Originally appeared in:
February 2014, pgs 71-74.
Used with permission.
HYDROCARBON PROCESSING®

HP | Maintenance

P. E. MYERS, PEMY Consulting, Pleasant Hill, California

Consider robust tank overfill prevention and independent alarm and gauging systems

Elimination of tank overfills is a significant problem for the petroleum industry. Since most tank receiving operations are manual, the operators rely heavily on tank level gauges and alarms for overfill prevention. Tracing the historical development of tank gauging and alarm systems provides insight into why independence is so important. This history is interwoven with interpretations, insights and guidance about applying independence in an appropriate context to overfill prevention systems. A discussion on future trends in instrumentation systems for tank overfill protection is also considered here.

Industry standards history. Reliability of equipment systems by duplication of components or systems is not new. The basic idea is that if one component or system fails then a backup system steps in and covers for the failed item. FIG. 1 shows how this idea has been used for typical tank gauging and alarm systems.

In the 1970s and 1980s, some major oil companies were already recognizing that the failure rate of alarms and of automatic tank gauging was too high, so they began to consider implementing standards requiring redundancy of high-failure-rate components (FIG. 2).

Although there are numerous components in any alarm and tank gauging system (power supply, wiring, electrical connections and relays), by far the most common failures occurred in the level sensing devices. In this era, the most common level sensors were electro-mechanical devices such as float and tape systems using pulleys, steel cabling and reel mechanisms that measured the position of the float, providing both level as well as alarm functions. Many overfills resulted from mechanical failures in these devices. The ubiquitous mechanical float and tape type device, common both in the past and in the present, depends on pulleys and cables that may eventually stick or bind in dirty services. When this happens, any alarm that is activated by the float and tape level sensor will also fail. Since the position of the cable reel mechanism not only establishes the actual measured level but also trips the switch that activates the alarm, the entire gauging system and alarm system are prevented from working as a result of this single point of failure. In this type of configuration, the alarm is dependent on the automatic tank gauge (ATG).

Two influential standards that contained the best practices of this period were *National Fire Protection Association (NFPA) 30* and *American Petroleum Institute (API) 2350*. These standards mirrored the best practices of the industry as a whole on an international level.

Even though tank gauging and alarm systems were not entirely dependable, they were made far more reliable by the recognition of redundancy and independence. The first real requirement for tank gauging and alarm system independence originated with the *NFPA standard 30-1993*.[1] It applied where NFPA Class I liquids were stored. These are products such as gasoline, crude oil or other petroleum-based liquids that have a high potential to ignite if there is a spill, due to the ease with which vapor is generated. *NFPA 30* required that petroleum liquid overfills be prevented by utilizing one of the following:

a) "Tanks gauged at frequent intervals by personnel continuously on the premises during product receipt with frequent acknowledged communication maintained with the supplier so that flow can be promptly shut down or diverted."
b) "Tanks equipped with a high-level detection device that is independent of any tank gauging equipment. Alarms shall be located where personnel who are on duty throughout product transfer can promptly arrange for flow stoppage or diversion."
c) "Tanks equipped with an independent high-level detection system that will automatically shut down or divert flow."

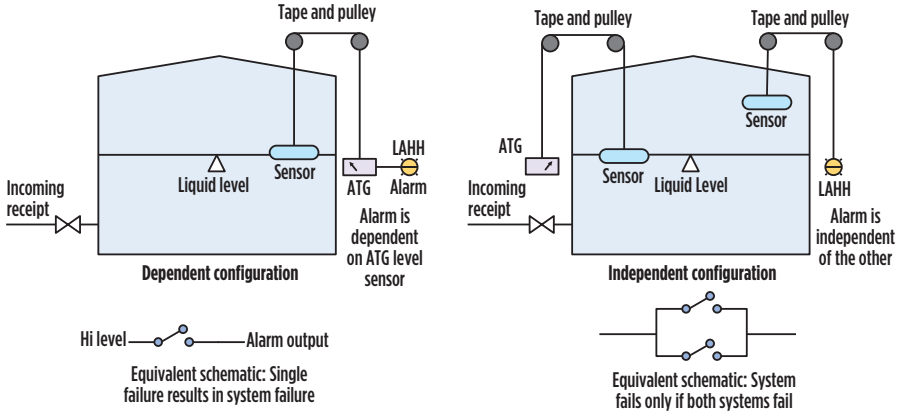

FIG. 1. Independence concept in API 2350.

d) "Alternatives to instrumentation described in b) and c) where approved by the authority having jurisdiction as affording equivalent protection."

