

Honeywell Process Solutions



Applying Buncefield Recommendations and IEC61508 and IEC 61511 Standards to Fuel Storage Sites

John Joosten
Global Product Manager Radar and Safety
John.Joosten@Honeywell.com

Contents

Introduction.....	3
Report Recommendations	5
Recommendation 1.....	5
Apply this Recommendation.....	5
Recommendation 3 and 6.....	5
Need for High Integrity	6
Apply this Recommendation.....	6
Apply this Recommendation.....	7
Apply this Recommendation.....	7
Recommendation 4.....	7
Apply this Recommendation.....	8
Recommendation 5.....	9
Apply this Recommendation.....	9
Proven-in-Use.....	10
Summary.....	11
References	12

Introduction

In Dec 2005, a massive explosion at the Buncefield oil storage and transfer depot in Hemel Hempstead, United Kingdom caused a large fire which engulfed over 20 large storage fuel tanks. The exact ignition points were not certain, but are likely to have been a generator house in the northgate car park and a pump house on the west site. Significant damage occurred to both commercial and residential properties in the vicinity and a large area around the site was evacuated on emergency service advice. The fire burned for several days, destroying most of the site and emitting large clouds of black smoke into the atmosphere. Over 40 people were injured; fortunately there were no fatalities.

The economic and environmental damage was substantial. An investigation was carried out by the UK Health and Safety Executive that resulted in the 45 page Buncefield Recommendation Report with 25 recommendations describing how to design and safely operate fuel storage sites.

This paper will explore some of the Buncefield recommendations along with the applicable safety standards and translate those into tangible solutions that can be applied to prevent such accidents from happening again.



Figure 1 Buncefield before and after explosion

Is This Unique?

Following a 2 year investigation, evidence showed that the explosion resulted from the ignition of a vapor cloud emanating from spilled unleaded motor fuel from an overfilled storage tank. Evidence suggests that the protection system which should have automatically closed valves did not operate. This resulted in an override of the high level safety switch responsible for stopping the tank filling, allowing petroleum to spill out of the tank.

Records show that overfilled or leaking petroleum tanks have been cited as the cause of an industrial accident almost every five years since the early 1960s.

Location	Date and time	Comments – background	Comments – explosion
1 Houston, Texas, USA	April 1962	'Severe leak' from a gasoline tank. Almost windless conditions. Ignition near adjacent highway.	Described as a 'blast', but no details are available.
2 Baytown, Texas, USA	27 January 1977	Overfilling of a ship with gasoline.	Few details are available, but it is likely that there would have been congestion.
3 Texaco, Newark, New Jersey, USA	7 January 1983 After 00.00 hrs	Overfilling of a tank containing unleaded gasoline. 114-379 m ³ (80-265 tonnes) of gasoline released. Slight wind, ignition source 300 m away.	Relatively uncongested area. High overpressures reported, but not quantified. Three minor explosions preceded the main blast.
4 Naples Harbour, Italy	21 December 1985	Overfilling of a tank containing unleaded gasoline. 700 tonnes escaped. Low wind speed (2 m/s).	Relatively congested area. The tank overtopped 1.5 hours before ignition. Various overpressures estimated from damage analysis, but they are minimum values (eg >48 kPa).
5 St Herblain, France	7 October 1991 04:00 hours	Leak of gasoline from a transfer line into a bund. Wind <1 m/s. 20 minutes delay, ignition in car park c. 50 m away. Volume of flammable cloud est. 23 000 m ³ .	Presence of parked petrol tankers may have been sufficient to generate turbulence. High overpressures produced, but not quantified.
6 Jacksonville, Florida, USA	2 January 1993 03:15 hours	Overfilling of a tank containing unleaded gasoline. 50 000 gallons (190 m ³ , 132 tonnes) released.	High overpressure produced, but not quantified.
7 Laem Chabang, Thailand	2 December 1999 23:25 hours	Overfilling of a gasoline tank. Few details.	High overpressure produced, but not quantified. Relatively low congestion in the area.

Figure 2: Incidents that have Buncefield similarities. Source: Buncefield final report

The repetition of these incidents demonstrates that it is difficult to learn lessons from the past. Additional risks are introduced as the industry faces an aging workforce and the retirement of trained, knowledgeable and experienced staff. There is a clear and urgent need for obtaining and maintaining knowledge on bulk storage safety and asset protection.

