victims, media and government officials publicly condemned the company for saving money on safety while making billions of dollars in profits

Lessons Learned

Major accidents are not only costly, but also receive considerable public attention. The company's reputation will be damaged and even the acceptance of its existence may be questioned. This also affects the company's employees and the executives may personally be liable for the accidents and be publicly condemned.

According to the US Chemical Safety and Hazard Investigation Board the key issues were:

- Safety culture
- Regulatory oversight
- Lack of process safety metrics
- Human factors

More specifically, the accident could probably have been avoided if level transmitters with a measurement range covering the entire tank had been installed.

Source: Loren, 2005

Fatalities, Injuries and Evacuation

Jaipur, India, 2009

Sequence of Events

During a routine transfer of kerosene between two terminals, a huge leak occurred at a "Hammer blind valve". The liquid rapidly generated vapors which made it impossible for the shift operators to address the problem. After about 15 minutes of the leak starting, there was a massive explosion followed by a huge fireball covering the entire installation. The fire which followed the explosion soon spread to all other tanks and continued to rage for 11 days.



Picture 2.8: Oil fire

Consequences

- 12 people lost their lives due to burns and asphyxia and more than 300 suffered injuries. Many of the fatalities were company employees
- Half a million people were evacuated from the area
- The Ministry of Petroleum & Natural Gas immediately thereafter appointed a five member committee to investigate the causes of the accident and submit a report within 60 days
- Accusations were raised against 20 employees
- The police arrested nine senior company officials including its general manager on charges of criminal negligence eight months after the accident

Lessons Learned

Tank spills can result in very serious consequences including fatalities, injuries and evacuation of nearby communities.

Source: Oil Industry Safety Directorate, 2010

Case 7: Fatalities, injuries and evacuation

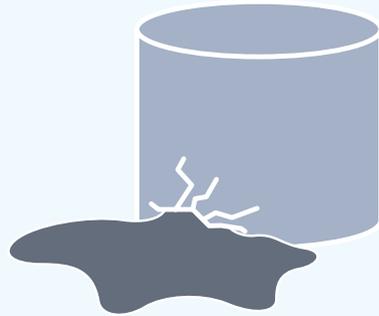
2.5 Additional Risks Associated with Tanks

There are numerous risks associated with tanks. Below are examples where the risk can be considerably decreased by using better level measurement.

Tank Leakages

Leaks occur for a number of reasons, for example corrosion, tank stress or improper welds. As a part of the ongoing safety trend, the need for leak detection has increased, and many countries mandate it by law for certain tank types (e.g. above ground and underground storage tanks).

By using accurate level measurement, abnormal product movements in the tank can be monitored and thereby used to detect leaks. The major advantage with using accurate level measurement for leak detection is that no additional equipment is required.



Tank Low Level

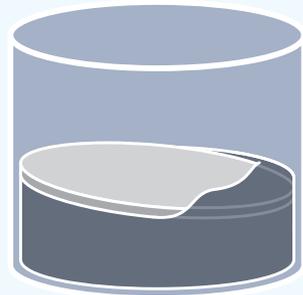
Low level in the tank can be a considerable risk in certain applications due to, for example, the potential for pumps running dry or heating coils or mixers being exposed.

The risk with low tank level can be minimized by using proper level measurements and alarms. An advantage with continuous level transmitters in this specific application is that a single device can be used for both high and low alarms.

Floating Roof Binding and Buoyancy Issues

Floating roofs are movable mechanical constructions that require regular maintenance. Problems with rain water, drain clogging or pontoon leakage, combined with wind and rain or snow may cause the roof to “get stuck” or sink.

The latest technical solution for floating roof monitoring is to use three wireless guided wave radar level transmitters mounted on the floating roof itself. The transmitters measure the relative level which can be used to calculate the angle of the roof and its buoyancy.



Fact box 2.5: Examples of risks associated with tanks

2.6 Financial Returns of Modern Overfill Prevention

This section describes how the usage of a modern overfill prevention system can generate immediate and long-term financial returns.

2.6.1 Increased Efficiency

2.6.1.1 Quicker Transfers and Better Tank Utilization

By having a better understanding of what's in the tank, operators will gain the trust to perform product movements faster and operate the process more efficiently. Additionally, with overfill prevention systems that more accurately measure the level, and have quicker response times, the set-points can be adjusted to increase the tank utilization.

2.6.1.2 Less Manpower

Verification of overfill prevention systems often occupies considerable resources. Modern overfill prevention systems require less testing and offer quicker testing procedures.

2.6.1.3 Management System

Modern overfill prevention requires the establishment of an appropriate overfill prevention management (OMS) system. Written accurate procedures that correspond with how the system works in the field; qualified personnel; management of change and lessons learned systems are a few of the components that will result in a more efficient facility.

2.6.1.4 Reduced Down-Time

Modern overfill prevention systems offer increased availability and reduce the need for hand-gauging or visual inspection of local level sensors, thereby minimizing down-time.

2.6.2 Reduced Cost of Risk

2.6.2.1 Insurance Costs

By implementing modern overfill prevention the insurance premium may be reduced if an external insurance company is used.

2.6.2.2 Emergency Response Costs

Modern overfill prevention results in fewer tank overfills, thereby lowering the need for costly emergency responses.

2.6.2.3 Hand-Gauging and Reading of Local Level Sensors

By having a better understanding of what's in the tank, fewer manual measurements are required.

2.6.2.4 Maintenance

Modern overfill prevention systems require less maintenance.

3



Key Elements

| Topic | Page |
|---|------|
| 3.1 The Traditional Approach to Overfill Prevention | 30 |
| 3.2 The Modern Approach to Overfill Prevention | 30 |
| 3.3 Requirements | 30 |
| 3.4 Risk Assessment | 31 |
| 3.5 Process Design | 31 |
| 3.6 Overfill Management System | 31 |
| 3.7 Protection Layers | 32 |
| 3.7.1 Basic Process Control System | 33 |
| 3.7.2 Safety Layer | 33 |
| 3.7.3 Passive Protection and Emergency Response Layer | 35 |
| 3.8 Commissioning and Subsequent Verification | 35 |
| 3.8.1 Site Acceptance Testing | 35 |
| 3.8.2 Proof-Testing | 35 |

3. Key Elements

3.1 The Traditional Approach to Overfill Prevention

Overfill prevention has traditionally been synonymous with equipment denoted “overfill prevention system” (OPS). This equipment has often been put in place to fulfil incomplete prescriptive regulatory requirements and has been treated accordingly. Capital expenditure has been minimized and maintenance and verification have not been prioritized. Operational key performance indicators (KPIs) have been prioritized over safety. As a result, written safety procedures have often been lacking and operations departments have not adhered to written procedures.

3.2 The Modern Approach to Overfill Prevention

There have been significant advancements in the understanding of tank overfill root-causes in recent years due to the increased availability of information. Often the information has originated from public investigations.

Modern overfill prevention is based on a holistic perspective with an understanding that a multitude of elements contribute to minimizing the risk of a tank overfill, and not just the equipment denoted as the “overfill prevention system”. An overview of these elements is described below and in greater detail in subsequent chapters.

3.3 Requirements

Usually several different internal and external requirements apply to tanks and overfill prevention:

- The foundation is regulations, which may originate from state, federal, national or union legislations. These are further described in chapter 4 “Regulatory requirements”.
- Additionally, many companies have internal codes and standards. These are not further described in this book because of their individual nature. However, it is worth mentioning that these internal documents should be based on, and in compliance with, the applicable external requirements.
- Along regulations, there are industry standards and Recognized and Generally Accepted Good Engineering Practices (RAGAGEP). These are often created and documented by industry associations. In some instances, there exist documented application specific and/or country specific requirements. This book addresses the globally accepted standards IEC 61511 and API 2350, which are discussed in chapter 5 “Industry standards”.

The structure and priority of these requirements, which are sometimes conflicting, are illustrated in figure 3.1.

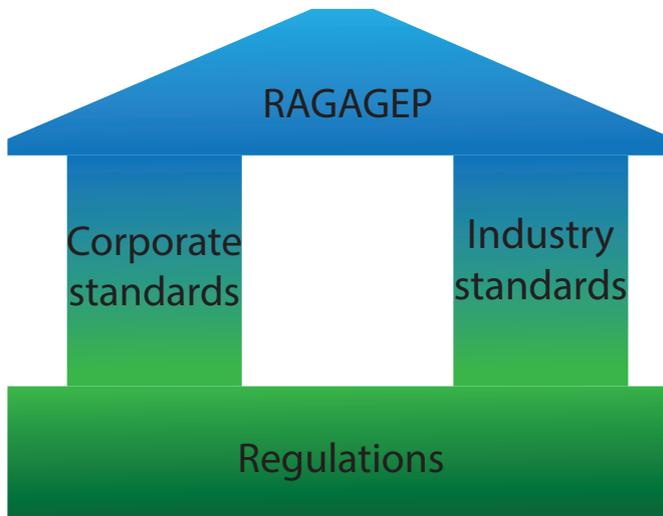


Figure 3.1: The origin, and priority, of internal and external overfill prevention requirements

3.4 Risk Assessment

Tank overfills are predictable. It is therefore crucial to create an understanding of the specific tank's risk for overfill. Probability factors are determined by, for example, evaluating how the tank is operated and what the effectiveness of the various protection layers are (e.g. the overfill prevention system). Also different consequence factors, such as fatalities and asset damage, are evaluated. The assessed risk is compared with the facility's tolerable risk to determine if there is an unacceptable risk and what size it is. This process is depicted in figure 3.2.

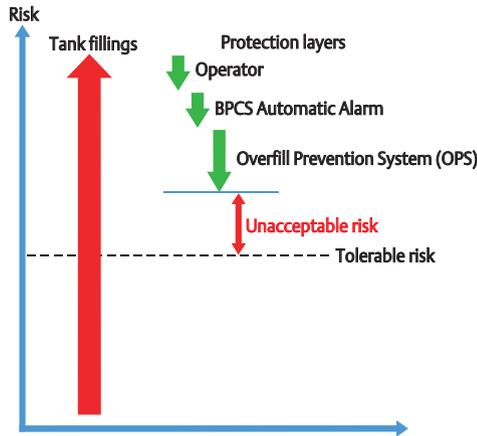


Figure 3.2: Basic concept of evaluating the assessed risk compared to the tolerable risk

Modern overfill prevention uses this risk (performance) based approach as opposed to the traditional prescriptive approach. This ensures that the safeguards are neither over nor under engineered.

An action to reduce the risk to a tolerable level must be taken if the risk assessment determines that the risk is unacceptable. Examples of actions that can be taken to reduce the risk:

- Inherent process design change
- Changes in the Overfill Management System (e.g. operational procedures)
- Implementing additional protection layers or modifying the existing ones

Risk Assessment is described further in chapter 6 "Risk Assessment".

3.5 Process Design

One of the elements that needs to be taken into consideration to prevent overfills is the design of the process or bulk liquid facility. For example, does the tank have the appropriate size to accommodate abnormal process behavior? Is the incoming and outgoing pipe sizing appropriate? Is there a need for connection to a relief tank?

Although the process design is a critical element to prevent tank overfills, it is not further described in this book due to its individual and varying nature.

3.6 Overfill Management System

Traditionally, tank overfills have been attributed to malfunctioning equipment. Although this is often a contributing factor, the actual root-cause is often more complex and involves human behavior. Therefore, a critical part of modern overfill prevention is to establish an adequate Overfill Management System (OMS) that corresponds with how it works in the field.

An OMS is the framework of processes and procedures used to ensure that the organization fulfills all tasks required to achieve the objective of tank overfill prevention. This includes components such as competent personnel, written procedures, lessons learned systems and management of change procedures. Although a large task at first, the creation of an adequate OMS is not just a necessity to prevent tank overfills, it will also result in a more efficient facility. OMS is described in chapter 7 "Overfill Management System".

3.7 Protection Layers

Generally, a multitude of independent protection layers (IPLs) are used to minimize the risk of tank overfills as depicted in figure 3.3, according to the principle “do not put all your eggs in one basket”. The commonly used IPLs for tank overfill prevention are depicted in figure 3.4 below.

To reduce risk, an existing IPL can be modified, or alternatively an additional IPL can be added. The selection process often involves a cost benefit analysis. Examples of additional parameters (besides internal and external requirements) that should be taken into consideration are:

- All IPLs are not alike. The Basic Process Control System (BPCS) and Safety layer can be used to prevent the accident and thereby reduce the probability, whereas the Passive protection and Emergency response layers mitigate the accident and thereby minimize the consequences.
- The IEC standard is for the use of electrical / electronic / programmable electronic safety-related systems in the process industry. Like IEC 61508 and IEC 61511 it focuses on a set of safety lifecycle processes to manage process risk. To reduce the risk is the major focus in the industry.

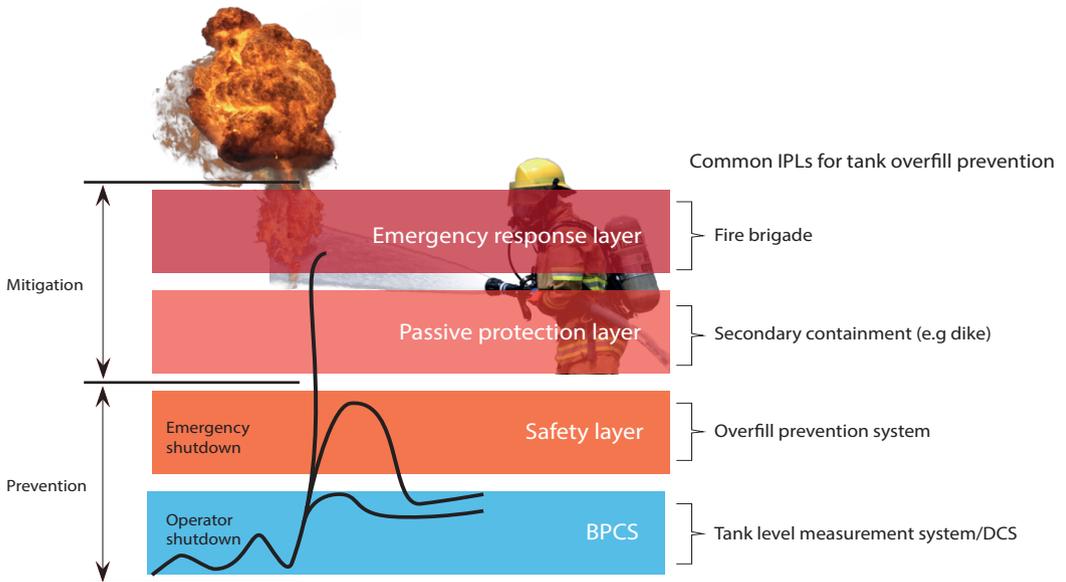


Figure 3.3: Commonly used independent protection layers (IPLs) to minimize the risk of tank overfills

3 - Key Elements

Manual Overfill Prevention System (MOPS) | Basic Process Control System (BPCS)

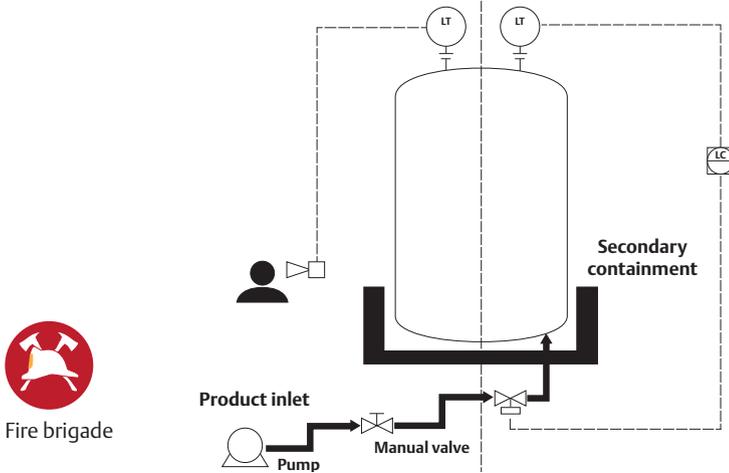


Figure 3.4: Generic tank example with the commonly used IPLs for tank overfill prevention and mitigation depicted

3.7.1 Basic Process Control System

One of the most overlooked elements of overfill prevention is probably the Basic Process Control System (BPCS). This is the primary IPL that continuously prevents tank overfills from occurring and, when functioning correctly, the other IPLs will not be activated as depicted in figure 3.5. Therefore, it may be argued that this is the most important IPL and as a consequence it needs to receive appropriate attention. For example, a BPCS relying on an unreliable mechanical level transmitter, as depicted in picture 3.1, is a major safety concern.



Picture 3.1: Unreliable mechanical level transmitter (servo type)

3.7.2 Safety Layer

In tank overfill prevention applications, the safety layer is typically denoted overfill prevention system (OPS). There are two basic types: manual overfill prevention system (MOPS) and automatic overfill prevention system (AOPS).

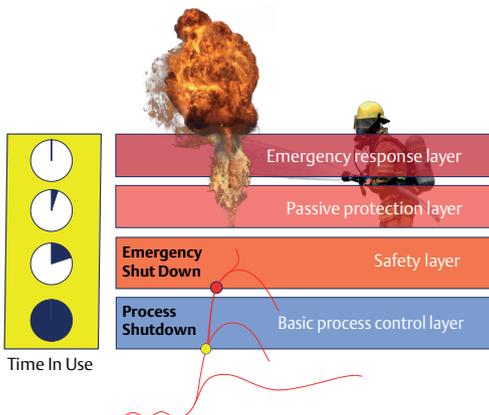


Figure 3.5: The BPCS layer is in use continuously and is the primary tool to prevent a tank overfill. The other IPLs are only activated upon failure of the subsequent IPL



Figure 3.6: Manual overfill prevention systems (MOPSs) usually consist of a level transmitter (LT) connected to an audiovisual alarm that notifies an operator to take the appropriate action, e.g. closing a valve



Figure 3.7: Automatic overfill prevention systems (AOPSs) usually consist of a level transmitter (LT), logic and actuator that automatically closes a valve to prevent overfills from occurring. No human intervention is required which usually increases the reliability and shortens the response time

Outlook: Industry trends

Proof-Testing Methods

For level measurement devices deployed in SIS applications such as overflow prevention, proof-tests have traditionally been carried out by multiple technicians in the field, with another worker stationed in the control room to verify the reaction of the system. This method can involve workers having to climb tanks to access instruments and perform the proof-test, which can expose them to a hazardous environment with increased safety risks. As well as being prone to errors, performing proof-tests in this way also consumes a significant amount of time and manpower and can lead to the process being offline for an extended period, affecting process availability during the outage with significant cost implications.

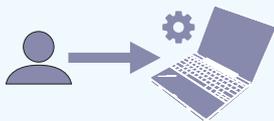


Figure 3.8: The trend is to replace manual activities with automatic control

Outlook box 3.1: Manual replaced with Automatic

Outlook: Industry trends

Adherence to IEC 61511

Functional safety is the part of the overall safety of plant and equipment that depends on the correct functioning of safety-related systems and other risk reduction measures such as safety instrumented systems (SIS), alarm systems and basic process control systems (BPCS).

Safety instrumented system SIS are instrumented systems that provide a significant level of risk reduction against accident hazards. They typically consist of sensors and logic functions that detect a dangerous condition and final elements, such as valves, that are manipulated to achieve a safe state.

The general benchmark of good practice is IEC 61508, Functional safety of electrical/electronic/programmable electronic safety related systems. IEC 61508 is the base standard for:

IEC 61511: process industry

IEC 62061: machinery

IEC 61513: nuclear power plants

IEC 61511, Functional safety - Safety instrumented systems for the process industry sector, is the benchmark standard for the management of functional safety in the process industries. It defines the safety lifecycle and describes how functional safety should be managed throughout that lifecycle.

Outlook box 3.2: Adherence to IEC 61511

Outlook: Industry trends

Continuous Level Measurement for the Safety Layer

Periodic proof-tests are a necessity for point level switches that form part of a safety instrumented system (SIS) in liquid level measurement applications. The traditional and modern methods of performing proof-tests and examines how modern partial proof-testing can be performed remotely with multiple devices tested simultaneously, increasing speed and safety and reducing operational cost. It compares the different test methods and explains how integrated functionality within the latest devices can reduce complexity and save significant cost.



Picture 3.2 and 3.3: Two continuous measurements of the same type are used as the level sensors in the BPCS and the safety layer (left: radar level gauges, right: guided wave radar level transmitters)

Outlook box 3.3: Continuous level measurement for the safety layer

3 - Key Elements

A critical aspect of overfill prevention is to correctly define the “levels of concern” (LOC) which include Critical High (CH), Level Alarm High High (LAHH or simply HiHi) and Maximum Working Level (MWL) as depicted in figure 3.9.

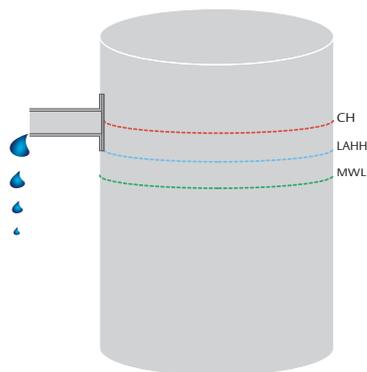


Figure 3.9: The Levels Of Concern (LOC) for tank overfill prevention

According to API 2350:

“Note specifically that an alarm requires immediate action, either manually (e.g. field operator closes a valve) or automatically through predetermined logic. In some instances a level alert high (LAH) or other alert may be used for optional operational notifications”.

