Automatic Overfill Prevention System (AOPS) - Learning from CAPECO incident

Suresh K Ravindran
Global Product Marketing Manager – Tank Gauging
FS Eng (TUV Rheinlad, # 8918/14, SIS)
# Table of Contents

- **Introduction** ........................................................................................................................................................................3
- **Overview** ........................................................................................................................................................................3
- **Standards, Recommendations and reports** ..........................................................................................................................4
- **CSB recommendation on AOPS** ...........................................................................................................................................4
- **Technology evolution** ............................................................................................................................................................6
- **Implementation of Automatic overfill prevention system (AOPS)** ............................................................................................7
- **Proof points** .............................................................................................................................................................................8
- **Notes** .....................................................................................................................................................................................11
- **Conclusions** ............................................................................................................................................................................11
- **References** ...............................................................................................................................................................................11
1. Introduction

Tank farms are crucial area in terminals and refineries, and have a significant impact on their overall business results and yet they are one of the most neglected areas of automation in the facility. With growing complexity in the off-sites piping network, increased workload of operators, and a continuing drive for higher efficiency and throughput, safe tank farm management has become an even greater challenge across the industry. Tank farms, storage areas and loading/unloading sites all need effective safety solutions to protect personnel, assets and the environment. The consequences of incidents at these facilities can be enormous.

![Safe Terminal operations](image)

Figure 1: Safe Terminal operations

The tank farm environment, being a hazardous area, requires continual monitoring of critical process parameters. Accurate and reliable tank level monitoring is especially important to prevent overfill situations. Incidents at refinery and terminal tank farms continue to occur. Several catastrophic incidents can be traced to ineffective use of technology leading to loss of level control and, ultimately, to loss of containment, lost lives, damage to environment and widespread disruptions.

Tank farm operations benefit from a holistic approach to industrial safety, which integrates advanced technology at all plant protection layers.

2. Overview

The recent public preview copy of the report from U.S. Chemical Safety and Hazard Investigation Board (CSB) has indicated serious lapse in deployment and maintenance of terminal operations at CAPECO facility.

This white paper describes critical recommendations from CSB specifically addressing overfill prevention safety systems in petroleum storage tank farms. It also discusses possible automatic overfill prevention technologies/solutions, which can be used to comply with industry guidelines and create a safe work environment.

Note: CSB report refers extensively to various standards, papers, recommendations and reports on safety, related to petroleum storage and operations and hence this white paper does not mention those references again to avoid repetition. Additional references are used for specific explanation purposes.
3. Standards, recommendations and reports:

IEC 61511 - Functional safety – Safety instrumented systems for the process industry sector
IEC 61508 - Functional safety of electrical/electronic/programmable electronic safety-related systems
ANSI/ISA-84 - Functional Safety: Safety Instrumented Systems for the Process Industry Sector
ANSI/API standard 2350-2012 - Overfill Protection for Storage Tanks in Petroleum Facilities
OISD STD 244 - Oil Industry Safety Directorate standard on storage and handling of petroleum products at depots and terminals including standalone crude oil storage facilities
IOCL Jaipur Fire Accident - M B LAL Committee recommendation
Buncefield depot fire accident - Major Incident Investigation Board (MIIB) recommendations on the design and operations of fuel storage tanks.
CAPECO Fire Accident - U.S. Chemical Safety and Hazard Investigation Board (CSB) public preview report copy.

4. CSB recommendations on automatic overfill prevention systems:

4.1. 2009-02-I-PR R1 (page 87 of CSB public preview report)

1) Ensure bulk above ground storage facilities conduct and document a risk assessment that takes into account the following factors:
   a) The existence of nearby populations and sensitive environments;
   b) The nature and intensity of facility operations;
   c) Realistic reliability of the tank gauging system; and
   d) The extent/rigor of operator monitoring

Applying these recommendations

- A Hazard and operability study (HAZOP) by third-party safety assessors.
- Reliability check on existing tank gauging system. Float and Tape type of level measurement instruments have proven to be unreliable as per the CSB report. The functional reliability of latest state of the art measurement technologies like servo type continuous electronic sensor, radar type continuous sensor is proven. These tank gauging measurement technologies must have a continuous functional testing mechanism ensuring the reliability of gauging system.
- An automated monitoring would reduce risk of manual errors in handling & monitoring terminal operations. Applying integrated automation of terminal operations is the simplest way to reduce risks.

