Overfill Prevention for Atmospheric Storage Tanks in Petroleum Facilities

ANSI/API STANDARD 2350-
FIFTH EDITION, XXXX, 20XX
REVISION 6
Final Ballot – Contains comments from Oct - Nov 2019 Recirculation ballot.

Note: Per the API and ANSI procedures - only the revisions from the 2019 Recirculation ballot are open for comment.

energy API

AMERICAN PETROLEUM INSTITUTE

Approved American National Standard ANSI

Overfill Prevention for Atmospheric Storage Tanks in Petroleum Facilities

AMERICAN PETROLEUM INSTITUTE

Special Notes

NEW WORDING FROM API LEGAL DEPARTMENT TO BE ADDED HERE. NO MODIFICATIONS TO THEIR WORDING WILL BE ACCEPTED.

Foreword

NEW WORDING FROM API LEGAL DEPARTMENT TO BE ADDED HERE. NO MODIFICATIONS TO THEIR WORDING WILL BE ACCEPTED.

Contents (Table of Contents to be revised by API)

Overfill Prevention for Storage Tanks in Petroleum Facilities

1 Scope

1.1 Scope

This document applies to atmospheric storage tanks associated with refining, marketing, pipeline and terminals that contain NFPA Class I or Class II liquids. This standard does not apply to:

— tanks of 1320 US gallons (5000 liters) or less, unless connected to a transporter or marine delivery system;

— tanks which are covered by PEI RP 600;

— tanks filled exclusively from wheeled vehicles (i.e. tank trucks or railroad tank cars), where the fill rate is less than 630 bbl/hr (440 gpm) (100m^3/hour);

— dedicated pipeline relief tanks; and

— tanks storing LPG and LNG.

The purpose of this standard is to assist Owner/Operators and operating personnel in the prevention of tank overfilling by implementation of a comprehensive overfill prevention system (OPS). The goal is to receive product into the intended storage tank without overfilling or mechanical damage.

1.2 Minimum Requirements

This standard is one of minimum requirements. Alternate approaches or variations on the principles of this standard that provide equivalent or more robust overfill prevention are acceptable. Alternate approaches may be needed when the tank system varies from the typical configurations described in this standard. The rationale for the implementation of each overfill prevention process (OPP) should be documented and retained by the owner and operator. This standard is not intended to prevent the use of systems, methods, or devices of equivalent or superior quality, effectiveness, durability and safety over those provided in this standard. Where the rules in API Std 2350 conflict with local, state, or federal regulations, the regulations shall ~~tank~~ take precedence over API Std 2350. In the event that there are conflicts, the more stringent of API Std 2350 or the regulations shall be applied.

2 Normative References

The following referenced documents are necessary for the application of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

API MPMS Manual of Petroleum Measurement Standards, Section 3.1a and b

IEC 61511 – Functional Safety – Safety instrumented systems for the process industry sector – Part 1: Framework definitions, system, hardware, and software requirements. (This document is only classified as normative when chosen as an option by the Owner/Operator.)

Other references in the document, including those in the Bibliography, are provided for information only and are not normative to this standard.

3 Terms, Definitions, and Acronyms

Acronyms used throughout this document are:

AHJ – Authority having jurisdiction

AOPS – Automated overfill prevention system

ATG – Automatic tank gauge

CH – Critical High

HH – High-High tank level

LAHH – High-High tank level alarm

LNG – Liquified Natural Gas

LOC – Level of concern

LOPA – Layer of protection analysis

LPG – Liquified Petroleum Gas

MOC – Management of change

MOPS – Manual overfill prevention system

MW – Maximum working level

OPS – Overfill prevention system

PHMSA – Pipeline and Hazardous Materials Safety Administration

PIC – Person in charge

PLC – Programmable logic controller

SCADA – Supervisory control and data acquisition system

SIS – Safety Instrumented System

WDT – Watchdog timer

For the purposes of this document, the following definitions apply:

3.1
alarm
Alarms are audible and visual means of indicating an abnormal condition or potential emergency that requires a specific response or action by operating personnel.

3.2
alert
Alerts are audible or visual notifications indicating an equipment or process condition that requires awareness. Alerts may not require specific action. Alerts may indicate need for investigation or Owner/Operator defined action.

3.3
atmospheric tank
A storage tank with internal design pressures not more than 17.2 kPa (2½ pounds per square inch) gauge.

3.4
attendance
The term describing when personnel are physically on site at the facility where the tanks are located during receiving operations. Personnel on site have the ability to monitor the tank level and either have the ability to terminate the receipt or are in real time contact with people who have the ability to terminate the receipt.

3.4.1
continually-attended facility
A competent person is on site for 24 hours per day and 7 days per week.

3.4.2
fully-attended facility
A competent person is on site continuously during the entire receipt or transfer of products.

3.4.3
semi-attended facility
At a minimum, a competent person is on site during the first and last thirty minutes of the receipt of products or transfer operations (first denoted by the flow of product, last denoted by the termination of flow).

3.4.4
unattended facility
A competent person is not required to be on site during any part of a receipt or transfer of products.

3.5
authority having jurisdiction (AHJ)
An organization, office, or individuals responsible for enforcing the requirements of a code or standard, or for approving equipment, materials or procedures.

3.6
automated overfill prevention system (AOPS)
An overfill prevention system not requiring operating personnel action in order to function. This system is intended to reduce the potential risk of a manual overfill prevention system failing to prevent overfilling.

3.7
automatic tank gauge (ATG)
A mechanical or electronic device designed to continuously measure the liquid level in a storage tank without manual action.

3.8
capacity
The volume (amount) of product contained in a tank at designated levels (i.e. the levels of concern (LOCs)).

3.9
Class I liquid
A Class I liquid as defined in NFPA 30, namely, a liquid that has a flash point ~~above~~ below 100 deg F (37.8 deg C) and below 140 deg F (60 deg C)**.**

3.10
Class II liquid
A Class II liquid as defined in NFPA 30.

3.11
competent person
An individual who is trained, capable, and able to perform the assigned duties as determined by the Owner/Operator.

3.12
continuous level sensor
A measuring device; a mechanical or electronic uninterrupted level sensor designed to measure the liquid level in a storage tank without personnel action.

3.13
control center
Locally or remotely manned operating center, which can monitor, control, and terminate operations at the subject facility. A control center can belong to the Owner/Operator or a third party.

3.14
Critical High (CH) level
The highest level in the tank that product can reach without detrimental impacts (i.e. product overflow or tank damage).

3.15
dedicated relief tank
A tank that does not store product on a normal basis, but is used to hold product during pipeline pressure relief events.

3.16
diagnostic alarm
Indication that there has been a malfunction of equipment. It applies to any condition affecting the proper operation of instrumentation, control or alarm systems (including power outages) that requires operating personnel response.

3.17
electrically supervised
OPS instrumentation that is electronically self-checking to indicate when communication between the sensor, logic solver, or final element has failed and can generate a diagnostic alarm.

3.18
facility
A location with tanks within the scope of this standard.

3.19
final element
Block valves, diversion valves, pumps or other equipment that terminates flow to prevent tank overfilling. ~~In the event of pump or other equipment shutdown, positive isolation will be initiated.~~

3.20
high-high tank level alarm (LAHH)
An alarm generated when the product level reaches the High-High (HH) tank level.

3.21
high-high (HH) tank level
A level sufficiently below the Critical High (CH) level to enable termination of a receipt or transfer before the Critical High (CH) level is reached. ~~In no case, shall receipt procedures be planned to reach the High-High (HH) level.~~

3.22

incident
An event with undesirable consequences affecting safety, health, the environment or financial impact to the facility.

3.23
independent alarm
An alarm function separate from the device or system used for routine operational tank level measurement.

3.24
levels of concern LOCs
Calculated product levels in a tank that allow the Owner/Operator to determine appropriate levels to set alerts, alarms or AOPS functions.

3.25
local
Located or operated on-site at a facility.

3.26
manual overfill prevention system - MOPS
An overfill prevention system requiring operating personnel to terminate receipt.

3.27
marine vessel
A barge or tanker ship that can deliver product directly into petroleum facility tanks (usually through temporary connections to facility pipelines).

3.28
maximum ~~expected~~ fill rate (in./hr)
The rate of liquid level rise in the tank at the maximum flow rate, excluding outflow from the tank.

3.29
maximum ~~expected~~ flow rate (bbl/hr)
The highest volumetric rate that product can enter a tank at the same time from various sources.

3.30
maximum working level
An operational level that is the highest product level to which the tank is routinely ~~be~~ filled during normal operations.

3.31
monitored
The observation of tank levels, alarms, flow rates, etc. during a receipt or transfer activity. The term describing the type of tank gauging and degree of observation of tank operations. The activity of monitoring can be local or remote.

3.31.1
Continuously-Monitored
A tank fitted with an automatic tank gauging system with real time transmission of operational information and/or alarms to a control center that is manned 24 hours per day, 7 days per week.

3.31.2
Fully-Monitored
A tank fitted with an automatic tank gauging system with real time transmission of operational information and/or alarms to a control center that is manned during the entire receipt period.

3.31.3
Semi-Monitored
A tank fitted with an automatic tank gauging system with real time transmission to a control center where tank alarms are monitored during the first and last thirty minutes of the receipt.

3.31.4
Locally-Monitored
A tank without signal transmission to a control center.

3.32
operating personnel
The person who manages tank receipt or dispatch operations; whether located at a facility, local or remote control center, operating personnel are available, have access to equipment and controls, and are competent to respond to notifications, alerts, alarms, and abnormal conditions pertaining to receipt operations at a facility.

3.33
overfill
Any product level that exceeds the Critical High (CH) level.

3.34
overfill prevention system - OPS
An engineered system consisting of the physical equipment and procedures to assure that safeguards directed at effectively receiving products and minimizing the potential for tank overfills are incorporated.

3.35
owner/operator
The company that owns and/or operates the facility.

3.36
parallel tanks
Two or more tanks at the same facility that can be filled simultaneously and effectively operated as one tank.

3.37
person in charge (PIC)
A U.S. Coast Guard regulatory term from 33 *CFR* 154.700 for a trained and experienced individual designated as a "person in charge" of transfer operations at marine terminals.

3.38
product
Class I or Class II liquids as defined by NFPA 30.

3.39
proof testing
A partial or complete overfill prevention system instrumentation loop test through the primary sensing element verifying appropriate response from sensors to the final control element including alarms to the extent possible.

3.40
receipt
A delivery or transfer of product into a tank.

3.41
response time
The time required to complete a set of actions to terminate a receipt. ~~Validating a response time means field testing the time actually required to terminate a receipt, including all of the factors mentioned in 4.4.2.~~

3.42
risk analysis
An estimate of likelihood and consequences in order to assess the degree of risk.

3.43
risk assessment
Overall process of risk analysis and risk evaluation.

3.44
risk screening
Often, a first step in the risk analysis process. An activity used to prioritize risk assessment activities typically by assigning weighting factors to provide a relative risk ranking.

3.45
supervisory control and data acquisition system - SCADA
A computer-based system or systems used by a controller in a control room that collects and displays information about a facility and could have the ability to send commands back to a remote facility.

3.46
sensors
Continuous or point type product level sensing elements that detect and measure physical properties of the media in which it is installed to trigger alarms, alerts, and shutdown and diversion actions.

3.47
terminal
An Owner/Operator or third-party facility with tanks that receive, ship, dispense or transfer product.

3.48
terminate
Stopping or redirecting receipt flow to prevent flow of excess product into a tank. Examples include:

a) Eliminating the source of pressure, e.g. shutting down a pump,
b) Diverting the incoming flow,
c) Shutting down the flow (closing a receipt valve), or
d) Using an alternative method for bringing the receipt process to a safe state without overfilling the tank.

3.49
transporter
The person(s)/organization responsible for delivering the product to/from either a refinery, marine, terminal, or pipeline organization.

3.50
valve lineup
The practice of opening or closing predetermined valves in the system to ensure that product is directed to the intended tank(s) and not diverted to incorrect tank(s).

3.51
watchdog timer - WDT
An external or internal diagnostic device that monitors the health of an electronic system and performs a specific operation after a certain period of time if something goes wrong with an electronic system and the system does not recover on its own.

3.52
wet probe test
Sensor test by simulation of overfill by exposure of sensor to a liquid (water or hydrocarbon) to verify the alarm and/or control system functionality.

4 Overfill Prevention System (OPS)

4.1 Overview

The likelihood and the associated consequences of overfilling a tank vary from one facility to another and even between tanks within a facility. Prevention of tank overfills requires taking into account the following factors:

- awareness and calculation of available tank capacity and inventory,
- careful monitoring and control of product movement and tank level during filling.
- use of reliable instrumentation, sensors and systems,
- use of human response to manually initiate the termination of flow (MOPS),
- use of automatic tank gauging systems, independent high level alarms, etc. to address the gaps arising from a risk assessment and risk analysis, and
- use of automated response systems to automatically ~~initiate the termination of~~terminate the flow (AOPS), where appropriate.

Consequently, a comprehensive and flexible approach to overfill prevention is provided in this document. Careful consideration was given to the benefits provided by overfill prevention for tanks in petroleum facilities relative to:

- safety and environmental protection,
- optimization of the work place and operating practices,
- inspection, testing, and maintenance,
- equipment and system selection and installation,
- safe work practices, emergency procedures and training,
- management of change programs relative to tank overfill prevention,
- inclusion of current technology and practices related to process control and automated safety instrumented systems.

This allows the Owner/Operator of each facility to assess the risks and implement appropriate facility-specific or tank-specific practices to prevent tank overfills.

The OPS consists of several fundamental components:

a) management system;

b) risk assessment process;

c) operational parameters;

d) procedures (including those for receipt termination) and training; and

e) equipment supporting OPS and its inspection, testing and maintenance.

4.2 Requirements for the Management System

A management system is the framework of administrative processes and procedures used to enable the Owner/Operator to fulfill the tasks required to achieve important corporate goals, including overfill prevention. A management system is required and shall be documented for conformance with API 2350, but this standard does not specify how to implement or document such a system. This management system may be integrated with existing safety or environmental procedures or be developed as a standalone system. This task is the responsibility of the Owner/Operator. A properly structured management system provides all the practices and components required for a good OPS and is managed and periodically assessed and updated to keep practices current as people and equipment change. API RP 1173, “Pipeline Safety Management Systems, provides some guidance on management systems.

At a minimum, the management system shall address:

a) formal documented operating procedures and practices, including safety and emergency response procedures;

b) competency of operating and maintenance personnel;

c) functional equipment systems, tested and maintained by competent personnel;

d) scheduled inspection and maintenance programs for overfill instrumentation and equipment;

e) systems and procedures to address both normal and abnormal operating conditions;

f) management of change (MOC) process that includes personnel and equipment changes;

g) system to identify, investigate, and communicate overfill near misses and incidents;

h) system to share lessons learned;

i) follow-up system to address any needed mitigation of circumstances leading to near misses or incidents;

j) communication systems protocols 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; and

k) management system should be periodically reviewed and updated for continuous improvement.

4.3 Requirements for Risk Assessment

Risk assessment for each tank subject to overfill shall be performed by the Owner/Operator. Risk assessment methods and procedures may conform to Owner/Operator's procedures. This standard does not specify how risk assessments should be conducted (e.g. qualitative or semi-quantitative, including LOPA), because tank operations, associated risks, corporate risk assessment knowledge and methods vary widely, and risk tolerance are site and Owner/Operator specific.

The Owner/Operator ~~shall comply by following~~may utilize the requirements in 5.2 where the Categories (found in Annex G) are used with the associated response times found in 4.4.2.2 until a risk assessment is undertaken. For a tank that does not fit into a Category, Owner/Operator shall default to the next more conservative applicable Category.

Personnel who are familiar with the site-specific tank facilities and operations, personnel familiar with the risk assessment methodology, and personnel who are familiar with impacts to and from the transporter should participate in these analyses.

Procedures for performing risk assessments on tank systems subject to overfills should be developed and implemented for use in OPS. These may be either qualitative or quantitative. Annex E provides a conceptual overview for a risk assessment program.

To assess the risk of overfill, the operating procedures and associated instrumentation described in this document and their effectiveness should be evaluated, including:

a) Consequences of overfill
b) Operation conditions (max flow rates, number of receipt lines operating at one time to fill tanks)
c) Procedures for pre-receipt activities
d) Procedures for activities during receipt
e) Procedures for emergencies, i.e. alarm response
f) Design, testing, operation, and maintenance of instrumentation systems
g) Design and maintenance of OPS

When a risk assessment shows the acceptance criteria is not satisfied, further risk reduction through additional safeguards including layers of protection (e.g. additional level instruments and procedures), changes in operations and procedures shall be provided to meet the acceptance criteria. AOPS may provide additional risk reduction; however, it is important to consider the potential for hydraulic surge.

Documentation of risk assessment(s) should include a description of the methods and procedures used to perform the assessment, including:

.

- Risk assessment methodology
- Determination on risk, risk mitigation and risk acceptability
- Team members and their expertise
- Probability and consequence factors and their evaluation to determine risk
- Basis for the assessment, including assumptions, data sources, and data analysis
- Owner/Operator risk criteria

Risk assessments should be reviewed when changes occur to a tank, facility, or surrounding areas that affect the overfill risk. Risk assessments results shall be reviewed and updated at least every 10 years.

4.4 Defining Operating Parameters

Operational parameters govern the establishment and setting of LOCs in addition to the determination of appropriate response times for operations. The following procedures may be used to establish operational parameters:

4.4.1 Establish Levels of Concern (LOCs)

The Owner/Operator shall establish and document the following levels of concerns (LOCs) (see Figure 1) that are applicable for tanks covered by this standard:

— Critical High (CH) level,

— AOPS activation level (if equipped with an AOPS),

— High-High (HH) level,

— High (H) level (optional), and

— Maximum Working (MW) level.

Establishing LOCs should take into account the equipment and ability to respond to alerts and alarms. In addition, the tank strapping table (whether hard copy or electronic) shall be accurate and current when calculating the response time. ~~If~~ When setting a response time ~~is used~~, ~~then~~ the response time calculation shall include the factors discussed in 4.4.2. Once this response time-volume (response time – maximum flow rate) is calculated, a tank calibration table or equivalent calculation method shall be used to determine the vertical distance in the tank corresponding to that time-volume.

Special cases exist such as:

- tanks used for pipeline relief (relief tanks) in addition to their normal product use. Non-dedicated relief tanks shall maintain the proper amount of free volume in the tank based on the anticipated relief event and associated capacity. When determining LOCs, the required relief volume should be taken into account ~~in the levels either~~ between ~~High-High (HH) level and Critical High (CH) level,~~ Maximum Working level and High-High (HH) level, or in some other way as defined by the Owner/Operator,
- tanks being operated in parallel or at different heights or elevations. One tank may be “full” (reached its overfill level) before the other(s),
- tanks may not fill at the same rate. If you are relying on a gauge from one tank to cover multiple tanks.

Operating personnel shall be notified of these LOCs through an operating practice developed by the Owner/Operator.

The LOCs shall be available and displayed so that they are visible to the personnel responsible for filling the tank, i.e. near the manual gauge hatch, tank gauging equipment, at the bottom of the tank, and be available at the control center.

