

Guidebook for Overfill Prevention & Tank Gauging

ABSTRACT

The public, the regulatory community and industry have expectations that tank overfills should be addressed proactively and in accordance with the current edition of API 2350. We aim to provide you with the knowledge and expertise to address the concern for hazardous liquid overfill unique to your facility, goals, and corporate interests.



Authors: PEMY Consulting and Endress+Hauser Experts
Philip Myers, Brock Trotter, Dean Mallon, Hai-Thuy Ngo
and Markus Wohlgemuth

Endress+Hauser 
People for Process Automation

Disclaimer

Whilst every effort has been made to ensure the accuracy of the information contained in this guidebook, Endress+Hauser will not warrant its accuracy or will, regardless of its negligence, assume liability for any foreseeable or unforeseeable use made thereof, which liability is hereby excluded. Consequently, such use is at the recipient's own risk on the basis that any use by the recipient constitutes agreement to the terms of this disclaimer. The recipient is obliged to inform any subsequent recipient of such terms.

This publication is made available for information purposes and solely for the private use of the user. Endress+Hauser will not directly or indirectly endorse, approve, or accredit the content of any course, event or otherwise where this publication will be reproduced.

Copyright notice

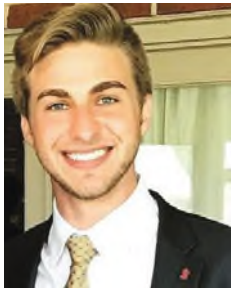
The contents of these pages are © Endress+Hauser.

No part of this work may be reproduced, translated, stored in a retrieval system, or transmitted by any means, electronic, mechanical, photocopying, recording, or otherwise, without prior written permission from the publisher. Contact the Publisher, Endress+Hauser AG, Kägenstrasse 2, 4153 Reinach BL, Switzerland, 2018

PEMY Biographies



Philip Myers has broad experience in the chemical, petrochemical, refining experience and has worked in these facilities in various roles for over 35 years. Of particular relevance, Philip Myers worked with the American Petroleum Institute developing the original 'Large Diameter Tank Fire Studies' as well as other groups such as the 'Last Fire' initiative sponsored by the major oil companies such as Exxon, Chevron, and BP. Philip Myers was the founder of the group at Chevron Engineering Research and Technology of the storage tank discipline which he felt was necessary as part of the fixed equipment (tanks, pressure vessels and piping) work that was being done. He served as the chairman of the API 2350 4th edition. Most of his career was at Chevron, but he has been a consultant and worked at a gas utility company. Email: phil@pemyconsulting.com



Brock Trotter graduated with a Bachelor's of Science in Chemical Engineering from the University of Oklahoma and is a registered EIT with the state of Oklahoma. Prior to joining the PEMY Consulting team he performed research in surfactant technologies at the University of Oklahoma with Dr. Jeffrey Harwell. He is also an attendee of the Shell Drilling and Production Camp where he was trained in a wide variety of offshore oilfield techniques. As a consultant he has written publications for Endress+Hauser and Emerson regarding tank level equipment as well as fire and overfill prevention. He has performed work in support of an expert witness regarding petroleum law and has written articles regarding API 2350, the impact of flooding on the Houston petroleum industry, and vapor related process safety engineering. His primary areas of interest include process safety engineering, performance engineering, emissions, overfill management, settlement analysis, automation, and risk analysis. Email: brock@pemyconsulting.com

Contributors



Dean Mallon has over 34 years' experience in chemical, petrochemical, refining and terminal automation, holding positions as a company owner to instrumentation sales and currently National Product Manager (Level/Tank Gauging) for Endress+Hauser in the USA. Dean Mallon has worked with the American Petroleum Institute for over 8 years, being involved with the API 2350 4th edition of overfill protection working group and most recently the 5th edition (currently being reviewed for publication).



Hai-Thuy Ngo has a business engineer degree and graduated in the top 5% of his university in 2005. He started in 2005 as Marketing/Product Manager for the Endress+Hauser Tank Gauging solution package in the Oil & Gas industry. Since 2009 he is responsible for the Oil & Gas industry for the Middle East, Central and South America, North Africa, Central Asia and Southeast Asia. In 2013 he became a TÜV certified functional professional and conducted trainings for Endress+Hauser safety specialists. In his global role he has visited more than 40 countries to share and learn the best practice of different Oil & Gas companies in different countries.



Markus Wohlgemuth has more than 25 years of experience across industries in project and product management, business development and compliance. Since 2007 he is working at Endress+Hauser and is member of several international networks and working groups. As a Business Development Manager for solutions he is one of the main responsible for the overfill prevention systems covering national and international requirements including API 2350 as well as IEC61508 and IEC 61511 related topics. He holds a BSc in electrical engineering, is certified computer validation manager and TÜV certified functional safety professional.

The Endress+Hauser Guidebook to API 2350 & Overfill Prevention

Chapter 1 – Safety Management Systems and Management’s Role	7
Overview	7
What is a Safety Management System?	8
Background of Overfill Prevention Process	9
OPP Requirements of API 2350	11
Overfill Management in the Larger Context of Safety Management Systems.....	12
Important Prerequisite for Overfill Prevention Process.....	12
Why is OPP Needed?	13
Chapter 2 – Introduction to API 2350 and Overfill Prevention	14
Why Overfills Matter to You.....	14
Understanding What’s at Stake for an Overfill	14
Buncefield Case	16
Puerto Rico Capeco Case.....	17
Chapter 3 – Regulatory Framework and Best Practices	19
The Process Safety Management Connection	19
Best Practices and Current Thinking on Ensuring Process Safety.....	19
Current Thinking on Ensuring Safety	20
Chapter 4 – Exploring API 2350	22
Introduction	22
Comprehensive Overfill Prevention.....	25
Applying API 2350	26
Chapter 5 – Risk Assessment	29
Why Overfills Pose Extraordinary Risk Levels	29
New Existing Facilities Issues.....	29
Difference Between Risk Assessment and Risk Management	29
Risk Assessment Screening	31
Logical Structure of Risk Assessment	32
Risk Screening Example.....	32

Chapter 6 – Role of Instrumentation and Technology 39

 Introduction and Motivation 39

 Tank Gauging Systems..... 39

 Manual Tank Gauging 42

 Automatic Tank Gauging..... 48

 Overfill Prevention Systems 50

 Proof Testing..... 52

 Contact vs. Non-Contact Level Sensors..... 61

 Categorization of Level Sensors 62

 Appropriate Level Sensor for Common Applications 62

 Point Level Sensors 63

 Continuous Level Sensors 68

 Oil Leak Sensors 74

Chapter 7 – Level Measurement Reliability 75

 Safety Instrumented Systems..... 75

Chapter 8 – Procedures, Operations, Testing, and Maintenance 81

 Procedures 81

Chapter 9 – How to Develop an OPP (Overfill Prevention Process) 82

Appendices..... 83

 Abbreviations 83

 Key Terms and Definitions..... 84

 Safety Management Systems 96

Introduction

One of the most significant sources of risk at facilities which store hazardous liquids is an overfill event. Risk is defined as the product of the probability of a risk event occurring and the consequential severity of that event. Overfill events create significant levels of risk because filling storage tanks occurs often, increasing the probability of overfill. The severity of an overfill event may be high because health and safety issues arise, or the environment is damaged – and fines and lawsuits tend to follow. The worst-case risk event scenario may be a vapor cloud explosion causing devastation both internally and externally of the offending company. In joint response to recent major overfill events, the industry developed API/ANSI Standard 2350.

Objectives

To address the most common cause of overfill near misses and incidents, the 4th Edition of API 2350 has introduced a new requirement related to safety management systems. API 2350 states, *“A management system is required for conformance with API 2350, but this standard does not specify how to implement such a system.”* Therefore, the purpose of this guidebook is to help organizations understand what this requirement means and why it is important for them to establish a safety management system or consider modifying an existing safety management system to include the overfill prevention process.

Scope

API 2350 is intended to provide operators with the best practices for implementing and maintaining petroleum storage tanks to prevent overfill events. The storage of any large amount of fuel crude oil and other hazardous liquid creates risk and potential danger at a facility if not properly operated, maintained and designed.

This guidebook is to support organizations to implement the current best practices by industry standards (like API/ANSI Standard 2350, Buncefield Report, IEC 61508 (Functional Safety) and IEC 61511 (Safety Instrumented Systems)) as they define the “Recognized and Generally Accepted Good Engineering Practice”.

Chapter 1 – Safety Management Systems and Management’s Role

Overview

“The Overfill Prevention Process (OPP)¹ is simple in concept - the termination of the source by:

- *Diverting the incoming flow*
- *Shutting down the flow (closing a receipt valve or terminating a pump)*
- *Using an alternative appropriate method of bringing the receipt process to a safe state without overfilling the tank such as enhanced communications, knowledge and control of receipts and ullage, and manually managed control systems*

While the desired end-result, the termination process, seems simple, experience indicates the need for a systematic Overfill Prevention Process to ensure success every time.”

The above excerpt, taken from API 2350, is everything that is required to prevent overfills - period! To successfully terminate a receipt for one time might seem to be easy. To do it safely a million times over is a Herculean task. The current edition of API 2350 requires that Owners and Operators set a goal to develop and implement a safety management system to control tank overfills. Experience has shown that while this goal appears to be simple, achieving this goal requires far more than good intentions. It requires both a systematic, sustained, continuously improved safety management system (SMS) and an overfill prevention process (OPP). Safety management system is the broad term used to describe the protocol, training, infrastructure, equipment, sensors, emergency response, and expertise that is developed to assist in the prevention of a risk event. The Overfill prevention process (OPP) is like the Safety Management System (SMS) but focuses exclusively on the prevention of a hazardous liquid overfill events.

As a prerequisite, achieving this goal requires senior level management commitment and a substantial investment in time and resources. More importantly, it requires that organizations recognize and establish core values that support the premise that potential hazards, such as overfills, are not only unacceptable and bad for business but are environmentally

damaging, dangerous, and potentially lethal. It is important that they understand the “insurance concept” as described later in this guidebook so that there is belief in the value of committing resources to ensuring these incidents do not happen in their companies. Management must promote and maintain support by developing and implementing the necessary standards, programs, safe work practices as well as providing the resources and funding required to achieve this goal.

It is not the intent of this guidebook to justify the need for such organizational values. However, it should be noted that there are many examples of companies that are either no longer in business or have had their businesses severely and negatively impacted, due to overfills or serious incidents. It is recognized by both industry and regulatory authorities that the failure to manage known and potential risks is a major contributing factor of tank overfills (as well as other major incidents).

To address the most common cause of overfill near misses and incidents, the 4th Edition of API 2350 has introduced a new requirement related to safety management systems. API 2350 states, “A *management system is required for conformance with API 2350, but this standard does not specify how to implement such a system.*” Therefore, the purpose of this guidebook is to help organizations understand what this requirement means and why it is important for them to establish a safety management system or consider modifying an existing SMS to include OPP.

The acronym SMS means any organization’s general safety management system or safety and environmental management system. The acronym OPP, means a specific reference to those aspects of SMS that apply directly to tank overfill prevention. Thus, when dealing with specific aspects of safety management systems related to overfill prevention, the term OPP is used. Often SMS and OPP are used interchangeably and therefore, the term OPP will be used interchangeably. Details on how any company can implement an OPP are provided for in Appendix: Safety Management Systems Continued.

¹ As used in this guidebook, OPP (overfill prevention process) is equivalent to the term used by API 2350, SMS, and means either a general safety and environmental management system that has been modified to include overfill prevention or a system. Moreover, OPP is equivalent to a Safety and Environmental Management System.

What is Safety Management System?

A management system is “*a formally established and documented set of activities designed to produce specific results in a consistent manner on a sustainable basis*”².

Safety management systems (or as referred to in API 2350 the Overfill Prevention Process (OPP)) can be defined as a management system embedded within an organization’s formal operating framework that includes safety and environmental goals. OPP includes all the elements of safety management systems but with a specific focus on tank product receipt operations. OPP should be integrated with any existing corporate management systems such as safety/environmental management systems. We will generically refer to the management systems as they specifically apply to overfill as OPP.

OPP compiles various management and operational procedures and practices into one coherent organizational structure that maximizes the level of safety and environmental protection.

For OPP to be effective, the following actions are required:

- OPP must be established, implemented, and actively supported by the organization’s leadership to be successful specific to the applicable tank population
- OPP requires formal responsibility and accountability at all levels of the organization
- OPP requires correctly aligned behaviors and attitudes by all employees
- OPP requires continued review and improvement through activities such as incident and accident investigation, audits, and management of change

² CCPS Guidelines for Risk – Based Process Safety, AIChE

Background of Overfill Prevention Process

The relationship between management and incident prevention became acute after several serious incidents in the chemical process industries caught the attention of the public and the regulators. In the 1970's and 1980's, it became increasingly evident that management systems, based on science, can effectively be used to adjust an organization's best management practices to focus on solving safety and environmental problems. Industry organizations such as the Center for Chemical Process Safety (CCPS), American Chemical Council (ACC) (formerly Chemical Manufacturer's Association), Canadian Chemical Producers Association, American Petroleum Institute and other associations and organizations, both in the US and in other countries, started developing approaches to incorporate safety and environmental management systems into the overall organizational structure.

These organizations represent the foremost experts in their individual fields and each aim to provide the information and protocols needed to proactively prevent a risk event.

The concept of management systems originated with Dr. W. Edwards Deming who used Shewart's work to show organizations how to improve consistency and quality of goods and services in the workplace. The Shewart Diagram, Figure 2, represents the rudiments of a simple management system, sometimes called "PDCA" (Plan, Do, Check, Act) or the "Shewart Cycle". The Shewart Cycle is a concept used for understanding the steps involved in continuous improvement. The circular pattern for the Shewart Cycle is never-ending, visually displaying the idea of continuous improvement.

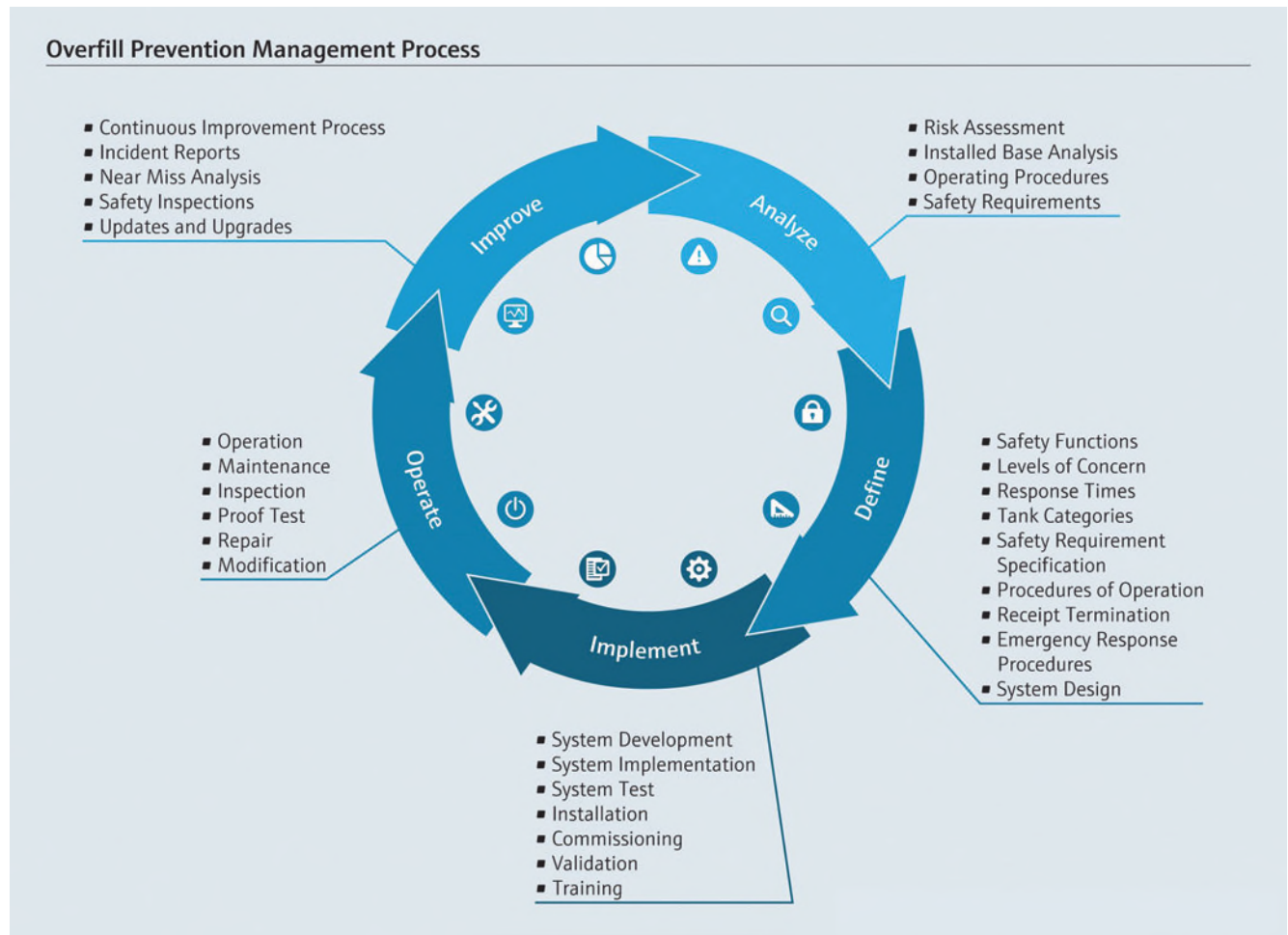


Figure 1: Overfill Prevention Management Process

Shewart Diagram – The 4 Steps of PDCA

PLAN

Determine the goals and objectives and develop and establish the processes necessary to deliver results in accordance with the expected output (the goals and objectives). *(Note: Focusing on the expected output differs from other techniques in that the completeness and accuracy of the specification is also part of the improvement).*

DO

Implement the new processes, often on a small scale if possible, to test effectiveness. *(Note: It is important to collect data for charting and analysis to perform the following "CHECK" step).*

CHECK

Measure the new processes and compare the results (collected in "DO" step) against the expected output (goals and objectives from the "PLAN" step) to ascertain any differences. *(Note: Charting data can aid in assessing trends to convert the collected data into information needed for the "ACT" step).*

ACT

Analyze the differences to determine their causes and determine where to apply changes that will facilitate improvements. *(Note: When an analysis of these four steps does not indicate a need to improve, refine the scope to which PDCA is applied and perform the PDCA again until there is a plan that provides for improvement).*

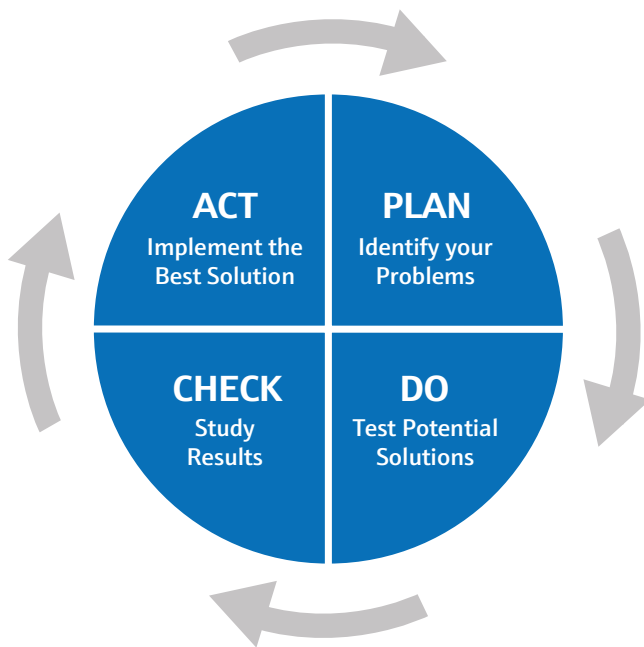


Figure 2: Shewart Diagram

As public reaction to serious safety and environmental incidents became increasingly less tolerant, there was a desire for regulatory activity. One of the first regulations to address incident prevention through safety management systems was the OSHA Process Safety Management rule (29CFR1910.119), aiming to prevent the release of hazardous liquids into the environment through government regulatory processes. Process safety management requires identification of hazards associated with processes using highly hazardous chemicals. The Seveso Directive⁴ was enacted in Europe and other countries, and it serves as the European model for hazardous liquid release prevention.

Today, most organizations agree that developing and implementing a safety management system is appropriate, even if not required by regulations. However, the requirements and application of a safety management system is specific to the processes, materials and potential hazards of individual organizations and facilities.

This guidebook is intended to assist organizations in understanding and applying safety management system to overfill prevention processes, a requirement of API 2350.

OPP Requirements of API 2350

API 2350 states, “A management system is required for conformance with API 2350, but this standard does not specify how to implement such a system.” The reason that API 2350 does not specify how to implement a safety management system is that each system must be specifically designed for the organization and facility using it. It must be remembered that safety management systems were initially created by and for large organizations. Smaller companies must design and implement safety management systems that fit their personnel, resources, equipment, and operations, all of which may be smaller than and different from those of the large corporations. However, many smaller organizations are not taking advantage of formal management systems which include OPP. One critical key to developing and using effective management systems for smaller organizations is to make the systems applicable to specific operations or purposes.

Some larger organizations have been so involved in multiple processes (often numbering in the thousands) and corresponding complexities that their OPP becomes excessively costly and difficult to implement and manage. The OPP often requires reevaluations and redesigns to meet specific changes in processes, operations, products, and conditions. Smaller companies can avoid this problem by carefully evaluating and determining the applicable parts of safety management systems and intelligently incorporating them into their own standards, operating procedures, and work practices. Many larger companies are in the process of making their corporate processes simpler and more effective for easier resource allocation and decision making.

API 2350 further states, “If procedures for a comprehensive OPP management system do not exist, then they shall be developed or shall be incorporated by reference into any suitable existing management system. The documented procedures for the management system shall address all components of OPP. These include typical administrative controls such as management of change, operating personnel training and auditability for the OPP components.”

API 2350 recommends that the following specific OPP requirements be established and implemented by organizations operating storage tank facilities:

- Formal written operating procedures and practices covering environmental, safety and emergency response requirements.
- Trained and qualified operating personnel.
- Functional equipment systems that are regularly tested and maintained by qualified personnel.
- Scheduled inspection and maintenance programs for overfill instrumentation and other equipment.
- Systems to address both normal and abnormal operating conditions including emergency shutdown and start-up following emergencies.
- A management of change (MOC) process which includes personnel, product and equipment changes. MOC is the systematic process of identifying all downstream effects that are caused by any change to a process. To conduct an MOC, the subject matter experts should gather to discuss the process change and how it will impact the downstream processes, emergency response aspects, and scheduling issues.
- A system to identify, investigate and communicate overfill near misses and actual incidents.
- A system to share lessons learned between management and employees.
- A follow-up system to address necessary mitigation of circumstances (causal factors) leading to near misses and actual incidents.
- Communication system protocols both within the Owner/Operator organization and between the Transporter and the Owner/Operator that are designed to function under abnormal as well as normal conditions.

⁴ This Directive (Seveso II) replaced Directive 82/501/EEC (Seveso I, named after the Italian town which suffered exposure to an accidental release of dioxin in 1976). It introduced major changes and new concepts. It focuses on protection of the environment, and was the first to cover substances considered dangerous for the environment, particularly aquatoxics. It introduced new requirements relating to safety management systems, emergency plans and land-use planning and tightened up the provisions on inspections and public information.

Overfill Management in the Larger Context of Safety Management Systems

Many organizations already have an active safety management system in place. In this case, an OPP can be easily integrated into their existing systems through the management of change process (MOC). This will require that all aspects of the existing safety management system be scrutinized to determine if and how the changes required by API 2350 can be adapted and incorporated into the organization’s management systems. Application of the MOC process will address overall improvements, not only to the existing management system, but will ensure that OPP is effectively integrated with the existing systems.

If an organization does not have an existing management system but intends to adopt the requirements of the current edition of API 2350, then it should not only develop an OPP but should consider doing so within the context of establishing and implementing a total and comprehensive management system. This is because it is doubtful that an OPP would be effective without the establishment of an overall functioning and operational safety management system. In other words, a comprehensive safety management system is a prerequisite for designing an OPP effectively.

Important Prerequisite for Overfill Prevention Process

Without the direct, active, and continuous support of the highest levels of management in the organization, management systems cannot be successfully implemented and maintained. It cannot be over-emphasized that safety and environmental protection are important corporate requisites and must be derived from and be supported by the very top levels of the organization. This is necessary to gain and keep the approval and support of employees

as well as the good will of customers and the public. An example of an actual company’s corporate values is shown in Figure 3. These eight key values have led this company to excellence and leadership in the industry. It should be noted that health, safety, and environmental protection are key values that are just as important as financial performance or any of the other corporate values listed.

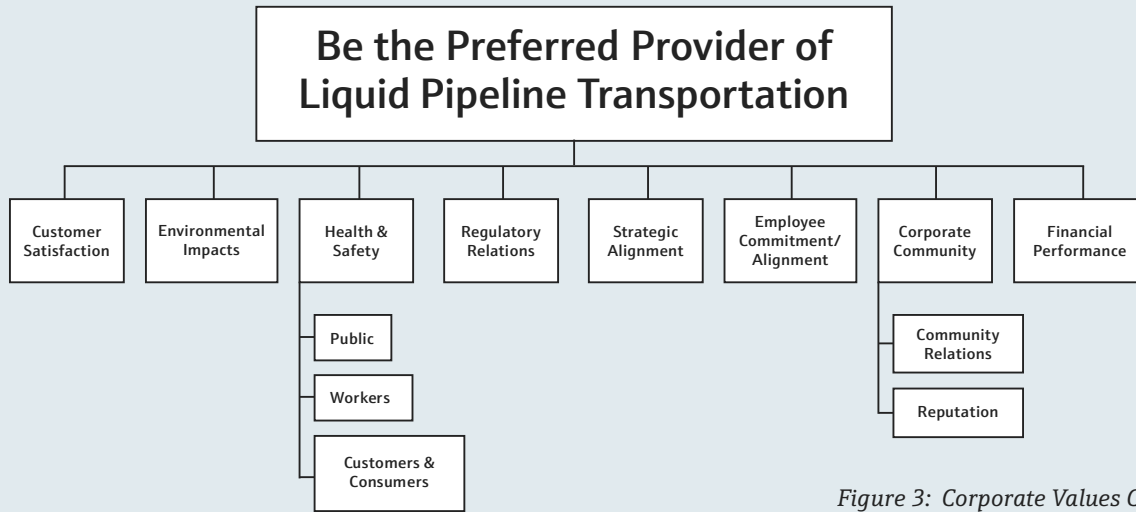


Figure 3: Corporate Values Chart

For organizations which store or transport significant quantities of flammable and combustible liquids, industry studies have shown that safety management systems result in a significant return on investment in terms of financial stability, safety performance and environmental compliance. In this guidebook Chapter 9 is intended to help organizations develop the OPP component of an

existing management system which is designed to fit the size, nature and complexity of the organization and its facilities and employees. Organizations that adopt the processes described herein will benefit from control of hazards, resulting in reduced exposure to risk and reduced incidents and accidents, with the additional benefits of reduced operating expenses and better employee retention.

Why is OPP Needed?

The principal reason for implementing OPP is an organization's desire to reduce the potential for safety and environmental near-misses and incidents through the application of OPP. (Note: Specific benefits are covered in the reference documents).

- OPP ensures that overfill prevention is prioritized and that the tank filling process is comprehensively addressed through risk assessment, risk management and SMS/OPP requirements.
- OPP ensures that the tools needed to systematically identify potential and actual hazards and manage risks are provided and supported by management.
- OPP ensures that incidents and near misses are systematically analyzed to determine the root causes of overfills.
- OPP ensures that process equipment, maintenance and operations procedures, and compliance measures are continuously evaluated and improved as needed to prevent and control overfills.
- OPP ensures that management, supervisory and employee behaviors, attitudes, values, skills, actions are totally committed to preventing, managing, and controlling overfills.
- OPP ensures appropriate allocation of resources.
- OPP ensures that the personnel who manage and operate tank facilities are knowledgeable and trained in the basic principles of overfill prevention.

OPP is a proven process for managing risks that ties all elements of the organization together laterally and vertically. OPP can be effective only if management and employees accept and support a safety culture which does not tolerate overfills.

Sidebar

OPP, SMS and PSM

API 2350 refers to Overfill Prevention Processes (OPP). In general, OPP is a subset of the Safety Management System (SMS) that a company has in place. In general, SMS is a broader definition which includes all safety concerns for all process, equipment and systems in a facility or organization.



Figure 4: Levels of Safety Management

Process safety management (PSM) is the most comprehensive term including all process safety concerns. This concept is displayed visually on Figure 4 where process safety management is the foundation for safety management. In turn, the safety management system forms the basis for the OPP which should be integrated within the context of safety management systems.

Chapter 2 – Introduction to API 2350 and Overfill Prevention

Why Overfills Matter to You

There have been many serious tank incidents resulting in environmental damage, property damage, injuries, fatalities, bankruptcies, and new regulations. So why should the tank overfilling events be singled out by a guidebook such as this?

What makes the tank overfill uniquely hazardous is that it, alone, of all tank accident scenarios, can generate a deadly vapor cloud which can flow out far past secondary containment, bunds and property lines resulting in a deflagration or even a detonation. Indeed, the Buncefield incident which we will review later, resulted from a gasoline storage tank overfill that set off the largest explosion in all of Europe since World War II.

The tank overfill also has major consequences that can result from any large spill of hazardous material including environmental or fire damage, as well as health and safety. The overfill of volatile petroleum liquids is the worst-case scenario for petroleum product storage and tanks.

If you are an owner or operator the next obvious question is, “how can I avoid becoming a victim of a tank overfill?” Well, there isn’t a simple, easy answer, unfortunately. Improving equipment systems and

operations is to a company as getting healthy by dieting and exercise is to a person. It takes planning, constancy of purpose, challenging work, and knowledge that the benefits outweigh the costs of the required work.



Figure 5: The Sky after Vapor Cloud Explosion (VCE)⁵

However, the benefits are not simply just overfilling avoidance. Many of the process changes needed to help prevent an overfill will dramatically improve operational capabilities and efficiencies.

Understanding What’s at Stake for an Overfill

Risk is the threat to values that we wish to keep intact and to preserve. For example, human health and safety, the environment, reputation, customer satisfaction, employee alignment are a few typical values that most companies have. Of course, we also value profitability and financial performance but there are often tradeoffs between financial performance and protection of those things we value. Tank overfills have caused public condemnation, bankruptcy and destruction of reputation and profitability.

When litigation is involved in tank overfills (and it always is on the serious cases) then the benchmark for credibility on the part of the tank owner/operator is the use of current best practices as reflected by industry standards such as API or IEC. The term RAGAGEP is used to represent the current best practices by industry standards as it stands for “Recognized and Generally

Accepted Good Engineering Practice”. The differences between the previous editions of API 2350 (3rd edition and older) and the current editions is vast.

Although, there are still many companies that are working from the 3rd edition, or even no industry standard. Failure to comply with these standards or to consider them and develop company specific versions is a substantial vulnerability for a company.

The best and most efficient way to deal with tank overfill prevention is to:

- a) Make sure that safety and environmental protection are core values and that appropriate senior leaders are embracing these principles by appropriately allocating resources as well as being held accountable.

⁵ http://www.hsmsearch.com/page_665072.asp

- b) Use management systems which in turn depend on:
- Communication protocols between transporter and operator
 - Written operations and abnormal operations procedures
 - Establishment of operational parameters
 - Risk assessment
 - Other elements of the current edition of API 2350
- c) Use API 2350 by setting up teams to plan and execute compliance.

Prior to the first edition of API 2350 there were many tank fires, and API 2350 was created to help reduce the problems of tank fires resulting from overfills. The scope of API 2350 was limited to NFPA Class 1 liquids which are petroleum liquids with a flash point below 100°F (37.8°C). The NFPA (National Fire Protection Association) is the professional organization which oversees the codes, standards, classifications, education, and compliance related to flammable liquids and fire events. A flash point is the temperature required for a combustible liquid to vaporize within the lower flammable limit (the concentration of vapor at which it will combust with atmospheric oxygen).

Originally the sole purpose of API 2350 was for fire prevention and protection. It was not until the 3rd edition and after the API ‘STEP’ (Strategies for Environmental Protection) program, an environmental responsibility program advocated by API to its member companies, that oil must also be handled in a way that

protected the environment. As a result, the 3rd edition included, as its sole change, NFPA Class 2 liquids which have a flash point between 100-140°F (37.8-60°C) such as diesel fuels. It should be noted that NFPA has simply played the role of API advocate where it comes to requirements and standards; there is no fundamental conflict between NFPA or API; NFPA 30, the NFPA standard related to hazardous liquid overfill from a storage tank, simply states to use API 2350 for overfill prevention.