4.2. 2009-02-I-PR R1 (page 87 of CSB public preview report)

2) Equip bulk aboveground storage containers/tanks with automatic overfill prevention systems that are physically separate and independent from the tank level control systems.

5) Regularly inspect and test automatic overfill prevention systems to ensure their proper operation in accordance with good engineering practice.

Applying these recommendations

- This recommendation is most important for overfill prevention and is similar to what was recommended in MIIB report from Buncefield investigation, M B Lal recommendation based on IOCL Jaipur investigation and most recently as per revised API 2350-2012 fourth edition.

- **Physically separate** – Use separate tap off point (mounting location) for the overfill prevention and tank level control instruments. For new tanks, this is not a big issue, as providing two nozzles or two stilling wells for instruments is possible. For operating tanks, the challenge is to have suitable nozzles / stilling wells. It is worth checking if the size, height and location of nozzle / stilling well poses any limitation on accuracy of the instruments for overfill and/or tank gauging instruments. A compromise on accuracy shall severely impact the reliability of overfill prevention system.

- **Independent** – As per API 2350 A.3 Independence (page 31)

The AOPS shall be designed and installed so that failures associated with any other overfill prevention system (OPS) or ATG hardware, software, communications, wiring connections or cabling cannot cause a failure of the AOPS. Correct operation of the AOPS shall not require communications to or from any location remote from the facility where the AOPS has been installed. AOPS shall not rely on wireless communication to initiate diversion or termination of receipt.
The term “independent” means that the AOPS shall be separate from any device or method used to measure, calculate or monitor tank receipts. The independent AOPS shall be designed and installed such that no fault in the ATG gauging and monitoring system is capable of causing a fault in the AOPS.

- This is achieved by using “additional” overfill prevention instrument which functions independent of tank level monitoring instruments on tank top. Misleading claims on use of same instruments (with multiple electronics within same housing) for auto level control and AOPS, is been proven wrong, being such instruments use common wave guides & wave focusing mechanism (antenna). And moreover they do not meet the requirement of providing two independent and separate device for AOPS and auto tank gauging (ATG) system and hence are not compliant. Extreme caution required and critical examination of reliability data of such instruments is mandatory before taking any risk in this direction.

- Use of “Wireless”, as stated in API 2350 A.3 (page 31), is allowed in a overfill prevention sensor, as long as the wireless communication is not used for initiating diversion or termination of receipts. For existing oil storage facilities, use of wireless for communicating the basic level measurement and other diagnostic data to a central system (for example a Tank inventory system and/or a Terminal Automation system), helps achieving enhanced reliability of the system and helps generating additional alarms. For such a design the safety function output (SIL rated relay or analog output) is hardwired to the logic solver, and AOPS actions are performed independently without relying on any other communication, information or intervention.

- Use of diverse technology is explained in the IEC 61508/61511(IEC 61508 Ch 2 Clause 7.4.2.3 page 20 and IEC 61511 Ch 1 Clause 11 in safety instrumented system design). A reliable deployment would need careful study of tank farm applications.

- The reliability of overfill prevention device in petroleum storage application depends upon the overfill prevention loop’s SIL requirements (as per result of HAZOP), accuracy requirements, reliability data, proof testing methods/interval, additional functional enhancements, and other constraints.

- Measurement Technologies - Industry experience confirms use of Radar type continuous sensor and Servo type continuous electronic sensor for overfill prevention applications meeting requirements of API 2350 ed 4, and additionally meeting the practical application challenges for safe and reliable operations. Practically, any device which has required SIL rating and has continuous measurement capability (Like Radar continuous sensor or Servo continuous electronic sensor) should be preferred over point measuring instruments.

- Proof testing – Major attention need to be paid towards regular proof testing which is an important part of validating the safety function in an overfill prevention system. This testing confirms the integrity of the level measurement portion of the loop and ensures the average Probability of Failure on Demand (PFD Average) is within acceptable limits. Without testing, this PFD value will increase to a point where the instrument no longer meets the specified SIL requirements for the SIS. For all practical purposes, the proof testing should validate the safety function and shall be:

- tested as close as possible to an actual event- For example a servo continuous electronic sensor type instrument lifting the displacer to the actual alarm CH (critical high) or HH (High-High) condition, And for example a Radar continuous sensor instrument is simulated for alarm condition. This simulation would be meeting partial proof testing requirements.

