

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



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)

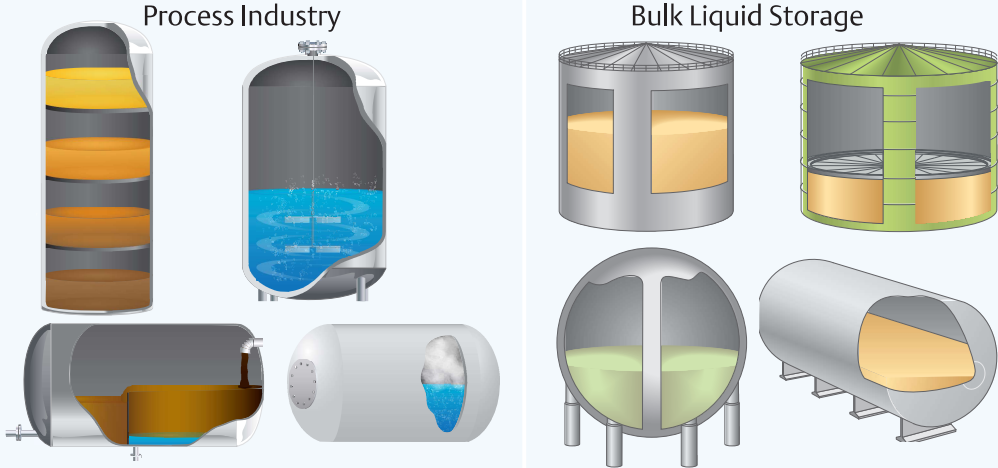
1 - Introduction

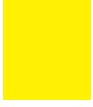
1.3 Scope

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.

Industry Overview	
Specific Industries	<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
Spill Causes	<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>
Tanks and Stored Products	<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>
Measurement Variables	<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 overfill prevention is good business because it not only reduces the statistically high risk of a tank overfill but also because it has an immediate positive financial impact.

Why invest in modern overfill 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 overfill, 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 overfill occurs statistically every 3,300 filling operations (Marsh and McLennan Companies, 2001). This equals one overfill 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 overfill equals one every year.

Historical industry data indicates:

One overfill 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 overfill if improper overfill 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 overfill 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 overfill prevention equipment can be examined.

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

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

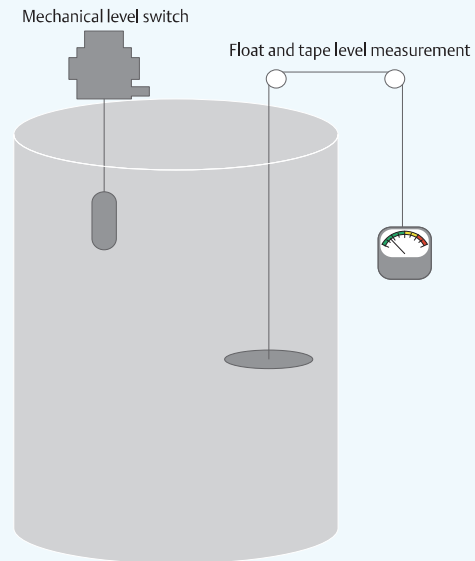


Figure 2.1: Generic tank example with a mechanical level transmitter and an independent switch

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 overfill will occur.

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

2.3 Consequence

Potential consequences of a tank overflow 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 overflow 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 overflow 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 overflow 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 overfill using specific case examples.

All the examples included relate to spills, but some of them are not a direct result of a tank overfill. However, these examples are included to show the potential consequences of a tank overfill; 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 overfill 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 overflow, 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 overflow 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 overflow 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 overflow 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

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

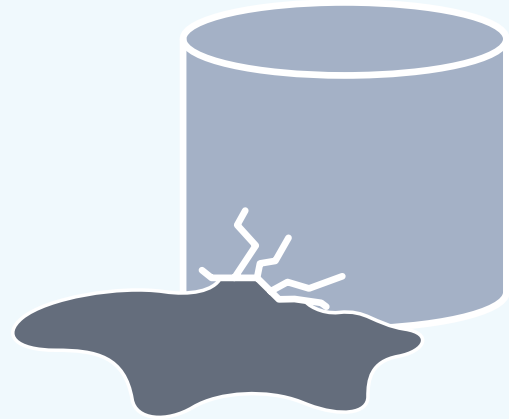
2.5 Additional Risks Associated with Tanks

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

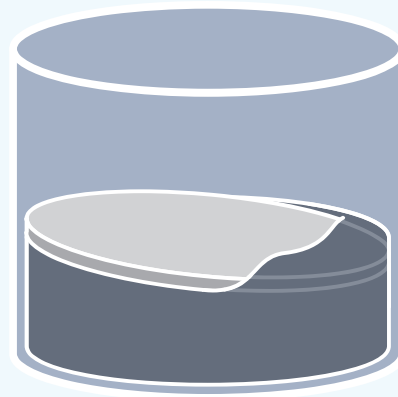
Low level in the tank can be a considerable risk in certain applications due to, for example, the potential for pumps running dry or heating coils or mixers being exposed.

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.