Overfill prevention system is further described in chapter 8 “Overfill prevention systems”.

3.7.3 Passive Protection and Emergency Response Layers

In the case of tank overfill protection, the passive protection layer usually consists of a secondary containment (e.g. dikes or concrete walls) and the emergency response layer consists of a fire brigade. These IPLs are merely used for mitigation of tank overfills, and they are consequently not included within the scope of this book.

3.8 Commissioning and Subsequent Verification

An essential element of modern tank overfill prevention is to ensure that the probability of systematic (human) errors and random hardware failures are minimized for the safety layer. The key methods to achieve this are Site Acceptance Testing (SAT) and Proof-testing.

3.8.1 Site Acceptance Testing (SAT)

SAT is performed to verify that the equipment has been commissioned correctly. The purpose is to detect systematic (human) failures. Best practice is that the SAT is performed by one or more people who were not involved in the commissioning procedure.

3.8.2 Proof-Testing

The purpose of proof-testing is to verify that commissioned equipment already in operation functions correctly. It is a useful tool to reduce the safety layer’s probability of failure on demand for infrequently used safety systems. Proof-testing is further described in chapter 9 “Proof-testing”.

| Level of Concern (LOC) | Abbreviation | Definition |
|------------------------|--------------|---|
| Critical High Level | CH | The highest level in the tank that product can reach without detrimental impacts (i.e. product overflow or tank damage) |
| Level Alarm High-High | LAHH | An alarm generated when the product level reaches the high-high tank level |
| Maximum Working Level | MWL | An operational level that is the highest product level to which the tank may routinely be filled during normal operations |

Table 3.1: Levels of concern

Outlook: Industry trends

Site Acceptance Testing and Proof-Testing

Minimizing accident risk

Ensuring the safety of assets and personnel is always high priority for manufacturing and process organizations, but unfortunately accidents do still happen. To help minimize the risk of accidents in liquid handling and storage applications, companies must implement properly designed SIS. The primary functions of SIS are to bring processes to a safe state and to prevent safety incidents such as overfills from happening. These systems include the liquid level sensors, logic solvers and the final control elements for each of the safety instrumented functions (SIF) that they perform.



Picture 3.4a: Climbing the tank to proof-test a level transmitter

Proof-testing requirement

Devices and systems that are part of a SIS must be proof-tested periodically to ensure that they will work properly when there is a safety demand, and to verify that SIFs are operating at the necessary safety integrity level (SIL) for their application. Proof-tests are operational tests conducted in accordance with the safety manual of an individual installed device to evaluate its ability to perform its safety function and to uncover random hardware failures. These are failures that prevent the device from performing its primary function and which would otherwise remain undetected by its built-in diagnostics during normal operation. Such failures could put the SIS in a hazardous or fail-to-function state and if undetected could, for instance, lead to an overfill and spill, with potentially disastrous consequences.



Picture 3.4b: On-line testing in the control room

Outlook box 3.4: Site acceptance testing and proof-testing

4

Regulatory Requirements

| Topic | Page |
|---|------|
| 4.1 Different Types of Regulations | 39 |
| 4.1.1 No Regulation Directly Applicable to Tank Overfills | 39 |
| 4.1.2 Prescriptive Regulation | 40 |
| 4.1.3 Performance Based Regulation | 40 |
| 4.1.4 Performance Based With Extensions Regulation | 40 |
| 4.2 Implications | 40 |



4. Regulatory Requirements

Regulations are binding legislative acts each facility must conform to. Non-conformance can result in both civil and criminal prosecution, especially in the event of an accident.

Unfortunately, and independently of country, it is not as simple as a single regulation for overflow prevention. Instead, multiple regulations aimed at different purposes may have an impact on the requirements for prevention and mitigation of tank overfills. These are examples of common fields of regulations that usually have an impact on the requirements for tank overflow prevention:

- Handling of hazardous substances

- Environmental protection
- Explosive products handling
- Water pollution
- Air emissions
- Fire protection
- Emergency response plan
- National security
- Protection of critical infrastructure
- Worker's rights
- Civil protection

An example of external regulations relating to tank overfills for above storage tank terminals can be seen in figure 4.1 below.

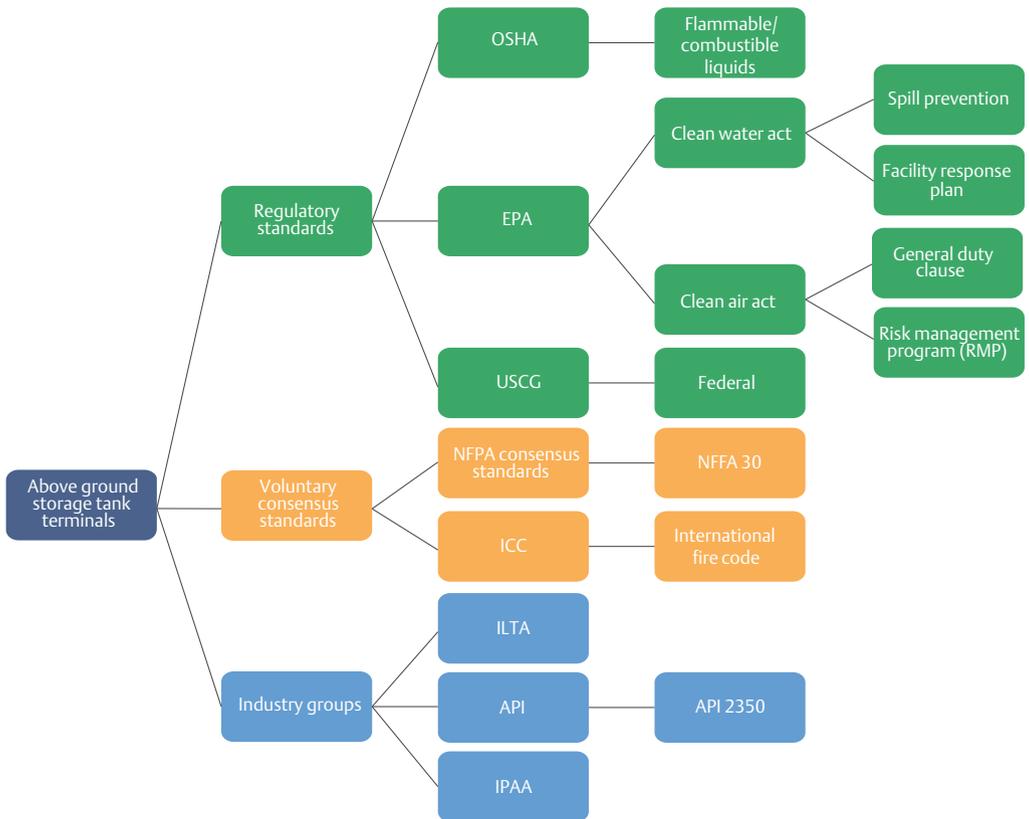


Figure 4.1: Example mapping conducted by the United States Chemical Safety Board in 2015 of external requirements relating to tank overfills for above ground storage tank terminals in the United States

4 - Regulatory Requirements

4.1 Different Types of Regulations

Regulation varies by union, country, state or even municipality. Currently the different regulatory frameworks that apply to the prevention and mitigation of tank overfills can be characterized in the following way:

- No regulation directly applicable to tank overfill
- Prescriptive regulation
- Performance based regulation
- Performance based with extensions regulations

These basic types of regulations are further described in subsequent chapters. Often a combination applies to a single tank.

Regulation is an evolutionary process that is highly affected by accidents (e.g. the Seveso accident in Italy, the Bhopal accident in India and the Texas city accident in the US). Based on the trend in the

industrialized countries depicted in figure 4.2, the world is heading towards a “Performance based with extensions” approach.

4.1.1 No Regulation Directly Applicable to Tank Overfills

In some countries there exists no applicable regulation for tank overfills. Alternatively, the regulation may be incomplete for certain tank types or stored products (e.g. if the tank is on wheels, or the regulators depend entirely on local industry associations).

It is important not to be mistaken if this is the case; usually if an accident occurs, the matter ends up in a court which probes the defendants against locally and internationally recognized standards (e.g. API 2350 or IEC 61511) and RAGAGEP. Consequently, in the advent of an accident there are also expectations and indirect requirements under this type of regulation.

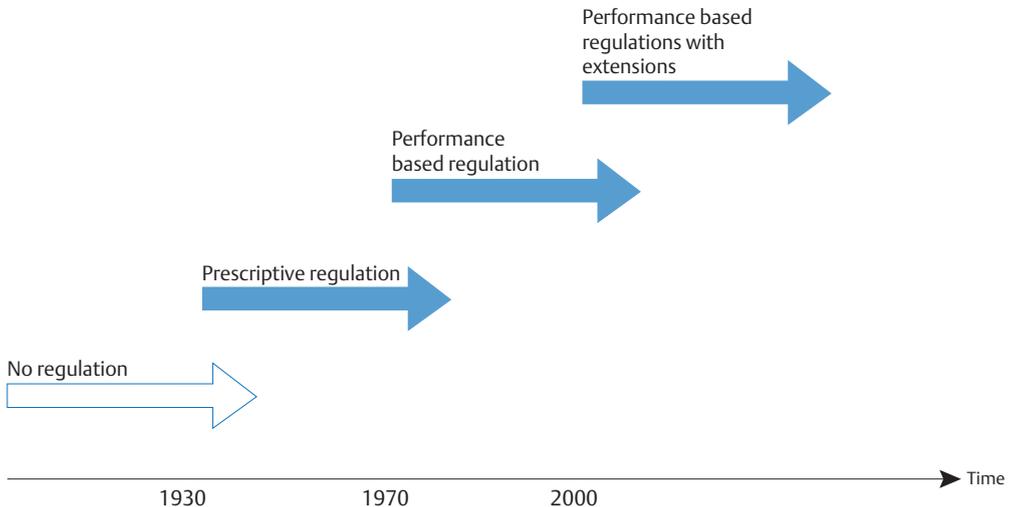


Figure 4.2: Developments of safety regulations in the industrialized world

4.1.2 Prescriptive Regulation

Prescriptive regulation such as “the tank shall have an independent level switch” puts requirements on the specific design. This type of regulation emerged as a response to accidents but has proven to be ineffective because “there is no great incentive for companies to go over and beyond the prescriptive compliance requirements. Instead of treating regulations as the minimum acceptable standard and continuing the search for best industry practices, companies stop their efforts as soon as prescriptive compliance is achieved” (Sreenevasan, 2015). The traditional approach to overfill prevention, described in chapter 3 “Key Elements”, is based on this type of thinking.

4.1.3 Performance Based Regulation

Performance based regulation is based on the actual risk that exists. The organization responsible for the risk is empowered to address it the way they find appropriate and the government reviews and approves their justification and follows up with inspections.

Benefits of this approach include:

- Reduces the amount of regulation required and allows government officials to act with increased flexibility
- Prevents over or under engineering of safeguards
- “Allowing for innovation and new technology, as well as creativity and advancement” (Goble, 2013)

The main disadvantage with performance based regulation is that it can be more cumbersome to implement. For example it requires that:

- The responsible organization is competent
- A risk assessment is conducted (which may or may not be accurate)
- Determination of tolerable risk criteria

Further information about performing risk assessment for a specific tank can be found in chapter 6.

It is not uncommon for regulations to be both prescriptive and performance based. One example is legislators who, due to previous accidents, stipulate that consequence or probability factors be included in the risk assessment.

4.1.4 Performance Based with Extensions Regulation

In recent years, the performance based approach has been augmented in many countries with a holistic perspective that also takes the workforce (or general stakeholders) into account, in addition to the regulator and the responsible organization. Other components of this augmented approach are:

- Process Safety Management (see Overfill management system, chapter 7)
- Increased transparency by presenting information to the public
- Sharing lessons learned across similar facilities
- Public investigation reports
- Public databases of accidents and incidents
- Competency requirements
- Standardized inspections

Although this approach increases the initial workload compared to the performance based approach, it also eventually results in a more efficient and safe facility.

4.2 Implications

Regulations are constantly changing and generally become stricter over time. This is partially because accidents keep occurring, but also because of the fact that societal acceptance for involuntary risk is decreasing.

The evolution of regulations makes it difficult for the industry to maintain compliance because solutions that were acceptable in the past may not conform to current requirements. The most efficient way to approach this problem is by the usage of future-proof solutions that also take anticipated future safety requirements into account. The remainder of this book describes the modern approach to overfill prevention, which is aimed at creating future-proof solutions.

Regulatory Evolution in the UK

The Secretary of State for Employment in the United Kingdom set up a committee in May 1970 to review existing safety and health regulations. The committee was chaired by Lord Robens who identified a problem with the existing body of regulations arising from their sheer volume and proliferation, in addition to their ineffectiveness.

The Robens Report stated that the safety laws were “intrinsically unsatisfactory, badly structured and written in a style that rendered them largely unintelligible even to those who were supposed to administer them”. His report, issued in June 1972, recognized a need for more self-regulation and that the industry should be encouraged to develop its own standards and criteria for improving health and safety performance. As a result of this report, the Health and Safety Executive (HSE) branch of the government was formed and the “Health and Safety at Work” act was issued in 1974.

The HSE embodies the following principles:

1. The organizations that create risks should control them
2. The benefits as well as the costs of regulations must be considered

Inspired by the developments in the UK, the European Union (EU) has taken the lead in regulations for process safety through the Seveso directive.

Case 4.1: Regulatory evolution in the UK



5

Industry Standards

| Topic | Page |
|---|------|
| 5.1 IEC 61511 | 44 |
| 5.1.1 Basic Concepts | 44 |
| 5.1.2 IEC 61508 Certification | 46 |
| 5.1.3 IEC 61511 Applied to Modern Overfill Prevention | 47 |
| 5.2 API 2350 | 47 |



5. Industry Standards

The need for industry standards and RAGAGEP arose with the industrial revolution in the mid 1700s. Conformance to the most recent globally recognized industry standards is a critical element of modern overfill prevention.

There are numerous national and tank specific standards available for overfill prevention (e.g. NFPA 30, PGS 29, OISD Guideline 152) that may also be applicable for individual facilities, but the globally accepted standards, which are covered in this book, are IEC 61511 and API 2350.

IEC 61511 and API 2350 have different scopes and purposes as depicted in figure 5.1. API 2350 is an application specific standard specifically for bulk liquid storage, whereas IEC 61511 is targeted towards the design of electronic safeguards in both the process and bulk liquid storage industries. The two standards do not compete; the usage of IEC 61511 for the design of an overfill prevention system for usage on bulk liquid storage tanks is an excellent way to comply with parts of API 2350.

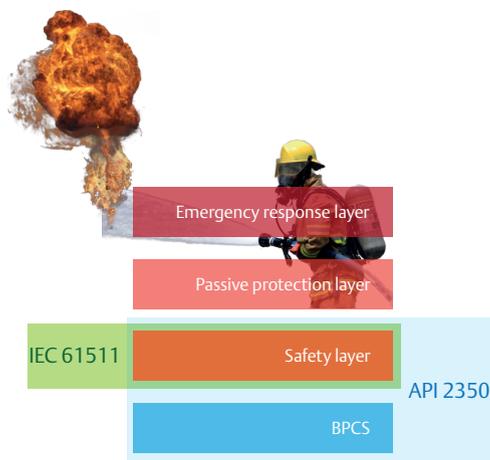


Figure 5.1: Industry standards IEC 61511 and API 2350 - comparison of intended scopes

5.1 IEC 61511: Functional Safety – Safety Instrumented Systems for the Process Industry Sector

IEC 61511 is intended for safeguards used in the process and bulk liquid industries based on completely, or partially, electrical/electronic/

programmable components.

IEC 61511 is recognized as the global functional safety standard and it has been adopted by the European standards body, CENELEC. This means that the standard is published as a national standard in each of the member states of the European Union. In the United States it is sometimes recognized as ANSI/

IEC 61511

Use this standard for: *Automatic Overfill Prevention Systems* in

- Process Industry
- Bulk Liquid Storage Industry

ISA 84.00.01-2004 or simply “S84”. This standard mirrors IEC 61511 in content with the exception that it contains a “grandfather” clause that allows the use of existing equipment that has been designed in accordance with older codes, standards, or practices. That is, assuming it has been operated in a safe manner as well as properly maintained, inspected, and tested.

5.1.1 Basic Concepts

5.1.1.1 Safety Instrumented Function (SIF)

A single electrical/electronic/programmable safeguard is denoted “Safety Instrumented Function” (SIF) and consists of a sensor, logic-solver and actuator as depicted in figure 5.2.

In the context of overfill prevention, this corresponds to an automatic overfill prevention system (AOPS) consisting of one or multiple level sensors, a logic-solver and one or multiple actuators controlling a corresponding valve.



Figure 5.2: Principal components of a Safety Instrumented Function (SIF)

5.1.1.2 Safety Integrity Level Definition From 61511 SIL

Discrete level (one out of four) allocated to the SIF for specifying the safety integrity requirements to be achieved by the SIS

Note 1 to entry: The higher the SIL, the lower the expected PFDavg for demand mode or the lower the average frequency of a dangerous failure causing a hazardous event for continuous mode.

The relationship between the target failure measure and the SIL is specified in Table 5.1.

| Safety Integrity Level (SIL) | Average probability of a dangerous failure on the demand of the safety function (PFD_{avg}) |
|------------------------------|---|
| 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 $< 10^{-1}$ |

Table 5.1: Overview Safety Integrity Levels (SILs) and corresponding risk reduction factors (RRFs)

SIL 4 is related to the highest level of safety integrity; SIL 1 is related to the lowest. This definition differs from the definition in IEC 61508-4:2010 to reflect differences in process sector terminology.

5.1.1.3 Safety Instrumented System (SIS)

A “Safety Instrumented System” (SIS) consists of multiple SIFs connected to a single logic-solver as depicted in figure 5.3. Although not theoretically correct, the words SIS and SIF are often used interchangeably.

5.1.1.4 Safety Life-Cycle

The foundation of IEC 61511 is the safety life-cycle which is depicted in figure 5.4. The safety life-cycle is based on a holistic perspective throughout the lifetime of a SIS (“from the cradle to the grave”).

The safety life-cycle can be segmented into the following steps:

1. Analysis: risk assessment and allocation of safety functions

2. Realization: design and implementation of the SIS – specification, design and engineering, installation, commissioning and validation (site acceptance test)
3. Operation: operation and maintenance, proof-testing, management of change and decommissioning



Figure 5.4: IEC 61511-1 safety life-cycle

These three steps are accompanied by the following phases that shall be conducted throughout the lifetime of the safety life-cycle:

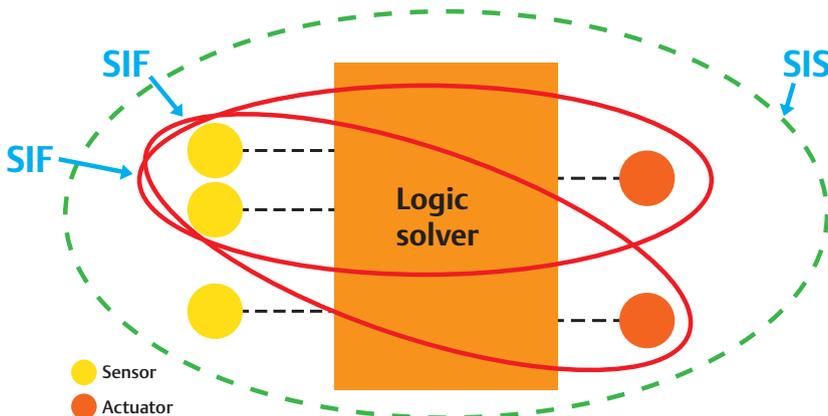


Figure 5.3: Principal overview safety instrumented function (SIF) an safety instrumented system (SIS)

5 - Industry Standards

- Accreditation by a recognized third party (See figure 5.5)
- Competency within the field of functional safety
- Proper engagement in the development project

A product developed according to IEC 61508 implies that:

- The developer has to have a rigorous documented management system including:
 - Product development process
 - Manufacturing process
 - Documentation system
 - Management of change process
 - Lessons learned system
 - Quality system
- During the design of the product the following must be included:
 - Failure Modes and Effects Analysis (FMEA)
 - Comprehensive testing including fault insertion tests
 - Documentation that provides traceability and evidence for all safety requirements
 - Development of proof-testing procedures
- Comprehensive user documentation requirements rendered in a:
 - Safety manual
- Involvement of a third party assessor that requires and issues:
 - Audits
 - Compliance reports
 - Certificates

Products developed and independently assessed for conformance to IEC 61508 is a lengthy and costly process for the manufacturer. This assessment, however, generates several benefits for the user:

- Quality assurance
- Quantified reliability figures and classification of safety integrity level (SIL) capability
- Proper documentation covering all parts of the life-cycle

- Product information and data (e.g. reliability and product life-time)
- Procedures (e.g. installation and proof-testing)
- Drawings

5.1.3 IEC 61511 Applied to Modern Overfill Prevention

Modern overfill prevention requires that automatic overfill prevention systems (AOPs) are designed according to the most recent globally accepted standard which is currently IEC 61511. This standard provides a solid framework throughout the life-time of the AOPS.