The current edition of API 2350 includes the following substantial changes with respect to previous versions:

- Requirement for an independent and diverse Overfill Prevention System and Process
- Requirement for tank overfill risk assessment
- Updating the standard to account for the rapidly evolving instrumentation and control technology
- Inclusion of and references to the control system based safety standards such as ISA S84 (Safety Instrumented Systems), IEC 61508 (Functional Safety) and IEC 61511 (Safety Instrumented Systems)
- The use of the terms ‘alert’ versus ‘alarm’ to reduce operator ‘alarm overload’ and consistency with ISA 18.2 for alarm management

The 5th edition should simplify and clarify the 4th edition, and it is not expected to have significant changes related to the concepts and ideas incorporated into the 4th edition.

API 2350 Edition	Class I Liquids	Class II Liquids	OPP	Risk Analysis
1	✓			
2	✓			
3	✓	✓		
4	✓	✓	✓	✓
5	✓	✓	✓	✓

Figure 6: Evolution of API 2350

Buncefield Case

The Buncefield terminal (Figure 7 before the incident) was part of the Hertfordshire Oil Storage Terminal, an oil storage facility located near the M1 motorway by Hemel Hempstead in Hertfordshire, England. The terminal was the fifth largest oil-products storage depot in the United Kingdom, with a fuel distribution facility supplied fuel across the region including Heathrow and Luton airports. On Saturday the December 10th, 2005 a part of the Buncefield oil storage depot was filling with gasoline. The tank capacity was about 60 million imperial gallons of fuel.



Figure 7: Buncefield Terminal Before Blast

The tank had two forms of level control: a gauge that enabled the employees to monitor the filling operation and an independent high-level switch which was to close operations automatically if the tank was overfilled. The first gauge stuck and the independent high-level switch was inoperable, so there was no means to alert the control room staff that the tank was filling to dangerous levels. Eventually massive quantities of gasoline overflowed from the top of the tank. About 260 cubic meters overflowed for a duration of 1380 seconds. A vapor cloud formed and was ignited causing a massive explosion and a fire that lasted for five days (Figure 8). A vapor cloud explosion is the result of an enormous collection of combustible vapors due to a hazardous liquid overflow. The liquid contacts the ground with a large amount of kinetic energy, rapidly vaporizing it. Once the air is saturated with combustible vapor above the lower flammable limit (LFL) it is capable of combustion from a flammable source.

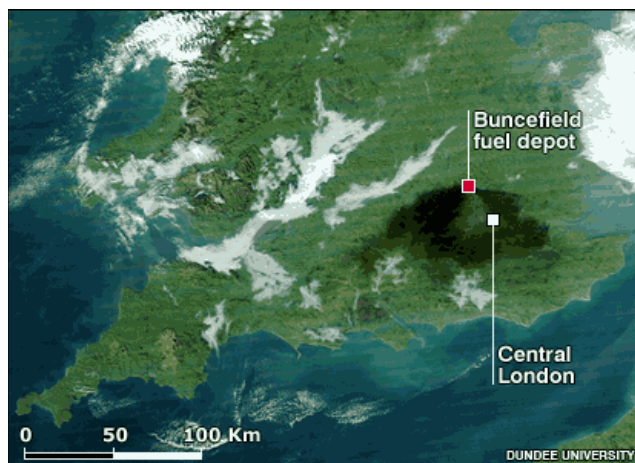


Figure 8: Location of Buncefield with Smoke from Fire and Blast Showing Large Area of Southern England Covered

The vapor cloud explosion (VCE) resulted in 43 injuries (no fatalities), millions in fines, criminal and civil litigation, new regulations, and more distrust of the oil industry by the public. Not only was most of the terminal devastated, but the vapor cloud explosion (VCE) destroyed buildings, offices, and homes for hundreds of meters outside of the facility (Figure 9).



Figure 9: Buncefield after the Incident with the Culprit Tank T-912 Initiating Event at Center Foreground⁶

All product tanks engulfed by the vapor cloud were ignited, tanks and piping were deformed by overpressure and buildings and houses within 100 m were destroyed. The Buncefield report found that the terminal had installed an independent high-level switch that could be routinely tested. The system was not fully understood by operators causing the alarm to become inactive when tested; this creating a false sense of security and increased the risk of an overfill.

⁶ <http://www.csb.gov/buncefield/buncefield-report.pdf>

The overfill occurred and progressed because operators were unaware that the tank was filled beyond capacity showing that overconfidence in an ATG system can lead to an overfill event.

A high-level dumb switch mechanical float was used. Such switches usually have no diagnostic functions. Therefore, there was no indication or alarm that the sensor was accidentally left out of operation.

Consequently, the Buncefield report recommends using “more advanced sensors (such as those based on tuning fork technology) that incorporate diagnostics so that all foreseeable failure modes are detected as they occur” for Overfill Prevention Systems.

State of the art point level sensors like a tuning fork level switch (see also Chapter 6) are equipped with continuous checking online diagnostic functions. Such sensors do not only detect and alert cable breaks and open circuits but also the correct operation of the electronics and of the vibrating fork itself. Build up and corrosion can be detected by analyzing the frequency. Therefore, such sensors are very reliable and are available with the requested SIL certifications.

Puerto Rico Capeco Case

Four years after the Buncefield incident a gasoline tank overfill formed a vapor cloud which detonated at the Caribbean Petroleum Company (CAPECO) Tank Terminal igniting the entire facility (Figure 10 & CSB Video - <https://www.csb.gov/videos/>). The huge explosion occurred at the Caribbean



Figure 10: 2009 Capeco Tank Overfill Incident⁷

Petroleum Corporation (CAPECO) facility in Bayamón, Puerto Rico on of October 23rd, 2009, while offloading gasoline from a tanker ship, the Cape Bruny, to the onshore CAPECO tank farm. A 5-million-gallon aboveground storage tank (AST) overflowed into a secondary containment dike. An aboveground API storage tank (AST) is any storage tank which operates above ground at atmospheric to 2.5 psig.

The gasoline spray formed a large vapor cloud while fuel fell to the ground and quickly evaporated and ignited after reaching an ignition source in the wastewater treatment plant. The blast and fire from multiple secondary explosions resulted in considerable damage to 17 of the 48 petroleum storage tanks, other onsite equipment and in offsite neighborhoods and businesses. The fires burned for nearly 60 hours.



Figure 11: View of Terminal Day after Incident

The VCE blast created a ground pressure wave registering 2.9 on the Richter scale⁸ and damaging nearly 300 homes and businesses up to 1.25 miles from the site. Consequently, the nearby Fort Buchanan military facility suffered over \$5 million in damages. Air and vehicle transportation was interrupted, and thousands of gallons of oil, fire suppression foam and contaminated runoff were released to the environment (Figure 10 & Figure 11 show a map of communities neighboring the CAPECO facility and community damage). CAPECO and the local fire department lacked the appropriate equipment or training to extinguish multiple tank fires, prolonging the environmental effects of the incident. The accident resulted in an emergency declaration for assistance from President Obama for the affected municipalities.

⁷ http://www.csb.gov/assets/Record/BAR_NI_2015-411.pdf

⁸ Puerto Rico Seismic Network. *Informe Especial, Explosión de Caribbean Petroleum en Bayamón, PR, 23 de octubre de 2009.* University of Puerto Rico Mayagüez Campus.

The standard procedure for the operator taking the receipt was to manually gauge the receipt tank at the start and end of the filling operation (open and close gauging). The tank used a float and tape type level measurement system at grade visible to the operator.

The US Chemical Safety Board (CSB) team arrived at the incident scene two days after the incident. The investigation team photo-documented the incident site, inventoried key evidence, interviewed witnesses and assessed community damages. The team consulted tank experts and researched previous tank overfill incident investigations. Even though CAPECO had installed transmitter cards from the tank gauge in the field to read signals in the control room, they had been faulty for some time and had not been in working order at the time of the incident.

Underlying the key findings and recommendations were faults in the management systems used at the facility. Some key findings by the US CSB related to the management systems were:

1. Inadequate tank filling procedures were restricted to a list of equipment to be manipulated. In addition, the outdated procedures were often applicable to the tank farm when the refinery was in operation.
2. The automatic tank gauging system, the only level control and monitoring system to support the operator in preventing overfill, was often out of service.
3. The defective level transmitter was not sending data for Tank 409 or 107 to the computer in the operator shack or to the supervisor's office on the day of the incident.
4. A nonexistent automatic overfill prevention system and the inability to rapidly stop transfer operations or divert flow before an overfill weakened CAPECO's safety program.

Ill-equipped CAPECO tanks were left with an unreliable level monitoring and control system or a high-level alarm system. It should be noted that these cases all involved motor gasoline. However, according to the latest research on vapor cloud explosion mechanisms resulting from the UK Health Executive studies¹⁰, these explosions can occur with tank filling operations involving any volatile flammable liquid such as acetone, methanol, condensate, as well as even some crude oils.

⁹ Fire and Blast Information Group (FABIG). Technical Note 12. Steel Construction Institute (2013).

¹⁰ British Health & Safety Executive. Vapour Cloud Formation Experiments and Modelling Research Report 908. Health and Safety Laboratory (2012).

Chapter 3 – Regulatory Framework and Best Practices

The Process Safety Management Connection

The long history of process safety management goes back thousands of years, but it was not until large industrial complexes handling massive quantities of dangerous materials proliferated and culminated that process safety management was coined and standardized. The standardization of chemical storage was a result of the worst industrial accident of all time – the deadly Bhopal incident that released 40 tons of highly toxic methyl isocyanate gas at Union Carbide in Bhopal, India plant in December of 1984.

This toxic release resulted in at least 4000 deaths and 200,000 injuries. As a result, in 1990 OSHA proposed the “Process Safety Management of Highly Hazardous Chemicals” standard referred to as the PSM standard. The emphasis of the program was to develop management systems which are integrated

and systematic, achieving the goals of the corporation while spanning people, processes, and equipment. The standard included 14 mandatory elements which are discussed in Appendix “Safety Management System Continued” of this guidebook. Much of the original work was developed and sponsored by the Center for Chemical Process Safety (CCPS) of the American Institute of Chemical engineers (AIChE).

In the 1996 MEER court decision exempted atmospheric storage tanks from PSM regulation regardless of storage quantity. The principles in PSM are necessary to prevent serious incidents regardless of whether they are regulated or not.

Best Practices and Current Thinking on Ensuring Process Safety

RAGAGEP is an acronym for “Recognized and Generally Accepted Good Engineering Practice”. It became important when it was used by OSHA in a memorandum to provide guidance on the enforcement of the Process Safety Management Standard’s recognized and generally accepted good engineering practices. Although OSHA does not define RAGAGEP it does refer to the Center for Chemical Process Safety’s (CCPS) Guidelines for Mechanical Integrity Systems:

“Recognized and Generally Accepted Good Engineering Practices” (RAGAGEP) - are the basis for engineering, operation, or maintenance activities and are themselves based on established codes, standards, published technical reports or recommended practices (RP) or similar documents. A recommended practice is a standards document which suggests or recommends operators and contractors on how a procedure should be conducted. Recommended practice documents

characteristically use the language “should” and “ought” to recommend these practices. RAGAGEP demonstrates approved ways to perform specific engineering, inspection or mechanical integrity activities, such as fabricating a vessel, inspecting a storage tank, or servicing a relief valve.

As used in the process safety management standard, RAGAGEP applies to process equipment design, installation, operation, maintenance, inspection, test practices and frequency of testing. RAGAGEP must be both “recognized and generally accepted” as well as contain “good engineering” practices. The process safety standards allow employers to select the RAGAGEP they apply in their covered processes. Although tank farms are not required to comply with the process safety management regulations, the principles of good, safe operations would embody these principles.

Current Thinking on Ensuring Safety

Where design of safety systems is involved then the concept of layers of protection becomes important; this is illustrated in Figure 12. Layers of protection are the multitude of activities and equipment which a company may incorporate to reduce the likelihood of a risk event. Layers of protection, such as a sensor and alarm relay or response procedures, will reduce the likelihood of a risk event (spill) occurring, but the layers of protection can never be 100% effective. No matter how well we prepare, the law of large numbers assures us that rare events are inevitable over extended periods of time. There are many variations of the diagram, shown in Figure 12, in the public domain but the concepts are consistent.

The basic process control system is shown as the bottom layer. This layer is often referred to as the Basic Process Control System (BPCS). The BPCS for overfill is typically the operator-controlled system of checks and balances and manual operation of valves that is used to fill tanks. The tank gauging system and an alert relay are components within the BPCS.

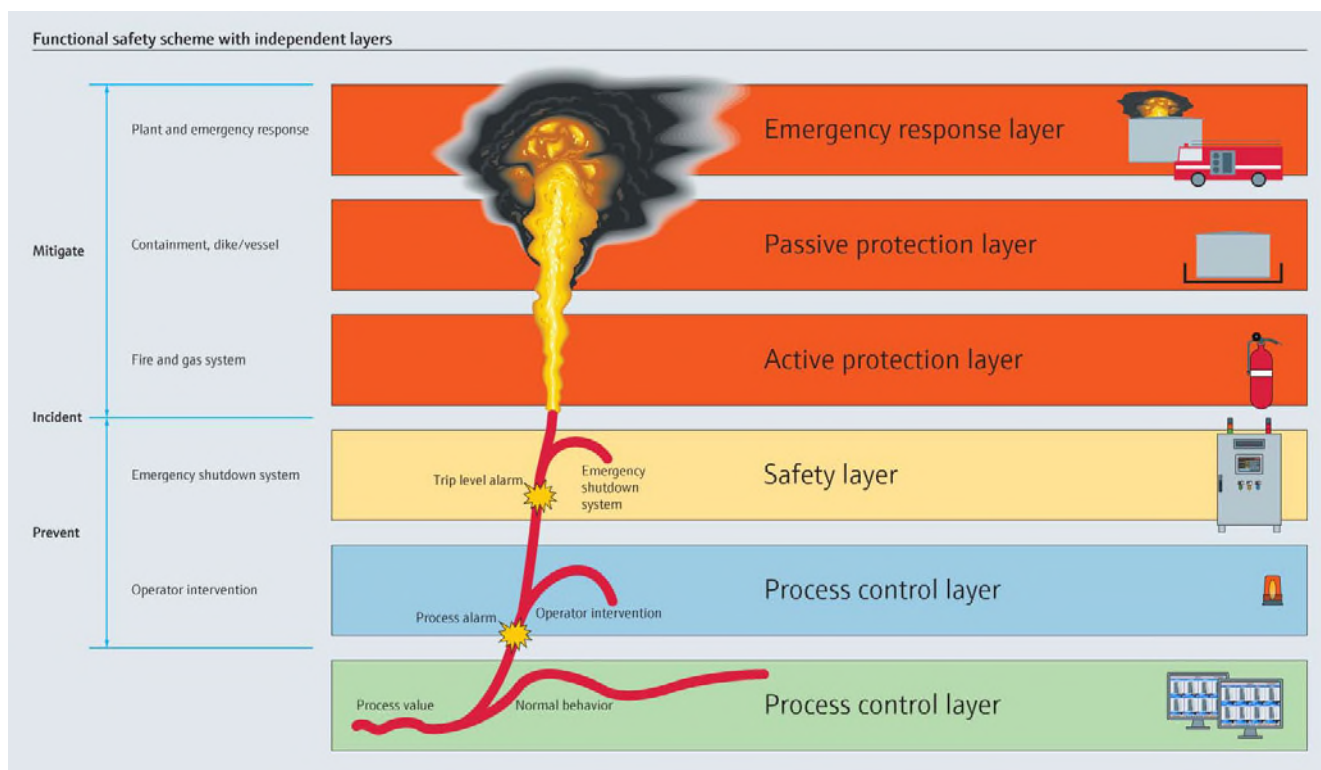


Figure 12: Functional Safety Scheme with Independent Layers

The overfill prevention process is within the safety layer, these alarms are treated in many ways but the current edition of API 2350 requires that alarms be actionable; that is, there must be no misunderstanding about the meaning of the alarm by operators, and there must be a written and specific procedure that is immediately acted upon by the operator when the alarm triggers. Depending on how the alarm is operated, the alarm might appear in the “Normal behavior” safety layer or the “Operator intervention” safety layer.

The “Operator intervention” layer and emergency shutdown layers are composed of alarms and receipt termination procedures as well as AOPS which act automatically causing the diversion or suspension of liquid flow into a tank.

A robust means of shutting down a system to a safe state requires a further development of the concept of layers. An *independent layer of protection* is one

that is not affected by any other layer and which cannot fail as the result of a fault in another layer. Numerous overfills on tanks with multiple shutdown systems have occurred. In these systems, both automatic shutdown relays are attached to the same instrument (control valve, pump, etc.) and powered from the same source.

Therefore, if a power outage occurs and there is no back-up power then neither system will operate as intended. Also, if the valve “freezes” then both controls systems acting to shut down the receipt will fail to do so because the valve is a common point of failure. Ideally, each system acting as a control should be independent of every other system acting to prevent the failure. This is the only way to add redundancy and reduce the likelihood of a failure event such as an overfill.

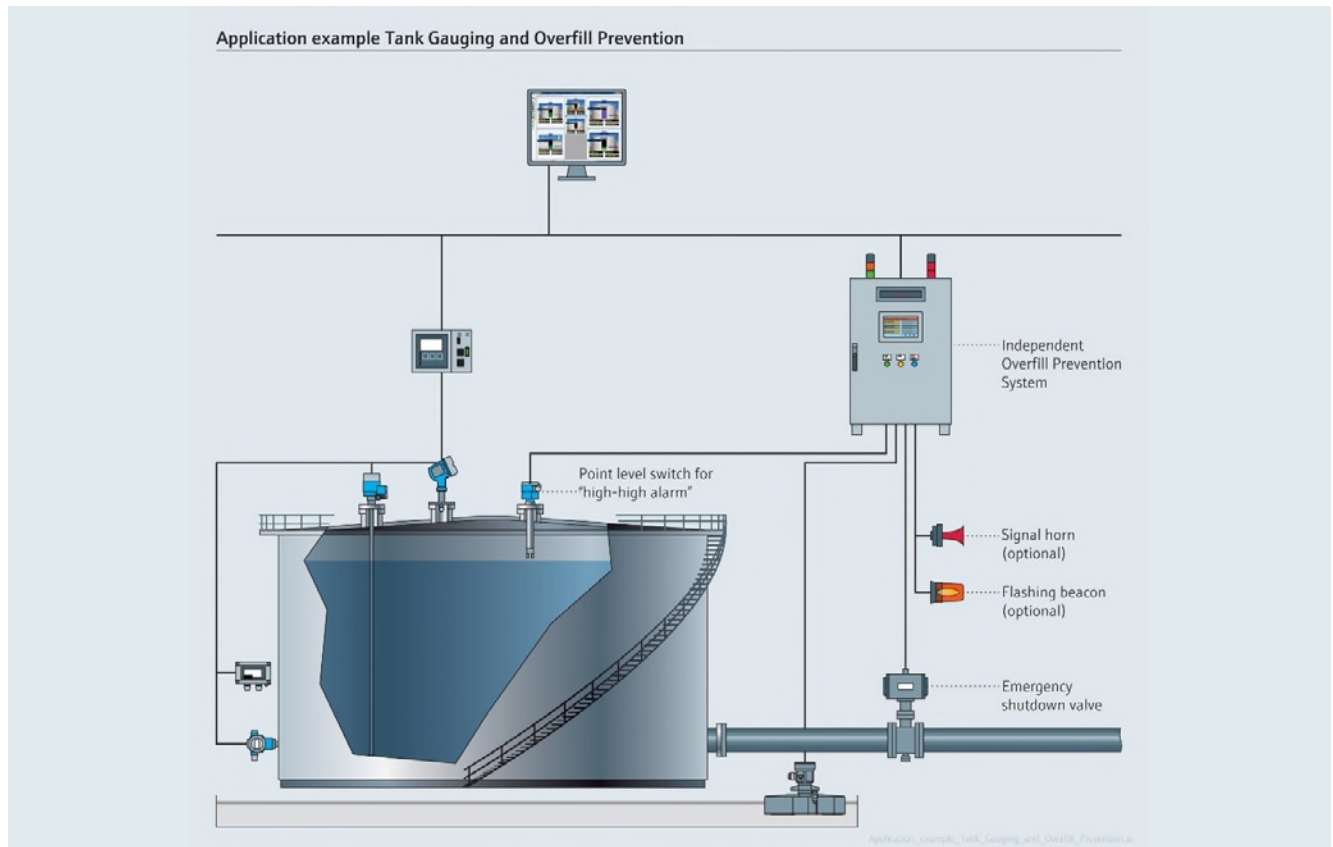


Figure 13: An example of a Tank Gauging System together with an independent and diverse Overfill Prevention System

Chapter 4 – Exploring API 2350

Introduction

One of the most significant sources of risk at facilities which store hazardous liquids is an overfill event. Risk is defined as the product of the probability of a risk event occurring and the consequential severity of that event. Overfill events create significant levels of risk because filling storage tanks occurs often, increasing the probability of overfill. The severity of an overfill event may be high because health and safety issues arise, or the environment is damaged – and fines and lawsuits tend to follow. The worst-case risk event scenario may be a vapor cloud explosion causing devastation both internally and externally of the offending company. In joint response to recent major overfill events, the industry developed API/ANSI Standard 2350.

Aim

API 2350 is intended to provide operators with the best practices for implementing and maintaining petroleum storage tanks to prevent overfill events. The storage of any large amount of fuel crude oil and other hazardous liquid creates risk and potential danger at a facility if not properly operated, maintained and designed. For example, spilling hazardous liquids is a violation of environmental regulations and results in fines, lawsuits, and additional stress. Because the legal response to an overfill event is so severe it is important for companies to implement procedure and technology to prevent the likelihood of event occurrence and to show good faith attempts to mitigate this risk. These companies should also prepare response procedures for the event of spilling oil.



Figure 14: Crude Oil Spill Cleanup Effort

Further, volatile fuels have the potential to cause a vapor cloud explosion and other fire hazards. Vapor cloud explosions result from the rapid volatilization of fuel spilled by overfilling a storage tank. The flammable vapors are capable of combustion by an ignition source at a concentration above the lower flammable limit. Once this ignition occurs, the fire may provide enough energy and a source of ignition to initiate a chain of petroleum storage tank failures.

This guidebook to API 2350 aims to simplify and summarize the RAGAGEP, risk analysis, overfill prevention process (OPP), and instrumentation aspects which are provided by the current edition



Figure 15: Results of Vapor Cloud Explosion

of API 2350, providing clear methods to implement industry best practices. To achieve these goals, we must consider in addition to management systems the concepts of redundancy, diversity, fail-safe systems, normal and abnormal condition in addition to procedures and preventative maintenance. The latest edition of the standard can be accessed from API's website at a nominal expense (www.api.org).

Scope

API 2350 applies to all storage tanks which are used for storing a Class I or Class II petroleum liquids. Class I fuels have a flash point below 100°F (37°C), and Class II fuels have a flash point between 100°F (37°C) and 140°F (60°C). The flash point is the temperature at which a multicomponent liquid, such as gasoline, will begin to generate sufficient vapor to ignite. In short, any fuel which reaches the lower flammable limit (LFL) when its temperature is below 140°F(60°C) falls within the scope of API 2350-4.

API 2350 does not apply to underground storage tanks, tanks of less than 1320 US gallons (5000 L), pressure vessels, nonpetroleum storage, tanks at service stations and natural gas storage tanks.

The standard is intended for facilities which market, refine, store and distribute fuels, but the principles of the standard can be applied to any chemical storage system which poses a grave risk due to overfilling. However, the recommendations of API 2350 are also useful in application for any storage of hazardous liquids (ships, truck tanks, upstream applications, etc.)

Primary Features of API 2350

One of the primary features of API 2350 is the categorization of tanks based on their liquid receipt shutdown process, whether the tank uses an Automated Overfill Prevention System (AOPS) or an operator to terminate the flow. The “Manual Overfill Prevention System (MOPS)” category is shown on Figure 16, and the “Automated Overfill Prevention System (AOPS)” category is shown in Figure 17. “Manual Overfill Prevention System (MOPS)” is any OPP system which requires human intervention to terminate the flow of liquid into a tank, whereas “AOPS” is any OPP system which terminates the flow of liquid into a tank without any human intervention.

For more details see “Overfill Management System Categories.”

The prime elements of API 2350 are as follows:

- Implement an Overfill Prevention Process (OPP)
- Implement and maintain a risk assessment system
- Apply preventative maintenance to Overfill Prevention system and equipment
- Written procedures for operating under normal, abnormal, startup and shutdown conditions as well as communications between the supply company and receiving company
- Initializing operating parameters for each tank:
 - Equipment category
 - Levels of concern (LOCs)
 - Response times
 - Alarm procedures

Developing operating parameters is a first step to implementing API 2350. The operating parameters include data such as Critical High Level, operator response time, operator attendance, High-High Level Alarm (HHLA) and Maximum Working Level (MWL). The definitions for these terms are available in Appendix – Key Terms & Definitions of this guidebook.

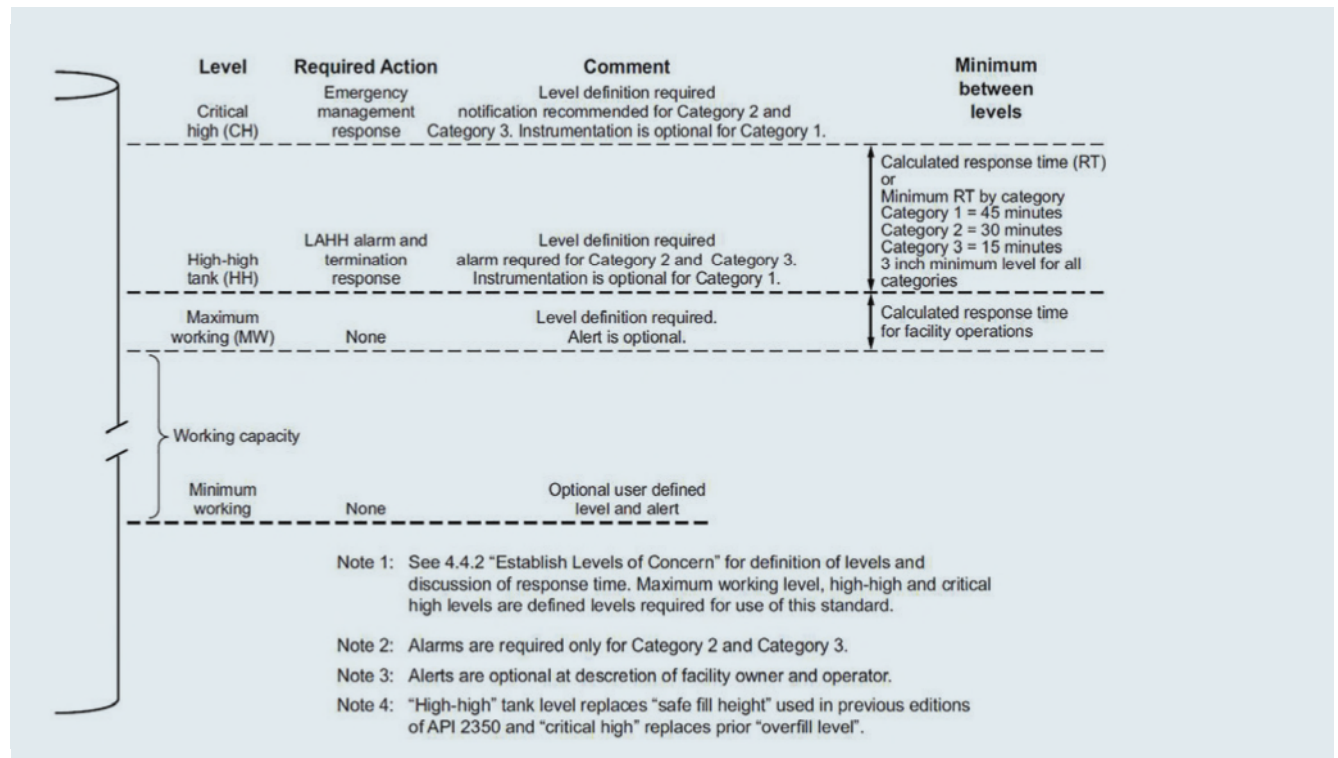


Figure 16: Levels of Concern without AOPS (API 2350 4th ed.)

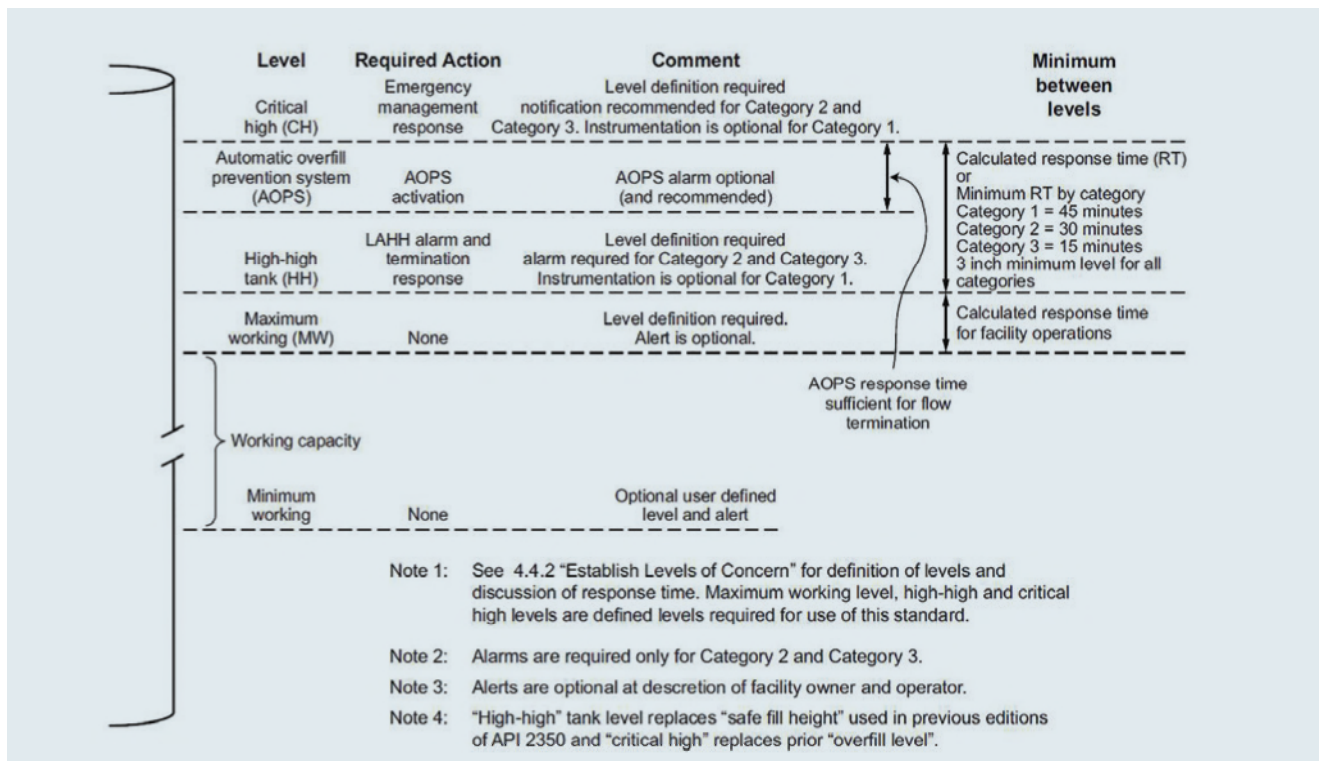


Figure 17: Level of Concern with AOPS (API 2350 4th ed.)

Operating Parameters

API 2350 refers to key variables related to the overfill prevention operation as operating parameters. These are:

- Levels of concern (LOCs)
 - Critical High (CH)
 - High-High (HH)
 - Maximum working (MW)
 - AOPS level (if used)
- Response times

Response times are composed of the time operations needs to detect and evaluate the alarm condition, the travel time to the control or valve, and any other delays such as severe weather or other conditions which could increase the response time. Because increasing response time is a trade off with tank capacity, making response times short is often the best choice in the owner/operators' perspective. But cutting the response time to a value that is too short is likely to lead to an overfill incident. Response times should be field tested and validated if a truly apt and robust response time is desired.

The owner should establish these various levels as a minimum. However, if the owner/operator is using alerts, then these could be added to the list of parameters and documented in the operating procedures as well.

Comprehensive Overfill Prevention

Eliminating Overfill Events

Preventing overfill events is vital to the continued normal operation of petroleum facilities and yields significant benefits to facility owners, operators, and the environment. Overfilling events can devastate a company, cause deadly explosions, and cause harm to the public. Implementing comprehensive overfill prevention can mitigate the likelihood of overfilling and the severity of a potential event. Comprehensive overfill prevention requires technological solutions and written response procedures. Alarms and sensors are only useful if personnel are trained to respond with the appropriate action.

The new practices urged by API 2350 can even improve normal operations and improve the efficiency at a facility. Improved operations are the result of specific, clear, and actionable procedures which

are understandable and accessible to operations. Removing uncertainty at facilities creates less variation in operations, creating an improved process. Efficiency of a facility may become improved because implementing API 2350 by also expanding the usable tank space using better equipment and procedures.

