

June 2009

# InTech



Scenes from the Buncefield, England explosion in 2005

Source: Royal Chiltern Air Support Unit

## High-integrity overflow protection

By Chris O'Brien

**Y**ear 2005 was a tragic year for level protection systems. First, there was the 23 March 2005 explosion at the BP Deer Park oil refinery near Texas City, Tex. Then on 11 December 2005, another explosion occurred, this time at the Buncefield fuel depot near Hemel Hempstead, U.K.

The resultant investigation reports for each produced a lengthy list of senior executive and plant management failures and inadequacies. However, when you look at the timeline leading up to these disasters, it is a failure of the level protection systems to perform-on-demand that failed to prevent the deaths of 15 people, injury to over 200 more, and the expenditure of billions of dollars.

### Setting expectations

Following the Buncefield incident, the U.K.'s Health and Safety Executive and Environment Agency conducted extensive investigations and issued a series of detailed reports over a three-year period. Included in Volume 2a of the final report is the section, "Protecting against loss of primary containment using high integrity systems."

The reports states, "Operators of Buncefield-type sites should protect against loss of containment of petrol and other highly flammable liquids

**FAST FORWARD**

- The level protection system failed, and 15 people died.
- The key items are sensors, logic solvers, final elements, software, and networks.
- You must show you were able to detect and record every dangerous failure.
- The alternative to self-certification is to use third-party certified devices.

## Vessel overflow protection systems seem so simple, so straightforward—that is until one of them fails to work properly and your plant is the six o'clock news

by fitting a high integrity, automatic operating overflow prevention system (or a number of such systems, as appropriate) that is physically and electrically separate and independent from the tank gauging system.”

The report continues, “Such systems should meet the requirements of Part 1 of BS EN 61511 for the required safety integrity level, as determined by the agreed methodology (see Recommendation 1). Where independent automatic overflow prevention systems are already provided, their efficacy and reliability should be reappraised in line with the principles of Part 1 of BS EN 61511 and for the required safety integrity level, as determined by the agreed methodology (see Recommendation 1).” British National Standard BS EN 61511 is identical to IEC 61511.

Following the BP Texas City, Tex., incident, four investigation reports resulted. Of these four reports, the one most referenced is the Baker Report. Though the Baker Report did not specifically address automated high-integrity level protection systems, it did reference the importance of proper shutdown system design and maintenance, and it referenced IEC 61511 as representing good-engineering practices.

The reports for both incidents estab-

lished unequivocal expectations regarding overflow protection—the application of the good-engineering practices and principles described in IEC 61511 is not an option. If that is not convincing enough, consider the National Technology Transfer and Advancement (NTTA) Act of 1995 requires U.S. federal agencies (i.e., EPA, FDA, OSHA, etc.) to recognize existing consensus standards, such as IEC 61511 and IEC 61508.

That means all U.S. government agencies must accept the premise of consensus standards, such as IEC 61511, and abide by the standard's requirements. That also means if you ignore using these consensus standards in their entirety and your plant experiences an incident, you have the burden of proving that whatever engineering methodology in use was at least equivalent to the consensus standards.

### Protection system traits

The underlying concept required of an automated overflow protection system seems so simple: If the level of a vessel reaches a pre-determined maximum, then stop the flow of liquid filling the vessel. Satisfying such a simple requirement occurs in toilets, clothes washers, and dishwashers every day, so what is the big deal?

The big deal is the liquid in toilets, washers, and dishwashers is water, not a highly flammable, possibly toxic, fuel or chemical. In addition, remember if the overflow protection system fails and there is even a minor incident, government investigators are going to want to see evidence you applied the principles of IEC 61511.

IEC 61511 is actually a process sector implementation of the international standard IEC 61508. The key principles of both standards are the:

- Safety lifecycle
- Safety Integrity Levels (SIL)

The safety lifecycle forms the central framework, which links together most of the standard's concepts and establishes the good engineering procedures necessary to design a robust safety instrumented system. Using the lifecycle design requires:

- Evaluating process risks
- Establishing Safety Instrumented System (SIS) performance requirements
- Analyzing the design of layers of protection
- Ensuring the SIS (if needed) is designed optimally to meet each identified process risk

SILs are the order of magnitude levels of risk reduction. There are four SIL risk reduction levels defined in the IEC stan-

dards with SIL 1 representing the lowest and SIL 4 the highest. The primary concern of IEC 61511 is the SIS, which consists of the sensors, logic solvers, final elements, software, and networks. It also addresses the interface between SISs and other safety and control systems and requires some kind of a formalized process hazard and risk assessment take place.