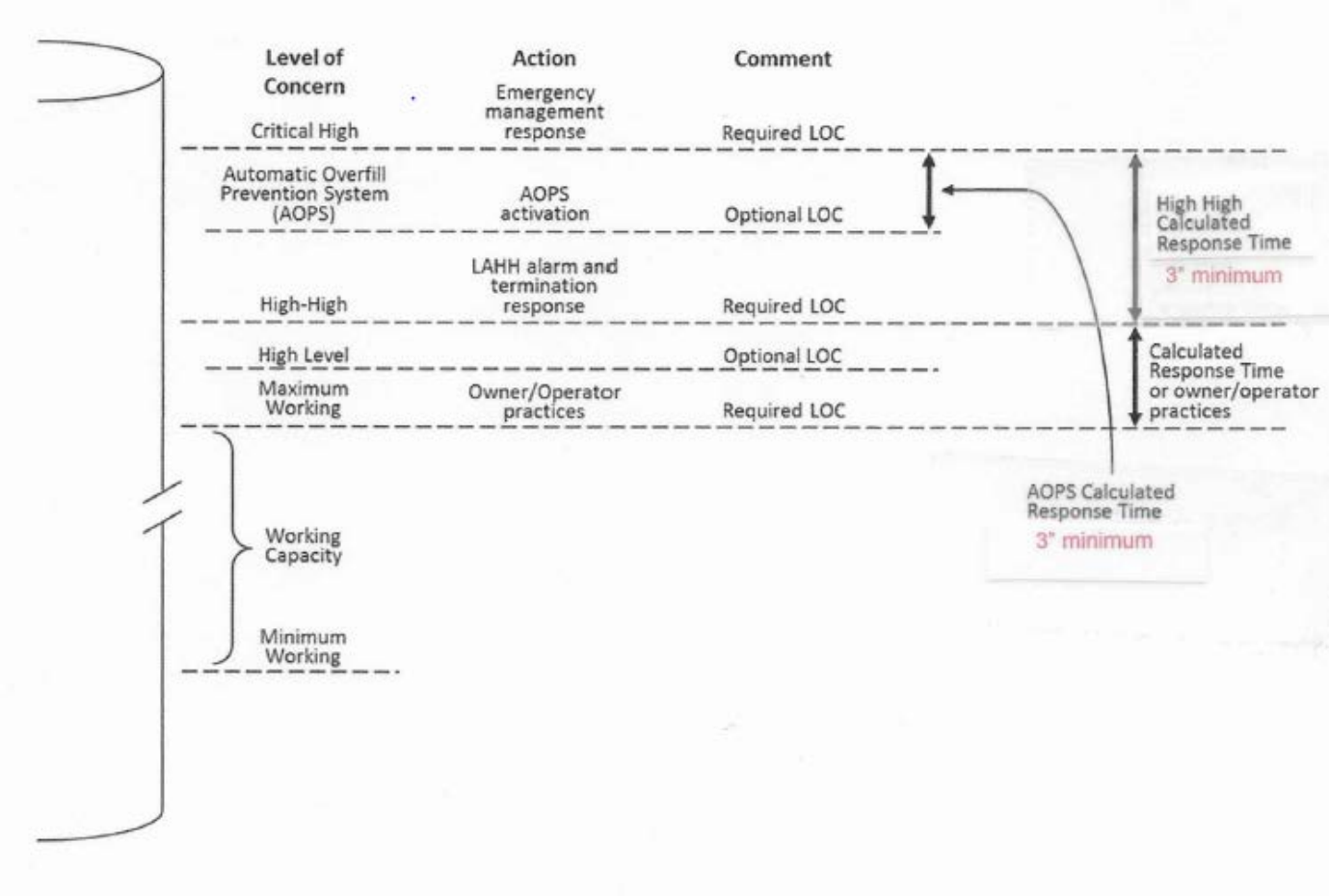


Figure 1—Tank Levels of Concern (LOCs) ~~Note to API: add 3" minimum between HH and MW levels~~

Note: In previous editions of this standard, a high-level alarm was utilized as a required LOC. Starting with the 4th edition, a LAH is not required. If used, an LAH may be applied as an alert or alarm. When used as an alert, no requirements of this standard apply. When used as an alarm, all appropriate requirements of this standard apply. The term High-High (HH) level is still used as the priority LOC where an alarm should be established to initiate immediate shutdown of filling operations (which reflects industry practice). The Owner/Operator is encouraged to establish a High Level and initiate shut down of the receipt if the level reaches the High Level. If an alarm is also established at the High level, then all of the applicable requirements of this standard, such as operational parameters, response times, and procedural requirements, shall apply to not only the LAHH but to the LAH, as well.

4.4.1.1 Critical High (CH) Level

The Critical High (CH) level is the highest level in the tank without detrimental impacts such as:

— overflow of product;

— exceedance of the allowable tank shell design stresses;

— leakage from a corroded area or temporary repair; or

— level designated by the Owner/Operator, considering:

- mechanical contact of: the floating roof, floating roof seals, floating roof legs, foam chamber deflectors or foam dams, or other appurtenances with the tank roof or platform/ladder structure;

- seals rise to a level where they are in contact with vents or top of the tank shell;

NOTE: Potential detrimental impacts are variable and resulting levels are determined by Owner/Operator evaluation. Depending on the structural design and geometry of floating and fixed roofs, experience shows some configurations may allow an overfill with minimization of structural damage to the fixed roof or loss of the internal floating roof; whereas, location of certain obstructions have caused damage to the fixed roof and/or caused the internal floating roof to sink without resulting in an overfill. Loss of the floating roof is a critical fire safety situation. Likewise, shell integrity may need to be evaluated by an Engineer experienced with storage tank design.

4.4.1.2 AOPS Activation Level

The AOPS activation level is the level at which an automated system, if applicable, terminates the flow into a tank before the Critical High (CH) level is reached.

- The level shall be set sufficiently below the Critical High (CH) level to account for the response time of the AOPS system to activate and terminate flow. The difference between the CH and AOPS activation levels shall not be less than 3 inches.

- The AOPS activation level shall be set at or above the High-High (HH) tank level. However, it may be preferable to have the AOPS set above the High-High (HH) tank level in order to provide additional overfill prevention through a manual overfill prevention system (MOPS) where operating personnel can terminate the receipt prior to the AOPS activation.

4.4.1.3 High-High (HH) Tank Level

The High-High (HH) tank level is the last opportunity for the operator to terminate the flow to prevent an overfill or damage to the tank.

- The HH tank level shall be set sufficiently below the CH level to enable operator action to terminate product receipt before the CH level is reached.
- The vertical distance in the tank between the Critical High (CH) level and the High-High (HH) level shall be calculated based on the response times required to terminate a receipt at the maximum fill rate, but shall not be less than 3 inches.
- The response time used in these calculations should include the factors discussed in 4.4.2. Once this response time-volume (response time $\times$ maximum flow rate) is calculated, a tank calibration table or equivalent calculation method shall be used to determine the vertical distance in the tank corresponding to that time-volume.
- In addition to the response time, the Owner/Operator shall include adequate space to accommodate:
    - Relief volume that may occur, where applicable;
    - Drain back volume to the tank due to line elevation, in the case of communication failure or valve malfunction;
    - Excess volume of the taller of two parallel tanks; and
    - Safety factor(s).

Filling past the Max Working level is only allowed with written authorization. Product levels reaching the High-High (HH) tank level should be lowered as soon as practical to the Maximum Working level.

Policies and procedures shall prohibit the use of high-high tank level alarms and AOPS for routine operation or control of tank filling operations.

4.4.1.4 High (H) Level (optional)

The High (H) Level may be used as a LOC alert ~~ahead of~~at a point lower than the actual High-High alarm or AOPS.

4.4.1.5 Maximum Working (MW) Level

- No alarm is required at the Maximum Working (MW) level, but alerts may be established by the Owner/Operator to aid operations.
- The MW level is set at a distance below the High-High (HH) level alarm or the High (H) level alarm (if used) on the tank based either on response time or Owner/Operator practices.

The MW level should be 3 inches (76 mm) below the High-High (HH) level alarm or a larger calculated level that accounts for thermal expansion or other conditions which can inadvertently activate the High-High (HH) level alarm.

4.4.2 Response Time (RT)

Response times shall be calculated and evaluated when determining the levels described above.

Factors that shall be evaluated when establishing the response time include:

a) time required to initiate alarm (electronically or manual observation of tank gauge);

b) time to validate alarm (avoid inappropriate response to false alarms);

c) time required to complete predefined response actions and terminate flow;

d) time required to verify that system elements are responding appropriately and take appropriate action if the system is not responding properly; and

e) Owner/Operator defined safety factor.

f) Other factors to consider include:

- time for communications,
- travel requirements,
- equipment action,
- staffing variations,
- seasonal weather conditions,

4.4.2.1 Response times between Max Working and High-High may be different than the response time between High-High and Critical High depending on the different actions required between the levels.

4.4.2.2 Response times less than 10 minutes between the High-High (HH) and Critical High (CH) levels of concern shall be validated by a physical walk-through of the factors outlined in Section 4.4.2 that is timed and documented. Actual validated response times can be shorter than those given in 4.4.2.2.

4.4.2.~~2~~3 Until response times are validated by the Owner/Operator, the minimum response times between maximum working/high-high levels and high-high/critical high levels shall be, as shown ~~in Annex G~~below:~~.~~

Tank Category	Minimum Response Time
0	60 minutes
1	45 minutes
2	30 minutes
3	15 minutes

4.4.3 Level of Concern (LOC) Changes and Periodic Reviews

4.4.3.1 General

LOCs shall be reviewed at an interval determined by the Owner/Operator. Any revised LOCs shall be documented, communicated to all affected personnel, and implemented.

4.4.3.2 Physical Conditions or Changes Warranting Level of Concern Review

A LOC review shall be conducted and documented for a new tank or when there are any physical changes to a tank, such as:

— changes to floating roof leg heights;

— change in floating roof seal dimensions;

— change in shell height (shell reduction or extensions);

— installation of geodesic domes or other fixed roofs (e.g. when external floating roof tanks receive retrofit covers);

— new internal or external floating roofs;

— side vent changes;

— new tank bottom or datum plate;

— addition of ancillary equipment (i.e. foam chambers);

— change in datum, strike plate, or gauge reference point, e.g. addition of gauge tube with datum; and,

— modifications to the tank-strapping charts/gauge tables, such as new overflow height, floating roof critical zones.

4.4.3.3 Operational Changes Warranting Level of Concern Review

A LOC review and documentation shall be required whenever any of the following changes occur:

— change in incoming or outgoing piping;

— change in product to one with different density or viscosity;

— change in maximum flow rates;

— adjustments to LOCs due to tank inspection findings (corrosion, temporary repairs);

— change in operations (e.g. parallel tank, floating or high suction, continuous mixer operation);

— change in ownership/operating control (e.g. acquisition); and

— change in response time resulting from adjustments in available personnel, accessibility, operation or equipment changes.

4.5 Requirements for Overfill Prevention System (OPS) Procedures

4.5.1 Procedures for Operations

Documented operating procedures shall be established by the Owner/Operator and (where appropriate) coordinated with and agreed to by the transporter. (Refer to Annex F on Transporter/Owner/Operator Interface.) The documented operating procedures shall be reviewed on Owner/Operator's requirements and revised or amended as the facility equipment, procedures, process, or personnel change.

Because the flow rate, equipment, instrumentation, tank configuration, and type of transporter can differ at a facility for each receipt, one set of general operating procedures typically cannot be used for all receipts. Therefore, Owner/Operators shall prepare documented operating procedures for each type of receipt. This standard does not preclude the use of common procedures for receipts or transfers where the factors are common.

Procedures require planning that determines:

a) the quantity of product to be received,

b) single or multiple receiving tanks;

c) maximum pressure allowed for the piping or equipment at the receiving facility;

d) receipt starting level, flow rate (including any expected variations), and receipt end time;

e) the amount of volume or space available in each tank, and any expected volume expansion, e.g. product temperature rise in the tank(s), or other receipts or activities;

f) valve lineup;

g) other simultaneous tank activities at the facility,

h) whether (and when) a switch in receiving tanks is needed

i) who is responsible for monitoring and/or attending the receipt;

j) who is responsible for terminating the receipt.

Specific procedures vary depending upon:

a) transfer quantity, e.g. single truck unloading vs. transfers from a significantly larger tank

b) flow rates into and out of the tank

c) mode of transfer, e.g. pipeline, rail, marine, or truck

d) tank gauging and instrumentation equipment, and

e) interaction with the transporter.

The requirements in the following sections shall be included in the pertinent, normal tank receipt and transfer procedures for all tanks.

4.5.1.1 Procedures for Planning the Receipt

4.5.1.1.1 Specific documented instructions for the receipt shall be prepared and reviewed (as appropriate) with personnel from the transporter and Owner/Operators. These instructions shall list specific procedures and any special controls needed to carry out the receipts.

More complicated operations requiring extra attention when creating procedures include:

a) Switching receiving tanks during the same receipt;

b) multiple tanks are being filled simultaneously;

c) a tank is receiving product from multiple sources; or

d) abnormal operations

4.5.1.1.2 Prior to receipt, product quantities to be received shall have been determined and compared to receiving tank available capacity to ensure that sufficient tank capacity is available. Planning shall be conducted sufficiently ahead of receipt to minimize the need for last minute product transfers or withdrawals from a designated receiving tank prior to receipt.

4.5.1.1.3 The planned final product level in each tank shall be determined prior to each scheduled receipt and shall not exceed the Maximum Working level without written authorization. In no case, shall receipt procedures be planned to reach the High-High (HH) level alarm or AOPS.

4.5.1.1.4 The Owner/Operator shall assign required duties to competent personnel before start of the receipt (or duties may be documented as normal duties of a particular designated job).

4.5.1.2 Procedures for Pre-Receipt Activities

4.5.1.2.1 Prior to product receipt or transfer, the available volume in the receiving tank(s) shall be verified and compared to the planned receipt volume and deliveries out of the tank, i.e. truck loading operations. If the planned receipt volume exceeds the available receipt volume, the transporter shall be contacted and plans adjusted.

4.5.1.2.2 The pre-receipt information that is recorded for the tank shall be available to the transporter. The minimum information shared between the transporter and the tank Owner/Operator includes:

a) Planned receipt volume,

b) Planned receipt start time and expected receipt end time, and

c) Expected flow rate, including any variations.

4.5.1.2.3 Before the product is transferred or received, the valve lineup shall be verified to confirm the product is delivered into the designated tank(s) and that only the intended valves are open and the valves for other tanks are closed.

4.5.1.2.4 Prior to starting product transfer to fully- or semi-attended facilities, communications between the transporter and the facility Owner/Operator shall be tested. Based on staffing and instrumentation, communication frequency between the facility Owner/Operator and the transporter shall be agreed upon and maintained throughout the transfer. See Table G1 in Annex G for an example of attendance and communication.

4.5.1.2.5 Prior to starting product transfer to unattended facilities, Owner/Operator shall ensure that electronic supervision is not indicating a diagnostic alarm.

4.5.1.3 Procedures for Activities During Receipt

4.5.1.3.1 Regularly scheduled monitoring of product levels during receipts shall be required and documented.

4.5.1.3.2 Regularly scheduled comparisons (planned vs. actual) and recording of the following information shall be made during the receipt:

a) Tank(s) involved in the receipt or transfer,

b) Receipt or transfer fill rate,

c) Remaining receipt or transfer volume(s),

d) Remaining tank volume(s); and

e) Estimated time of receipt or transfer completion.

4.5.1.3.3 Tanks that are connected to the same product manifold, but that are not scheduled to receive product shall be monitored to ensure that there is no unintended flow.

4.5.1.3.4 Immediately after the start of product receipt, a competent person or automatic system shall verify that product is only flowing into the correct tank(s) and that the gauging equipment is operative.

4.5.1.3.5 Procedures shall be established that ensure continuity of communications and control between operations personnel for shift changes while receipts are in progress.

4.5.1.4 Procedures for Post Receipt Activities

At the conclusion of the receipt, the valve lineup shall be secured. This may include closing tank, manifold, pipeline or marine valves and other safeguards appropriate for the facility.

4.5.1.4.1 Documentation for Product Receipt

At the conclusion of the receipt, the following (along with the time and date) shall be documented:

a) The tank(s) involved in the receipt,

b) The actual receipt volume, and

c) The final tank level(s).

All documentation associated with the product receipt shall be maintained for a period of time defined by the Owner/Operator or by regulation.

4.5.1.5 Procedures for Emergencies and Abnormal Conditions

Documented procedures for managing the following emergencies and abnormal conditions shall include:

a) alarm activation (e.g. diversion or termination of receipt);

b) overfill, including mitigation and any required emergency response actions;

c) automatic tank gauge system component failure, loss of communication for levels or alarms or utility outages (e.g. used for verifying communications between operator and transporter);

d) abnormal conditions, (e.g. operating, equipment, environmental, power outages, weather related);

e) a 5% or greater deviation in the planned and actual receipt conditions detected during the regularly scheduled comparisons required by 4.5.1.3.2.

If the tank gauging or the tank monitoring system fails, previously established abnormal operating procedures shall be initiated. The tank may take receipts after the written authorization from the appropriate member of management who has ensured that adequate risk mitigation has been employed, unless that specific event is covered in the local abnormal operating procedures. This documented authorization shall be reviewed for each receipt until the monitoring system is repaired. Abnormal operations caused by equipment or control system failures shall be addressed as soon as practicable.

4.5.2 Procedures for Training on Overfill Prevention Systems

4.5.2.1 Owner/Operator shall establish procedures for the training of operating personnel involved with product transfer in overfill prevention and emergency response measures.

4.5.2.2 Training program procedures shall be reviewed (and updated as necessary) when operating procedures, equipment, instrumentation or regulatory requirements change.

a) Owner/Operator and transporter personnel shall be trained on the OPS procedures before participating in a product receipt or transfer.

b) Personnel training shall be documented. This documentation shall contain the identity of the employee, the date of training, the means used to verify that the employee understood the training to a competency level allowing him/her to perform the receipt/transfer tasks.

4.5.3 Procedures for Testing, Inspection, and Maintenance of the Equipment of an OPS

4.5.3.1 General Requirements

Documented procedures shall be developed by the Owner/Operator for testing, inspecting, and maintaining a manual or automatic overfill prevention system and its components. Where appropriate, the Owner/Operator shall consult with the transporter regarding the development of these procedures:

a) the manufacturer's recommendations shall be taken into consideration when developing procedures and frequency for testing, inspecting, and maintaining the equipment of an OPS;

~~a)~~b) industry standards, government regulations, facility Owner/Operator policies, and special situations may necessitate additional inspection, testing, and maintenance procedures;

~~b)~~c) records of overfill prevention system testing, inspection, and maintenance shall be maintained for at least three years (or longer if required by Owner/Operator policy or regulations); and

~~c)~~d) reviews should be conducted when changes occur in Owner/Operator and transporter practices, products, equipment, tanks and tank assignments, instrumentation, systems and conditions, or applicable regulatory requirements that may be subject to MOC review.

4.5.3.2 Procedures for Testing OPS Equipment

Schedules shall be established for periodic testing, inspection, and maintenance to ensure the accuracy and proper operation of tank level gauges, sensor alarms and signals, floats, displacers, automatic shutdown systems, electronic supervision, and other equipment and instrumentation associated with product transfer:

a) an overfill prevention system shall be tested upon initial installation and retested at least annually until its reliability data or calculations show that the testing, maintenance, and inspection schedules may be adjusted;

b) the facility owner and operator shall establish these schedules based on experience and performance; however, the initial inspection and testing interval shall not exceed one year unless justified by calculations determining probability of failure on demand;

c) specific recommendations of the relevant equipment manufacturer should be considered when establishing inspection and maintenance procedures and intervals;

d) some facilities choose to test newly installed systems on a more frequent basis during the first few months as they develop an experience database;

e) facilities subject to regulations, e.g. PHMSA (DOT) should review relevant regulatory test schedule requirements; and

f) AOPS implementations shall follow testing per Annex A or IEC61511, whichever was the design basis.

All components of OPS system shall be tested and documented, including:

a) testing of hand gauges shall comply with requirements in API *MPMS* Ch. 3.1A;

b) testing of continuous-level sensors shall comply with requirements in API *MPMS* Ch. 3.1B;

NOTE: Verify at least quarterly the continuous-level sensor reading. (As noted in API *MPMS* Ch. 3.1B, Section 9.2.2 "If operating experience confirms stable performance within the verification tolerance, the verification schedule can be extended to once a year".)

c) proof testing of OPS components shall be conducted annually unless otherwise supported by a technical justification (e.g. a probability of failure on demand calculation);

d) proof testing of point- level sensor systems shall be conducted annually unless otherwise supported by a technical justification (e.g. a probability of failure on demand calculation); and

e) proof testing shall be conducted at least annually ~~of~~ on all other OPS components not listed above that are required to terminate the receipt including components (e.g. operator alerts and alarms).

4.5.3.3 Proof Testing Procedures

The proof testing procedure will cover what needs to be tested and what to be considered before carrying out the proof test.

The following proof testing requirements for equipment shall be outlined in the procedures:

a) Level alarms (such as High Level (if established), High-High (HH) Level and/or ~~ATG~~ AOPS Level),

b) All OPS and LAHH system components such as sensor, logic solver and the final element,

c) Systems related to OPS and LAHH systems such as communications, diagnostic alarms, or loss of power alarm,

d) Any other requirements, such as valve closure time (valve closure time and surge hazards are addressed in 5.3.5).

4.5.3.3.1 Proof testing of OPS and LAHH systems is required to verify that the tank overfill prevention system is in place and all associated components and their related systems are working properly and effectively to prevent the overfill scenario. Proof test also includes a functional test as part of the validation of the system.

a) The proof testing of the instrumentation associated with the OPS systems shall be carried out as part of Validation/Revalidation Procedures whenever changes are made to the OPS instrumentation.

b) The Owner/Operator shall develop a proof testing procedure for the instrumentation associated with the OPS. Training shall be provided to the personnel who will be proof testing the instrumentation associated with the OPS. The proof test procedure shall include the manufacturer's instructions on how to perform proof testing in the maintenance mode and how to put the OPS back into the operational mode after testing.

c) Proof testing shall not require filling the tank above its Maximum Working level, as there could be a risk of overfilling during the testing. The testing should simulate an actual high liquid level situation as realistically and as closely as possible. While the testing can be done on partial elements of the loop, the combined procedure shall ensure that all elements of the entire loop are tested within the proof testing interval even if different parts of the loop are tested at different times within that test interval.

d) A written testing procedure shall be developed by the operator that includes functional testing of the sensor, the logic solver, the manufacturer's instructions, management of change from test mode to operation mode and vice versa:

- for MOPS – the annunciation system and operations response (verbal description of written alarm response procedure,
- for AOPS – the final element.

e) A wet probe test uses the actual process liquid or water to trigger the sensor in situ that in turn provides the alarm or OPS/LAHH function. All components, logic solvers and final elements are thereby tested from sensor to output function (alarm or OPS/LAHH activation). However, for tanks in service with hazardous liquids, this kind of test may not be practical or it may not be deemed to be safe in its implementation. Technical justification shall be documented to show how the integrity of the sensor is maintained.

f) Owner/Operator shall document the results of proof testing.