Report Recommendations

The Buncefield report recommendations cover both organizational aspects, such as job organization, management of change, monitoring and supervision, training and control room layout, as well as implementation aspects, such as how to apply overfill protection systems.

One challenge for process manufacturers is to map the Buncefield report recommendations with current applicable safety standards (IEC61508 / IEC61511 / ISA 84.1) to create a safe, reliable and cost effective overfill solution. This document explores some of the recommendations, indicates the relationship with the applicable standards and discusses how to interpret and apply those recommendations. The sections of the Buncefield report discussed in this paper are “**Systematic assessment of safety integrity level requirement**” and “**Protecting against loss of primary containment using high integrity systems**”.

The recommendations explored in this document include:

- **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.
- **Recommendation 3:** Operators of Buncefield-type sites should protect against loss of containment of petrol and other highly flammable liquids by fitting a high integrity, automatic operating overfill prevention system (or a number of such systems, as appropriate) that is physically and electrically separate and independent from the tank gauging system.
- **Recommendation 4:** The overfill prevention system (comprising means of level detection, logic/control equipment and independent means of flow control) should be engineered, operated and maintained to achieve and maintain an appropriate level of safety integrity in accordance with the requirements of the recognised industry standard for ‘safety instrumented systems’, Part 1 of BS EN 61511.
- **Recommendation 5:** All elements of an overfill prevention system should be proof tested in accordance with the validated arrangements and procedures sufficiently frequently to ensure the specified safety integrity level is maintained in practice in accordance with the requirements of Part 1 of BS EN 61511
- **Recommendation 6:** The sector should put in place arrangements to ensure the receiving site (as opposed to the transmitting location) has ultimate control of tank filling. The receiving site should be able to safely terminate or divert a transfer (to prevent loss of containment or other dangerous conditions) without depending on the actions of a remote third party, or on the availability of communications to a remote location.

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.**

Apply this Recommendation

This recommends developing one consistent methodology for terminal safety analysis. The IEC61511 provides such a common methodology for functional safety including the analysis and determination of the Safety Integrity Level (SIL). Using one common approach for terminal safety analysis allows a more transparent overview of the various applications and safety requirements resulting in a widely accepted and adopted method. This is also more cost effective to maintain and easier to audit by authorities.

Recommendation 3 and 6

Operators of Buncefield-type sites should protect against loss of containment of petrol and other highly flammable liquids by fitting a **high integrity, automatic operating** overfill prevention system (or a number of such systems, as appropriate) that is physically and electrically separate and **independent from the tank gauging system.**

The sector should put in place arrangements to ensure the receiving site (as opposed to the transmitting location) has ultimate control of tank filling. The receiving site should be able to safely terminate or divert a transfer (to prevent loss of containment or other dangerous conditions) **without depending on the actions of a remote third party**, or on the availability of communications to a remote location.

This is an important recommendation because it contains three very important aspects of the safety philosophy as defined by the IEC61508 and IEC61511 / S84.

Need for High Integrity

A device being used for any safety function (such as overfill protection) consists of hardware and software. If we observe the IEC61508 standard, there are two failure modes considered for safety related modules: random hardware failures and systematic failures

Random Hardware Failures

The effect of random hardware failures can be calculated by carrying out a Failure Mode and Effect Analysis (FMEA) on the module hardware. This FMEA will result in a Safe Failure Fraction (SFF): a percentage that identifies for how many random faults in hardware components, the module will automatically go to the safe state. The IEC61508 mandates that when using an overfill sensor in a SIL-2 function, this SFF must be >90%.

Random hardware failures can not be avoided: hardware components can and will fail. Those failures can only be detected by sufficient diagnostics. That is why today all major suppliers of Safety Instrumented Systems (SIS) now offer diagnostics-based systems typically with a SFF > 99%

Systematic Failures

Systematic failures are all failures unintentionally “designed-in” to the safety function. Example causes of systematic failures include human errors in:

- the safety requirements specifications,
- the design, manufacture, installation and operation of the hardware, and
- the design, implementation, etc. of the software.

Typically, 90% of all failures are systematic failures: software bugs introduced during hardware and software design. A level sensing device such as a radar gauge has a considerable amount of software lines of code and uses complex algorithms to be able to select the actual measured level out of a dynamic reflection diagram. The selection of a measured level is always an interpretation of the software algorithms.

