Tank Overfill Protection - API 2350 and IEC 1511 Safety Considerations

Authors: Don Newell, Shamrock Gulf
         Gene Cammack, Siemens Industry Inc.
         Praveen Muniyappi, Siemens Industry Inc.

Keywords: Tank Overfill; Safety; Process Safety; Level Control

ABSTRACT

For overfill protection on tanks holding volatile, petroleum fluids, the industry best practice has been documented in API 2350. Recent events have begun to cause the industry to rethink the overfill protection requirements and to move to a more functional safety approach. For the process industry, the standard for designing a Safety Instrumented System (SIS) is IEC 61511. The IEC 61511 standard for Safety Instrumented Systems (SIS) has been widely adopted to evaluate risk associated with safety related systems in the process industry. Many companies want to apply the IEC standard, in addition to the API Standard. This creates consistency in their approach to safety and helps verify the specific risks associated with their facilities.

This paper examines trends in the industry, particularly related to the Buncefield incident and the report of the Major Incident Investigating Board, and the issues and possible solutions to designing Tank Overfill Protection Systems that can meet both the API Recommended Practice and the IEC standard.
INTRODUCTION
The American Petroleum Institute (API) has a Recommended Practice (API 2350)\(^1\) that was published in January of 2005 that details the recommended practice for Overfill Protection on Petroleum Fluid Storage Tanks. Since that standard was released, a number of incidents, most noticeably the Buncefield Explosion in 2005 and the significant consequences of those events have heightened the interest in safety issues around Petroleum Storage Tanks. The final report of the Major Incident Investigation Board on the Buncefield Incident\(^2\) made significant recommendations that begin to marry the previous prescriptive standards of API RP 2350 to the functional safety standards described in IEC 61511:

![The Buncefield Explosion](https://www.buncefieldinvestigation.gov.uk)

**Figure 1: The Buncefield Explosion**
From the Buncefield Investigation Homepage: www.buncefieldinvestigation.gov.uk
Courtesy of Royal Chiltern Air Support Unit

**The Buncefield Final Report: Recommendation 1**
The Competent Authority and operators of Buncefield-type sites should develop and agree a common methodology to determine safety integrity level (SIL) requirements for overfill prevention systems in line with the principles set out in Part 3 of BS EN 61511.(ref 3) This methodology should take account of:

- the existence of nearby sensitive resources or populations;
- the nature and intensity of depot operations;
- realistic reliability expectations for tank gauging systems; and
- the extent/ri
gour of operator monitoring.

Application of the methodology should be clearly demonstrated in the COMAH [Control of Major Accident Hazards] safety report submitted to the Competent Authority for each applicable site. Existing safety reports will need to be reviewed to ensure this methodology is adopted.

![Recommendation 1 of the Final Report of the Major Incident Investigation Board on the Buncefield Incident](https://www.buncefieldinvestigation.gov.uk)

**Figure 2: Recommendation 1 of the Final Report of the Major Incident Investigation Board on the Buncefield Incident**

**Functional safety: Safety Instrumented Systems for the process industry sector**\(^3\) API is preparing a revision of API 2350 that will reflect these changes.

This paper examines the current API 2350 standard, and the IEC standards in process safety and how they might work together. In addition, it looks at some of the issues in applying IEC 61511 to tank overfill and how they can be addressed.

PRESCRIPTIVE AND FUNCTIONAL STANDARDS
In the process industries, there are two approaches to Safety. A prescriptive approach defines a precise solution for an application. A functional approach defines a methodology and performance standards in lieu of a specific remedy. For specific applications, like tank overfill protection, which are consistent and definable, a prescriptive standard can be written that can work very well. However,
when a consistent, unified approach is needed for a variety of processes and variables, a functional standard provides a more usable approach.

API 2350, as currently written, draws a very narrow box around the application. It is industry specific and deals with only certain classes of petroleum fluids. When handling and storing Class I and Class II Fluids, the current API 2350 Recommended Practice on Overfill Protection for Storage Tanks in Petroleum Facilities\(^1\) provides a straight-forward, prescriptive solution. As a recommended practice in the industry, it sets a minimum standard for a company to follow. However, a prescriptive standard cannot foresee the individual issues in a specific location and application as pointed out in the Buncefield recommendation \(^1\).

That is where functional standards can be useful. The IEC 61511 standard for Safety Instrumented Systems (SIS) has been widely adopted to evaluate risk associated with safety related systems in a variety of applications across the process industry. Companies see two major benefits to applying the functional IEC standard even when a less restrictive prescriptive standard exists. First, they are aware that the functional standard will uncover other mitigating factors that may warrant additional safeguards, i.e. mitigate the specific risks associated with their facilities. Second, they use IEC 61511 to provide consistency in their approach to safety across facilities and areas of facilities.

### APPLICATION OF THE STANDARDS

#### API 2350 REQUIREMENTS

It must be noted that the API is in the process of revising API 2350 and that one of the major areas being addressed is in the area of correlation with safety standards\(^4\). We are addressing only the current (2005) version.