API 2350 includes details on comprehensive safety management rather than just listing safe technologies and procedures such as in older editions. A comprehensive safety management system is necessary to eliminate the risk of an overfill event.

Adding Value to Processes

Eliminating the risk of an overfill occurrence is one of the most sought-after and difficult to achieve objective from API 2350. However, additional benefits from API 2350 processes include improving safety management systems and operations procedures:

- Written procedures for normal, abnormal, start-up and shut-down operations reduces liability, improves safety, and reduces the downtime in processes
- Preventative maintenance and inspection fixes degradation in the tank and its components before a serious event, such as an overfill, can occur.
- Creating a regular Management of Change (MOC) procedure reduces risk by professional inspection and accounting for the changes and all the influences on upstream and downstream processes.
- Additional operable tank capacity is possible by adopting the current of API 2350.
- Having written practices and training for alarm response provides a robust human barrier and adds simplicity for operators.

Applying API 2350

Review of Overfill Management Systems

Preventing overfills requires two vital steps: recognizing the product level before it reaches critical high and terminating the product receipt prior to that event. Determining the level within a tank is usually done by some sensor and alert equipment. Level monitoring equipment is described in detail in this guidebook: Chapter 6 – Role of Instrumentation and Technology.

Terminating the transfer could mean turning off a valve, diverting the flow, closing the receipt valve, turning off a pump, or some other means of bringing the product receipt to a safe state without overfilling. The process of terminating flow requires a systematic approach and thorough understanding of the entire system. For more information please review Chapter 1 – Safety Management Systems and Management’s Role.

Overfill Management System Categories

API 2350 categories are only a way to simplify and group the many kinds of tank overfill prevention systems by key features. They cannot really be directly used for risk assessment. While it is true that the higher the category the lower the probability of an overfill, given all else is equal, the problem is “all else is equal”. Things are rarely, if ever, equal in terms of a given tank compared to another. This difference then makes it necessary to perform more sophisticated risk assessment methods rather than trying to screen risk based on category. In the Risk Assessment Section, we provide some tips about how to execute a risk assessment system for tank overfill systems, see Chapter 5 – Risk Assessment in this guidebook.

The use of tank categories also makes it easy to define what kinds of requirements should apply to a tank overfill system. For example, suppose that we have a Category I system which is entirely reliant on an operator to successfully terminate a receipt. Obviously, a Category I system should always be a fully attended operation and this is a requirement in API 2350.

Pipeline, refinery, vessel, and terminal operations utilize API 2350 to standardize the management of hazardous liquid containment and transfer. These operations include the use of a Category I, II or III system to monitor and control the transfer of hazardous liquids.

API 2350 requires that each tank be categorized according to one of the following systems:

Tank	Category 0	Category 1	Category 2	Category 3
System	Manual measurements (Hand-dip)	Local system (local gauge or ATG)	Local or remote system (ATG with alarming)	Independent systems (ATG and OPS)
Attention	Fully attended	Fully attended	Semi attended	Unattended
Operation	Local operation	Local operation	Local and remote operation	Remote operation

Figure 18: Categories by API 2350-4

Category I: A local or remote operator is responsible for terminating the receipt of product the flow of product as well as the remaining capacity or ullage in the tank. The operator monitoring the receipt should be in communication with the operator who may be transferring or terminating the receipt. High accuracy hand gauges may be used for custody transfers. What characterizes Category I tank receipts is that they are tank-local operations entirely under the control of an operator. There is a low limit to how many Category I tanks may be addressed by a single operator. Category I tanks systems are considered Manual Overfill Prevention System (MOPS).

Category II: A local or remote operator is responsible for terminating the flow of product by monitoring the level using tank gauges. The tank gauge must be equipped with an HLA. The alarm allows for centralizing the tank receipt data so that an operator can be more efficient in handling more tanks than would be possible for Category I tanks. However, the Category II tank has a critical weakness. The alarm function is not independent from the tank gauge and thus a failure of the gauge can cause a failure of the alarm. The characteristic feature of Category II tanks is that there is not an independent alarm. Category II tanks systems are considered Manual Overfill Prevention System (MOPS).

Category III: A local or remote operator is responsible for terminating the flow of product by monitoring the level using a tank gauge with a High-level alert system. The alert signals to an operator that an overfill will occur if filling operations are not terminated. Alerts bring awareness of a circumstance to an operator but do not legally require an actionable response. This category has an additional alarm, HHLA, that is independent and provides a more diverse and robust overfill prevention through increased reliability. In a Category III system the HHLA is redundant and independent of the primary alert system and tank gauging system. The HHLA can divert or terminate the receipt of liquid into a tank without any action by an operator making the system completely independent (redundant) to the operator/alert system.

AOPS (automatic overfill prevention systems): The termination of product flow is performed by an automatic control valve rather than an operator. It requires no human assessment, judgement, or intervention and is completely automated to trigger a receipt termination automatically. A point level sensor determines whether the level within the tank has reached a critical condition (Maximum Fill Level). Once the point level sensor is activated (liquid level has reached a critical high position) the sensor sends an output to a control valve or pump terminating the flow of liquid into the tank.

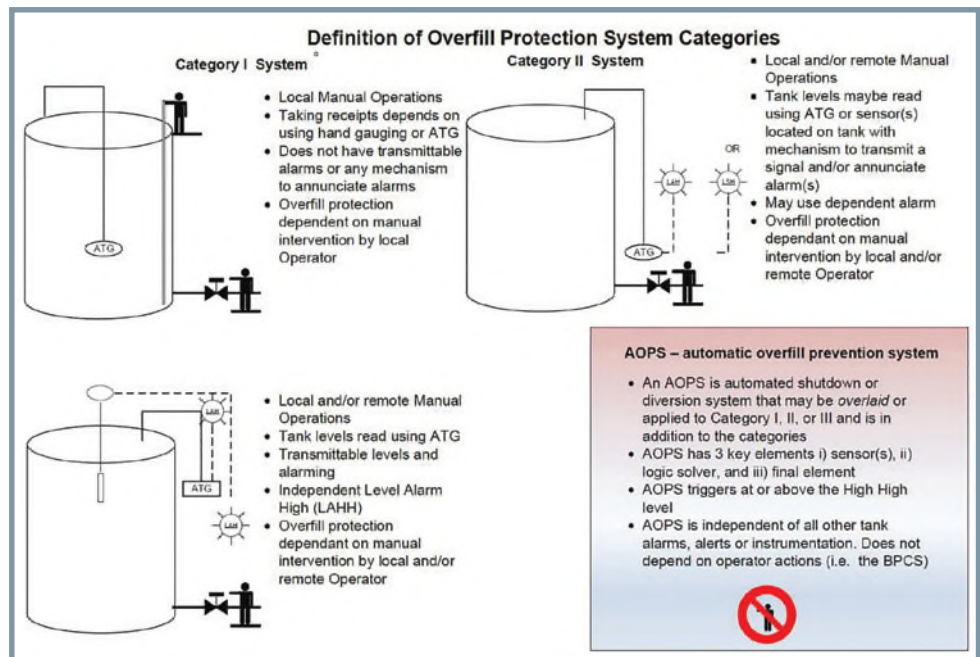


Figure 19: OPP Categories by API 2350-4

AOPS are supplementary systems, independent of the basic tank process operations which are normally used to terminate receipts. “LOPA” or “Levels of Protection Analysis” treats an AOPS systems as providing an additional barrier between normal operations and the overfill event, see Figure 12. AOPS can be thought of as an “insurance policy” for failure of the basic operations for a tank overfill system. If an AOPS triggers a receipt termination, then it is given that there was a failure or breakdown in the basic operations for that tank.

Redundancy in a system is the parallel arrangement of components which perform the same function. Therefore, if one of the components fails then a replacement is simultaneously able to compensate. An example for redundancy is the parallel arrangement of components which has a $\frac{1}{100}$ chance of failure. The probability of both the component failing simultaneously is then:

$$\left(\frac{1}{100}\right) \times \left(\frac{1}{100}\right) = \frac{1}{10,000} \quad \text{or } 0.01\% \text{ chance of failure.}$$

Diversity is another important aspect in the design of an OPP. For example, a float & tape gauging system poses the risk of a mechanical failure due to sticking, but will be uninfluenced by the loss of electrical power. Therefore, having a mechanical gauging system in addition to an electrical gauging system provides diversity in addressing the concerns of normal operating conditions and electrical failure conditions. Layers of protection should be diverse and account for a multitude of initiating risk events. The concepts of redundancy and diversity are applied to level gauging and control in Chapter 6 of this guidebook.

Chapter 5 – Risk Assessment

Why Overfills Pose Extraordinary Risk Levels

A tank has a finite and well-defined capacity. However, the volume of liquid that can flow into a tank may be many times larger than the tank capacity. In some circumstances if an overfill continues for an extended period, then not only would the spill volume exceed the tank capacity but even exceed the final barrier or protection layer, the secondary containment system or system of liquid containing walls that enclose most tank facilities. Because petroleum and chemical products usually have the potential for serious health, safety and environmental impacts and the amount of product stored is specifically intended to be maximized for optimizing processing, transportation or distribution operations, the hazards may be much higher than any other process or operation undertaken in a facility. The overfill event has proven capable of decimating entire tank farms.

New Existing Facilities Issues

The new-existing dilemma has been around a long time. Older facilities may be using equipment and operating practices that pre-date modern standards. The problem is that these older systems may be very hazardous and pose significant risk to the facility and to the public. It would be fair to say that no reasonable person or entity would require wholesale upgrades or modernizations to a facility without prioritizing those tanks that have the highest risk and then determining if that risk is acceptable or must be mitigated. This is the principle of grandfathering high risk existing facilities. A risk assessment drives the need for change to existing facilities, if any change is needed.

Difference Between Risk Assessment and Risk Management

Knowing what a company's level of risk and acting to reduce that risk portrays the difference between risk assessment and risk management. Risk assessment aims to determine likelihood and consequence of harmful events that threaten a company and its values. Just knowing what your risk level is does not help unless you can reduce those risks to what you or your stakeholders consider acceptable. It is through risk management that harmful events can be avoided or changed by actions or projects. To do effective risk management implicitly assumes that the risk assessment uses a valid approach that is timely, effective, auditable, explainable, and practical.

A robust risk management approach is an integral and important part of any management system. In terms of requirements for risk assessment and management, the range of regulations throughout the world vary tremendously from no requirements to very intense regulations such as those in the Americas, Asia, Africa and in Europe. The best roadmap of required principles for an effective safety management system are those principals embedded in the Process Safety Management regulations promulgated by OSHA. Although today most tank facilities are not subject to the Process Safety Management regulations (PSM), the principles should be applied regardless of regulation to minimize the likelihood of being surprised by a disastrous event.

Sidebar

Risk Factors Influencing Probability of an Event

Factors Influencing the Probability of an Overfill Event

The severity of an event is dependent on a corporation's values and unique situation.

- Reliability of level sensor(s)
- Existence and reliability of OPP (e.g. SIL levels)
- Number of fills, duration and amount transferred
- Overfill Management System and its reliability
- Calibration of the flowmeter
- Strapping tables accuracy
- Additional complexity due to:
 - process conditions
 - operator duties
 - multiple receipts

Factors Influencing the Severity of an Overfill Event

- Toxicity of the material spilled
- Rate of overfilling
- Volatility of the product
- Proximity to ignition sources
- Number of employees at the facility
- Proximity to neighboring communities
- Sensitivity of the surrounding environment
- Value of assets that could be damaged

As shown in Figure 20, effective process safety management and hence risk management requires safety leadership followed by the deployment of risk assessment and risk management processes. These are all processes and not tasks so that they are periodically reviewed and changed as needed. These processes are continuous and never-ending cycles.

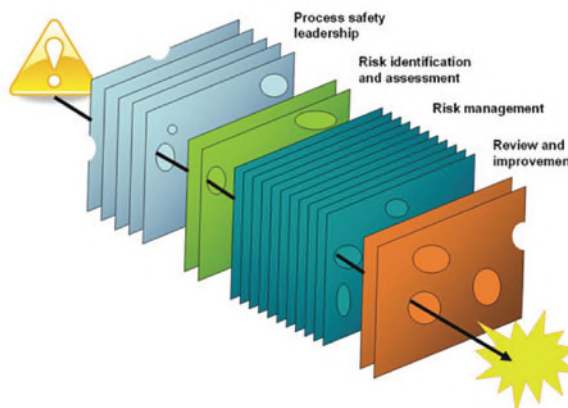


Figure 20: Ensuring Process Safety Using Principle of API 2350

API 2350 also requires that companies develop a risk assessment system. There is some level of risk associated at each tank because the filling rates are different, sensors have differing reliability and other factors influence the tanks. The likelihood of an overfill event requires tank specific information such as filling rate, previous spills or near misses and operator reliability. The other component of risk is the severity of the individual failure modes.

The probability of an event occurring is a unitless value between 0 (totally improbable) and 1 (totally certain to occur). The severity of an overfill event not only includes monetary loss but combines other values such as the statistical value of life, the environment, corporate reputation, etc. By monetizing the associated risk events, the failure modes can be compared in some convenient unit such as dollars. This method allows tank farm owners and operators to invest appropriately to reduce the facility risk in the optimal way. Understanding quantitative risk assessment and decision sciences allows facilities to make the best decisions to improve facilities and reduce risks of an overfill event.

API 2350 does not implement a specified risk analysis system because risk assessment methods and techniques are variable from one company to the next. One resource for those interested in developing a risk

assessment system is in IEC 61511-3 Part 3: “Guidance for the determination of the required safety integrity levels – informative” and IEC/ISO 31010 “Risk Management – Risk Assessment Techniques.”

Risk Assessment Screening

Risk assessment as a requirement for overfill prevention requires a carefully considered and systematic approach. If a tank facility owner has only one or two tanks then the risk problem is straight forward. However, if the tank facility has hundreds or thousands of tanks then a more strategic approach is needed just to deal with the resources and time required to make a dent in the risk assessment process. Moreover, if the facility owner wants to accomplish a specific management objective such as complying with the current edition of API 2350 within a specific period, say 5 years, then it is essential to formulate a strategy that ranks and prioritizes risks for accomplishing this goal.

In a complex environment such as those portrayed in API 2350 for overfill prevention, everything can’t be assessed or measured at the same time; data collection, assessments and risk assessment resources must be prioritized. It is obvious that most effective approach would be to perform the most important assessments first – those addressing the most important threats first. Prioritizing risk assessment or risk screening studies are the quickest way to get to those actions that reduce larger or more imminent risks first. Before providing an approach, we discuss the common use of risk assessment matrices and their role in risk assessment and risk management.

Risk matrices are a common tool often used to summarize risks which serve as a basis for discussion of risks and risk management at all levels within organizations. This graphical presentation of risks is typically denominated in two dimensions: one of estimated likelihood or frequency and the other of impact to the organization, often measured in financial units. The events (a tank loss of containment, for example) are typically shown as individual dots plotted on the likelihood and consequence axes, usually representing either a worst case or sometimes a most likely case. The coordinate space is sometimes broken into differently colored squares to indicate distinct levels of priority. API 580 discusses the principles of risk assessment in general and addresses the use of risk matrices.

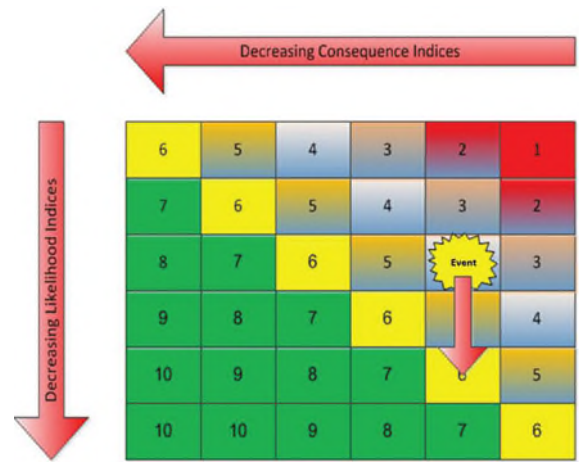


Figure 21: Risk Assessment Matrix 6x6

The matrix-like structure is useful for high-level summaries of risks but cannot easily be used to help inform management about the best decisions to make for resource allocations for risk reduction. As an aggregation tool, matrices aid in graphically showing relative risk and organizational priorities in a rectangular prioritization scheme. The step to an improved resolution in characterizing risks must be done in a separate way from risk matrices, typically, for some of the following reasons:

- Risk matrices do not show the range of what can happen because at any given event on the chart, only the worst case or most likely case – usually the worst case (an event, an overfill for example, can result in a range of outcomes, not just one: no loss of contents, a small release, a large but contained release, a large and uncontained release, no impacts, major impacts, etc. This detail is lost in risk matrices.)
- Risk matrices don’t provide a template for evaluating mitigations of events on the graph. This is often a separate and different activity.
- They don’t account for correlation and dependencies among risk events; at least at the graphical level, they are treated separately and as independent.
- They are not useful for semi-quantitative or quantitative risk analyses.
- They are not useful for comparing risk tolerability of different events on a common basis or impacts of distinct types other than “consequence” in a single metric (often estimated cost or, in some settings, estimated lives lost from the incident). Other types of consequences are handled more informally.

Logical Structure of Risk Assessment

There are two technical issues typically guiding risk assessment activities: what information to collect and how much information to gather. In simplest form, something like a starting rule (where to start measuring and what to measure) and something like a stopping rule (when is there enough information to finalize a decision). Missing on either of these issues makes the information gathered and organized by risk assessors less valuable as an aid to the organization's resource allocation decisions.

Since risk is about threats to things an organization values, as mentioned earlier, risk assessment starts by focusing not just on events – but more importantly on values. An uncontrolled release of the contents of a tank is an event; it is not of interest to risk assessment unless that release adversely impacts things the organization values. The seriousness of that release – that is, the level of risk that is associated with that event – depends not directly on its size but on what it impacts and how severely; a large release in a non-sensitive area that has insignificant impact is less risky than a small release in a highly sensitive area. Most events that adversely impact an organization's values impact more than just one value. Consequences may include adverse impacts on the health of people nearby, the nearby environment, the firm's financial performance, its regulatory compliance, corporate reputation and more.

Risk assessment must be structured around a clear description of the organization's values. This clarity comes from the senior management of the organization: What are the organization's strategic objectives? What are its core values employed in pursuing those objectives?

Risk assessment focuses on the key things to measure; secondly, risk assessment gathers just enough information to support the decision makers and the decisions they must make. It is a means to an end. Too much information is a waste of energy and money, but more importantly, key personnel and time. The information could have been made available earlier and key personnel assigned to other valuable activities.

Some organizations avoid designing their own risk assessments by relying on third-party decision making by trusting compliance with regulatory requirements or industry guidelines. This practice, however, does not consider all the of an organization's specific objectives, values, and unique operating threats. Without the

guidance of specified organizational objectives, it is difficult to design effective risk assessment: it isn't clear where to start, what most needs measurement, or when there is enough information gathered for quality decision making on allocation of resources.

To summarize these two basic defining features of risk assessment:

- By defining the organization's strategic objectives, senior management is directly involved in identifying where and how to focus risk assessment activities in support of risk management decision making.
- Identification of the management decisions (size of budgets, personnel allocations, changes in equipment or policy and procedures, etc.) influences the scope of information gathering.

Risk Screening Example

There are many references¹¹ on how to perform risk analysis with varying degrees of accuracy and usefulness. There are many ways to perform risk assessments and each has its pros and cons. Moreover, each company must develop the individualized styles and methodologies for executing risk assessments. Therefore, the intent of the examples here is not to influence the nature or method of executing risk assessments. The examples are simply meant to serve as a starting point for how a company might approach the problem as a "first pass" on risk ranking tanks for overfill potential.

The first order of activity is to set the scope of the risk assessment: Will risks other than those arising from tank overfills be addressed? Is facility security to be included as part of the risk scope? Even if the focus is a risk assessment specific to tank overfills, then there are many issues related to setting the scope and extent of the risk assessment, as shown in Figure 22, which might apply to an integrated oil company.

An integrated oil company will have different organizations and operational centers to consider in the risk assessment. If the risk assessment arises in one of the operating companies then they may not have control over the information, assessment and management of the risk process needs across organizations, then the challenge will be to set clear boundaries and interfaces. Often, as demonstrated by Figure 22, there are various equipment, operational and procedural overlaps at the interfaces of the various operating companies. From an efficiency and effectiveness perspective it is always better if the

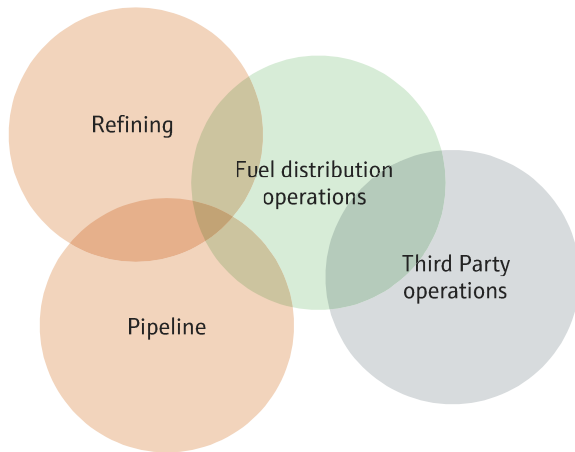


Figure 22: Defining the Boundaries and Scope of the Risk Assessment

risk assessment is lead at the direction of top senior management so that intracompany disagreements do not become the highlight of the process.

A “first pass” ranking of risks based on organizational objectives can be qualitative and provide more efficiency in risk assessment by focusing data collection and analysis on those tanks that provide the greatest exposure to the organization’s objectives. Once the higher-risk tanks are identified, then more precise estimates can be made to support decisions about more costly or intensive risk assessment methods.

For example, a first pass analysis might separate all storage tanks storing Class 1 liquids (gasoline, octane, etc.) from those storing higher class liquids (diesel, jet fuel, etc.) As another example, a company may categorize those tank operations that are legacy and under its direct control, but create another group of tank and terminal operations that are joint ventures which are not under their direct control. How a company prioritizes its risk analysis program is dependent on the corporate values and unique situation. A company should use subject matter experts to identify the most effective way to attaining the risk analysis data and develop the scoring metrics to meet the corporate goals (less risk).

Rank ordering is a common technique that can be done in several ways. The overall process is illustrated here using an example of managing operating risks for a simplified group of three tanks.



Figure 23: Risk Assessment Flowchart

¹¹ International Electrotechnical Commission (IEC) 31010:2009 Risk Management – Risk Assessment Techniques
 ISO 31000 Risk Management
 IEC 61508 Functional Safety
 IEC 61511 Safety Instrumented Systems and many more

Step 1: The surveyor¹² specifies the tank attributes or factors related to rising operational risks.

Assume the organization's objectives have been specified as financial performance, employee and public health and safety and environmental protection. In addition, their relative importance has been determined as well. A subject matter surveyor (engineer, the tank manager, or other personnel) then determines the ways (scenarios) in which the tank could fail and their contributions to the likelihood of failure. For this example, the following failure likelihood and magnitude factors are used:

- Tank rate of rise and flow rates
- Type of instrumentation and controls
- Operational capability

Step 2: Likelihood scale: the surveyor specifies a likelihood scale and metric.

As an example, this can be a scale (for a first-pass model) that can be used for all attributes and isn't specifically tailored for each attribute:

Levels of contribution to a tank overfill	Metric (Score)
De minimus	0
Minor contribution to overfill	.1
Ordinary or average contribution to tank overfill	.3
Above average contributor to tank overfill	.6
High contributor to tank overfill	1.0

Note: the metric for likelihood contribution is not a probability estimate or a frequency estimate but a representation of the relative contribution to the failure of a tank. The metric can be represented by any number on any scale. For convenience, we illustrate the metric on a scale of 0 to 1.

Step 3: Consequence scale: the management, representing the organization's objectives, specifies a consequence scale and metric.

As an example, this can be a scale (for a first-pass model) that can be used for any attribute that impacts the potential for the severity of the incident:

Consequence	Metric (Score)
Little to no impact	0
Minor business impact	.15
Middle range impacts	0.8
High impact	1.0

¹² Surveyor is meant to be one or more persons who serve as knowledgeable people about the process, equipment, operations, procedures, and methods of operating the tanks for overfill prevention. Surveyors can include both internal personnel and consultants.

Step 4: Relative likelihood: the surveyor scores each tank on each attribute using the likelihood scales. For the three tanks (A, B, and C).

Factors:	Tank A		Tank B		Tank C	
	Value	Score	Value	Score	Value	Score
Rates	Minor	0.1	High	1	High	1
Instrumentation	Average	0.3	High	1	De minimus	0
Operations	High	1	Average	0.3	Minor	0.1

Step 5: The surveyor checks for dependencies between factors in scoring.

Correlation is not a significant problem at this level of scoring (for example tank diameter and tank capacity could be listed together as factors affecting the potential overfill size even though they are highly correlated). The surveyor, knowing the dependencies, can adjust the score for appropriate representation in the table of relative likelihood.

For example, if additional factors were considered such as time since last inspection or level of automation as contributors to the likelihood of a failure, the impact of time since last inspection is less important for a new tank overfill system than it is for an older tank.

The factors contributing to likelihood of failure can be adjusted for these interactions by including “interaction effect” factors so that the impact of “time since last inspection” on likelihood is a function of the “age of the tank overfill system” in the likelihood estimate model.

In addition, the relative contribution to overall likelihood of failure from each factor is weighted by the surveyor; in this example all the factors are considered to contribute equally to the likelihood of a tank failure, but weighting adjustments can be made for fine tuning the relative likelihood of overfill scoring.

Step 6: Consequence scoring: Managements representation of relative impact of consequence proxy scoring are developed next.

Factors:	Tank A		Tank B		Tank C	
	Value	Score	Value	Score	Value	Score
Flammable	No impact	0	High	1	High	1
Public	High	1	High	1	De minimus	0
Environment	Middle	0.8	Middle	0.8	Minor	0.15

Step 7: Summary risk score: Tank ranking by relative risk: aggregate likelihood score × aggregate consequence score

For this simple model, it is assumed that the likelihood factor scores are additive (they combine to impact likelihood in an additive fashion) and the consequence factor model is also additive. These models are determined by the subject matter surveyors based on their knowledge of tanks and experience in managing and inspecting tanks. The aggregate model could be multiplicative or could have interaction factors. There are ways to determine this structure empirically, but here it is assumed it is additive.

The mathematical approach to the chart below is to multiply the factor weight by the score. This is done for both the likelihood factors and consequence factors. Each of these values are summed to get a relative likelihood and relative consequence for each tank. The relative likelihood and relative consequence values are multiplied. The calculation method for tank A is provided below:

Tank A Example:

Likelihood Factors:

$$\begin{array}{ll} \text{Rates} & \text{Factor weight} \times \text{Likelihood score} = 0.4 \times 0.1 \\ & = 0.04 \end{array}$$

$$\begin{array}{ll} \text{Instrumentation} & \text{Factor weight} \times \text{Likelihood score} = 0.3 \times 0.3 \\ & = 0.09 \end{array}$$

$$\begin{array}{ll} \text{Operations} & \text{Factor weight} \times \text{Likelihood score} = 0.3 \times 1 \\ & = 0.3 \end{array}$$

Relative Likelihood:

$$\begin{array}{l} \text{Relative Likelihood} = \text{sum (weighted likelihood factors)} = 0.04 + 0.09 + 0.3 \\ = 0.43 \end{array}$$

Consequence Factors:

$$\begin{array}{ll} \text{Flammable} & \text{Factor weight} \times \text{Consequence score} = 0.25 \times 0 \\ & = 0 \end{array}$$

$$\begin{array}{ll} \text{Public} & \text{Factor weight} \times \text{Consequence score} = 0.45 \times 1 \\ & = 0.45 \end{array}$$

$$\begin{array}{ll} \text{Environment} & \text{Factor weight} \times \text{Consequence score} = 0.23 \times 0.8 \\ & = 0.184 \end{array}$$

Relative Consequence:

$$\begin{array}{l} \text{Relative Consequence} = \text{sum (weighted consequence factors)} = 0 + 0.45 + 0.184 \\ = 0.634 \end{array}$$

Total Relative Risk:

$$\begin{array}{l} \text{Total Relative Risk} = \text{Relative Likelihood} \times \text{Relative Consequence} \times 1000 \\ = 0.43 \times 0.634 \times 1000 \\ = 273 \end{array}$$

		Tank A		Tank B		Tank C	
Factors:	Factor weights:	Value	Score	Value	Score	Value	Score
Likelihood Factors							
Rates	0.4	Minor	0.1	High	1	High	1
Instrumentation	0.3	Average	0.3	High	1	De minimus	0
Operations	0.3	High	1	Average	0.3	Minor	0.1
Consequence Factors							
Flammable	0.25	No impact	0	High	1	High	1
Public	0.45	High	1	High	1	De minimus	0
Environment	0.23	Middle	0.8	Middle	0.8	Minor	0.15
Rel likelihood		0.43		0.79		0.43	
Rel consequence		0.634		0.884		0.2845	
Total relative risk		273		698		122	

The relative risk scores show that Tank B is the most at risk. This is a result of the high likelihood of failure combined with the high consequences.

This structure allows the evaluator to see the contributors to likelihood, the contributors to consequence, how consequence is defined and scored, and the reason that Tank B has the highest risk of these three. This is the “audit trail.” If someone disagrees that Tank B has the highest relative risk of the three, they would need to show how either relevant risk factors are not included or the factors are not evaluated correctly (or are combined in

the wrong fashion). This focuses the discussion on relative risk and makes it value driven.

When this approach is applied across a very large organization with, say, hundreds of tanks, a basic relative risk assessment process can be constructed based on that organizations empirical data and expert judgment on both the risk factor contributions to an event as well as the factors contributing to the consequences of an event. The company management would also specify the objectives they care about their relative importance.

The scores are between 0 and 1.0, as the three-tank example above, but are multiplied by 1000 to expand the scale for the graph comparing tank relative risk scores as shown in Figure 24.

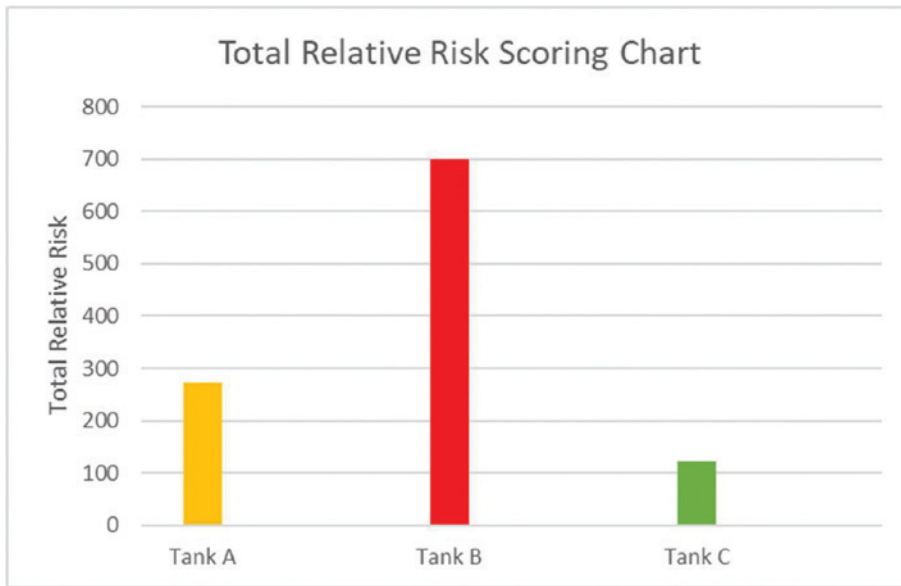


Figure 24: Total Relative Risk Scoring Chart Example (green-best to red-worst)

When a risk assessment process is applied across all of company's tanks, it can be used to yield a ranking of the tanks by this relative risk (scale 0-best to 1000-worst), as shown in Figure 25.

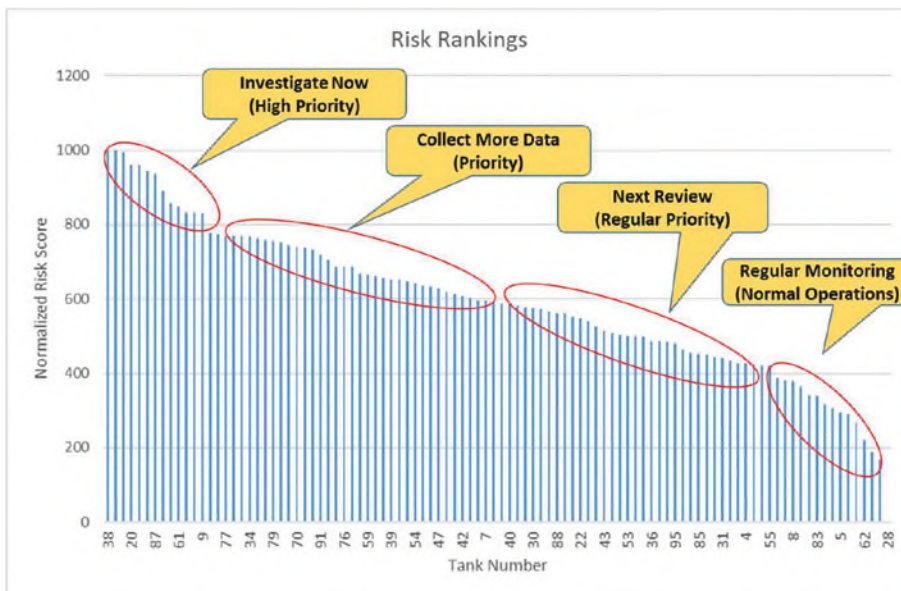


Figure 25: Example Ranking of Tanks by Relative Risk (0-best to 1000-worst)

This ranking was done using the method described previously. Such a ranking by relative risk based on empirical data plus judgmental assessments by a team of knowledgeable tank professionals and surveyors can be an aid for identifying, as illustrated above, where to start more detailed risk assessments. Note that each one of the likelihood and consequence metrics can be developed using in house or industry data.