Systematic failures can only be eliminated by using a very rigid development process both for hardware and software. This development process needs to be compliant to the IEC61508 standard that mandates validation activities during every step of the development process.

Only a design centre that has been qualified and certified by the TÜV will be able to deliver a “high integrity” overfill prevention systems compliant to the IEC61508 safety standards.

Apply this Recommendation

For adequate overfill detection, one should select a device that is developed by a certified hardware and software design center that is independent from the level gauge used as a primary level indicator and uses a different method of level measurement.

Automatic operating and without depending upon the actions of a remote third party

Numerous investigations have researched the ability of operators to be able to make good decisions under upset conditions. Typically, during normal operations and at the beginning of a shift, a healthy operator without stress will make a faulty decision 1 out of 10 times(10%).

When the circumstances are more difficult, such as at night time or during an abnormal situation, about 30% of operator decisions are incorrect. This is one of the reasons that the IEC61511 standard and the Buncefield recommendations use the word “automatically”. This goal is to remove the “human factor” from the safety functions for any safety critical activity. The IEC61511

prescribes a complete automated and autonomously independent safety layer to be used for critical processes such as tank overfill detection and prevention.

Apply this Recommendation

The overfill prevention system (consisting of overfill sensor, safety critical switching function (e.g. logic solver) and a valve/pump) should carry out the safety function autonomously, without any human interference.

Independent from the tank gauging system

Why is it so important that the systems used for overfill protection solution is independent from the tank gauging system? The process industries have employed a long and successful practice of applying redundant process control and safety systems to operate their profitable critical processes. Redundant process control systems and safety systems have achieved their superior reliability and high availability through the application of a very important architectural first principle entitled the "separation principle". The design criteria behind this principle are simple: separate safety and control.

The separation principle is not new. It was already recognized in the earlier eras of plant automation and later consolidated in the IEC 61508, the umbrella safety standard for all automated process applications. Some statements from that standard are very clear about this principle:

"Where a safety-related system is to implement both safety and non-safety functions then all the hardware and software shall be treated as safety-related"

...and...

"Caution should be exercised if non-safety functions and safety functions are implemented in the same safety-related system. It may lead to greater complexity and increase the difficulty in carrying out safety lifecycle activities (for example design, validation, functional safety assessment and maintenance)."

Apply this Recommendation

Dedicated safety relevant parts in any safety function, such as the actual overfill sensor and the logic solver in an overfill protection system, must be independent from the tank gauging system. Using the same primary measurement for monitoring the tank level for operational (custody transfer) as well as overfill protection is mixing two independent layers of protection in such a way that both will have the same systematic failures. This means that they can fail simultaneously.

Without true separation, certification to a higher SIL rating is needed, which means increased costs as the complete system needs to be compliant to this higher SIL rating.

Some suppliers of overfill protection systems promote the use of a second identical gauge and compare the result of the two gauges. Although that seems a thorough method for increasing safety, a major pitfall is that adding a second gauge will only detect some random hardware failures (<10% of the failures in a overfill sensing device). What is more, because of the identical circumstances (same temperature, same level, same product, same contamination) in which the two gauges are operating, the likelihood that systematic failures will be revealed at the same time will increase dramatically. This can result in overfill without being detected.

Comparing the results of the primary level measurement and the secondary level measurement will increase the safety and improve the proof test interval only if two different measurement principles are being used, such as radar and servo

Recommendation 4

The overfill prevention system (comprising means of level detection, logic/control equipment and independent means of flow control) should be engineered, operated and maintained to achieve and maintain an appropriate level of safety integrity in accordance with the requirements of the recognised industry standard for 'safety instrumented systems', Part 1 of BS EN 61511.

Apply this Recommendation

Analogous to the ISO standards on quality, the IEC61508 and IEC 61511 safety standards stress the need for quality measures on safety during the operation’s lifetime from fluid to fluid. The majority of measures are related to human behavior/tasks/risks.

Experiences, rules and disciplines are introduced to manage the risks related to employees in various operational disciplines which all contribute to the overall profitable operation of the company. The figure below shows the entire process from the concept phase to the decommissioning phase of a facility.