Specifically applying the safety life cycle and SIL principles to an overfill protection system requires:

- Use of a proven and approved methodology that considers the:
  - Existence of nearby sensitive populations and/or resources
  - Intensity and nature of filling and/or depot-like operations
  - Realistically establishing tank and gauging system expectations
  - Establishment of rigorous monitoring requirements
- Use of an appropriate SIL determination methodology
- Use of a high-integrity automated safety system as the means of protecting against loss of primary containment
- Intentionally separating physically and electrically the automated safety system from tank gauging systems
- Completion of periodic proof testing in accordance with procedures established during the overfill protection systems design
- Documented proof that regularly scheduled protection system reviews were conducted per applicable regulatory and standard's requirements

### API 2350's influence

The American Petroleum Institute (API) issued the first edition of API 2350 "Overfill Protection for Storage Tanks in Petroleum Facilities" in 1987. A second edition applied lessons learned and grew to include emergency spill prevention programs. The third edition built upon the second edition by addressing new and evolving technologies as well as Class I and Class II hydrocarbon liquids. The fourth edition, still in development, continues that experience and lessons learned tradition with special emphasis on the principles associated

with operations and the use of alarms as well as the interaction between operators and alarms.

IEC 61511 appears as a reference in several places in API's fourth edition, for instance Section 7.1, "AOPS Considerations," addresses existing and new Automated Overfill Protection Systems (AOPS). At press time for this article, the fourth edition was still in development, so the exact language remains undecided. However, "draft" language indicates the fourth edition will be very specific

## The American Petroleum Institute (API) issued the first edition of API 2350 "Overfill Protection for Storage Tanks in Petroleum Facilities" in 1987.

regarding existing and new AOPS installations. Current draft language states, "When installing a new AOPS, then the requirements of IEC 61511 shall be mandatory."

Notice it does not indicate it "should be" or "is optional," it clearly states it "shall be mandatory" to conform to IEC 61511 requirements.

Regardless of the exact final wording, when API 2350 fourth edition is released, it will undoubtedly reference IEC 61511, thus API 2350 will join IEC 61508 and IEC 61511 under the NTTA Act of 1995 further reinforcing regulatory agency insistence on the use of IEC 61511 for high-integrity overfill protection systems.

### Self-proven vs. certified

Automation designers often cite the reliability of existing overfill-protection systems as justification to use the same design and device manufactures for new applications. In their opinion, the performance of existing overfill-protection systems justifies reusing these "self-proven" or "proven-in-use" designs.

As noted, IEC 61511 is a process sector implementation of the international standard IEC 61508, therefore IEC 61511 often refers back to IEC 61508; meeting the requirements of "self-proven" is one such reference.

An owner/operators decision to "self-

prove" devices for a high-integrity overfill protection system must include a "self-certification" process that is well documented and fully conforms with both IEC 61511 and IEC 61508 requirements. Though neither IEC standard specifically outlines these requirements, the key elements of a self-certification program includes having:

- A clear description of each device's design revision information
- Reliability data for identical or very similar applications including appli-

cable conditions and/or restrictions for use of each device

- Results of operating software compliance as defined in IEC 61508-3
- Acknowledged competency to review the design aspects of both mechanical- and/or electrical-components including component failure modes,

## TERMINOLOGY

**API RP 2350:** Overfill protection for storage tanks in petroleum facilities

**IEC 61508:** Functional safety of electrical/electronic/programmable electronic safety-related systems

**IEC 61511:** Functional safety - Safety instrumented systems for the process industry sector

**National Technology Transfer and Advancement (NTTA) Act of 1995** leads the public and private sectors in coordination of standards and conformity assessment activities to meet the needs of U.S. industry in the global marketplace.