It is important to understand that IEC 61511 is focused solely on SIS and therefore does not cover all the elements of modern overfill prevention (see chapter 3 “Key elements”). For example, it covers:

- Internal and external requirements such as regulations and local standards
- Process design
- Overfill Management System (e.g. lessons learned procedures)
- Non-safety layers (i.e. Basic process control system, Passive protection, and Emergency response layers)

The performance (risk) based approach in IEC 61511 corresponds to the legislative approach “Performance based regulation” but does not cover all the elements of “Performance based with extensions regulation”.

IEC 61511 is one of multiple invaluable elements of modern overfill prevention.

5.2 API 2350: “Overfill Protection for Storage Tanks in Petroleum Facilities”

API 2350

Use this standard for: Overfill Protection in

- Process Industry
- Bulk Liquid Storage Industry

Note: API 2350 contains generic principles that are also applicable to the process industry sector (although this is not the intended scope)

5 - Industry Standards

With the introduction of the 4th edition, which was a major change compared to previous editions, API 2350 became the first globally recognized overfill prevention standard for the bulk liquid storage industry.

The purpose of this standard is to provide a holistic perspective that is synchronized with (but does not cover all parts of) the legislative approach “Performance based with extensions regulation” seen in figure 4.2 in chapter 4.

API 2350 contents include:

- Overfill Management System
- Risk assessment
- Operations and procedures
- Overfill Prevention System
- Tank Gauging System

Although API 2350 is generically written, the intended scope is non-pressurized above-ground storage tanks containing petroleum products as defined in table 5.2.

The standard is a mix of prescriptive and performance based requirements. It requires a risk assessment to be conducted and evaluated against the tolerable risk, while still describing the minimum required tank overfill equipment on the tank.

A common confusion relates to the standard in the tank categories that are required to be determined and the associated minimum equipment requirements. In practice, most modern facilities are category 3 according to the API 2350 classification and require the usage of an Automatic Tank Gauging (ATG) system with independent overfill prevention system (OPS). Additionally, when the required risk assessment is conducted it is unlikely that the determined equipment requirements are lower than the API 2350 specified minimum requirements.

API 2350 accepts both MOPS and AOPS, but in case the latter is used, the basic practical requirement is that it shall be designed according to IEC 61511. The standard does not place any specific requirement on the AOPS’s SIL. Instead, this is referred to the risk assessment.

| Class | Definition (NFPA 30-2008) | Example | Covered by API 2350 |
|-------|---|---|---------------------|
| I | Flash Point less than 100 °F (38 °C) | Motor and aviation gasoline | Yes - Required |
| II | Flash Point equal to or greater than 100 °F (38 °C), but less than 140 °F (60 °C) | Diesel fuel, paint thinner | Yes - Required |
| III | Flash Point equal to or greater than 140 °F (60 °C) | Home heating oil, lubricating oils, motor oil | Yes - Recommended |

Table 5.2: Products included in API 2350’s scope

6

Risk Assessment

| Topic | Page |
|---------------------------------------|------|
| 6.1 Corporate Risk Management | 51 |
| 6.1.1 Tolerable Risk | 51 |
| 6.2 Risk Analysis | 54 |
| 6.2.1 Hazard Identification | 54 |
| 6.2.2 Hazard and Scenario Analysis | 54 |
| 6.2.3 Risk | 55 |
| 6.3 Application Risk Management | 55 |
| 6.3.1 Assess Risk | 55 |
| 6.3.2 Identify Risk Reduction Options | 56 |
| 6.3.3 Prioritization | 56 |
| 6.3.4 Implementation | 56 |
| 6.4 Monitoring and Review | 56 |
| 6.5 Communication | 56 |



6. Risk Assessment

There are inherent risks in the process and bulk liquid industries and in particular with tanks containing hazardous substances. The vision is zero accidents but there is recognition that risk cannot be eliminated completely and instead needs to be controlled. This realization resulted in risk assessment techniques emerging in the process industry during the 1970s. Today, risk assessment is a cornerstone of modern overfill prevention because it:

- Creates awareness of hazards and risks
- Identifies who or what may be at risk and the potential cost
- Determines if existing risk reduction measures are adequate or if more needs to be done
- Prioritizes risk reduction activities
- Addresses risk over time
- Can provide both personnel and the public with transparent information about the actual risks

An introduction to the concept of risk assessment is presented in figure 6.1.

Risk assessment is an integral part of both IEC 61511 and API 2350. It is a requirement in countries that have implemented a performance (risk) based legislation and sometimes also in countries with prescriptive legislation. Increasingly it is also becoming an internal company requirement.

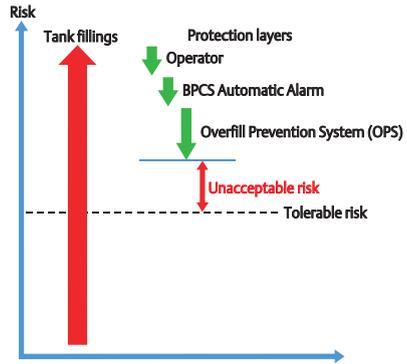


Figure 6.1: Basic concept of evaluating assessed risk compared to tolerable risk

A risk assessment is no guarantee of zero accidents. But tank overfills are predictable and risk assessment is a necessary tool to determine what (if any) protection layers should be implemented as well as how they should be designed and managed over time. In the case where an overfill prevention system is used to reduce risk, the risk assessment determines the required safety integrity level (SIL).

There are entire standards (e.g. ISO 31000) and books dedicated to the subject of risk assessment that contain numerous models, concepts and definitions. There is no single definition of what a risk assessment should contain and it often varies by context. One basic model that reflects typical process industry consensus and is useful for overfill prevention is presented in figure 6.2.

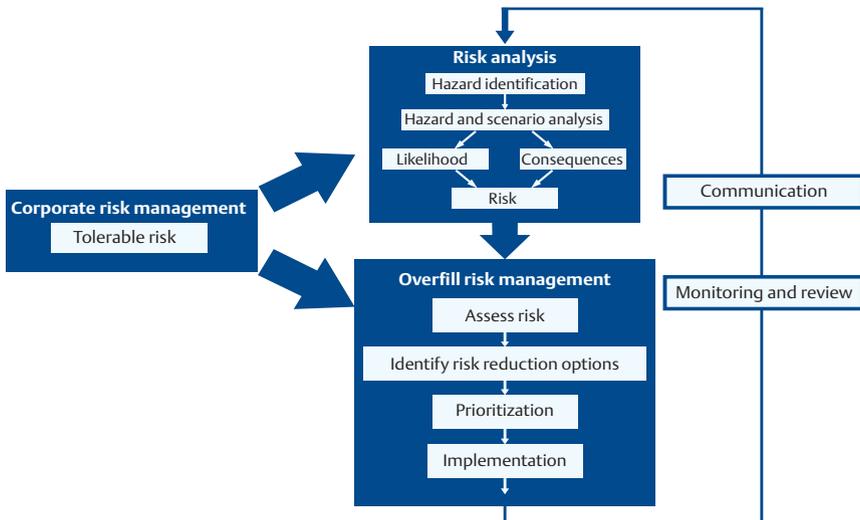


Figure 6.2: Basic risk assessment model for overfill prevention

This model is merely informational and is used to organize subsequent sections; most medium and large sized companies in the process and bulk liquid industries already have similar risk assessment processes in place which, if they are adequate, may equally be used. Overfill prevention is an organizational responsibility. The tasks described in figure 6.2 require team work among a variety of different competencies including operators, instrument engineers, maintenance staff, design engineers and safety specialists.

Subsequent sections describe the individual steps in figure 6.2, but the procedural aspects are a part of the overfill management system (OMS) which is described in chapter 7.

6.1 Corporate Risk Management

A critical fundament of risk assessment is for corporate risk management to define the amount of risk that the company deems acceptable, commonly denoted as “tolerable risk”.

Some countries, territories or even cities (e.g. United Kingdom, New South Wales in Australia, and Hong Kong) have regulations for tolerable risk, commonly based on the consequence of fatalities. These need to be taken into consideration when defining the corporate tolerable risk levels in case the company only operates in that territory; otherwise these should be taken into consideration during the “application risk management” phase in the step “assess risk” described further below.

6.1.1 Tolerable Risk

Risk consists of two components: Probability x Consequence. Probability is equivalent to the probability of a certain identified hazard occurring, and consequence reflects the severity of such an incident. The consequence factor, and thereby also the concept of risk, is ambiguous since it can be defined differently. In the process and bulk liquid industries it is common to define the consequence factor as having an adverse effect on:

- Health
- Environment
- Company image
- Asset or property
- Loss of production
- Financial impact

The tolerable risk can be defined as multiple risk levels based on different consequences. Companies need to consider carefully the definition used for tolerable risk since it indirectly communicates the company’s safety focus. A direct consequence of the tolerable risk format is that it determines the structure and outcome of the risk assessment.

6.1.1.1 ALARP

In theory, the tolerable risk can be defined as one absolute value for each selected consequence, as depicted in figure 6.3.

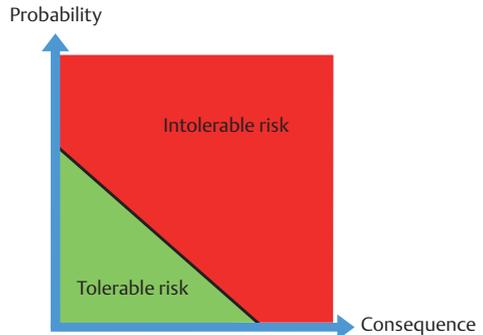


Figure 6.3: Simplified example with tolerable risk

In practice the determination of tolerable risk is more complex, which the following example indicates. Spending £1m to prevent five staff suffering bruised knees may be disproportionate; but to spend £1m to prevent a major explosion capable of killing 150 people is obviously in proportion.

Therefore the British Health and Safety Executive (HSE) invented the principle of ALARP which is an abbreviation of “as low as reasonably practicable”. Reasonably practicable involves weighing a risk against the trouble, time and money needed to control it. The purpose is to enable proportionate risk reduction measures and the principle has been widely adopted in the process industry and by other countries. An overview of the principle is depicted in figure 6.4 and the specific numbers used in the United Kingdom are presented in figure 6.5 along with a comparison in figure 6.6

6 - Risk Assessment

6.1.1.2 Tolerable Risk Examples

The theoretical models described above are typically implemented by corporations as multiple risk graphs for the selected consequences, e.g. health,

environment and financial losses. The risk graphs may either be quantitative, semi-quantitative or qualitative as described in figure 6.7 and 6.8.

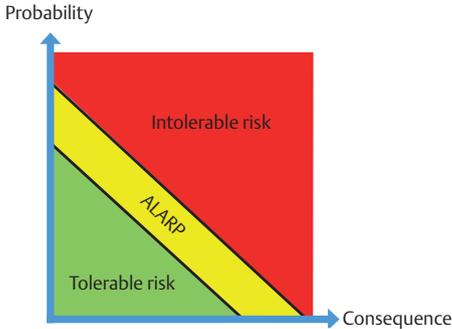


Figure 6.4: The principle of "as low as reasonably practicable" (ALARP)

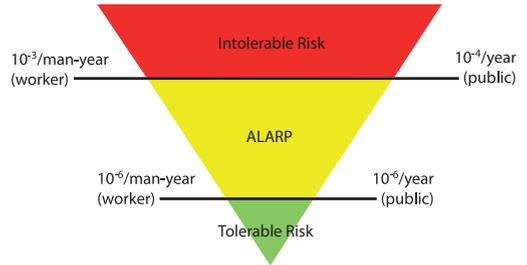


Figure 6.5: Typical depiction of tolerable risk levels as defined by the British Health and Safety Executive (HSE)

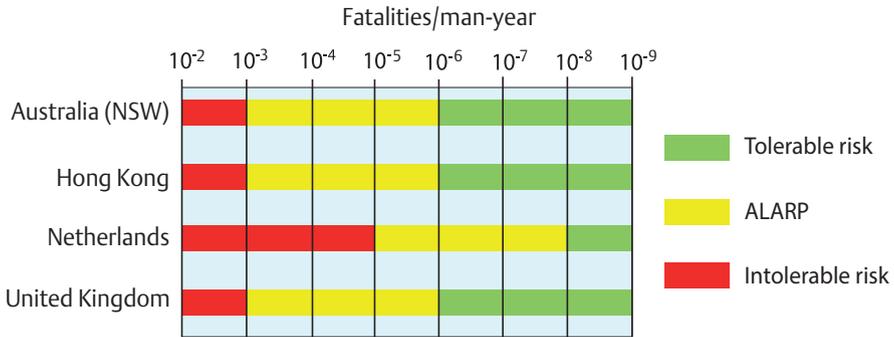


Figure 6.6: Comparison of tolerable risk levels for the consequence of fatalities

| | | |
|--------------|-------------|---------------|
| Catastrophic | Red | STOP |
| Unacceptable | Orange | URGENT ACTION |
| Undesirable | Yellow | ACTION |
| Acceptable | Light Green | MONITOR |
| Desirable | Dark Green | NO ACTION |

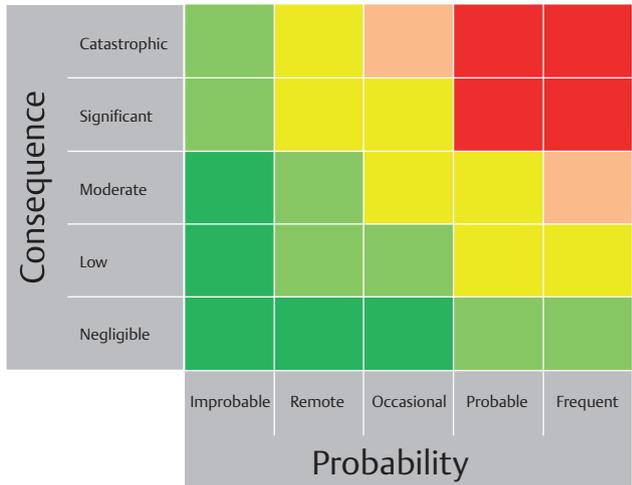


Figure 6.7: Example of qualitative corporate risk graph

| Health | Asset | Environment | Company image | Frequency | | | | |
|---|---------------------------|------------------|----------------------|-------------------|---------------------|-------------------------------------|---------------------------------|-------------------------------------|
| | | | | >0.1/yr Likely | <0.1/yr Probable | <10 ⁻² /yr Occasional | <10 ⁻³ /yr Remote | <10 ⁻⁴ /yr Improbable |
| Multiple fatalities (<10 ⁻⁵ /yr) | Extensive damage (>\$10M) | Massive effect | International impact | Stop | Stop | SIL 3 | SIL 2 | SIL 1 |
| Single fatality (<10 ⁻⁴ /yr) | Major damage (<\$10M) | Major effect | National impact | Stop | SIL 3 | SIL 2 | SIL 1 | OK |
| Major injury (<10 ⁻³ /yr) | Major damage (<\$500K) | Localized effect | Considerable impact | SIL 3 | SIL 2 | SIL 1 | OK | OK |
| Minor injury (<10 ⁻² /yr) | Minor damage (<\$100K) | Minor effect | Minor impact | SIL 2 | SIL 1 | OK | OK | OK |
| Slight injury (<0.1/yr) | Slight damage (<\$10K) | Slight effect | Slight impact | SIL 1 | OK | OK | OK | OK |
| None | None | None | None | OK | OK | OK | OK | OK |

Figure 6.8: Example corporate risk matrix. Worst-case consequence outcome determines the required risk reduction

6.2 Risk analysis

6.2.1 Hazard Identification

The first step of the risk analysis is to conduct hazard identification. A hazard is an object, a property of a substance, a phenomenon, or an activity that can cause adverse effects. This is not to be confused with a risk, which is the probability and consequence of a hazard actually causing its adverse effects.

Multiple tools exist to identify hazards such as HAZOP (hazard and operability study), HAZID (hazard identification) and "What if analysis". Usually, these are based on a checklist containing keywords such as temperature, level, pressure, chemical reaction and agitation used as input parameters to identify hazards. Within the scope of this book, the hazard identification covers tank overfills.

6.2.2 Hazard and Scenario Analysis

Numerous techniques can be used to estimate the risk of a tank overfill. These techniques can be based on either historical data or an analytical approach, or a mix of the two. Ultimately they all depend on the estimation of the probability and the consequence of a tank overfill.

6.2.2.1 Probability Estimation

The probability of an overfill occurring depends on a number of different parameters. API 2350 provides a useful list of considerations originally intended for the bulk liquid industry but, to a large extent, are also applicable to the process industry:

- Frequency, rate and duration of filling
- Systems used to properly measure and size receipts to tanks
- Accurate tank calibration
- Systems used to monitor receipts
- Extent of monitoring and supervision of manual and automatic tank gauging
- Impact of complexity and operating environment on the ability of operating personnel to execute overfill prevention tasks
- Filling multiple tanks simultaneously
- Switching tanks during receipt

A basic example based on an analytical model and the risk reduction factors specified in IEC 61511 is provided in figure 6.9. The example assumes that the operator and BPCS automatic alarm are independent - which is not always the case.

In the example given in figure 6.9, an operator is estimated to reduce overfill risk by a factor of 10. A BPCS automatic alarm reduces risk by an additional factor of 10 and an independent overfill prevention system by a factor of 100. Consequently, the three layers combined results in a risk reduction factor of $10 \times 10 \times 100 = 10,000$. Alternatively, the probability of overfill each filling is $0.01\% = 1/10,000$. With 30 fillings per year, this tank's yearly overfill probability becomes 0.3%.

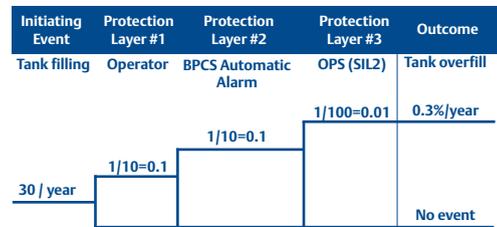


Figure 6.9: Example probability estimation of tank overfills using an event-tree analysis

This number can be compared to the historical data provided by Marsh showing that an overfill occurs once every 3,300 fillings. (Marsh & McLennan Companies, 2001). In other words, the average risk reduction factor of protection layers against overfill currently being used is 3,300, and probability of overfill each filling is $0.03\% = 1/3,300$. Three times as unsafe.

6.2.2.2 Consequences Estimation

The consequences estimated depend on the expected output of the risk analysis, which is usually governed by the corporate tolerable risk criteria.

The assessed consequences depend on a number of different parameters. API 2350 provides a useful list of factors to take into consideration. This is intended for the bulk liquid industry, but is to a large extent also applicable to the process industry:

- Hazard characteristics of material (product) in tank
- Volatility, flammability, dispersion, vapor cloud explosion potential
- Number of people onsite who may be affected by a tank overfill
- Number of people offsite who may be affected by a tank overfill
- Possibility of a tank overflow resulting in escalation of hazardous events onsite or offsite

- Possibility of impact to nearby sensitive environmental receptors
- Physical and chemical properties of product released during overflow
- Maximum potential overflow flow rates and duration

A simplified example based on an event analysis is provided in figure 6.10. In this fictitious scenario, the estimated financial consequences from the single event of product overflow into secondary containment is estimated as \$480,000 in clean-up costs. As shown in figure 6.10, this estimation is based on the assumption that 80% of the product will be contained by the secondary containment costing \$250,000 (80% x 350,000), 5% will overflow the secondary containment costing an additional \$50,000 (5% x 1,000,000) and a final 15% leakage from the secondary containment will drive yet another \$150,000 (15% x 1,000,000)

6.2.3 Risk

Combining the probability and consequences result in an estimation of the risk.

Using the examples provided in figures 6.8 and 6.9, the estimated risk for a single tank to experience a single event of product in the secondary containment is \$1,440/year = 0.3%/year x \$480,000. Notice that this is an incomplete fictitious example; when including other events and consequences such as fatalities, injuries, environment, company image, asset damages and loss of production the risk is likely to be much higher.

6.3 Application Risk Management

6.3.1 Assess Risk

The estimated risk obtained from the risk analysis needs to be assessed to determine if additional (or less) risk reduction is required. Often several stakeholders need to be taken into consideration:

1. Corporate tolerable risk criteria
2. Regulatory requirements
3. Industry standards and RAGAGEP

During this step, it will be determined how much (or little) risk reduction for a tank overflow is required. When determining the required risk reduction it is essential to not only consider current requirements but also expectations for the future. Historically the tolerable risk has been decreasing, and it is probable that this trend will continue. According to the Flixborough report:

“... for what is or is not acceptable depends in the end upon current social tolerance, and what is regarded as tolerable at one time may well be regarded as intolerable at another.”

For example, if current requirement is a risk reduction factor of minimum 100 (SIL 2), then the input to subsequent steps in the risk management process may be that a risk reduction factor of 1,000 (SIL 3) is recommended, or alternatively the identified risk reduction option shall be SIL 2 but easily upgradable to SIL 3.