Because of close collaboration and alignment between NFPA and API committees, these same requirements were echoed in the second edition of *API 2350 Tank Overfill Protection,* published in 1996. These organizations were charged to respond to the unacceptable rate of tank overfills, since fires resulting from petroleum storage tank overfills were (and continue to be) a significant petroleum industry problem.

Notice how broadly the requirements address tank filling operations. Item a) was included to address the many tank operations that had no instrumentation and to give ultimate control to the operator.

The requirements for "independence" are found in Item b) and Item c). Item b) was intended to address alarm function separation from the automatic tank gauging system (FIG. 1 and FIG. 2).

Most tank filling operations then as well as today are essentially a manual operation (i.e., the operator manually or remotely operates valves based on estimated time to fill or as the result of an alarm to safely terminate a receipt). However, in the requirements, the wording requires independence of the "tank high-level detection device." Today, we would refer to this as the tank level sensor. In essence, the level sensing device for the tank level gauging must not share the same sensor with the alarm system. Two sensors are required: one for the tank gauging or level reading and one for the alarm function (FIG. 1).

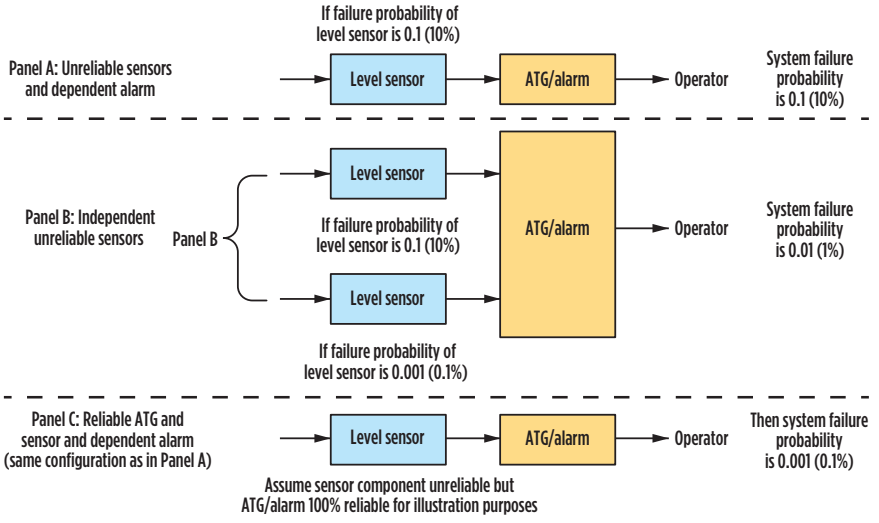

FIG. 2. Independence can achieve improved reliability.

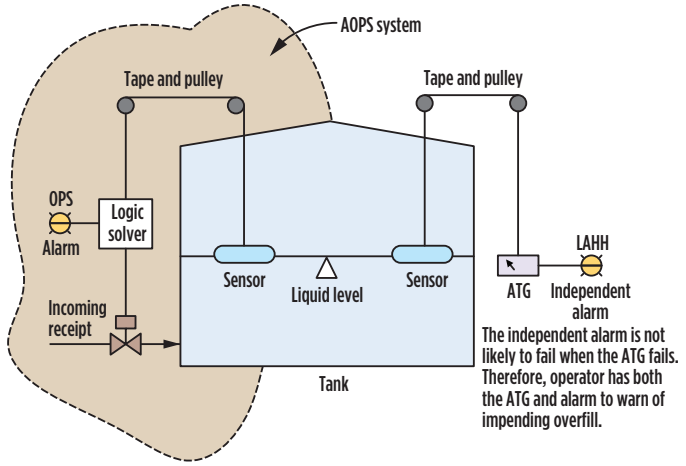

FIG. 3. AOPS system and independent alarm diagram scenario.