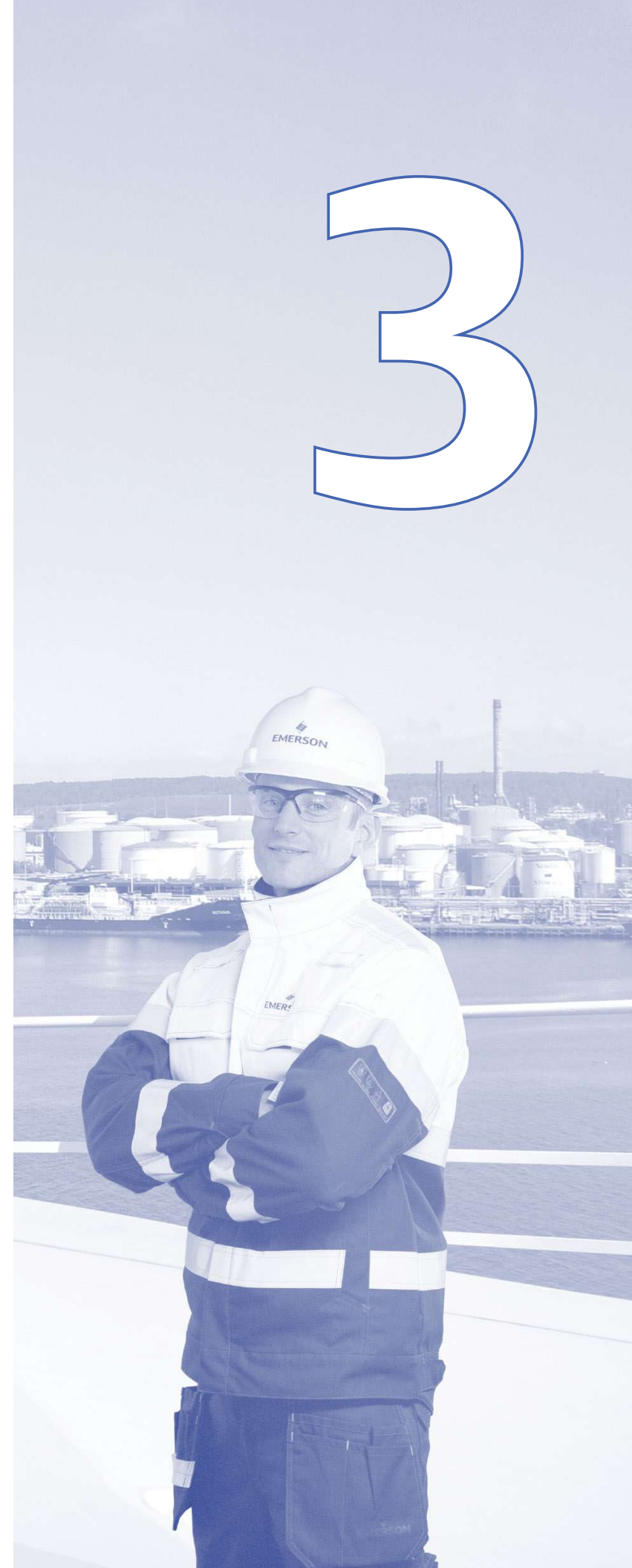
2.6.2.4 Maintenance

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.

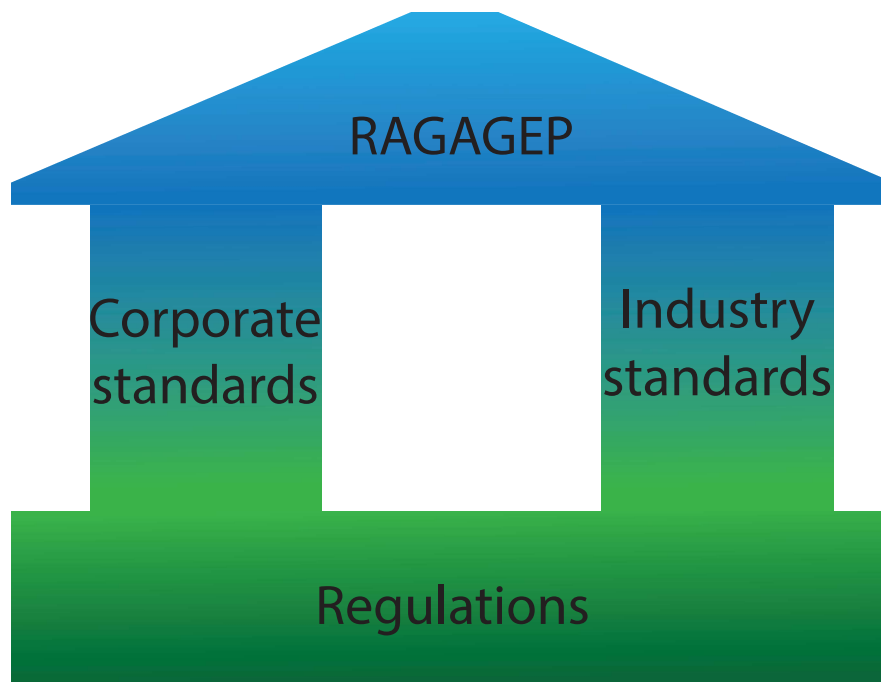


Figure 3.1: The origin, and priority, of internal and external overfill prevention requirements

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.

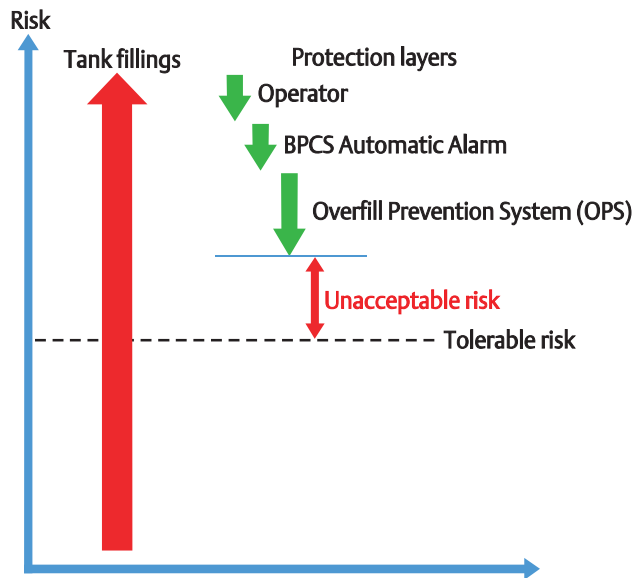


Figure 3.2: Basic concept of evaluating the assessed risk compared to the tolerable risk

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.