4.5.3.3.2 When new tank systems are fitted with sensors or tanks are out of service for inspections, cleaned and gas free, consideration shall be given to testing alarms. Alarm testing methodology should be determined by the Owner/Operator and may include:

a) Performing full wet probe tests either with water or with product of the same density as the product stored in the tank:

   a. Address operational and safety considerations when product is used.
   b. Verify ability of the sensors to detect water.

b) Performing a test designed to simulate a high liquid level. Alarm testing may include:

   a. Testing different components at different times.
   b. Function testing of loop elements
   c. Review of potential failure modes and effects of the device.
   d. Testing OPS and LAHH system functions as specified at the required trip level.

c) Management of change from test mode to operation mode and vice versa.

d) Any manufacturer and vendor or jurisdictional requirements.

Additional proof testing information is provided in Annex H.

4.5.3.4 Procedures for Inspection of Overfill Prevention System Equipment Components

Inspection procedures specific to the system in use should be established by the Owner/Operator in accordance with manufacturer's recommendations.

a) When the tank is in service, inspection of OPS components should be done from the outside without entering the tank. Such inspections can provide visual evaluation of moisture intrusion, corrosion, and possibly operation of switches, cables and floats (where installed). Entry onto a floating roof tank may constitute confined space entry (see API 2026).

b) When the tank is out of service for internal work, the inspection of gauging equipment elements should be conducted as discussed in 4.5.3.3.2. Preferably, this inspection or testing should be done shortly before the tank is returned to service to ensure that gauge functionality was not compromised by other work.

4.5.3.5 Maintenance of Overfill Prevention Systems Procedures

Maintenance instructions should include performing diagnostic tests in accordance with manufacturers' recommendations. Causes of false alarms shall be investigated and corrected.

Where automatic gauging and measuring systems are used, regular inspection, maintenance, and checks of their capability and performance are required in accordance with API MPMS CH3.

Owner/Operator shall document results of maintenance.

4.5.4 Training for Testing, Inspection, and Maintenance of Overfill Prevention Systems

4.5.4.1 Personnel involved with testing, inspection, and maintenance of Overfill Prevention Systems shall be trained on specific procedures and equipment associated with OPS.

4.5.4.2 Training given to personnel shall be documented by Owner/Operator or Service Provider. This documentation shall contain the identity of the employee, the date of training, and the means used to verify that the employee understood the training.

4.5.5 Proof Test Documentation

Owner/Operators shall document results of proof testing and maintenance and keep for at least five years.

4.5.6 Tank Alarm Records

Records of tank alarms (both false and legitimate), AOPS actuation (both false and legitimate), and tank overfill spills should be kept for the life of the tank to improve and justify Owner/Operator risk assessment data.

5 Overfill Prevention Systems

5.1 Types of Overfill Prevention Systems

There are two types of OPS and their related equipment that are generally used to terminate a receipt:

— MOPS: Manual overfill prevention system that depends on the interaction of operating personnel to terminate the receipt. A person physically turning a valve or pushing a button that remotely closes a valve or turns off a pump are both manual operations. In MOPS, the alerts and alarms provide the operating personnel with information only that require actions. Sections 4.4 and 4.5 in this standard outline the requirements for the design and procedures.

— AOPS: Automated overfill prevention systems (discussed in Annex A) use instrumentation, sensors, logic solvers and final elements at the receiving terminal or tank which prevent overfill by automatically terminating the receipt. AOPS systems require no manual intervention.

The AOPS shall conform to Annex A as a minimum. AOPS designed and managed in accordance with requirements of ANSI/ISA 84.00.01 (IEC 61511 modified) "Functional Safety: Safety Instrumented Systems for the Process Industry Sector" shall be implemented when required by the Owner/Operator practices or other authority.

5.2 Tank Category Criteria

General

As specified in Section 4.3, a risk assessment shall be conducted to determine the manning, monitoring, and control requirements. Until a risk can be completed, the tank category as defined in Annex G shall define these requirements.

Minimum operating and equipment requirements for tanks shall be determined based on the operation of the facility and how level data and alarms are transmitted and monitored. The table below provides a starting point until a risk assessment is completed. A risk assessment shall be used to determine if more or less equipment is required based on the procedures and operating characteristics of each facility or tank.

There is a balance between how the tank is instrumented, how tank operations are monitored, and having people at the facility.

Category	Attendance	Monitor Levels	Alarm Surveillance
0,1,2,3	Fully Attended	Local	Local
2,3	Semi Attended	Local	Local / Remote
3	Unattended	Remote	Remote

The categories depict the most commonly found equipment configurations for facilities taking receipts from marine or mainline pipelines and for tank-to-tank transfers. However, these are not the only possible configurations. Other configurations offering comparable protection are permitted.

5.2.1 Category 0 Facility

5.2.1.1 A Category 0 overfill prevention system does not have instrumentation and does not transmit liquid level or alarm data to the transporter. If shutdown or diversion is required to prevent an overfill, it shall be done manually requiring personnel action by:

a) intervention at the local facility to terminate flow to the tank; or

b) by the transporter after receiving “manual” communications, e.g. a telephone call, from personnel at the site.

5.2.1.2 Category 0 shall be operated as a fully attended facility for receipts with monitoring continuously during the first hour of receipt, every hour during the receipt, and continuously during the last hour of the receipt, as indicated in Table G.1, since there are no remote monitoring capabilities by the transporter for either alarm or level information. Safety considerations may prohibit hand gauging during product receipt or during the 30 minutes after completion (see API 2003).

Category 0 shall not be used where, because of the frequency of receipts or the complexity of the facility or terminal as determined by the Owner/Operator, that the operator cannot reasonably be expected to focus fully on termination of one receipt at a time or may be distracted with other duties or responsibilities. The only overfill prevention in a Category 0 system comes from planning receipts less than the available volume.

5.2.2 Category 1 Facility

5.2.2.1 A Category 1 overfill prevention system will have local readout level instrumentation that is local to the tank or the facility and does not transmit liquid level or alarm data to the transporter. If shutdown or diversion is required to prevent an overfill, it should be done manually requiring personnel action by:

a) intervention at the local facility to terminate flow to the tank; or

b) by the transporter after receiving “manual” communications from personnel at the site.

5.2.2.2 Category 1 shall be operated as a fully-attended facility for receipts with monitoring continuously during first hour of receipt, every hour during the receipt, and continuously during the last hour of the receipt, as indicated in Table G.1, since there are no remote monitoring capabilities by the transporter for either alarm or level information. Safety considerations may prohibit hand gauging during product receipt or during the 30 minutes after completion (see API 2003).

5.2.2.3 Owner/Operators shall specify in procedures where, because of the frequency of receipts or the complexity of the facility or terminal, the operator cannot reasonably be expected to focus fully on termination of one receipt at a time or may be distracted with other duties or responsibilities. In these cases, Category 1 shall not be used.

5.2.3 Category 2 Facility

5.2.3.1 A Category 2 overfill prevention system shall have an ATG system with level transmittable to a local control center or a remote control center. It uses the same sensor for level and high-high alarm (LAHH) both of which can be transmitted. Typically, alarms are transmitted to a remote control center. This transmission of alarm data to a remote control room is a key difference between Category 0 or 1 and Category 2.

5.2.3.2 Category 2 systems may be operated as a semi-attended facility for receipts if the level alarms are monitored by a remote control center. At a minimum, personnel shall be at the facility with tanks at the start of a receipt ~~and~~ or transfer operation (start denoted by the flow of product) and attend the operation for 30 minutes. In addition, personnel shall attend the last 30 minutes of the receipt and transfer operation (end denoted by the stop of product flow.) Personnel may also be required to be at the facility periodically during the receipt.

5.2.3.3 If operated as semi-attended, the ~~transporter~~ remote control center is required to assist with monitoring the receipts via the high- high tank level alarms and shall be in communication with personnel responsible for the receiving tank. The control center shall have the ability to terminate (stop or divert) product flow to the facility. The control center shall terminate product flow upon loss of signal ~~or~~ for a duration exceeding the facility/tank response time, unless operating in an abnormal condition which has been communicated by attending personnel.

5.2.4 Category 3 Facility

5.2.4.1 A Category 3 overfill prevention system uses both an ATG and an independent level alarm high-high sensor (LAHH). The key difference between Category 2 and Category 3 is that the LAHH sensor is independent of the ATG and alarm data is transmitted to a control center (with transmission of level data as determined by facility and shipper agreed protocols).

5.2.4.2 A Category 3 site may be unattended if both level data and alarms are monitored by the ~~transporter~~remote control center, and the transporter has the ability and the time to terminate the ~~filling~~ flow if ~~it~~ the filling cannot be completed prior to overfilling the tank.

5.2.4.3 The independent LAHH sensor (either a point level or continuous level device) may be connected to a second ATG ~~and~~ if it is electrically supervised and providing diagnostic alarms to the transporter.

5.2.5 AOPS

An AOPS can be added as an additional level of protection to any category of facility.

5.3 Instruments and Equipment Used for Overfill Prevention

5.3.1 General Requirements for Instruments and Equipment Used for Overfill Prevention

The equipment related to a MOPS or AOPS includes:

a) sensors (e.g. level, temperature, flow – see Annex C for commonly used liquid level sensors),

b) communications equipment ,

c) alarm and/or alert system(s),

d) final elements, automated valves (i.e. pneumatic, electric, hydraulic) and manual valves, and

e) logic solvers (e.g. relays, PLCs).

All components that make up equipment used for OPS (including cable, junction boxes, etc.) shall be suitable for the application and environment for which they are exposed and installed in accordance with the component supplier's specification.

5.3.1.1 Level Instruments

Level measurement devices consistent with Owner/Operator's practices and suitable for the application shall be used for OPS. Annex C provides selection guidance concerning some common sensor types in Table C.1 – Commonly Used Types of Liquid Level Sensors.

For higher risk storage tank operations based on tank size, product and fill rate, consider installing an ATG so that level data is available to the operators on a real time basis and to monitor the LOCs as tanks are filled.

5.3.1.2 Communications

When a diagnostic alarm is used to signal a system fault or other system malfunction, operations personnel shall act to implement "abnormal operating" procedures for the equipment that has potentially failed.

If a wireless infrastructure is being considered as the primary communication, the provision in ISA TR84.00.08 Guidance for Application of Wireless Sensor Technology to Non-SIS Independent Protection Layers ~~shall~~ should be followed to ensure appropriate reliability.

5.3.2 Alarm

Alarms set at the High-High (HH) Level serve as an ~~additional indication that~~actions should be undertaken, because the level has exceeded the maximum working level and any additional authorized volume. Procedurally based specific actions shall be taken by operations to terminate the receipt. These actions shall be pre-defined and shall not require operations to make an assessment or evaluation of the potential for overfill since an immediate response is required and is pre-defined.

The alarms that are part of the OPS shall annunciate so that the assigned personnel are notified to take actions in accordance with agreed procedures when a sensor signals that the liquid level in a tank has reached an established level of concern (see Figure 1). Assigned personnel can include facility Owner/Operator, operations personnel and transporter.

5.3.2.1 Control and Alarm Systems

Different types of control and alarm systems may be used to monitor field sensors. These systems typically provide notification for people to respond with a required action. They can also be used to control or activation of remote final control devices (i.e. closing valves, stopping pumps or initiating diversion), or share the alarm system functionality. Control panel selection depends on Owner/Operator and transporter policies and practices, and the various functions desired.

Alarm annunciators, computer display systems, SCADA and alarm and signal control panels should include appropriate visible and audible alarms with test features (where appropriate), power backup, and communications to remote locations.

Control system options include:

a) alarm and signal indicator lights whereby colors may be selected in accordance with Owner/Operator or transporter practices or local requirements;

b) audible and visible alarm display with silence and acknowledge features;

c) alarm (annunciator) systems and control panel push button provided with lights (incandescent or LED) shall be provided with the ability to "test" the light without initiation of the alarm or push button;

d) ability to activate visible display signals and audible alarms to alert personnel at locations remote from the control panel location;

e) ability to activate or control automated valves associated with automatic shutdown or diversion;

f) ability to signal to or communicate with remote locations (i.e. pipeline control centers, Owner/Operator remote offices, marine dock, security services);

g) capability to “reset” an indication when reset is required;

h) capability to initiate a manual termination; and

i) an alarm and signal to indicate a power failure to the alarm and signal control system (including field devices) and an alternate power source for backup.

5.3.2.2 Alarm Signals

Alarm signals shall annunciate at a continuously occupied location where personnel can respond according to the OPS.

Selection of audible and visual alarm equipment (i.e. horns or lights) shall comply with the electrical classification of the area in which they are installed (see API 500).

Audible and visual alarms shall be activated on detection of fault or failures within the alarm system, which initiate predetermined actions.

A visual and audible alarm shall be activated in the event that the High-High (HH) level is reached. ~~Alarms and alerts are recommended for other LOCs.~~ The High-High (HH) level alarm signal shall be distinctive from all “alerts”.

In some facilities, the main control panel (or control center) is located in an area that is not continuously staffed, or in continuous communication (e.g. radio) with field operating personnel. In these situations, High-High level alarms, shall alarm at an additional/alternate location like the storage tank area, marine dock, pipeline manifold, receipt operation control centers and transporter control center. Personnel in those areas are responsible for initiating corrective action to prevent a tank overfill. Facilities where personnel are not on site full time during receipts shall ensure that the alarm and signals are activated at locations where personnel can respond and initiate action in time to prevent an overfill incident.

5.3.3 Alerts

Use of alerts to provide information for operations personnel is acceptable, but not required by this standard. Alerts shall only be used for operational aids,~~.~~ (e.g. an alert might be set for minimum level whereas the ~~AOPS~~ OPS activation point must be an alarm. For any cases involving OPS activation, alarms shall be used.

Alerts are not a part of this standard, however, the operator may have as many alerts as desired. Responses to alerts should be understood by operators and the required actions documented.

Examples of optional information alerts:

— High level,

— Maximum Working level, and

— Minimum Working level.

5.3.4 Power and Electrical Reliability

Selection and installation of instrumentation, control systems, and electrical equipment shall comply with applicable codes and listing requirements.

Uninterruptible power supply (UPS) or redundant power supply should be specified where continuity of power to OPS monitoring and control equipment is required to ensure safe termination of product delivery in the event of loss of power. When UPS is specified, UPS availability shall be monitored and an alarm shall be provided on failure of UPS. When redundant power supply is specified, availability of power supplies shall be monitored and a ~~trouble~~ diagnostic

alarm activated on failure of a redundant power supply or power source.

The complete one-line diagrams of the electrical distribution systems for tank facility equipment and installations should be developed and maintained in accordance with the Owner/Operator's procedures.

5.3.5 Automated/Manual Valve Closure – Hydraulic Surge/Water Hammer Effect

The valve closure (opening) rate for OPS that terminates tank receipt or transfer lines shall be determined to prevent excessive hydraulic pressure transients or hydraulic surge, also known as water hammer effect. This may require analysis of facility piping system to determine whether a relief system shall be needed to protect low pressure manifold piping or offsite (transporter) piping from overpressure.

Where AOPS trips the final element closed, hydraulic surge is possible. The pressure wave can cause major problems from noise and vibration to pipe collapse or rupture. To address hydraulic surge, a study to calculate the maximum pressure of the MOPS valve must be considered unless specifically waived by the transporter. The closure time of the AOPS valve may be adjusted to prevent the hydraulic surge.

The design, operation, and conditions of any OPS that affects the transporter shall be discussed, communicated, and agreed to by the facility Owner/Operator and the transporter.

Note: In some cases where relief is directed to tankage, one valve on the tank header connection or dedicated relief line at the tank will be required to be Car Sealed Open (CSO) or Lock Open (LO) to meet API 520/521 relief discharge header requirements (see API 520 and API 521 for guidance). Thus, caution should be taken when considering AOPS, so that piping or equipment is not compromised by an automatic action.

5.3.6 Security

Access to instrumentation and the ability to change instrument configuration parameters should be restricted to ensure the physical security of the OPS equipment. Consideration should be given to cyber security concerns. IEC 62443, Security for Industrial Automation and Control Systems, provides information regarding cyber security risk assessment.

Annex A
(normative)

Automated Overfill Prevention Systems

A1 Scope

The use of an Automated Overfill Prevention System (AOPS) is not mandatory, but if an AOPS is chosen by the Owner/Operator, Annex A becomes normative. This Annex provides guidance on the required design, operation and maintenance practices for the implementation of AOPS. The Owner/Operator's design of an AOPS shall be implemented by appropriate personnel knowledgeable in the design, periodic reviews, and management practices associated with instrumentation, control systems, shutdown systems, and tank facility operations**.**

A2 Automatic Overfill Prevention System (AOPS)

An AOPS is an automatic system that terminates filling ~~that terminates filling~~ because of the risk associated with the procedural elements of the overfill prevention system failing is too high. An AOPS does not depend on any human intervention nor require communications to or from any remote facility. AOPS operation shall be sufficient to prevent an overfill without exceeding process constraints on control element operation.

The AOPS shall be designed and installed so that failures associated with ATG hardware, software, communications, wiring connections or cabling will not affect the availability of the AOPS or cause premature activation.

A3 Equipment

A.3.1 AOPS Sensor

The sensor shall be installed in a manner to minimize common cause failure between any other overfill prevention system (or automatic tank gauge) and the sensor.

The level sensor system shall be connected to a logic solver.

A.3.2 AOPS Logic Solver

The following equipment can be used as Logic Solvers:

a) Distributed Control System (DCS)
b) Programmable Logic Controller (PLC)
c) Trip Amplifier
d) Solid State Relay circuit.

Where programmable electronic systems (e.g. PLC) are used as the logic solver, the relevant considerations are as follows:

1. Design of AOPS shall address unsafe failure modes of logic solvers by:

   a) Detection of input and output (I/O) failures via frequent diagnostic of the I/O point and confirmation of correct action and detection by the PLC.

   b) Detection of process program requires an external watchdog timer (WDT). In many cases, a watchdog timer consists of a time delay relay that is installed external to the PLC. The PLC sends a reset to this watchdog timer frequently enough to prevent the timer from timing out. The watchdog "timing out" is an indication that the PLC has failed and the state of the tank being monitored by the PLC is unknown.

c) Users shall analyze and specify the actions required when PLC failure is detected. Some actions to be considered if a PLC failure is indicated by the I/O failure detection or WDT are:

— send an alarm to monitoring locations (local and remote); this alarm should be generated by the WDT and not the PLC it monitors;

— automatically or manually terminate flow to or divert the flow of product from any tanks that have a LAHH monitored by the failed PLC; and/or

— activate AOPS; where possible PLC's shall be programmed to detect and alarm cabling faults, blown fuses and open circuits.

2. Where programmable electronic equipment is applied, user-developed AOPS applications shall confirm to Owner/Operator practices.

3. Design of AOPS shall address protection of AOPS equipment from unauthorized or unintended modifications.

4. Any changes to the AOPS logic solver hardware or firmware shall be implemented in accordance with the instructions of the manufacturer and shall be subject to management of change procedures.

A.3.3 AOPS Final Element

A.3.3.1 Pump Stop

If pumps are used to transfer product into the tank, the pumps may be considered as the final element in the AOPS. Pumps shall be stopped automatically by introducing an interlock in the pump starter circuit to terminate the flow and should be isolated in a timely manner.

A.3.3.2 Automated Valves

When automated shutdown or diversion systems are provided, the receiving valve (or valves) for each facility or tank shall be equipped with an automated actuator that has provisions for both local and remote automated closure. Valves shall provide valve status (Open/Closed) to both local and remote operating stations. Where fail-safe operation of valves is specified, valves shall be equipped with mechanical devices designed to move the valve to the safe state. Selection of Hold, Open, or Close fail-safe operation shall be specified by the Owner/Operator.

If the AOPS valve is located inside the tank dike, it shall be fire safe to withstand fire for a duration defined by the Owner/Operator, based on the fire safety response. Aboveground AOPS valve cabling and support structure should be protected from the fire. If the AOPS valve is not fire safe, fire proofing shall be considered.