Chapter 6 – Role of Instrumentation, Systems and Technology

Introduction and Motivation

Here we cover the fundamental principles of liquid level measurement and how liquid level measuring systems are applied to tank storage. A simple and important operation for companies that use liquid storage tanks is the measurement of the liquid level within a tank. Making a liquid level measurement in a tank is called tank gauging. When an operator makes this measurement manually by use of a measuring tape or electronic hand line, it is called manual gauging. Making a manual measurement requires the operator to climb to the top of the tank, open a port or hatch that has line of site to the liquid, and drop a measuring device such as a weighted tape measure directly into the liquid.

When the measurement is made by permanently fixed tank instrumentation, it is called automatic tank gauging. Automatic tank gauging (ATG) can provide continuous level measurement and record the level changes with time. ATGs can transmit the level data to remote locations but this feature is not always used. The measurement can usually be read at the side of the tank at grade level but is also commonly transmitted to a central control room where all tank measurements are readily available on computer display screens. The requirements for tank gauging are specified in the API standards and the key points will be covered in the appropriate sections. API MPMS Chapter 3.1A¹³ covers manual tank gauging and API MPMS Chapter 3.1B¹⁴ covers automatic tank gauging. These are the most widely used tank gauging standards in the petroleum industry.

The product level is the distance between the reference point at the bottom of a tank to the product level. The level within a tank determines the volume of product within the tank, and this information is required to safely fill tanks, execute customer orders, and inform production of the demand.

The level measurement also fulfills an important alternative role of controlling the risk of overfilling. Overfill events can range from a simple clean up to a vapor cloud explosion. Overfill events endanger a company, their personnel, the environment, and the petroleum industry. The technology available

to monitor the level within a tank has improved significantly since the dawn of the oil industry with ever improving instrumentation reliability.

Tank Gauging Systems

A tank gauging system measures and displays the level within a tank. Modern systems automatically calculate the volume of product from the liquid level. Crude oil and other petroleum products are traded by volume, so the measurement of level is integral to business transaction accuracy. A tank gauging system is necessary at facilities or plants for inventory management and custody transfers. Inventory management is the internal corporate audit of the volume or mass within a tank or tank system. Custody transfer is the purchase and transfer of liquid between parties. Both custody transfers and inventory management have standard accuracy requirements discussed in API MPMS 3.1A&B, the European MID Directive, or comparable national standards documents.



Figure 26: Example of a Tank Gauging System

Tank gauging systems are employed in large storage tanks, pipelines, depots, refineries, airports, power plants, chemical plants, mines and elsewhere. A tank gauging system is typically capable of measuring the liquid level, temperature, pressure, and water bottoms

¹³ Manual of Petroleum Measurement Standards Chapter 3.1A. Standard Practice for the Manual Gauging of Petroleum and Petroleum Products – 3rd Edition (2013).

¹⁴ Manual of Petroleum Measurement Standards Chapter 3.1 B. Standard Practice for Level Measurement of Liquid Hydrocarbons in Stationary Tanks by Automatic Tank Gauging – 3rd Edition (April 2018).

(thickness of the water layer at the bottom of the tank). Peripheral equipment to tank gauging systems includes communications technology, computer hardware and software and wiring/signaling. The water and oil levels, temperature and pressure data are necessary to calculate the corrected or standardized volume of fluid within the tank.

Gauging systems support functions related to inventory control, custody transfer and overfill prevention. Custody transfer tank gauge systems are used to

calculate the net volume of oil which enters or exits a tank. Customers are billed based upon the standardized net measured volume of oil transferred, therefore the sensing technology must be very accurate. Failure to accurately gauge and bill for a transfer can result in lawsuits, loss of revenue and loss of consumer confidence. Government authorities or intercompany contractual arrangements hold jurisdiction over typical custody transfer standards such as API MPMS 3.1A&B and the European MID Directive and they are usually based upon the country of operation.

Sidebar

Brief History of Tank Gauging

At the beginning of the oil industry in the 1860s, the accuracy of level measurement was very poor. Customers were growing concerned that they were being overcharged for the volume of oil purchased. In order to maintain consumer confidence, oil companies agreed to create the standard 42-gal barrel. Although the volume is 42-gal, oil companies agreed to charge customers at the rate of 40-gal per barrel to compensate for spillage, evaporation, and measurement error.



Figure 27: Standardized 42-gal Barrel

In the 1960s the accuracy of custody transfer was $\pm 0.5\%$. This error was attributed to error in temperature measurement, sampling, and other factors. The accuracy was built into the API standards of the time. This meant that the purchaser of the crude oil was losing a barrel for every 200 barrels purchased. This became an extreme concern in the 1970s due to the dramatic increase in the price of crude oil. The increased price per barrel pushed the petroleum industry to adopt new methods, the API Manual of Petroleum Measurement Standards (MPMS). This method of transfer practice has an accuracy of 0.25%. MPMS protocol has been revised several times since its conception.



Figure 28: Bloomberg WTI Crude Oil (2013-2018)

Innage vs. Ullage Measurements (Liquid Length vs. Empty Length Measurements)

An innage measurement extends a sensor or tape through the entire vertical distance of the product at the tank bottom to surface of the liquid level. A dipstick in an engine is a simple analogy for an innage measurement. Innage gauging is a direct liquid level measurement but it does have some drawbacks. It may

be impractical if the liquid is highly viscous. Another inconvenience of innage gauging is the tape can be coated with sticky oily products that must be cleaned when reeled in. This can also pose a potential hazard to tank operators.

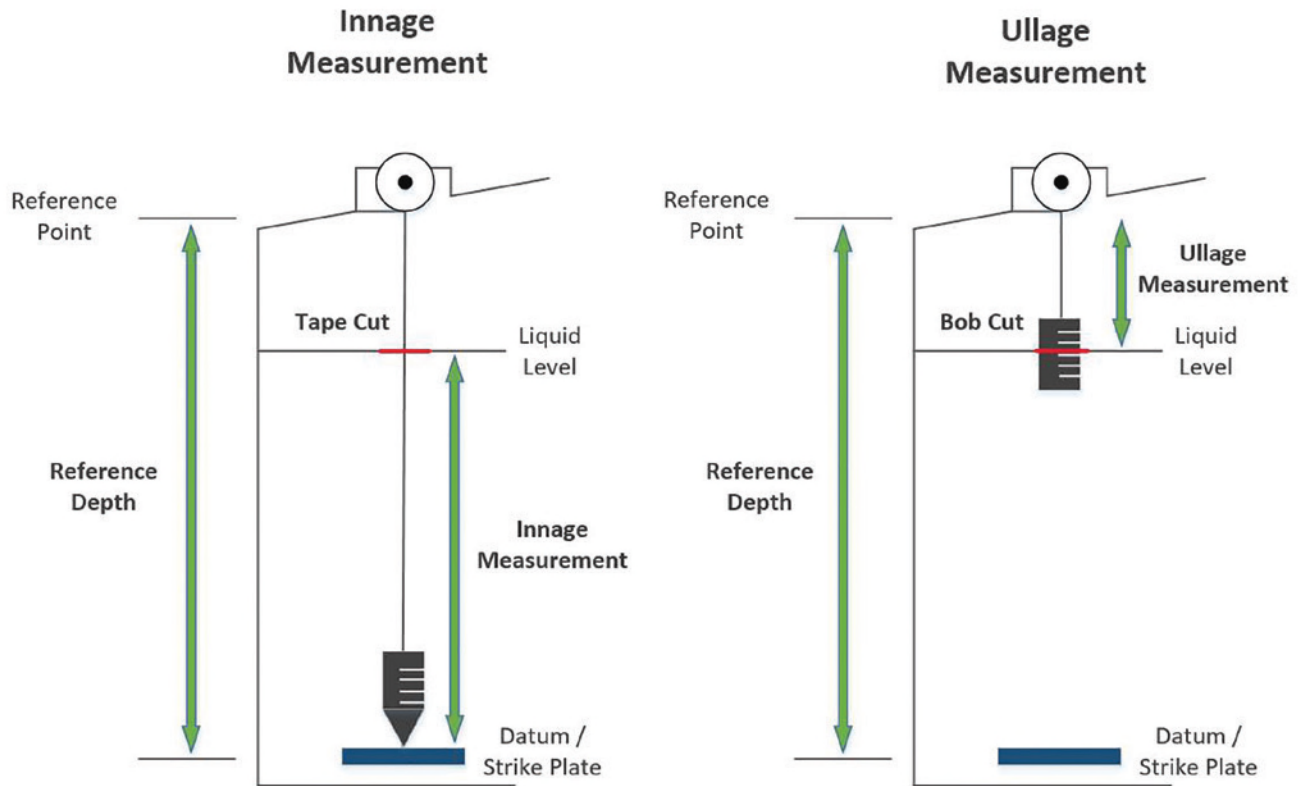


Figure 29: Innage & Outage (Ullage) Diagram

$$Reference\ Depth = Innage + Ullage$$

$$\therefore Innage = Reference\ Depth - Ullage$$

An ullage measurement is the measurement of empty air space as a vertical measure from a fixed point usually located on the tank roof to the liquid surface. The reference point is the uppermost measurement point in a manual tank level measurement. The reference point is usually a metal slit or extension inside the gauge hatch at the top of a tank.

The innage measurement is the difference between the datum plate (strike plate) and the top of liquid surface. A datum plate is a metal extension that is attached above the tank bottom and underneath the reference point. The liquid volume in the tank is inferred by measuring the difference in ullage to obtain the change in liquid volume.

Level and Mass Measurement Technology Concepts

Both innage and ullage measurements use the simple distance measurement to relate it to the concept of volume in a cylinder and its relationship to the height of the liquid column. Most of the information contained in API Chapters 3.1A and 3.1B are based on this principle.

A different technique for determining the amount of product within a tank is based upon the product mass and its effect on pressure at the base of the liquid column. API Standards governing this type of measurement are covered by a section in API Chapter 3.6 and 16.2. Mass measurement techniques use the hydrostatic pressure created by the vertical column of product liquid above the sensor or pressure gauge. The hydrostatic pressure is then related to the stored liquid volume through the density.

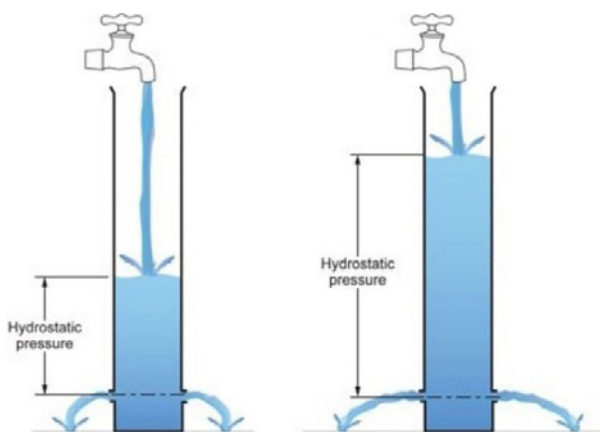


Figure 30: Mechanism for Hydrostatic Pressure Due to Liquid Column

Level measurements directly determine the amount of product within a tank, whereas mass measurements are a measurement of pressure. If density is known, then pressure can be used to determine level which allows for determination of the volume within a tank.

Manual Tank Gauging

Manual tank gauging is accomplished when an operator measures the product level and the water bottoms from the top of a tank. The measurement can be done either with non-electronic measuring tapes or by portable electronic liquid measuring devices. There are some hazards associated with manually tank gauging. For additional information regarding safety and manual gauging see Side Bar – Safety Concerns of Manual Tang Gauging. The measurement must occur from a fixed reference point from the top of the tank, account for temperature of the petroleum and water phases and account for water bottoms depth. The process of manual tank gauging is specified in API MPMS, Chapter 3.1A, “Standard Practice for the Manual Gauging of Petroleum and Petroleum Products”¹³. The scope of API MPMS, Chapter 3.1A is limited to the manual gauging of aboveground storage tanks which apply to API 2350-4. This includes the use of portable electronic gauging technology (PEG).

Chapter 3.1A describes:

1. Procedures for manual gauging of atmospheric flat-bottom vertical cylindrical tanks.
2. Methods applied when there is a need to measure water bottoms or sediment and emulsions that may exist at the bottom of the tank.
3. Methods to verify the accuracy of the measuring devices being used.
4. How the accuracy is affected by the selection of the reference and datum points.

Variables

- Innage level**
- Water/sediment bottoms level**
- Ullage level**
- Temperature of both phases**
- Tank dimensions – provided by the manufacturer**

The bold type indicate the variables as they appear in the Manual Level Measurement Process section below. Also, Figure 29 shows the measurement point locations referred to in Details of Manual Level Measurement.

Open gauge is the liquid level prior to a custody transfer. Closing gauge is the liquid level after a custody transfer. The difference in liquid level before and after a transfer is used to verify or quantify the amount of petroleum transferred or sold. An example of open and closing gauge are displayed on Figure 31, the liquid levels would be reversed if the tank was receiving liquid.

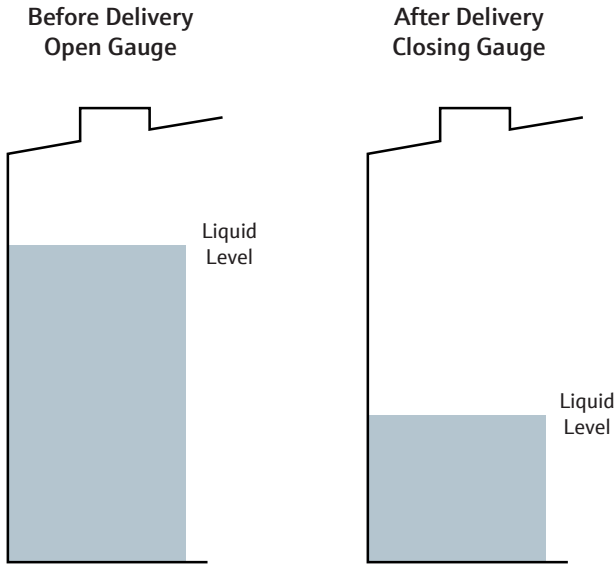


Figure 31: Open and Close Gauging Diagram

Details of Manual Level Measurement Process

Discover the Reference Point (Mark)

The reference point is a position near the top of the tank which is used for accurate level gauging. The reference point is usually a fixed plate inside the gauging hatch, a groove cut horizontally inside a gauging hatch, or the edge of a fixed metal arm that is not in contact with the gauging hatch. See Figure 29 and Figure 32 for an example of reference point.

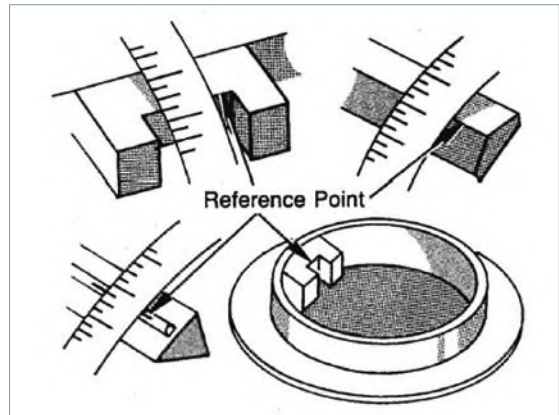


Figure 32: Reference Point Diagram

Determine the Reference Height (Depth)

The reference height is the length from the reference point at the top of the tank to the datum plate at the bottom of the plate. Measuring the reference height requires an operator to lower a tape gauge from the reference point to the datum plate and record the length. See Figure 29 and Figure 33 for an example of reference depth/height.

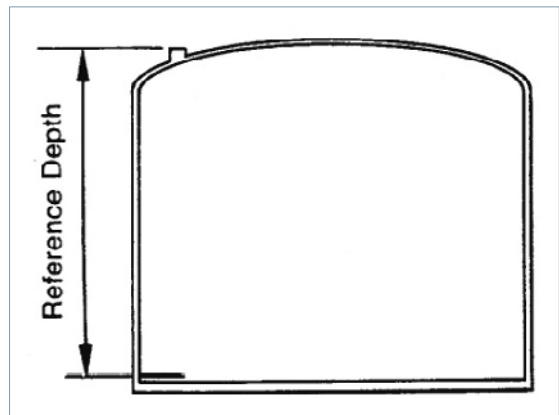


Figure 33: Reference Depth Diagram

Datum/Strike Plate

A datum plate is a metal plate attached to the tank shell or bottom that is located below the reference point. The reference point and datum plate create a straight, unobstructed line that is useful for manual tank gauging. Although the bottom is sometimes used, the bottom can build up sludge and cause error measurement. In addition, the bottom tends to flex and settle over time and so would lead to inaccurate measurements. See Figure 34 for an example of a datum/strike plate.

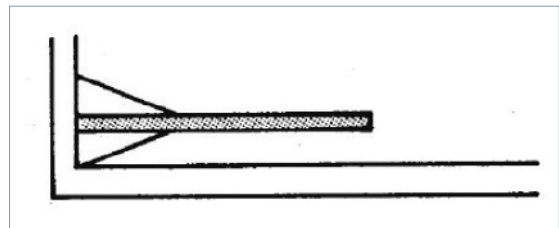


Figure 34: Strike Plate Diagram

Measuring the Cut (Total Liquid Level)

When using a measuring tape, a first step in the process is to apply an oil paste, or paste to the tape which dissolves or changes color in petroleum, at the expected product position on the manual tape.

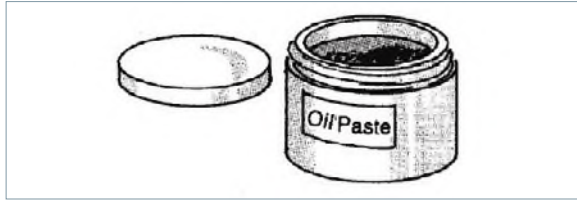


Figure 35: Oil Paste (determine the Product Cut)

The reference height, see Figure 29, is the length of the tape and bob from the reference point after striking the datum plate. The height between the datum plate and product cut is the **Product level***. The **Ullage level***** is the height between the reference point and the product cut. See Figure 29 for an example of product cut and see Figure 29 for an example of ullage and innage.

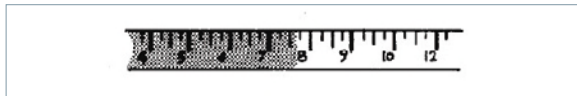


Figure 36: Product/Water Cut

An operator will then slowly unreel an innage tape and bob (Figure 37) or Portable Electronic Gauge (PEG, Figure 38) into the product through the gauge hatch while the tape lies along the reference point, see Figure 29. A PEG is an electronic tool sometimes used to manually gauge the level in a tank. The PEG bob is lowered into the product and displays the length on a digital display. When the bob strikes the datum plate, see Figure 29, the operator should slowly reel up the tape. The height of the product liquid should create a clear line on the oil paste, called a product cut, see Figure 36.



Figure 37: Example of Manual Gauging Tape and Bob



Figure 38: Example of Portable Electronic Gauge (PEG)

Gauging standards are set by Manual of Petroleum Measurement Standards Chapter 3.1A¹³. The standard requires two identical consecutive measurements of the cut or three consecutive measurements within 3 mm of each reading. Manual gauging measurement requirements are summarized in Figure 39. A minimum of 2 measurements are required and if they are the same, then the reading is recorded. If they differ, then three trials are conducted (within 3 mm) and the readings are averaged. The equation for averaging level measurements is provided below:

$$Level_{Avg} = \frac{\sum Level_i}{i_{total}}$$

Number of Level Measurements	Accuracy Requirements
2	Both trials are the same
3	Each trial within 3 mm

Figure 39: Manual Gauging Requirements by API Chapter 3.1A¹³

Measuring Water and Sediment Bottoms

A first step, if water bottoms exist and will be measured, is to apply a water finding paste, or paste which dissolves or changes color in water, at the expected water position on the bob of the manual tape. The paste should not be soluble in the product. The **Water/sediment bottoms level**** is the height between the datum plate and the water cut.

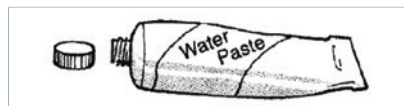


Figure 40: Water Finding Paste (determine the Water Cut)

Temperature Gauging

Determination of temperature, density, API gravity, suspended sediment and water are not addressed by Chapter 3.1A or 3.1B. These requirements are established in API Chapter 7 and the appropriate requirements from this standard are covered here as relevant to tank gauging.

The minimum number of temperature measurements that are required per liquid level based upon Figure 41. The temperature of each layer, usually water and product layers, must be measured separately and recorded.

Depth of Liquid	Minimum Temperature Measurements	Measurement Level
> 10 feet (3.05 meters)	3	Center of upper, middle, and lower thirds
≤ 10 feet (3.05 meters)	1	Center of Liquid

Figure 41: Minimum Number of Temperature Measurements Based on Height of the Liquid by API Chapter 3.1A¹³

For example, if the **Water/sediment bottoms level**** is 2 ft. in height then the water layer would require one temperature measurement. If the **Product level*** is 25 ft. in height then the product layer would require three temperature measurements. This concept is displayed in Figure 42.

Temperature Measurement Example

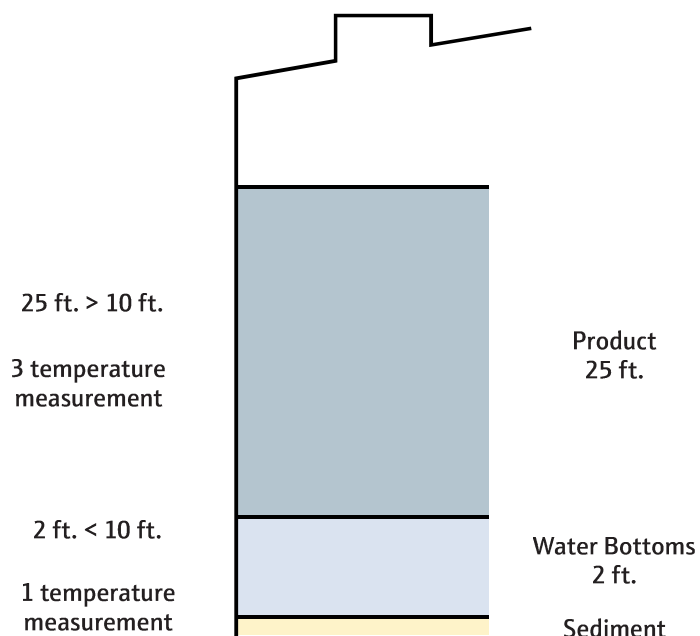


Figure 42: Temperature Measurement Example Diagram



Figure 43: Multipoint Prothermo NMT539 for average temperature measurement

Once the operator has determined the necessary number of temperature measurements per phase and knows the levels of those phases, they can begin to take temperature measurements using a Cup-Case Thermometer, Armored Case Assembly, Angle-Stem Thermometer, or Portable Electronic Thermometer (PET) to take measurements.

Portable electronic gauges (PEGs) should be calibrated or tested prior to use for inventory management or custody transfer purposes under the requirements of MPMS Chapter 3.1A¹³. The should be made in accordance with ASTM E-1.

The general specifications for each type of PET tank thermometer is provided below in Figure 44:

Name	ASTM Thermometer	Range	Length (inches)	Graduation	Accuracy
ASTM Tank	50°F-80°F	-30°F to +120°F	12	1°F	±0.5°F
ASTM Tank	50°F-80°F	0°F to +120°F	12	1°F	±0.5°F
ASTM Tank	50°F-80°F	0°F to +180°F	12	1°F	±0.5°F
ASTM Tank	50°F-80°F	60°F to +180°F	12	1°F	±0.5°F
ASTM Tank	50°F-80°F	170°F to +500°F	12	1°F	±0.5°F
Angle-stem	~	Suitable Range	12	1°F	±0.5°F
Tank thermometer	~	20°F to +220°F	12	1°F	±0.5°F

Figure 44: General Specifications by Thermometer Type

The immersion time is dependent on the thermometer type and the API gravity of the liquid temperature being measured. Tables for the suggested immersion times for various thermometers and API gravities are provided below in Figure 45 & Figure 46.

API Gravity at 60°F	Immersion Time in Minutes	
	In Motion	Stationary
> 50	5	10
40 to 49	5	15
30 to 39	12	25
20 to 29	20	45
< 20	45	80

Figure 45: Recommended Immersion Times for Woodback Cup-Case Thermometer

API Gravity at 60°F	Immersion Time	
	In Motion	Stationary
> 40	30 Seconds	25 Minutes
20 to 40	45 Seconds	45 Minutes
< 20	75 Seconds	80 Minutes

Figure 46: Recommended Immersion Times for Portable Electronic Thermometer

One temperature measurement trial requires lowering, immersing, and receiving the temperature reading of the thermometer. Repeat these steps and record the temperature data for each recommended trial. The calculation for average liquid temperature is provided below:

$$T_{Avg} = \frac{\sum T_i}{i_{total}}$$

Upon completing these steps, you will have obtained the **Temperature of both phases******. The temperatures and level measurements are then used to determine the volume of petroleum at standard temperature conditions. The density of a liquid is dependent on the temperature, so it is necessary to standardize the temperature used for custody transfers.

$$\rho = \frac{m}{V}$$

Because the mass inside the tank is constant:

$$\rho_0(T) \times V_0 = \rho(T) \times V$$

The density within the tank is dependent on the temperature, therefore the volume will fluctuate with temperature.

$$V_0 = \frac{\rho(T) \times V}{\rho_0(T)}$$

Sidebar

Safety Concerns of Manual Tank Gauging

These safety concerns are generalized for normal manual tank gauging operations (what does this mean?). The safety concerns for manual gauging are dependent on the environment, OPP, community fire prevention abilities and other factors.

- Personal protective equipment
- Confined space entry
- Hazardous vapor exposure
- Falling hazards
- Weather related safety factors
- Personnel training
- Corporate gauging procedures
- Safety preplan/preparedness
- Ignition sources
- Lightning and storms

Automatic Tank Gauging

The most common API standard for automatic tank gauging are available API Ch.3.1B¹⁴. Other relevant automatic tank gauging API documents are:

- **Chapter 3.3.** Standard Practice for Level Measurement of Liquid Hydrocarbons in Stationary Pressurized Storage Tanks by Automatic Tank Gauging
- **Chapter 3.6.** Measurement of Liquid Hydrocarbons by Hybrid Tank Measurement Systems
- **Chapter 16.2.** Mass Measurement of Liquid Hydrocarbons in Vertical Cylindrical Storage Tanks by Hydrostatic Tank Gauging

An automatic tank gauge or ATG is a method of determining the level of liquid within a tank without human intervention within a tank. Automatic tank gauging tends to be more reliable than manual tank gauging because of the reduction/elimination of human error. The reliability of an ATG is dependent on the instrumentation and system, their calibration, installation and maintenance of that instrumentation and system.

Where an automatic tank gauge is used, an automatic tank thermometer (ATT) system should be installed. As in manual tank gauging, the temperature must be known to convert the experimental volume to standard temperature volume. Remote monitoring systems use data from the ATG and ATT to provide inventory information in real-time. This system and information is valuable and critical for inventory control and tax purposes. An ATG system generally includes:

- A contact or non-contact level sensor (see section Contact vs. Non-Contact Level Sensors) which measures either the height of the liquid in the tank (innage) or distance between the liquid level and the reference point (ullage)
- A local display for operators to see the level
- A transmitter that sends data to monitoring computer
- A remote readout device that transmits information to a central data system

Factors influencing the accuracy of tank measurements:

- Accuracy of tank capacity/strapping tables
- Bottom deformations
- Thermal expansion of tank diameter
- Errors in density, temperature, or level measurements
- Incrustation
- Movement of the reference point
- Temperature affects the density of the liquid and therefore affects the volume of liquid but not the accuracy of the level measurement (the thermal expansion is accounted for in custody transfers)
- If an ATG is used, then it must utilize appropriate measurement techniques for the liquid product it is measuring (a float and tape gauge should not be used to measure viscous liquids)
- Operators should allow for settling time prior to taking a gauge reading to prevent inconsistencies, especially when monitoring a custody transfer

It is essential to accurately calibrate and verify the performance of an ATG. Verification if performed by operators who will adjust the liquid level in the tank to three distinct levels and record the results of the ATG and manual gauge. Note, the manual gauge should be calibrated and verified based upon MPMS Chapter 3.1A¹³ prior to the ATG verification process.

At each level, the ATG measurement shall be recorded and a manual tank gauge measurement shall be recorded. This process is repeated for the three liquid levels selected by the operator. After this process is concluded, the difference between the manual gauge readings and ATG readings shall be evaluated. An ATG used for internal inventory purposes should be verified on a quarterly basis, and an ATG used for custody transfers should be verified on a monthly base.

Purpose of Measurement	Frequency of Verification
Inventory Management (Internal)	Quarterly
Custody Transfer (External)	Monthly

Figure 47: ATG Subsequent Verification Requirements

Verification of an ATG is defined by API MPMS Ch3.1B as the process of manual gauging the liquid level in a tank at three positions and recording the measurements obtained for the ATG and manual gauge. The ATG must be within 1 inch (25 mm).

The difference between the manual gauge and ATG should be less one inch (25 mm). If the ATG does not match the manual gauge reading, consider a different type of ATG, installation parameters, or accuracy of the manual gauge. Specific tank gauges and sensors are described in detail in Chapter 6.



Figure 48: NXA82x Tank Scanner

NXA82x Tank Scanner with embedded Tank Vision:

Application

Tankvision is a dedicated tank inventory system which is operated by a standard web browser and does not require proprietary software or licensing costs. Tankvision is based on a distributed architecture on a Local Area Network (LAN). Due to its modular structure it can be adjusted to any application. It is ideally suited for small tank farms with only a couple of tanks, but also for large refineries with hundreds of tanks.

Tankvision consists of the following components:

- Tankvision Tank Scanner NXA820 scans parameters from tank gauges and performs tank calculations (option)
- Tankvision Data Concentrator NXA821 summarizes data from various Tank Scanners NXA820
- Tankvision Host Link NXA822 provides data to host systems (such as PLC or DCS) via Modbus

Inventory Calculations:

Based on measured variables and tank capacity tables, Tankvision calculates:

- Gross volumes
- Net volumes
- Mass

Overfill Prevention Systems

An Overfill Prevention System detects, indicates, and prevents hazardous overflow levels in storage tanks. Because of recent incidents, systematic overhauls to overfill prevention systems have taken place and industry best practice for managing storage tanks now combines the existing API 2350 prescriptive standards with the IEC 61511 functional safety standards.

The IEC 61511 functional safety standards describe Safety Instrumented Functions (SIF) that are designed to prevent or mitigate a hazardous event by taking a process to a tolerable risk level. This is the core function of every Overfill Prevention System. A SIF is composed of a combination of sensor(s), logic solver(s), and final control element(s). A SIF has an assigned Safety Integrity Level (SIL) depending on the amount of risk that needs to be reduced.

One or more SIFs comprise a Safety Instrumented System (SIS). To ensure safe functionality and meet the highest safety standards, every SIS must be independent of all other control systems controlling the equipment. All control elements including level devices, controls and alarming devices must be dedicated exclusively to the SIS. Therefore, an Overfill Prevention System must be completely independent of all other process control systems and devices.

Safety Instrumented Systems

Mostly because of the Buncefield incident and the UK HSE demand for better tank overfill performance through regulatory channels of API 2350 included the use of Safety Instrumented Systems (SISs) which are called AOPS (automated overfill protection systems) in API 2350. These systems are like what has been done in the past where tank receipts have been terminated by a valve closure. However, SISs compliant with industry standards such as IEC 61511 safety standards is a major challenge for many owners and operators. Using AOPS warrants a careful and thorough review by management and engineers to ensure that the implementation is realistic and will work.

When the risks are sufficiently high given a conventional overfill protection system and risk mitigation beyond the ordinary and traditional tank overfill protection methods is not sufficient to reduce risks to acceptable levels, then AOPS is one way to further reduce risks. The detailed discussions of AOPS can be found in industry standards such as IEC 61508 and IEC 61511. These standards are 'safety standards'

and follow the ideas of ISA S84 which address the lifecycle management of 'Safety Instrumented Systems'. These systems for tank overfill protection are simple in concept but a monumental challenge to accomplish in fact. This is because of the complexity and comprehensive implementation requirements required by these standards. Without going into all the details, it can be said that it takes from 1 to 2 years for large companies to develop an appropriate tank overfill protection standard that incorporates the safety component of API 2350.