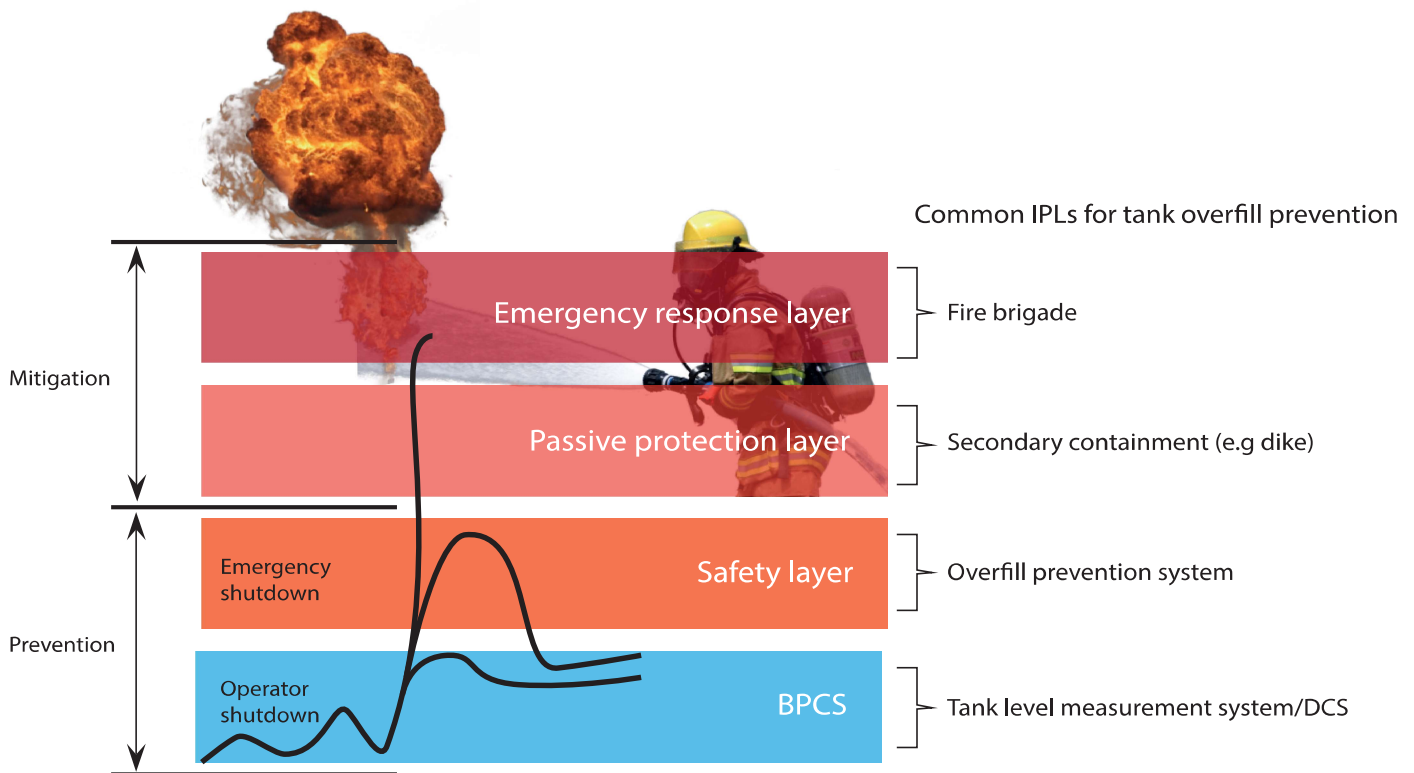


Figure 3.3: Commonly used independent protection layers (IPLs) to minimize the risk of tank overfills

3 - Key Elements

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

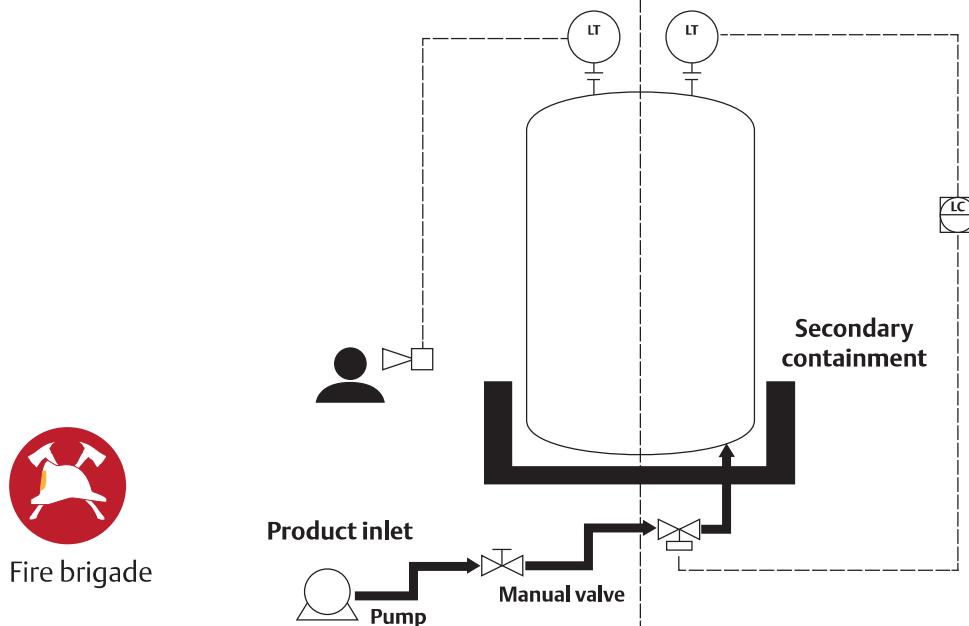


Figure 3.4: Generic tank example with the commonly used IPLs for tank overfill prevention and mitigation depicted

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)

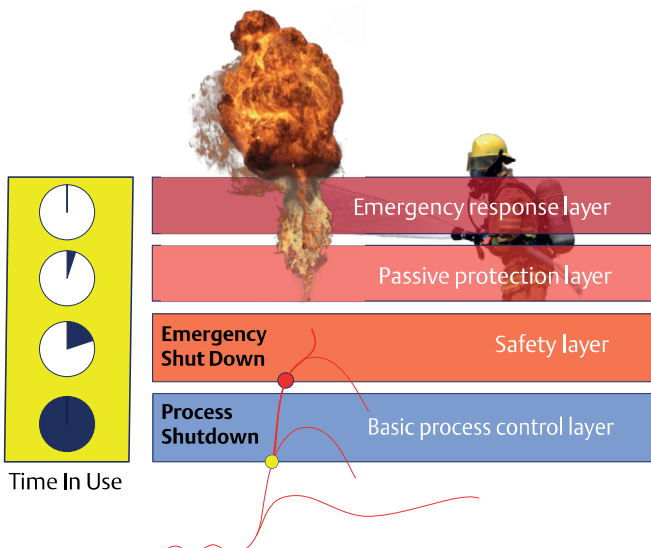


Figure 3.5: The BPCS layer is in use continuously and is the primary tool to prevent a tank overfill. The other IPLs are only activated upon failure of the subsequent IPL

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).

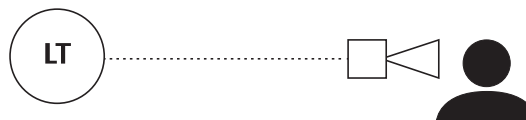


Figure 3.6: Manual overfill prevention systems (MOPSS) usually consist of a level transmitter (LT) connected to an audiovisual alarm that notifies an operator to take the appropriate action, e.g. closing a valve



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.

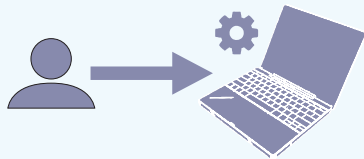


Figure 3.8: The trend is to replace manual activities with automatic control

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.