Actuators can be electrical, hydraulic, hydroelectric or pneumatically operated. Automated valves should be interlocked with the tank liquid level transmitter. Emergency Shutdown button, if available for valve closure or for pump stop, must be located in a safe area outside of the tank dike. Remote valve operation stations shall be in a control room or other safe, continuously-occupied location. An additional manual valve or valve actuator(s) located outside the tank dike or other safe location easily accessible to the operator should be identified to prevent tank overfill in the event of loss of motive power to the AOPS valve.

It is recommended to have a fail-safe design for the automated valve. The rate of valve operation shall be controlled, as necessary, to prevent hydraulic hammer and permit safe operation. If the automated valve is not failsafe, UPS backup or loss of motive power alarm with an operator response must be considered. Loss of valve operator motive power shall initiate an alarm, triggering procedures for abnormal conditions. If the valve operator system has no manual operations feature outside the tank dike, then the back-up system shall be sized adequately to permit operator response to alarm on loss of motive power supply to the actuator. Operation of fail-safe devices shall not prevent emergency manual operation of the valve.

For scenarios with higher risk acceptance criteria, consideration should be given for use of two valves in series (or one valve and one pump) to lower the likelihood of automated valve failure.

When the AOPS system receives notification that the product in the tank has reached the AOPS level the system shall inhibit movement of the valve(s) from the safe position until the system has been reset from the local alarm and

signal control panel, the site has become attended, and operating procedures for abnormal conditions have been implemented.

A.3.3.3 Fail Safe Design for AOPS

Fail Safe Design of AOPS equipment is recommended to mitigate the "loss of primary (utility)" power scenario. If the risk assessment shows a direct and credible risk of overfill is immediately caused by lack of utility power during normal receipt operations, then the AOPS shall be fail-safe. If the AOPS valve is not fail-safe, then abnormal operations procedures shall be implemented upon loss of utility power. To address the loss of primary power scenario, the Owner/Operator should consider a UPS or loss of power alarm with an operator response option to address risk associated with the loss of primary power.

In the event of loss of communication between AOPS components, i.e. between sensor, logic solver, and/or valve, the AOPS valve should move to its fail-safe position, as determined by the Owner/Operator.

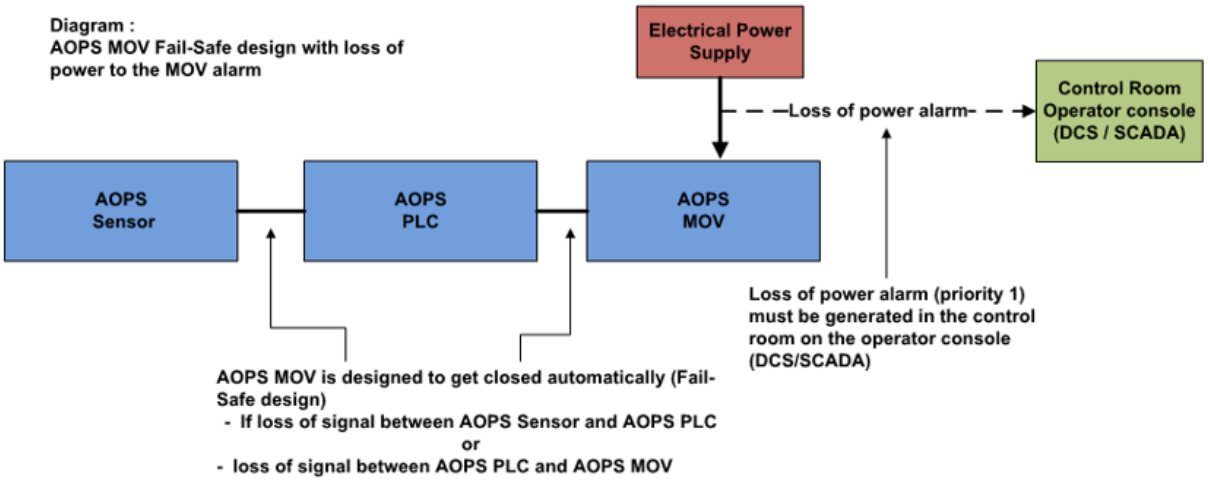


Figure 2 – AOPS Fail Safe Design and AOPS Valve Loss of Motive Power Alarm

Note to API: Change the wording from “designed to get closed automatically” to “designed to close automatically”.

A.3.4 Documentation

The following documentation shall be maintained and approved by an authorized representative of the Owner/Operator:

1. piping and instrumentation diagrams that clearly show the current state of all AOPS equipment;

2. functional descriptions (i.e. logic narratives or loop diagrams) that clearly describe the AOPS functional requirements and how frequently the system must be tested;

3. proof test procedures detailing how the AOPS is tested, what equipment is used, and what records are retained;

4. preventive maintenance plan showing planned inspection and maintenance to ensure ongoing integrity of the AOPS;

5. override and bypass management procedure detailing how the use of overrides and bypasses shall be reviewed and approved;

6. AOPS maintenance records related to proof testing, maintenance history, change history and a history of all equipment failures and action implemented to correct those failures;

A.3.5 Installation and Commissioning

1. All equipment and cabling shall be installed in accordance with design documentation and manufacturer's instructions.

2. All equipment and cabling shall be protected against likely physical damage.

3. All equipment and communications subsystems shall be clearly tagged to allow identification and association with design and maintenance documentation.

4. Installed AOPS shall be proof tested after initial installation.

5. All new AOPS equipment shall be proof tested as a complete functional entity (sensor through logic solver to final element) following installation and prior to start-up and introduction of hydrocarbons.

A.3.6 Testing

Proof testing shall be as described in Section 4.5 and Annex H.

A.3.7 Maintenance

All operations and maintenance shall be carried out according to defined and documented procedures. Operating personnel and maintenance personnel shall be trained to ensure that they are competent. Where operation or maintenance is permitted with AOPS bypassed, overridden, or not in service, Owner/Operator shall determine any necessary operational limitations or additional measures to prevent overfill and include them in operating and maintenance procedures.

Annex B
(informative)
Management Systems
(This Annex has been deleted.)

Annex C
(informative)

Liquid Level Instrumentation Considerations

The types of sensors available are:

C.1 Point Level Sensor

C.1.1 This type of sensor can be used for a High-High (HH) tank level alarm

C.1.2 If point level sensors are used, they should include self-diagnostic and system analysis for proof testing options: these types of sensors should be used. Mechanical point level sensors without self-diagnostic or system analysis functionality are not recommended.

C.2 Continuous Level Sensor

C.2.1 This type of sensor continuously measures the level of the product in the tank;

C.2.2 Continuous level sensors may be used to measure both level and provide a High-High (HH) tank level alarm in tanks;

C.2.3 Continuous level sensors may be used as an Independent High-High (HH) level alarm. Additional continuous level sensors can be used as an independent High-High (HH) level alarm for AOPS tanks;

C.2.4 There are mechanical, electromechanical and electronic continuous level sensors for tank gauging systems. Mechanical level sensors without self-diagnostic or system analysis functionality should not be used.

C.3 Automatic Tank Gauge (ATG)

C.3.1 For ATG, use a high accuracy continuous level sensor that meets the specifications for API *MPMS* Ch. 3.1B recommendations;

C.3.2 This gauge automatically calculates the tank ullage and innage for the operator to determine the tank capacity for a receipt;

C.3.3 An additional ATG can be used as an Independent High-High (HH) tank level alarm in conjunction with another ATG in AOPS tanks; and

C.3.4 these additional features:

i) water measurement,

ii) temperature measurement,

iii) volume correction, and

iv) high and low level relays for alerts.

NOTE High-High (HH) tank level sensors used as part of the OPS on floating roof type tanks that measure the roof position instead of the product level should also be able to detect the presence or level of product on top of the roof in the event the roof sticks or sinks into the liquid.

Table C.1 represents the more commonly used types of liquid level sensors.

Table C.1—Commonly Used Types of Liquid Level Sensors

Type	Description
Float point mechanical sensors	Used to determine product level in cone roof tanks. As a tank is filled, the product rises within the tank lifting the float until a predetermined fill level is reached. The float then activates the alarm and signal using either a mechanical relay or reed switch.
Displacement electronic point sensors	Sometimes used in lieu of float sensors in tanks where product may be agitated, surging, foaming or have low specific gravity The sensor driver is calibrated to provide a specific voltage for a corresponding change in capacitance (i.e., gap or displacement). In turn, this allows the displacement or position to be determined.
Opto-electronic point sensors	Used to determine product level in all types of clear liquids. Opto-electronic level sensors use an infrared light source that passes through a light conductor that is refracted at a different rate when surrounded by air or liquid. When the liquid covers the tip of the sensor, there is a change in the refraction rate which activates the alarm and signal.
Weight (slack cable) mechanical point sensors	Mechanical level sensors are used to determine product level in a floating roof tank. As the tank is filled, the floating roof rises to a predetermined fill level where it contacts the weight. As the weight is lifted by the roof, the cable goes slack and the level switch opens, activating the alarm and signal. Electronic capacitance switches with a flexible cable can also be use to determine the position of the floating roof.
Tuning fork electronic point sensor	Vibrating fork level switches utilize a piezoelectric-driven tuning fork that exhibits a large change in resonant frequency when immersed into a liquid process changes from dry to wet or wet to dry.
Ultrasonic point sensors or Gap switches	Work on the principle that the signal strength from a sending piezo-crystal is less in air than in liquid.
Capacitance point and continuous electronic sensors	Uses the change in dielectric constant to determine the presence of the liquid for a high switch or the rise of the level for continuous measurement.
Radar (non-contact) point level and continuous sensors	Use a microwave signal that is reflected off of the liquid. FMCW or pulse time of flight is used to measure the time it takes for the signal to be returned to the sensor that is then converted into the distance traveled.
Radar (TDR or GWR) continuous sensors	Sends a microwave signal down a cable or rod, measures the time for the signal to return to the sensor and calculates the distance to determine the level. Can use rigid or flexible probes.
Servo continuous electronic sensors	Uses a displacer with neutral buoyancy supported on a wire that is connected to a resolver that measures the distance from the top of the tank to the top of the liquid.
Mechanical float and tape continuous sensors (electronic option)	Use a neutral buoyancy float to measure the distance from the top of the tank to the top of the liquid. This system uses a gear driven indicator to show the tank level and does not require power. An electronic option is available.
Magnetostrictive continuous sensors	Measures the position of the permanent magnet located in a float on a magnetostrictive wave guide. Can use rigid or flexible probes.
NOTE These are examples and are not intended to be inclusive of all possible technologies	

Annex D
(informative)

Determining Levels of Concern and Tank Capacity

D.1 Scope

This annex provides assistance in establishing levels of concern with regard to the operation of storage tanks and development of an overfill prevention program.

D.2 General

D.2.1 The methods described in this annex for determining levels of concern utilize strapping charts for accurate gauge level equivalence although other methods are acceptable. This annex is not intended to outline all methods, considerations, or tank configurations an Owner/Operator might consider when determining levels of concern. Whatever method is chosen, it is essential that tank levels be determined with the most current measurements and information. The levels of concern are established and recorded by the Owner/Operator using their preferred method.

D.2.2 Management of change principles are recommended to be applied, and level settings adjusted, whenever a tank modification affects levels of concern. This includes mechanical changes (e.g. adding a double bottom, adding an internal floating roof, changing construction of the floating roof or placing a cover over an open top tank) as well as operational changes (e.g. a change in receiving flow rates, procedures, or product type).

D.2.3 Levels of Concern Order of Determination

D.2.3.1 Critical High (CH) Level– should be determined prior to any other dependent level (High-High (HH), Max Working, etc.). Critical High (CH) is dependent on tank dimensions and allowable stresses. Justification of Critical High (CH) occurs at initial construction or during an inspection. Conceptually, there are two main factors that limit Critical High (CH):

- Allowable Stresses – Critical High (CH) may be limited by the allowable stress, see API Standards 650 and 653 for more details.

- Physical Limitations – Critical High (CH) may be limited by a tank's physical attributes (e.g. the level at which product overflows, mechanical contact between the floating roof and/or its appurtenances with stationary roof or shell attachments, or any other limit designated by the Owner/Operator). Depending on the tank specifics, the following factors may warrant further consideration:
-
    - Attention to venting locations, fire-fighting piping, and tank/floating roof geometry may avoid interferences which can result in structural damage to the tank and/or sinking of a floating roof.
    - Per Figure D-1, measurements may be determined computationally by calculation of the roof buoyancy or experimentally by observation of liquid line marks (measured when the tank is out of service or getting on the roof using accepted access requirements). A safety factor may be applied to mitigate differences in product, thermal expansion, or potential measurement errors.

- Dynamic Changes – Changes that occur to the tank such as settlement (which can cause tilting) or hydrostatic testing (which can deform the tank bottom).

D.2.3.2 Response Time – should be determined before any of the independent levels (e.g. High-High (HH), Max Working, etc.) are set. The response time (Section 4.4.2) gives details on common considerations when a specific response is known, assuming that the Owner/Operator has determined the specific response beforehand. However, when the specific response is not clear or there are a number of potential operator responses in various conditions, determining responses and times may be a challenge. Below is a list of considerations that may help determine

potential responses so all response actions are examined.

- List different operations of the tank and respective flow rates – different movement types may have significantly different responses or lines of communication. For example, shutting down a movement from a tank may be as simple as pressing a button, but shutting down a similar movement from a vessel requires communication to the PIC, who then communicates with the ship captain. That captain then passes along the order to shut down the energy source.
- List potential responses for each operation above – an operation may have multiple methods of shutdown. For example, a small inbound pipeline delivery is normally shutdown by telephone communication with the pump station's transporter. Alternatively, in an emergency condition, the pipeline may be blocked in with incoming flow diverted to a relief tank.
- Determine response time for each unique response action (see Section 4.4.2) – analysis of multiple response actions may be required to ensure all operating circumstances and potential responses are covered and consistent with procedures.
- If warranted, consider responses to abnormal conditions – if any abnormal conditions were to occur during a normal fill, ensure that the response time is adequate.
- Ensure that all response actions are consistent with practiced and documented procedures.

D.2.3.3 AOPS (if installed) – level may be established at any point lower than the Critical High (CH) Level as long as the AOPS response time is sufficient to close the valve before CH. It shall also be installed at least as high as the HH ~~plus a margin of 3 in.~~ after the (CH) is established See the AOPS level section for additional information and minimum distances that may apply. An AOPS Response Time is the total response time of the automated system from sensing AOPS level set point to termination of the receipt.

D.2.3.4 High-High (HH) Level– after Critical High (CH) level, maximum fill rates and response times are established, the High-High (HH) level may be determined (see Section 4.4.1.3). There are multiple acceptable approaches to this calculation because of conversions that must be made with the strapping chart, in essence:

$$HH = CH - (\text{Max Fill Rate}) \times (\text{Response Time}).$$

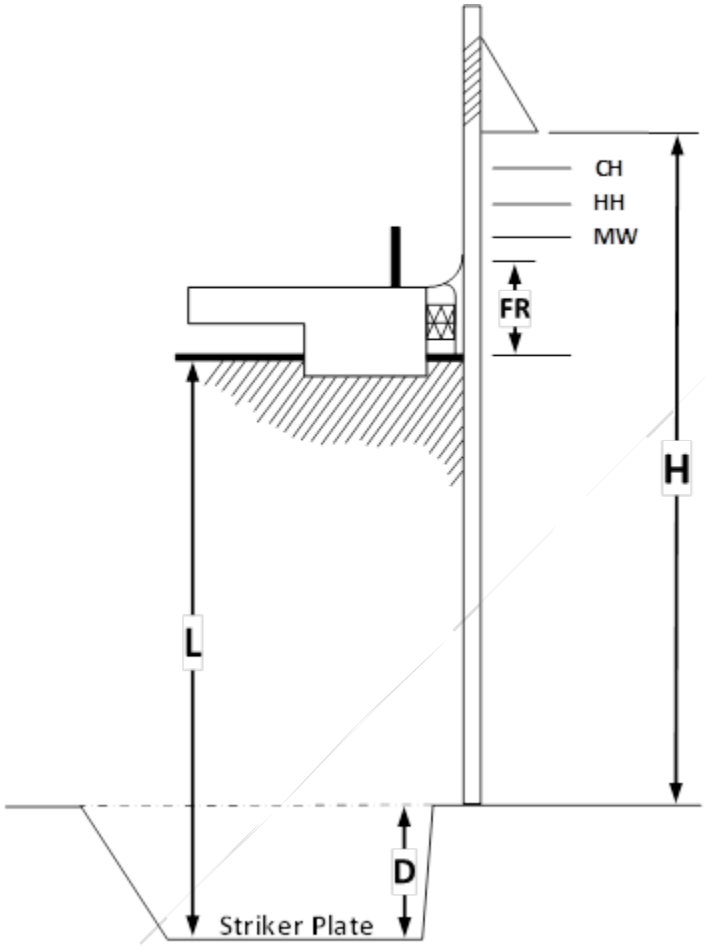
Whether the fill rate is converted into a linear rate of level rise or levels are converted to volumes, the result should be the same. See the High-High (HH) tank level section of this document for more details. A minimum distance from the Critical High (CH) may apply.

D.2.3.5 Maximum Working Level (MW) – calculated after High-High (HH). Specific rules for determining this level are left up to the Owner/Operator (see section 4.4.1.4). If the MW is response time dependent, the calculation may be similar to that described for High-High (HH) above with an alternate (Maximum Working) response time. See the Maximum Working level section for additional information.

D.3 Worked Examples

The following worked examples are for illustrative purposes only. Actual tank configurations may be simpler or more complex.

D.3.1 Working Example 1



Example 1 Tank Information:
Pontoon External Floating Roof (EFR) with Sump and Overflow
Tank gauged out of sump
Not to Scale

A responsible party determined the measurements below:

Example Tank 1: Measurements		
Description	Symbol	Value
1. Effective Overflow Height	H	48.6’
2. Depth of Sump	D	5.3’
3. Floating Roof Thickness	FR	4.15’
4. Tank Appurtenances above EFR	-	None

1. Effective Overflow Height (H) - was measured from the floor reference point to the bottom of the overflow vent.
2. Depth of Sump (D) - was measured from the floor reference point to striker plate at the bottom of the sump.
3. Effective Floating Roof Thickness (FR) - this measurement was calculated using the roof dimensions and expected buoyancy with 10° API gravity product.
4. Tank Appurtenances above EFR - None, there is nothing above the EFR sufficiently close to be of concern.

Example 1 Critical High (CH) Calculation Information

CH was determined to be the lowest of:

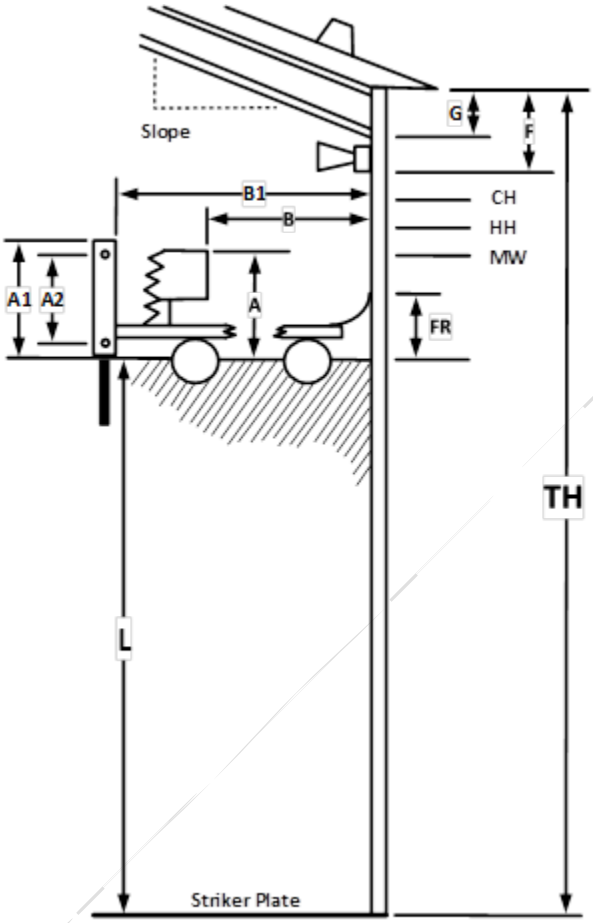
Example Tank 1: Critical High (CH) Calculation		
Critical High (CH) Factor	Calculation Method	Calculated Height
1. Overflow (H + D)	H + D	53.9’
2. Shell Stress/Maximum Fill Height	See below	51’ @ 10 API
3. Corroded Areas	-	N/A
4. Mechanical Contact of EFR	-	N/A
5. Mechanical Contact of Appurtenance	-	N/A
CH (minimum of above CH factors)	Minimum of above	51’

1. Overflow - Potential sources of product overflow include the shell overflow vents since there are no lower openings within the shell. The overflow height from the striker plate is equal to measurements H + D; Measurements H and D are the bottom of overflow height and striker depth, respectively.
2. Shell Stress/ Maximum Fill Height - Allowable tank shell design stress was determined using API 653 section 4.3 (other calculation methods such as API 579 membrane stress may be used) and information from the inspection report. Using the design product gravity of 10° API, the Maximum Fill Height was calculated to be 51’.
3. Corroded areas (or temporary repairs that affect the operating height) – Not Applicable. Repairs and current condition of the tank were taken into account when calculating the Shell Stress / Maximum Fill Height above.
4. Mechanical contact of Floating Roof – Not Applicable; mechanical contact of the roof (above) and/or appurtenances (below) was also considered per the owner operator standard. However, the responsible party observed that the tank was without a fixed roof and concluded there were no reasonable contact points between the EFR and any overhanging equipment or platforms.
5. Mechanical contact of Appurtenance – Not Applicable; See Mechanical Contact of Floating Roof above.