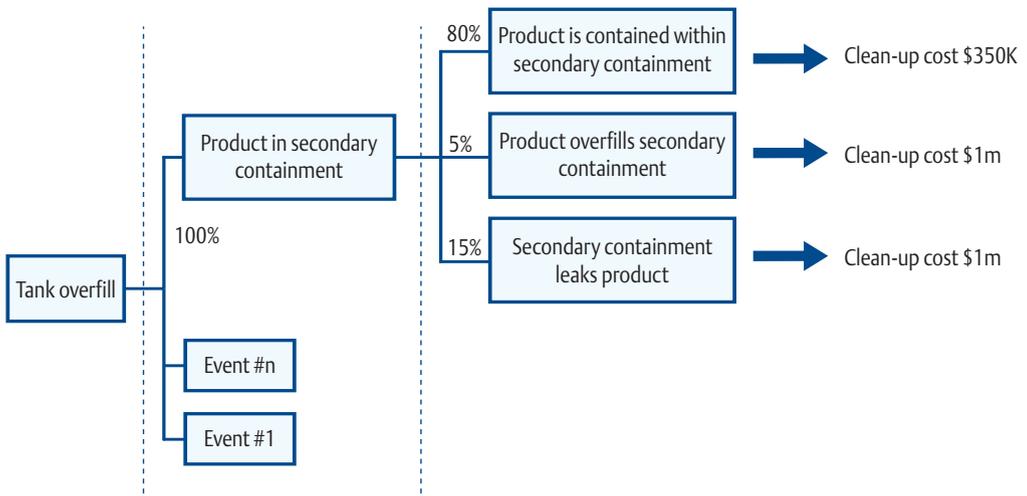


Figure 6.10: Parts of a simplified example consequence analysis of a tank overflow

6.3.2 Identify Risk Reduction Options

The purpose of this step is to identify options to sufficiently reduce the risk of a tank overfill. Typically, several different options are available:

- Inherent process design change
- Changes in the Overfill Management System (e.g. operational procedures)
- Implementing additional protection layers or modifying the existing ones

The identified risk reduction options should be accompanied with the information required for subsequent prioritization:

- Risk reduction factor
- Type of risk reduction; prevention or mitigation
- Cost
- Time to implement
- Operational costs such as maintenance and testing
- Effect on operations
- Upgrade cost to increase the risk reduction factor

It should be noted that according to IEC 61511, the risk reduction factor is limited to 10 for protection layers that are not designed according to IEC 61511.

6.3.2.1 Consequence Reduction

Protection layers such as secondary containment and fire patrol are targeted towards reducing the consequence. Although these protection layers reduce the risk, the result is only a mitigation of the tank overfill.

6.3.2.2 Probability Reduction

Protection layers such as the BPCS and overfill prevention system are designed to reduce the probability of a tank overfill through prevention.

6.3.3 Prioritization

During this step, it should be decided what risk reduction option to use and the prioritization compared to other projects in the company.

When determining what risk reduction option to use it is especially important to evaluate whether the solution prevents or mitigates the risk, and whether the risk reduction option meets future requirements.

In the case of tank overfill, the most commonly selected risk reduction option is an overfill prevention system (OPS) because it:

- Prevents (rather than mitigates) the risk of tank overfill
- Is the considered Recognized And Generally Accepted Good Engineering Practices (RAGAGEP)
- Commonly a regulatory requirement
- Can provide a higher risk reduction factor than 10 if designed according to IEC 61511
- Is the most cost efficient approach

6.3.4 Implementation

During this phase, the risk reduction option is implemented. In case the selected risk reduction option is an overfill prevention system, more information can be found in chapter 7.

6.4 Monitoring and Review

Risk assessment is a life-cycle process that requires continuous monitoring, review and management of change.

6.5 Communication

Modern risk assessment recognizes the value of providing both personnel and the public with transparent information. This includes the results from the risk analysis, risk management and monitoring and review phases (e.g. inspection protocols and proof-test records).

7

Overflow Management System

| Topic | Page |
|-------------------------------|------|
| 7.1 Why OMS is Needed | 58 |
| 7.2 The Basic Elements of OMS | 59 |
| 7.3 Success Factors | 59 |



7. Overfill Management System

Traditionally, tank overfills are attributed to malfunctioning equipment. Although this is often a contributing factor, the actual root cause is often more complex and involves human behavior. Therefore, a critical part of modern overfill prevention is to establish an adequate Overfill Management System (OMS) that is implemented throughout the organization, including how it actually works in the field.

The Center for Chemical Process Safety describes management systems as “a formally established and documented set of activities designed to produce specific results in a consistent manner on a sustainable basis” (CCPS Guidelines for Risk Based Process Safety, AIChE). Although a large task at first, the creation of an adequate OMS is not just a necessity to prevent tank overfills, it also eventually results in a more efficient facility.

The relation between OMS, corporate management system and safety management system is described in figure 7.1.

7.1 Why is an OMS Needed?

Most companies today have implemented generic management systems, but not necessarily a specific system for overfill management. The need for OMS, however, is becoming increasingly recognized. It is an integral part of API 2350, and it is incorporated into the Occupational Safety & Health Administration’s (OSHA) Process safety management (PSM) regulation in the US and through the Seveso directive in Europe.

An OMS can help reduce the number of tank overfills in the following ways:

- OMS ensures that overfill prevention is prioritized and that risk for overfills is appropriately addressed
- OMS ensures that the tools needed to systematically identify potential and actual hazards and manage risks are provided and supported by management
- OMS ensures that incidents and near misses are systematically analyzed to determine the root causes of overfills
- OMS ensures that equipment, procedures and operations are continuously evaluated and improved as needed to prevent and control overfills
- OMS ensures that the personnel who manage and operate tank facilities are knowledgeable and trained in the basic principles of overfill prevention and protection
- OMS ensures that organizations have the information needed to support business decisions that justify necessary resources, and appropriate controls and other measures needed to reduce risks to acceptable levels
- OMS ensures appropriate allocation of resources for overfill prevention
- OMS ensures that management, supervisory and employee behavior, attitudes, values, skills and actions are totally committed to preventing, managing and controlling overfills

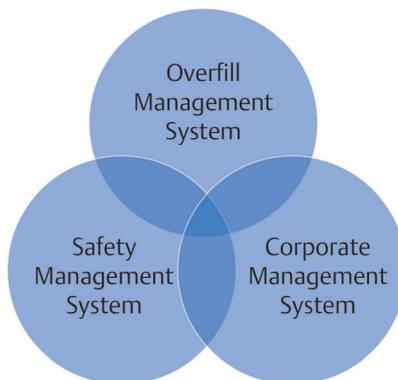


Figure 7.1: Venn diagram perspective showing how OMS relates to other corporate management systems

7.2 The Basic Elements of OMS

There is no commonly accepted way to organize and name the elements of an OMS. Text box 7.1 provides a listing of common elements included in an OMS as a part of a modern overfill prevention approach.

| | |
|------------------------|--|
| Key Element 1: | Safety and environmental advocacy |
| Key Element 2: | Safety and environmental information |
| Key Element 3: | Risk assessment |
| Key Element 4: | Management of change |
| Key Element 5: | Procedures and safe work practices |
| Key Element 6: | Training and competent personnel |
| Key Element 7: | Equipment integrity |
| Key element 8: | Conformance to industry standards |
| Key Element 9: | A permit system |
| Key Element 10: | Pre-startup safety review |
| Key Element 11: | Pre-shutdown safety review |
| Key Element 12: | Emergency response and control |
| Key Element 13: | Near miss and incident investigation (“lessons learned”) |
| Key Element 14: | Auditing |
| Key Element 15: | Document and data information management systems |
| Key Element 16: | OMS oversight, review, reevaluation and adjustment |

Text box 7.1: Common elements of an overfill management system (OMS). The listing is a customized version of OSHA’s PSM regulation

7.3 Success Factors

The key elements of an OMS are generic, but the implementation is company and facility specific. Established success factors for an OMS to be effective include:

- **Top management support**

OMS must be established, implemented and actively and continuously supported by the organization’s leadership.

- **Employee engagement**

OMS requires formal leadership responsibility and accountability at all levels of the organization.

- **Safety culture**

OMS requires correctly aligned behavior and attitudes by all employees, working together, so that proactive hazard identification, risk management, information control, training, procedures, and management of change are recognized and accepted principles of operation.

- **Continuous improvement**

OMS requires continual review, evaluation and improvement through activities such as incident and accident investigation, audits and management of change.



8

Overfill Prevention System

| Topic | Page |
|--|------|
| 8.1 Manual Overfill Prevention System | 62 |
| 8.2 Automatic Overfill Prevention System | 63 |
| 8.3 AOPS vs. MOPS | 64 |
| 8.4 Hardware Fault Tolerance | 64 |
| 8.5 Levels of Concern | 66 |



8. Overfill Prevention System

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

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

8.1 Manual Overfill Prevention System

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

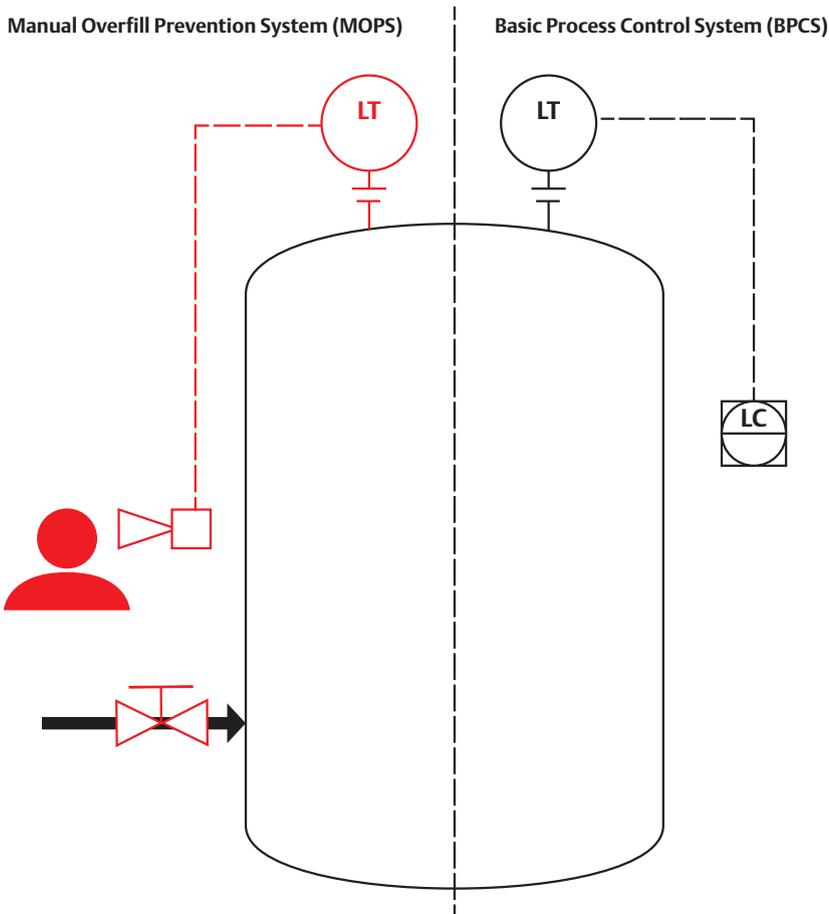


Figure 8.1: MOPS usually consists of a level transmitter (LT) connected to an audiovisual alarm that notifies an operator to take the appropriate action, e.g. closing a valve. API 2350 classification: category #3

8 - Overfill Prevention System

8.2 Automatic Overfill Prevention System

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

An typical AOPS consists of the principal components illustrated in figure 8.2. It is also common that the

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

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

AOPS consists of the following non-safety critical functions:

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

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

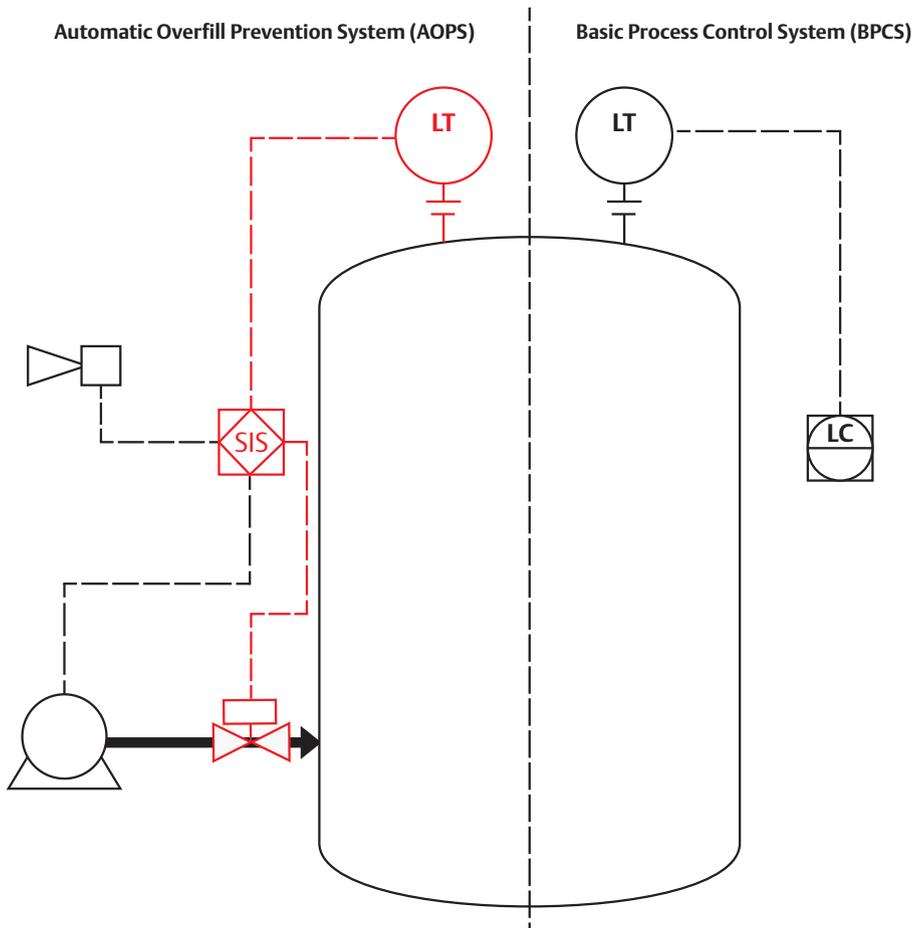


Figure 8.2: AOPS usually consists of a level transmitter (LT), logic and actuator which automatically closes a valve to prevent overfills from occurring. The logic may also execute non-safety critical tasks such as shutting down a pump and notifying the operators through audiovisual alerts. API 2350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

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

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

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

8.3 AOPS vs. MOPS

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

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

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

8.4 Hardware Fault Tolerance

An AOPS needs to consist of a sensor, a logic solver, and an actuator. However, it is a common practice to add more than one of certain elements within the same AOPS. This is referred to as a system’s Hardware Fault Tolerance (HFT) and can be employed to increase both reliability and availability of an OPS. Hardware Fault Tolerance (HFT) can be employed to both increase the reliability and availability of an OPS as described in the following examples. Figure 8.3 illustrates the most basic setup. A single sensor is

connected to a single logic solver that communicates with a single actuator. There are no redundant elements, hence $HFT=0$. This system is referred to as 1oo1 (1-out-of-1) since each element single-handedly determines the action of the system.

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

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

8 - Overfill Prevention System

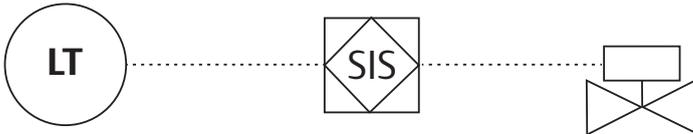


Figure 8.3: OPS consisting of 1oo1 sub-systems (HFT = 0)

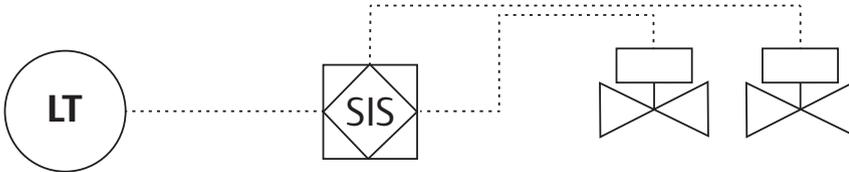


Figure 8.4: OPS consisting of 1oo2 actuators (HFT = 1). This configuration increases the reliability, but decreases the availability, compared to a 1oo1 configuration

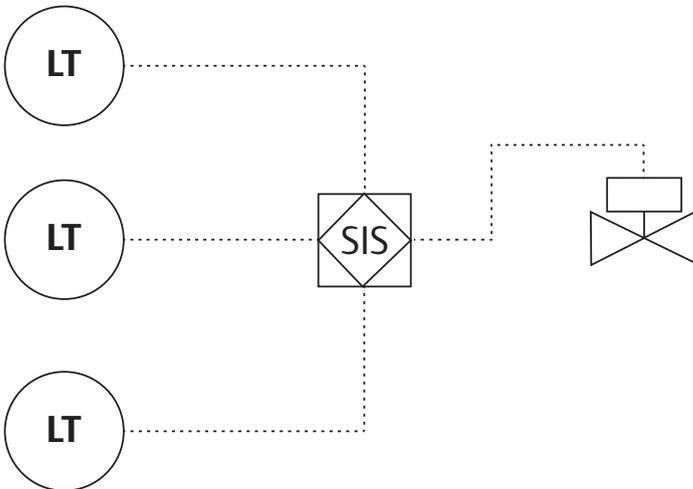


Figure 8.5: OPS consisting of 2oo3 sensors (HFT = 2). This configuration increases both the reliability and availability, compared to a 1oo1 configuration

8.5 Levels of Concern

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

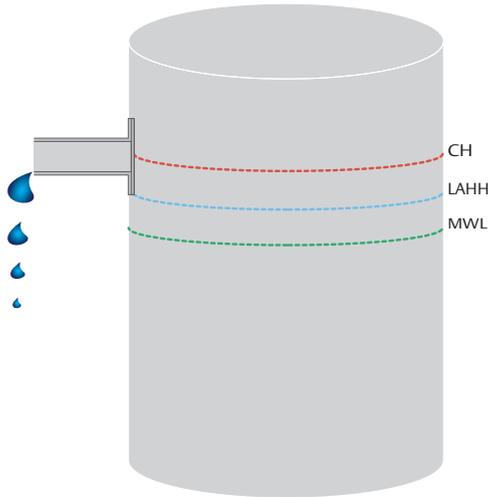


Figure 8.6: The Levels Of Concern (LOC) for tank overfill prevention

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

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

$$CH - LAHH = \text{Max level rate} \times \text{Response time} + \text{Safety margin}$$

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

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

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

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

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

9

Proof-Testing

| Topic | Page |
|--|------|
| 9.1 Proof-Testing Requirements_____ | 69 |
| 9.1.1 IEC 61511_____ | 69 |
| 9.1.2 API 2350_____ | 70 |
| 9.2 Proof-Test Interval_____ | 70 |
| 9.2.1 IEC 61511_____ | 71 |
| 9.2.2 API 2350_____ | 74 |
| 9.3 Traditional Approach to Overfill Prevention_____ | 74 |
| 9.3.1 Traditional Proof-Testing Procedures Exemplified With Point Level Sensors_____ | 75 |
| 9.4 Modern Approach to Proof-Testing____ | 77 |
| 9.4.1 Benefits_____ | 77 |
| 9.5 Implications_____ | 78 |



9. Proof-Testing

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

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

proof-test cost over the lifecycle of the device.

