

Incidents Triggered by Failures of Level Sensors

Silvia M. Ansaldi, Patrizia Agnello, Paolo A. Bragatto

INAIL Italian Workers' Compensation Authority DIT Department of Technological Innovation Centro Ricerca Monteporzio Catone (Rome) Italy

s.ansaldi@inail.it

Level gauging is a basic item of automatic and manual systems for preventing the overfilling of hazardous materials from atmospheric storage tanks. Failures or misuses of these sensors may trigger severe accidents, such as the Buncefield disaster in 2005. Some thirty short reports of minor incidents, near misses and mishaps triggered by failures of the level gauging system, have been found in the documents acquired in recent years during inspections at industrial establishments in the framework of Seveso legislation. They have been investigated, using advanced sematic methods, to understand whether tanks' operators have implemented the lessons learnt from Buncefield disaster. Among the analyzed documents, in a few cases a serious incident was avoided only by luck, while in other cases the event was very "far" from a real accident, because the resilience of the other safety barriers. The method developed to analyze the collected documents may be useful also to analyze, within the safety management system, the near misses triggered by a sensor failure.

1. Introduction

Sensors play a very important role in all chemical process industries. Among the many sensors, the most popular is the level gauge. Even though quite simple it is essential to prevent severe accidents, including the overflow of hazardous materials from atmospheric tanks. Because so simple and important, the present paper focuses only on these sensors and related accidents.

1.1 Importance of level gauges in process industries

A level sensor, basically, detects the height of the free surface of a liquid, which is assumed horizontal in its containers because of gravity. The measurement may be point values or continuous. A continuous sensor measures level within a specified range and determines the exact amount of substance, while point-level sensor only indicates whether the substance is above or below a sensing point. Level sensors are available or can be designed using variety of sensing principles. Since the beginning of industrial era, the most usual systems for level measurement have been based on floating items. These devices may be very simple and cheap indeed, but a great variety of measuring instruments have been developed in recent decades, to provide the process industries with systems adequate for different needs and budget. The available systems are based on very different physical principles. Sensors for point level detection may be based on Pneumatic or Conductive devices. Sensors for either point level detection or continuous monitoring include Ultrasonic, Capacitive, Optical and Microwave devices. Continuous measurement of liquids include Magnetostrictive, Resistive chains, Magnetoresistive, Hydrostatic pressure, Air bubbler and Gamma ray. The indication of the level value may be only local (on-site), but most of the time the signal is transmitted to the control room, where it is used for display, recording, alarm, adjustment. The level measurement often controls an automatic interlock system, such as a valve automatically stops the entering flow in a tank, when the higher level is detected. The average failure rates of the level sensors is also an essential parameter for fault tree calculation and, consequently, for the quantitative risk assessment.

1.2 Recent disasters triggered by level gauges

Many major accidents in process industries have been triggered by failures of level gauge. The most typical accident is the overflow of a hazardous fluid from a tank, due to either a wrong or lacking measurement of its level. This type of accident is well known in the history of process industries, but, unfortunately, it continues to

repeat over the years. The best known accident in recent years is the disaster, that occurred on December 11th, 2005 at a large tank farm in Buncefield (UK) (Nicholas & Whitfield 2013). The immediate cause of the accident was the overflowing of a petrol tank, triggered by the automatic tank gauging system, which got stuck indicating 2/3 full level, and by the independent high level switch, installed for overflowing prevention, which had been left unintentionally deactivated after a previous test (Paltrinieri & al 2012). A similar disaster occurred again a few years later October 23rd, 2009 at the Capeco Refinery in Portorico (CSB 2015).

1.3 Lesson learnt from recent accidents

After the Buncefield disaster, the Process Safety Leadership Group (PSLG), set up by the Competent Authority, issued in 2009 a report on "Safety and environmental standards for fuel storage sites" (PSLG 2009). According to this document, the overflow prevention system should be engineered, operated, tested and maintained to achieve and maintain an appropriate level of safety integrity in accordance with the requirements of EN 61511 (2003). The target SIL (Safety Integrity Level) of the safety instrumented functions assessment should be determined by suitable methodology, such as the LOPA (Layers Of Protection Analysis). According to Fanelli (2012) the flammable storage tank normal fill level, high alarm level and high-high level trip/alarm level should be set in compliance tank capacities and operating levels (designated according to the guidance) not to routinely operate on alarms. The management systems for maintenance of equipment and systems should include the procedures for periodic proof testing of storage tank overflow prevention systems as well as the procedures for implementing changes to equipment and systems to ensure any such changes do not impair the effectiveness of equipment and systems. Furthermore, advanced and modern sensors should be installed, aiming to increase, in particular, the dependability of tank level gauging systems.