As evident above, the lowest calculated Critical High (CH) Factor is Shell Stress / Maximum Fill Height at 51' for the design product. Therefore, it marks the Critical High (CH) level at 51' for this example tank.

Note: While overfill prevention allows this set point, it should be noted that emission regulations, if applicable, might be violated because the seal breaches the overflow vents.

D.3.2 Working Example 2



Example 2 Tank Information:
Pontoon Aluminum Internal Floating Roof Tank
Not to Scale

With the purpose of setting tank levels for a newly constructed tank, a responsible party examined Example Tank 2 for potential Critical High (CH) limitations in accordance with Section 4.4.1.1. The following measurements (shown in Example Tank 2) were collected by a 3rd party calibration company using a certified plumb bob. Additional notes on the measurements follow:

Example Tank 2: Measurements		
Description	Symbol	Value
1. Effective Shell Height	TH	60.10'
2. TOS to Bottom of Foam Nozzle	F	1.08'
3. Effective Floating Roof Thickness	FR	1.00'
4. Girder Depth from TOS	G	0.75'
5. Appurtenance Height from Liquid	A	2.67'

6. Floating Roof Leg Height from Liquid	A1	1.50’
7. Floating Roof Leg Pin to Pin Difference	A2	2.33’
8. Appurtenance Distance from Shell	B	20.00’
9. Floating Roof Leg Distance from Shell	B1	5.00’
10. Roof Slope	SLOPE	0.75 : 12

1. Effective Shell Height - measured from top of shell to the datum plate
2. TOS to Foam Nozzle - measured from the top of shell down to the bottom of the foam nozzle
3. Effective Floating Roof Thickness – measured from the designed float level to the top of the wiper seal

The responsible party gathered the remainder of the information from as-built tank drawings and a field visit utilizing a measuring tape:

4. Girder depth from TOS - estimated from as-built drawings showing steel shape and configuration
5. Appurtenance Height from Liquid - The measurement is not readily measurable from the top of the roof, consequently the responsible party back-calculated “A” using field measurements and information provided by the strapping chart company. To perform the calculation, it was observed in the field that the appurtenance was approximately 20 inches higher than the top of the wiper blade, adding the relative height of the wiper blade (“FR”) results in the approximate measurement from the appurtenance relative to the liquid
6. Floating Roof Leg Height from Liquid – the estimated height from liquid calculated similarly to Appurtenance Height from Liquid above
7. Floating Roof Leg Pin to Pin Difference – the measurement from pin to pin on a floating roof leg
8. Appurtenance Distance from Shell – the measured horizontal distance from the appurtenance to the closest point on the tank shell
9. Floating Roof Leg Distance from Shell – the measured horizontal distance from the outer most floating roof leg to the closest point on the tank shell
10. Roof Slope – measured slope of the fixed roof

Example 2 Critical High (CH) Calculation Information

CH was determined to be the lowest of:

Example Tank 2: Critical High (CH) Calculation		
Critical High (CH) Factor	Calculation Method	Calculated Height
1. Overflow	TH – F	59.02’
2. Shell Stress/Maximum Fill Height	See below	60.10’ @ 1.0 SG
3. Corroded Areas	-	N/A
4. Mechanical Contact of Appurtenance	TH - G - A + (B x slope)	57.93’
5. Mechanical Contact of Floating Roof Leg (Second Appurtenance)	TH G - (A1 + A2) + (B1 x slope)	55.83’
6. Mechanical Contact of FR	TH - F - FR	58.02’
CH (minimum of above CH factors)	Minimum of above	56.58’

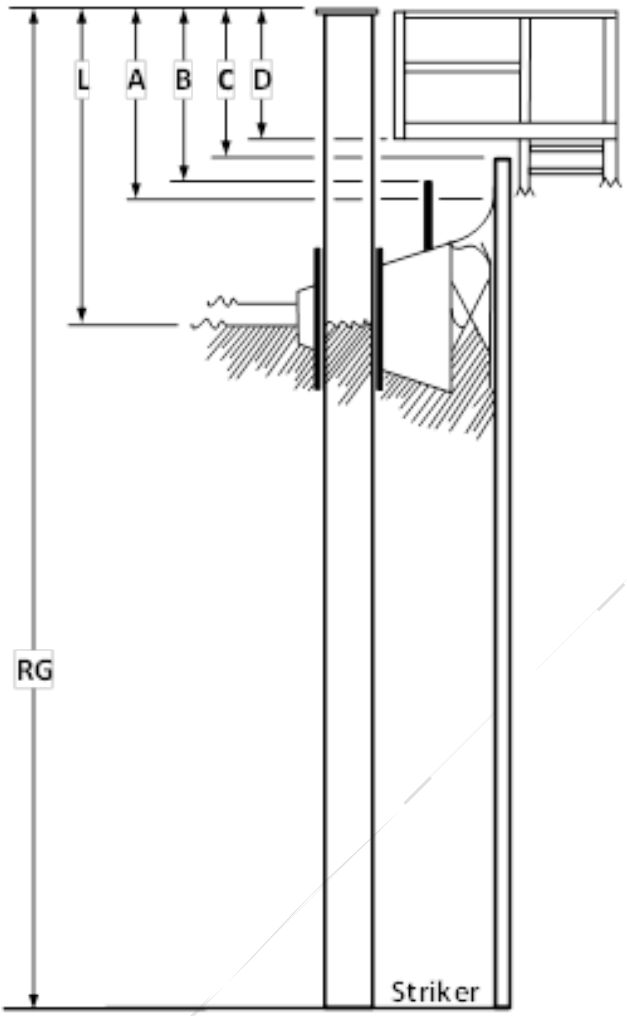
1. Overflow - Although Example Tank 2 does not have a designed overflow, per company standard, the

foam nozzle is used as an overflow level in this calculation, since it was not designed to contain product.

2. Shell Stress / Maximum Fill Height – Shell thickness was calculated by the tank design firm using API 650 section 5.6. Design conditions were calculated using a liquid full shell with 1.0 specific gravity fluid.
3. Corroded Stress - Corroded stress limit did not apply for this new tank and corrosion allowance was provided for in the above stress calculation.
4. Owner/Operator Level - Mechanical contact of the roof appurtenances was considered per the Owner/Operator's standard. In creating the equation used above, the responsible party reasoned that as the tank level ("L") rose, the appurtenance ("A") would first impact the girder ("G") before any other appurtenance impact. Because the roof sloped slightly and the appurtenance was some distance from the shell, the responsible party reasoned that the girder height at which the appurtenance would impact was effectively higher than it was measured at the shell. Distance ("B x slope") was added to the girder height to indicate the actual girder height in plane with the appurtenance.
5. Owner/Operator Level – Mechanical Contact of Floating Roof Leg (Second Appurtenance) was also considered. Calculated similarly to the Mechanical Contact of Appurtenance above, this calculation includes factors for current leg height and leg pin difference used for determining the height of the leg at its maximum extension from the liquid (A1 + A2). This calculation did not take into account the girder level from the roof as it was determined that the legs were spaced between the girders and should not make contact.
6. Owner/Operator Level - Mechanical contact of roof wiper seal was also considered per Owner/Operator's standard. In creating the equation used above, the responsible party reasoned that as the tank level ("L") rose, the wiper brackets ("FR") were likely to contact the fire nozzle ("F") before any other contact of the main roof body occurred.

The minimum height of the above Critical High (CH) Factors sets the Critical High (CH) for this example at 56.58' (mechanical contact of floating roof legs).

D.3.3 Working Example 3



Example 3 Tank Information:
Steel Pontoon External Floating Roof Tank
Not to Scale

With the purpose of checking levels of concern on a newly acquired tank asset, a responsible party examined Example Tank 3 for potential Critical High (CH) limitations in accordance with section 4.4.1.1. With the tank in service, liquid level held static and all necessary safety protocols in place, entry was made onto the roof to obtain measurements. The following measurements were taken by a competent person using a calibrated plumb bob and a calibrated tank gauge. Additional notes on the measurements follow:

Example Tank 3: Measurements		
Description	Symbol	Value
1. Product Hand Gauge	L	39.60 ft
2. Reference Gauge Height	RG	56.12 ft
3. Gauge Point to Secondary Seal	A	10.62 ft
4. Gauge Point to Foam Dam	B	10.20 ft
5. Gauge Point to Top of Shell	C	7.18 ft
6. Gauge Point to Lowest Obstruction	D	5.60 ft

1. Product Hand Gauge – measured liquid level in tank from datum plate
2. Reference Gauge Height – measured from datum plate to gauge point
3. Gauge Point to Secondary Seal – measured from level with gauge point to top of secondary seal nearest the gauge point
4. Gauge Point to Foam Dam – measured from level with gauge point to top of foam dam nearest the obstruction
5. Gauge Point to Top of Shell – measured from level with gauge point to top of shell nearest the gauge point
6. Gauge Point to Bottom Lowest Obstruction (gauging platform) – measured from level with gauge point to the bottom of the lowest obstruction nearest the foam dam

Example 3 Critical High (CH) Calculation Information

CH was determined to be the lowest of:

Example Tank 3: Critical High (CH) Calculation		
Critical High (CH) Factor	Calculation Method	Calculated Height
1. Overflow (H + D)	RG – C	48.94’
2. Shell Stress/Maximum Fill Height	See below	48.94’ @ 30 API
3. Corroded Areas	-	N/A
4. Mechanical Contact of Appurtenance	L + (B - D)	44.20’
5. Mechanical Contact of EFR	L + (A - C)	43.04’
CH (minimum of above CH factors)	Minimum of above	43.04’

1. Overflow – Overflow is the equivalent to reference gauge less the vertical distance to the overflow
2. Shell Stress / Maximum Fill Height – Per the latest API 653 report, shell thickness was acceptable for a liquid full tank at a design level of 30° API. Actual product in the tank was less dense than design product and therefore, the calculations from the report were deemed sufficient.
3. Corroded Stress - Corroded stress limit would be evaluated on the next API inspection scheduled in 11 years or if deemed pertinent by monthly external inspections or some other means.
4. Owner/Operator Level - Mechanical contact of the roof and appurtenances were considered per the Owner/Operator’s standard. The responsible party reasoned that as the tank level (“L”) rose, the foam dam (“B”) would first impact the gauging platform (“D”) before any other roof or appurtenance impact. In effect, (“L”) could rise the difference between the foam dam and the gauging platform, or “B – D”.

5. Owner/Operator Level – Exposure of roof seal was also considered per Owner/Operator's standard. The responsible party reasoned that as the tank level ("L") rises the wiper ("A") would also rise and could continue to rise until it was above the top of the shell ("C"), violating company standard and causing emission concerns. In effect, ("L") could rise the difference between the wiper and the top of shell, or "A – C".

The minimum height of the above Critical High (CH) Factors set the Critical High (CH) for this example at 43.04 feet (mechanical contact of appurtenance).

Response Time (Continuation of Example 3):

1. Response Time, MW to HH
    a. Tank is operated inbound by pipeline, outbound by trucks, no marine or rail. Maximum inbound rate is dictated by the pipeline at 5000 BPH. First shutdown will be manual via a call to the Transporter and manual shutdown of pump.
    b. Visual and audible alert at MW notifies Operator that MW level has been breached.
    c. 5 minutes is allotted for 1) acknowledgement of alarm, 2) a call from Owner/Operator to Transporter, and 3) discussion of emergency condition.
    d. 9 minutes is allotted for 1) Transporter's donning of PPE, 2) physical travel time to pump location and, 3) initiation of shutdown response (stop pump).
    e. 2 minutes is allotted for 1) pump shutdown and 2) closure of inbound and tank valves
    f. Total MW Response Time:

MWRT = 16 minutes

2. Response Time, HH to CH
    a. Second shutdown response will be closure of tank valve and diversion of flow through surge valve into surge relief tank. This is the procedural response in the event that communication is down or the Transporter is unresponsive.
    b. 1 minute is allotted for 1) acknowledgement of alarm and 2) initiation of shutdown response (initiate tank valve closure for diversion to surge relief tank)
    c. 2 minutes is allotted for tank valve closure
    d. Total HH Response Time:

HHRT = 3 minutes (Reference HHRT Test Document Number XXX Dated XXX)

Alarm Levels Calculation – Volume Conversion Method (Continuation of Example 3):

Example 3: Given Info		
Description	Symbol	Value
1. Critical High (CH) Level	CH	43.04 ft
2. Critical High (CH) Volume	CH_{vol}	31,846 BBL
3. Maximum Fill Rate	MFR	5000 BPH
4. High-High (HH) Response Time	HHRT	3 min
5. Maximum Working Response Time	MWRT	16 min

Example 3: Calculated Values (Volumetric Rate)			
Description	Symbol	Calculation Method	Value
6. High-High (HH) Volume	HH_{vol}	= CH_{vol} - (MFR x HHRT)	31,596 BBL
7. High-High (HH) Level	HH	Convert HH_{vol}	42.70 ft
8. Maximum Working Volume	MW_{vol}	= HH_{vol} - (MFR x HHRT)	30,262.7 BBL
9. Maximum Working Level	MW	Convert MW_{vol}	40.88 ft

1. Critical High (CH) is typically calculated as a level. These example calculations use the previous example from Example Tank 3 above.
2. Using the strapping chart, determine the volume at Critical High (CH) and interpolate, as needed.
3. Maximum flow rate of 5000 BPH was confirmed via email from the Transporter/pipeline.
4. Define the equation and include unit conversion when necessary.
5. Convert High-High (HH) Volume to High-High (HH) level and interpolate, as needed.
6. Now that High-High (HH) has been determined, Maximum Working can be calculated by subtracting the expected volume increase over the response time period.
7. With the High-High (HH) Volume, Max Working Response Time, and Maximum Flow Rate above calculate Max Working Volume
8. Convert Max Working Volume to Max Working Level and interpolate, as needed
9. Required API 2350 Levels are complete, calculate any AOPS or Owner/Operator defined levels, as needed.

Alternative Alarm Levels Calculation – Rate Conversion Method
(Continuation of Example 3 Response Time):

This alternative alarm levels calculation example starts at 6a below and continues from number 5 of the calculation above. Although the approaches are slightly different, both methods may be valid for calculating tank levels and should result in the same levels, unless extreme tank irregularities exist. Alternative approaches may also be used if deemed sufficient by the Owner/Operator.

Example 3: Calculated Values (Linear Rate)			
Description	Symbol	Calculation Method	Value
6a. Conversion Factor	CF	From Strappings	731.615 BBL/ft
7a. Maximum Fill Rate Linear	MFR_l	MFR / CF	6.843 ft/hr
8a. High-High (HH)	HH	=CH – MFR_l x HHRT	42.70 ft
9a. Maximum Working Level	MW	= HH – MFR_l x MWRT	40.88 ft

6a. Using the strapping chart volumes and levels near Critical High (CH), calculate a volumetric to linear conversion rate (CF). This rate may be given in the strappings in the form of a conversion or strapping table.

7a. Convert maximum volumetric fill rate (MFR) to linear rate of rise, noted above as the maximum fill rate linear (MFR_l).

8a. Calculate the High-High (HH) response time with the respective High-High Response Time (HHRT) and the linear maximum fill rate (MFR_l). As you can see above, using the linear maximum fill removes the need to return to the strapping chart for a volume to height conversion

9a. Now that High-High (HH) is calculated, the Max Working Volume may be calculated in a similar fashion using the Maximum Working Response Time (MWRT).

The required API 2350 Levels are complete. Now, any AOPS or other Owner/Operator defined levels may be calculated, as needed.

Annex E
(informative)
Risk Assessment

E.1 Introduction

Risk management is a strategic process aimed at controlling risk to an acceptable level by managing both the likelihood (probability) and the severity (consequences) of hazardous events through operational, process, and other changes. Risk analysis is used to assess likelihoods and consequences in order to support the decision-making process so that effective measures can be taken to reduce risk to acceptable levels.

A risk assessment must include likelihood and consequences for overfill events, but risk management also requires that if risks are unacceptable to the stakeholders, risk must be reduced by changes in equipment, systems, or other methods of control that can be exercised by the tank Owner/Operator. Factors that influence the consequence are the process fluid properties, location, types of containment, flow rate, vapor generation, structural damage, environmental and safety impacts, and others.

The risk assessment methodology typically requires implementation of these tasks:

- Hazard identification
- Determination of initiating events
- Postulating scenarios, or event-chains that may result in unwanted outcomes
- Likelihood estimates for the identified scenarios
- Consequence estimates for the identified scenarios
- Combining of likelihood and consequence to rank the level of risk
- Identification of risk reduction projects, changes in operations, equipment or business processes that result in lowering risk
- Resource allocation decisions, budgeting and timescale considerations
- Deployment of the resources and a commitment to follow the plan

Risk analysis looks at the combination of the probability of some event occurring during a specified time period (annual) and the consequences associated with the event. One way to combine probability and consequences to obtain risk magnitude is:

$$Risk = Probability \times Consequence$$

One objective during the risk analysis is to determine the likelihood or probability of a scenario occurring is measured in terms of the frequency or occurrences per year for a specific event. This estimate covers the chain of events from the initiating event through to eventual outcome. The estimation of the likelihood is determined by looking at the reliability and availability of both equipment and human performance.

The second objective of the analysis is to determine the consequences that occur as a result of the incident. The consequence of a scenario occurring is measured in terms of the potential harm to people, property and/or the environment. Some of the consequences are that a release:

- creates a vapor cloud that could ignite causing human health impacts and facility or adjacent property damage
- creates a cloud or toxic release, such as hydrogen sulfide

- results in a spill that causes environmental damage to soil, surface water, and/or groundwater or potable water
- causes a business interruption

When evaluating the consequences, a qualitative or quantitative approach can be taken. The use of descriptors like minor or severe injury can be used based on experience or the potential outcomes such as jet fire, flash fire, pool fire, Vapor Cloud Explosion (VCE), Boiling Liquid Expanding Vapor Explosion (BLEVE) and/or spills to better estimate the consequences.

Once the risk analysis is complete, the identified risk reduction measures are evaluated. Risk reduction is required for those risks that management judges to exceed acceptable risk. Risk reduction can be accomplished through a wide range of measures including engineering and/or operational control measures or by changes to the process and configuration of the facility. There are several approaches to decisions concerning risk reduction measures. These approaches include subjective, code-based, risk improvement, risk criteria, and cost-benefit. API publications 340 and 353 and *UK HSE Safety and environmental standards for fuel storage sites – Appendix 2 Guidance on the application of layer of protection analysis (LOPA) to the overflow of an atmospheric storage tank* provide additional guidance regarding risk assessment and selection of risk reduction measures.

This may be accomplished by a change of operating characteristic (i.e. receipt flow rates), by a change of operating procedures and practices (i.e. attendance), facility design and/or alarms, automation of systems through the transporter or facility owner, or other changes.

Special consideration should be given to certain types of installations to ensure that the High-High (HH) tank level alarms meet the expectations of the system as it is operated, e.g. if tanks being operated in parallel, are of different height or elevation, then one tank may be “full” (reached its overfill level) before the other(s).

When evaluating the risk associated with storage tank overfill, an operator that has only a few tanks at a single site, may complete a relatively straight forward approach requiring limited resources. However, if the operator has multiple storage tanks at multiple sites, then a more strategic and complex approach may be needed to prioritize resource allocation and implementation of any risk reduction measures. Moreover, if the operator wants to accomplish additional management objectives such as complying with this edition of API 2350 within a specific period of time, then a strategy where tanks are ranked and prioritized based on hazards may be essential so that a multi-year implementation plan is feasible

When evaluating the effectiveness of these procedures that support OPS, an understanding of the design, inspection, testing, and maintenance of the level instruments that support the above procedures is important.

Risk management resources addressing tank overfills can be found in API Publication 353, Managing the Risk of Liquid Petroleum Releases, and provides a conceptual overview of risk assessment elements. For greater discussion on risk assessment options, see API 353 and other references in the Bibliography.