A major consideration for these safety systems is that for a pipeline company the risks of hydraulic transients resulting from closure against flow increases the risks of more incidents. So, a balance between the various risks must be obtained by considering all risks and optimizing the risk reduction solutions. For example, in some cases the risk may be sufficiently low that AOPS is not needed and the risks can be controlled by operations. In other cases, the scenario that is preferred is to have an overfill occur in the terminal as opposed to rupturing the pipeline at some unknown upstream location. Still, in other cases, the best solution to prevent a spill over water may be to properly design the AOPS for all conditions so that the receipt may be safely terminated in an emergency without overfills and without blowing piping components. This may require extra and unused tank ullage, longer response times and so forth. There is no single optimal answer and each specific situation for the tank and its overfill scenarios must be addressed individually if optimal benefits are to be derived.

One should be able to see that there is much analysis and optimization required to accomplish these goals. This takes much discussion with knowledgeable stakeholders and appropriate analyses to be able to have robust systems that have been well thought out and universally agreed to by stakeholders and which can stand up to the questions of regulators. Because there are tradeoffs in costs and benefits, the solution usually requires these basic optimization elements of discussion, analysis, more discussion, consensus, and a plan for implementation.

This is achieved by consulting all relevant parties including independent subject matter surveyors as well as suppliers.

Some activities that are required to accomplish a uniform standard for tank overfill protection that would stand up to the scrutiny of internal corporate managers, regulators and the public or peer level organizations the following should be considered:

- Define the management system in detail for tank overfills. This management system could be incorporated into the corporate management systems or a separate system could be implemented under the umbrella of the larger corporate management system.
- Select and develop the type of risk assessment systems that will be applied to the tanks. This involves probabilistic estimates of overfills as well as consequence analysis. Because the fluids in many cases are Class 1 liquids, vapor cloud formation and the size of the vapor clouds must be estimated as a function of time. Many other fire related conditions must also be considered. In addition, if there is no fire then the impact of crude spills on the environment and impacts on other receptors must be developed.
- Set up a meeting to discuss exactly how tank overfills are controlled today and what the changes will be for the new systems.
- Implement a new standard that addresses all the current issues that arise because of using the current edition of API 2350 including a rationale for why AOPS was used or not used, under what conditions, and how risks are mitigated in other ways.

Addressing the Entire Safety Loop

The API 2350 standard prescribes methods by which owners and operating personnel can prevent tank overfills. It requires the use of a risk assessment system. Functional safety itself can only be applied to complete functional loops. Therefore, the complete Overfill Prevention System elements (including level devices, controls, and alarming devices) must be certified according to functional safety standards. Such system usually fulfills the requirements of levels SIL2 and SIL3.

An Automated Overfill Prevention System (AOPS) per definition is directly connected to the valve or pump. This means, if the system detects a High-High level alarm, the valve will be closed and/or the pump will be stopped immediately. Usually this happens quickly (typically less than 1 minute).

An Manual Overfill Prevention System (MOPS) per definition is a system which requires human intervention to terminate the flow of liquid into a tank. For a MOPS the worst-case Response Time must be calculated by considering the following additional factors:

- + the maximum communication time needed for the notification of the personnel who can respond (close the inlet flow)
- + the time the personnel need to analyze the situation
- + time needed to initiate the shutdown (close the valve)
- + time required to complete the response action (termination of receipt)
- + time to verify that all elements are reacting correctly and the required time needed if they don't
- + a safety factor.

According to API 2350 minimum response times are defined depending on the tank category. For a “fully attended” Category 1 tank the minimum response time is defined as 45 minutes. A Category 1 tank is a so-called “fully attended” which means:

- Attend at least 1h prior to start of filling
- Attend at least 1h after the receipt
- + periodically visual check the tank gauge on site, but do not manual hand dip until at least 30 min after a product receipt!

This means there are always people present in the field. Typically, there is only one transfer at a time in a tank farm with Category 1 tanks.

For a Category 3 tank “Automated Tank Gauging with an independent Overfill Prevention System” the minimum response time is defined at 15 minutes, if it can be proved that the personnel are able to terminate the inlet flow in all circumstances within this time!

Proof Testing

Even though rigorous testing of instrumentation control loops is often considered in the context of safety instrumented systems, the principles apply to any control system and these kinds of tests should be used for any overfill protection control system regardless of vintage.

The purpose of proof testing is to ensure that a control system works under realistic conditions and to find faults and problems so that they can be corrected. The act of proof testing also provides information that enables the owner/operator to re-assess the system reliability over time. Common sensor variables are pressure (or differential pressure), temperature, level, pH, density, speed (RPMs), etc. Proof testing is commonly referred to as a “wet probe test” because the probe or sensor experiences a process change that is sufficient to drive the loop into its alarm or other designated function. Ideally, a test of the complete control system should be done by changing the process variable (i.e. level) sufficiently to trip the control system sensor. However, this is ill advised for reasons discussed below.

The very first problem encountered with proof testing is to test a control loop from sensor to final element under realistic conditions. With instrumentation loops that use pressure, the loop test is relatively easy to conduct since the pressure sensor can be subjected to the appropriate test pressure which will then activate the control system and valves to see if they operate correctly. However, this should not be entertained as a practical methodology if the process is driven into a demand state or a state where an actual process hazard exists without a risk assessment to ensure that the risks are acceptable.

But most instrument loops for tanks are using liquid level height in the tank as the primary means of performing the alarm or final element function. One way to implement the proof test is to increase the physical liquid level to at least the alarm or final element set point. But this can be hazardous and is usually not easy to perform and can be also time consuming.

First, consider changing the liquid level in a tank to trigger an HH alarm. Running the liquid level into a restricted region (above the maximum normal working level) itself can be hazards and can result in an overfill. Strict control over this process would be tightly controlled by procedures and is certainly one way to conduct a proof test. It should be noted that most major oil company owners/operators consider this too

hazardous to allow, especially where flammable liquids are involved.

Another option is to set the liquid level sensor trip at a lower liquid level to test the alarm or final element operation. This procedure is often the only way to proof test a continuous level sensor. But this has a few problems as well. Changing the set point of the sensor introduces the distinct possibility that the correct original set point is not properly reset. In addition, it may be possible that the alarm function works in the lower contrived set point but does not actually work at the original set point depending on the technology.

In general, a proof test of a high-level alarm function performed with a continuous level sensor can be complex and involves the risk of leaving incorrect settings after the test. Most issues with a measuring loop are connected to wrong installations and wrong configurations. Therefore, the simpler a sensor is to install and to configure the smaller is the chance that something is done wrong.

Yet another option is to test parts of the system at different points in time (something allowed by API 2350). For example, suppose that we have an alarm system which uses a displacer or float which hangs down on a wire from a sensor head which is mounted on top of the tank. If we did not want to increase the level process variable to the actual set point, we could test just the functionality of the displacer by lifting the wire connecting the displacer to the control head, which should activate the switch and the alarm. Indeed, manufacturers of these devices have often built into the device a physical lever that lifts the displacer so that a switch is actuated. But note that this approach can have failure modes. Since the lever lifts the displacement wire and displace physically upward, the test will be successful. However, if the displacer is made of a hollow metal object weighted to float on the surface or an interface, it could be that the weight is incorrect, and it will not actually rise with the liquid level. A common example of this is a corrosion hole that penetrates the displacer and causes it to fill with liquid. In this case, the displacer will never float and even though the test lever simulated most of the functionality of the alarm loop it missed the problem with the sensor. This type of failure is called an “dangerous undetected” meaning that it is hidden until a full test from the sensor to the output is conducted. It must be emphasized that each technology has its own set of hidden failure modes and subject matter surveyors and manufacturers should be brought to the table to discuss these.

To perform a “bucket test” the sensor will be removed (typically at the top of the tank) and put in a bucket with a fluid of similar density. The problem with all “bucket tests” are that the sensor can be damaged or lose its calibration and this type of failure will not be detected because of the removal/reinstallation process. Furthermore, the operator must climb tanks and is exposed to dangerous environments as the tank is “open” during the test.

State of the art point level sensors like a tuning fork level switch (see also Chapter 6) are equipped with continuous checking online diagnostic functions. Such sensors do not only detect and alert cable breaks and open circuits but also the correct operation of the electronics and of the vibrating fork itself.

Build up and corrosion can be detected by analyzing the frequency. Therefore, such sensors are very reliable

and are available with the requested SIL certifications. Proof testing is an important part of tank overfill protection and it can be technical. Subject matter experts and the manufacturers should be consulted so that the proof testing procedures produce the desired results.

Another part is the documentation of these proof tests. Any proof test needs to be formally documented in a report. In these reports the proof test results (pass or fail) as well as the date and time when the proof test was performed must be noted. These reports should be easily accessible and protected against tampering at the same time.

Special attention must be given to the backup and restore concept of such report as they are needed most after any kind of event.

Example: FTL8x point level measurement system

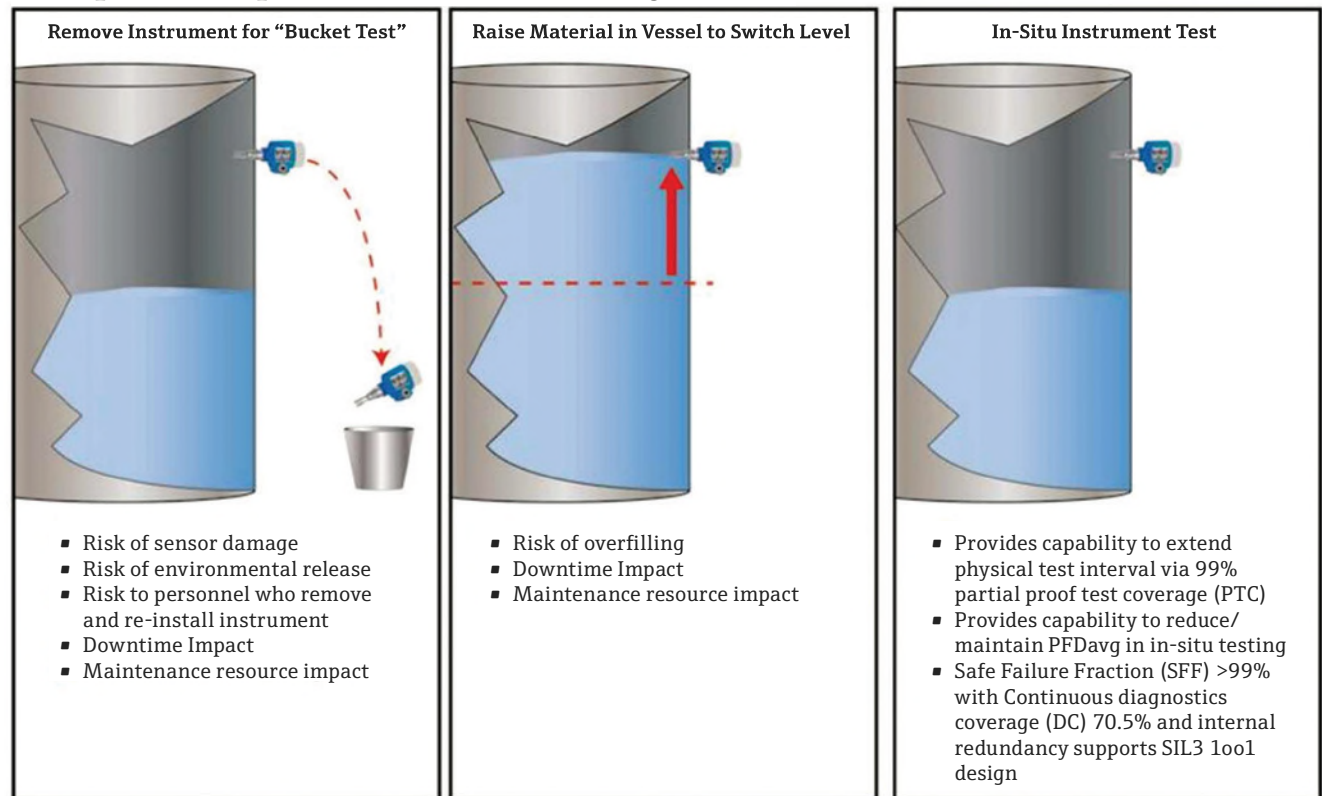


Figure 49: Methods of Proof Testing Sensors

Independence and Layers of Protection

The idea of independence arose as far back as the first edition of NFPA 30-1984 and API 2350-1987 where it was required that tanks must be “equipped with a high-level detection device which is independent of any tank gaging equipment”. API 2350 further defined that “An independent level alarm is an alarm function actuated by a primary level-sensing device that is separate and independent from any automatic tank gauging equipment on the tank.” These were required on unattended facilities because it was recognized that overall system reliability was enhanced by the independence concept.

In the early days of API 2350 the level sensors or “detectors” which operated the ATGs were typically mechanical devices that had a high rate of failure. By employing an independent alarm, the failure of the ATG would not impact the alarm function. Moreover, the alarm function could be independently proof tested to ensure that it worked. However, there are still numerous systems that do not have an independent alarm and when there is a failure of the level sensor everything associated with overfill protection, except for the operator has failed.

The independence concept is still in use in the current edition of API 2350 as it is fundamental to system reliability.

Another good example of independence is the use of an Automated Overfill Prevention System (AOPS). Because an AOPS requires no human intervention to fulfill its duty it is independent of operations. For this reason, in various risk assessment methodologies, risk reduction credit is given to these systems as a “layer of protection”, independent of other layers such as the operating layer or the emergency response layer. In all cases, this allows one to take full probability credit for reduced likelihood of system failure.

These ideas apply when the failure rates of the equipment (such as the Automated Tank Gauging System (ATG) are high. But with today’s highly reliable equipment and sensors, the idea of independence is not so straight forward. So, suppose that you had perfectly reliable ATG that never failed, then there would be no need for the independent alarm. It could operate from the ATG and its sensor would never fail because the ATG never fails. While this is hypothetical, the idea shows that independence has variable value depending on how good or bad the instrumentation is.

A good example of this idea in practice is the removal of the requirement starting with the 4th edition of API 2350 to have both H and HH alarms; only a single HH alarm is required. This was justified by the concept that the use of redundant alarms was to enhance overall alarm reliability, but with the highly reliable and self-diagnostic alarm sensors and alarms today, there is no need to require redundancy in the physical alarm system function. The concept should obviously be supported by the tank owner/operator and the type and reliability of level sensing equipment judged to be sufficiently reliable for this configuration. To judge whether it is better to use a single alarm or the pre-4th edition really requires detailed calculations and management philosophy and decision making.

Another often debated topic involves one of degree. If the power that feeds alarm sensors is common meaning that a failure of the power system will fail any and all sensors connected to the power, then this is a “common cause” failure which is amenable to simplistic methods of analysis. However, if there are independent power sources supplying the sensors then are they truly independent if they run in the same conduit? If the conduit is destroyed in a fire or severed by a mistaken operation such as by a back hoe then the failure will cut both power supplies and they would not be considered “independent”. These types of arguments can only be resolved by computation and common sense. For example, if the conduit is well protected and unlikely to be involved in a fire, then one could consider the electrical or signal circuits independent enough so that the two circuits could be considered “independent”.

One example of independence that arises is whether putting two radar level sensors in the same manway can be considered “independent” since they are in the same manway. One can argue that they are indeed independent because the reliability of a manway is so much more reliable than an electrical device.

However, these debates come up it is important to understand the relative failure rates to make common sense judgements and decisions about what is most appropriate for the overfill protection systems.

Compliance

That an Overfill Prevention System complies to the current regulations and Standards and therefore fulfills the RAGAGEP (Recognized and Accepted Good Engineering Practices) at least the following points should be considered:

- The system has to be completely (physically and electrically) independent of any other system.
- The system should be designed according to IEC 61511: “Functional safety” standards
- The system should offer an easy proof test function that can be operated remotely from the “outside of the storage tank” without the need of filling or emptying the tank and that covers the complete system from the sensor to the final element
- The system should be equipped with self-monitoring and failsafe sensors that offer highest on-line diagnostics.
- The system (including the sensors and actors) should be supplied by an uninterruptible power supply (UPS) to ensure highest availability
- The system should use diverse measurement devices (e.g. continuous level sensor for tank gauging and point level for overfill prevention) to reduce common cause failures

Typical applications for Overfill Prevention Systems are shown on the following figures:

Note: Visit our our Oil & Gas virtual tour at <http://apps.endress.com/oil-gas-virtual-tour/web/html/?homes>

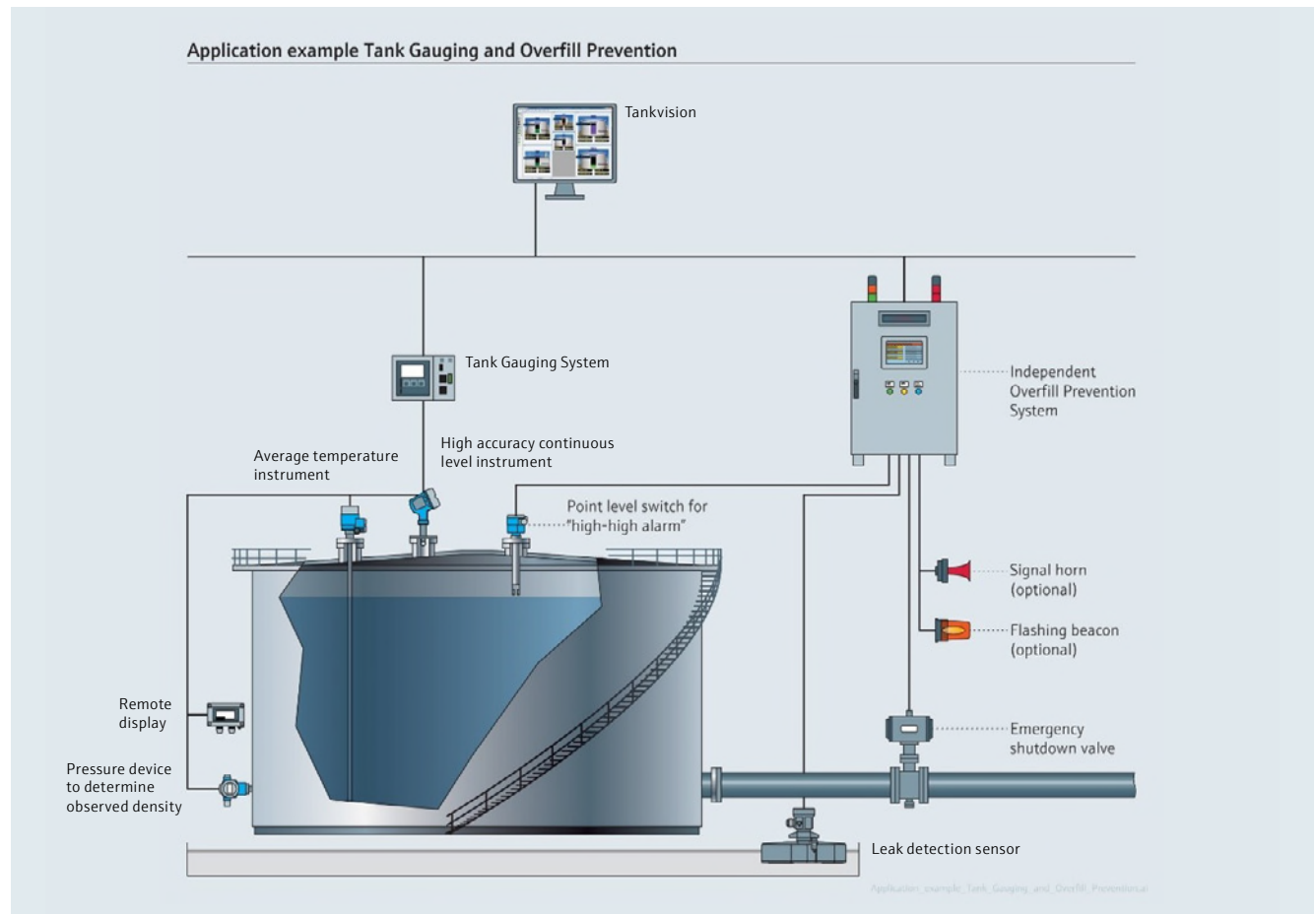


Figure 50: Typical architecture of a tank management system using a tank gauging system and independent overfill prevention system.

Additional Tank Systems

Continuous level and integration of Tank Gauging

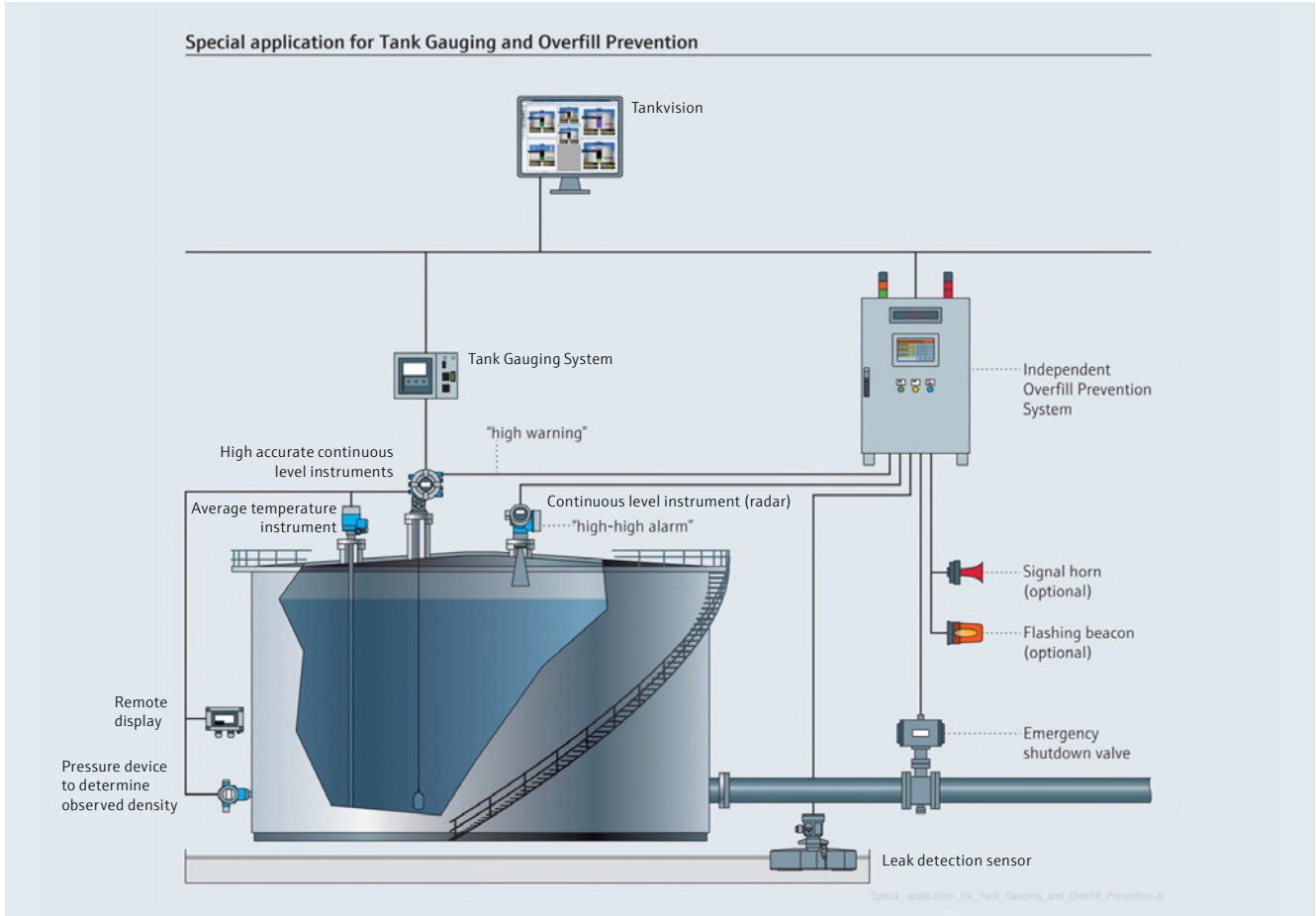


Figure 51: Setup for continuous level measurement with integrated tank gauging

Floating Roof Tanks

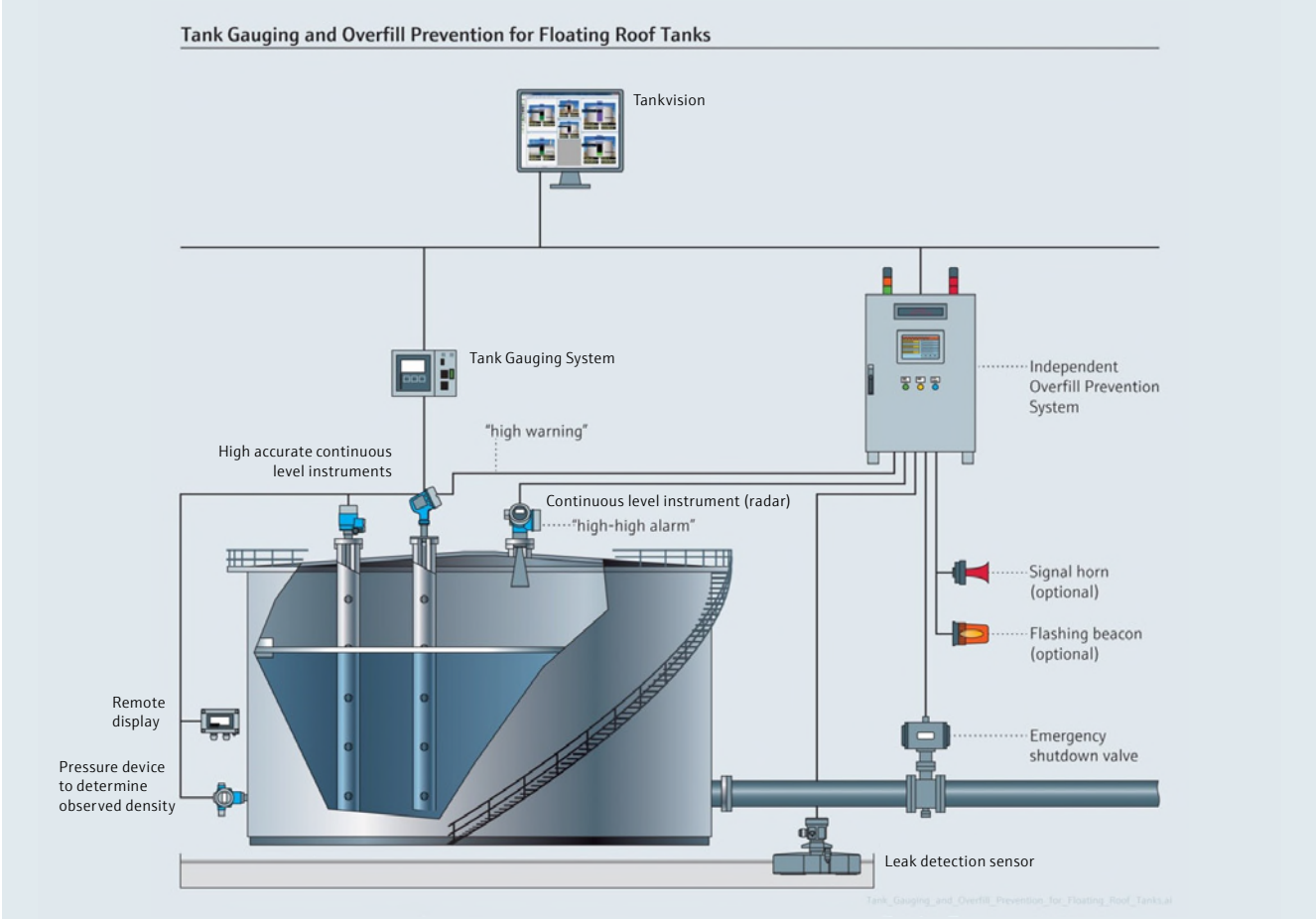


Figure 52: Setup for a floating roof tank

Spherical tanks

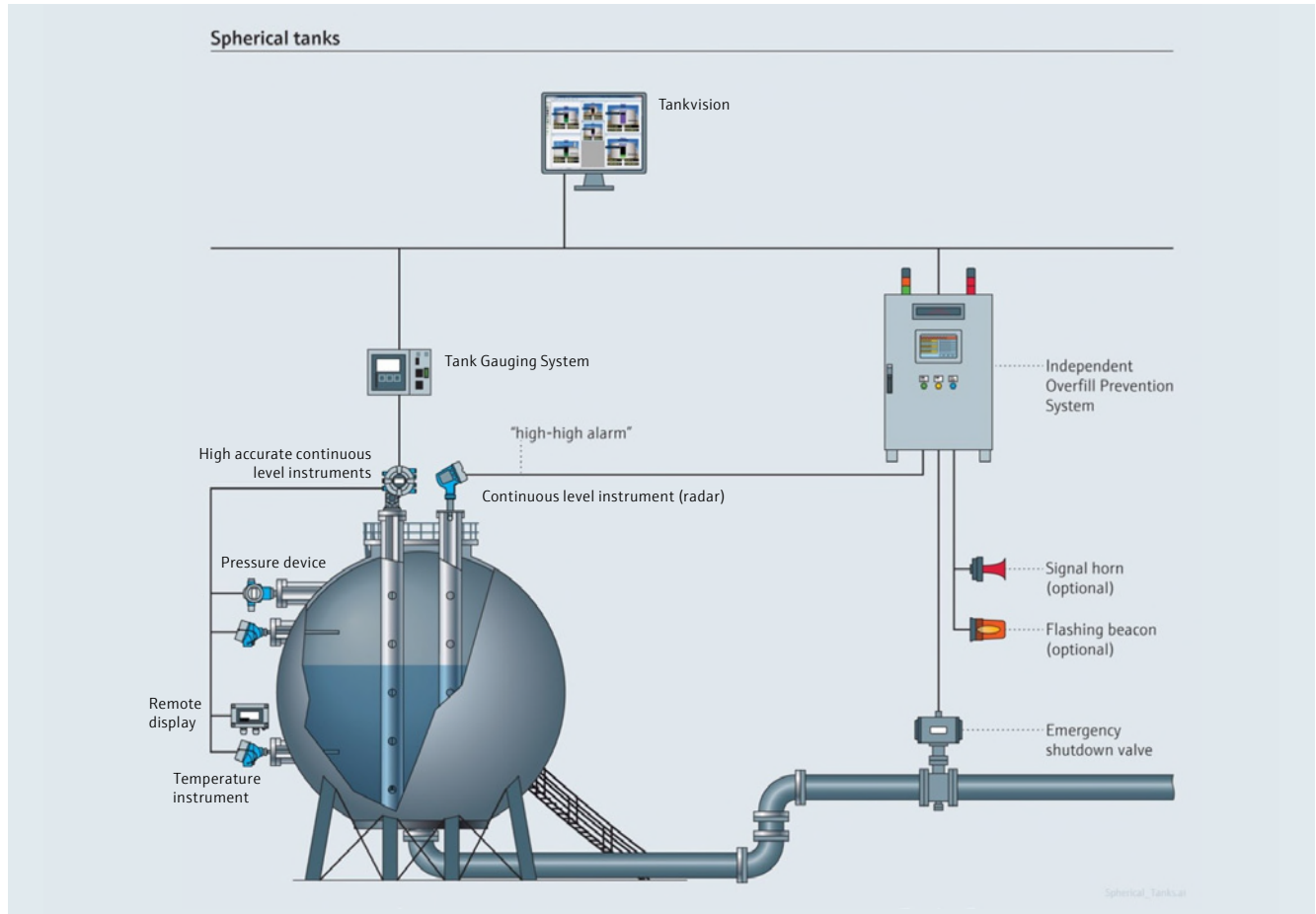


Figure 53: Setup for a spherical tank

Considering the whole setup

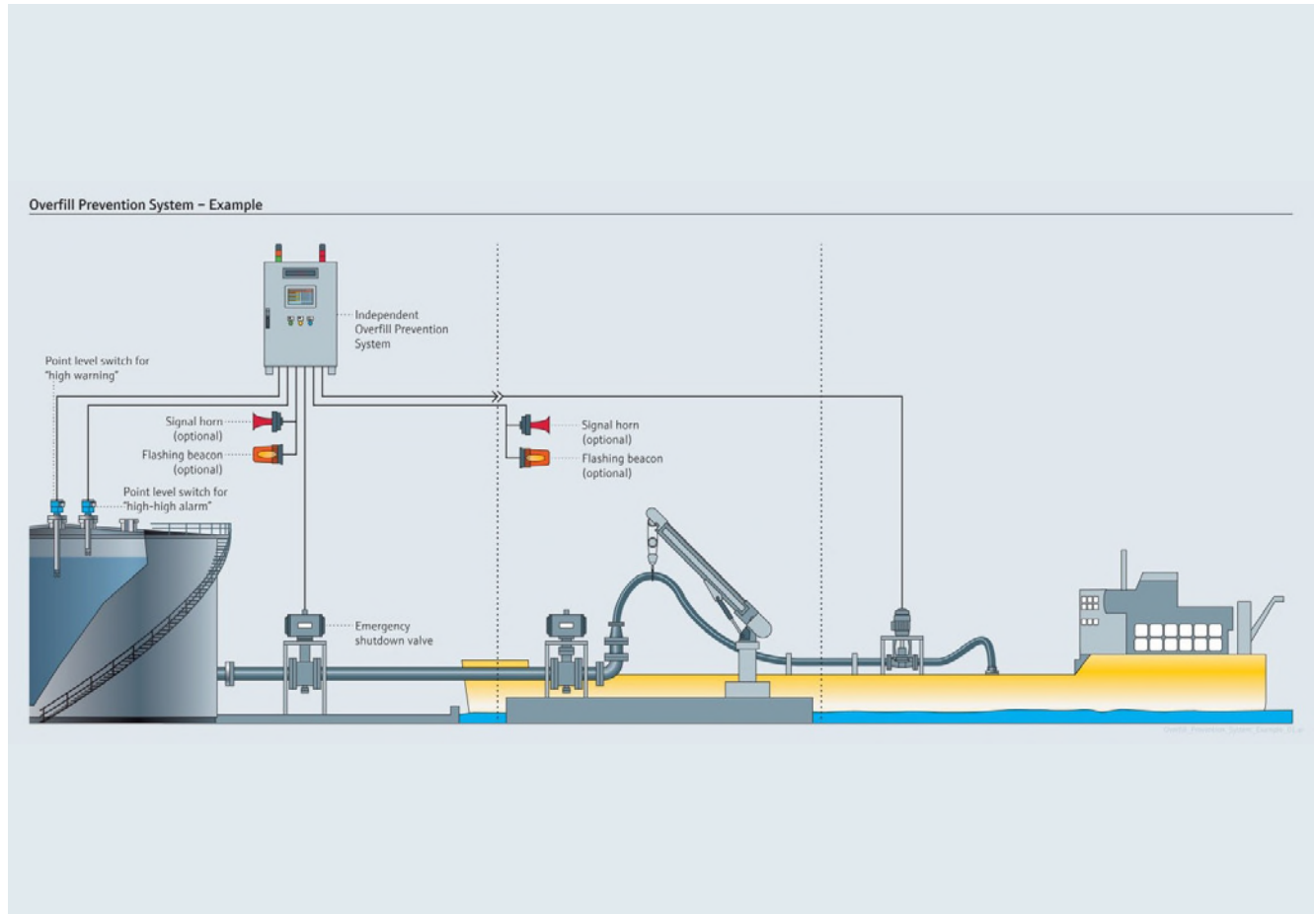


Figure 54: Complete setup for a tank farm

When installing an emergency shutdown system like an overfill prevention system, it is essential to consider the complete process.