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

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

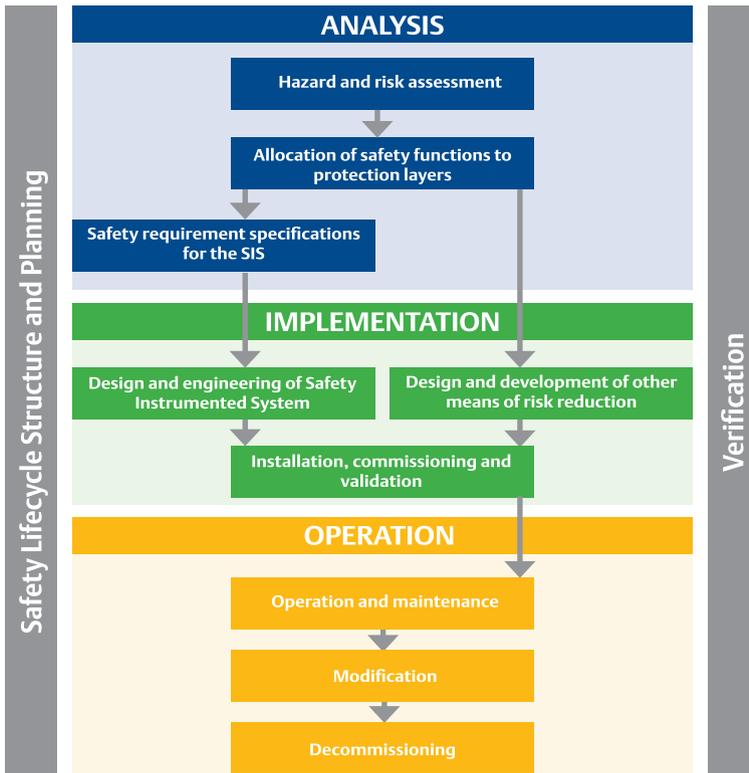


Figure 9.1.1: Management of functional safety

9 - Proof-Testing

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

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

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

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

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

9.1 Proof-Testing Requirements

9.1.1 IEC 61511

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

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

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

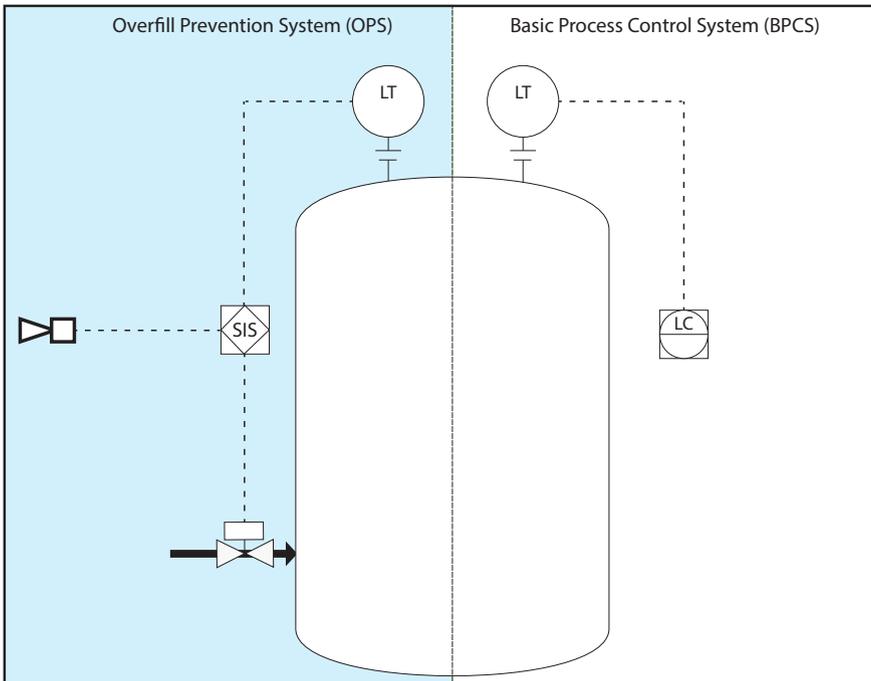


Figure 9.1.2: Proof-testing applies to all components of an overfill prevention system (OPS)

9 - Proof-Testing

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

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

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

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

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

- Proof-testing can be dangerous. Immediate safety concerns can arise, or the safety function may be

forgotten in an inoperable state. It is therefore critical that the proof-test is performed by qualified personnel who are properly trained and execute the procedure exactly according to the instructions, without any deviations

- The user shall maintain records that certify that proof-tests and inspections were completed as required. These records shall include the following information as a minimum:
 - Description of the tests and inspections performed
 - Dates of the tests and inspections
 - Name of the person(s) who performed the tests and inspections
 - Serial number or other unique identifier of the system tested
 - Results of the tests and inspection

9.1.2 API 2350

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

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

9.2 Proof-Test Interval

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

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

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

In practice, a number of factors based on internal and

external requirements must be taken into account when determining the proof-test interval. The remainder of this section describes the requirements according to IEC 61511 and API 2350.

9.2.1 IEC 61511

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

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

9.2.1.1 The Bathtub Curve

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



Figure 9.2: The bathtub curve

9.2.1.2 What is the Proof-test definition?

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

9.2.1.3 Why do proof-testing?

Testing of safety system components to detect any failures not detected by automatic on-line

diagnostics i.e. dangerous failures, diagnostic failures, parametric failures is followed by repair of those failures to an equivalent as- new state. Proof-testing is a vital part of the safety lifecycle and is critical to ensuring that a system achieves its required SIL throughout the safety lifecycle.

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

9.2.1.4 Probability of Failure on Demand

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

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

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

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

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

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

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

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

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

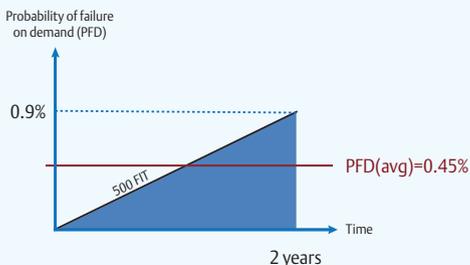
An automatic overfill prevention system has a total failure rate of $\lambda_{DU} = 500 \text{ FIT} = 500 [1/10^9 \text{ hours}]$. The probability of failure on demand at $T=2 \text{ years}$ approximately equals:

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

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

$$\text{PFD}_{\text{avg}} \approx 0.9\% / 2 = 0.45\%$$

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



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

9.2.1.5 How is Proof-Testing Performed?

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

9.2.1.6 What is Proof-Test Coverage?

The diagnostic coverage combined with proof-testing determines the percentage of dangerous failures that can be detected for a device. Proof-test coverage is a measure of how many undetected

dangerous failures, not identified by a device's diagnostics, that can be detected by the proof test.

9.2.1.7 Does Diagnostic Coverage Affect the Proof-Test Coverage?

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

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

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

9.2.1.9 Proof-Test Coverage Factor

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

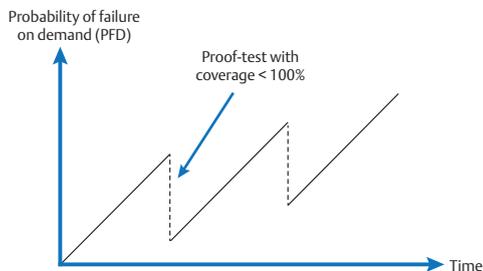


Figure 9.3: The repetitive effect on the probability of failure on demand caused by an imperfect proof-test procedure

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

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

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

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

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

9.2.1.10 Combining a Safety Function's Sub-Systems

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

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

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

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

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

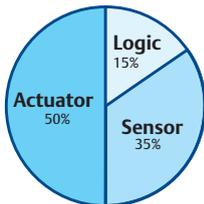


Figure 9.4: Commonly used model to estimate the approximate PFD_{avg} requirements for the different sub-systems in a safety function

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

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

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

According to the standard model, the sensor is allowed to contribute $PFD_{avg} = 35\% \times PFD_{avg} = 35\% \times 1/200 = 0.18\%$.

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

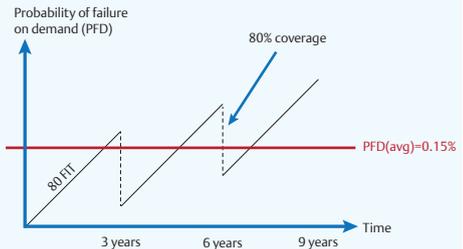


Figure 9.5: Visualization of example PFD and PFD_{avg} calculation

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

9.2.1.11 Comprehensive and Partial Proof-Testing

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

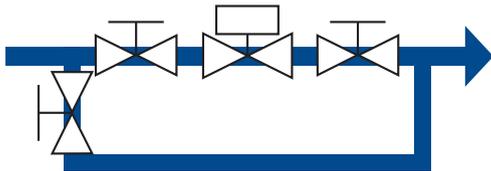


Figure 9.6: Principal overview bypass pipe used for actuator and valve testing

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

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

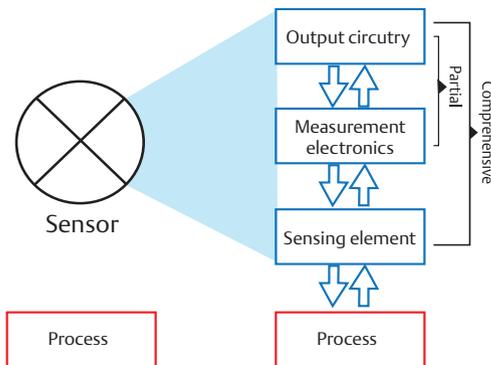


Figure 9.7: Sensor segmented into the functional elements Output circuitry, Measurement electronics, and Sensing element

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

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

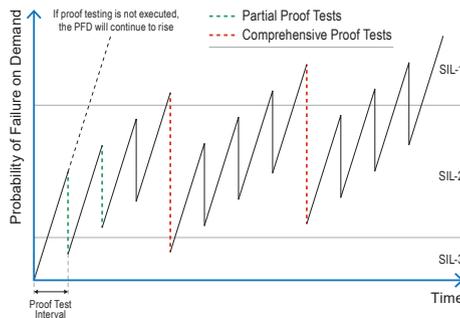


Figure 9.8: Test coverage of partial and comprehensive proof-testing

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

9.2.2 API 2350

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

For the prescriptive numbers, API 2350 specifies that:

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

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

9.3 The Traditional Approach to Overfill Prevention

Proof-testing has attracted little attention in the traditional approach to overfill prevention (described in chapter 3 “Key Elements”). Test effectiveness has often been low and the test intervals have often not been determined analytically. The personnel’s trust

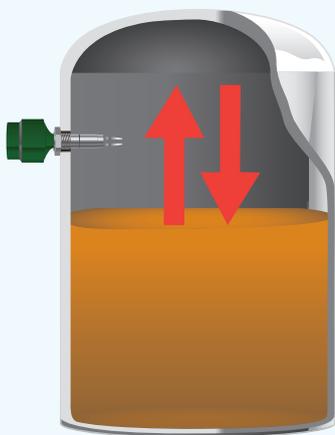
in the tests has been low and execution has therefore not been stringent and often close to random. The often non-documented procedures have been cumbersome and in some cases dangerous and resulted in considerable downtime. Documented evidence that the proof-test has been executed correctly is often incomplete or non-existing.

9.3.1 Traditional Proof-Testing Procedures Exemplified with Point Level Sensors

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

Live Simulation of Alarm Condition

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



Test Buttons and Remote Proof-Testing

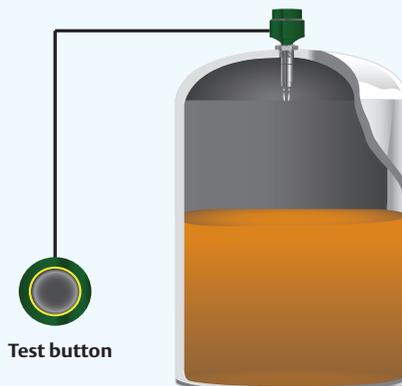
Versions of the test lever principle have also been designed for electronic point level sensors, often implemented as a local test button inside the level sensor's enclosure. This can be performed in-situ but requires an enclosure cover to be removed, which is a potential risk. Therefore, some designs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

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

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

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

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

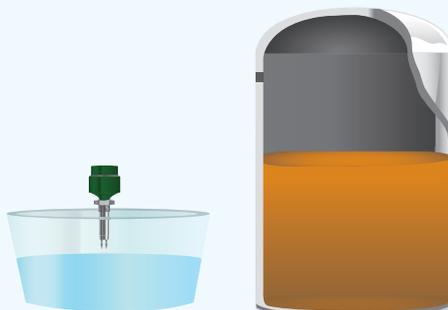


Bucket Testing

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

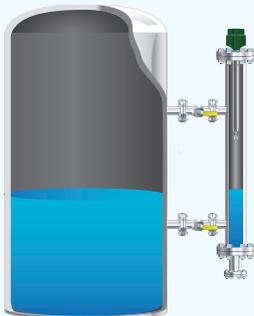
When the test is not performed with the media to be measured, there is an obvious risk that test results become irrelevant for the true process conditions. Furthermore, when sensors are dismantled, there is no guarantee that re-commissioning is correctly executed. There may be cable glitches, gaskets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

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



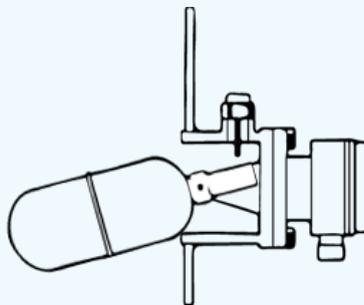
Test Chambers

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



Test Levers

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



9.4 The Modern Approach to Proof-Testing

9.4.1. Benefits

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

The benefits of a modern approach also include safety improvements:

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

Efficiency Improvements

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

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

Proof-testing point level measurement: $4 \text{ hours} \times 2 \text{ tests/year} \times 10 \text{ years} \times \$100/\text{hour} = \$8000$

Proof-testing continuous level measurement: $0.5 \text{ hours} \times 1 \text{ tests/year} \times 10 \text{ years} \times \$100/\text{hour} = \$500$

Proof-Testing Case: LA Refinery

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

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



Picture 9.1: Refinery

Case 9.1: Proof-testing case: LA Refinery

9.5 Implications

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

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

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

Proof-Testing Radar Level Sensors: Latest Advancements

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

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

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

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

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

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

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

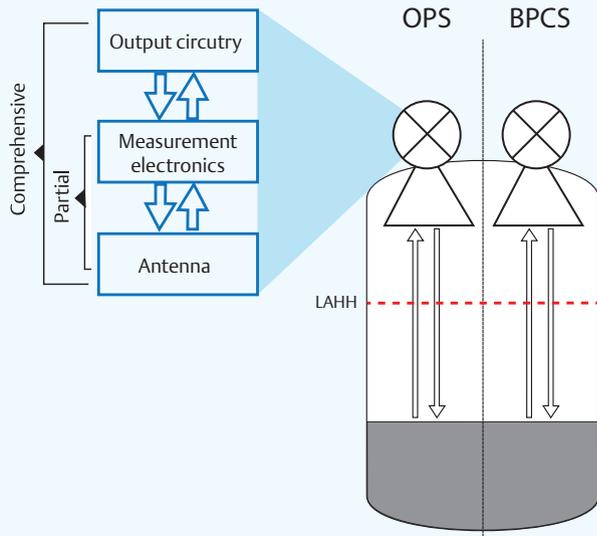


Figure 9.10: Example of better proof-testing methods with modern overfill prevention equipment

Proof-Testing in Rosemount TankMaster™

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

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

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

Comprehensive Proof Test

- High level alarm verification using a reference reflector

Partial Proof Test

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

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

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

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

Comments:

* Test performed by: Mike

* Test approved by: Anders

NOTE: Report will be generated when pressing "Finish" button Test date: 2019-1-11

Proof Test Report

LT-TK-12

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

HUB-110

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

Simulated Reference Reflector Verification

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

One-Point Level Verification

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

Analog Output Verification

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

10



Available Technologies

| Topic | Page |
|--------------------------------|------|
| 10.1 Vibrating Forks_____ | 82 |
| 10.1.1 Advantages_____ | 82 |
| 10.1.2 Limitations_____ | 82 |
| 10.2 Guided Wave Radar_____ | 82 |
| 10.2.1 Advantages_____ | 83 |
| 10.2.2 Limitations_____ | 83 |
| 10.3 Non-Contacting Radar_____ | 83 |
| 10.3.1 Advantages_____ | 83 |
| 10.3.2 Limitations_____ | 84 |



10. Available Technologies

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

10.1 Vibrating Forks

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

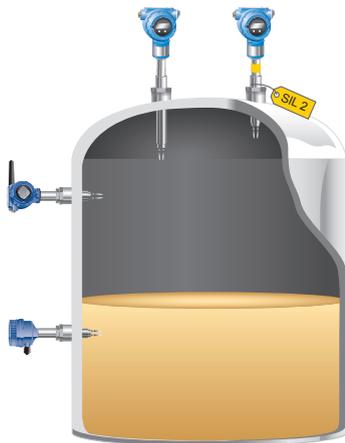


Figure 10.1: Vibrating forks

10.1.1 Advantages

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

10.1.2 Limitations

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

10.2 Guided Wave Radar

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

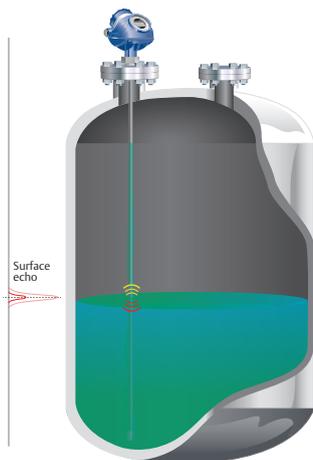


Figure 10.2: Guided wave radar technology

10.2.1 Advantages

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

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

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

10.2.2 Limitations

While GWR works in many conditions, some precautions need to be taken with respect to probe choice. Several probe styles are available and application, length, and mounting restrictions influence the choice. Unless a coaxial probe is used,

probes should not be in direct contact with a metallic object, because that will impact the signal. If the application tends to be sticky or coat, then only single lead probes should be used. Some of the latest GWRs on the market have advanced diagnostics, with the ability to detect build-up on the probe. Chambers with a diameter less than 3 in. (75 mm) may cause problems with build-up and may make it difficult to avoid contact between chamber wall and probe.

10.3 Non-Contacting Radar

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

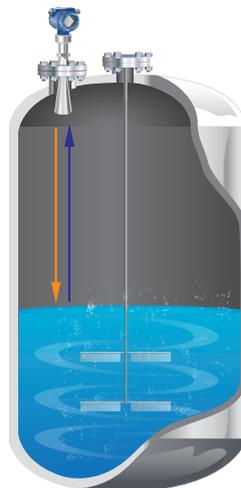


Figure 10.3: Non-contacting radar technology

10.3.1 Advantages

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

measured media it is also good for corrosive and dirty applications.

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

10.3.2 Limitations

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

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

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

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

11



Rosemount™ Products

| Topic | Page |
|--------|---|
| 11.1 | Rosemount 2120 Vibrating Fork_____86 |
| 11.2 | Rosemount 2130 Vibrating Fork_____87 |
| 11.3 | Rosemount 2140:SIS Vibrating Fork_87 |
| 11.4 | Rosemount 5300 Guided Wave Radar_88 |
| 11.5 | Rosemount 5408:SIS Non-Contacting Radar_____89 |
| 11.6 | Rosemount 5900S Radar Level Gauge_89 |
| 11.7 | Rosemount 5900S 2-in-1 Radar Level Gauge_____90 |
| 11.8 | Rosemount 5900C Radar Level Gauge_90 |
| 11.9 | MTBF (Mean Time Between Failure)___91 |
| 10.9.1 | Random Failures_____91 |
| 10.9.2 | The Model_____91 |
| 10.9.3 | The Calculation_____91 |
| 11.10 | Product Specification Overview _____92 |

11. Rosemount Products



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

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

11.1 Rosemount 2120 Vibrating Fork



Picture 11.2: Rosemount 2120

11.1.1 Operating Environment

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

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

11.1.2 Certificates and Approvals

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

* DRY=ON configuration

11.1.3 Product Features

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

11.2 Rosemount 2130 Vibrating Fork



Picture 11.3: Rosemount 2130

11.2.1 Operating Environment

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

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

11.2.2 Certificates and Approvals

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

* DRY=ON configuration

11.2.3 Product Features

- Flexibility of Rosemount 2120 options and features with extended capabilities for challenging process conditions
- Extended operating temperature range
- Advanced built-in diagnostics continuously check electronic and mechanical health
- Visible Heartbeat led for device status and health

- Adjustable switching delay for turbulent or splashing applications
- Magnetic test point for quick and simple partial proof test
- DiBt/WHG overfill protection certification

11.3 Rosemount 2140:SIS Vibrating Fork



Picture 11.4: Rosemount 2140:SIS

11.3.1 Operating Environment

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

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

11.3.2 Certificates and Approvals

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

11.3.3 Product Features

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

11.4 Rosemount 5300 Guided Wave Radar



Picture 11.5: Rosemount 5300

11.4.1 Operating Environments

The Rosemount 5300 (picture 11.5) is highly accurate and reliable direct level measurement with

no compensation needed for changing process conditions (such as density, conductivity, viscosity, pH, temperature, and pressure) and is suitable for most liquid and solids level applications and liquid interface applications.

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

11.4.2 Certificates and Approvals

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

11.4.3 Product Features

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

11.5 Rosemount 5408:SIS Non-Contacting Radar



Picture 11.6: Rosemount 5408:SIS

11.5.1 Operating Environments

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

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

11.5.2 Certificates and Approvals

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

11.5.3 Product Features

- Unique energy-efficient two-wire FMCW radar technology for optimal performance
- Engineered and user tested for best in class safety, reliability, and ease-of-use
- A Smart Diagnostics Suite provides operators with early alerts in case of antenna build-up, weak power supply, or abnormal surface conditions
- A local memory enables full insight into the last seven days of measurements, alerts, and echo profiles

- Safe, easy, and remote proof testing without process interruptions
- Hazardous area approvals: ATEX, IECEx, FM, CSA
- DiBt/WHG overfill protection certification
- Immune to intermittent power loss

11.6 Rosemount 5900S Radar Level Gauge



Picture 11.7: Rosemount 5900S

11.6.1 Operating Environments

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

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

11.6.2 Certificates and Approvals

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

11.6.3 Product Features

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

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



Picture 11.8: Rosemount 5900S 2-in-1

11.7.1 Operating Environments

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

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

11.7.2 Certificates and Approvals

| Output Type | Level of Integrity | SFF |
|-------------|---------------------------------------|-----|
| Relay | SIL3 @ HFT=0, Route 1 _H | 99% |

| | | |
|---|---------------------------------------|-------------------------|
| 4-20mA Relay 4-20mA & Relay combined | SIL2 @ HFT=0, Route 1 _H | 91.9% 91.6% 90.9% |
| 4-20mA Relay 4-20mA & Relay combined | SIL2 @ HFT=0, Route 2 _H | N/A |

11.7.3 Product Features

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

11.8 Rosemount 5900C Radar Level Gauge



Picture 11.9: Rosemount 5900C

11.8.1 Operating Environments

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

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

11.8.2 Certificates and Approvals

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

11.8.3 Product Features

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

11.9 MTBF (Mean Time Between Failure)

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

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

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

number of units that statistically will fail is 20 units (2000 unit-years / 100 years).