The risk assessment approach may require consideration of:

- The internal and external expertise and qualification of the risk assessment team
- The availability of resources
- The corporate and stakeholder values
- Risk levels and impacts of interest
- Risk reduction costs
- Time required to reduce risks to acceptable levels
- The risk assessment methodology

A risk assessment strategy will depend on level of accuracy and precision needed to help make decisions. For example, risks associated with equipment or facilities that are lower risk may utilize a qualitative risk assessment that requires less time, whereas risk assessments for equipment or facilities that have substantial risks may require more sophisticated and advanced methods to improve the accuracy and precision. API 353, Managing

the Risk of Liquid Petroleum Releases and Integrity of Terminal and Tank Facilities, provides useful guidance.

The resources and time required to perform risk assessments will vary depending on a number of factors, including:

- Type of analysis (qualitative or semi-quantitative)
- Implementation strategy/plans
- Knowledge and training of risk facilitators
- Availability and quality of data and information
- Availability and cost of resources
- Complexity of processes and equipment
- Degree of accuracy desired
- Methodologies used

E.2 Risk Screening

In a complex operating environment, not everything can be assessed or measured at the same time; data collection, evaluations, and risk assessments have to be prioritized. It is obvious that the most effective approach would be to assess the higher risk storage tanks first, but site-specific conditions and external constraints will need to be considered when determining the overall pace of the assessments. Prioritizing the studies through a risk screening process is the quickest way to organize and conduct the required assessments, studies, and actions that need to be taken.

If the risk assessment covers multiple tanks at many facilities representing different levels of risk, then a risk screening activity may assist with prioritizing and focusing resources on the highest risks first. Screening can point out areas that are higher in priority and suggest which facilities or operating equipment merit first consideration and resources. It also provides insight about the type and effort of assessment that may be required for equipment at different facilities. Priorities may be assigned based on any of the following:

- Relative risk of the equipment
- Relative economic impact of loss of the equipment
- Relative consequence of failure from the equipment
- Relative reliability of the procedures and equipment
- Experience with similar equipment in similar service conditions

It is often advantageous to group equipment within a facility into similar categories where there are common filling characteristics and operations, e.g. stored product, operating temperature, equipment design, operating history, environmental consequences. By dividing a number of tanks into common operations, the equipment can be screened together and time can be saved by not treating each piece of equipment separately.

The bibliography provides numerous references that provide a framework for the study of risk assessment. The intent of this annex is not to influence the nature or method of executing risk assessments but to serve as an example of one way to implement a risk screening process.

A “first pass” screening of risks based on organizational objectives can provide more efficiency in risk assessment by focusing data collection and analysis on those tanks that provide the greatest threats to the organization’s objectives. Once the higher risk tanks are identified, then more precise risk assessment methods can be deployed to support risk management decisions. For example, a first pass analysis might separate storage tanks storing Class I liquids from those storing class 2 or 3 liquids if the risk of fires is the most important risk to reduce initially.

E.3 Qualitative Risk Assessment

E.3.1 Generally, a qualitative analysis using broad ranges requires a higher level of judgment, skill, and understanding from the user than a semi-quantitative approach. Ranges and summary fields may be evaluated for circumstances with widely varying conditions that require the user to carefully consider the impact of input on risk results. The accuracy of results from a qualitative analysis depends on the background and expertise of the analyst. Consequently, despite the approach's simplicity, it is important to have knowledgeable and skilled persons in the operations and others in risk assessment perform the qualitative risk assessment analysis.

E.3.2 As mentioned, the qualitative approach typically does not require all of the data required of a quantitative risk assessment method. Furthermore, items required are typically categorized only into broad ranges or classified based on a reference point. It is important to establish a set of rules to assure consistency in categorization or classification. One way in which risk can be represented is in qualitative terms, such as low, medium, or high. The qualitative assessments of likelihood and consequence can be assigned to risk categories with these values displayed in a risk matrix.

E.3.3 Risk matrices are a common tool often used to summarize risks on a relative basis and serves as a means to evaluate risks and assist with making risk management decisions. Risk matrices provide a graphical presentation of risks typically in terms of likelihood or probability and consequence or impact to the organization. The potential risks (a tank loss of containment, for example) are typically shown as individual spots, typically representing the highest risk associate for each tank. The rows and columns for risk cells on the matrix that are translated into different risk categories. API documents provide guidance on risk assessments that use risk matrices including API Publication 353 and 580. Figure E.1 is a risk matrix example from API 353.

E.3.4 There are a number of storage tank attributes that can impact the consequence of an overfill. Some of these attributes to consider include the rate of a potential overfill, handling of flammable liquids, ability to contain a spill such as individually diked tanks versus common containment, soil conditions and/or liner in the containment system with the ability to hold liquids, location to public areas including residences and roadways, location of occupied buildings to the storage tank, location of ignition sources, fire protection facilities to minimize vapor generation or extinguish fires, and location of waterways to the storage area.

E.3.5 After completion of the risk analysis, the results are reviewed with the risk manager(s) to begin management of the risk. Risk management decisions need to evaluate many factors include those developed during the risk assessment to identify the best risk reduction options including those impacts to communities and resource allocation. Decision analysis should consider:

- Significance of the risk,
- Risks that may lead to different outcomes,
- Effectiveness of the potential risk reduction measures, and
- Further action to be taken to reduce the risk to an acceptable level.

	CONSEQUENCE								
	First Aid	Minor Injury	Injury w/ hospital stay	Severe Injury	Fatality				
	No Public Impact	First Aid to Public	Minor Injury to Public	Injury w/hospital stay to public	Severe Injury to Public				
	No Significant Cleanup	Minor Cleanup (Onsite)	Moderate Cleanup (Onsite)	Major Cleanup (Offsite)	Severe Cleanup (Offsite)				
	Not Significant	**Minor**	**Moderate**	**Major**	**Severe**				
5	**Higher –**	**Medium**	**Risk**	**Higher**	**Risk**	**Almost Certain**	Expected to occur more often than once per year	≥0.1	**PROBABILITY**
4						**Likely**	Expected to occur once every 10 years	≤0.1	
3						**Possible**	Expected to occur once every 100 years	≤0.01	
2	**Lower**	**Risk**	**Medium**	**Risk**		**Not Likely to Occur**	Expected to occur once every 10 years at 100 similar sites	≤0.001	
1						**Impractical**	Expected to occur once at 100 years at 100 similar sites	≤0.0001	
	A	**B**	**C**	**D**	**E**				

Figure E-1
Risk Matrix Example from API 353
Note to API: Would the use of other colors be easier to differentiate?

E.3.6 Considerable judgment is involved in this activity since the risk reduction benefits and cost effectiveness of some potential risk reduction measures may be difficult to quantify. The potential benefits of risk reduction measures must also be evaluated against potential implementation risks.

E.4 Semi-Quantitative Risk Assessment

E.4.1 Semi-quantitative risk assessment is a methodology that uses relevant information about facility design, operating practices, operating experience, equipment reliability, and human actions to determine the likelihood and consequences of a risk scenario. Semi-quantitative risk analysis typically uses logic models (event and fault trees) to depict the combination of events that could result in harm to personnel, public, facilities and/or the environment (see event tree model in Figure E-2). The models provide a systematic method of evaluating potential hazards present at the facility being studied by developing incident scenarios based on these hazards along with different mitigation measures that could be implemented, assessing the numerical likelihood that each scenario can occur, and using mathematical models to predict the impacts if a scenario does occur.

E.4.2 The models are evaluated probabilistically to provide both qualitative and semi-quantitative insights about the level of risk and to identify the site, design, and operational characteristics that are the most important to manage the risk; hence, more detailed information and data are needed for semi-quantitative risk assessment

to provide input for the models. Semi-quantitative risk analysis is distinguished from the qualitative approach by the depth of the analysis and quantification of the probabilities.

E.4.3 Semi-quantitative risk assessment logic models generally consist of an organized methodological approach such as event tree and fault tree types of analysis. Event trees delineate by starting with an initiating event(s) that are combined with probability factors/safeguards/events of successes and failures that lead to an outcome/consequence, while fault trees begin with the failure or outcome and builds backwards to understand the different characteristics that can lead to the failure. These models are used to estimate the likelihood of scenario and the sequence of events included in the scenario. Results using this approach are typically presented as risk (likelihood and consequence) and are either plotted on a risk matrix or risk curve.

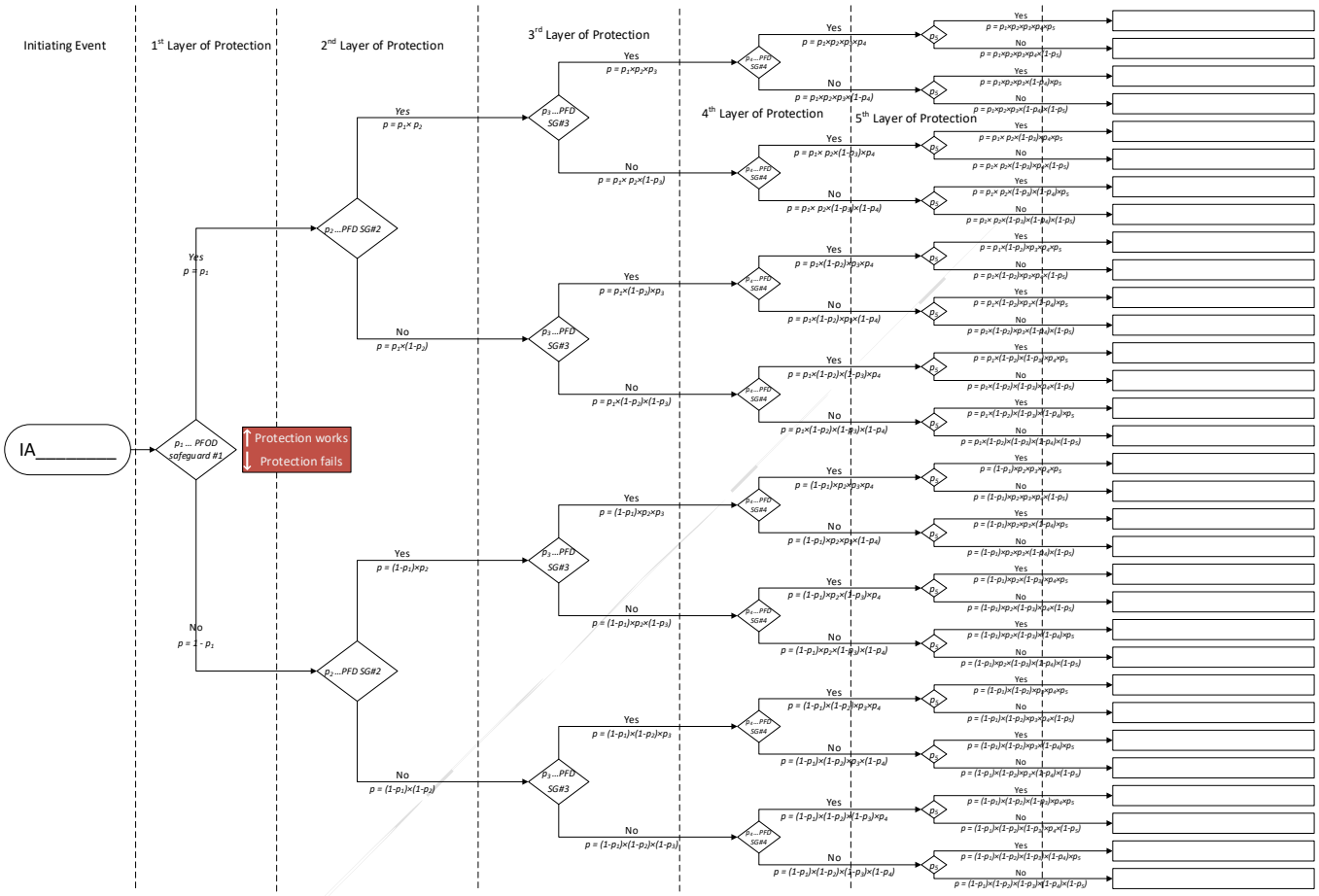


Figure E-2
Event Tree Model

E.5 Supplemental Risk Reduction Examples

To improve the effectiveness of existing risk reduction measures, supplemental facilities and/or procedures can be implemented. Examples of risk reduction measures include the following:

E.5.1 The valve lineup is verified by a second operator at a different time than the initial operator. (High level alarms on other tanks would not be considered as providing additional risk reduction for this aspect of the procedure.)

E.5.2 Reduced time intervals are implemented to verify the tank ATG is operating by comparing to the metered flow measurement.

E.5.3 Facilities and/or procedure are provided for the transporter is independently monitoring the delivered flow rate/volume and will stop the flow at the prearranged time/volume even if communication is lost. Transporter stopping on a loss of communication would be sufficient for this risk reduction.

E.5.4 More than one independent level gauge and the readings are compared for consistency and action is taken when readings vary by more than some indicator of a gauge malfunction. The difference can be a range such as ½% of full scale or some reasonable basis depending on the actual gauging equipment.

E.5.5 Owner/Operator is continuously engaged and there are not multiple filling operations conducted simultaneously. This could be measured by the maximum number of active tanks, valves to be operated, or site conditions (e.g. size, degree of automation).

E.5.6 Fitting a high integrity, automat operating overfill prevention system that is physically and electrically separate and independent from the tank gauging system, with a required reliability determined by a suitable risk assessment.

E.6 Example

Company 'A' has decided to develop risk screening criteria and follow a qualitative risk assessment method when evaluating their tanks. If the storage tanks and operating procedures meet the risk screening guidance, a team to complete a more detailed qualitative risk assessment is not required. The risk screening guidance outlines instrumentation arrangements, attendance and monitoring criteria based on the consequence expected from a release, spill and ignition for flammable materials.

The risk matrix was developed by the company to apply at the operating sites. The risk matrix will be used for tanks that do not meet the risk screening criteria. The risk matrix has been divided into four risk categories and are providing guidance that the risk with mitigation should be considered lower risk or medium risk with sign-off by site management accepting the risk.

To apply the risk screening guidance, the following assumptions were made for this example: 1) overfill prevention procedures identified in chapter 4 are undertaken, 2) from tanks have adequate secondary containment sized for 100% containment, 3) containment system are at least 500 feet from third-party buildings and major roadways (dispersion model defined), and 4) the containment system is impervious.

Risk Screening Example

Product	Receipt	Fill Rate	Instrumentation	Attendance	Monitoring
Flammable Liquids	Pipeline	>440 gpm	Category 3	Semi-Attended	Attendance continuously during the first 30 minutes of receipt; hourly checks afterwards then continuous monitoring during the last 30 minutes
Flammable Liquids	Marine	>440 gpm	Category 2 plus flow meter and continuous monitoring	Semi-Attended	Attendance continuously during the first 30 minutes of receipt; hourly checks afterwards then continuous monitoring during the last 30 minutes
Flammable Liquids	Any	<440 gpm	Category 2	Semi-Attended	Attendance continuously during the first 30 minutes of receipt; hourly checks afterwards then continuous monitoring during the last 30 minutes

Combustible Liquids FP 100 – 140°F	Any	Any	Category 2	Semi-Attended	Attendance continuously during the first 30 minutes of receipt; hourly checks afterwards then continuous monitoring during the last 30 minutes
Combustible Liquids FP >140°F	Any	Any	Category 1	Semi-Attended	Attendance continuously during the first 30 minutes of receipt; hourly checks afterwards then continuous monitoring during the last 30 minutes

E.6.1 One of the gasoline storage tanks does not meet Category 3 in this example and does not meet the initial risk screening criteria (fill rate exceeds 440 gpm) and, as a result, a detailed assessment is being completed. The overfill scenario for the storage tank receives gasoline product once a week (or ~52 times a year).

The shipment will be split between tanks; each 90-foot diameter by 45-foot high storage tanks via a pipeline receipt with a fill rate of 1,000 barrels per hour (~700 gpm). The tank is contained in a 145-foot by 145-foot containment dike sized to contain 100% of the tank's contents and constructed of impervious clay. The tank containment is located less than 500 feet away from the fence line where there are commercial buildings.

E.6.2 The tank is equipped with a float and tape level instrument that is monitored at the tank and in the control room. A field operator is assigned to monitor the tank operation via the field gauge and will intervene when the maximum operating level is reached. There is no second instrument for the High-High (HH) level alarm. The float and tape instrument has been hanging up such that the availability of the instrumentation is at 90%. In this example, the initiating event is determined to be the ATG.

E.6.3 There has not been a tank overfill at the terminal during the last 20 years. As a benchmark, the terminal where 5 tanks are operated, there is 100 tank operating years without an overfill. The terminal has good Pre-Planning, Tank Filling and Post-Receipt procedures (section 4.5) such that failures in the procedures are estimated to be 0.001 per fill. The response to the High Level Alarm associated with the ATG reduces the probability further as does the likelihood of ignition. The scenario is estimated to be Not Likely to Occur.

E.6.4 If the tank were to overfill, fatalities may occur as far as 1,300 ft due to overpressure or thermal effects (due to formation of large flammable cloud and subsequent explosion), especially to exposed persons not within a protective building specifically designed to withstand this kind of event and cleanup is defined as a moderate cleanup which results in Moderate Consequence. If the vapors from the spill would ignite, there is the potential for the field operator to be severely injured and potential for some in the public to suffer a minor injury. Or, fatalities could occur both onsite and offsite. In addition, there is potential for a major accident to the environment (e.g. if the rainwater drain valves in the containment dike are mistakenly left open. Therefore, the consequence is considered Severe.

As frequency mitigation apply Independent High-High level alarm, annunciated in the control room, with operator response to terminate pipeline receipt within 30 minutes. It is assumed that this alarm layer reduces the risk by one order of magnitude.

Added frequency mitigation: Probability of calm and stable weather is 10%, based on 2009 – 2018 hourly average data from local Met Office station. Hence, conditional modifier of 10% can be applied.

E.6.5 The risk assessment team's conclusion is that the risk is a Higher - Medium Risk based on the risk matrix and the team recommends fitting an overfill protection system to reduce the risk by one order of magnitude.

Annex F
(informative)

Transporter/Owner/Operator Interface

F.1 Scope

API 2350 and its annexes are generally written around hazards and procedures related to tank filling operations. Due to a variety of different business arrangements, there often exists an arrangement where an operator of a pipeline, marine vessel or other system of inbound product movement delivers to facility tankage operated by another operator. The purpose of this annex is to provide examples, best practice and vulnerabilities for some of these types of situations.

F.2 Types of Pipeline Third Party Operations

F.2.1 Delivery to a Third Party Facility via Pipeline

As shown in Figure F.1, in certain circumstances, facility tankage can be operated by one organization, and the inbound pipeline operated by another organization as a third party. In many cases, a pipeline operator is contracted to manage delivery into a truck terminal, marine terminal, rail terminal, military base, rail road station, chemical manufacturing plants, farm co-ops or other types of businesses. To follow this standard, it is important for them to understand the issues relating to tank overfill within an appropriately designed secondary containment unit and what must be done to terminate an inbound product movement without transferring the danger of a release outside of secondary containment.

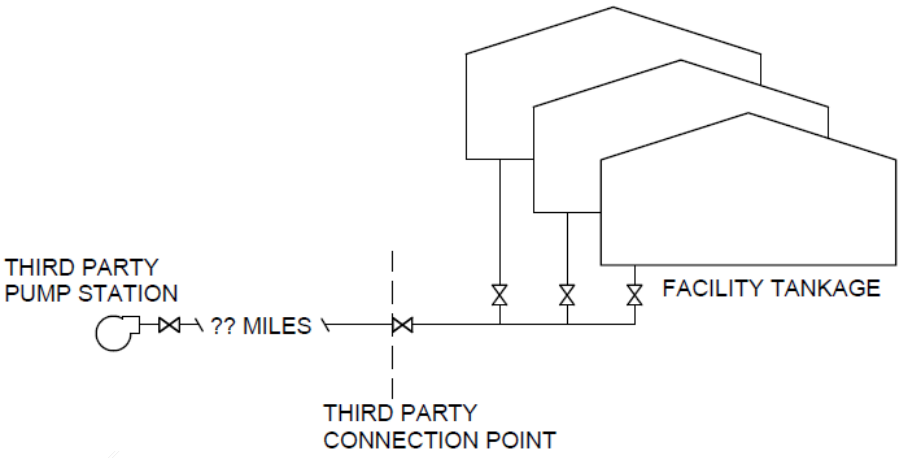


Figure F.1

For either facility or pipeline operator, the originating pump could be miles from the facility and significant engineering design must occur to properly size pumps and product lines. Typically starting up a pump against a closed valve at a facility, or a valve closing during inbound movement can cause significant problems. In some instances, both operators may have instrumentation that manage and communicate data from one to the other. In other instances, one or both operators may not have any controls at the delivery point, and as such may not have ability to supply a data interface. For these reasons, Automatic Overfill Prevention Systems may not simply close a valve within the facility, unless appropriate engineering steps (such as surge analysis) have been taken and the pipeline operator agrees to the design. Otherwise a designed, controlled shutdown of the incoming pipeline is required.