2. Objectives

Level measurement in no pressure tanks is a well-known technology, but accidents continue to repeat itself and lessons learned in the past are quickly forgotten. For this reason, it is interesting to investigate how the issue deals with the experience of operating Seveso sites. An interesting source of knowledge, in particular, can come from reports of near misses, collected during the inspections at chemical establishments, in the framework of Seveso legislation. The main scopes of the research were:

- a) To understand whether the importance of the level meters for the prevention of major accident is taken into due consideration by the operators of Seveso, as suggested by the guidelines in previous paragraph.
- b) To promote the awareness of the importance of the level sensors for the accident prevention, in the process industries, and provide the operators of Seveso establishments with a few suggestions for strengthening the level measurements and the prevention of overflowing and similar accidents.

2.1 Level sensors within the safety management system

To achieve the second objective, the present study focused on the near misses involving a failure in the level measurement of a hazardous liquid. The management of near misses is a pillar of the safety management system and may provide a valuable source of knowledge. Events apparently negligible may give an early warning of latent accident conditions. For such a reason, the research attempts to answer the question whether it is possible to use the near misses to understand the weakness in the management of level measurement and prevent events with more severe consequences. It is important to understand if the most serious consequences were avoided by pure luck, or because other security barriers have worked well. In other words, the operator should understand how a potential accident was close. For this purpose is essential to have a sort of "metric" to measure the distance between the real recorded "near miss" and potential accident scenarios in the risk assessment document. The "distance" must take into account the other safety barriers that have prevented the occurrence of a more serious accident. The actual consequences are not taken into account, especially if they are only due to a "lucky" condition, rather than the effectiveness of the other barriers. The "distance" from accidents could be interesting for any type of near misses and incidents, but in this study is restricted to the issue of level sensors.

3. Materials and Methods

3.1 Materials

Some thirty short reports of incidents, near misses and mishaps, were acquired during inspections of plants and depots throughout Italy. Incidents involve just failures or misuses level gauges installed at atmospheric tank containing mainly flammable or toxic liquid. Most reports come from distinct establishments, except of some cases where similar events occurred at the same site more than once. Most events occurred years after

Buncefield accident. The reports follow a format, which drives the detailed analysis of technical and procedural barriers involved in the event.

A few extra reports extracted from the public access incidental databases, such as EMARS of MAHB/JRC and the ARIA BARPI, have been included as a sample in the study, just to have a comparison between Italian and foreign experience.

3.2 Method

In order to study the available documents, a systematic search of the keywords has been done. Advanced or “semantic” search methods have been applied, including automatic control of synonyms and compounds, different language dictionaries, redundancies, and context-dependency. The first activity has been the identification of the most representative terms, their classifications and relations, which will drive the search.

The tool used is IBM OmniFind©, which has all search capabilities as well as the automatic summaries, based on input keywords. A very important feature of OmniFind© is the semantic proximity calculation. It is used to define the “similarity” or “proximity” of different documents and it is based on the “min-hash” technique. According to the MinHash algorithm, proximity is defined as:

$$P_{a-b} = \left(\frac{K^a \cap K^b}{K^a \cup K^b} \right) \quad (1)$$

Where P_{a-b} is the proximity of event records a and b ; K_a and K_b are key sentences singled out, respectively in the event records a and b by the search engine.

In order to apply the proximity index, automated summaries are essential. For trustable summaries, the possible keywords should be organized a priori. Synonyms should be duly considered. Proximity index defines a metric for this space, thus it is possible to build a set of similar events, which may be considered “frequent failures”. A cluster of failures is eligible as “frequent failure” if the number of events is > 3 and all proximity are higher than 0.67. The minimum of the proximity index is defined “radius of the cluster”. Using the strength of advanced search, a number of clusters may be obtained, which may be considered typical or frequent cases. For the correct application of the technique, it is essential the management, within the analysed texts, of synonyms, ambiguity of meaning, different languages, redundancies, and context-dependency. A number of keywords have been used to obtain automatic summary and to correctly apply the technique of “min-hash”.

Underlying to this method, there is the assumption that the distance between the documents corresponds to the distance between the events. It is acceptable, however, because the documents are formally as based on a unique format. The idea of a distance between the accidents, however, is not new, because Gnoni & Lettera (2012) already proposed it, in a different shape. The use of “semantic distance” is not completely new in incident investigation, as Bragatto & all (2015) to find frequent failures in pressure equipment have successfully used it.

