

INSTRUMENTATION & CONTROL DISASTERS – LESSONS LEARNED THE HARD WAY

Paul Gruhn, P.E., C.F.S.E., L&M Engineering, Houston, TX

Abstract

Engineering is a bold discipline. Engineers are always reaching for new heights, trying new materials and reaching for greater efficiencies. Unfortunately, part of that process means we occasionally exceed known boundaries. It is regrettable, but it would appear that human nature requires that we learn “the hard way”. It is only when expected conditions are exceeded, and things fail as a result, that we actually learn where we went wrong. There are valuable lessons to be learned from failures and there are plenty of examples of failures of instrumentation and control systems, such as the Brenham gas explosion, the Ocean Ranger, Chernobyl, the Mars Polar Lander and others. This paper will cover six disaster examples and ways to avoid them in the future.

Introduction

Many books, papers and reports have been written about accidents in a variety of industries (1-17). Trevor Kletz stated, “Accidents are not due to lack of knowledge, but failure to use the knowledge we already have”. It is the author’s experience that few instrumentation and control professionals are aware of the wealth of information available to them and all that can be learned from it. It is human nature to feel “it won’t happen to me”. However, it is this very complacency and overconfidence that has led to many accidents. James Belke (US EPA) stated in a recent report (3):

“From the perspective of the individual facility manager, catastrophic events are so rare that they may appear to be essentially impossible, and the circumstances and causes of an accident at a distant facility in a different industry sector may seem irrelevant. However, from our nationwide perspective at EPA and OSHA, while chemical accidents are not routine, they are a monthly or even weekly occurrence, and there is much to learn from the story behind each accident. Furthermore, when we look beyond the obvious to the underlying systemic causes of an accident, we see that the same root and contributing causes keep popping up again and again.”

The risks involved in our industries are simply too great to be learned by trial and error. We must learn from the mistakes of others.

Brenham Gas Explosion

The Brenham gas explosion occurred in 1992 northwest of Houston. An underground salt dome was used for the storage of LPG. The control room was located 90 miles away. There was no automated remote way to shut the well in. There was no local breathing apparatus at the site. There was no flare system to burn off escaping gas. The operating company did not have an accurate estimate of the size of the gas inventory. Back flow out of the well was detected with a single pressure switch. The pressure switch had a rated operating range of 160 to 2,000 psi, yet the operators had the setpoint set at 100 psi. Operators reported in their depositions that half the time they tested it, it didn't work. And they didn't *do* anything about it! The switch was also not maintained properly. There was a back flow out of the well that wasn't detected. A car drove into the gas cloud and ignited it. The blast killed 3, injured 23 and caused more than \$6.5 million in damages. The explosion had an estimated force of a three-kiloton bomb and was heard 100 miles away. A jury recently awarded \$138 million in punitive damages and \$5.4 million in compensatory damages.



Figure 1: Aerial View After the Brenham Gas Explosion

Questions Raised

1. Do you have an accurate indication of your capacity and/or throughput and is it within your design limit?
2. Are your safety devices installed, set, functioning and maintained properly? Are your maintenance records adequate enough to indicate if they weren't?
3. Do you have adequate safety layers?

Ocean Ranger

The Ocean Ranger was the largest floating offshore drilling rig when it was built in 1976. It sank off the eastern coast of Canada in 1982 with the loss of all 84 aboard. (It was not a good time for the offshore oil industry. In 1980 alone there were 22 rigs reporting fires, blowouts, capsizes, or sinkings.)



Figure 2: Ocean Ranger

The rig's support legs were 40 feet in diameter and used for storage and working compartments. The designers located the ballast control room in one of the smaller middle legs 27 feet above the water's surface – within wave-splashing range of the ocean. The operators needed to observe the draft marks on the outer legs, so the ballast control room had 4 glass windows. These windows could not be opened, but the glass could be broken under stress. (The glass was thinner than specified.) Operators used buttons that operated electric solenoids that controlled compressed air that ran down pipes that controlled valves in the pontoons. The valves connected pumps spaced along the pontoons that used seawater to control the trim of the rig. The rig had a mechanical

backup system installed during construction (as an afterthought). It was designed to bypass the electrical ballast control in the event of an electrical failure. Operation of the system was not documented. The operator was not formally trained on either system. His understanding of the backup system was backwards. (Mechanically operating the solenoids opened the valves, not closed them, as he thought.)

At the top of each larger outer leg was a huge chain locker used to store wire rope and anchor chains. The top of the lockers had large holes (5 feet across) used to feed out the rope and chains. There were no means to close these holes and no indication if the lockers began to fill with water.

The rig was stationed over 180 miles offshore in the North Atlantic. The rig had three (possibly four) working lifeboats, ten life rafts, and a helipad. There were no full-immersion exposure suits. The crew had not trained or attempted evacuation during a storm. The only way to survive would be to get everyone in the lifeboats and into the water safely – not an easy thing to do during a storm.