- as per API 2350 clause 4.5.5.3 (page 24)

4.3. 2009-02-I-PR R6 (page 90 of CSB public preview report)

- a. More than one safeguard to prevent a tank overfill, all within an automatic overfill prevention system as described in ANSI/API Standard 2350 (2015) Overfill Protection for Storage Tanks in Petroleum Facilities with an independent level alarm as one of the safeguards. The safeguards should meet the following standards:
  1. Separated physically and electronically and independent from the tank gauging system;

Applying this recommendation

- Refer to earlier pages of this white paper.

- This recommendation emphasize that more than one safeguard to prevent overfill might be required.
• The word “electronically” added in this recommendation puts greater emphasis that overfill prevention and auto level gauging has to be achieved by two (2) independent devices.

• This could be achieved by safety alarm function of auto level control system (ATG system) also to be interfaced with logic solver which has independent level alarm as the main safe guard. This mechanism helps using 1oo2 logic for overfill prevention systems.

• Logic solver (safety control system like SIL certified hybrid control system) then acts as per safety system design to prevent the overfill situations.

4.4. 2009-02-I-PR R7 (page 90 of CSB public preview report)

The safeguard, Automatic overfill prevention system, should meet the following standards:


Applying these recommendation

• Refer to earlier pages of this white paper.

• IEC 61511 part 1, refers to a safety instrumented system (SIS), implemented over a safety life cycle considerations starting from hazard and operability studies, allocation of safety functions to protection layers, safety requirement specifications(SRS), safety design, testing at factory, installation & commissioning, validation, operation and maintenance, modification, decommissioning and documentation.

• AOPS documentation need includes records of proof testing and maintenance. Use of continuous type sensors helps to automatically capture proof testing results with time stamping and also the records of automatically generated maintenance completion reports ensures high level of integrity and commitment to safety.

5.0. Technology evolution

![Figure 2: Evolvement of safety configuration](image)

The figure above shows the how the safety system configuration within a safety element and within a safety instrumented system evolved over last several decades. While redundancy is important for a safe system, the embedded diagnostic over the redundant safety architecture (example 2oo4D) has become a necessary enhancement.
6. Automatic overfill prevention system (AOPS) implementation

While the above chapters explained the key requirements of an overfill prevention system, this chapter detail some of the possible practical solutions. Figure 3 shows the safety life cycle service model based on IEC 61511.

Figure 3: Safety Lifecycle service model as per IEC 61511

As shown in figure 3, safety lifecycle demands a high integrity and reliable solution, which needs to qualify each phase. A simple understanding of above model is as below:

- HAZOP is important first step and shall be done by safety experts.
- Site surveys to assess the suitability of various types of measurement technologies to be used for overfill prevention, with minimum disruption to operation, in case of existing facility. Normally, this should be done by solution experts.
- Designing of SIS, selection of best solution, installation & commissioning, and operation & maintenance by trained professionals are critical for safety instrumented system’s performance.
- Implementation of an overfill prevention system is recommended to be done by a solution provider, who can make an initial assessment, design an automatic overfill prevention system (AOPS) and implement the same at site. Generally, such solution providers have in house safety experts who ensure faster solution implementation at site.
- Honeywell is well known for their global safety organization, structured on forming discipline-based team for skills, processes, best practices, tools, knowledge and expertise deployment closely aligned with project engineering.
7. Automatic overfill prevention system (AOPS) proof points

7.0 a) – Basic AOPS in petroleum storage terminals

In above example of figure 4:

- Overfill prevention sensor (option 1) - Radar type continuous sensor is used as SIL 2 (note*1,*5) certified overfill sensor which is physically separate and independent from the automatic level gauge. Proof testing is done through a display unit mounted at tank bottom, avoiding tank climbing. Also, this meets the requirement of overfill prevention sensor being fully functional and operable with no intervention from any other system. Honeywell's SmartRadar FlexLine radar type continuous sensor can be mounted on a 6” or bigger nozzle/stilling well and can be installed very close to tank shell with no drift in performance. These radars are known for their best in class accuracies of +/-0.4 mm (note*2) and superior safety features like SFF of 97%, 2004D internal safety architecture and internal diagnostic cycle time (note*3) of less than 3 milliseconds.