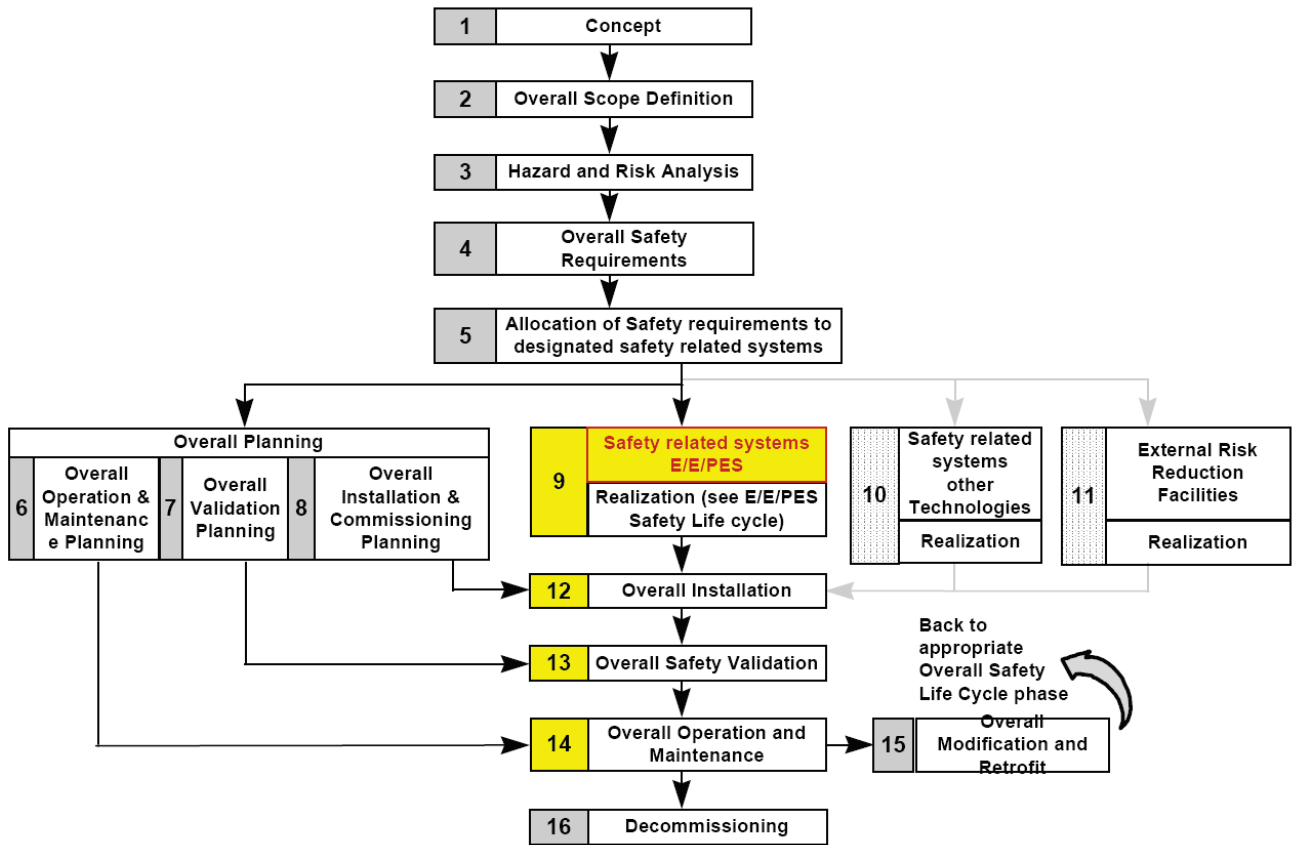


Figure 3: Opportunities to apply safety disciplines throughout the entire plant lifecycle

In order to be successful and safe, companies should adapt the above principles into their common processes and make sure through activities such as audits that those processes are the backbone of the daily working activities. Also, when implementing new functionalities, or changes to the existing facility, a thorough safety analysis should be completed that reveals any weak points in the safety protection layers.

Recommendation 5

All elements of an overfill prevention system should be proof tested in accordance with the validated arrangements and procedures sufficiently frequently to ensure the specified safety integrity level is maintained in practice in accordance with the requirements of Part 1 of BS EN 61511.

Apply this Recommendation

Every Safety Instrumented Function (SIF) in a facility will have a defined Safety Integrity Level (SIL). This is also applicable for overfill detection and prevention systems. Typically, for petrol-like storage tanks the SIL for such loops is SIL 1 or SIL 2.