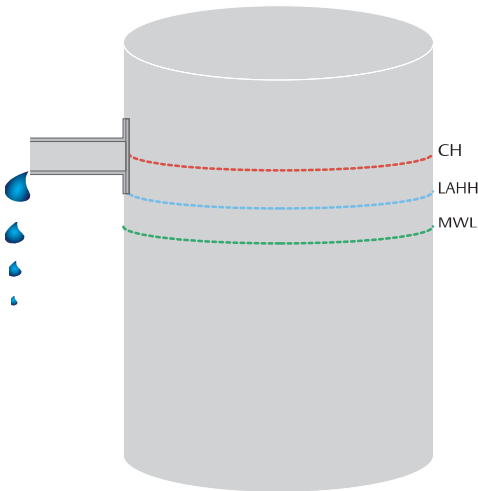


Figure 3.9: The Levels Of Concern (LOC) for tank overfill prevention

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 overfill 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 overfill 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.

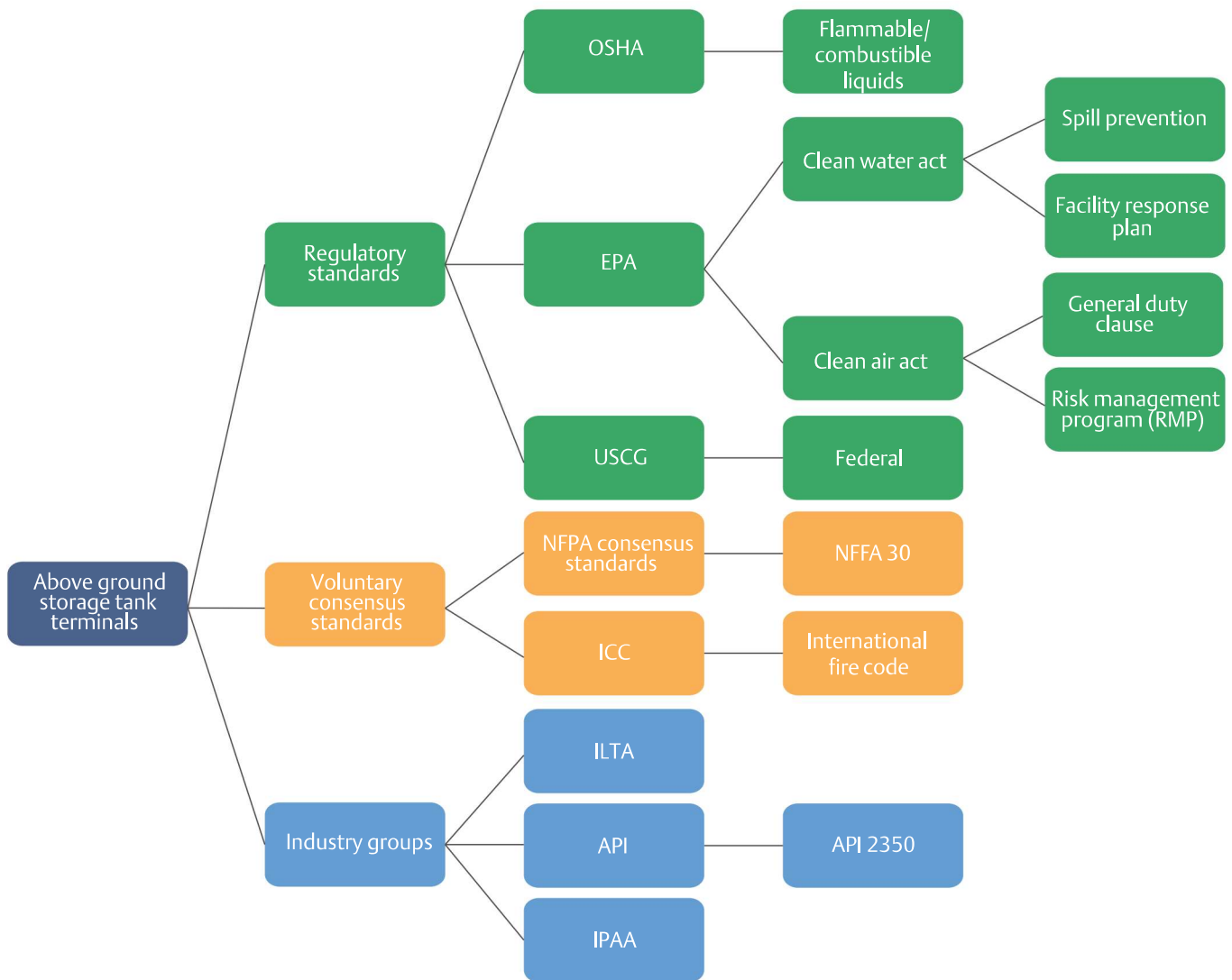


Figure 4.1: Example mapping conducted by the United States Chemical Safety Board in 2015 of external requirements relating to tank overfills for above ground storage tank terminals in the United States

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.