Requirement c) (FIG. 3) was intended to apply to those systems for which an automated system acted to terminate a receipt on being triggered by the level sensor. Such systems are called automated overfill protection systems (AOPSs), as found in the 4th edition of *API 2350.* These are also referred to as safety instrumented systems (SISs) in other international safety standards. While these systems are much less common than the typical manual operation of tanks, they do exist, and it is anticipated that such systems will be applied to tank overfill protection at an increasing rate in the future. Tank systems with AOPSs are also addressed in the present version of *API 2350.* It should be pointed out that, after the Buncefield incident, the authorities having jurisdiction in the UK required such systems on any tank that receives *NFPA 30* Class I liquids.[2]

Independence requirements. The requirements for independence can readily be understood by reviewing this definition from the 2nd edition of *API 2350:*

> **"Independent level detector:** A product level sensing device that is separate and independent from any automatic gauging equipment on the tank. High-high-level detectors in single-stage and in two-stage detector systems shall always be independent detectors. A high-level detector in a two-stage detector system may or may not be an independent detector."

Because the authors of *NFPA 30* and *API 2350* standards during this era were charged with the responsibility to reduce tank overfill incidents, they understood the necessity of separating the alarm function from the level gauging function where the failure of a single component (the level detector) could cause failure of the entire level and alarm system. Therefore, to meet the intent and requirement of these early editions, a tank owner/operator simply needed to ensure that the float and tape type automatic tank gauge were separate from the device that set off the alarm. Typically, this would be accomplished by use of a separate float or other sensor that is operable and independent of the tank gauging system, in spite of a possible failure of the tank gauging system. Of course, a failure in the independent alarm system could remain hidden or undetected, but at least the gauge would likely be working (FIG. 1).

Current standards approach. The new version of *API 2350* (4th edition) carries forward the concepts of independence originating from the 2nd edition, and does so with even more specificity. This is done by leveraging off of other standards that require high reliability for critical safety systems (*ISA S84* or *IEC 61511*).[3] Today, *API 2350* identifies tanks that have independence in their instrumentation through several categories.

API 2350 Category 3 is illustrated in **FIG. 4.** Because almost all tanks fit into several fundamental tank gauging configuration patterns, *API 2350* establishes three categories for tank overfill protection systems:

- **Category 1 systems** are manual systems without the ability to transmit any gauging information
- **Category 2 systems** are tanks with the ability to transmit level and alarm information, but the level gauging and alarm functions are not independent
- **Category 3 systems** are tanks which have the ability to transmit level and alarm information and the alarm system is independent of the tank gauging system.

The *API 2350* task committee recognized the critical importance of Category 3 systems, which embrace the idea of independence. In general, they are more reliable than a Category 1 or Category 2 system. For an unattended terminal tank receiving operation, Category 3 is required. This, of course, is based on the implied higher reliability of the Category 3 system than Category 1 and Category 2 systems.

However, *API 2350* does not really say much about the reliability or risks associated with the category designations, because there are so many other factors that impact actual risk and the decision-making process. For example, if you had an idealized, totally reliable alarm system (zero failure rate), the overall risk of overfills could still be a significant problem if the operating practices were not robust. Risk is also a function of receptor sensitivity and population density. Risk is specific to location, configuration of receptors and many other factors, so that risk assessment cannot be directly correlated to a tank category. Therefore, API makes no statements regarding the relative reliability of categories.