The SIL for each loop is analysed and calculated during the HAZOP (hazard and operability) analysis. During this HAZOP, the risks are identified and risk reduction measures such as overfill protection, adequate process design or bunds are defined.

The equipment used to fulfil the safety needs for every loop typically consists of one or more sensors, a logic solver (Safety PLC) and an actuator. See the figure below.

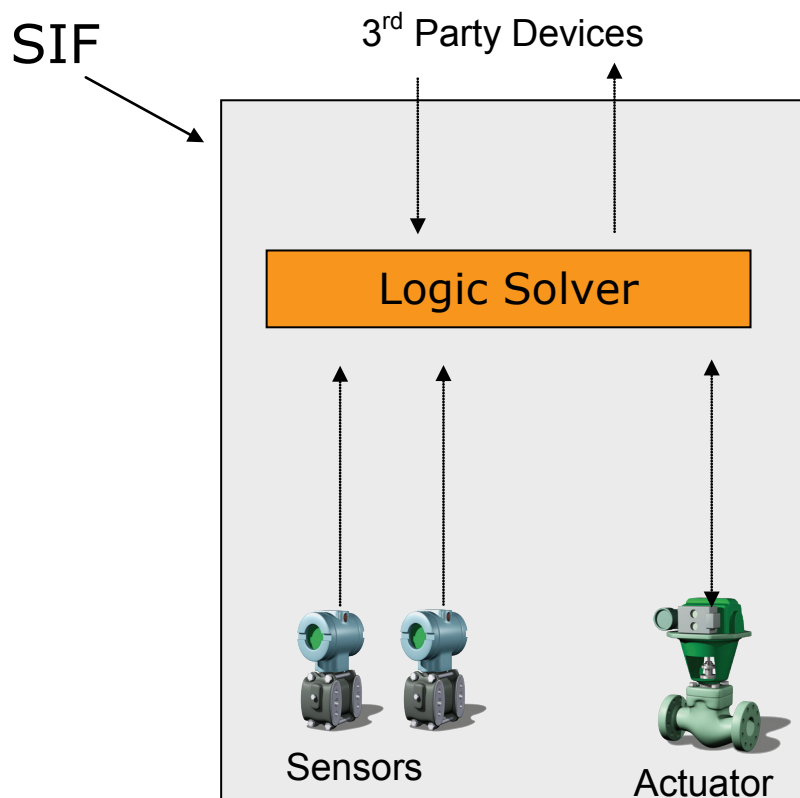


Figure 4: Diagram showing the equipment used to fulfill the safety needs for every loop

As an example, imagine a petrol tank that requires an overfill prevention system with a SIL-2 requirement. Just after the installation, commissioning and testing of the equipment, one can assume that the SIL is 2 at that time. But what will it be later, for example, after 6 months?

All hardware equipment is prone to deterioration. In particular, equipment used in harsh environments and subject to high or low temperatures (like on a tank roof) will change over time. Therefore, after a certain period, the SIL of the hardware used for overfill prevention systems can not be guaranteed to remain SIL 2. Conducting a proof test will guarantee that the hardware and software are still doing the intended job. Typically, a proof test will simulate overfill and to verify that the overfill detection and prevention systems are still able to function on demand. The figure below shows the SIL over time.