- Overfill prevention sensor (option 2) - Alternately SIL 2 (note*1,*5) certified Servo type continuous electronic sensor can be used for AOPS. Honeywell Enraf's servo type electronic sensor is “multifunction automatic tank gauge” for accurate petroleum storage tank farm measurements (+/-0.4 mm) and safety in tank farms. Servo electronic sensors are equipped with patented “servo auto test” (SAT) feature, which ensures superior diagnostic coverage of entire device. Honeywell Servo gauge has unmatched safety performance of servo auto test, internal diagnostic cycle time (note *3) of less than 3 millisecond and Mean Time Between Failure (MTBF) of 667 years. Servo ATG mounting is possible on a 6” or bigger stilling well.

- Use of Radar or Servo type continuous sensor depends upon the applications, mounting provisions etc.

- Logic solver is a SIL2/3 (note *1, *5) safety control system and is designed specifically for safety applications.

Safety control systems need a careful selection, to meet the minimum requirements of a reliable safety control systems as described in API 2350-2012 annex A A.4.3 (page 32). A tank farm would have many safety instrumented functions (SIFs) like AOPS, dyke valve sensing, hydrocarbon detection and vapor cloud detection etc., hence it is critical to design the logic solver such a way that it is capable of accommodating all such SIFs. A scalable safety control system such as Honeywell’s safety manager or HC 900 safety controllers ensures seamless expansion of safety loops as needed during any phase of of safety implementations and/or safety enhancement of the terminal operation.

Honeywell’s safety systems, Safety Manager or HC900 Hybrid Controller, are proven for their safety and integrity.
- Remote operated shut off valve is used as first tank body valve.
- Entire AOPS safety loop is independent of any other system and has no manual intervention involved.
- **Diagnostic cycle time** – Refer to notes at the end of chapter 7. (note *3)

7.0 b) – AOPS with enhanced safety diagnostics

![Figure 5 – AOPS – Design of AOPS with ATG system with enhanced safety diagnostics](image)

In above example of figure 5:

- **Overfill prevention sensor** - Radar type continuous sensor is used as SIL 2 (note *1,*5) certified overfill sensor which is physically separate and independent from the automatic level gauge. Proof testing is done through a display unit mounted at tank bottom, avoiding tank climbing. Also this meets the requirement of overfill prevention sensor being fully functional and operable with no intervention from any other system. While the safety function of radar which could be SIL (note *1,*5) certified relay or analog output, is connected to safety control system, the measured parameters (level) data goes to Tank Inventory and Terminal Automation system as a redundant input. This gives additional diagnostic at supervisory levels as the inputs of measured parameters are compared with ATG, and an additional alarm is generated in terminal automation system.

  Honeywell’s SmartRadar FlexLine radar type continuous sensor can be mounted on a 6” or bigger nozzle/stilling well and can be installed very close to tank shell with no drift in performance. These radars are known for their best in class accuracies of +/0.4 mm (note *2) and superior safety features like SFF of 97%, 2oo4D internal safety architecture and internal diagnostic cycle time (*3) of less than 3 milliseconds.

- **Auto Level Control gauge** – Servo type continuous electronic sensor is used in ATG system, and is also SIL2 (note *1, *5) certified. Using different measurement principle meets diverse separation requirements. The safety function of this servo sensor (SIL certified relay or Analog output)(note *5) is being given to logic solver. Hence the overfill loop forms a 1oo2 architecture, contributing to enhancement of the safety system.

  - Logic solver is a SIL2/3 (note *1,*5) safety logic solver and is designed specifically for safety applications.
  - Logic solvers need careful selection, to meet the minimum requirements of a reliable safety control systems as described in API 2350-2012 annex A A.4.3 (page 32).
  - Remote operated shut off valve is used as first tank body valve.
  - Entire safety loop is independent of any other system and has no manual intervention involved.
• Both the sensors (ATG and overfill) are highly reliable and high precision devices, ensures higher integrity and higher availability. Accuracy of both these instruments shall be same, to monitor level input in control room as a redundant data.