F.2.2 Multiple Concurrent Third Party Operations

As shown in figure F.2, some tankage receives product from a pipeline operated by a separate operator, who may be receiving product into their pipeline system from yet another operator. In this situation, an originating station may

have a pump supplying product to a pipeline that is subsequently pushing product, possibly by use of booster pumps, into some other party's tankage.

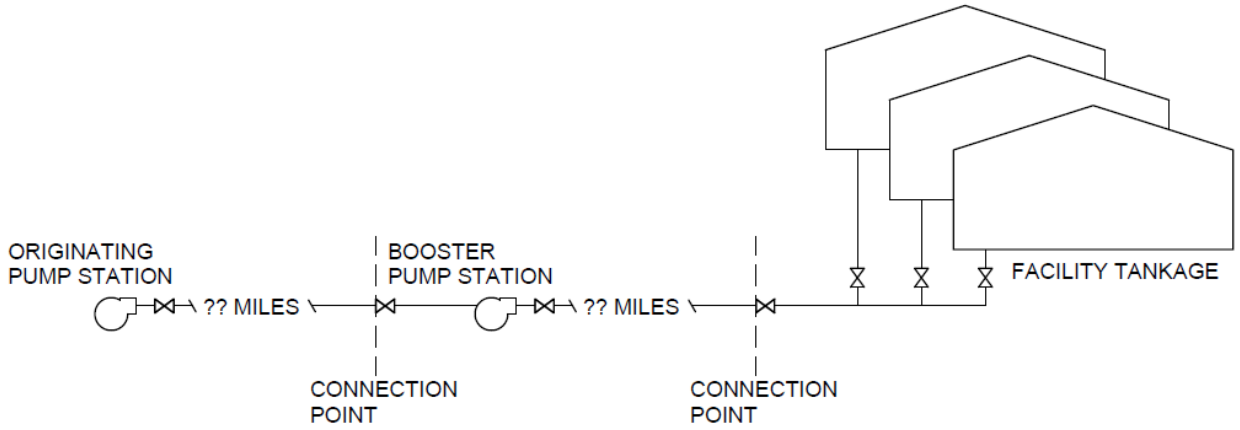


Figure F.2

F.2.3 Marine Inbound Operations

Some tankage receives product directly from marine vessels such as barges and ships. These vessels typically have their own engine-driven pumps that are operated by individuals qualified to operate marine vessels. Typically the tank operator will provide operations personnel at the dock for interface with the individuals operating the marine vessel. Also, personnel hired by both onshore and marine vessel operator may be on-call for liquid level measurement.

Alarms from tank levels may or may not be available at the dock. For the same reasons discussed in section F.2.1, Automatic Overfill Prevention Systems may not simply close a valve within the facility against an inbound movement, unless appropriate engineering steps have been taken and the vessel operator agrees to the design. Otherwise a designed, controlled shutdown of the incoming product movement is required. Local standard operating procedures should be developed for managing these movements and should outline what form of communication between parties is required.

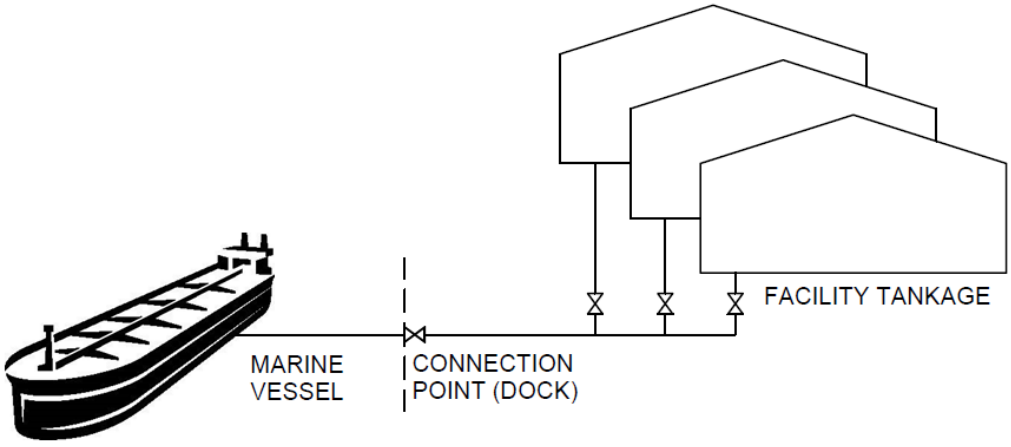


Figure F.3

F.3 Connection Arrangements

F.3.1 Connection Agreement

These types of arrangements can typically be managed by a "connection agreement". This legal agreement can include information on who owns which assets specifically, how operations are to occur on a routine basis, who is

responsible for maintenance, site access arrangements, what type of routine communication should occur between parties and limits of responsibility. The communication may be by phone conversation between control center operations personnel, data transfer between control systems, or other.

Typical operation within these agreements requires a formal request for product be transferred from the operator of the storage tank to the operator of the inbound pipeline or vessel. This provides a paper trail with respect to room available in destination storage tank and quantity of product due into the site.

F.3.2 Data Transfer Between Parties

High level alarm information can be passed between two operators in a variety of ways. Typically, two sites may be connected by radio modem or hardwire as shown in figure F.4.

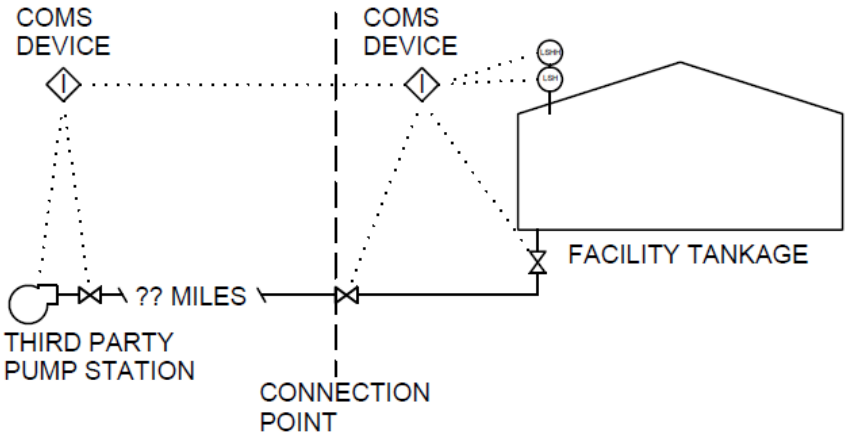


Figure F.4

Most sites will have two programmable logic controllers (or similar device used for communications), one belonging to each operator. These units can have registers that can be coordinated between operators to pass back and forth particular data. Tank level gauge readings and high level alarms are amongst this data that can be transmitted from the tank site to the pipeline. In some situations, there can only be a limited number of points transmitted, or when additional information is not desired by the shipping pipeline, rather than each tank high alarm status or the fill information, a tank-high signal, a tank High-High (HH) signal, or simple shut down command may be the only pieces of information transmitted.

Alarm systems being transmitted from tank operator to inbound pipeline or vessel operator should be monitored by personnel where possible. These personnel may be in a control center for the pipeline or at a local site near the delivery point.

SCADA and Control Center methodologies may vary between operators. Some may prefer to see specific data, such as tank high level alarms, rather than a shut-down request. Each operator must determine their methodology for control and may or may not automatically shut down. Many control centers are staffed 24/7 and these facilities have capability of shutting down based on human interface with alarms, when not automatic. Depending on the source of the product and source of the subsequent batches already in the line, shutdown sequences could vary.

The tank facility should establish operating procedures governing response to the alarms generated by their system, and those procedures should be communicated to and agreed upon with the pipeline operator. The tank facility should also perform routine maintenance of their alarm system and during that maintenance should notify the pipeline operator of scheduled maintenance so the pipeline operator can respond to alarms appropriately.

Annex G
(normative, if used)

Tank Categories

G.1 Scope

API 2350 and its annexes provide different methods to consider for overfill prevention. One method presented in earlier editions of API 2350 assigned tank categories and applied different levels of prevention based on the complexity of the facility and the monitoring and manpower available. The purpose of this annex is to provide examples of types of categories and the overfill prevention dictated by those groupings.

G.2 Categories

Tank categories are a convenient classification system that illustrate the most common combination of monitoring & attendance and instrumentation. Categorizing tanks make communicating the fundamental features and attributes of the tank overfill system configuration more manageable. Figure G1 provides illustrations of the four categories that are described in the following sections.

Prior to starting product transfer to fully- or semi-attended facilities, communications between the transporter and the facility Owner/Operator should be tested. Communications frequency between the facility Owner/Operator and the transporter should be agreed upon and maintained throughout the transfer. The lower the category level, the more frequent the communications should be. For example:

— Category 0 and 1, the parties may communicate at least once at start of receipt, periodically during the receipt, and once within one hour prior to the end of receipt; but

— Category 2 and 3, the parties should communicate at the start and end of a receipt, additional communication, as agreed upon.

Table G 1— Tank Categories

Categories-> Minimum LOC Response Times ->	**Category 0 Tanks 60 Minutes**	**Category 1 Tanks 45 Minutes**	**Category 2 Tanks 30 Minutes**	**Category 3 Tanks 15 Minutes**
Attendance at facility	Fully Attended	Fully Attended	Semi-Attended or better	Unattended or better
Instrumentation	No automatic tank gauges	Single Level Instrument (Side Gauge or ATG)	*Single Level Instrument*	*Two independent level instruments (ATG monitored and Independent High-High (HH) Level Alarm)*
Alarm System	Local Monitoring or None	Local Monitoring Only – No Alarm	Alarms sent to continuously occupied location	Levels and independent alarms sent to continuously occupied remote site.

Monitoring	Locally monitored, 1. Attendance continuously during first hour of receipt. 2. Then hourly ~~periodically~~ during receipt per procedure. 3. Attendance continuously during the last hour of receipt.	1. Attendance continuously during first hour of receipt. 2. Then every hour during receipt. 3. Attendance continuously during the last hour of receipt.	1. Attendance continuously during the first 30 minutes of receipt. 2. Hourly not applicable. 3. Attendance continuously during the last 30 minutes of receipt.	No local monitoring requirements. For unattended facilities, continuous monitoring during receipt by the operator, transporter or by computer.

Tank categories may be changed by the Owner/Operators whenever it is operationally convenient to do so or is an appropriate change to reduce risk, as long as the requirements of this section are considered.

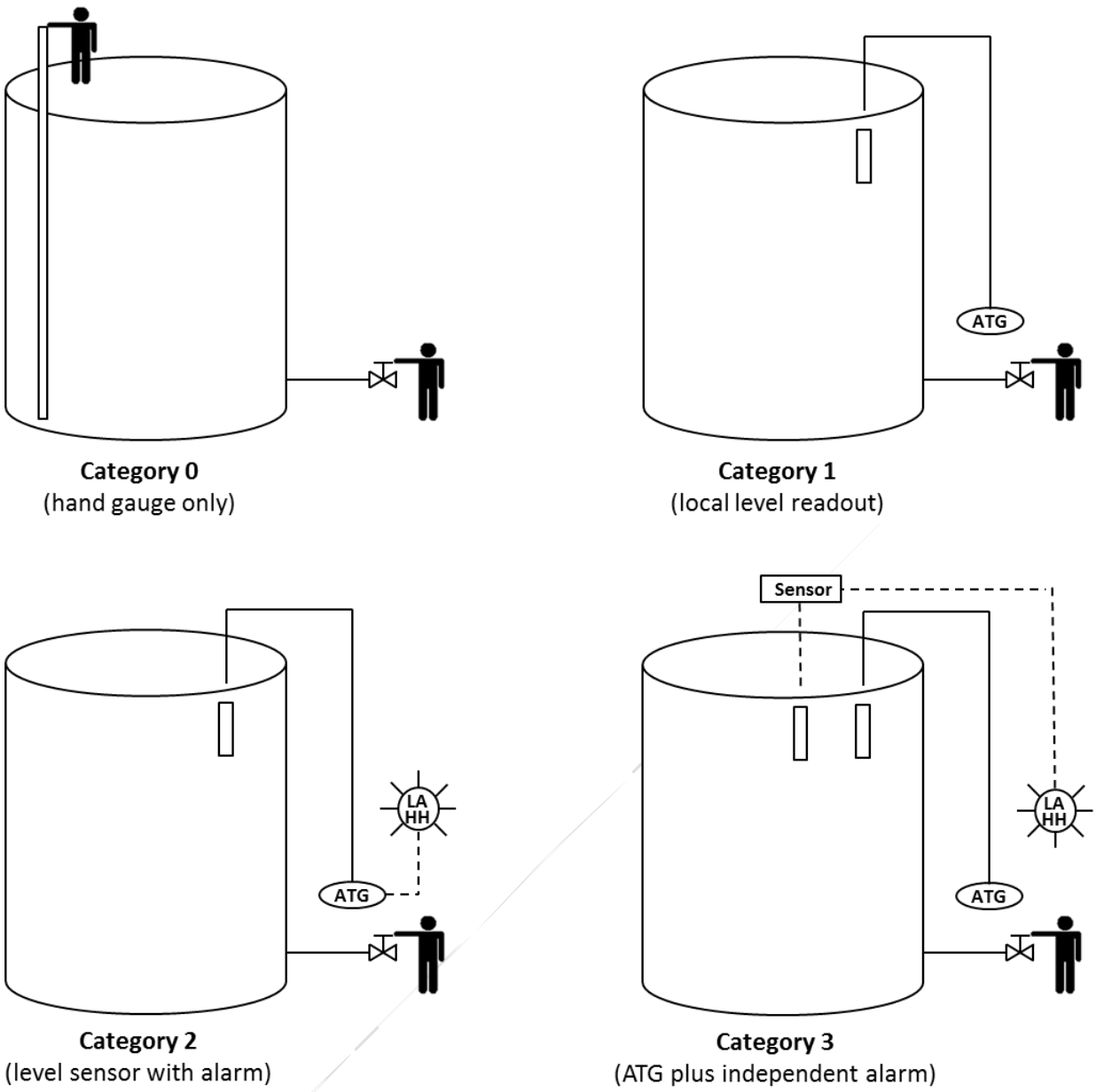


Figure G1—Illustration of Categories Applied to Overfill Prevention Systems

~~Note to API: Remove person manually operating valve in Category 3.~~

G.2.1 Category 0 Tank

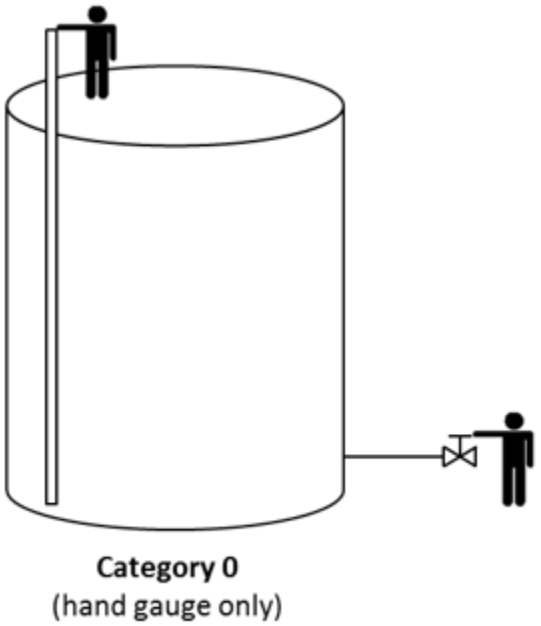


Figure G2 – Illustration of Category 0

G.2.2 Category 0 Instrumentation

Category 0 tanks has no automatic tank gauge available to monitor movements during receipts. Safety considerations may prohibit hand gauging during product receipt and for 30 minutes after filling is complete (See API 2003 on static.) The only overfill prevention in a category 0 system comes from planning receipts less than the available volume.

G.2.2.1 Category 0 Attendance: Fully-Attended

Category 0 tanks shall be fully-attended during receipts.

G.2.2.2 Category 0 Monitoring: Locally Monitored

Category 0 tanks shall be operated as a locally-monitored facility for receipts with monitoring continuously during the first hour of receipt, every hour during the receipt, and continuously during the last hour of the receipt. As indicated in Table G.1, there are no remote monitoring capabilities by the transporter for either alarm or level information.

G.2.3 Category 1

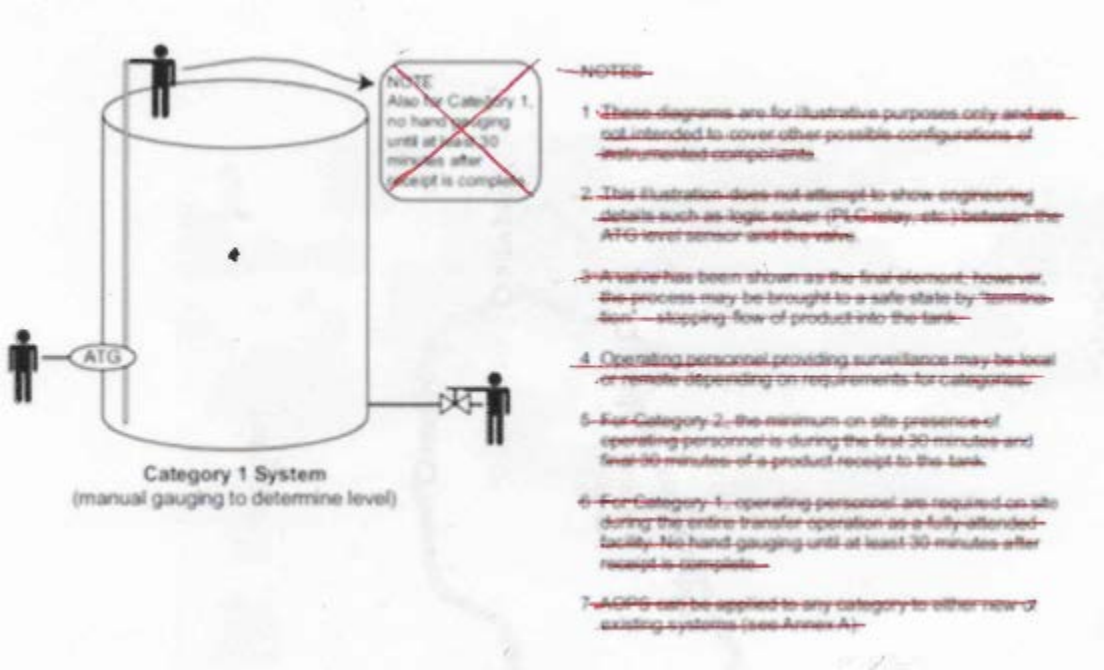


Figure G3 – Illustration of Category 1 Overfill Prevention Systems

G.2.3.1 Category 1 Instrumentation: Local Gauging Equipment

Category 1 tanks require a local level instrument, e.g. level gauge or automatic tank gauge that has a local display or read out. Typically, level data and alarms are local to the tank or the facility and are not transmittable to the transporter. If receipt termination is required, it is likely done manually by attending operating personnel or by the transporter after receiving communications from attending personnel.

G.2.3.2 Category 1 Attendance: Fully Attended

Category 1 tanks shall be fully-attended. Assigned personnel are on the premises continuously during the entire product receipt. Personnel on site either have the ability to terminate the receipt are in constant contact with people who have the ability to terminate the receipt. Safety considerations may prohibit hand gauging during product receipt and 30 minutes after completion (see API 2003).

G.2.3.3 Category 1 Monitoring: Locally-monitored

Category 1 tanks shall be operated as a locally-monitored facility for receipts with monitoring continuously during the first hour of receipt, every hour during the receipt, and continuously during the last hour of the receipt. As indicated in Table G.1, there are typically no remote monitoring capabilities by the transporter for either alarm or level information.

Category 1 should not be used where the operator cannot reasonably be expected to focus fully on termination of the receipt or may be distracted with other duties or responsibilities. Sites where distractions can occur are those where there are frequent receipts or the facility or terminal has complex operations. Addition of an AOPS and/or upgrade to category 2 or 3 tanks should be considered where the risk does not meet the Owner/Operator risk criteria.