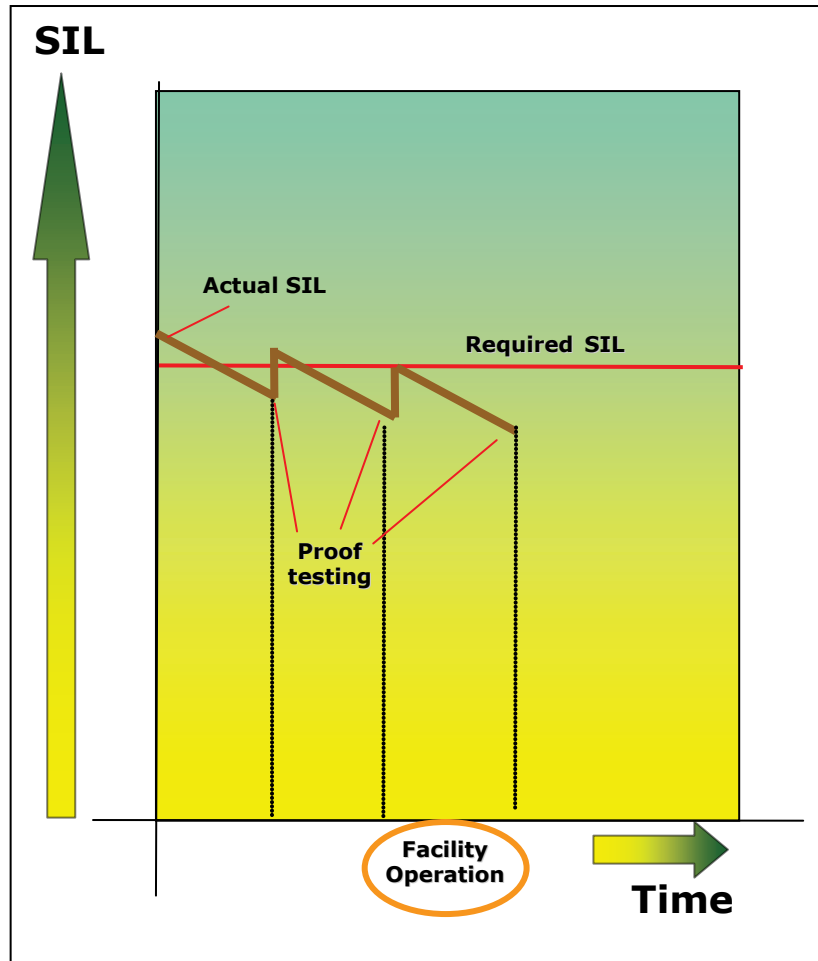


Figure 5: Safety integrity level over time

As indicated in the diagram, the SIL starts at an adequate level, but after some proof tests, the actual SIL will not comply anymore with the required SIL. A proof test will not deliver 100% test coverage. This means that for most overfill prevention systems the gauge needs to be removed from the tank and tested independently, which is a tedious and expensive activity.

But, is this always needed? It is needed for those systems that can not guarantee a sufficient proof test and diagnostic coverage.

For systems, however, that can guarantee a high diagnostic coverage, the proof test interval can be extended and there is no need to remove the gauge. Using two level measurements and comparing the results will increase the safety and improve the proof test interval (if two different measurement principles are being used)

Proven-in-Use

The IEC 61508 standard was published in the early nineties as an umbrella standard for safety functions. This standard had an extensive number of requirements and recommendations on the various safety aspects of the safety equipment, its installation, design, maintenance, etc. Unfortunately, most of the equipment installed on-site at that time was not designed in accordance with the 61508 standard, leaving plants to wonder what to do with the installations already safely running for years. It wasn't feasible to

shut down the plants or abandon all existing equipment. Instead, end-users adopted the proven-in-use clause which required no changes.

Proven-in-use should be used for older equipment and installations, but only for a limited number of years and only to bridge the gap between the standard timing (1999) and the availability of certified products. Ten years is an acceptable time for this transition. Unfortunately, both end-users and manufacturers of equipment used for safety functions are cutting corners and still using the proven-in-use principle for newly installed devices.

Summary

To combat challenges resulting from a sometimes uncertain economy, the terminal industry is taking aggressive action to stabilize profitability. History proves, however, that accidents in terminals occur over and over again. Adequate understanding and interpretation of the various measures, recommendations and standards is needed to implement a safe working environment at acceptable economic cost.

Only through the use of a systematic methodology that includes an integrated safety culture, long term reliable operation can be guaranteed.

References

- [1] Recommendations on the design and operation of fuel storage tanks (MIIB)
<http://www.buncefieldinvestigation.gov.uk/index.htm>
- [2] IEC 61511 Functional safety – Safety instrumented systems for the process industry sector
- [3] API RP 2350 Overfill Protection for Storage Tanks in Petroleum Facilities
- [4] IEC 61508 Functional safety of electrical/electronic/ programmable electronic safety-related systems

More Information

For more information about Honeywell's approach to safety at fuel storage sites, visit our website at www.honeywellenraf.com or contact your Honeywell account manager.

Automation & Control Solutions

Process Solutions
Honeywell
1860 W. Rose Garden Lane.
Phoenix, AZ, 85027
www.honeywell.com/ps

WP-10-3-ENG
April 2010
© 2010 Honeywell International Inc.

The Honeywell logo is displayed in a bold, red, sans-serif font.