The rig crew did not ignore the approaching storm and they were securing the rig. A few waves reached 50 feet and one of them blew out a window in the ballast control room. The steel storm covers over the windows were not in place. Salt water shorted out the electrical control panel and there was no way to dry it out. The mimic panel indicated valves were opening and closing by themselves. Power to the panel was turned off one hour after the event forcing all valves to go to their closed position. (In hindsight, power should have been shut off immediately.) Three hours later, they restored power to the panel, exactly why is not known.

The rig continued to list out of balance. The operators did not fully understand the implications of their actions. Eventually, water started entering the chain locker at the top of one leg and the larger storage compartment below. There were no indications of this happening. This made the rig list even further out of balance.

The crew tried to evacuate. The combination of high winds and seas caused the fiberglass lifeboats to crash against the rig legs, cracking them open. The crew called their support vessel, just five miles away, to evacuate them. It took the support vessel one hour to reach them in the rough seas. Only one lifeboat was left floating. The eight occupants perished trying to climb up the high gunwales of the supply boat's aft deck in the rough seas. The supply boat was not a rescue craft and its crew had no gear to save the men.

The world's largest, supposedly unsinkable rig, was lost with all aboard, due to a small porthole.

Questions Raised

1. How many undocumented systems do you have operating in your facility?
2. Have your personnel been formally trained on their operation?
3. What would happen if people were to use these systems without a full understanding of their operation?
4. Have you done a complete HAZOP?

Chernobyl

One of the Soviet reactors at Chernobyl exploded in 1986. Two dozen operators and firefighters died within days. Thousands probably died downwind. At least 70,000 people across northern Europe were contaminated.



Figure 3: Chernobyl

The accident was primarily due to reactor operators performing an undocumented test. They wanted to see if after steam was shut off from the turbo-generator, whether the still rotating generator would create enough power before they could get auxiliary motors online. They thought it was an electrical test, not a nuclear test. In fact, it was both. They thought operating the reactor at low power would be inherently safe. They didn't understand the unstable operation of the particular reactor design under such conditions. An analogy compared it to driving your car at one mile an hour – with the gas and brake pedals both floored. The reactor designers knew operation under such conditions was dangerous, so automated safety systems were installed. Unfortunately, the operators really wanted to do their test, so *they intentionally disabled* all the automatic safety shutdown systems. They violated their own safety rules.

Questions raised

1. How well do your operators understand the operation of their facility?
2. Are safety policies being violated? How would you even know if they were?
3. Does Engineering and Management *really* know what Operations is doing?
4. Is the design of your facility inherently safe? Could it be modified to be safer?

Terra Industries

Terra Industries, Inc. operated an ammonium nitrate unit in Port Neal, Iowa. An explosion on December 13, 1994 killed four employees and hospitalized 18 others. 5700 tons of anhydrous ammonia and 25,000 gallons of nitric acid were released. Residents were evacuated from the surrounding area and ammonia plumes were detected several miles away.

A probe was used to monitor pH in an ammonium nitrate neutralization tank. It was out of service for two weeks prior to the accident, yet operations continued. Operators were unable to determine when unsafe acidic conditions developed in the tank, which contributed to the accident.

A process hazards analysis had not been performed on the ammonium nitrate plant. Interviews with Terra personnel indicated they were not aware of many of the hazards of ammonium nitrate. No single engineer was assigned responsibility for overseeing operation of the ammonium nitrate plant or reviewing operating procedures.

Questions raised

1. Have you done a hazards analysis?
2. Are your operators aware of the process risks?
3. Are your instrumentation and safety devices operating properly?
4. What procedures are in place for operating with bypassed instrumentation?

Mars Polar Lander

The Mars Polar Lander was launched in January 1999 and was intended to land on Mars in December of that year. Legs were designed to deploy prior to landing. Sensors would detect touchdown and turn off the rocket motor. It was known and understood that the deployment of the landing legs generated spurious signals of the touchdown sensors. The software requirements, however, did *not* specifically describe this behavior and the software designers therefore did *not* account for it. The motor turned off at too high an altitude and the probe crashed into the planet at 50 miles/hour and was destroyed. Mission costs exceeded \$120 million.

