Investigating Beyond the Human Machinery: A Closer Look at Accident Causation in High Hazard Industries

Cheryl Mackenzie and Don Holmstrom
US Chemical Safety and Hazard Investigation Board, NW, Washington, DC 20037; Cheryl.Mackenzie@csb.gov (for correspondence)

Published online 18 December 2008 in Wiley InterScience (www.interscience.wiley.com). DOI 10.1002/prs.10283

Human error is not a cause of an accident—it's a symptom of underlying problems. Attempting to modify operator behavior to prevent human error will not rectify those underlying problems nor will it prevent major catastrophic accidents. This article will provide evidence to support why an organization's safety focus should not be solely on behavior-based safety. It will demonstrate how an equal emphasis and focus needs to be placed on the safety systems of the organization, as these aspects of safety provide a more accurate assessment of a company's true safety state. By taking another look at the US Chemical Safety Board's completed investigations, this article will demonstrate how one must go beyond the actions and decisions of frontline operators to truly understand the causes of any given incident and to safeguard against major accident hazards. © 2008 American Institute of Chemical Engineers Process Saf Prog 28: 84–89, 2009

Keywords: human error, accident causation, safety systems

INTRODUCTION

Read any newspaper article covering a recent high-hazard industry incident and it is clear that the phrase "human error" has become ubiquitous in discussions of accident causation. But human error is not a cause of an incident. It's a symptom of underlying problems. To say that an accident was caused by human error is easy, is misleading and it can prevent recognition of deeper more serious problems. Diverting blame and attention to that of the frontline staff does very little to help companies prevent future incidents. This limited focus may influence the actions and decisions of the staff that was directly affected by the incident, but it will not prevent individuals from other units, other plants, or other companies from making similar mistakes. The attention is often too directly aimed at those that "erred," leading all others to assume that the problem was with the individuals, not the environment in which those individuals worked. However, "accidents are not the result of a breakdown of otherwise well-functioning processes; accidents are actually structural by-products of a system's normal functioning" [1, p. 17]. The focus on safety, therefore, should go beyond the individual level, to the safety systems of the organization, as these upper levels of safety provide a more accurate assessment of a company's true safety state.

The BP Texas City explosion is a significant example of how safety system deficiencies resulted in a catastrophic incident [2]. But the incident was only unique in the severity of its consequences. The state of safety at the BP Texas City refinery has many important lessons for other refineries and chemical

This article is prepared for presentation at American Institute of Chemical Engineers 2008 Spring National Meeting, 42nd Annual Loss Prevention Symposium, New Orleans, LA, April 7–9, 2008.

process plants. By taking a look at BP Texas City and other US Chemical Safety Board's investigations, this article will demonstrate how all companies must go beyond the actions and decisions of frontline workers and supervisors to truly understand the causes of any given incident and to safeguard against major accident hazards. A review of several incidents—the Tosco Avon refining fire in Martinez, CA, the Formosa Plastics refinery fire in Illiopolis, IL, the Giant Industries refinery fire in Gallup, NM, and the investigation of the CAI explosion in Danvers, MA—will support this view and will (hopefully) spur managers at high hazard facilities to reassess their companies' focus on more fundamental issues of prevention such as human factors and safety systems.

HUMAN "ERROR" IS THE STARTING POINT

It is important to recognize that individuals do not plan to make mistakes. They are doing what makes sense to them at the time, given the work environment, the organization's goals, and other job-related factors [1, p. 18]. Any given worker doesn't come to the job with the mindset of "I'm going to blow up the plant today." But they do come into work: with expectations of how to do their job that they get from supervisors, leadership, trainers, and fellow coworkers; with previous experience as a personal guide; and with the idea of getting the job done, and in many cases, as quickly and efficiently as possible.

Therefore, to truly understand why an incident occurred, one must ask: "Why did those individuals take the actions that they did?" Just like one would investigate why a malfunctioning piece of equipment or technological machinery failed, one must ask why the human machinery failed. Understanding and correcting the factors in the work environment that are conducive to human error will help prevent not just the same incident from reoccurring but will also aid in preventing other similar incidents and, therefore, have a much greater preventative impact in industry overall. In other words, only by understanding the context that provoked the error made can we hope to succeed at preventing it from happening again.