For example:

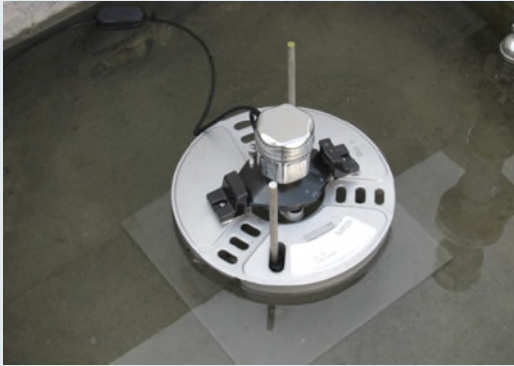
If a vessel is equipped with a pump to deliver hazardous fluids into a tank that may be located at a remote site, it is important to switch off the pump before closing the inlet valve to prevent overpressure in the pipeline. Sometimes the inlet flow will be diverted into another tank.

Any use case must be examined with a safety expert during a risk assessment. As an outcome of such a risk assessment, clear working procedures and interface descriptions should be created to have a mutual understanding of the safety measures.

Sidebar

Leak Detection Around Tanks

Tank spills can have several causes. Overfilling of tanks is one of the most common incidents but it is not the only one. **Tank leaks** from damaged seals, broken connections, or simply leaving a valve open have also to be considered. The Overfill Prevention System can be used to connect different sensors and therefore to detect any tank spill. Using sensors in a pump sump is a typical way to detect small spills at an early stage.



Oil Detectors in a drainage pipe (e.g. NAR300) can close a drain valve as soon as any oil is detected in a drain line.



With **Leak Detection** Sensors for basins, a basin can be checked for tightness.



Using an **Oil Leak Detector**, the detectable volume is much smaller than detecting leaks with a level measurement.

Contact vs. Non-Contact Level Sensors

Automatic tank gauging relies solely on sensors which are discussed throughout this chapter. Contact measurement devices use a probe that must “touch” the liquid to make a measurement. Contact measurement technologies include capacitance, mechanical, electromechanical, hydrostatic, tuning fork, float, and servo measurement methods. Contact methods may be point-level or continuous.

Non-contacting measurements typically measure the time-of-flight (TOF) taken by energy waves to emit from the transmitter, bounce off the liquid surface and return to the instrument. These methods include ultrasonic, radar and radiometric. These measurement methods can be point-level or continuous. Some manufacturers are working with sonar to allow mounting the transmitter at grade and sending the signal to the liquid service where the TOF is measured to determine the liquid level.

Sidebar

API Standards Related to Tank Level Measurement

API standards relevant to tank level measurement include:

- Chapter 3.1A. Standard Practice for the Manual Gauging of Petroleum and Petroleum Products
- Chapter 3.1B. Standard Practice for Level Measurement of Liquid Hydrocarbons in Stationary Tanks by Automatic Tank Gauging
- Chapter 3.3. Standard Practice for Level Measurement of Liquid Hydrocarbons in Stationary Pressurized Storage Tanks by Automatic Tank Gauging
- Chapter 3.6. Measurement of Liquid Hydrocarbons by Hybrid Tank Measurement Systems
- Chapter 16.2. Mass Measurement of Liquid Hydrocarbons in Vertical Cylindrical Storage Tanks by Hydrostatic Tank Gauging

Categorization of Level Sensors

Several level measurement techniques are shown in Figure 55. The earliest measurement systems were Float and Tape, or else hand gauging tapes. Even today many tanks are manually measured by a tape measure inserted into a manway and measuring how much of the tape is wetted by product to obtain the liquid level.

Sensor	Contacting	Non-Contacting	Mass	Point Level	Continuous Level	Interface	Density
Mechanical							
Float Switch	✓			✓		✓	
Float and Tape System	✓				✓		
Electromechanical							
Magnetic Float	✓				✓		
Tuning Fork (Vibronic)	✓			✓			
Servo	✓				✓	✓	✓
Electronic							
Capacitance	✓			✓	✓	✓	
Differential Pressure	✓		✓		✓		
Guided Wave Radar	✓				✓	✓	
Free Space Radar		✓			✓		
Ultrasonic (Sonar)		✓			✓		
Radiometric (Nuclear)		✓		✓	✓	✓	✓

Figure 55: Categorization of Level Sensors

Appropriate Level Sensor for Common Applications

The properties of the liquid being measured play a significant role in selection of the appropriate level control sensor. For example, highly viscous fluids such as asphalts and condensates are sticky. The sticking of the product fluid caused mechanical measurement methods to fail rapidly. Because of the sticking failure, a noncontact level measurement method, such as radar, is more appropriate sensor. A summary of appropriate sensors for common scenarios is shown in Figure 56.

Sensor	Viscous Asphalt	Crudes	Black Oils	White Oil	LPG/LNG	High Temp
Mechanical						
Float and Tape System		Poor	Poor	✓		✓
Electromechanical						
Magnetic Float		Poor	Poor	✓		✓
Servo		✓	✓	✓	✓	✓
Electronic						
Differential Pressure		Poor	Poor	Poor		
Guided Wave Radar		✓	✓	✓	✓	✓
Free Space Radar	✓	✓	✓	✓	✓	✓

Figure 56: Appropriate Level Sensor for Various Applications

The cost associated for the available level sensors and technologies depends on the tank system and corporate desires. The cost of the sensor generally increases with technological complexity. The cheapest option tends to be a mechanical probe such as a float and tape system. The higher cost options tend to be electric non-contacting technologies such as radar sensors.

Each type of level gauging technology has a capital expenditure (CAPEX) and operating expenditure (OPEX). The capital expenditure (CAPEX) is the cost to purchase something, such as the cost to purchase a level gauging system. The operating expenditure (OPEX) is the cost to maintain something meet operational standards, such as the electric costs to operate a guided wave radar system. Systems which use continuous electricity must purchase electricity to operate that system, but continues level monitoring improves the reliability of the system and reduces the potential for an overfill event.

Consequently, more complex technologies tend to have higher reliability because contact with product fluid and mechanical contact is minimized. Product fluid can corrode and mechanical contact points can become lodged. Because of this, the trend between the reliability of the level measurement and sensor technology is like the trend in cost.

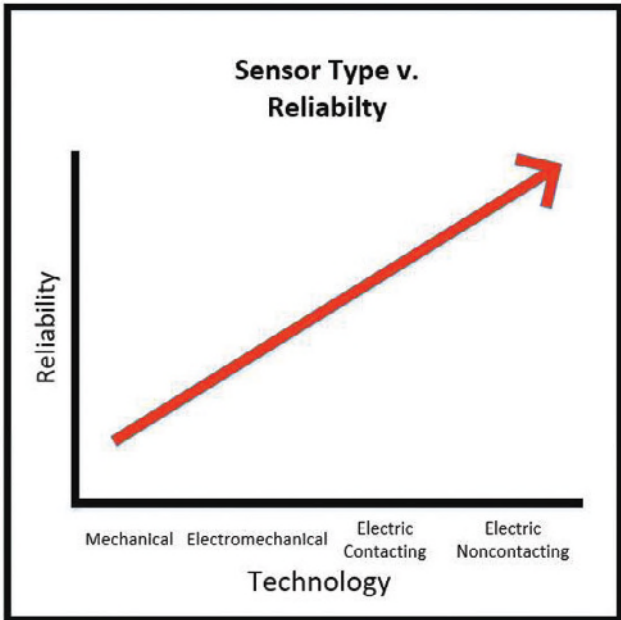


Figure 57: Generalized Trend of Technology and Reliability

Point Level Sensors

These are devices that display if the liquid level reaches a certain height in the tank or vessel. Point level measurement is binary information (i.e. the level is either below the sensor, or the level is at or above the sensor). So, point level sensors deliver binary information (ON/OFF), displaying whether the level has passed a specified point. Point level indicators have the benefit of being lower cost and simple, without the need for complex signal transmission protocols.

Point levels can be used as alarm switches that activate when setpoint conditions are achieved (liquid levels become too high or too low). Point levels are used in addition to continuous level transmitters to notify operators of critical process conditions. Next, we will describe the application of various point level indicators and their capabilities. In all cases, the sensor must be immersed by the liquid and will trigger a contact at that elevation point. These devices are useful for level alarms.

Mechanical float switch

With a mechanically actuated float switch, switching occurs because of the movement of a float against a miniature (micro) switch. For such level sensors, chemical compatibility, temperature, specific gravity (density), buoyancy, and viscosity affect the functionality. The choice of float material is also influenced by temperature-induced changes in specific gravity and viscosity – changes that directly affect buoyancy. Some mechanical float switches offer a test function where the float is manually moved into the alarm state. These manual test functions are generally error-prone and unreliable. Usually such basic sensors have no diagnostic functionality but float switches are popular for simplicity and low cost.

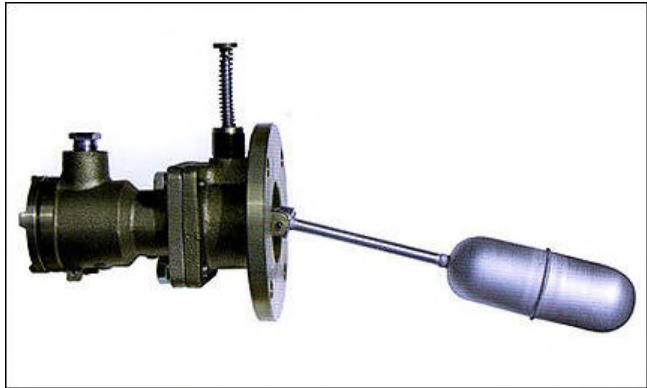


Figure 58: Mechanical Float Switch

Tuning Fork Level Sensor (Vibronic Measurement)



Figure 59: Endress+Hauser Liquiphant FTL50 Point Level Sensor

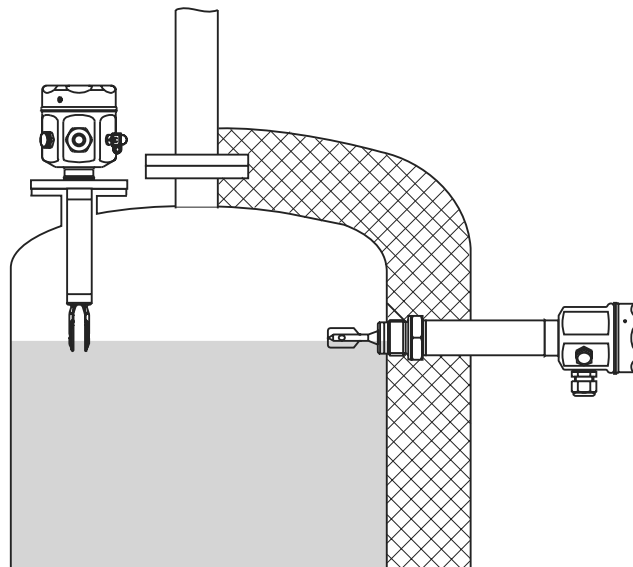


Figure 60: Endress+Hauser Liquiphant FTL50 Point Level Sensor

Tuning fork (vibronic) point level sensors are electronic and contacting. A piezoelectric motor vibrates two metal protrusions, referred to as a “tuning fork”. The tuning fork is excited to its resonant frequency by piezoelectric material. When the tuning fork enters the product the frequency of vibrations is damped by the liquid immersion of the tuning fork. The change in frequency is detected and used to determine if the liquid level is above the tuning fork position. The tuning fork method is advantageous when compared to a mechanical displacement because the output of the tuning fork sensor is diagnostic and continuous. The tuning fork is a reliable sensing method because if the liquid is in contact with it, or the sensor requires maintenance, than the setpoint conditions would be achieved and an alarm would activate. Operators would receive a signal and act accordingly.

Such sensors are typically used for maximum or minimum detection for liquids in tanks or pipes (leak monitoring, dry running protection/pump protection or overfill protection), particularly for the chemical, energy, and oil & gas industry.

The point level switches make a distinction between two states: “covered” and “exposed”

Continuous checking and online diagnostic functions

Compared to other physical principles, e.g. floats, the vibronic point level switches can offer a decisive advantage with the frequency evaluation facilitating automatic self-monitoring of the fork. Such sensors do not only detect and alert cable breaks and open circuits but also the correct operation of the electronics and of the vibrating fork itself. Build up and corrosion can be detected by analyzing the frequency.

Cable breaks and open circuits as well as the correct operation of the electronics are continuously checked by using current pulses (PFM signals = pulse-frequency modulation or LIVE signal) between the sensor and the logic solver.

Therefore, such sensors are continuously monitored and therefore very reliable and are available with the requested SIL certifications.

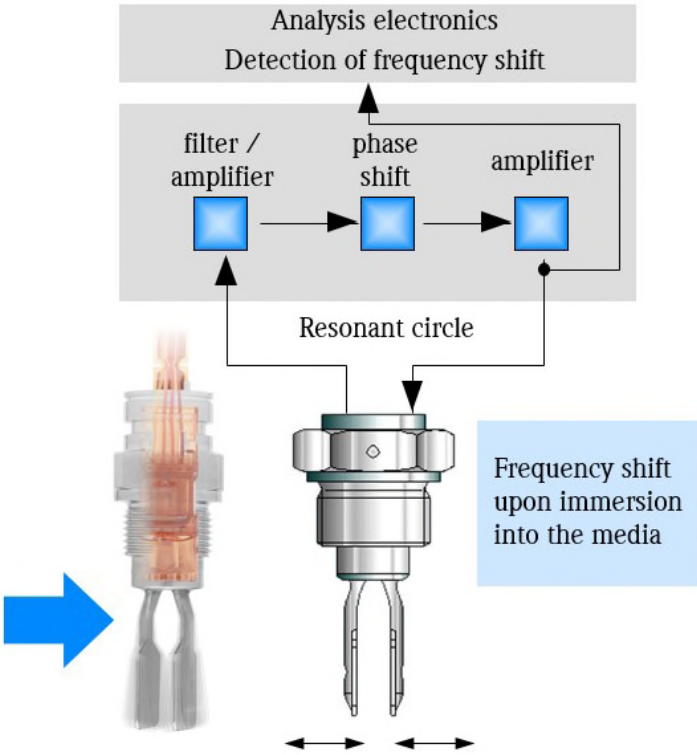


Figure 61: Detection of frequency shift

Safe alarm function

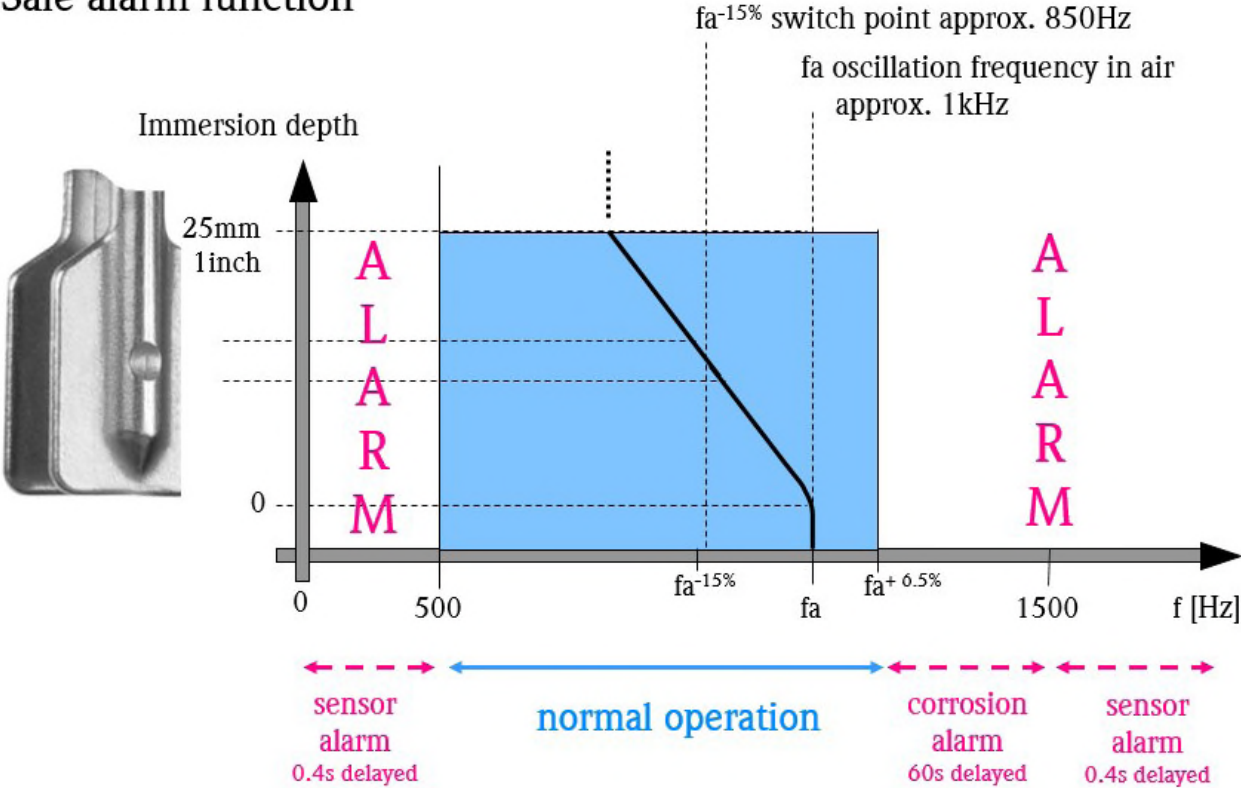


Figure 62: Safe alarm function. fa = failure alarm

Capacitive Level Sensors used as level switch

The capacitive measuring principle is based on the method of the operation of a capacitor. A capacitor is formed by two differently charged electrodes isolated from each other. Applying an alternating current between the electrodes will create an electric field. This electrical field depends on the distance between the electrodes, the size of electrodes surface, and the isolating medium between the electrodes.

If the distance between electrodes and size of surface of the electrodes are kept constant, only the medium would influence the electrical capacitance. When the medium changes the electrical field changes also consequently the capacitance evolves as follows:

Capacitance (C) = Dielectric constant (ϵ_0) \times Relative Dielectric constant (DC) \times Electrode Surface Area

Where the dielectric constant (ϵ_0) is the electric field constant ($\epsilon_0 = 8.8 \times 10^{-12} \text{ C}/(\text{Vm})$).

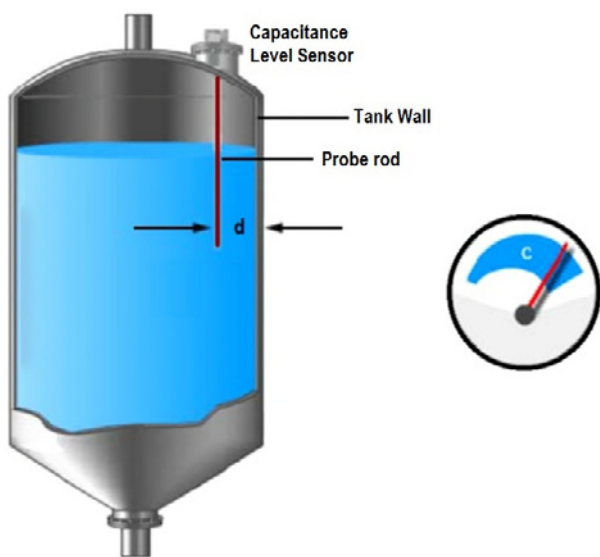


Figure 63: Capacitance measurement principle

Special application as level switch for floating roofs

The capacitive measuring principle may be used as level switch for floating roofs.

A sample installation is shown below:



Figure 64: Floating roof detection

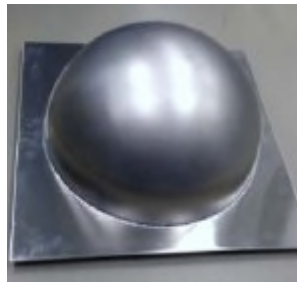


Figure 65: Floating roof detector plate

- The capacitive sensor is installed on a suspension arm at the tank wall.
- The sensor itself is selected with a long rod weight and a short flexible robe and a long inactive length.
- This makes the measurement unsusceptible of wind.
- On the floating roof a detector plate is mounted.
- This plate can be designed in a hemispheric shape to avoid deposits.
- If the floating roof rises to the defined high level, the sensor touches the detector plate.
- This leads to a change of the capacitance and triggers the sensor to switch.

Continuous Level Sensors

Continuous level sensors perpetually monitor the height of product within a tank. Whereas the point level sensor provides only a yes/no answer to whether the liquid is at or above the sensor, the continuous level sensor outputs real time level. More information is obviously available to the control systems and the operator with continuous level measurement. While continuous level measurement is important for both inventory and custody transfer operations, it provides the ability for operations to project or estimate when a tank will be filled or emptied because of the extra information provided beyond just point level readings. In custody transfer applications, level transmitters need to be accurate within 4 mm.

Older technologies, such as mechanical point level indicators, may be less accurate and reliable than newer electronic technologies. Continuous level transmitters range in complexity, but best practices such as redundant alarm sensors and self-diagnostic systems can significantly improve process reliability and safety.

Float Level Sensors

A float transmitter is a mechanical or magnetic device which moves vertically with the liquid surface. The float device moves up only when the level increases because the buoyancy of the float is just enough to suspend it in the liquid, much like a fishing bob. This method of level monitoring has the benefit of being simple and usually low cost but poses some risks such as sticking, buoyancy failure, and lack of redundancy. While there are many applications which are ideally suited to this technology those applications using it should avoid services which can degrade service such as sticky fluids, dirty liquids, or highly variable densities which change the relative float location with respect to level.

Float and Tape Sensor

Float and Tape sensors are mechanical and have moving parts in addition to requiring liquid contact to function. A tape measure attaches to a float, and the float rises with the liquid level. The float rising creates slack at the counter weight. This slack is pulled by the external housing which is at grade and which winds up the tape, displaying the height of the liquid level. This method of level measurement is simple and inexpensive.



Figure 66: Endress+Hauser LT5 Mechanical Tank Gauge

However, unless the installation is properly made and the device used in the appropriate service, there can be risks of sticking and failure to operate correctly. Devices with moving components require periodic maintenance and may have lower reliability when compared to recently developed electronic measurement systems.

Magnetostrictive Float Level Sensor (Magnetic Float)

This measurement is an electromechanical contacting method because a float moves up and down with the liquid level, but the level is determined by an electric signal. The float contains magnets which produce a magnetic field. The voltage of the resistor chain changes with position of the magnetic field created by the magnetic float. The voltage of the resistor chain is calibrated at known product levels. The change in voltage across the resistor chain is used to continuously calculate to the product level.

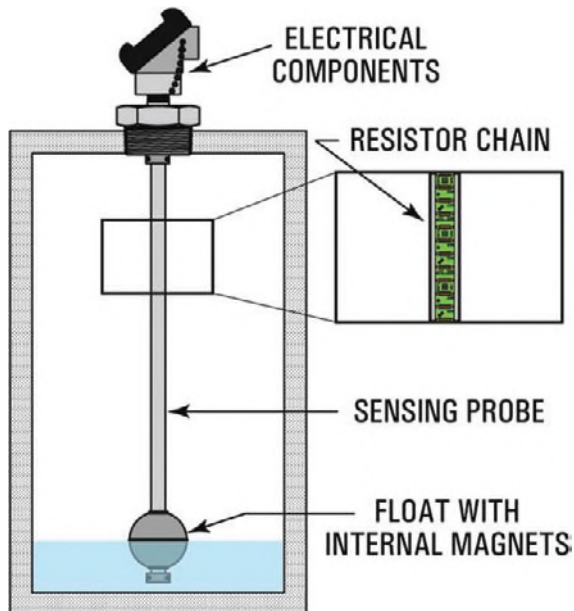


Figure 67: Diagram of Magnetic Float Level Sensor

Magnetic float indicators are superior to the tape float transmitters because they have less moving parts. Less moving parts reduces the risk of sticking, however magnetic float indicators are not considered highly reliable.

However, unless the installation is properly made and the device used in the appropriate service, there can be risks of sticking and failure to operate correctly. Devices with moving components require periodic maintenance and may have lower reliability when compared to recently developed electronic measurement systems.

Electro Mechanical Servo Transmitter

Servo measurement technology is based on the Archimedes Principle that, “any object, wholly or partially immersed in a stationary fluid, is buoyed up by a force equal to the weight of the fluid displaced by the object.” – Archimedes, 250 BC.

Servo level transmitters are electronic and contacting. Servo measurement works through a displacer (which is not a float) that is attached to a servo motor. The displacer is suspended on a fine wire that is lowered into the liquid product. When the displacer contacts the liquid surface, buoyant forces reduce the weight of the displacer. Because the servo motor is suspending the displacer, the force on the servo motor is reduced by the buoyant forces acting on the displacer. That change in force changes the torque within the magnetic coupling of the servo motor. Electromagnetic sensors measure the change in torque of the servo motor and the position of the displacer. The position of the displacer when the torque change occurs is converted to a product height.

The change in torque is based upon the density of the fluid. This allows servo measurement to determine a liquid level, interface level, and product density.

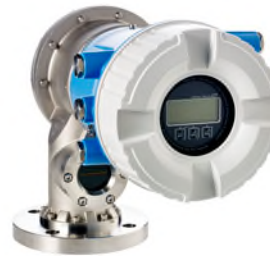


Figure 68: Endress+Hauser NMS8x Servo Level

Servo measurement is reliable and often used in custody transfers. The benefits of servo measurement include high reliability, unaffected by dielectric constants and the vapor phase, capable of determining an interface, capable of detecting water bottom, and capable of determining product density (both points and profiles). The ability to determine mass within a tank makes servo measurement one of the most robust and valuable form of level measurement. Further, servo level sensors are versatile enough for application in a crude oil vessel or liquified gas (LNG/LPG) tank.

Capacitance Level Sensors

Capacitance level sensors use an electronic contacting measurement method. Capacitance transmitters work by lowering an electric probe into the tank. The tank wall and the probe create a current, and that flow of current is dependent on the liquid level within the tank. The probe detects little to no current when the tank is primarily full of air because air has a high resistance to electric current. As the liquid level rises, more current flows between the probe and the tank walls. This is because water and oil are less resistive than air.

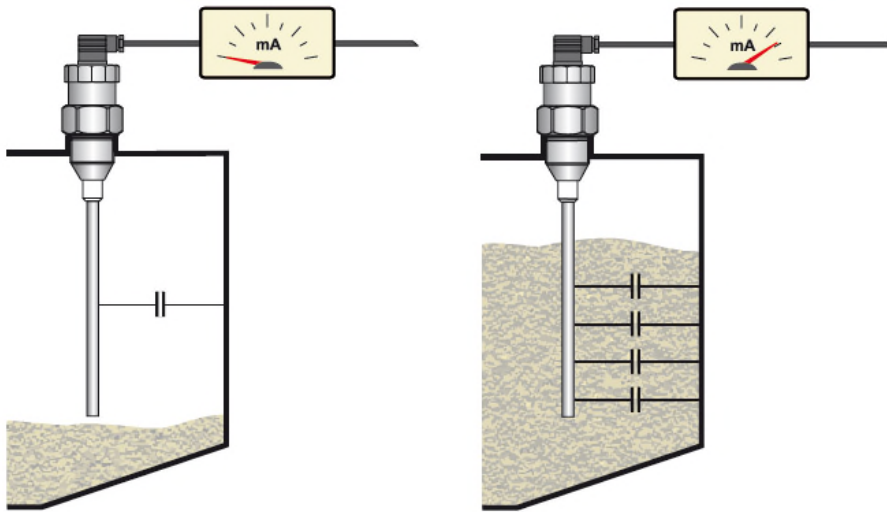


Figure 69: Diagram of Capacitance Level

Likewise, hydrocarbons are more resistive to an electric current than water. This is because the dielectric constants are different for the species. The dielectric constant is the measured ability of a substance to store electric energy created by an electric field. The dielectric phenomenon is utilized in capacitance measurement devices to gauge both the liquid level and interfacial level. The interfacial level is crucial to many separation and storage processes.

In industrial application, continuous capacitance level sensors are not used to measure the hydrocarbon product level in large tanks but are effective at monitoring the level of water bottoms.



Figure 70: Endress+Hauser Capacitance Level Sensors

Ultrasonic Level Transmitters (TOF Sensors)

Ultrasonic level transmitters are electronic and can contact the liquid surface or not depending on the sensor type and application. This method works by measuring the free space within a tank by emitting ultrasonic pulses towards the liquid level. Ultrasonic pulse frequencies are above 20KHz, which is inaudible by the human ear. Ultrasonic waves bounce off the liquid surface and the reflections return to the sensor. The time required for the ultrasonic signal to emit and return to the sensor, is the “Time-of-Flight”, or TOF. The TOF is used to determine the distance the signal travels using the speed of sound in air as the velocity of the ultrasonic pulse. The time for the pulse to emit from the sensor and return to it is inversely proportional distance between the sensor and the liquid level. Therefore, as the liquid level drops the signal response time increases. The speed of sound in air at 20°C is 343 m/s. Therefore, the distance travelled is:

$$Distance_{ultrasonic\ pulse} [m] = \frac{\left(343 \left[\frac{m}{s} \right] \right) \times (Time\ of\ Flight [s])}{2}$$

The height of the liquid is then obtained by the difference between the height of the tank and distance travelled by the ultrasonic pulse.

$$h_{liquid} = Distance_{sensor\ to\ base} - Distance_{ultrasonic\ pulse}$$

Ultrasonic level sensors tend to be easy to install, reliable, and lower cost than alternative electric noncontacting sensors. Ultrasonic vibrations are vulnerable to changes in the density of the medium it propagates through. Therefore, it is difficult to have high accuracy level measurement of volatile liquids using the ultrasonic method.



Figure 71: Endress+Hauser Prosonic FMU40 Level Sensor

Radar Level Transmitters (TOF/FMCW Sensors)

Radar level transmitters are electronic and non-contacting, using the principle of TOF (Time-of-Flight). The primary difference between the radar method and ultrasonic method is the type of wave used to measure the TOF. Radar level transmitters emit radio waves rather than ultrasonic pulses. Radio waves are generated electromagnetically by an antenna and directed towards the product surface in the tank. The radio waves contact the product surface and bounce back towards the top of the tank. The sensor on the top of the tank then registers the incoming radio waves.