G.2.4 Category 2

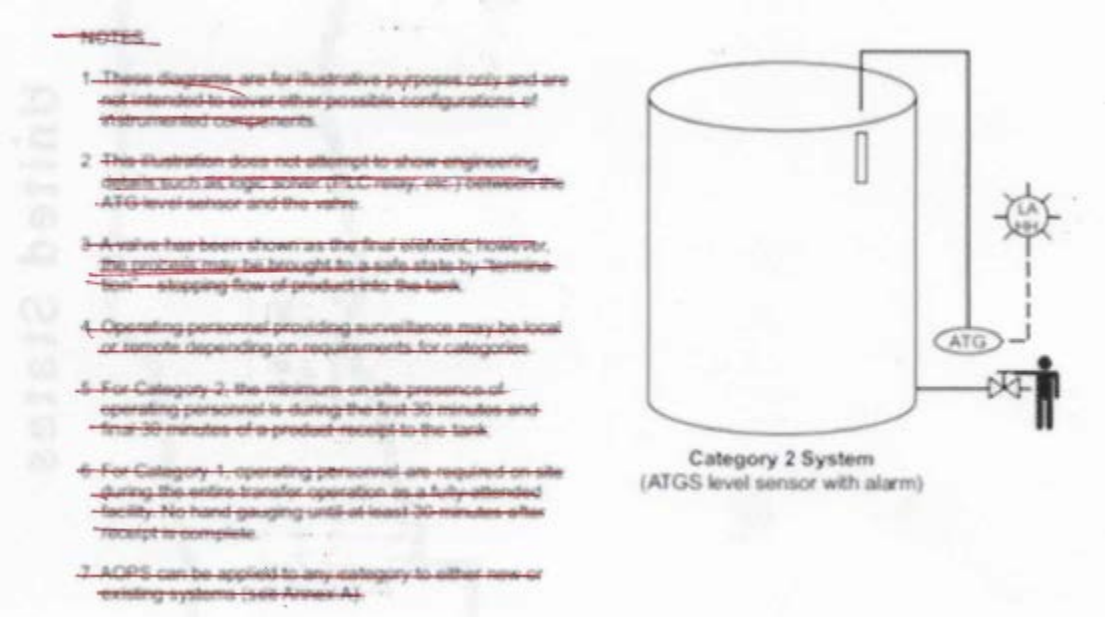


Figure G4 – Illustration of Category 2 Applied to Overfill Prevention Systems

G.2.4.1 Category 2 Instrumentation: Automatic Tank Gauge with Level Transmission to Control Center

Category 2 tanks have an automatic tank gauge system with levels that are transmittable to a local or remote control center. Tanks may use the same instrument for level, high, and the HH level alarm. This transmission of alarm data to a control center is a key difference between Category 1 and Category 2 tanks. The lack of independence of the level measuring system and the alarm system is the fundamental difference in terms of level indication and alarm function reliability.

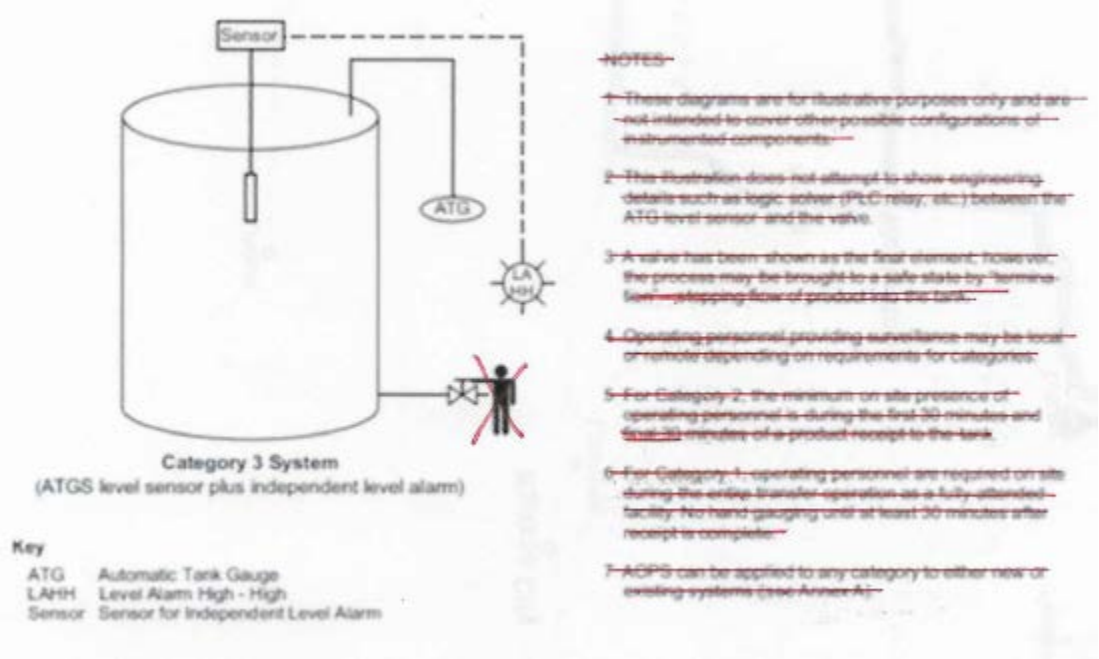
G.2.4.2 Category 2 Attendance: Semi-Attended

Category 2 tanks shall be operated as semi-attended or fully-attended tanks. At a minimum, personnel shall be at the facility with tanks at the first and last 30 minutes of a receipt and transfer operation (start denoted by the flow of product, last denoted by termination of flow.)

G.2.4.3 Category 2 Monitoring: Transitionally-Monitored

Category 2 tanks shall be capable of being remotely monitored. At a minimum, transfer and automatic tank gauge data are monitored by a control center that is attended when the tank is active, i.e. flow into or out of the tank. The transporter is required to assist with monitoring the receipts via the HH level alarms and shall be in communication with operating personnel responsible for the receiving tank. The operating personnel monitoring the system shall have the ability to terminate the transfer.

G2.5 Category 3



~~NOTES~~

~~1 These diagrams are for illustrative purposes only and are not intended to cover other possible configurations of instrumented components.~~

~~2 The illustration does not attempt to show engineering details such as logic solver (PLC relay, etc.) between the ATG level sensor and the valve.~~

~~3 A valve has been shown as the final element; however the process may be brought to a safe state by "terminating/stopping flow of product into the tank.~~

~~4 Operating personnel providing surveillance may be local or remote depending on requirements for categories.~~

~~5 For Category 2, the minimum on site presence of operating personnel is during the first 30 minutes and final 30 minutes of a product receipt to the tank.~~

~~6 For Category 1, operating personnel are required on site during the entire transfer operation as a fully attended facility. No hand gauging until at least 30 minutes after receipt is complete.~~

~~7 AOPS can be applied to any category to either new or existing systems (see Annex A).~~

Figure G5 – Illustration of Category 3 Applied to Overfill Prevention Systems

G.2.5.1 Category 3 Instrumentation: Automatic Tank Gauge with Level Transmission to Control Center

Category 3 tanks uses both an automatic tank gauge and an independent level alarm High-High sensor (LAHH). If a high alarm is used, then it shall be independent of the level measuring system. If a high level alarm is used it is not required that there be two independent sensors for each of the high and the HH levels. The key difference between Category 2 and Category 3 is that the LAHH sensor is independent of the automatic tank gauge and alarm data is transmitted to a control center (with transmission of level data as determined by facility and shipper agreed protocols).

The independent LAHH instrument (either a point level or continuous level device) may be connected to the common automatic tank gauge may be connected to a second ATG ~~and~~ if it is electrically supervised and ~~provides~~ providing diagnostic alarms to the transporter.

G.2.5.2 Category 3 Attendance: Unattended

Category 3 tanks may be unattended. Personnel are not required to be on the premises during any part of a receipt or transfer.

Tanks at unattended facilities shall be equipped with systems that automatically terminate the receipt or activate an alarm with the personnel (potentially the transporter) that have the ability and adequate response time to initiate termination procedures. These systems shall also initiate receipt termination procedures in the event of a power failure in the level measuring system.

G.2.5.3 Category 3 Monitoring: Remotely-Monitored

Category 3 tanks shall be remotely-monitored. The LAHH instrument data (and, if appropriate, the automatic tank gauge levels) shall be transmitted in real time to a control center that is manned 24 hours per day, seven days per week.

ANNEX H
(informative)

Proof Testing

H.1 Scope

API 2350 and its annexes provide different methods to consider for overfill prevention. Section 4.5.14 discusses the proof testing requirements. The purpose of this annex is to provide basic information on proof testing.

H.2 Proof Testing

H.2.1 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 prevention control system regardless of vintage.

H.2.2 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. Commonly used 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 is actually experience 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 generally ill advised for reasons discussed below.

H.2.3 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 generally 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.

H.2.4 But most overfill prevention instrument loops for tanks use the 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.

H.2.5 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 possibly 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 owners/operators consider this too hazardous to allow, especially where flammable liquids are involved.

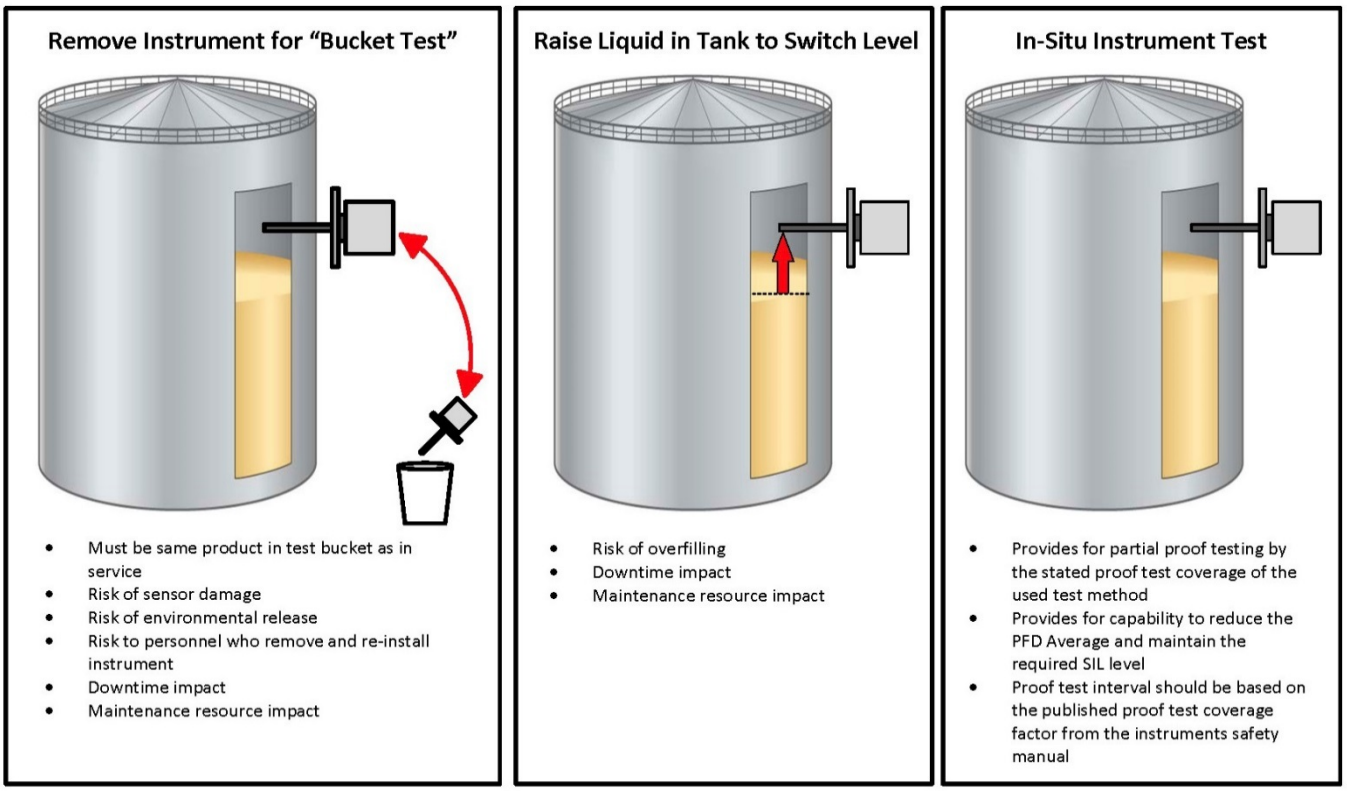
H.2.6 Another option is to set the liquid level sensor trip at a lower liquid level to test the alarm or final element operation. But this has a few problems as well. Changing the set point of the sensor introduces the distinct possibility that the correct original set point is not properly reset. In 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.

H.2.7 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 “unrevealed failure” 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 experts and manufacturers should be brought to the table to discuss these.

H.2.8 The problem with all “bucket tests” are that the sensor can damaged or lose its calibration and this type of failure will not be detected. Bucket tests mean that the sensor (level) is removed from its installation on the tank and the sensor immersed in product.

H.2.9 A comparison of the various modes of testing is shown below:



H.2.10 Proof testing is an important part of tank overfill prevention and it can be rather technical. Subject matter experts and the manufacturers should be consulted so that the proof testing procedures actually produce the desired results.

Bibliography

[1] API Manual of Petroleum Measurement Standards (American Petroleum Institute) 2.2A, *Measurement and Calibration of Upright Cylindrical Tanks by the Manual Tank Strapping Method*

[2] API Manual of Petroleum Measurement Standards (American Petroleum Institute) 2.2B, *Calibration of Upright Cylindrical Tanks Using the Optical Reference Line Method*

[3] API Manual of Petroleum Measurement Standards (American Petroleum Institute) 3.1A, *Manual of Petroleum Measurement Standards – Chapter 3: Tank Gauging, Section 1a – Standard Practice for the Manual Gauging of Petroleum and Petroleum Products, Section 1b -*

[4] API Publication 353, *Managing Systems Integrity of Terminal and Tank Facilities – Managing the Risk of Liquid Petroleum Releases*

[5] API Publication 2026, *Safe Access/Egress Involving Floating Roofs of Storage Tanks in Petroleum Service*

[6] API Recommended Practice 500, *Recommended Practice for Classification of Locations for Electrical Installations at Petroleum Facilities*

[7] API Recommended Practice 1165, *Recommended Practice for Pipeline SCADA Displays (January 2007)*

[8] API Recommended Practice 1168, *Pipeline Control Room Management 09/00/2008*

[9] API Recommended Practice 2003, *Protection Against Ignitions Arising Out of Static, Lightning, and Stray Currents*

[10] API Recommended Practice 2009, *Safe Welding, Cutting, and Hot Work Practices in the Petroleum and Petrochemical Industries*

[11] API Recommended Practice 2021, *Management of Atmospheric Storage Tank Fires*

[12] API Recommended Practice 2201, *Safe Hot Tapping Practices in the Petroleum and Petrochemical Industries*

[13] API Standard 620, *Design and Construction of Large, Welded, Low-pressure Storage Tanks*

[14] API Standard 650, *Welded Tanks for Oil Storage*

[15] API Standard 653, *Tank Inspection, Repair, Alteration, and Reconstruction*

[16] API Recommended Practice 1173, *Pipeline Safety Management Systems*

[17] API Standard 2545, *Method of Gauging Petroleum and Petroleum Products*

[18] API Standard 2610, *Design, Construction, Operation, Maintenance and Inspection of Terminal and Tank Facilities*

---

[1] American Institute of Chemical Engineers, Center for Chemical Process Safety, 3 Park Avenue, 19th Floor, New York, New York 10016, www.aiche.org/ccps.

[19] AIChE[1] Center for Chemical Process Safety (CCPS), *Guidelines for Hazard Evaluation Procedures, 3rd Edition*

[20] AIChE Center for Chemical Process Safety (CCPS), *Layer of Protection Analysis*

[21] AIChE Center for Chemical Process Safety (CCPS), *Simplified Process Risk Assessment*

[22] American Industrial Hygiene Association[2], ANSI/AIHA Z-10, *Occupational Health and Safety Management Systems (OHSMS)*

[23] American Society of Safety Engineers[3], ANSI/ASSE Z690.1-2011, *Vocabulary for Risk Management (identical national adoption of ISO Guide 73:2009)*

[24] American Society of Safety Engineers, ANSI/ASSE Z690.2-2011, *Risk Management – Principles and Guidelines (identical national adoption of ISO 31000:2009)*

[25] American Society of Safety Engineers, ANSI/ASSE Z690.3-2011, *Risk Assessment Techniques (identical national adoption of ISO 31010:2009)*

[26] BSI Group[4], BS OHSAS 18001:2007 (BSI 2007), *Occupational Health and Safety Management Systems – Requirements*

[27] International Electrotechnical Commission (IEC)[5], *IEC 61511 Functional Safety: Safety Instrumented Systems for the Process Industry Sector*

[28] International Society of Automation (ISA)[6], ANSI/ISA 84.00.01-2004 (IEC 61511 modified), *Functional Safety: Safety Instrumented Systems for the Process Industry Sector*

[29] International Society of Automation (ISA) TR84.00.08 Guidance for Application of Wireless Sensor Technology to Non-SIS Independent Protection Layers

[30] International Society of Automation (ISA), ANSI/ISA S84.01 – 1996 – ISA TECH 1999, *The Treatment of Existing Systems,* Angela E. Summers, Kimberly A. Dejmek

[31] International Standards Organization[7], IEC/ISO 31010:2010, *Risk Management, Risk Assessment Techniques*

[32] International Standards Organization, *The Integrated Use of Management System Standards – 2008*

[33] McGraw-Hill[8], *Dictionary of scientific and technical terms (4th ed.). Parker, S. P. (Ed.). (1989)*

[34] McGraw-Hill, ISBN: 007044272X, *Aboveground Storage Tanks by Phillip E. Myers*

---

2 American Industrial Hygiene Association, 2700 Prosperity Ave., Suite 250, Fairfax, Virginia 22031, (Tel.) 703-849-8888, (Fax) 703-207-3561, www.aiha.org.

3 American Society of Safety Engineers, 1800 East Oakton Street, Des Plaines, Illinois 60018, www.asse.org.

4 BSI Group, 389 Chiswick High Road, London, W4 4AL, United Kingdom, www.bsigroup.com/en/.

5 International Electrotechnical Commission, 3, rue de Varembé, P.O. Box 131, CH-1211, Geneva 20, Switzerland, www.iec.ch.

6 The Instrumentation, Systems, and Automation Society, 67 Alexander Drive, Research Triangle Park, North Carolina, 22709, www.isa.org.

7 International Organization for Standardization, 1, ch. de la Voie-Creuse, Case postale 56, CH-1211, Geneva 20, Switzerland, www.iso.org.

8 The McGraw-Hill Companies, P.O. Box 182604, Columbus, OH 43272, www.mcgraw-hill.com.

9 National Fire Protection Association, 1 Batterymarch Park, Quincy, Massachusetts 02169-7471, www.nfpa.org.

10 Petroleum Equipment Institute, P.O. Box 2380, Tulsa, Oklahoma 74101-2380. www.pei.org.

[35] McGraw-Hill, *OGP Risk Assessment Data Directory Report No. 434 – 15 March 2010 (free download – http:// www.ogp.org.uk/pubs/434-15.pdf)*

[36] McGraw-Hill, Systems Psychology. De Greene, K. B (Ed.) (1970)

[37] National Fire Protection Association (NFPA)9, NFPA 30, Flammable and Combustible Liquids Code 2008

[38] Petroleum Equipment Institute (PEI)10, Recommended Practice 600, Recommended Practices for Overfill Prevention for Shop-Fabricated Aboveground Tanks - 2007

[39] UK Process Safety Leadership Group and UK HSE, *Safety and environmental standards for fuel storage sites - Appendix 2 Guidance on the application of layer of protection analysis (LOPA) to the overflow of an atmospheric storage tank* – Process Safety Leadership Group, published by the Health and Safety Executive (UK) 2009, ISBN 978 0 7176 6386 6

[40] U.S. Coast Guard, Department of Homeland Security[11], 33 CFR PART 154, *Subpart D – Facility Operations for Facilities Transferring Oil or Hazardous Material in Bulk*

[41] U.S. Environmental Protection Agency[12], 40 CFR 112, *Spill Prevention Control and Countermeasure (SPCC) Rule Regional EPA Inspection SPCC Plan Guidance Manual Nov. 28, 2005 – www.epa.gov/OEM/docs/oil/ spcc/guidance/SPCC_Guidance_fulltext.pdf*

[42] U.S. Harry G. Armstrong Aerospace Medical Research Laboratory Wright Patterson AFB, Dayton, OH: Crew System Ergonomics Information Analysis Center (CSERIAC), *CSERIAC-89-01 Human Factors, Ergonomics, and Human Factors Engineering: An Analysis of Definitions,* Deborah M. Licht and Donald J. Polzella, Kenneth R. Boff

[43] U.S. OSHA[13], CFR 29 1910.119, *Process Safety Management of Highly Hazardous Chemicals*

[44] API Standard 520, *Sizing, Selecting and Installation of Pressure-relieving Devices*

[45] API Standard 521, *Pressure-relieving and Depressuring Systems*

11 U.S. Coast Guard Marine Safety Center (part of DOT), 2100 Second Street, S.W., Washington, DC 20593, www.uscg.mil.

12 U.S. Environmental Protection Agency, Ariel Rios Building, 1200 Pennsylvania Avenue, N.W., Washington, DC 20460, www.epa.gov.

13 U.S. Department of Labor, Occupational Safety and Health Administration, 200 Constitution Ave., NW, Washington, DC 20210, www.osha.gov.