New developments. *API 2350* has brought the automated shutdown or diversion of incoming receipts to a whole new level (**FIG. 3**). This is truly one of the big changes in the new edition of *API 2350.*

While the earlier 2nd and 3rd editions of *API 2350* only had the requirement that the sensors be independent of the tank gauging system, the new 4th edition relies on the relatively new industry standards for safety instrumented systems *IEC 61511* or *ISA S84.*

AOPS basics. In order to understand how independence applies to AOPSs, key requirements for AOPS must be reviewed.

The definition of AOPSs is any system that automatically, and without operator intervention, operates valves or other equipment elements (called final elements) to terminate a receipt upon being triggered by the high-high-level sensor. An AOPS is most often applied to simply close a valve on a receipt when the high-high sensor detects liquid. Valve closing time must be sufficient to prevent "water hammer."

An AOPS is optional, and it is only used when the user chooses to apply an AOPS for tank overfill protection. However, when the user chooses to use an AOPS, then the mandatory requirements in *API 2350* apply.

If the tank owner/operator chooses to use an AOPS, then there are two options:

- **Option 1:** This option applies when an AOPS is applied to existing tank systems
- **Option 2:** The second option applies if an AOPS is applied to new facilities.

For new facilities, it is practical and expected that systems such as AOPSs shall be designed in accordance with appropriate safety standards such as *ISA S84* or *IEC 61511.* These safety standards are designed to systematically remove faults or flaws throughout the entire system lifecycle. However, these standards are not really applicable for retroactive application to older equipment. Therefore, the *API 2350* committee exempted required compliance with these standards and, instead, provided a compiled list of best practices for AOPSs in *API 2350* Annex A, which must be applied to existing systems.

AOPS independence. Independence is specifically addressed in detail in *API 2350* Annex A. While this annex applies only to AOPS retrofits of existing equipment, there is no doubt that the requirements and implied meaning for independence will be generally interpreted from this annex. For reference, here is the section from *API 2350:*

> **"A.3 independence.** 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. The 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

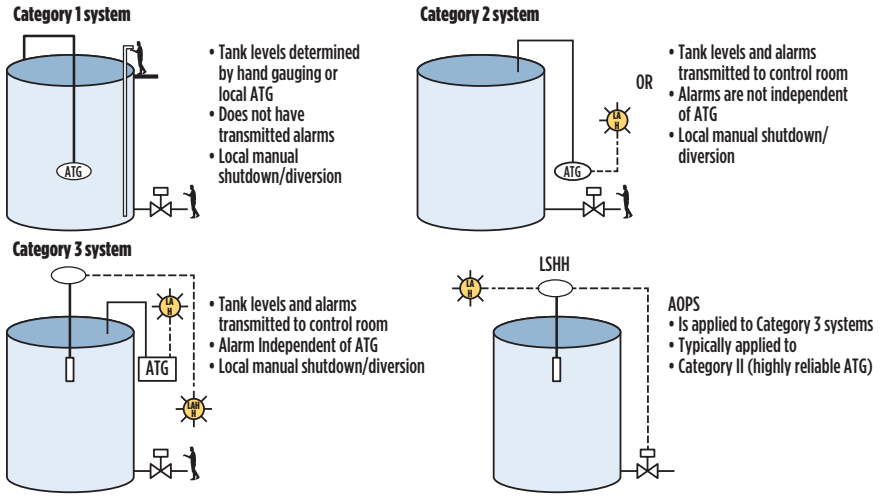

FIG. 4. Overfill protection system categories.

and installed such that no fault in the ATG gauging/monitoring system is capable of causing a fault in the AOPS."

Remember: The hazards associated with petroleum storage tanks rank far above pressure vessels and piping in terms of loss (financial, injuries and fatalities). Because of recent notable tank overfills, the regulatory landscape will become far more stringent than in the past. It is in the best interests of owner/operators to accept this premise and to start thinking about efficient ways to align with the new practices and standards.