Radio waves travel at the speed of light, so the time required to return can be converted into a distance. Like the ultrasonic method, the time required by the radio wave to return to the sensor is inversely proportional to the liquid level. Therefore, as the time between emission and return increases, the liquid level decreases. Because the speed of light is extremely fast, the frequency of the radar must be large to obtain high resolution from the sensor.



Figure 72: Endress+Hauser FMR60 Radar Level Sensor

Frequency-Modulated Continuous Wave (FMCW) radar is different from normal continuous wave (CW) radar methods. FMCW can change the frequency of the pulses from the radar emitter. The FMCW method accounts for the delay caused by the wave frequency and creates higher accuracy measurements than CW. Endress+Hauser utilizes FMCW on its radar technology, rendering the measurements highly accurate for level control and custody transfer applications.

The radio waves can be free to propagate through a tank (see Figure 72) or restricted to a guide tube (Figure 73). Emitting and receiving radar waves through a guide tube can further reduce the noise in the measurements.

Free space radar level transmitters

The success of a radar level sensors is dependent on good installation. The radar needs an unrestricted path to the liquid surface, as all other continuous level measurements require. Any obstruction, such as piping, can cause unwanted echoes in radar measurement. Although, modern radar technology has software algorithms to mask and compensate for these echoes. The new Endress+Hauser radar sensors operate at a higher frequency than previously. The new 80GHz signal achieves a tighter beam angle and reduces the horizontal spread of the radio transmission.



Figure 73: Endress+Hauser Micropilot FMR540 TOF Radar Level Sensor

Radar level sensors have high reliability and require little maintenance. Radar waves are unaffected by vapors in the tank, unlike sonar waves.

Free space radar for custody transfer and inventory control applications

Free space radar sensors that are used for custody transfer and inventory control applications usually need a NMI- and PTB-approval and must meet the requirements according to OIML R85 and API 3.1B. Modern devices offer drip-off lens antennas a sharply focused beam angle of to avoid obstacles even close to tank wall by using a higher transmitting frequency.



Figure 74: Endress+Hauser Radar Measurement Micropilot NMR81

Radiometric (Nuclear) Level Transmitters

Radiometric level transmitters are electronic and non-contacting, but operate differently from the radar and ultrasonic methods. The largest difference is that radiometric measurement can be used for continuous measurement, point level measurement, and product density measurement. Because of the ability to determine product density, radiometric measurement devices can determine the mass of material within a tank. The abilities of the radiometric measurement, including the ability to measure liquid density, makes radiometric measurement a robust forms of level measurement.

Radiometric transmitters emit gamma radiation from radioactive isotopes of Cesium (137) or Cobalt (60). These isotopes only emit β (particle) and γ (wave) radiation. The isotopes are secured in a double-walled stainless-steel vessel. This vessel prevents the emission of particle radiation, specifically β radiation. Therefore, only γ radiation can penetrate the stainless-steel vessel. The radioactive source is surrounded by an

external container such that the γ waves are directed in one direction, towards the storage tank. A contact transmitter is positioned on the opposite side of the tank to receive the gamma radiation.

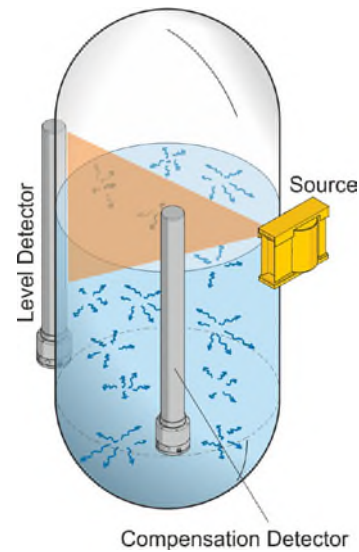


Figure 75: Diagram of Radiometric Level Transmitters

The radiation adsorbed is dependent on the density of the medium which the radiation passes through. High density mediums absorb more radiation. Therefore, more radiation is absorbed by product fluid than air. The contact transmitter measures the strength of radiation across the vertical length of the tank, determining the level. Water and hydrocarbons are immiscible and have different densities. Therefore, radiometric methods can also determine the level of an interface.



Figure 76: Endress+Hauser Gammapiilot FMG60 Radiometric Level Transmitter

Oil Leak Sensors

Because overfilling and spilling events are dangerous and punishable by law, it is important to detect product liquid early during a spill event. Innovative technology combines different sensors to distinguish water and oil in a dike, sump, or floating roof. The different sensors within in the NAR300 can distinguish hazardous liquids such as gasoline from water, preventing a false alarm. The sensor can be placed within a drainage dike, runoff containment, underneath a tank bottom or wherever the application is most valuable for your company. The benefit of an oil leak sensor is early detection. Early detection is becoming aware of a risk event very quickly after it initiates. Early detection can be the difference between a small leak and a massive overfill event.

An oil leak sensor cannot prevent a spill event, but it can reduce the severity of the event if it were to occur. Therefore, oil leak sensors can detect very small leaky from flanges and pumps at a tank.



Figure 77: Endress+Hauser NAR300 Oil Leak Sensor

Differential Pressure Sensors

Differential pressure transmitters are electromechanical and contacting. This category of continuous level sensors uses the hydrostatic pressure created by the column of liquid in the tank to gauge the level. As the liquid height in the tank rises, the pressure on the bottom of the tank increases.

The distance across a capacitor in the differential pressure sensor changes by a diaphragm, changing the current. This change in current is related to the change in liquid height.

Differential pressure level measurement has been popular for a sustained period but is falling out of favor for more reliable and modern techniques. DP level measurements have the disadvantages of clogging, lack of redundancy, and are unable to detect an interface.



Figure 78: Endress+Hauser electronic differential pressure

Chapter 7 – Level Measurement Reliability

Safety Instrumented Systems

Reliability for a component is defined to be the probability that a component or system will perform a required function for a given period when used under stated operating conditions.

Single components can typically be modeled by probability distributions such as exponential or Weibull distribution. The lambda value or λ for a given system/instrument is the failure rate. The lowest lambda value possible is the goal for each system, but it is impossible to reach a zero λ value. It is impossible to ensure that a system will operate correctly every single time for an infinite period. Because of this, systems are developed with redundancy and variety, minimizing the likelihood of many failure modes.

A “dangerous undetected” failure is one in which the safety instrumented system appears normal when a risk event is occurring. An example of a “dangerous undetected failure” is when a high-level alarm remains in the inactive state when setpoint conditions have been achieved. This may occur due to mechanical sticking, such as what occurred at the CAPECO facility.

The functional safety aspect of process safety instruments is analyzed in IEC 61511. This standard defines fault tolerance based upon the likelihood of a dangerous event/failure occurrence. These are called Safety Integrity Levels (SIL) and are defined in Figure 79.

SIL	Probability of Dangerous Failure Average	Safety Availability	Risk Reduction
SIL 1	0.1 – 0.01	0.9 – 0.99	10 – 100
SIL 2	0.01 – 0.001	0.99 – 0.999	100 – 1000
SIL 3	0.001 – 0.0001	0.999 – 0.9999	1000 – 10000
SIL 4	0.0001 – 0.00001	0.9999 – 0.99999	10000 – 100000

Figure 79: Safety Integrity Levels

These SIL levels define the probability of a dangerous failure based upon the failures per year. This is an uncomplicated way to quantify and understand the inherent risk of your process or equipment. IEC 61511 defines allowable SIL based upon the danger or potential damage that would be caused if a failure did occur.

Even if sensors were reliable, the installation could produce unreliability. For example, modern cartridge loaded float and tape devices are quite reliable, but if the pulley system for routing cables up and over the top of the tank are incorrectly installed or the tank has moved due to settlement then the cables can stick, fall off the pulleys, and fail to operate correctly.

Moreover, the reliability of a system depends not only on component reliability but on the combination of many components. Reliability block flow diagrams begin with a series or parallel arrangement as shown in Figure 80.

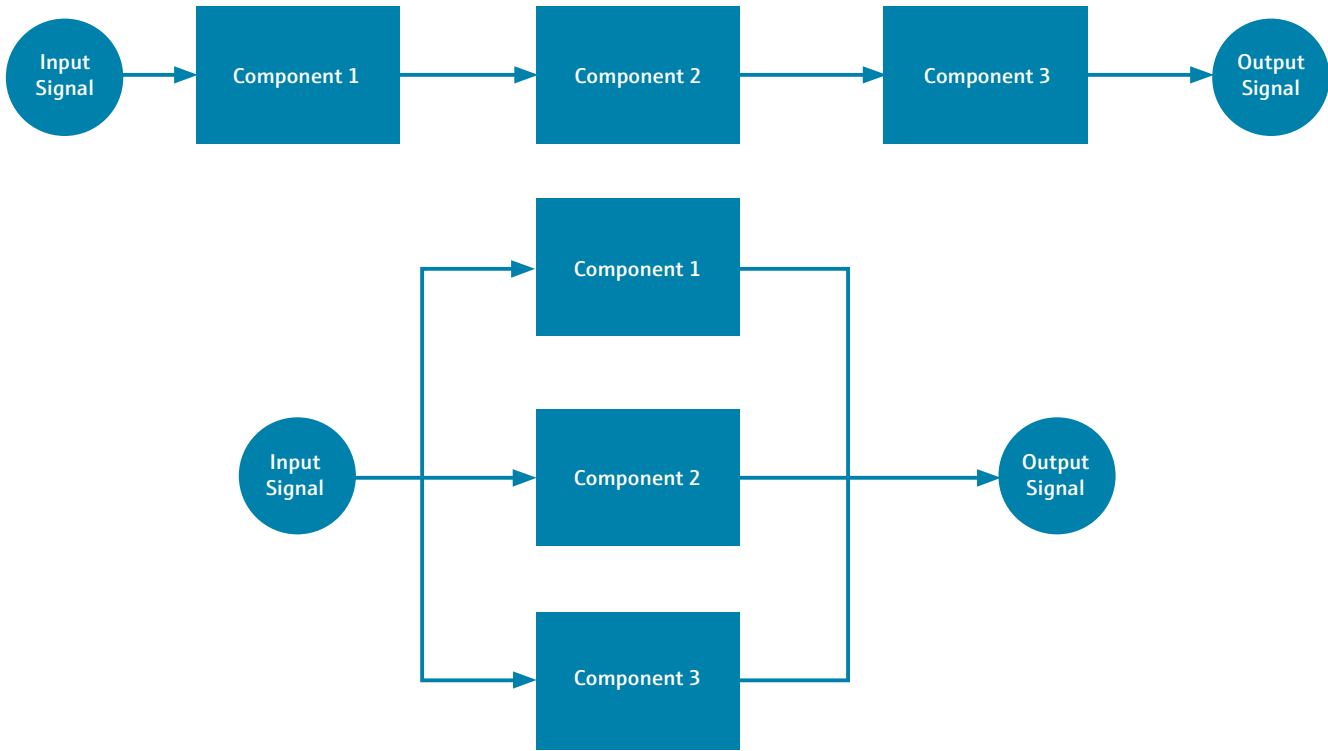


Figure 80: Series and Parallel Component Arrangement Diagram

If each component is independent of the other components in the series diagram and generalizing to n components then the system reliability in terms of component reliabilities is given by

$$R_s(t) = R_1(t)R_2(t) \dots R_n(t)$$

This is the product of reliabilities of the individual components and since reliabilities are probabilities meaning that they have a value bounded by (0,1) then

$$R_s(t) \leq \min (R_1(t), R_2(t), \dots, R_3(t))$$

This says that the system reliability $R_s(t)$ can be no greater than the reliability of the most unreliable component. This means that wherever components are connected in serial manner then high reliability components must be used to maintain a reasonable level of system reliability.

In a parallel configuration as shown in Figure 65, the system reliability generalizes to

$$R_s(t) = 1 - \prod_1^n (1 - R_i(t))$$

And it is always true that $R_s(t) \geq \max (R_1(t), R_2(t), \dots, R_n(t))$

The large “pi” symbol means that the quantity $(1-R_i(t))$ must be multiplied together for all i in the set $(1, \dots, n)$. A consequence of this is that the system reliability $R_s(t)$ is always at least as high as the best reliability component.

Real systems always are some combination of series and parallel component reliabilities and detailed calculations are needed to determine system reliability.

A good example of using these principles is to increase system reliability by use of redundancy (i.e. parallel systems). The concept is displayed in Figure 81.

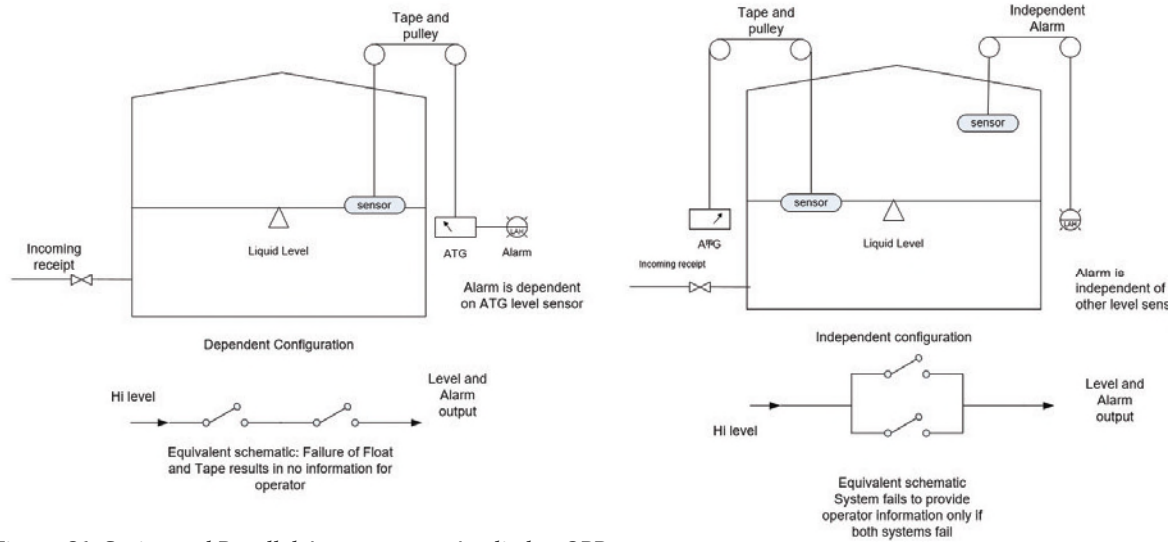


Figure 81: Series and Parallel Arrangement Applied to OPP

In the “old days” it was common to use the left panel configuration where the normal condition is shown by the open switches. In an alarm condition the switch is supposed to close. If either of the high-level sensors fail, then the level gauge and the entire system fails because the alarm condition is blocked by the failed open switch. This failure is a dangerous undetected failure (i.e. the operator will never know that there has been a failure). To increase reliability, the level sensing circuit is separate from the ATG so that a failure of one or the other does not cause a total loss of level information for the operator (i.e. either the alarm operators or the ATG is likely to remain operating). Because failure of level sensors (called “level detectors” in the 1st and 2nd editions of API 2350) resulted in numerous overfills, the standard suggested using independent and diverse technologies for the ATG system and the alarm system so that a failure of one would not cause a failure in the other system.

The concept of redundancy is shown in the right panel of Figure 81. Redundancy in a system is the parallel arrangement of components which perform the same function. Therefore, if one of the components fails then a replacement is simultaneously able to compensate. An example for redundancy is the parallel arrangement of components which has a $\frac{1}{100}$ chance of failure.

The probability of both the component failing simultaneously is then:

$$\left(\frac{1}{100}\right) \times \left(\frac{1}{100}\right) = \frac{1}{10,000} \text{ or } 0.01\% \text{ chance of failure}$$

Diversity is another important aspect in the design of an OPP. For example, a float & tape gauging system poses the risk of a mechanical failure due to sticking, but will be uninfluenced by the loss of electrical power. Therefore, having a mechanical gauging system in addition to an electrical gauging system provides diversity in addressing the concerns of normal operating conditions and electrical failure conditions. Layers of protection should be diverse when feasible and account for a multitude of initiating risk events.

These ideas apply to modern electronic systems as well except that there may be hundreds or thousands of components in a single instrument. In fact, the idea of SIL Certification (safety instrumented system certification) depends on assessing the overall system reliability using formal methods before the system can be SIL rated. It must be mentioned that even a perfectly reliable device could fail to operate if other components affecting reliability are not addressed. A good example of this is a perfectly reliable alarm system. Despite system optimization, an overfill can still occur if the operator is gone, cannot hear the alarm or is unavailable to act. Inevitably the λ value for a system can never achieve zero, because it is impossible to account for every potential failure mode.

Failsafe Circuit Design

The method of powering and activating an alarm, sensor, control valve, and other process control equipment is a large factor towards the safety and reliability of a process. Control systems should be designed in a way that operators can determine when equipment is not operating properly. A broken High-Level Alarm could lead to an overfill event which means millions of dollars in losses or worse.

Therefore, it is critical to design process control equipment which is “failsafe”, meaning that the failure mode for the equipment is designed in the safest conceivable way. The design of failsafe systems is never perfect but can be continuously improved. The choice of how to invest company money to improve process safety is dependent on the results of risk analysis at a facility.

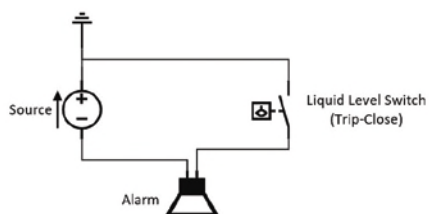


Figure 82: Simple Level Alarm Circuit Diagram (Failure Prone)

The primary concern when designing failsafe electronic systems is the failure mode when a wire breaks or the circuit opens somewhere preventing signal transmission. A simple circuit for a level alarm is shown in Figure 82. If the line were to break at any position, current would be unable to flow through the alarm, and operators would be unaware when setpoint conditions are reached. This design is unreliable because a cable break at the level switch would be a “dangerous undetected failure”; that is, the operator is unaware that the level could be approaching an overfill condition.

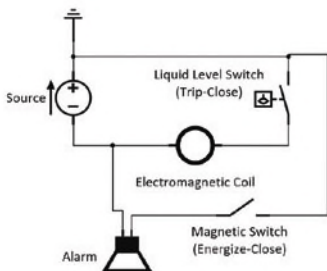


Figure 83: Alarm Relay Circuit Diagram (Failure Prone)

Figure 83 shows a relay circuit used for level alarm. When the level setpoint is achieved, the liquid level switch closes allowing current to flow through the electromagnetic coil. The current through the

coil generates an electric field which energizes the magnetic switch. The magnetic switch then closes when energized by the coil, activating the alarm. This system is prone to the same failures as the simple diagram above. A wire break at any position will cause failure of the alarm without notifying operators. This type of failure is called “fail-to-danger” because even though the alarm function has failed because of a fault in the electrical circuit, no one can know about it without looking for it.

It is therefore advantageous to design such a system where breaking a wire or tripping the level switch results in activation of the alarm.

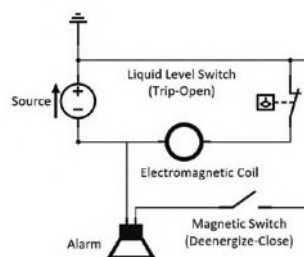


Figure 84: Alarm Relay Circuit Diagram Trip on De-energize

Figure 84 appears like the relay circuit in Figure 83 but with some key differences. The liquid level switch opens when setpoint conditions are achieved, opposite the previous relay design. The liquid level switch is in the closed position during normal operations, energizing the electromagnetic coil. The electric field produced by the coil keeps the magnetic switch in the open position, opposite previous relay design. When the coil is deenergized, the magnetic switch closes, allowing current to flow through the alarm.

The system in Figure 84 is a better option of the two schematics shown because breaking a line between the level switch and coil will deenergize the coil, closing the magnetic switch and activating the alarm. This type of failure mode is called a “fail-to-safe” condition, because in this configuration, the alarm will activate upon the liquid level reaching setpoint conditions or there is a fault in the electrical sensor circuit.

There are additional opportunities to improve the circuit shown in Figure 84. If the power source were to fail, then the alarm system would be inoperable. Auxiliary power, such as generators, may be installed for redundancy and increased process safety. Implementing failsafe circuit design with redundant power is a major step towards implementing a true Overfill Prevention System. It is critical for level sensors, controllers, and actuators to continuously perform within specifications to prevent an overfill.

Level Gauging Accuracy

Type if Gauging	Number of Measurements	API Required Accuracy
Manual Gauging	3	1/8 inch (3 mm)
Automatic Gauging (Inventory)	3	1 inch (25 mm)
Automatic Gauging (Custody Transfer)	3	3/16 inch (4 mm)

Figure 85: Accuracy Requirements by API MPMS Ch3.1A (Manual Gauging) and Ch3.1B (Automatic Gauging)

By API MPMS Ch3.1B the values above are corresponding to the installed accuracy of the ATG, not bench accuracy. Bench accuracy is dependent on the sensor type and quality of the sensor. The bench accuracy should never be below the installed accuracies as provided in Figure 85.

The international standard and recommendation regarding hazardous liquid overfill preventing is OIML R 85 – Automatic level gauges for measuring the level of liquid in stationary storage tanks. This standard has different specifications than API MPMS Ch3.1 or API 2350 that are often used in Europe and around the globe. OIML is a Metrology organization and has developed rated operating conditions, as shown in Figure 86.

(a)	Ambient temperature	low	+5°C, -10°C, -25°C or -40°C (**)
		high	+30°C, +40°C, +55°C or +70°C (**)
(b)	Relative humidity	up to 93%	
(c)	DC mains voltage (*)	As specified by the manufacturer	
(d)	AC mains voltage (*)	$U_{nom} - 15\%$ to $U_{nom} + 10\%$	
(e)	The minimum and maximum temperatures of the liquid and the medium above the liquid		As specified by the manufacturer
(f)	The minimum and maximum pressure in the tank		
(g)	The characteristics of the liquid and of the medium above the liquid		
(h)	The minimum and maximum densities of the liquid and of the medium above the liquid		
(*) Whatever is applicable			
(**) This value is to be decided by the national authority as it depends on the climatic conditions and the expected conditions of application (indoors, outdoors, etc.) that are different in different countries.			

Figure 86: OIML R 85 Metrological Requirements

OIML R 85 also lists maximum allowable errors for an ATG immediately after installation and thereafter. These standards are shown in Figure 72.

Description	MPE
Prior to installation	1 mm
After installation	4 mm

Figure 87: OIML R 85 - ATG Maximum Permissible Error

Each form of level measurement requires assumptions that limit the reliability of the measurement. For example, piping, buoys, and prerreferral equipment

displace some liquid within the tank. This volume of displaced liquid is accounted for but varies throughout the depth of the tank.

Importantly, the accuracy of an ATG is dependent upon the accuracy of the manual gauge because the ATG is calibrated and verified by using a manual gauge. A verified and accurate manual gauge is necessary to calibrate an ATG. This dynamic requires that a manual gauge must be more accurate than an ATG to assure the measurements of the ATG.

Recall, both the ATG and manual gauge must be verified monthly when used in custody transfer applications and quarterly when used for internal inventory control.

Further, it is assumed that the level in a tank is a flat plane that is parallel to the radius of the tank. The level is not perfectly flat or parallel. The liquid level fluctuates between points on the surface due to surface tension with the shell as well as pressure fluctuations. The shell of a tank is never perfectly perpendicular to gravity because of variations in the tank foundation and settling over time. These factors cause the liquid level to have some pitch compared to the vertical centerline of the shell.

Also, the density of liquids is dependent on the temperature and pressure of the surroundings. Therefore, temperature fluctuations cause some variation in density throughout a tank. We generally assume temperature is constant throughout the liquid during level measurement, but the temperature will vary throughout the tank due to heat transfer occurring across the shell and roof. Additionally, the cross-sectional is usually assumed to be constant for vertical cylindrical tanks, where:

$$\text{Area} = \Pi r^2$$

In application, hydrostatic pressure on the walls of the tank create a bulging effect on the tank walls. Bulging can increase the cross-sectional area of the tank, yet go unnoticed. This bulging would increase the total volume of the tank.

Sidebar

Power Sources

Power sources are categorized by their method of operation and the intention of use. The definition for each class of power sources is defined by Federal Standard 1037C and MIL-STD-810. All systems, instruments and actuators which require electric power for normal operation are dependent upon their power supply and should always be considered in design, maintenance, emergency preparedness, and emergency response of a storage tank facility.

Primary Source:

Class A sources are primary power sources that assure a continuous supply of power.



Auxiliary Source:

Class B sources offer standby power that can provide for extended periods, on the order of days.

Class C sources are quick start units (10-60 seconds) that can cover short-term outages, order of hours.

Class D sources are units which use stored energy to provide continuous electric power within a specified voltage and frequency tolerance, uninterrupted power supply (UPS).



Chapter 8 – Procedures, Operations, Testing and Maintenance

Procedures

Once the user understands the important of preventing overfills and the responsibilities that they have, the next question is 'how do we do it'. This chapter will provide the long standing corporate proven method of focusing resources to achieve a result. In this case, it is the management systems as applied to overfill prevention systems. Here we emphasize that an abstract model for such a system is built into API 2350. The owner/operator of tanks should develop overfill management system templates to ease the problem of companies adapting to the current edition of API 2350.

Because most tank filling operations use manual operations to transact the receipts, procedures provide the foundation for correctly operating the tank facilities under the wide variety of circumstances that occur. Overfill procedures are integral to the facility overall operating criteria and may be written as a single document or broken down into detailed and specific entities. In some cases, the owner/operator may wish to write procedures that are exclusively for overfill prevention and do not cover day to day operations. These choices are entirely up to the owner/operator and to a significant extent depend on what the owner/operator already has in place before API 2350 4th or 5th editions are incorporated for compliance.

Various procedures can be categorized as follow (although there is no universal categorization):

- Basic operations (pre-receipt planning, communications with transporters, etc.)
- Operator training
- Maintenance
- Inspection
- Testing
- Calibration
- Abnormal operations (power out, storms, etc.)
- Equipment systems
- Risk assessment
- Management system
- Management of change
- Safe operating limits
- Pre-startup and post-shutdown
- Unique operations (such as multiple tank filling at same time, gravity filling procedures, etc.)
- AOPS related

Some of the most essential elements of these procedures are now discussed. We only consider formal written procedures since they are the only way to ensure that there is a procedure, that it is universally understood and that everyone involved is subject to these same requirements.

At the top of the heap are the procedures for management systems. Management systems translate the key corporate leadership messaging to the details in the field. They state what shall be done and how it shall be done. They set the umbrella under which all activities related to tank receiving and overfill prevention is accomplished.

Next, procedures that guide the way to assess risk are important to ensure that there is uniformity and consistency in the way that risk analyses are conducted especially for larger companies which may have multiple facilities with multiple tanks. The application of consistent approaches will do much to ensure that risk ranking processes and assessments are as accurate as possible especially given that different people may be conducting the assessments for different facilities.

Operating procedures are critical because they set the requirements for how and when communications are to take place between operations and the transporter, before, during and after the receipt. They enforce a degree of awareness of what the state of the tank filling operation is which turns out to be one of the most important ways to prevent overfills. Procedures also specify how and when operational parameters are defined and implemented. In addition, the procedures can be used to help get the population of tanks transitioning to compliance with the standard in a systematic and formal way.

Because operating needs may lead to the need to fill a tank beyond its normal level or H or HH level, they ensure that a pre-thought out plan is established to handle these kinds of events where the risk has been dealt with in advance by a qualified person or team.

Although we do not go into detail related to testing, inspection, and maintenance these are all critical activities that require well written procedures. One cannot over emphasize the importance of rigorous procedures for proof testing. Proof testing is what the name implies; it tests a complete instrument loop to validate the belief that the system is operating correctly.

Chapter 9 – How to Develop an OPP (Overfill Prevention Process)

Developing an OPP is challenging for many reasons. One key reason is that it takes top management support as well as resources applied to the problem over extended periods of time. Many tank owner/operators are not even aware that serious tank overfill incidents have taken place. Moreover, if there is not a recent incident fresh in corporate memory it is natural to believe that “this type of incident doesn’t happen in my company”. Without drive by the top senior management, the effort to follow API 2350 will be minimal and not effective.

Another challenge for larger companies is the vast quantity of tanks that must be addressed. Getting to a point where a company could say that it complies could take several years to a decade. This is because valid risk assessment requires information ranging from tank configuration to environmental factors for each tank. It also requires establishing a practical and effective database or data management system that tracks the inventory of tank overfill protection systems as well as the progress over time. While this is being done there will usually be various changes occurring to different tanks which may not be reported to those responsible for the tank overfill protection program.

Another challenge is the integration of the overfill management system into any existing management system if the company has a management system. For companies that do not have management systems, the adoption of an overfill management system will raise the question of the broader overall safety management system. Each company must consider how they will credibly use a management system to ensure that OPP is a part of that system. This requires subject matter expertise and a good understanding of how safety management systems are used, developed, and deployed.

Risk assessment is another major challenge. There are many schools of thought about how to do risk assessment and how the results should be treated. A first reasonable step in the process is to do risk screening so that focus can be applied to the correct priorities. Examples of how this could be done were given earlier in this guidebook. But where considerable risk is thought to exist, then more formal and quantitative methods may be required. Despite guidance provided by API publications such as those in API 353 or API 581 there are many alternatives and the alternatives may be more suitable to a better and more practical answer.

Even if each tank were perfectly risk assessed the problem would not be over. The risk assessment will likely generate many projects that will require a significant budget and schedule to implement. The question of how to allocate resources to implement the risk reduction project then becomes important. Moreover, other risk reduction projects will be competing for resources to reduce risk. A sound decision making process is therefore required. This is an area for which the science and technology has been developed but which maybe underutilized.

Overall, the challenges are significant. Therefore, top-level leadership and messaging is required to install the culture that puts in the resources and effort required to operate flawlessly without overfills. We hope that this guide will provide your company with the necessary tools and ideas to implement a robust and effective tank overfill program.

Appendices

Abbreviations

- ACC – American Chemical Council
- AIChE – American Institute of Chemical Engineering
- AOPS – Automatic overfill prevention system
- API – American Petroleum Institute
- API 2350 – API standard regarding overfill of aboveground storage tanks
- API 2610 – API standard regarding design, construction, operation, maintenance and inspection of terminal and tank facilities
- API 580 – API standard related to risk based inspection of aboveground storage tanks
- API 650/653 – API standard regarding construction and maintenance of tanks
- API MPMS Ch 3.1 – American Petroleum Institute Manual of Petroleum Measurement Standards
- AST – Aboveground storage tank
- ATG – Automatic tank gauge
- BPSC – Basic process control system
- CAPECO – Caribbean Petroleum Corporation Oil Refinery
- CAPEX – Capital expenditures
- CCPS – Center for Chemical Process Safety
- CHL – Critical high level
- CLL – Critical low level
- FMCW – Frequency-modulated Continuous-wave
- HHLA – High-high level alarm
- HLA – High level alarm
- IEC – International Electric Commission
- ISA – International Standards Association
- LFL – Lower flammable limit
- LOC – Levels of Concern
- LOP – Local Oversight Program
- LOPA – Layer of Protection Analysis
- MEER – US court decision, atmospheric storage tanks do not apply to OSHA Standard 1910.119
- MOC – Management of Change
- MOP – Maximum operating pressure
- MOPS – Manual overfill prevention system
- MWL – Maximum working level
- NFPA – National Fire Protection Association
- OPEX – operating expenditures
- OPP – Overfill prevention process
- OSHA – Occupational Safety and Health Administration
- PEG – Portable electric gauge
- PSM – Process safety management
- RAGAGEP – Recognized and Generally Accepted Good Engineering Practices
- RP – Recommended practice
- SIF – Safety instrumented function, hardware and software used in a critical process system.
- SIL – Safety integrity level, measurement of performance of a Safety Instrumented Function (SIF)
- SMS – Safety management system
- STI – Steel Tank Institute
- TOF – Time of Flight
- UFL – Upper flammable limit
- UK HSE – United Kingdom Health & Safety Executive
- VCE – Vapor cloud explosion

Key Terms and Definitions

Alarm:

Alarms require action. They are an auditory and/or visible means of indicating to operating personnel an abnormal condition requiring a specific response (high tank level, equipment malfunction or process deviation). Some alarms connect with an AOPS which act automatically to prevent an overfill.

Alert:

Alerts are audible and/or visible notification indicating an equipment or process condition that requires awareness.

Attendance:

The term describing when personnel are physically on site at the facility where the tanks are located during receiving operations.

Automatic Tank Gauge System (ATGS):

A system incorporating an ATG; the system is designed to continuously measure liquid level in a storage tank. No operating personnel action is required to determine the level. The measured values, alerts and alarms are transmitted to a local and remote monitoring and control center that can display the levels and receive alerts and alarms. An ATG system may also have a local display at the tank.

Critical High Level (CHL):

The highest level in a tank before an overfill or tank damage begins to occur. After hazardous liquid has surpassed the CHL emergency management response is required to clean up spilled liquid and repair tank damage. "The highest point of no return."