Indeed, the Chemical Safety Board (CSB) found numerous underlying conditions and safety system deficiencies that influenced operators' decision-making and actions in each of the aforementioned incidents. This article will review those findings.

TOSCO REFINERY FIRE

In February 23, 1999, a fire occurred in the crude unit at Tosco Corporation Avon oil refinery in Martinez, California. Workers were attempting to replace piping attached to a 150-foot-tall fractionator tower while the process unit was in operation. During removal of the piping, flammable material was released onto the hot fractionator and ignited. The flames engulfed five workers, four of whom died from their injuries.

In the days leading up to the incident, a pinhole leak was discovered in the vertical piping of the tower. On inspection, it was discovered that the piping had become extensively thinned and corroded over time. A decision was made to replace this piping to stop the leak. To isolate the line from the running process unit, two valves in the piping were closed. However, they were not drained, isolated, and blinded[1] to ensure that material could not leak through the valve.

An attempt was made to remove the flammable contents of the piping, but the area where operators tried to drain the contents was plugged with residue that had built up over time from the products of corrosion. Meanwhile, the piping continued to leak warm product (thereby hinting that something was amiss). Yet despite being unable to remove any flammable liquid or verify that the piping was isolated, a management decision to carry out the work was issued and the maintenance crew began making cuts into the piping. In the middle of removing sections of the piping, the flammable material from the running process unit leaked through the closed valves and suddenly released out of the piping. It came in contact with nearby hot surfaces of the tower and ignited.

At first glance, several "human error" type events can be identified. The piping was unable to be isolated and the unstoppable pinhole continued to leak, yet the maintenance work continued. Additionally, to make matters worse, known flammable material was contained within the unit and multiple sources of ignition were present in the work area (as close as three feet from the pipe being replaced).

Was this just a case of careless workers?

No. The CSB's analysis of the refinery's safety systems revealed higher-level deficiencies that influenced the decisions and actions of the workers that day.

The procedures for isolating piping required that the piping be drained, depressurized, and flushed before opening. This could not happen because of the plugging, but the procedures did not specify an alternative course of action if safety preconditions, like the draining, could not be met.

On top of that, the refinery's job planning procedures did not require a formal evaluation of the hazards when there was a deviation from the procedure (such as an inability to perform the step of draining and isolating the piping). The potential risks in making the change to the procedure were not assessed. Managing changes to procedures, as well as changes to staff and equipment, is a safety must.

The CSB also found that the work permit policy allowed a single unit operator to authorize a job and there was insufficient supervision during non-normal work activities. Supervision by technically trained personnel and secondary checks to ensure the work is safely conducted are necessary in high-hazard industries, particularly during abnormal or infrequent work tasks.

Finally, the CSB also found that there were no management audits of safety procedures or policies

[1]Blinding is a technique where (to put it simply) a separate piece of metal is inserted into the piping to block the flow of any product through the piping.

concerning line breaking, lockout/tagout, or blinding for 3 years before the incident. Management audits of the organization's safety systems provide key opportunities to identify risks and proactively work to reduce those risks before a catastrophic incident occurs.

For Tosco, the lack of a hazard evaluation when deviating from a procedure, reduced staffing and supervision, and insufficient auditing of safety systems created a workplace where error was likely to occur.

It must be emphasized that all too often the CSB finds similar situations like this where audits are poorly done or not conducted at all. Other times, the agency finds companies conducting very thorough and useful audits, only to not effectively fulfill the subsequent action items and recommendations. The Valero McKee refinery fire in 2007 provides examples of both situations. The company's 2006 PHA audit did not identify a dead-leg in a propane mix control station of its propane de-asphalting unit (PDA), a known risk for process units where temperatures drop below freezing. Had this risk been identified and assessed, the 2007 propane leak that ignited and resulted in a complete shutdown of the refinery may have been prevented. On the other hand, a hazard was aptly recognized in a 1996 PHA, where it was recommended that remotely operable shut-off valves be installed in the PDA unit to stop the flow of propane in emergency situations. Had this recommendation been acted upon, the amount of flammable material released during the 2007 incident could have been reduced and the severity of the resulting fire dramatically lessened.