**SIL:** Safety Integrity Level is a relative level of risk-reduction provided by a safety function, or to specify a target level of risk reduction. In simple terms, SIL is a measurement of performance required for a Safety Instrumented Function. There are four SILs, with SIL4 being the most dependable and SIL1 being the least.

fail-safe vs. fail-danger, any claimed automatic diagnostics, and internal redundancy in order to produce a quantitative failure rate (This number will eventually plug into calculations that determine if a particular design meets its defined SIL requirements.)

- Acknowledged competency capable of combining sophisticated design analysis processes, tools, and testing methods with a thorough review of both the device original design and all subsequent modifications to the electrical, mechanical, and software aspects of each device with the intent of uncovering design errors
- Regularly conducted audits of device manufacturers change management processes for each device being used or being considered for use in an overfill protection system
- A detailed documented technical file or “Safety Case” describing how each manufacturer’s device meets each requirement of IEC 61508
- Procedures in place to verify each device meets functional requirements, is qualified (rated) for use in the expected environment, and the materials of construction are suitable for expected process conditions including actual test results from use in similar but non-safety critical applications

Because a self-certification program must rest on actual operating experience, IEC 61508 establishes the minimum operating experience hours necessary for each SIL level as:

- 100,000 hours for SIL 1
- 1 million hours for SIL 2
- 10 million hours for SIL 3

Certainly, meeting these requirements is onerous, but you must also be able to show you were able to detect and record each-and-every dangerous failure that occurred during these times.

The alternative to establishing a self-certification program is to use third-party certified devices in combination

with a through evaluation that ensures each high-integrity overfill protection system is well suited for the application.

There are a growing number of manufacturers offering devices certified for safety applications including overfill protection systems. Some of these manufacturers have invested the resources necessary to have a qualified third-party organization conduct a through investigation of a specific revision for a specific device. Upon successfully completing this investigation, that device revision is fully-certified per IEC 61508 requirements. Included with the purchase of these fully certified devices are the third-party certification and a detailed user safety manual that includes such things as device use restrictions.

The two qualified third-party certification companies are exida Certification (Geneva, Switzerland) and one of the TÜV companies (Cologne, Munich, and Essen, Germany).

Other device manufacturers have paid to have a third-party assessment conducted of a specific device’s field failure records thereby helping owner/operators meet “self-proven” requirements. Lastly, a few device manufacturers have chosen to self-certify their own devices.

### Lives saved, lessons learned

The message to designers of overflow protection systems is clear, what you must do in order to avoid your company from “being” the 6 o’clock news is:

- Understand and fully apply applicable good-engineering standards, such as API 2350, IEC 61508, and IEC 61511
- Embrace the principles of the safety life cycle and SIL as defined in IEC 61508 and IEC 61511



Source: Hertfordshire Constabulary

- Ensure the use of well-documented “proven-in-use” devices and/or specify devices that have been third-party certified per IEC 61508 standards

Lastly, everyone from senior executives to plant managers to operators and field operators to engineering and maintenance personnel to contractors must recognize and appreciate ignoring any or all of these points can result in death, injury, destruction, and possible criminal charges.

### ABOUT THE AUTHOR

**Chris O’Brien** (cobrien@exida.com) has over 20 years experience in the design and manufacturer of process and safety control systems. He holds five patents. His new book is *Final Elements and the IEC 61508 and IEC 61511 Functional Safety Standards*.

View the online version at [www.isa.org/intech/20090602](http://www.isa.org/intech/20090602).

### RESOURCES

#### Buncefield Investigation

[www.buncefieldinvestigation.gov.uk/index.htm](http://www.buncefieldinvestigation.gov.uk/index.htm)

#### Safety Instrumented Systems Verification: Practical Probabilistic Calculations

[www.isa.org/link/SISV\\_pdf](http://www.isa.org/link/SISV_pdf)

#### Baker Report

[sunnyday.mit.edu/Baker-panel-report.pdf](http://sunnyday.mit.edu/Baker-panel-report.pdf)

#### A comprehensive list of devices with varying degrees of third-party certification/review

[www.exida.com/applications/sael/index.asp](http://www.exida.com/applications/sael/index.asp)

Reprinted with permission from InTech, June 2009. On the Web at [www.isa.org](http://www.isa.org).

© ISA Services, inc. All Rights Reserved. Foster Printing Service: 866-879-9144, [www.marketingreprints.com](http://www.marketingreprints.com).