4. Results

4.1 Topics definition

The domains considered for the search are the following: level measurement types, equipment affected by such devices, causes of event (near miss or incident). Further to them, the analysis of possible consequences and protective barriers, and the different hazards of substances involved are other topics considered.

For each topic, its lexicon is defined through a set of keywords, synonyms, translations in different languages, and their relations, which may avoid ambiguities or correspondences out of context.

The level devices are characterized by functionality (e.g. measurement, sensor, control), some characteristics (e.g. gauge, alarm, interlock), and parameter (i.e. level).

There are different types of causes considered: device failure, device absence, bad management or human factors, wrong device installation. Negative events (e.g. overflow, spill, and leak) are also considered, pointing out if some protective barriers or human interventions were involved to avoid worst consequences (e.g. fire or explosion), depending on the dangerousness of the fluid involved.

The next paragraph shows and discusses in major details some of the search results. For all incidents founded in such results, the distance measure with respect to the meaningful major accident occurred (e.g. Buncefield) shows how far (or close) they were. Further searches are able to clarify if the most serious consequences were avoided by lucky situations or by right working of protective barriers.

4.2 Frequent failures

Some thirty short reports of near misses, in a collection of more than 480 documents, describe events involving level devices, twenty of which connected to atmospheric vessels or tankers.

Below, some tables show the results of search queries using different domains, e.g. device characteristics, types of failure.

The first column contains the percentage of the tokens found with respect to the search, which means to measure how much the events are close or distant from the query. The second column specifies if the event refers to an accident or an incident (or near miss) report, identified by a number. Finally, the third column contains the dynamic summary, automatically provided by the system OmniFind©; the items matched in the defined domain are highlight in different colour. They correspond to the keywords belonging to different domains, such as the device characteristics and functionality (violet^V), parameter (light blue^B), failure or other types of event (yellow^Y), equipment (green^G).

Table 1: A set of “similar” accidents and incidents due to device failure

Distance	Id	Search results
100%	ACC01	...was being filled Dec. 11 at 3 am the level ^B gauge ^V remained static ^Y while the output remained the same 5 20 am the tank ^G began to overflow 5 50 am The filling of another tank ^G stops and the output to ...Neither ^Y of the 2 alarm ^V systems connected to the filling level ^B detectors ^V of tank ^G 912 operated ^Y level ^B gauge ^V high ^V level ^B ...The supply was thus not stopped automatically and the malfunction ^Y was not reported by the supplier's system as it should have been via the high ^V level ^B alarm ^V ...
100%	N01	... Anomaly ^Y generator ^G ... during the start-up fortnightly generator ^G highlights the failure ^Y of the fuel level ^B gauge ^V . Malfunctioning ^Y fuel gauge ^V generator ^G Contacted maintenance company ... operation of the generator ^G ...
86.60%	N02	... Rupture ^Y of propeller meter ^V during load Collection of the product Realization lock system load in case of high level ^V in tank ^G ... During the loading of a tanker ^G was checking to overfilling to break ^Y the meter ^V ...
86.60%	N03	... Anomaly ^Y of high level switch ^V of the tank ^G ... during a maintenance scheduled session on the real simulation of high level ^V in the tank ^G ... It was found the failure ^Y of the alarm ^V level ^B . Critical technical systems: alarm high-level ^V tank ^G Scheduled replacement denied the opportunity to load the tank ^G ...
86.60%	ACC02	...high ^V level ^B alarm ^V button plate by mechanical contact with the floating roof relayed to the control room was activated while the gauge ^V was indicating a level ^B of ... for a high ^V level ^B mark set at 14 6 m. Nonetheless the tank ^G continued to be filled and at 4 45 pm the gauge ^V posted a level ^B stabilized at 11 135 m. An error message notifying the disagreement between tank ^G status filling and gauge ^V stability was sent to the ...The tank ^G overflow was caused by both a defect ^Y in the level ^B gauge ^V due to ...
83.22%	N04	.. During unloading of sulfuric acid in the tank ^G ... there was a spill of raw material from the top vents the electronic ^V level ^B indicated 90. Re-calibrated ^Y measuring instrument ^V however present in list of critical components subject to scheduled periodic maintenance ...
77.76	N05	Formaldehyde spill from the tank ^G confined within the bund ... The failure ^Y of the level ^B device ^V to measure fill caused the spill by the top vent of about 400 ... Technical systems critical first inaction ^Y level ^B sensors ^V ...