Separation of sensors. The first bullet requires the separation of the ATG and AOPS so that failures in one system do not cause failures in the other system, as previously described for the alarm/gauging systems. However, here more specificity is applied to the support systems such as wiring, cabling, communications and software. Does this imply that separate conduits and wiring are required for these systems?

The meaning of *independence* takes on different degrees. In the real world, there is no such thing as true independence. If a terrorist attack or meteor were to knock out an entire terminal, then not even the "independent" wiring, conduits and other equipment would be independent. At the other extreme, consider poor wiring practices where electrical wiring is vulnerable to destruction by a single fire or by vehicular traffic. In this case, independent circuits and wiring located separately would reduce the likelihood of failure of both gauging and AOPS circuitry. From these hypothetical considerations, it is clear that the concept of independence is relative and a matter of degree.

So making relatively unreliable components redundant and independent can have a big impact on improving reliability. But redundant and independent components for highly reliable systems will have less overall impact on the system reliability (FIG. 2). These concepts can be analyzed quantitatively, using formal methods such as reliability block diagrams and other probabilistic methods. But common sense may be more useful and effective in establishing how far to take the concept of independence. Just remember that, in the origination of these concepts in the tank industry, it was adequate to simply make the level sensor or the alarm separate from the level sensor for the tank gauge, in spite of common and dependent power supplies, wiring and other components.

Two continuous level sensors. On first reading, one might be led to the conclusion that two identical level gauges cannot be used where one is for the tank level gauging function and the other is for the purpose of initiating the AOPS (or an independent alarm system), as it says that *independent* means separate devices and methods. If the devices are using the same method of measurement, then one might conclude that such use of instrumentation is prohibited by this language. However, this was not the intent of the committee.

It might be clearer to read the particular sentence this way, "The term *independent* means that the AOPS shall be separate from any device or method used to measure, calculate or monitor tank receipts." If the wording is interpreted to mean an automatic tank gauge or gauging system, then the sentence reads, "*independent* means that the AOPS shall be separate from any automatic tank gauge or gauging system." Clearly, two identical automated tank gauges may independently serve the function of the ATG and AOPS or alarm sensor. It was this interpretation that the committee intended when drafting language regarding independence.

Indeed, some companies are using two ATGs, one functioning as a level gauge and the other functioning as an alarm. A diagnostic alarm is then set to indicate any wide variation between the two ATG level readings. In this way, two continuous level sensors (vs. one point level and one continuous level) are even more robust in terms of reliability and diagnostics. One could almost conclude that continuous proof testing is occurring.

As a result of evolving technologies and lower costs, it is important to note that a trend is now firmly established where two tank gauges are being used to perform the function of the ATG and a high-high alarm sensor or AOPS sensor. The reason for this is twofold. First, the costs of equipment have come down relative to the other general costs associated with tank work projects. Second, the ability to get continuous level as a check on the primary ATG provides both redundancy and independence and provides the highest possible reliability with relatively little extra investment.

Think efficiently. Keep in mind that the hazards associated with petroleum storage tanks rank far above pressure vessels and piping in terms of loss (financial, injuries and fatalities). Because of recent notable tank overfills, the regulatory landscape will become far more stringent than in the past. It is in the best interests of owners/operators to accept this premise and to start thinking about efficient ways to align with the new practices and standards. One way to go about this moving forward is to do so incrementally and systematically. This can only be done effectively if the tank gauging system replacement policy and the policy for new systems are not based on the existing systems, but are aligned to the best equipment and practices available.

Owners should be using independent and redundant level sensors or ATG systems and following the proof testing requirements outlined in the appropriate standards. By doing so, this can ensure that robust management systems for companies are in place so that they support the appropriate use of these standards. HP

LITERATURE CITED

[1] National Fire Protection Assocation, *NFPA 30, Flammable and Combustible Liquids Code,* 1993.
[2] www.buncefieldinvestigation.gov.uk/reports/index.htm#final, December 12, 2005.
[3] IEC 61511 Safety Instrumented System Standards, *Functional Safety: Safety Instrumented Systems for the Process Industry Sector,* 2003.