The API 2350 standard requires a formal approach to training and procedures that is consistent with safety standards and regulations and IEC 61511 specifically. While not as detailed in the “Safety Lifecycle”, it is clear that operators and procedures are critical and must be part of the overall approach to safety.

In terms of an overfill protection system it separates “attended operation” and “unattended operation”.

<table>
<thead>
<tr>
<th>Petroleum Liquids Classification System</th>
</tr>
</thead>
<tbody>
<tr>
<td>used by</td>
</tr>
<tr>
<td>• National Fire Protection Association (NFPA)</td>
</tr>
<tr>
<td>• The US Department of Transportation (DOT)</td>
</tr>
<tr>
<td>• US Environmental Protection Agency (EPA)</td>
</tr>
<tr>
<td>• US Occupational Safety and Health Administration (OSHA)</td>
</tr>
<tr>
<td>and others</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Class</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Liquids with Flashpoints below 100 °F</td>
</tr>
<tr>
<td>2</td>
<td>Liquids with flashpoints between 100 and 139 °F</td>
</tr>
<tr>
<td>3</td>
<td>Liquids with flashpoints equal to or greater than 140 °F</td>
</tr>
</tbody>
</table>

Table 1: Petroleum Liquids Classification System
For attended tanks, the basic monitoring system, with the backup layer of qualified personnel on site is deemed adequate. For unattended tanks, the additional layer of protection of independent safety detection (level sensor) and shutdown system is required.

**IEC 61511 REQUIREMENTS**

The IEC 61511 standard would not require a specific remedy but rather a performance level based on a Process Hazard Analysis (PHA) and determination of an acceptable risk factor for the application. The benefit of a functional standard is that it can take into account a wide variety of location and application specific issues. After the risks are determined, an analysis of available methods to mitigate those risks identifies what safety systems might be needed. Layers of Protection Analysis (LOPA) method is the most popular method for determining required systems and the resulting Safety Integrity Level (SIL).

For the attended tanks, the qualified personnel would constitute an independent layer of protection but as operators, would be limited to no more than one order of magnitude reduction in the process risk. For a SIL 1 requirement of the tank’s overfill safety function, no additional SIS system would be required which is consistent with the API Standard. For unattended tanks, timely operator intervention cannot be assumed and a SIL 1 requirement for the tank process would require an additional Independent Protection Layer. A separate Instrumented Safety Monitoring system as detailed in API 2350 could be designed to meet that requirement. If additional risks are identified that require a higher than SIL 1 SIS, then additional or higher SIL systems would need to be employed.

The IEC 61511 methodology is a way to validate the requirements and account for additional risk factors such as high volatility or proximity to other processes and personnel. This makes the systems consistent with the analysis and documentation in other process facilities using IEC 61511.

**SAFETY SYSTEM ISSUES IN TANK OVERFILL PROTECTION**

There are several SIS related issues that should be addressed with tank overfill protection.

**SAFETY RESPONSE TIME**

The safety response time in tank level is typically slow relative to other process safety applications. API 2350 gives a good description of response time and the effect on tank level alarm settings. However, the other consideration is that often the tanks are in more remote locations and therefore the human response time to emergencies may be delayed. This may increase the risk factors in the SIS Analysis.

**REDUNDANCY**

Redundancy on Process Safety Systems is done for one of three reasons, 1) either the safety system requires it to meet certification to a specific SIL level (i.e. 2oo3 architectures), 2) the user desires higher system reliability (i.e. there is an economic or safety penalty for going to a failsafe condition) or
3) at higher SIL Levels, IEC 61511 specifies a minimum redundancy level. Typically in Tank Overfill, the SIL levels are low and, more importantly, the penalty for shutdown is generally low as well. Therefore, redundancy may only be required if the system selected requires it for certification or to meet higher SIL levels under IEC 61511.

PROBABILITY OF FAILURE ON DEMAND (PFD)

One area not currently addressed by API 2350 but recommended by the Buncefield report, is the possibility of undetected failures in the Safety Monitoring System. In IEC 61511, the PFD is tied to the Diagnostic Coverage, i.e. how well is the device monitored for failures. By using devices that are either independently certified (TUV) or Proven-in-Use, the Probability of Failure on Demand for the system can be determined.

TESTING

API 2350 requires a formal testing schedule. In IEC 61511, the time between system proof testing (test interval) is the ultimate watchdog against undetected failures in the Safety System. If API testing intervals are used, then the IEC 61511 test interval used in the calculations must match in the analysis and proof testing must be carried out on that schedule.

APPROACHES TO A COMBINED SOLUTION

OVERFILL PROTECTION CHALLENGES

While monitoring and protecting an individual tank is not very complex, the tank location and use can present challenges in system design.

I/O COUNT

Tank Overfill Safety Systems present unique challenges for implementing a system. The safety system needs to be separate from the basic tank monitoring system. Therefore the number of Input and Outputs (I/O) at each tank is very low, typically 2 to 5 signals. Small, relay type or stand-alone systems can be used however; the advantages of electronic systems for communications and diagnostics make them attractive. Traditional Process Safety Systems have been designed for large, highly reliable, emergency shutdown systems and may not adapt to small, geographically separated systems with the need for high integrity but not for high reliability.