The table 1 shows an example of results from a search query that looks for the types of failure occurred to the level devices. The query expression is based on key factors of Buncefield accident, i.e. the conditions that caused the accident, the state of devices and the equipment involved. For this reason, the table starts with a summary from Buncefield report, while the others, considered similar events, are ordered by the distance from the first result.

In the list, there is another accident (ACC02), extracted by Aria database and considered similar to Buncefield event; while the other results correspond to incidents, no-conformity, or near misses, collected in Italian establishments by our inspectors. Usually, these reports describe the events briefly, and, unlike the accident report, may do not contain detailed information such as specific types of failure occurred or substances involved.

Some of the results in table 1 refer to generic “failure” (or anomaly or malfunctioning) without specifying the real nature of such a failure, e.g. N01, N03, N05; while one deals with a “rupture” N02 and another N04 requires a re-calibration of the sensor.

Another interesting point is related to the activities that were going on during near misses or incident reporting. During maintenance activities some anomalies have been revealed, see N01 and N03, both of them points out the needs to make a plan for controlling such devices. N02, N04 and N05 occurred during load/unload

operations. In N04, the operator noticed that the instrument needed a re-calibration, but also recognizes it is a critical component and therefore require a “periodic maintenance”.

Looking at the consequences, all were potentially close to be accidents, three of them, N02, N04 and N05, had an overflow of hazard fluid and occurred during operations. In those cases, released materials were not highly flammable and bund walls were adequate to avoid major consequences.

The table 2 shows the results of a query done for looking incidents or near misses related to the lack of device. All are incidents, since they give rise to some consequences, which vary from minor leakage (N08) to overflow of a fluid. In all cases, it has pointed out the needs of installing a device for controlling the level, for monitoring both the containment and the transfer operation of a fluid. It is also interesting to note that some reports suggest the installation of devices with special characteristics, e.g. “radar level transmitter”.

Table 2: A set of “similar” incidents due to lack of device

Distance	Id	Search results
100.00%	N06	... During the refilling of the water operations in the treatment tank^G leaving the tap running. The tank^G is overfilled and starts to overflow on the ward floor. ... Actions envisaged programmed installed^Y high-level sensors alarmed^V about the treatment tanks^G ...
86.60%	N07	... Spill sol. thiosulfate nh4 tank^G .. due to lack^Y of lock high^V level^B occurred event of spill product critical technical systems ... Implementation^Y of dedicated level^B control system^V with automatic recycling pump block ...
86.60%	N08	... Erosion of the inner wall of the electrodeposition bath^G Install^Y the level^B probe alarmed^V
86.60%	N09	... Lacking^Y technological upgrading plant ... Technical intervention^Y made with alarm^V level^B on the tank^G Installation^Y reported in ...
84.99%	N10	... Lack^Y of a signaling^V system of high-level^V values ... Installed^Y a radar^V level^B transmitter^V on tanks^G with control from the control room, and high-level^V reporting ...
76.34%	N11	... Release of caustic soda from tank^G ... The restart of the pump to fill another tank^G caused overflowing of S1411. ... Plant safety change to install^Y a valve and a level^B switch^V implemented on S1411...

Almost all of the establishments dealt with these results are small sized, and the incidents occurred in quite recent years, between 2004 and 2011, therefore the technology of such types of devices should be already available and known. The reasons why such devices lack are not always clear, perhaps, the economic crisis might have interfered with the choices of investments; on the other hand, the examined incidents report simple type devices to monitor the level of a fluid, only few cases refer to sensors that are more sophisticated.

Table 3 A set of near misses related to human factors wrong actions

Distance	Id	Search results
100.00%	N12	... The meter^V at the highest^V level^B intervened^Y by stopping the pump and the discharge but incorrect operation of the measuring gauge^V installed^Y on tanks^G containing liquid waste to prevent overflowing of the ... Modify plant, to ensure the correct activation^Y of the meter^V at the highest liquid waste level^B in the tanks ...
100.00%	N13	... Value high-level^V tank^G with beeper^V the operator switch off^Y the alarm^V and temporarily did not follow the steps of operating instructions ... Upon reaching the extent of a very high^V level^B corresponding to the 95 contents of the tank^G took place the wastewater spill... Blocks^V to the highest^V level^B included in the critical instrumentation control plan ...
86.60%	N14	... Leakage of the product from the coupling flange of the collecting tank^G contained alcohols ... For maintenance work on the tank^G the alarm^V of high-level^V had been switched off^Y ...
84.60%	N15	... Malfunction in the level^B sensor^V for improper placement^Y of the loading arm Ensure that exist and are implemented training programs and exercises to improve the operator's behavior ... Use of absorbent material for the recovery of the spilled product...