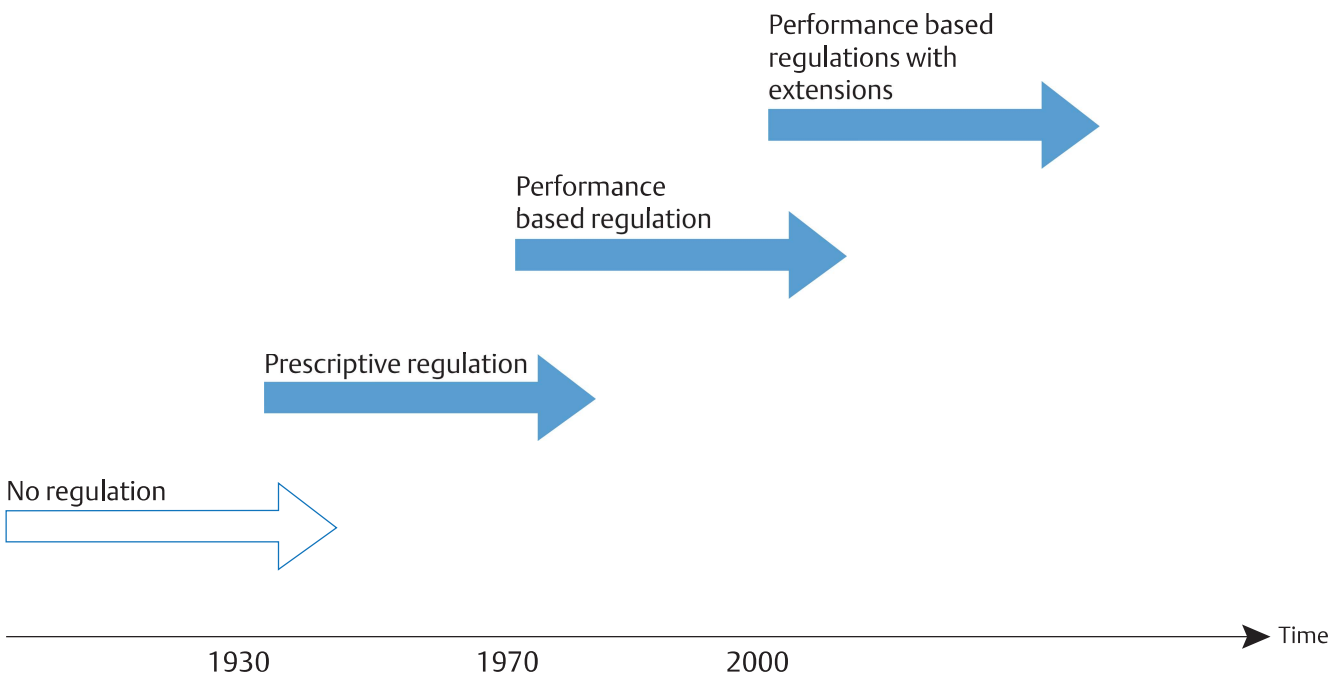


Figure 4.2: Developments of safety regulations in the industrialized world

4 - Regulatory Requirements

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.

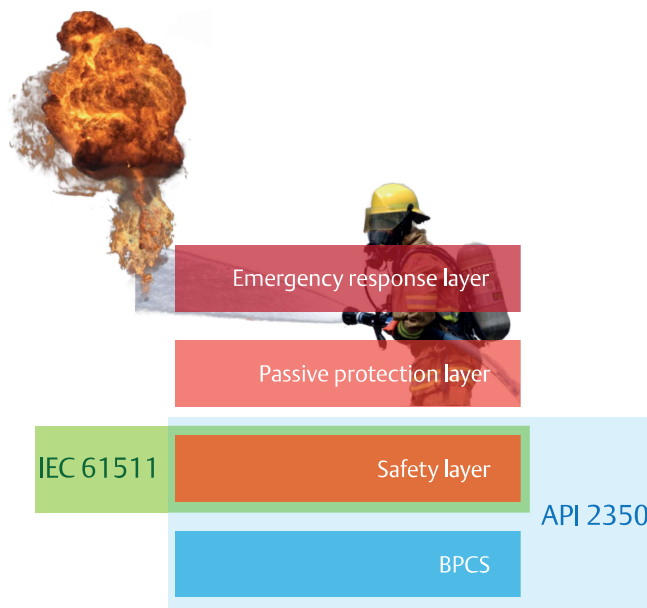


Figure 5.1: Industry standards IEC 61511 and API 2350 - comparison of intended scopes

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.

5 - Industry Standards

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 life-time 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

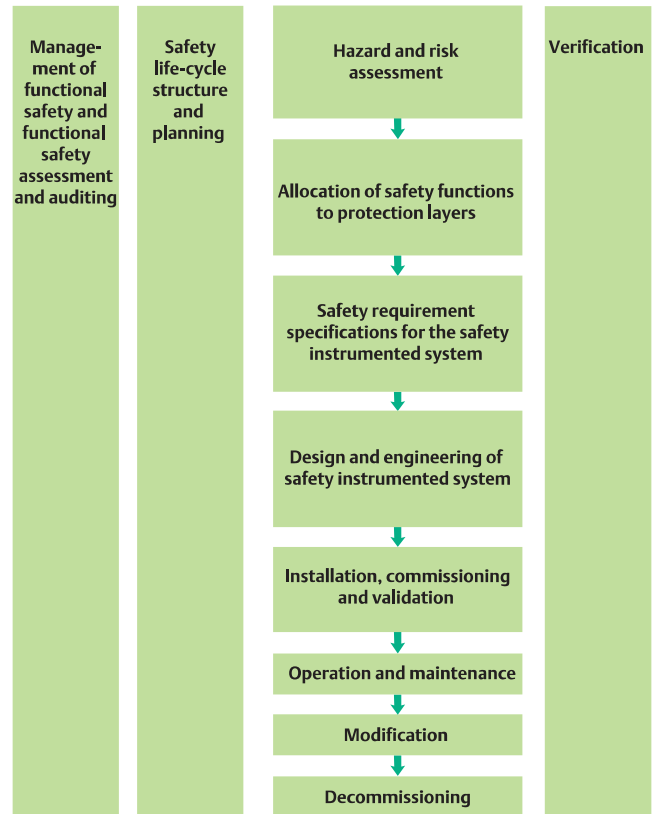


Figure 5.4: IEC 61511-1 safety life-cycle

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

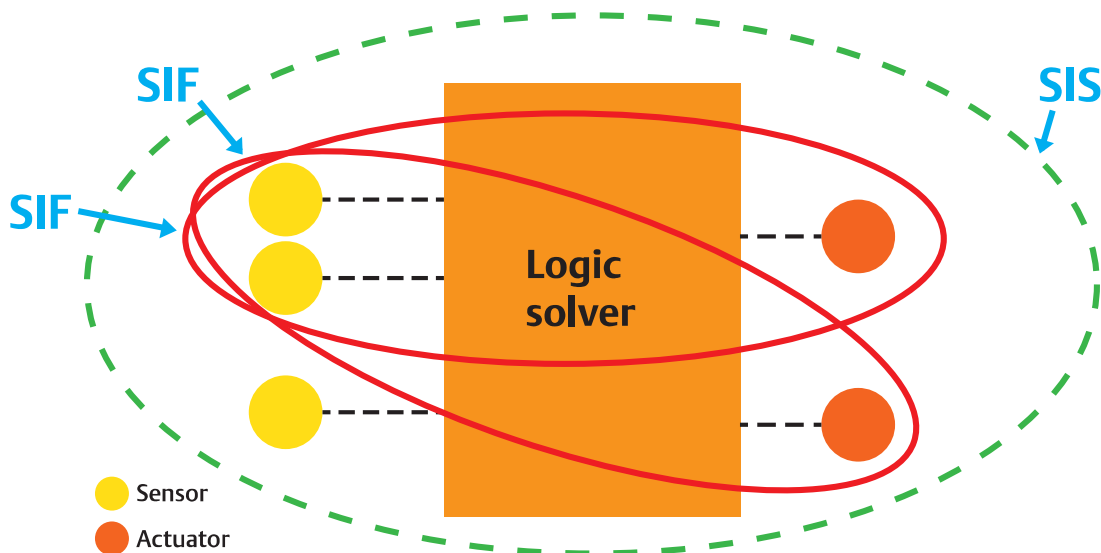


Figure 5.3: Principal overview safety instrumented function (SIF) an safety instrumented system (SIS)

- Management and planning
- Validation
- Verification

Every phase has a set of inputs and outputs, at the end of each phase a verification process shall be performed to confirm the required outputs are as planned.