Critical Low Level (CLL):

The lowest level in a tank before tank damage begins to occur. The legs, internal piping, and support features for a tank may become damaged, logged, or inoperable when the liquid level goes below the CLL. "The lowest point of no return."

Gap Analysis:

An analysis to determine if results of a risk-based analysis meet the acceptable levels as determined by the owner and operator.

High-High Level Alarm (HHLA):

One response time level below the critical high level (CHL). The HHLA has a required alarm (by API 2350) and operator response. The HHLA is the last warning during a filling operation prior to an overfill event.

Hydrostatic:

Relating to the equilibrium of a liquid body at rest and the resulting pressure.

Independent Alarm:

An alarm system in which no components are also used in the (ATG) system.

Level Alarm:

At a specified level, a sensor is triggered, sending a digital, visual, or audio signal to the operator or system. The operator or system must then act to intervene.

Levels of Concern (LOCs):

Calculated product levels in a tank that allow the owner and operator to determine appropriate levels to set alerts, alarms or AOPS functions. See: Critical high level, Critical low level, High-high level alarm and Maximum Working.

Level Control System (Closed-loop System):

A system which sends an electronic signal from a level sensor to a control valve to prevent overflow. The automated control valve is responsible for intervening the flow of liquid into or out of the tank.

Level Indication System (Open-loop System):

A system which displays the height, volume, or mass of liquid within a tank. An operator must intervene to stop of flow of liquid into or out of the tank.

Liquid/Liquid Interface:

The surface area between two insoluble liquids, such as water and octane.

Maximum Working (MW):

The highest intended level for normal operations. This level is defined by the company and is below the HHLA. An alarm or alert is optional at the MW. By API 2350, the company must define the MW for compliance.

Noise:

The variability of sensor measurement at steady state operating conditions.

Operator attendance:

This is the term that describes the number of individuals required to terminate tank receipt operations. For example, an AOPS system is automatic and require zero operators in attendance, whereas as Category 3 tank requires an operator to terminate the flow when the intended level is achieved.

Parallel Tanks:

Two or more tanks at the same facility that can be filled simultaneously and effectively operated as one tank.

Piezoelectric:

Relating to certain materials which generate an electric field in response to mechanical stress and produce mechanical stress when subjected to an electric field, such as quartz.

Reference Point:

Protrusion from the gauge hatch used when conducting manual gauging operations by API MPMS Ch3.1.

Response Time:

The amount of time required to terminate a tank receipt. This is a measured variable and is dependent on procedures, the safety management system, operators, and overall circumstance.

Risk Assessment:

The identification and analysis with judgments of probability and consequences (either qualitative or quantitative) of the likelihood and outcome of specific events or scenarios that result in harm or damage.

Sensors:

Continuous or point type sensing devices used to display an alert, calculate a value, trigger an alarm, initiate a shutdown and other diversion actions.

Servomechanism:

A powered mechanism that produces force at a higher level of energy than the input.

Span:

The range of liquid height at which a level transmitter can determine the liquid level.

Vapor cloud explosion (VCE):

The rapid evaporation and explosion of light hydrocarbons due to the overfilling of a tank.

Radiometric:

Relating to the measurement of radioactivity

Safety Management Systems – Key Elements

There is no “correct way” to organize and name the elements of an SMS/OPP. The OSHA Process Safety Management (PSM) regulation originally had 12 elements (which were later revised to 14 elements). The number and names of these elements vary; however, the exact number and name of an element is not important.

The key elements are listed below and correspond similarly to the elements of the PSM regulations. These elements can be applied in developing an SMS/OPP for any organization, however each system must be designed to work in an optimal manner within the organization developing and implementing it. *(Note: The key elements of an SMS are expanded in Supplement A in the specific context of overfill prevention)*

- Key Element 1: Safety and Environmental Advocacy
- Key Element 2: Safety and Environmental Information
- Key Element 3: Hazard and Risk Assessment and Analysis
- Key Element 4: Management of Change
- Key Element 5: Procedures and Safe Work Practices
- Key Element 6: Training
- Key Element 7: Equipment Integrity and Industry Standards
- Key Element 8: A Permit System
- Key Element 9: Start Up Safety Review
- Key Element 10: Emergency Response and Control
- Key Element 11: Near Miss and Incident Investigation
- Key Element 12: Auditing
- Key Element 13: Document and Data Information Management Systems
- Key Element 14: SMS/OPP Oversight, Review, Reevaluation, and Adjustment

General SMS/OPP Plan

An SMS/OPP Plan should define its objectives and how the organization intends to initiate, implement, and support the plan, then measure its effectiveness. The plan should also indicate how SMS/OPP will support and enhance the organization's business plan and objectives. The success of a plan depends on the following actions:

- Management must express positive and continuing commitment to safety, environmental protection and overfill prevention and state the policies, objectives, and requirements of the SMS/OPP
- The organization must define the structure of the SMS/OPP as well as the responsibilities and authority of key individuals for managing the SMS/OPP
- Management must consider, define, and incorporate each element of the SMS/OPP into the overall organization's operations, work practices and procedures. (*Note: See Supplement A*)
- Management must convey the expectations and objectives of the SMS/OPP to all employees
- All employees must be able to identify and apply the elements and objectives of SMS/OPP and understand their responsibility to maintain compliance with organization policy.

The SMS/OPP plan must address many details, including, but not limited to, equipment evaluations, automatic tank gauges and alarms, facility and site engineering, equipment procurement and installation plans, product changes, tank receipts and delivery operations, how and when to upgrade existing systems and many other considerations. The SMS/OPP plan must be documented and written so that those responsible for administering it, implementing it, evaluating it, auditing it, upgrading it, and changing and improving it have a clear and concise understanding of the requirements and application of SMS/OPP in relationship to the facility's operations and potential hazards.

Summary: Recommendations and Conclusions

Organizations may ask - "Why should we adopt the current edition of API 2350". The answer to this question is different for each organization. API 2350 has made a notable change in the 4th edition by requiring that a management system be deployed for overfill prevention. If an organization decides to adopt the requirements of API 2350, either fully or partially, then the recommendations herein need to be considered. Complying with the requirements of API 2350 is a major task that needs to be done within the framework of the organization's overall safety and environmental management programs and policies.

Although API 2350 requires a management system for overfill prevention and protection, it does not specify how to develop or implement one. Organizations typically rely upon management systems that have been developed because of serious incidents in the past. These management systems are common among large and mid-size organizations. These organizations have learned to use these systems to reduce, control and manage serious incidents as well as to improve other aspects of their businesses. To be effective, these systems must be integrated into the "corporate culture". They require significant time, energy and resources and must be actively supported by the very top level of the organization.

It is recommended that organizations which do not use any form of safety management systems consider developing not only a basic SMS/OPP if they operate storage tanks, but that they ensure that the safety management system incorporates the relevant principles outlined here and in API 2350. The conclusion is that organizations need to manage health and safety with the same degree of expertise and to the same operating standards and practices as their other core business activities if they are to effectively control risks and prevent hazardous incidents.

Resources for Developing an SMS/OPP

There are numerous resources available to provide guidance and information to assist organizations in the development of SMS/OPP programs. Some suggestions for reference documents that may be used by organizations considering implementing an SMS/OPP include, but are not limited to, the following:

OSHA Process Safety Management (PSM) Standard (CFR 1910.119)

Many large organizations and facilities are required to comply with the OSHA Process Safety Management (PSM) standard. Due to specific regulatory exemptions, the OSHA PSM standard is not applicable to numerous tank facilities. There are, however, many aspects of the PSM Standard that are important to these exempt facilities in conducting safe operations. A careful review and adaptation of specific requirements of the PSM standard can provide a good starting point for an organization considering developing an SMS/OPP. These requirements can be reviewed, modified, and incorporated into the organization's SMS/OPP as appropriate to their specific operations and facilities. OSHA is an agency within the US Department of Labor, but OSHA policies are used internationally. Europe, Asia, and other countries have their own OSHA agencies which collaborate to develop worldwide standards for worker health and safety.

API 75L Guidance Document for the Development of a Safety and Environmental Management System (SEMS) for Onshore Oil and Natural Gas Production Operations and Associated Activities, First Edition, November 2007:

API 75L is intended for use by the upstream sector of the oil industry. Nevertheless, all the fundamentals of the SEMS can be applied to downstream facilities as appropriate.

Health Safety Executive HSG65

The UK Health Safety Executive document HSG65 provides information to assist users in understanding the requirements and ingredients needed to develop good safety management systems. *(Note: HSG65 can be downloaded at no cost)*

This document provides a “performance based approach in framing the requirements of a management system to include OPP. Its intention is to assist organizations to choose their best way to achieve their safety performance.

The Key Elements of SMS/OPP

The following sections identify the prerequisites and requirements associated with each of the key SMS/OPP elements. Successful overfill management systems are tailored to fit an organization's size, nature, requirements, and operational complexity. Although the specific details and levels of documentation of SMS/OPP may vary, considering the key fundamental attributes will assist organizations in the development of a viable SMS/OPP.

The fundamental element of SMS/OPP is that it is based on the PDCA (Plan, Do, Check, Act) cycle. This provides for the process to be continually monitored, upgraded, and improved using metrics that support and justify improvements. (*Note: Figure 2 is a graphic from HS65 which illustrates the PDCA concept*). Although the details and level of documentation of a SMS/OPP may vary, the following key elements will assist in developing and ensuring the SMS/OPP will be effective for any organization:

Key Element 1: Safety and Environmental Advocacy

Safety and environmental protection (elimination of overfills) must be recognized, supported, and accepted as "key organizational values". Procedures, practices, training, and the allocation of resources must demonstrate management's commitment to safety, environmental protection and overfill control and elimination.

The first key element in SMS/OPP is to initiate a policy that states the organization will adopt API 2350 (or an equivalent version of the standard). When top management establishes this policy, it signals to the entire organization that preventing overfills is serious business and that resources will be allocated to establish, implement, and support SMS/OPP.

The key elements that are important to effectively promote the values that are necessary to support and sustain SMS/OPP include, but are not limited to, the following:

- Express in writing a clear and unequivocal commitment to SMS/OPP by top management.
- Demonstrate top management's commitment to SMS/OPP by example (i.e. by funding SMS/OPP projects, procedures, and standards and by ensuring that management supports control, prevention, and elimination of overfill incidents and near misses by funding training, equipment, and processes.
- Establish a management position that requires supervisor and employee engagement and participation in SMS/OPP at all levels of the organization.
- Provide for universal management communication to all employees regarding the goals and benefits of SMS/OPP.
- Define competency requirements for those individuals in responsible positions.
- Provide appropriate training for personnel based on levels of involvement and responsibilities for SMS/OPP and document, review and, as necessary, update training requirements.
- Network with other organizations and industry associations to share "lessons learned" that promote improvement of the SMS/OPP.
- Develop and implement a feedback system for near misses and incidents that promotes participation by all personnel for improving control, management, and elimination of incidents through behavioral changes.
- Develop and implement a "Just Culture" process that ensures fairness and open reporting in dealing with human error.

Key Element 2: Safety and Environmental Information

Process safety provides the organization with complete and accurate written information concerning the products stored and the equipment and processes used in a facility. This information is needed to implement the other elements of SMS/OPP. Detailed product information, operational procedures, safe work practices and environmental implications are required for each tank for SMS/OPP to be viable,

The key elements of safety and environmental information include, but are not limited to, the following:

- Determine and set product levels in the tank (levels of concern or LOC) including maximum working level, high-high level, and critical high level.
- In addition, because of operating preferences or if required, the organization may also decide to set alert levels, such as a high operating level.
- Evaluate tanks that have automated high level shut off valves for suitability for service (in the context of safety instrumentation systems standards such as ISA S84.01 or IEC 61511).
- Establish a level of attendance for each facility or tank (i.e.: fully attended, semi-attended, and unattended)
- Determine the type of automatic tank gauge (where provided) and whether the alarm is independent or dependent upon the automatic tank gauge.
- Determine types of sensors used for alarms.
- Establish criteria for alarms and/or automatic operations.
- Determine the tank alarm type (audible and/or visual) and whether it is distinctive from other alarms (fire, vapor, or gas release, etc.)
- Review and update as needed, existing inspection, testing and maintenance procedures and practices.
- Establish whether alarms are to be treated as operational aids or as specific actionable procedural notification devices.
- Determine the type of liquid (NFPA 30 Class I, II, or III) contained in each tank and requirements applicable to their storage, handling, and fire protection.
- Establish for each facility, the appropriate methods of receipts from pipelines, tank cars or tank trucks, marine vessels, or combinations thereof, dependent upon the types of tanks and products involved.
- Review and update as needed, existing operating procedures and safe work practices, including those for daily (normal) operations, periodic inspection, maintenance and testing, on-site contractor work and emergency situations (vapor releases, liquid spills, fires, explosions, inclement weather, floods, civil disturbances, etc.
- Determine the amount of response time required by operations to terminate receipts safely and effectively.
- Determine and record the API 2350 category for each tank.
- Develop and implement a risk assessment and management process that can be applied to meet the risk component requirements of API 2350.
- Establish protocols for handling and managing receipts between outside parties and the organization on a regular basis and during emergency conditions.
- Establish procedures for handling operations when power is interrupted (i.e.: which facilities have uninterruptible or emergency power supplies, which revert to another mode of operation, which shut down, etc.).

Most important, it is essential that an organization have knowledge of what existing industry best practices are regarding similar operations. Some of the best places to obtain this knowledge is through industry standards. (*Note: Additional information about industry standards is covered in Key Element 7: Equipment Integrity and Industry Standards*) and by networking with other organizations.

Key Element 3: Hazard and Risk Identification, Analysis, and Assessment

It is most important that the SMS/OPP include an organized process to identify, analyze, assess and manage hazards (including potential hazards) and risks.

The key elements of hazard and risk identification, analysis and assessment include, but are not limited to, the following:

- Identifying the numbers and types of tanks involved and their contents.
- Recognizing and understanding the impact of tank storage and potential incidents upon adjacent equipment, facilities, and operations (and vice-versa).
- Identifying and determining the risks associated with existing and potential overfill hazards. This includes those risks associated with organizational changes (such as when an organization is undergoing rapid growth; experiencing a reduction in resources; installing or acquiring new equipment; changing services, products or methods of operation and reducing, increasing, or reassigning personnel).
- Performing an analysis that shows the existing system contrasted to the idealized system and identify where the least to most significant gaps exist
- Developing and implementing a process to assess, prioritize, analyze, and manage risks, including tracking identified risks and benchmarking actual progress against projected progress

This guidebook does not provide detailed methods of risk analysis and assessment. There are many resources available to assist organizations in performing these analyses. Some organizations may have internal expertise to analyze and assess risks. Other organizations may use consultants and outside experts who can assist in performing these analyses and assessments. Each analysis, assessment and management technique has pros and cons and each requires a different level of expertise and resources. Organizations may wish to use a variety of techniques so that results are optimized.

A multidisciplinary team, which has sufficient expertise in both tank operations and equipment and in risk analysis and assessment process, is required to achieve the best results. This is true with all types of risk techniques because (1) qualitative methods rely on intuitively assigning appropriate likelihoods and consequences, whereas (2) quantitative methods require sophisticated modeling skills. For example, in very simple cases, a what-if or checklist type or other qualitative technique may be adequate. For more involved assessments, a matrix type approach (*Note: see Figure 19*) or other semi-qualitative approach may be appropriate. For cases where the hazards and risks are high, a quantitative analysis may be required. (*Note: One resource for information regarding the development and implementation of a hazard and risk analysis and assessment program is the IEC Standard 31010 "Risk Management - Risk Assessment Techniques*).

Key Element 4: Management of Change

Unless properly managed, changes in organizational structure, personnel, documentation, processes, equipment, operations, products, and procedures can result in the inadvertent introduction of hazards and risks. The potential for hazards and risk is prevalent when the organization acquires a new facility, new and different equipment, or changes products. Management of change is the SMS/OPP process by which organizations control the impact of these occurrences and minimize the potential of increased risk.

The Management of Change Elements applicable to tank overfill prevention and protection include, but are not limited to, the following:

- Analyzing changes in operating procedures, practices, and processes to identify any required changes in training, documentation, or equipment
- Analyzing changes in equipment, products and operating conditions for potential risks and hazards
- Ensuring all maintenance, operating procedures, and manuals are kept up-to-date with the most current changes
- Establishing a system to ensure that all personnel are made aware of and are trained or knowledgeable in and understand all changes and requirements in equipment, operations, procedures, and products including applicable maintenance and operator manuals
- Designating the level of management that must approve a change and assigning responsibility and accountability

Key Element 5: Written Procedures and Safe Work Practices

API 2350 requires that written procedures and safe work practices be developed and implemented within the organization. It is highly recommended that each organization establish a requirement to review, analyze and determine, on a regular, ongoing basis, the need for changes in procedures and work practices. Typically, this results from the process that manages changes to an overfill system, including, but not limited to, installing a new tank or equipment, upgrading tanks or technologies; changing operating methods or products and acquisition of a new facility. Updating procedures and safe through the management of change process ensures that the quality of equipment and the state of technology increases with the passage of time.

The key elements to be covered by written procedures and safe work practices include, but are not limited to, the following:

- Normal operations
- Abnormal operations
- Emergency operations and response
- Equipment testing, inspection, maintenance
- Procedures covering working with third parties such as pipeline operators, the transporter of marine receipts, outside contractors working within the facility, etc. (Note: Details are included in API 2350)
- Training and educating workers and defining and evaluating competencies and work practices through the management of change process.

Management system elements specific to overfill prevention include, but are not limited to, risk identification, analysis and assessment, establishment of operational parameters (LOCs, alarms types and levels, response times, etc.), incident and near miss data collection and evaluation and other elements of the safety management system.

Key Element 6: Training and Education

All personnel should be given introductory and recurrent SMS/OPP training and education commiserate with their work assignments and the degree of training required by their involvement in the SMS/OPP process. The key elements for establishing training and education requirements for the organization include, but are not limited to, the following:

- Mandating and providing safety orientation for all new and reassigned employees and contractors, stressing the organization's commitment to, environmental protection, safety, and everyone's role in the OPP.
- Providing training and education in operational procedures and safe work practices for all supervisors, employees, and contractors applicable to their regular and extraordinary work assignments.
- Establishing and implementing a system to track training requirements, objectives, and fulfillment.
- Assuring and documenting that all personnel have met job competency requirements.
- Making effective use of regularly scheduled safety training meetings, daily safety reminders, conferences, workshops, and educational materials such as literature and trade journals

Key Element 7: Industry Standards and Equipment Integrity

Industry standards and best practices are the primary and most reliable resources for developing and implementing a SMS/OPP. API 2350 is the important industry standard that a terminal operation should depend upon to manage, control, and prevent overfills. API 2610 and the Buncefield Report are valuable resources as they reference all the best operating practices and relevant tank standards applicable to terminal operations. Organizations should understand that it may not be necessary to comply with each requirement of every standard in every detail. Depending upon specific terminal equipment, products and operations, each organization needs to make an informed decision as to what requirements are relevant and appropriate to their facility and incorporate these into their organizational standards, procedures, and safe work practices. *(Note: Industry standards are considered "minimum" requirements)*

If an organization uses AOPS (automated overfill protection systems), these should be reviewed in accordance with the requirements of ISA S84.01 or IEC 61511 for safety instrumented systems. It is good practice to include all the critical overfill protection systems, including, but not limited to, sensors, logic solvers, final elements, alarms, etc. into a fully managed system of procedures as addressed by these standards. *(Note: Most owner/operators will not perform a full loop test because of the difficulty of performing such without raising the liquid level to the point that there is a risk of an accidental overfill. Therefore, it is important to minimize the potential that some part of the loop may remain untested.)*

Endress+Hauser has developed proprietary technology which includes full loop testing for a wide variety of its systems. Including full loop testing into a company's routine maintenance program will reduce the likelihood of a "dangerous undetected" event. Proof testing the full loop of a system ensures that all the components within the system are operating properly when of tested. Regular proof testing gives both operators and investors the utmost confidence in the ability to control the hazardous liquid inventory at your facility. Regular proof testing adds value in the form of robust safety and peace of mind.

Each organization should have a written program to ensure the ongoing inspection, maintenance and integrity of equipment and processes. It is recognized that organizations may have several types of alarms, automatic tank gauges, sensors, data collection and transmission systems, communication systems, etc. Each of these items must have a regular schedule of checks, inspections, and routine maintenance to ensure continuing integrity.

Key Element 8: Permit Systems

No physical work of any kind should be conducted within, around or near storage tanks or the impound areas without the use of a formal work permit system. Hot work, cold work, lockout-tagout and any other work that has the potential to impact upon storage tank operations or processes should require permits.

The key elements of permit systems include, but are not limited to, the following:

- Permits ensure that potential and existing hazards are recognized, evaluated and appropriate control measures are implemented.
- Permits assure that personnel responsible for the facility are fully aware of on-going work.
- Permits provide for communications between employees and contractors.
- Permits ensure that appropriate safe work procedures and practices, including, but not limited to, required atmospheric testing and monitoring, use of appropriate protective equipment, control of sources of ignition and control of vapor releases are implemented before, during and after the work.
- Permits assure that abnormal conditions are addressed by requiring safe operating procedures for specific occurrences. Abnormalities include, but are not limited to, inclement weather and lightning in the area, malfunctioning or disconnected equipment, inoperative instrumentation caused by disuse or electrical system failure and unauthorized personnel, vehicles, and equipment in the permit area
- Permits assure that specific safe work procedures are applicable at times when work is performed near a tank receiving product if vapor or product is released from the receiving tank.

Key Element 9: Pre- Start-up Safety Review

A comprehensive safety review should be performed before start-up operation of any new or existing tank or system. Start-up typically occurs following routine or unplanned maintenance, reconstruction or repair and emergency shut-down.

The key elements of a start-up safety review system include, but are not limited to, the following:

- The review should cover management of change and risk analysis.
- The review should ensure that all essential action items identified by the risk analysis that involve the safety of the operation are completed prior to start-up. This includes, but is not limited to, validation of strapping tables and operational parameters such as response times and LOC settings.
- The review should assure that procedures and training required to operate a new or reconstructed tank are consistent with existing equipment and processes.

Key Element 10: Emergency Response Plan

Each facility should develop and implement a written Emergency Response Plan that outlines what specific actions are required when an accident, incident, overfill or near miss occurs, including the appropriate notifications to make and who is responsible for each action. The better prepared an organization is for an emergency, the better the chances that injuries to personnel and damage to equipment, property or the environment can be eliminated, controlled, or minimized.

The key elements of an emergency response plan include, but are not limited to, the following:

- The plan should address necessary actions to be taken in the event of overfills that result in fires or explosions, vapor or liquid releases, hazardous exposures, and environmental damage, as applicable.
- The plan should identify and assure that personnel that are to be the first to be notified or required to respond are readily available.
- The plan should assure that its requirements are relevant and useful to personnel on duty and designated outside emergency responders.
- The plan should be exercised and tested periodically to ensure the adequacy of the plan and the readiness and capability of the responders.
- The plan should be updated whenever changes to SMS/OPP occur (management of change) and whenever personnel assignments or responder contact information or reporting criteria changes.
- The plan should be available to all personnel and management shall assure that all employees (and contractors working in the facility) are aware of, trained and knowledgeable in their responsibilities in the event of an emergency.
- The plan should be regularly practiced with training exercises and performance evaluations and feedback to assure that the procedures are correct, emergency response materials and equipment is available and that all personnel and responders can perform their assigned emergency response activities.
- The plan should be managed using a documented procedure like other operating procedures.

Checklists that are easy to use in an emergency should be developed and included as part of the emergency response plan. There may be several different checklists, each specific to the type of incident (explosion, fire, vapor release, spill, etc.) and its severity (near-misses, incident contained within the facility, exposure and impact on outside environment, population, or structures, etc.).

The key elements of checklists include, but are not limited to, the following:

- Identification and notification of designated facility first responders for emergency shut-down operations, control of releases, mitigation of exposures, fire control and suppression and site security and protection including external fire department and police response.
- Identification and notification of other responders including, but not limited to, the organization's top management, public relations safety, environmental and legal departments as well as local government, regulatory agencies, and public health department, as applicable.
- Priority of notification calls to make for flammable and toxic releases depending upon potential and actual hazards within and outside of the facility.
- Evacuation plans, including assembly areas within and outside the facility and a means of accountability for employees and contractors working in the facility.
- Establishment of an alternate emergency management and control center outside the facility in event of need to evacuate.
- After-incident site security and accident/incident investigation.
- Next of kin notification for injuries and fatalities.
- Initiating claims and insurance procedures in accordance with organization policy.
- Handling news media (during incident) and public relations (following incident).

Key Element 11: Near Miss and Incident investigation

Every near miss and actual incident should be thoroughly investigated for gathering information to help prevent similar occurrences and to evaluate the performance of the safety management system and make improvements where needed. Just because a near-miss occurs or an incident is contained within the facility with no harmful impact is not a reason to neglect a thorough investigation to determine the cause. The next time a similar event occurs, it may lead to a fire, explosion or release of hazardous materials impacting internal and/or external facilities and operations.

The key elements of near-miss and incident investigations include, but are not limited to, the following:

- Determining how, when, what and why the event happened, rather than “who’s to blame”.
- Using a reporting system that does not assign blame, but near misses and incidents as learning opportunities to help employees achieve a higher level of performance. Once blame enters the picture, the entire system is in jeopardy and fails to have any value as a management tool. *(Note: This can be better understood by reviewing one or more available behavior based safety systems).*
- Ensuring that the person conducting the investigation is technically qualified, unbiased and has access to information, resources and other personnel with expertise that may assist with the investigation.
- Identifying immediate causal and contributing factors.
- Identifying and evaluating organizational factors that may have exacerbated the hazard or incident.
- Determining the potential to improve the SMS/OPP.
- Identifying both acts of “omission” and “commission”.
- Providing a written report to management with recommendations for improvements to the SMS/OPP to prevent similar incidents

Near misses and incidents, related to overfills, provide the opportunity to learn how to prevent similar occurrences in the future. SMS/OPP requires that procedures be in place for internally reporting near misses and incidents. Provided that the reporting process is timely and handled seriously, the information obtained allows the organization to analyze, determine cause, and adjust its SMS/OPP. The incident/near-miss report form should be simple, concise, and available to all employees.

The key elements of reporting programs include, but are not limited to, the following:

- A process for analyzing data, safety reports and other safety related information.
- Ongoing evaluation to confirm the effectiveness of corrective action.
- Ongoing monitoring to identify potential hazardous trends.
- A non-punitive disciplinary policy for persons that report hazards.
- Provisions for anonymous reporting of hazards.
- Feedback to the reporting person(s) and employees regarding proposed improvements or changes to the SMS/OPP.

Key Element 12: Monitoring and Auditing

The organization's safety performance needs to be continually monitored and evaluated to ensure that the key elements are not only kept up-to-date but are improved and that management and employees are properly implementing SMS/OPP. Because there are many variables that can lead to incidents or near-misses, there is a need to audit the management system to establish criteria and measure performance. The monitoring, evaluating, and auditing of SMS/OPP should be commensurate with the size, nature, and complexity of the organization.

The key elements of monitoring and auditing include, but are not limited to, the following:

- The results of all safety performance monitoring, evaluating, and auditing should be documented and used as feedback to improve the system.
- Specific and individual areas of concern should be addressed.
- Audit findings must be specific, measurable, achievable, results oriented and timely (SMART)
- Relying on accident rates as a measure of safety performance is not particularly effective and can lead to a false sense of security
- An assessment of improvements made to operating procedures and work practices is usually more effective than measuring accident rates

Key Element 13: Documents and Data Information Management Systems

Organizations should develop and implement written policies and procedures to identify, manage and document the information necessary to ensure compliance with both SMS/OPP and applicable regulatory requirements.

The key elements of documentation include, but are not limited to, the following:

- Establish a specific SMS/OPP document (based on API 2350) that applies to the organization's tank facilities and storage and receipt operations.
- Develop and publish a written document stating the organization's safety and environmental overfill policies and objectives.
- Provide access for all employees to pertinent regulatory and policy information.
- Implement a process to document SMS/OPP changes and updates and to communicate these to all personnel.
- Arrange for the prompt removal of obsolete or non-applicable documents.

An important part of documentation and information management involves SMS/OPP. This requires developing and implementing a comprehensive database for all facilities listing critical data about the tanks, the operations, equipment, and the facilities.

The key elements of an SMS/OPP database include, but are not limited to, the following:

- Determine the existing operating levels (such as maximum working level, high level alert, and high-high level alarm as well as the overfill/damage level), for each tank at each facility.
- Determine when the last tank was calibrated and if (and when) recalibration needs to be repeated.
- Determine how the alarms function (visible, audible, distinctive, etc.).
- Establish the maximum filling rate, both in flow rate and in level change in the tank per unit time,
- Determine if the facility is fully or part time attended or unattended.
- Establish the actual overflow level for each existing operating tank. *(Note: While this may be a challenge, it is necessary to set as accurate as possible. This is because the critical level is the starting point for establishing specific levels of concern per API 2350)*
- Classify each tank by assignment to API 2350 Categories I, II, and III
- Determine, for each tank, whether an AOPS (automated overfill protection system) is required *(Note: Application of risk assessment and risk management will help identify this requirement)*
- Develop an organization standard that specifies the minimum requirements by providing a system wide acceptable level of risk. *(Note: The standard should address how long a tank may continue to be out of compliance based on the risk it poses).*
- Ensure that each tank database includes the automatic tank gauging hardware manufacturer and model number and the types of logic solvers (relays and programmable logic controllers) that are used in the overfill operations.
- Establish the procedures for each type of filling operation for each specific product stored in each tank at every facility.
- Perform a risk analysis of each tank and integrate it into a facility and/or system wide risk assessment for all tanks.
- Establish an organization standard that addresses how long a tank may remain out of compliance based on risk. *(Note: Because of operating requirements and resource limitations it may not be possible to fix multiple tanks the same time, therefore prioritization, based on a gap analysis and compliance with the overall standard, is important).*
- Develop a gap analysis indicating how far each tank may be (or may not be) out of compliance with the tank standard and how much risk is incurred by this deviation.
- Ensure that each tank has an applicable written operating and emergency response procedure that is consistent with its risk and with the organization's standards.
- Establish and implement procedures to proof test all systems covered by the standard.
- Establish and maintain communications with all transporters to discuss and agree on the requirements and provisions covered in the organization's or facility's policies and procedures and in API 2350.
- Establish a protocol for managing and safeguarding out-of-service tanks.

Key Element 14: SMS/OPP Oversight Program

It is imperative that each organization establish and implement an oversight program to help management improve safety and environmental policy. The oversight program not only evaluates the effectiveness of an organization's SMS/OPP but also demonstrates management's seriousness and the importance of SMS/OPP to all employees. To achieve a balanced and effective evaluation of SMS/OPP, the oversight program should include independent assessments by personnel from various facility departments or from other organization facilities or even by outside professionals or organizations.

The key elements of an SMS/OPP oversight program include, but are not limited to, the following:

- Conducting internal assessments of SMS/OPP at regularly scheduled intervals.
- Utilizing checklists when conducting SMS/OPP evaluations.
- Assessing the activities of contractors or third parties where their services may affect SMS/OPP
- Documenting results, recommendations, and corrective actions (or non-actions and reasons) as well as positive and negative observations.
- Categorizing findings to assist in prioritizing corrective actions.
- Sharing the results and corrective actions (or non-actions and reasons) with all personnel.

Some OPP Plan Specific Initializing Elements

The OPP plan must begin with "initialization". The initialization process is perhaps the most challenging aspect of planning. The OPP plan must address key issues of integration and consistency of tank operations for successful implementation. This is because all facilities with more than one tank have variations between the tanks, not only in location (proximity to important structures, adjacent properties, and other tanks), protection (dikes, drainage, etc.), size, product stored and configuration, but also in terms of operating parameters such as receipt procedures, rates, and duration of flow, gaging and level devices, alarm points, tank volume, etc. (*Note: Section 4.4.1 of API 2350 discusses establishing levels of concern (LOCs), part of the OPP initialization process*).

The SMS/OPP plan must account for many types of tank overfill systems, different operating practices and procedures, personnel with different ideas about how to operate tanks and a multitude of variability in equipment that must be considered when developing the OPP plan. These are just some of the data that must be collected and understood for each tank to develop a plan that supports and enhances organizational goals and objectives and provides for consistency so that all tanks will meet the organization's safety and environmental requirements.

Related links

Endress+Hauser Oil & Gas virtual tour:

<http://apps.endress.com/oil-gas-virtual-tour/web/html/?homes>

YouTube Video:

Comply with API2350 and IEC61511 - automated overflow prevention system

https://www.youtube.com/watch?v=2XyMJ3_Yp3w&t=1s

Level Product YouTube Playlist:

<https://www.youtube.com/playlist?list=PLQRFGW1Z4TGHsxqg5-ZzKblstj0PmZrGT>



www.addresses.endress.com

GL01027F/24/ENV/01..18
\$59,000 USD