11.9.1 Random Failures

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

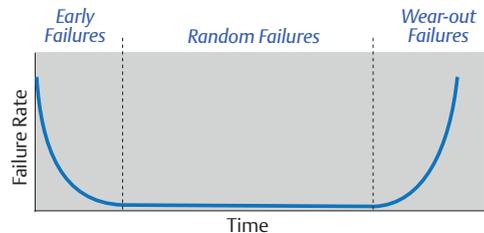


Figure 11.1: The Bathtub Curve showing hypothetical failure rate over time

11.9.2 The Model

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

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

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

11.9.3 The Calculation

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

The accumulated time-in-operation has been estimated as the time interval between shipment date to the creation date of this document subtracted by six months. Here, five months represent the average time between shipment of a unit and the time of commissioning. Additionally one month is used to represent the average time it

11 - Rosemount Products

takes a user to notify the manufacturer of the device failure. (5+1 = 6 months)

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

Accumulated Time-In-Operation = 48900 years

Accumulated No. of Random and Verified Failures = 66

Field Experienced MTBF = 48900 / 66 years

| Field Experienced MTBF Rosemount 5900 |
|--|
| 741 years |

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

11. 10 Product Overview Specification

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

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

12

Overfill Prevention System Examples

| Topic | Page |
|---|------|
| 12.1 Bulk Liquid Storage _____ | 94 |
| 12.1.1 Fixed Roof Tanks _____ | 94 |
| 12.1.2 Floating Roof Tanks _____ | 96 |
| 12.1.3 Spherical Tanks _____ | 98 |
| 12.1.4 Bullet Tanks _____ | 100 |
| 12.2 Process Vessels _____ | 102 |
| 12.2.1 Top Mounted - OPS Level Sensor _____ | 102 |
| 12.2.2 Chamber Mounted - OPS Level Sensor _____ | 105 |
| 12.2.3 Side Mounted - OPS Level Sensor _____ | 107 |
| 12.2.4 Separator Tank _____ | 108 |
| 12.2.5 Distillation Column _____ | 109 |
| 12.2.6 Boiler Drum _____ | 110 |
| 12.2.7 Reactor Tank _____ | 111 |



12. Overfill Prevention System Examples

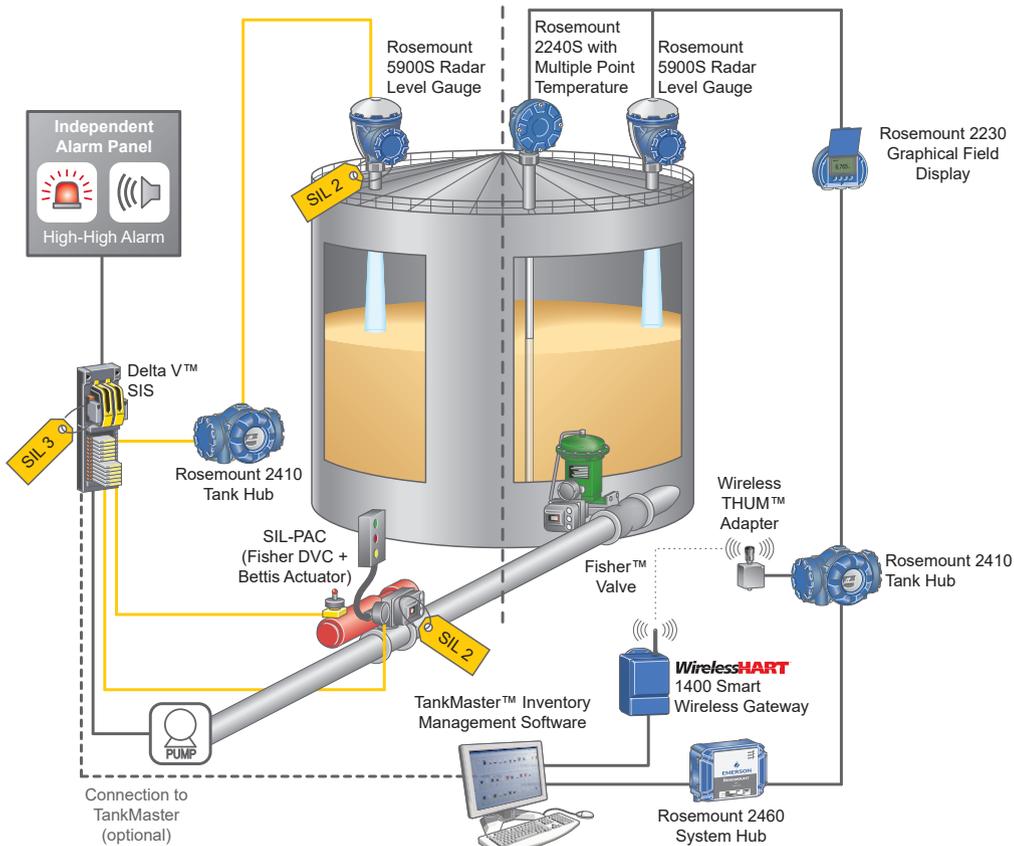
12.1 Bulk Liquid Storage

12.1.1 Fixed Roof Tanks

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

Automatic Overfill Prevention System (AOPS)

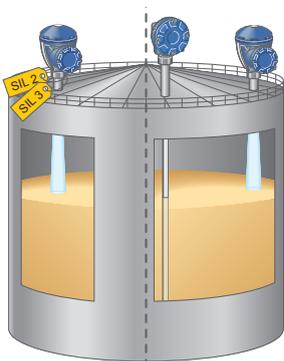
Automatic Tank Gauging (ATG)



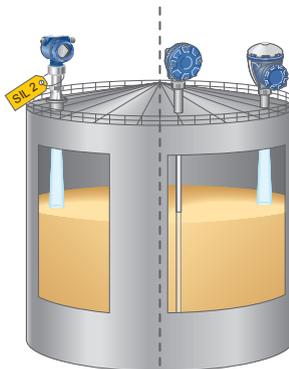
Includes Visual & Audible Level Alert High and Level Alarm High-High (optional)

12 - Overfill Prevention Systems Examples

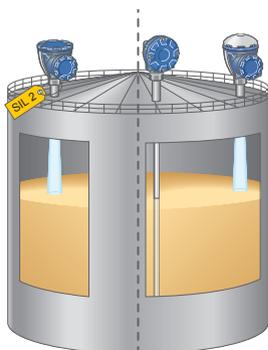
Below are alternatives of recommended Rosemount level sensors for fixed roof tanks:



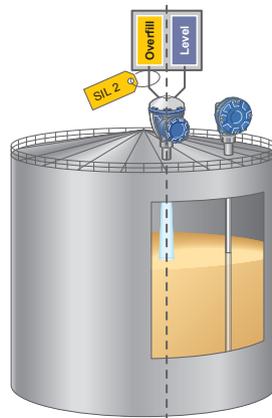
Rosemount 5900S (AOPS, MOPS) Rosemount 5900S



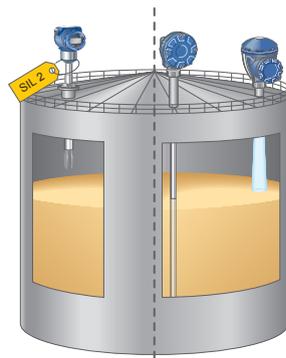
Rosemount 5408 (AOPS, MOPS) Rosemount 5900S



Rosemount 5900C (AOPS, MOPS) Rosemount 5900S



Rosemount 5900S 2-in-1 (AOPS)

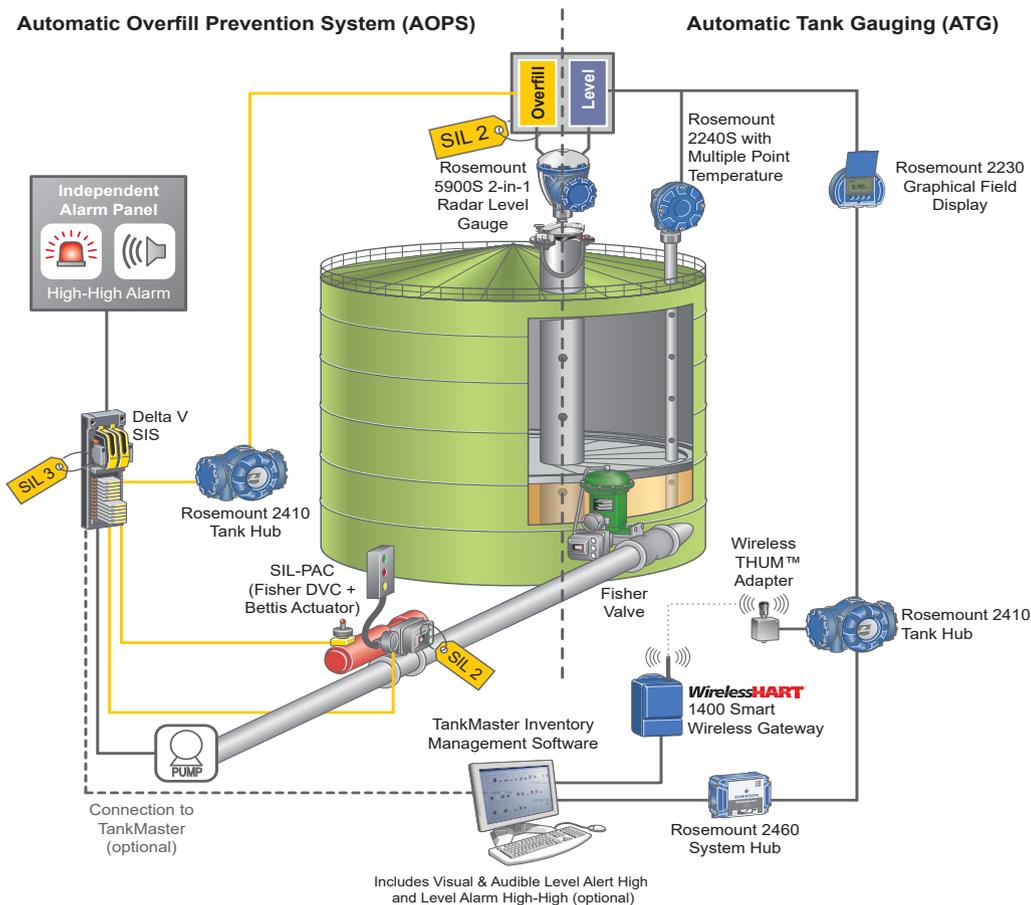


Rosemount 2140 (AOPS, MOPS) Rosemount 5900S

12 - Overfill Prevention Systems Examples

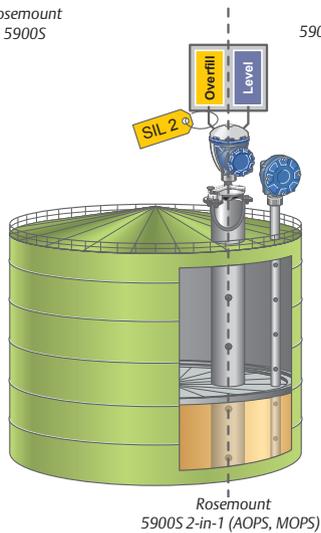
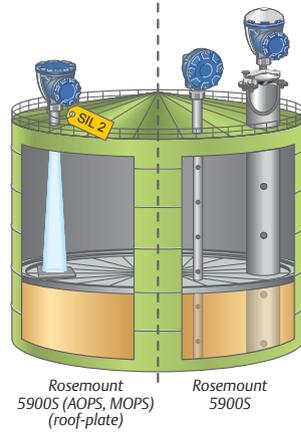
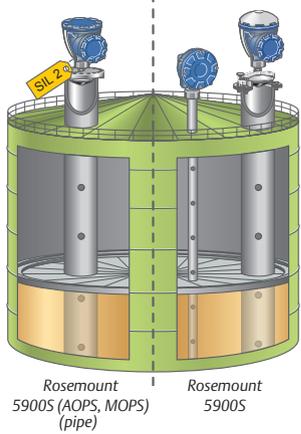
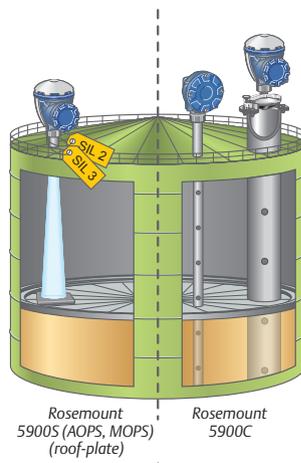
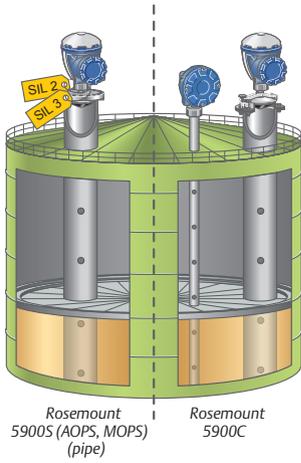
12.1.2 Floating Roof Tanks

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



12 - Overfill Prevention Systems Examples

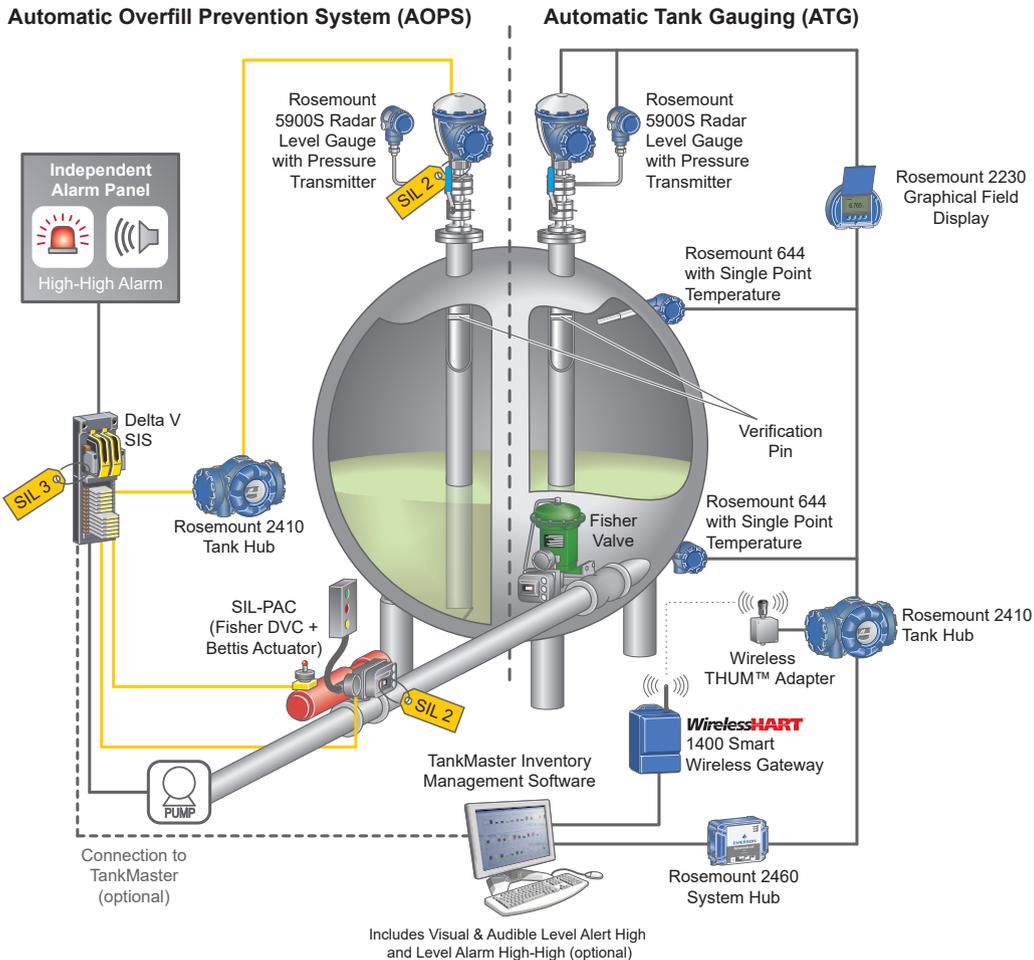
Below are alternative Rosemount level sensors for floating roof tanks:



12 - Overfill Prevention Systems Examples

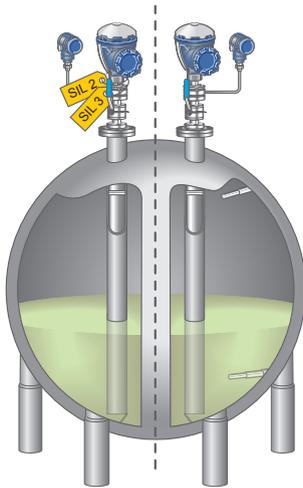
12.1.3 Spherical Tanks

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



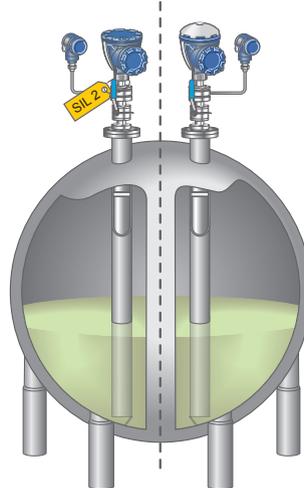
12 - Overfill Prevention Systems Examples

Below are alternative Rosemount level sensors for spherical tanks:



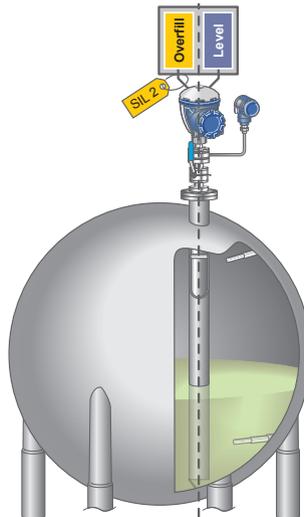
Rosemount
5900S (AOPS, MOPS)

Rosemount
5900S



Rosemount
5900S (AOPS, MOPS)

Rosemount
5900C



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

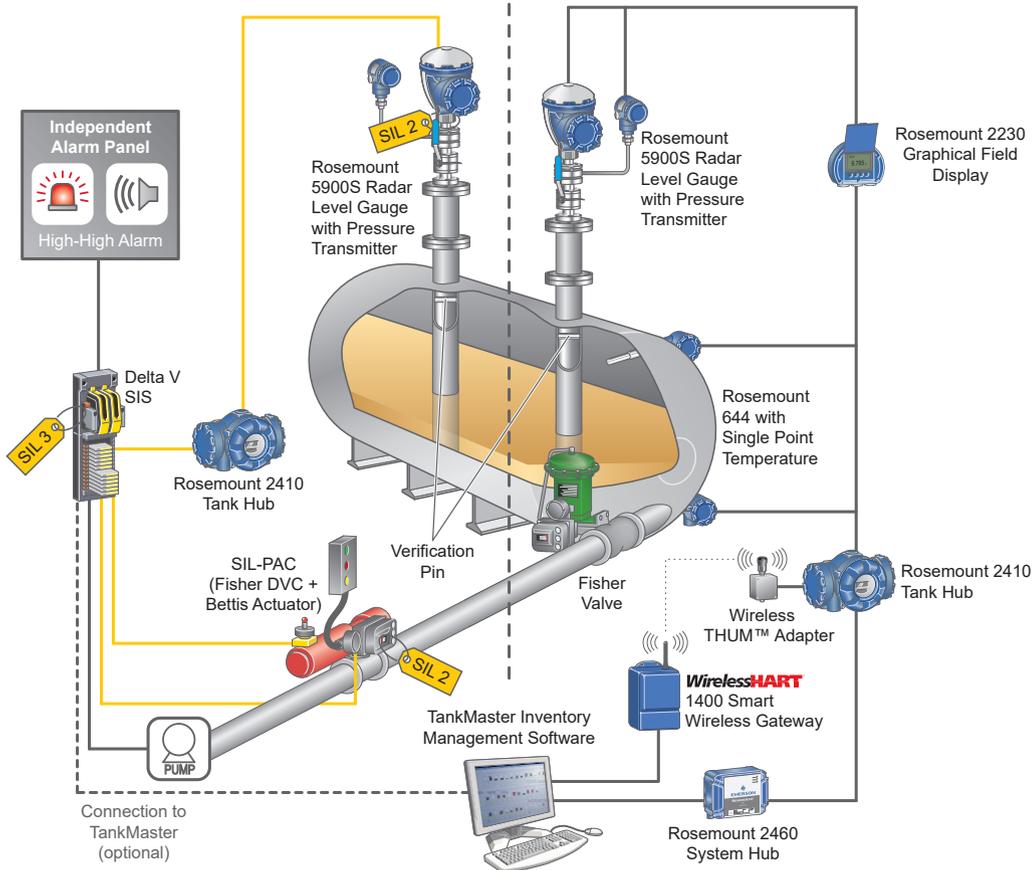
12 - Overfill Prevention Systems Examples