Some of the benefits to implement correctly IEC 61511 standard are:

- Avoid SIF over-engineered / under-engineered
- Improved safety
- Reduce downtime
- Cost-effective systems and maintenance processes
- Compliance with safety authorities' regulations.

5.1.1.5 Equipment Selection

Obtaining a company certification under IEC 61508 and IEC 61511 demonstrates that your company has the capability to supply safety-related products and process that conform to the requirements of IEC 61508 and for the process industry IEC 61511.

The scope of the certification covers your management system for functional safety and the lifecycle activities that are appropriate to what you supply (for example, SIL determination, hardware/software development, product manufacture, systems integration, installation, operation and maintenance, etc). These aspects are often referred to as 'Functional Safety Capability in the certificate document'.

Certification is highly respected in the market and marks the company out as a serious supplier with the capability to ensure functional safety is achieved for every deliverable.

5.1.1.6 IEC 61508 and IEC 61511

The international standard IEC 61508 defines SIL using requirements grouped into two broad categories: hardware safety integrity and systematic safety integrity. A device or system must meet the requirements for both categories to achieve a given SIL.

The SIL requirements for hardware safety integrity are based on a probabilistic analysis of the device. To achieve a given SIL, the device must have less than the specified probability of dangerous failure and have greater than the specified safe failure

fraction. These failure probabilities are calculated by performing a Failure Modes and Effects Analysis (FMEA). The actual targets required vary depending on the likelihood of a demand, the complexity of the device(s), and types of redundancy used.

PFD (Probability of Failure on Demand) and RRF (Risk Reduction Factor) for SIL Levels as defined in risk assessment that follow the criteria from IEC 61508 and IEC 61511 for the industry.

5.1.2 IEC 61508 Certification

This International Standard covers those aspects to be considered when electrical/electronic/programmable electronic (E/E/PE) systems are used to carry out safety functions. A major objective of this standard is to facilitate the development of product and application sector international standards by the technical committees responsible for the product or application sector. This will allow all the relevant factors, associated with the product or application, to be fully taken into account and thereby meet the specific needs of users of the product and the application sector. A second objective of this standard is to enable the development of E/E/PE safety-related systems where product or application sector international standards do not exist.

Often, the conformance to IEC 61508 is audited by an independent third party. These assessors usually issue a compliance report and a certificate. The value of these certificates is dependent on the specific assessor. It is therefore important to ensure that the assessor adheres to the following minimum requirements:



Figure 5.5: Third party assessors generate certificates stating that the equipment conforms to IEC 61508

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.

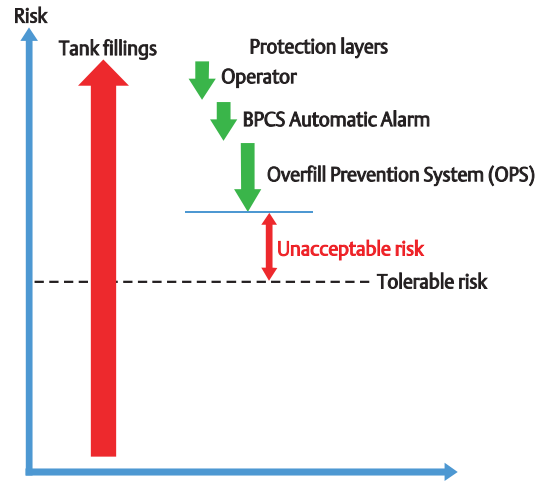


Figure 6.1: Basic concept of evaluating assessed risk compared to tolerable risk

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.

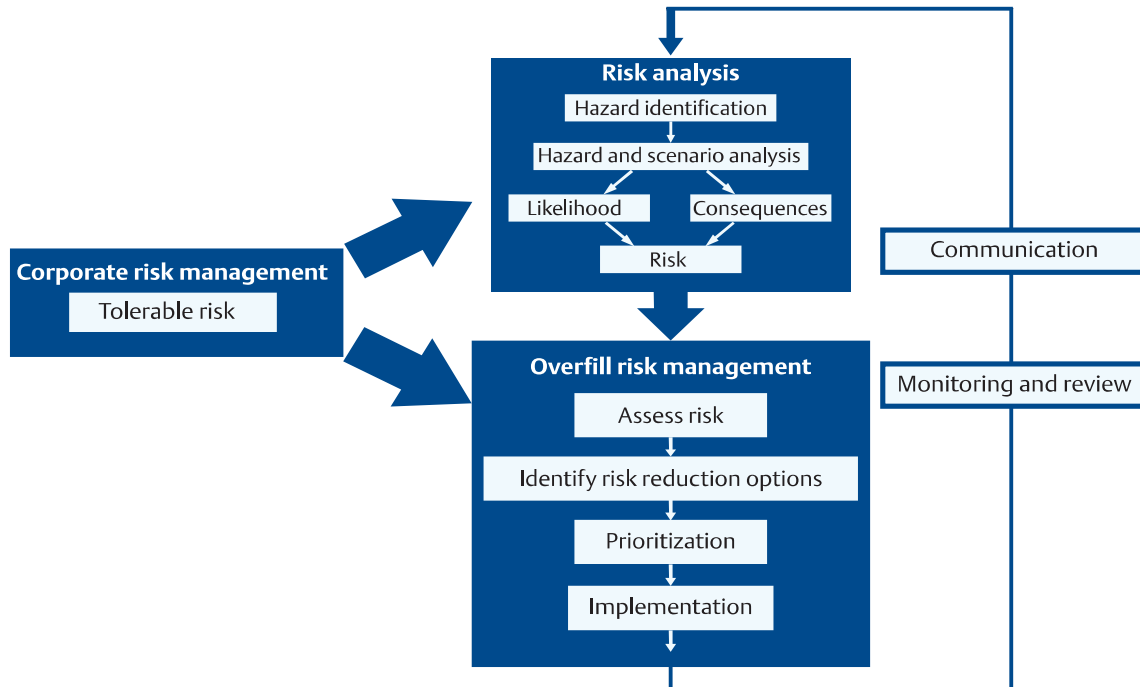


Figure 6.2: Basic risk assessment model for overfill prevention

6 - Risk Assessment

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.