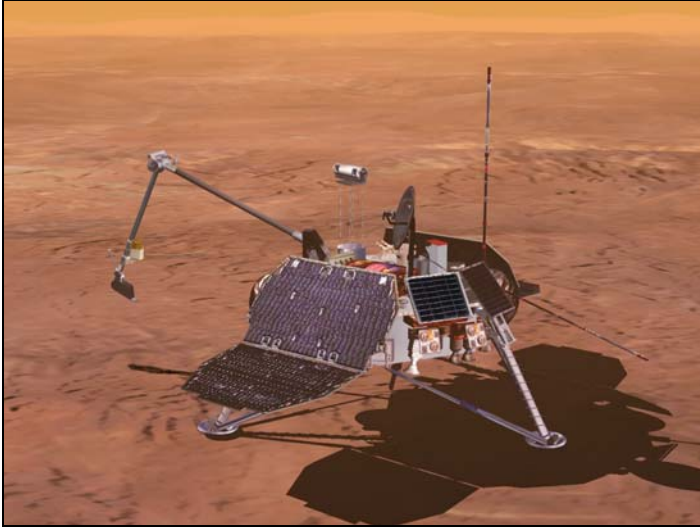


Figure 4: Mars Polar Lander

Questions raised

1. Have all operating parameters been accounted for in your design (e.g., start-up, operation, maintenance, shutdown, etc.)?
2. Have all parameters been fully documented?
3. Has the impact of spurious sensor signals been accounted for in the rest of the system design and operation?

Airbus

Control in the process industry is becoming increasingly automated. Facilities are cutting staff. The author has heard complaints of increased automation leading to a ‘dumbing down’ of plant operators. Other industries have experienced an increase in automation. What might our industry be able to learn?

In 1993 a Lufthansa Airbus A320 landed at Warsaw airport during a thunderstorm. It overran the runway and collided with an earthen bank. One crew member and one passenger were killed. The aircraft was destroyed in the subsequent fire.

Modern aircraft are heavily automated with redundant diverse computer systems. In the Airbus, ground spoilers and engine thrust reversers can only be utilized when *both* main landing gear are compressed. Wheel brakes may be used once *both* main landing gear are above a certain reference speed. The crew is not able to override and operate the ground spoilers and engine thrust reversers manually.

The plane landed at a faster than normal speed to counteract the effects of windshear reported at the time. The plane touched down beyond the normal touchdown point. The plane did not fully

touch down on both main landing gear, so the ground spoilers, thrust reversers and wheel brakes did not activate until many seconds later (due to hydroplaning) when the plane had finally slowed enough to compress both main landing gear. By this time it was too late to stop the plane before it collided with an earthen bank.



Figure 5: Airbus A320, Warsaw

Many aircraft accidents are attributed to human error. Many, however, can be traced back to design issues.

The Airbus philosophy was to give the computer final authority whenever there was a discrepancy between it and the pilot. While there may be good reasons for this, we are not at the point where we can build software to account for every possible condition. Trusting it above human intelligence and flexibility may be a mistake. There are at least three other Airbus accidents resulting in hundreds of deaths due to similar computer vs. pilot control issues.

Questions raised

1. How confident are you that *all* operating conditions have been accounted for in your automated control system?
2. Are your automation systems operating beyond the capabilities of your operators to adequately override them in the event of an emergency?

Conclusions

There are common themes to many accidents and much can be learned from them. Unfortunately, it is human nature to believe “it won’t happen to us”. Overconfidence and complacency can be dangerous attitudes. The questions raised in this paper would hopefully be applied to all instrumentation and control systems in the process industry. Additional reference material is provided for those wishing to read and learn from *hundreds* of other examples.

References

1. **Inviting Disaster**, James R. Chiles, Harper Business, 2001, ISBN 0-06-662081-3
2. **Safeware - System Safety and Computers**, Nancy G. Leveson, Addison-Wesley, 1995, ISBN 0-201-11972-2
3. Recurring Causes of Recent Chemical Accidents, James C. Belke, U.S. Environmental Protection Agency
4. *Seminole Pipeline Co. v. Broad Leaf Partners, Inc.*, (Tex. App., Houston, TX), 1998
5. Chemical Emergency Preparedness and Prevention Office (CEPPO) excerpts from the EPA Chemical Accident Investigation Report, (January 1996) and the Expert Reviewers' Report including EPA's Response to Recommendations (September 1996)
6. Systemic Factors in Software-Related Spacecraft Accidents, Nancy G. Leveson, MIT, 2001
7. Evaluating Accident Models using Recent Aerospace Accidents, Nancy G. Leveson, MIT, 2001
8. **Out of Control, Why control systems go wrong and how to prevent failure**, Health & Safety Executive (UK), 1995, ISBN 0-7176-0847-6
9. **Computer Control and Human Error**, Trevor A. Kletz, ISBN 0-88415-269-3, Gulf Publishing Co., Houston, TX, 1986
10. **What Went Wrong? Case Histories of Process Plant Disasters**, Trevor A. Kletz, ISBN 0-88415-027-5, Gulf Publishing Co., Houston, TX, 1986
11. **An Engineer's View Of Human Error**, Trevor A. Kletz, The Institute of Chemical Engineers (Warwickshire, England), 1985, ISBN 0-85295-192-2
16. **Lessons From Disaster - How organizations have no memory and accidents recur**, Trevor A. Kletz, Gulf Publishing Co., Houston, TX, 1993, ISBN 0-88415-154-9
17. **To Engineer Is Human**, Henry Petroski, Vintage Books, 1992, ISBN 0-679-73416-3