The table 3 depicts a different query, the objective was to search the cases where the sensors might have worked correctly, but for some reasons, due to either human error or improper organization, incidents occurred.

The reports do not refer to any sensor failure, so that it is reasonable to think about likely right operation of sensors. Indeed, the first two summaries contain some words (“highest level intervened”, “beeper”) that point

out the sensors operated well. In the first case, the sensor was able to block the pump for stopping the transfer of a fluid into a tank, but too late and the overflow of the substance could not be avoided, the action planned is a plant modification to install the sensor in a right position to ensure its correct activation.

The N13 report tells that an operator switched off the alarm; while the second level sensor, installed to waste basin, was correctly treated, but the fluid was already leaked. N13 and N14 have in common that the sensors were off-line, even if in the second case it was a correct action of the maintenance activity, but the operator forgot to switch it on at the end of the work (something that sounds familiar with “unintentional deactivation of the sensor”, taken place in Buncefield). In both cases, the operators did not follow the operating instructions and maybe did not fully understand the importance and criticality of such sensors and alarms.

5. Discussion

Among the studied reports, in a few cases a serious incident were avoided only by luck, while in other cases the event was very “far” from a real accident, because other barriers (technical or procedural) worked well and the system was able to resist. A detailed statistical picture, which was not in the scope of the paper, has not been outlined, but the results has highlighted a number of frequent dangerous situations, which in the future could lead to new disasters if the lessons learnt from Buncefield will not be implemented diligently by the duty holders. In particular, it is worrying to see that we continue to prefer the cheaper technologies without taking account of reliability and safety.

6. Conclusions

A few technical solutions for gauging systems and overfill prevention may be poor due to the economic crisis of the present decade and to the small size of most Italian enterprises; but it is, anyway, essential for Italian control bodies, in the framework of Seveso III legislation, to promote the awareness of the importance of overfill prevention in process industries.

The semantic search engine has been demonstrated suitable to extract from a set of documents as much knowledge as possible. In the present paper, a specific method has been developed to “measure” how much a minor incident or a near miss has been close to a potential disaster. This capability could be very useful also for improving the study of the near misses within the safety management system. The method could be applied to understand the distance of a near miss, triggered by a sensor failure, from the top events identified in the risk assessment. Thus, the system manager could understand the resilience of safety barriers and, consequently, prioritize the technical interventions and the training programs.

In order to avoid the same accidents recur at a distance of years, it is necessary to revive continuously knowledge and increase operators’ awareness. The discussion of anomalies and near misses in the safety management system could be exploited to do that.

Reference

- Bragatto P, Agnello P, Ansaldi S, Artenio E, Delle Site C, 2015 Reviving Knowledge On Equipment Failures And Improving Risk Management At Industrial Sites, *Journal of Applied Engineering Science* 13 (4), 271 - 276
- Fanelli P, 2012, Safety and environmental standards for fuel storage sites: How to enhance the safety integrity of an overfill protection system for flammable fuel storage tanks, *Chemical Engineering Transactions*, 26, 435-440.
- Gnoni M. and Lettera G, 2012, Near-miss management systems: A methodological comparison, *J. of Loss Prevention in the Process Industries*, 25(3), 609-616.
- Nicholas M. and Whitfield A. 2013, The Buncefield accident and the environmental consequences for fuel storage sites and other sites in the UK regulated under the Seveso Directive, *Chemical Engineering Transactions*, 31, 457-462
- Paltrinieri N, Øien K. and Cozzani V. 2012 Assessment and comparison of two early warning indicator methods in the perspective of prevention of atypical accident scenarios, *Reliability Engineering and System Safety* 108 21–31
- CSB U.S. Chemical Safety and hazard investigation Board, 2015, Final investigation report on Caribbean petroleum tank terminal explosion and multiple tank fires, <http://www.csb.gov/caribbean-petroleum-refining-tank-explosion-and-fire/>
- IEC 61511, 2003, "Functional Safety: Safety Instrumented Systems for the Process Industry", IEC CH
- PSLG Process Safety Leadership Group, 2009, Safety and environmental standards for fuel storage sites Final report, <http://www.hse.gov.uk/comah/buncefield/final.htm/>