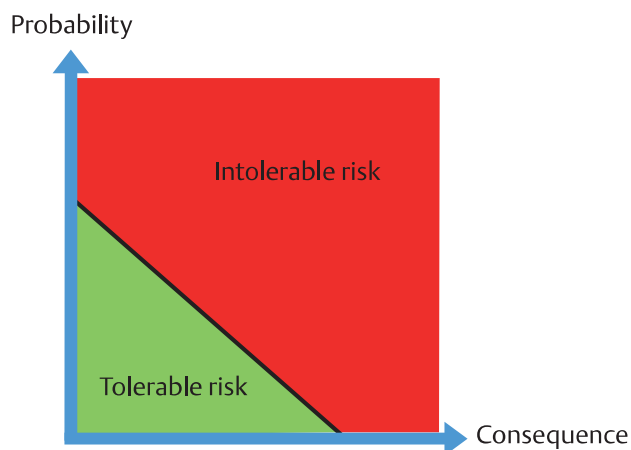


Figure 6.3: Simplified example with tolerable risk

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.

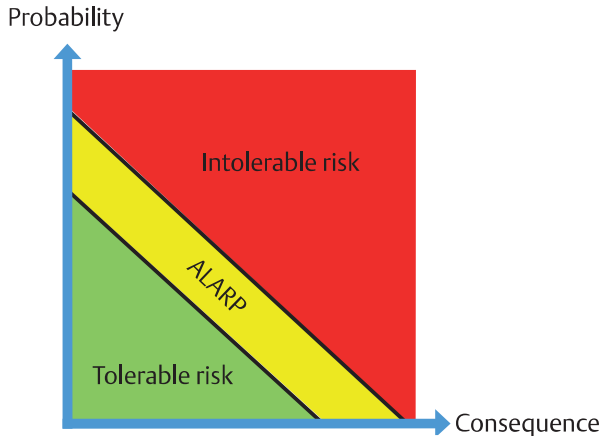


Figure 6.4: The principle of "as low as reasonably practicable" (ALARP)

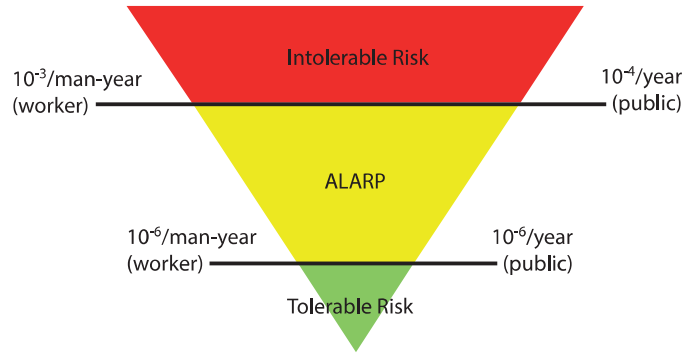


Figure 6.5: Typical depiction of tolerable risk levels as defined by the British Health and Safety Executive (HSE)

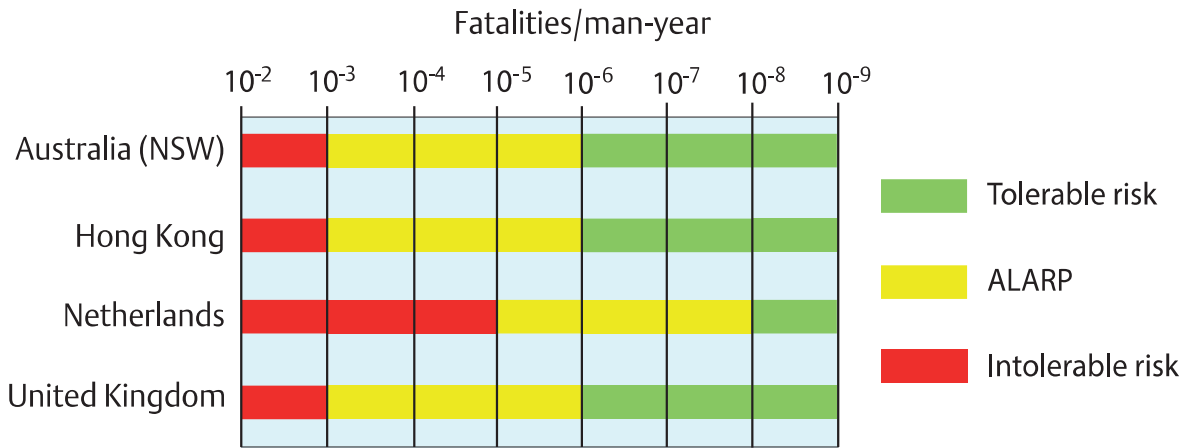


Figure 6.6: Comparison of tolerable risk levels for the consequence of fatalities

- Catastrophic ■ STOP
- Unacceptable ■ URGENT ACTION
- Undesirable ■ ACTION
- Acceptable ■ MONITOR
- Desirable ■ NO ACTION