Additional challenges are presented by existing facilities where existing communication infrastructures may not be designed for creating a parallel safety system.

GEOGRAPHY

In addition to the small number of small I/O drops, many tank farms are spread over a large area or
located a sizable distance from the main monitoring site. This means a large, but separate communication path must be established.

These two issues combine to make a traditional approach to tank level monitoring and safety system implementation very expensive. However, by examining the needs of the system, alternatives exist that will achieve the protection intent of the system while keeping the cost structure more reasonable.

ARCHITECTURE

SYSTEM ARCHITECTURE

Traditional process safety systems for emergency shutdown functions are designed for large central systems with large I/O counts and high reliability. Architectures are generally 2oo3 or 1oo2D and minimize spurious trips. These systems do not lend themselves to the spread geography of a typical tank application. The lesson to be learned from Buncefield is that the solution should not be a lack of safety. On a tank farm, the economic cost of a spurious trip is often low, i.e. a delay in loading or unloading. Therefore in the system design we have to separate “Safety” which is the availability of the system to act when needed (demand) and “Reliability”, which is the number of times the system goes to a failsafe condition when the process did not demand it (spurious trips). The tank application will need the “safety” part but not necessarily extremely high “reliability”.

While each installation is unique, at the system level, two basic options exist for implementing a Tank Overfill Protection System in compliance with both API 2350 and IEC 61511. One approach is to use a small, non-redundant SIL rated Safety System can be placed at each tank or tank cluster with safety rated communications back to a central for reporting and alarm system.

![Figure 3: Independent SIL System at Tank](image)
A second approach is to use remote I/O located at each tank or cluster of tanks and communicate back to a central Safety CPU over safe communications. For either option, the system can be SIL rated and equipped with Hart or Fieldbus options for remote diagnostics and parameterization.

The use of smaller, modular and non-redundant, SIL rated systems provides the high integrity for Safety considerations while substantially lowering the capital costs. In addition, the communication options in electronic Safety Instrumented Systems should allow non-interfering connections to the monitoring SCADA or DCS systems through proven interfaces.

SAFETY COMMUNICATIONS

The cost of the safety system hardware can be overwhelmed by the cost of the communication network. If the monitoring is considered safety critical as detailed in API 2350, the safety portion of the system must extend to the safety monitoring package as well. This means that the data from the tank is transmitted in a failsafe manner to a central monitoring site. In order to maintain the overall Safety Integrity Level of the system, a high “safety” communication channel must be implemented. Several safety rated communications networks are emerging, for example, TÜV certifies ProﬁBus and ProﬁNet (Ethernet) with ProﬁSafe protocol for SIL 3 applications. Foundation Fieldbus is following with its certification. These safety protocols are
usually independent of the media and instead rely on high diagnostics on either end of the link to verify that the communication systems is working properly.

As mentioned, retrofit installations present particular challenges. While wireless has not been generally accepted for safety applications, the low penalty for spurious trips and the relatively slow response time requirements for tank applications allow longer communication cycles for a more reliable wireless implementation.

If an existing communication link is available on the monitoring system it may be possible to use the same infrastructure for the Safety communication in a non-interfering mode. This maintains safety while lowering installation costs.

**INSTRUMENTATION AND FINAL CONTROL ELEMENTS**

The traditional tank monitoring system can consist of a variety of inputs including Level, Pressure, Temperature and Flows. Depending on the requirements of the system for inventory, custody transfer or difficult fluids, the tank monitoring systems can become quite complex. When looking at process safety issues, simple is typically better. API 2350 only requires a level indication. After the SIL verification phase under IEC 61511, a simple level transmitter or point level switch may be adequate and many are available with a TÜV SIL rating. In addition, other sensors could be included in the SIS if they are deemed safety critical, either to the basic level SIF or to other defined SIFs.

Finally, the mitigation method, should the tank overfill protection be triggered will need to be
considered. Particularly at unmanned locations, an Emergency Shutdown Valve may need to be included in the Safety System.

CONCLUSION
In examining petroleum tank overfill protection, the API Recommended Practice 2350: Overfill Protection for Storage Tanks in Petroleum Facilities and IEC 61511: Safety Instrumented Systems for the Process Industry Sector both can be used to address the issues. API 2350 takes a prescriptive approach and IEC 61511 uses a functional safety approach. In light of some recent major accidents, the industry is moving to a more functional approach that addresses a wider range of issues. While API 2350 is being revised to reflect this trend, companies want to be consistent with both the API document and the more general IEC 61511. This gives them the ability to address more complex issues specific to the facility and also provides a consistency methodology across the safety landscape for other applications on the facility and across the enterprise. For companies wanting to meet API RPs and still provide consistent safety implementation and validation through the IEC 61511 methodologies, the standards can be combined to yield a solution that meets both. By careful examination of the core issues around tank automation, the restrictions around safety, and emerging technologies, systems can be designed to accommodate both of the standards and still manage to operational and budget constraints.
REFERENCES