12.1.4 Bullet Tanks

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

Automatic Overfill Prevention System (AOPS)

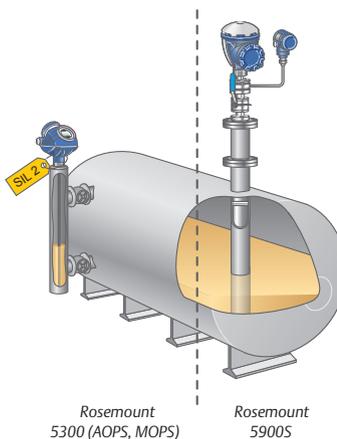
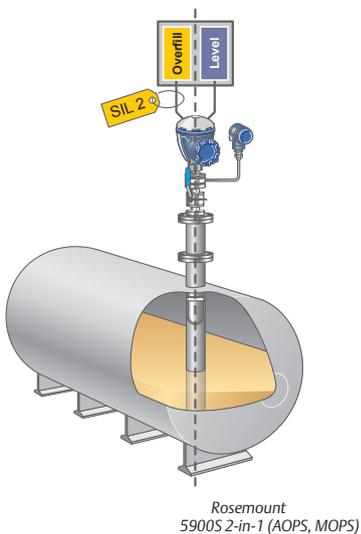
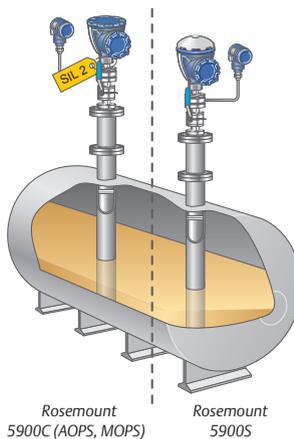
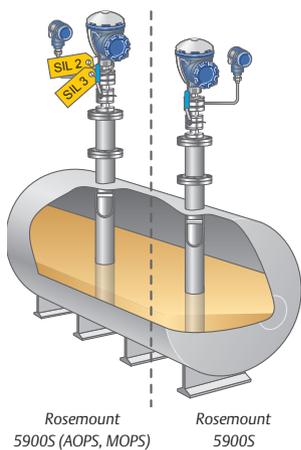
Automatic Tank Gauging (ATG)



Includes Visual & Audible Level Alert High and Level Alarm High-High (optional)

12 - Overfill Prevention Systems Examples

Below are alternative Rosemount level sensors for bullet tanks:

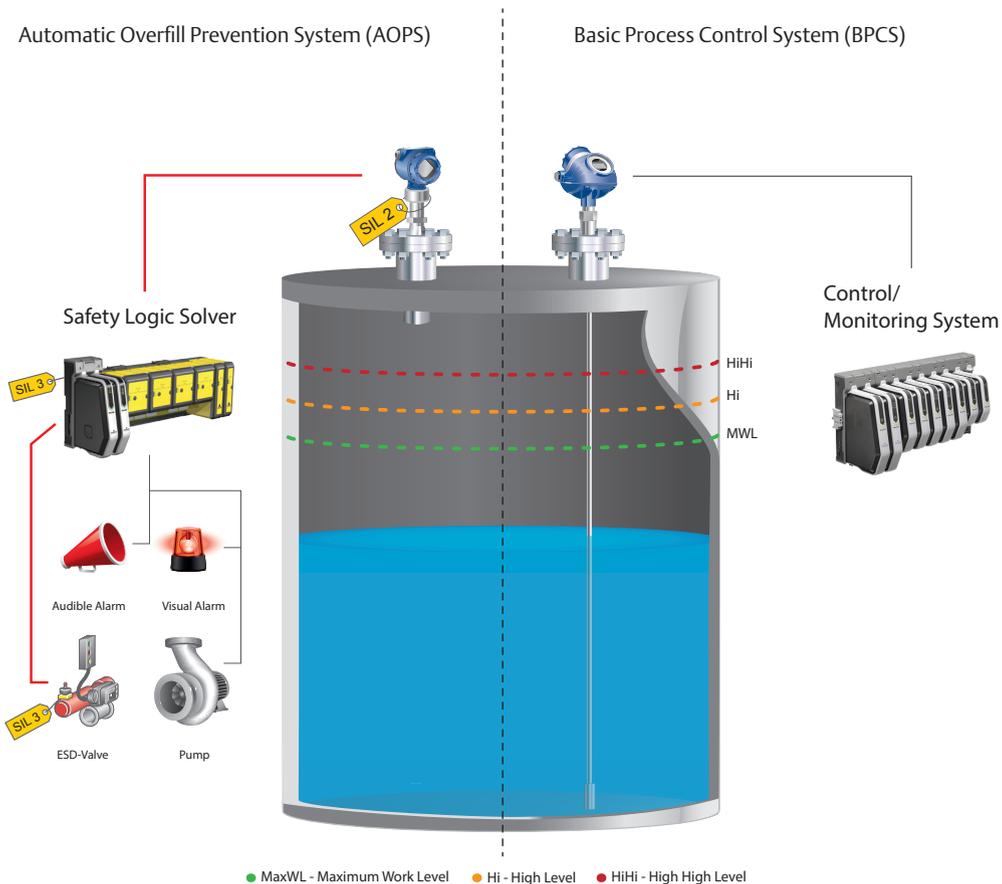


Additional bulk liquid storage tank examples is available in "The Complete Guide to API 2350" (Ref.No. 901030)

12.2 Process Vessels

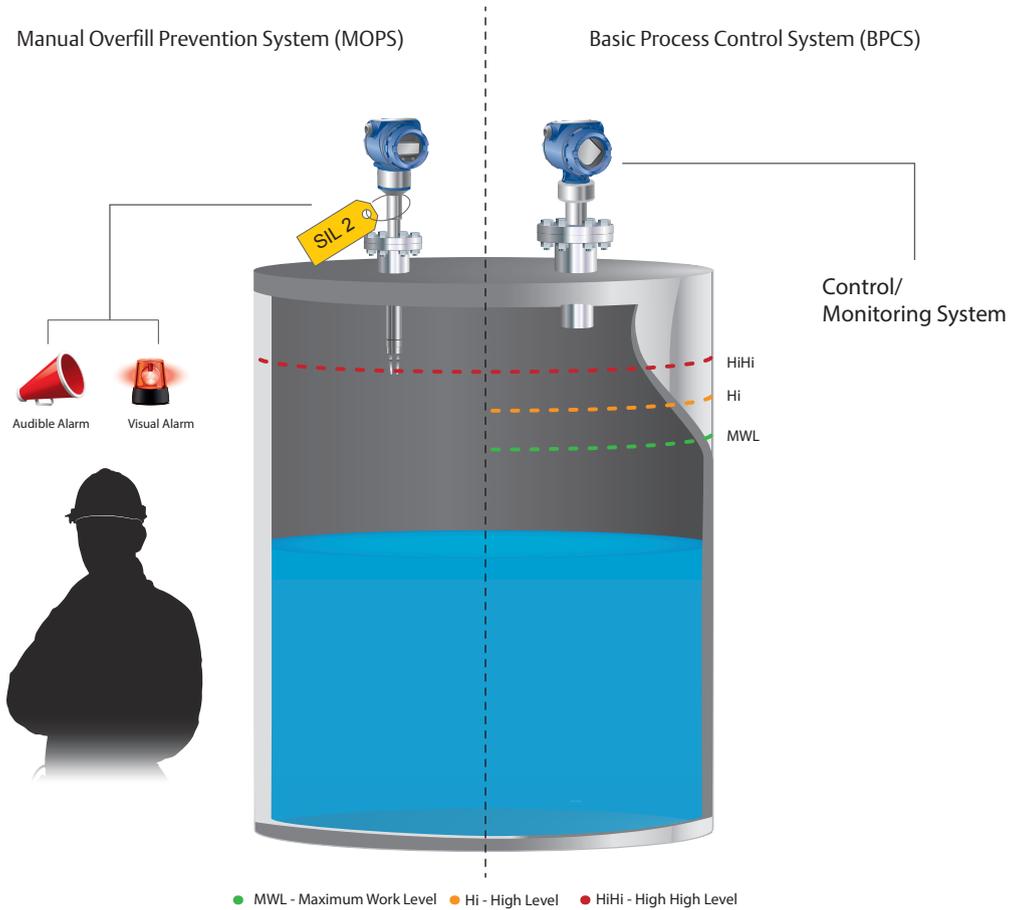
12.2.1 Top Mounted OPS Level Sensor

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



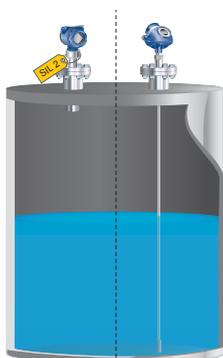
12 - Overfill Prevention Systems Examples

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

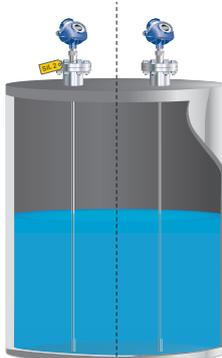


12 - Overfill Prevention Systems Examples

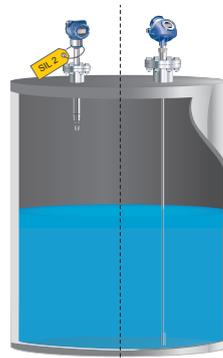
Below are alternative Rosemount level sensors top mounting:



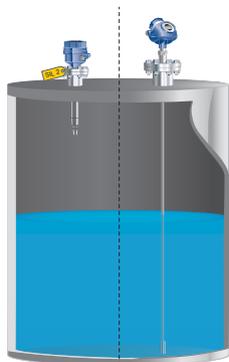
Rosemount 5408 SIS (AOPS) Rosemount 5300



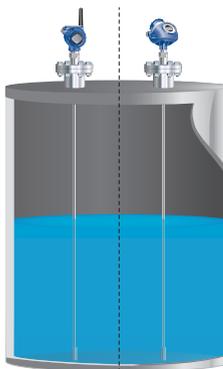
Rosemount 5300 (AOPS) Rosemount 5300



Rosemount 2140:SIS (AOPS) Rosemount 5300



Rosemount 2100 (AOPS) Rosemount 5300



Rosemount Wireless 3308 (MOPS) Rosemount 5300

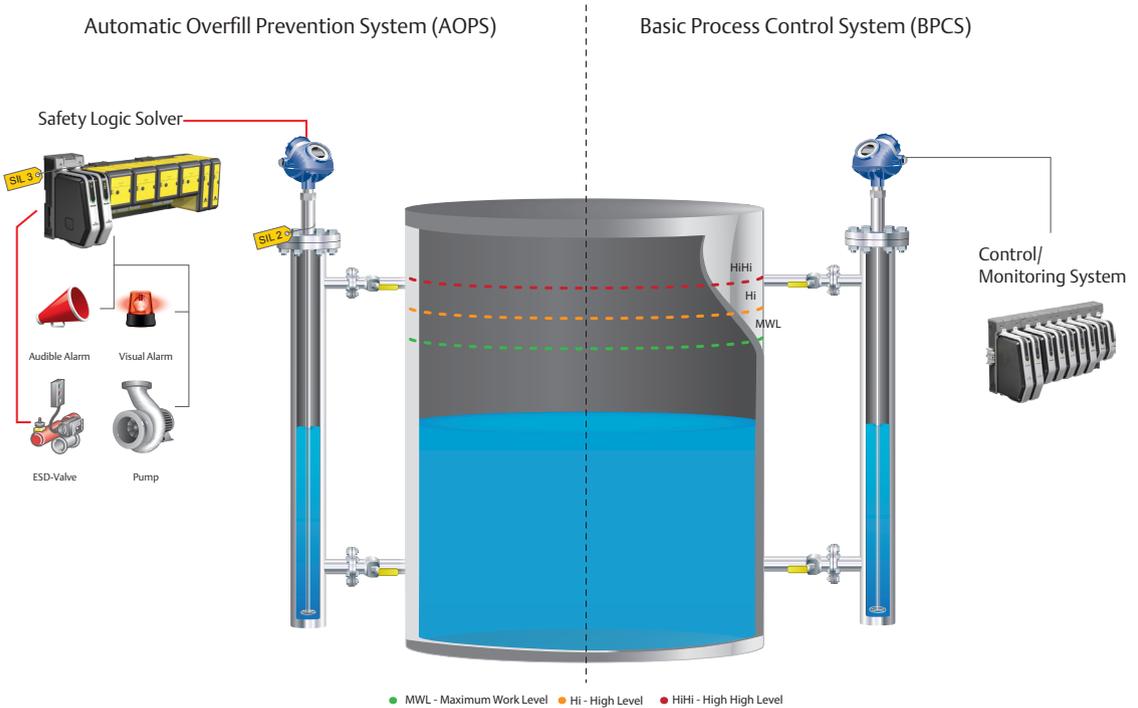


Rosemount Wireless 2160 (MOPS) Rosemount 5300

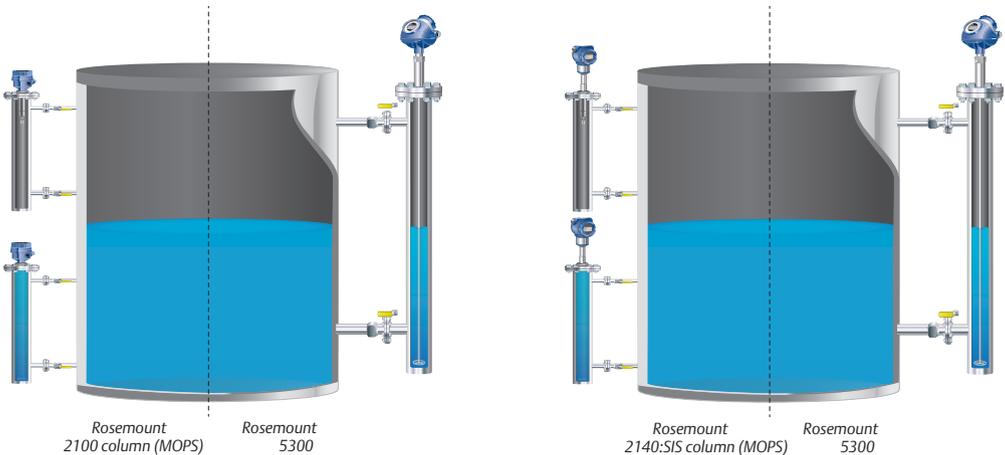
12 - Overfill Prevention Systems Examples

12.2.2 Chamber Mounted OPS Level Sensor

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

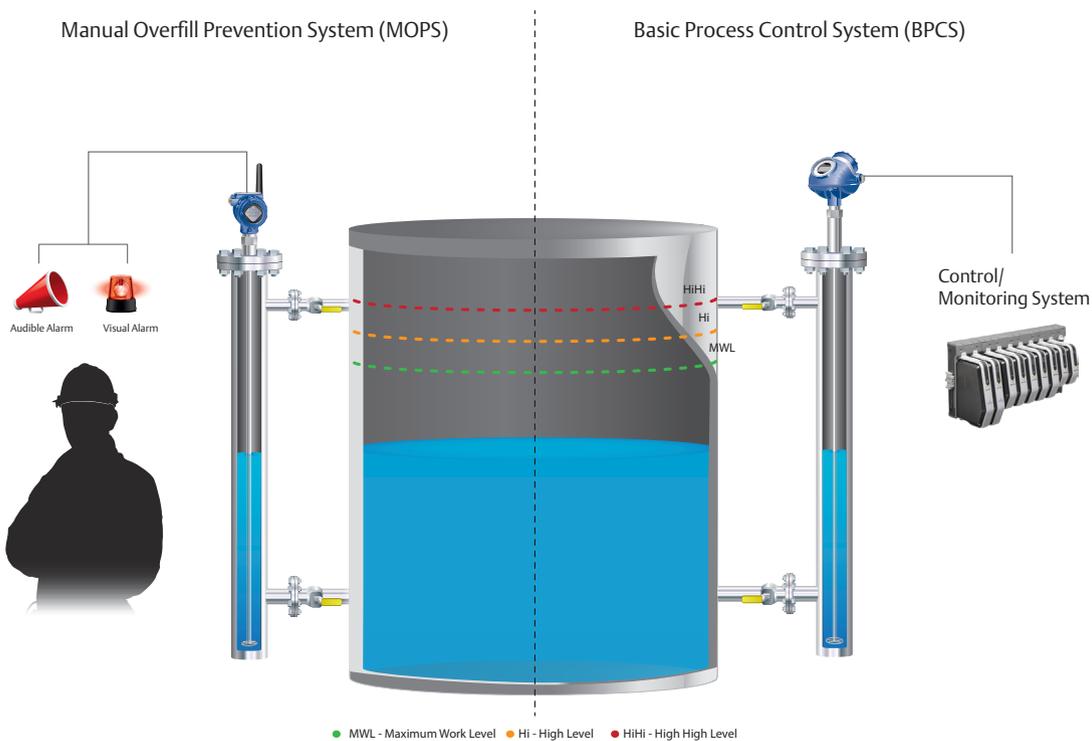


Below are alternative Rosemount level sensors for chamber installations:

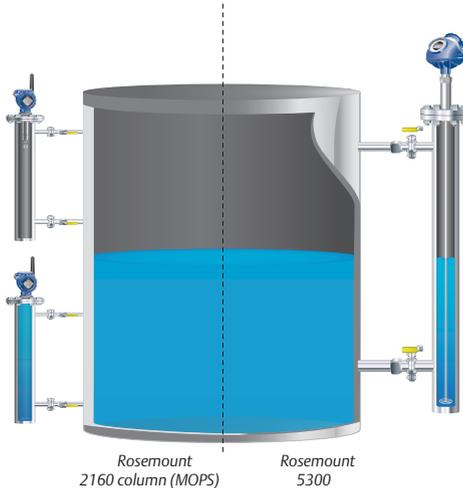


12 - Overfill Prevention Systems Examples

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



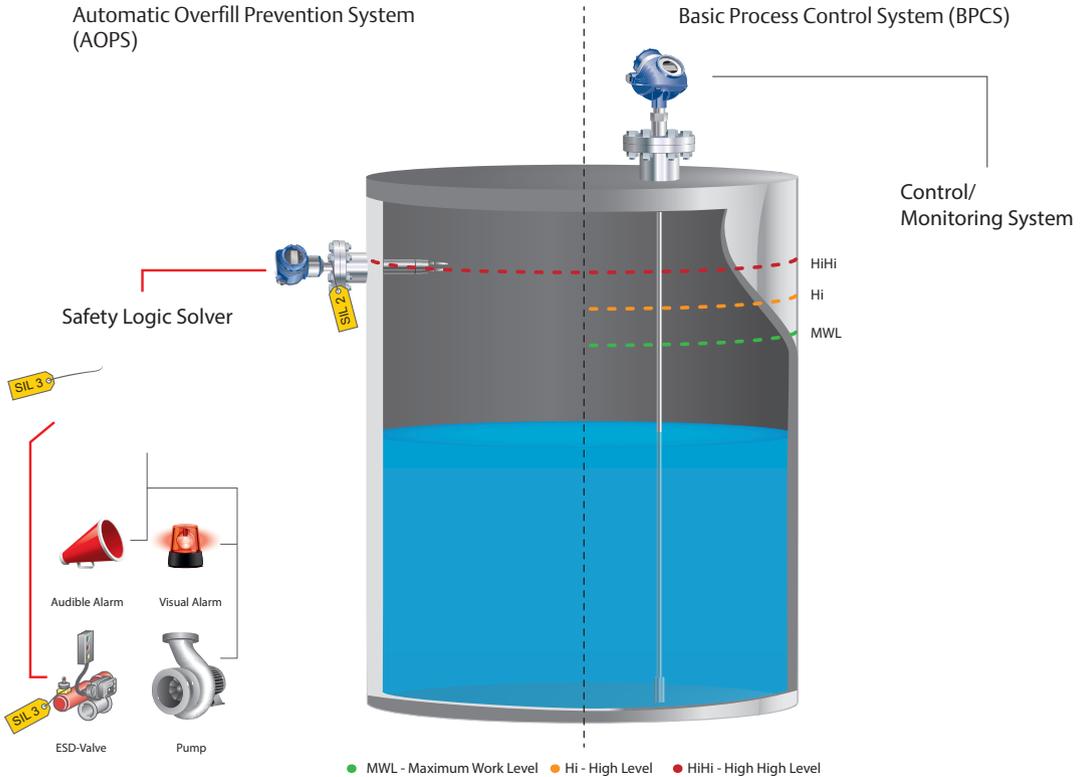
Below are alternative Rosemount level sensors for chamber installations:



12 - Overfill Prevention Systems Examples

12.2.3 Side Mounted OPS Level Sensor

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

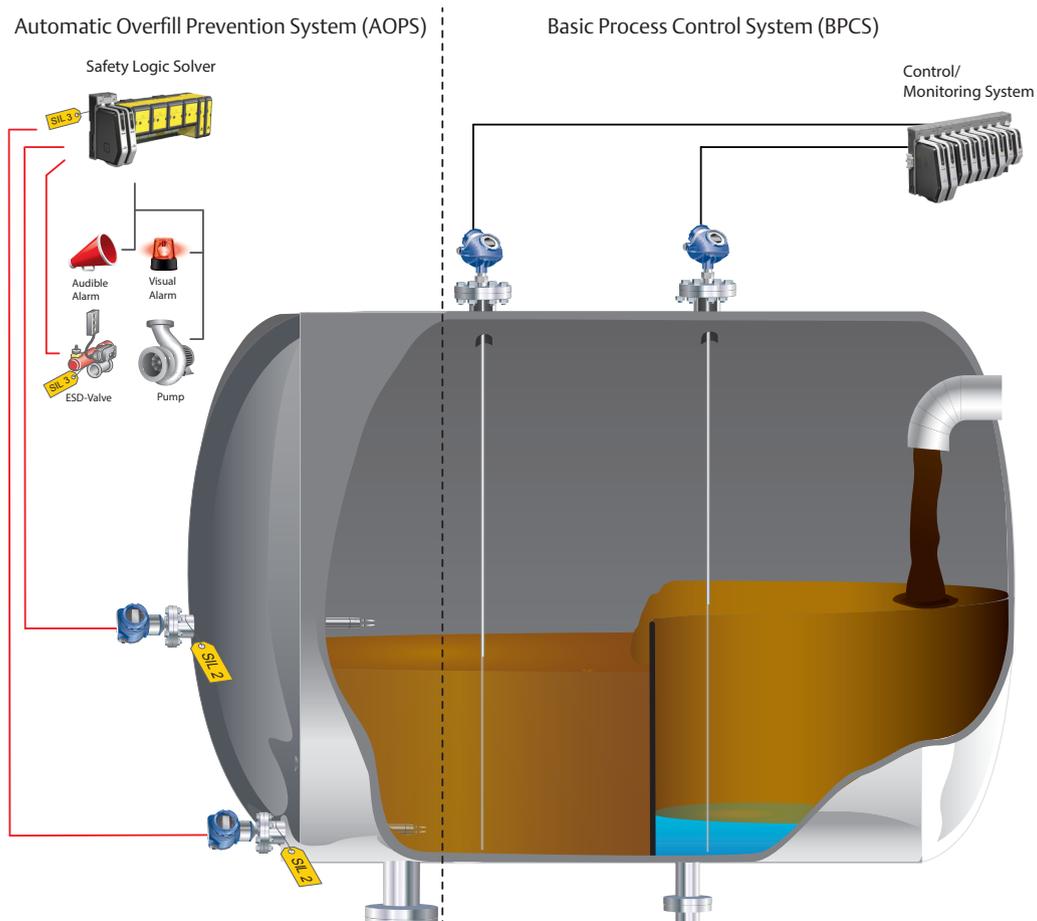


Below is an alternative Rosemount level sensor for side mounting:



12.2.4 Separator Tank

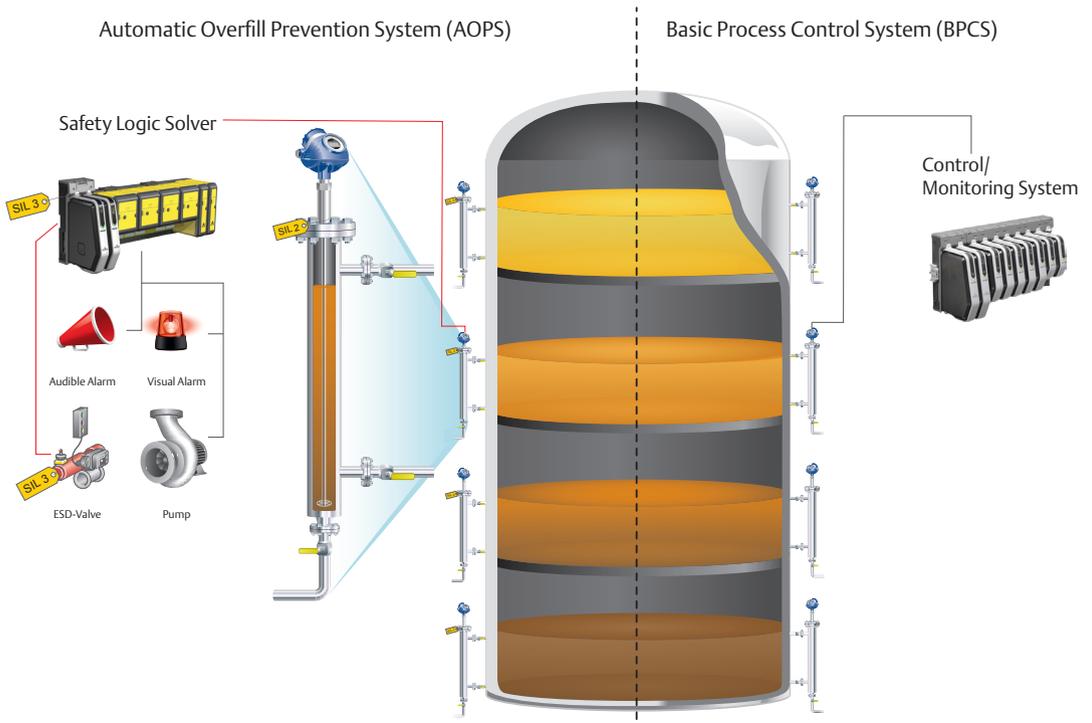
The separator tank is a vessel that allows fluids to separate into different components. Illustration shows a separator tank equipped BPCS with two Rosemount 5300 for level and interface measurement and SIL2 AOPS and SIL2 dry-run protection based on Rosemount 2100, DeltaV SIS and Bettis actuator.



12 - Overfill Prevention Systems Examples

12.2.5 Distillation Column

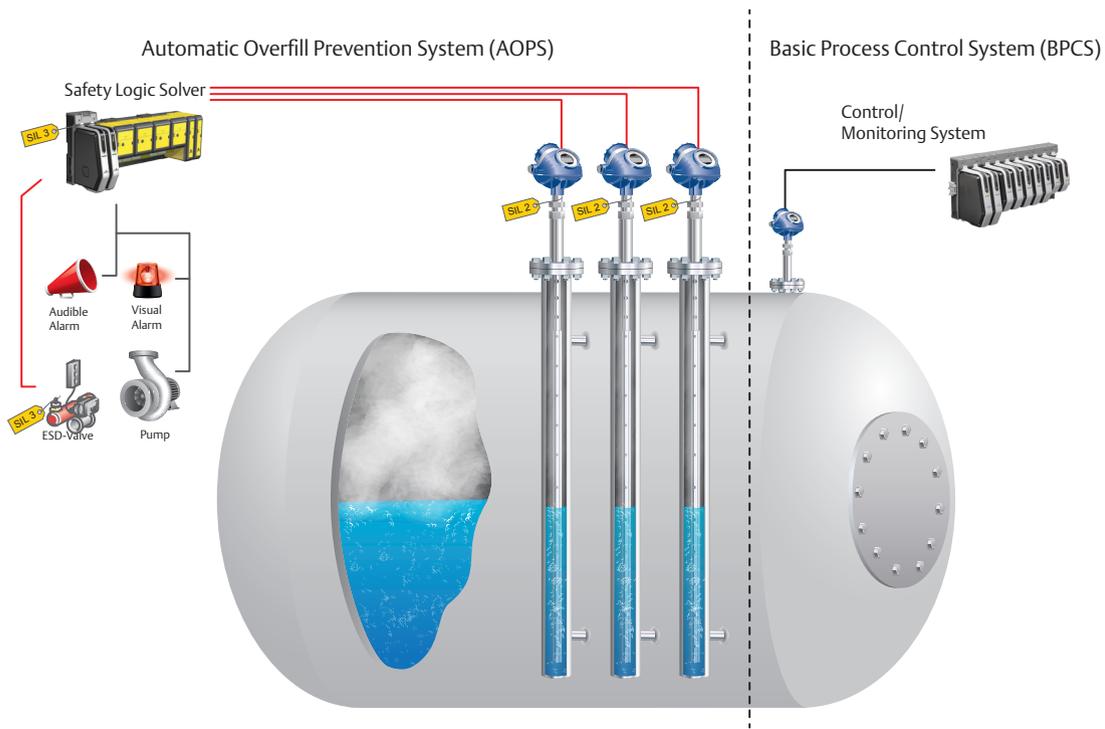
Distillation columns allow separation of fluid mixtures based upon their boiling points. As vapors rise through the column, different components will condense at different temperatures and accumulate for withdrawal. Illustration shows a distillation column equipped with a BPCS with a Rosemount 5300 for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



12 - Overfill Prevention Systems Examples

12.2.6 Boiler Drum

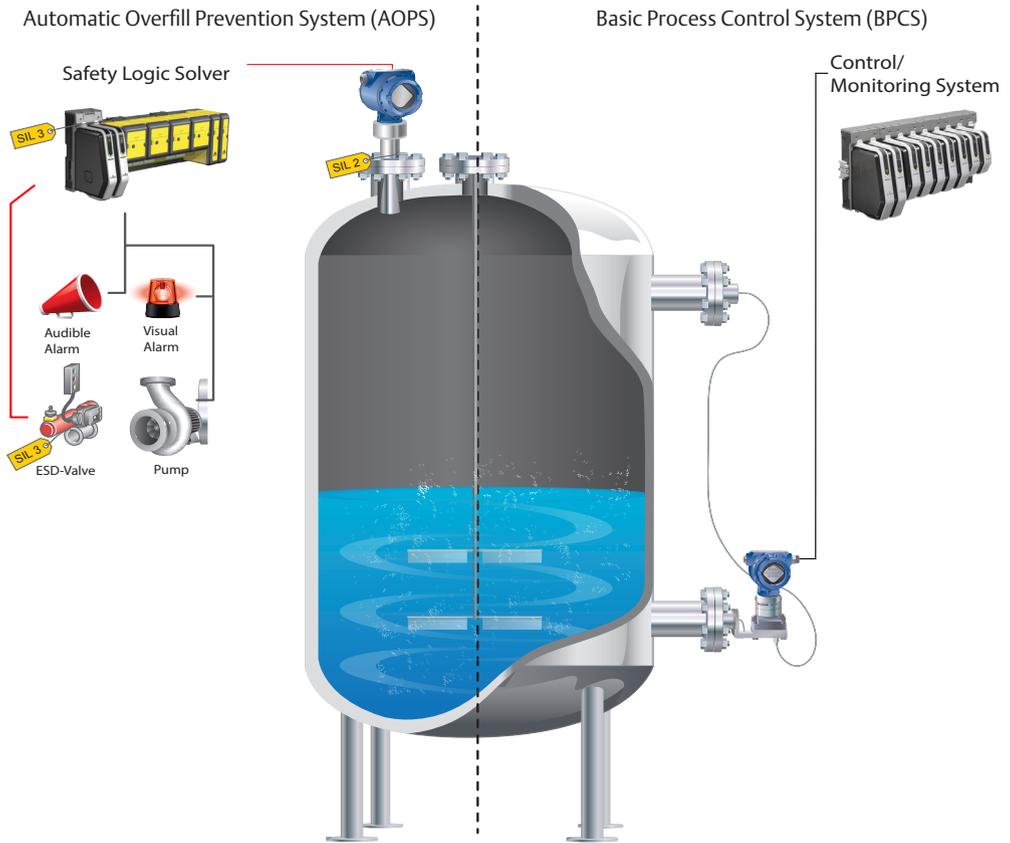
Illustration shows a boiler drum equipped with a BPCS with a Rosemount 5300 for level measurement and SIL3 AOPS based on three Rosemount 5300 (2oo3), DeltaV SIS and Bettis actuator.



12 - Overfill Prevention Systems Examples

12.2.7 Blending Tank

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



13

References

| Topic | Page |
|----------------------------|------|
| 13.1 Literature References | 114 |
| 13.2 Picture References | 114 |



13. References

13.1 Literature References

- American Petroleum Institute (2012) *API 2350. Overfill Protection for Storage Tanks in Petroleum Facilities*, Fourth edition
- Central Intelligence Agency (2015) *The World Factbook*, <https://www.cia.gov/library/publications/the-world-factbook/rankorder/2246rank.html> 2015-09-04
- Center for Chemical Process Safety (2007) *Guidelines for Risk Based Process Safety*, Wiley
- Control of Major Accident Hazards (2011) *Buncefield: Why did it happen?* <http://www.hse.gov.uk/comah/buncefield/buncefield-report.pdf> 2015-09-03
- Felten, D., (2015) *When Prevention Fails: Managing Your Spill Response*, NISTM 17th Annual International Aboveground Storage Tank Conference & Trade Show, Florida
- Goble, W., (2013) *Make the IEC 61511 into a cookbook?* <http://www.exida.com/Blog/Make-IEC-61511-into-a-Cookbook#sthash.oqiYamB1.dpuf> 2015-07-21
- International Electrotechnical Commission (2010) *IEC 61511 Functional safety - Safety instrumented systems for the process industry sector*
- International Electrotechnical Commission (2010) *IEC 61508 Functional Safety of Electrical/Electronic/Programmable Electronic Safety-related Systems*
- Loren (2005) *BP reveals costs of Texas City settlements*, <http://blog.chron.com/lorensteffy/2005/07/bp-reveals-costs-of-texas-city-settlements/> 15-07-17
- Marsh & McLennan Companies (2011) *Management of Atmospheric Storage Tank*, Rev 01, United Kingdom
- Mars (2007) *Recommendations on the design and operation of fuel storage sites*, Buncefield Major Incident Investigation Board
- M B Lal Committee Report (2009) *Independent Inquiry Committee Report on Indian Oil Terminal Fire at Jaipur* <http://oisd.gov.in/> 2015-09-04
- Puerto Rico Seismic Network (2009) *Informe Especial, Explosión de Caribbean Petroleum en Bayamón*, University of Puerto Rico Mayagüez Campus.
- Sreenevasan, R., (2015) *The effect of regulations in improving process safety*, Tetra Tech Proteus, https://www.engineersaustralia.org.au/sites/default/files/shado/Learned%20Groups/Technical%20Societies/Risk%20Engineering%20Society/australian_regulations_res_wa_paper.pdf 2015-07-21
- United States Environmental Protection Agency (2014) *Response to Oil Spills*, <http://www.epa.gov/ceppo/web/content/learning/response.htm> 2015-07-14
- U.S. Chemical Safety and Hazard Investigation Board (2015) FINAL INVESTIGATION REPORT CARIBBEAN PETROLEUM TANK TERMINAL EXPLOSION AND MULTIPLE TANK FIRES http://www.csb.gov/assets/1/16/06.09.2015_FINAL_CAPECO_Draft_Report__for_Board_Vote.pdf 2015-09-03

13.2 Picture references

In order of appearance:

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

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

13 - References

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

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

Picture 2.2: Copyright Emerson

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

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

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

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

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

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

Picture 3.1: Copyright Emerson

Picture 3.2: Copyright Emerson

Picture 3.3: Copyright Emerson

Picture 3.4: Copyright Emerson

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

About the authors



Author

Phil E. Myers

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



Author

AnnCharlott Enberg

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



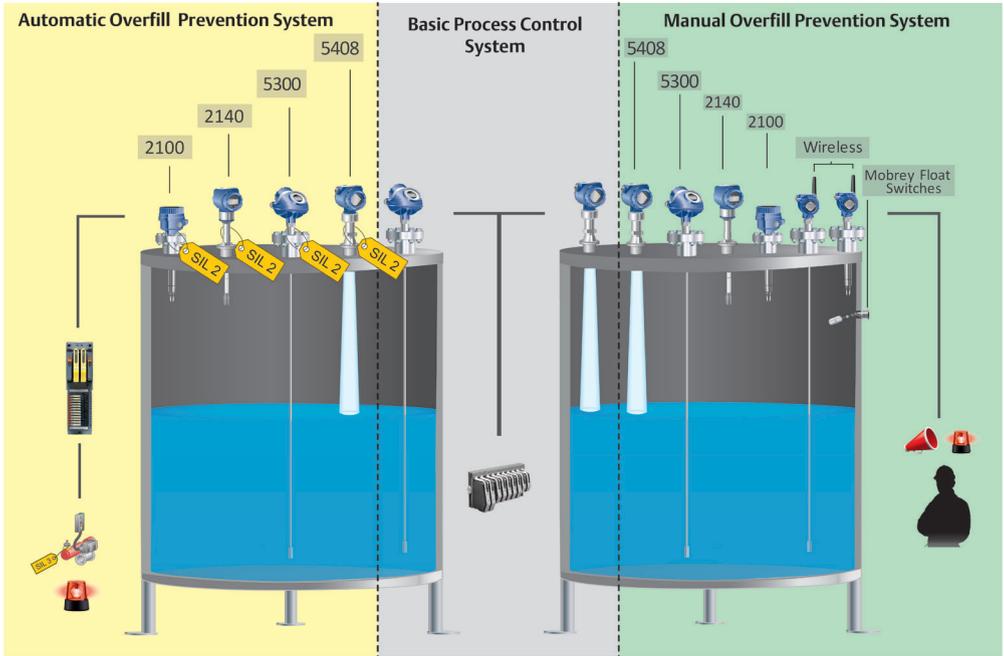
Author

Carl-Johan Roos

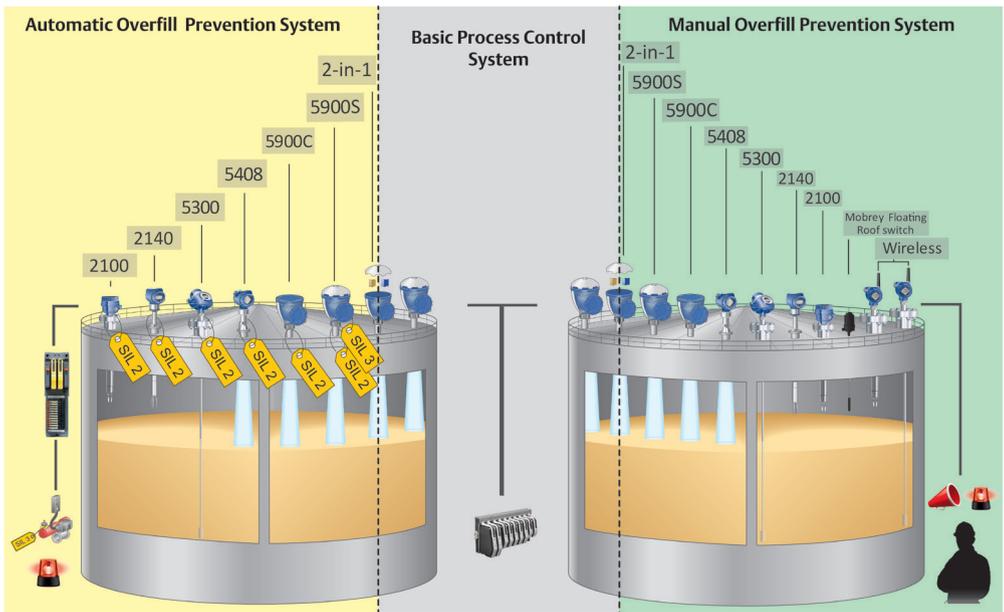
Carl-Johan "CJ" Roos was previously functional safety officer for Process Level and Tank Gauging at Emerson. Besides API2350, he has actively participated in numerous product specific IEC61508 certifications and site specific IEC61511 related projects. Roos has a Masters degree in Electrical and Computer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

Rosemount products for overfill prevention

Process Industry



Bulk Liquid Industry



Introduction

Why Invest?

Key Elements

Regulatory Requirements

Industry Standards

Risk Assessment

Overfill Management System

Overfill Prevention System

Proof-Testing

Available Technologies

Rosemount Products

**Overfill Prevention
System Examples**

References

Global capabilities

Global Headquarters

Emerson Automation Solutions

6021 Innovation Blvd.

Shakopee, MN 55379, USA

 +1 800 999 9307 or +1 952 906 8888

 +1 952 949 7001

 RFQ.RMD-RCC@Emerson.com

Europe Regional Office

Emerson Automation Solutions

Neuhofstrasse 19a P.O. Box 1046

CH 6340 Baar

Switzerland

 +41 (0) 41 768 6111

 +41 (0) 41 768 6300

 RFQ.RMD-RCC@Emerson.com

Asia Pacific Regional Office

Emerson Automation Solutions

1 Pandan Crescent

Singapore 128461

 +65 6777 8211

 +65 6777 0947

 Enquiries@AP.Emerson.com

Middle East and Africa Regional Office

Emerson Automation Solutions

Emerson FZE P.O. Box 17033,

Jebel Ali Free Zone - South 2

Dubai, United Arab Emirates

 +971 4 8118100

 +971 4 8865465

 RFQ.RMTMEA@Emerson.com

www.Emerson.com/OverfillPrevention

Recommended retail price \$75.99

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://www.twitter.com/Rosemount_News)