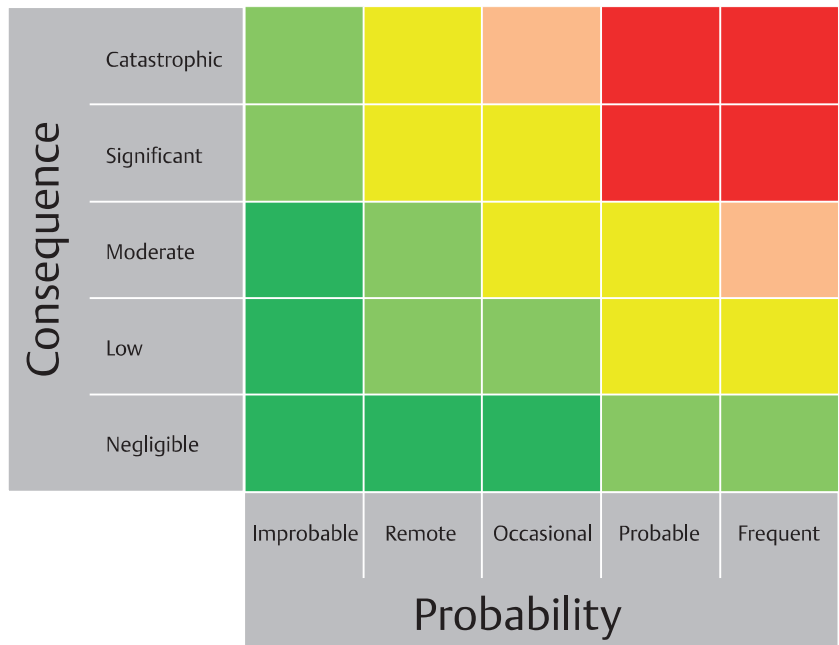


Figure 6.7: Example of qualitative corporate risk graph

6 - Risk Assessment

Health	Asset	Environment	Company image	>0.1/yr	<0.1/yr	<10 ⁻² /yr	<10 ⁻³ /yr	<10 ⁻⁴ /yr
				Likely	Probable	Occasional	Remote	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	
Major injury (<10 ⁻³ /yr)	Major damage (<\$500K)	Localized effect	Considerable impact	SIL 3	SIL 2	SIL 1		OK
Minor injury (<10 ⁻² /yr)	Minor damage (<\$100K)	Minor effect	Minor impact	SIL 2	SIL 1		OK	OK
Slight injury (<0.1/yr)	Slight damage (<\$10K)	Slight effect	Slight impact	SIL 1		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%.

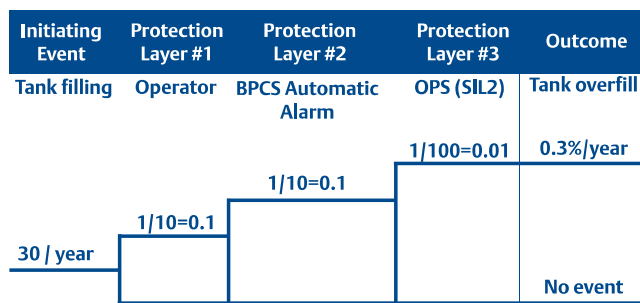


Figure 6.9: Example probability estimation of tank overfills using an event-tree analysis

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

6 - Risk Assessment

- 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.

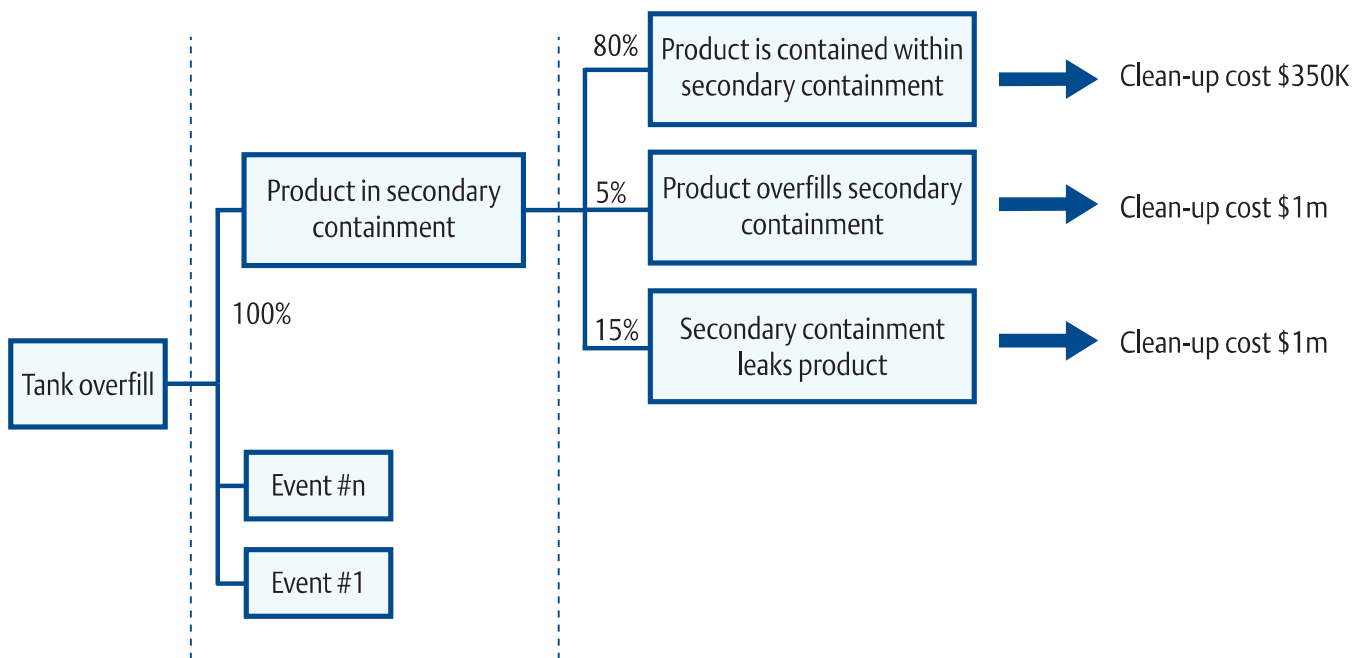


Figure 6.10: Parts of a simplified example consequence analysis of a tank overflow

6.3.2 Identify Risk Reduction Options

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

- Inherent process design change
- Changes in the Overflow 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 overflow.

6.3.2.2 Probability Reduction

Protection layers such as the BPCS and overflow prevention system are designed to reduce the probability of a tank overflow 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 overflow, the most commonly selected risk reduction option is an overflow prevention system (OPS) because it:

- Prevents (rather than mitigates) the risk of tank overflow
- 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 overflow 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

Overfill 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

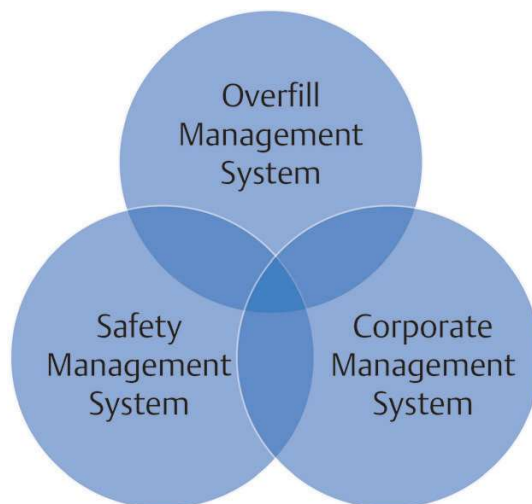


Figure 7.1: Venn diagram perspective showing how OMS relates to other corporate management systems

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.