• **Diagnostic cycle time** – Refer to notes at the end of chapter 7. (note *3)

7.0 c) – AOPS in a crude oil storage terminal

![Diagram of Automatic Overfill Prevention System](image)

**Figure 6 – Automatic overfill prevention system (AOPS) - Use of SIL certified Radar (guided wave radar/TDR)**

In above example of fig 6:

• For the applications where accuracies are not as demanding as per requirements API 3.1B, Radar type (TDR or GWR) sensors can be used for AOPS. The safety function of these overfill sensors are connected to logic solver independent of ATG system. Proof testing mechanism need to be evaluated before deploying these sensors for AOPS use.

Honeywell’s SmartLine Level transmitter (guided wave and non-contact TDR radars) meets such needs.

• The configuration in figure 5 shows, that in addition to safety function of Radar (GWR/TDR), the safety function of ATG radar also is given to logic solver, creating a 1oo2 logic for overfill prevention system. This additional logic enhances the reliability of overfill prevention safety instrumented function (SIF).

7.0 c) **Point level Sensors/Switches**

• Refer to note at the end of chapter 7. (note *4)
8. Notes:

**Note *1:* As per API 2350 Ch 5.4 page heading "automatic overfill prevention system"

In this standard, when an AOPS is required (by the risk analysis, owner and operator policy or regulation), it shall be applied according to the following options:
- option 1 – for existing facilities: an AOPS as described in Annex A provides an acceptable approach for achieving and demonstrating adequate integrity; and
- option 2 – for new facilities: an AOPS designed and managed in accordance with requirements of ANSI/ISA 84.00.01-2004 (IEC 61511 modified) "Functional Safety: Safety Instrumented Systems for the Process Industry Sector" shall be required.

**Note *2:* For certain instrument vendors, accuracy and performance of radar type continuous sensor, depends upon the nozzle size, heights and also applications.

**Note *3:* Fault detection time/Internal diagnostic cycle time - Extreme caution is required, while designing overfill prevention SIFs, involving devices which have a diagnostic cycle time (internal fault detection time) of more than one minute. Some devices have 90 minute worst case internal fault detection time, which could lead to a disastrous situation, as potential (detectable) fault would be sleeping in system for 90 minutes, before it gets detected and reported.

**Note *4:* Point level sensors or switches - Use of point level sensors (level switches, ultrasonic point level sensors etc.) for overfill prevention systems are not preferred due to increased proof test requirements, and absence of continuous internal diagnostics on functional checks.

**Note *5:* SIL certified instrument referred in this white paper refers to the equipments certified to be used in SIL rated loops.

9. Conclusion

With growing complexity in terminal operations in view of the off-sites piping network, increased workload of operators, and a continuing drive for higher efficiency and throughput, profitable and safe tank farm management has become a challenge, leading to neglect of applicable standards.

Apart from AOPS and tank gauging systems there could be several other critical safety loops in any bulk petroleum storage facilities. Facilities involved in receipt, storage and distribution of petroleum products, must not neglect any of the below operational areas:

- Fire water system and alarms
- Tank farm sub systems- AOPS, auto tank gauging, dyke valve sensing, hydrocarbon gas detection and vapor cloud alarm monitoring system through digital video monitoring systems
- Automation of loading/unloading operations and valve control subsystem
- Management Information System & reporting system interface
- Maintenance, training and documentation

To design and implement a comprehensive terminal safety system, readers are encouraged to read as a minimum U.S. CSB public preview report on CAPECO incident, MIIB final report on Buncefield incident, M B Lal recommendations on IOCL Jaipur incident, standard OISD STD 244 and standard API 2350-2012.

As outlined in this white paper, adequate understanding, interpretation and implementation, of various recommendations and standards is critical for a safe working environment while achieving the economic goals of terminal operations.

10. References

[1] Recommendations on the design and operation of fuel storage tanks (MIIB)
[7] OISD STD 244 - Oil Industry Safety Directorate standard on storage and handling of petroleum products at depots and terminals including stand-alone crude oil storage facilities.
For More Information
Learn more about how Honeywell’s safety solutions, visit our website
www.honeywellprocess.com or contact your Honeywell account manager.

Honeywell Process Solutions
Honeywell
1250 West Sam Houston Parkway South
Houston, TX 77042

Honeywell House, Arlington Business Park
Bracknell, Berkshire, England RG12 1EB UK

Shanghai City Centre, 100 Junyi Road
Shanghai, China 20051

www.honeywellprocess.com