FORMOSA PLASTICS EXPLOSION

On April 23, 2004, five workers died and two others were seriously injured when an explosion occurred in a polyvinyl chloride (PVC) production unit at Formosa Plastics in Illiopolis, Illinois. The explosion followed a release of highly flammable vinyl chloride, which ignited. It forced a community evacuation and lighted fires that burned for several days at the plant.

On the day of the incident, one of several reactors at the facility was being cleaned. The reactors were housed in a two-floor building, with the primary reactor controls located on the top floor and the reactor drain valves located on the ground floor (see Figure 1).

The chemical batch in the reactor to be cleaned had been transferred out, and the interior of the reactor had been power washed with cleaning water from the top floor. At this point, the next step was for an operator to go downstairs to the bottom drain valve and open it to drain out the cleaning water.

An operator went down a couple flights of stairs to open the drain valve. When he got to the bottom level, he walked to the wrong reactor—a reactor that was full of vinyl chloride monomer. Each reactor's drain valve had an interlock to prevent unintentional opening of the valve while the reactor was in use. Therefore, when the operator attempted to open the drain valve of the (wrong) reactor, the interlock prevented the valve from opening. However, because the operator did not realize he was at the incorrect reactor, he bypassed the interlock. He did this without discussing the decision with his fellow operators or supervisor. Once he bypassed the interlock, he was able to open the valve. The polyvinyl chloride monomer contents of the full reactor were released. As a large amount of the chemical released into the building, other operators and supervisors attempted to stop it. Shortly after, the material ignited, killing five of the employees, including the operator who bypassed the interlock.

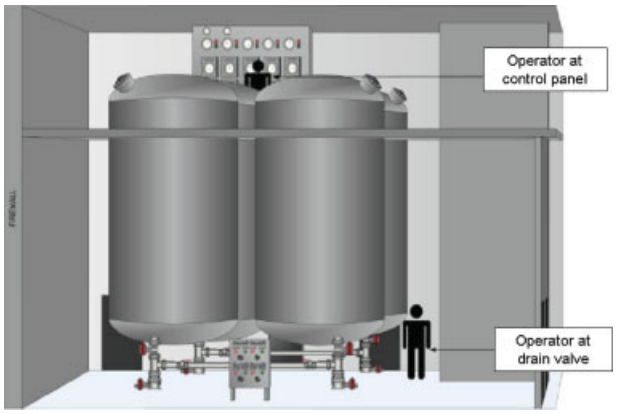

Figure 1. Interior view of the Formosa reactor facility. [Color figure can be viewed in the online issue, which is available at **www.interscience.wiley.com.**]

Were the actions of the operator the cause of the accident?

No. Although hindsight tells us that it was clear the operator should not have bypassed the interlock, a deeper look at the facility's safety policies and procedures revealed gaps.

The company controlled risk associated with inadvertent opening of reactor valves through procedures and training instead of changing the interlock with better technology that would prevent the operator from bypassing the interlock without managerial authorization or intervention. Although training is imperative for maintaining a skilled and knowledgeable workforce, it is also crucial to recognize that even the most highly trained individuals will make mistakes. It is, after all, human nature to err. Eliminating a workplace risk through an engineering control is a better solution to continually training and reviewing procedures with the hope of employees never making a mistake. Companies need to focus on correcting or minimizing the source of the problem, instead of only attempting to change the actions taken by those who have to deal with the problem.

Additionally, Formosa's emergency procedures for evacuation at the site were ambiguous and facility staff had not conducted large-scale chemical release emergency drills in more than 10 years. Had the employees evacuated on seeing the massive quantity of chemical released, they likely would have survived. The employees' collective response during the emergency demonstrates an organizational-level

Figure 2. The shut-off valve and valve wrench (indicated by arrow on far left). [Color figure can be viewed in the online issue, which is available at **www.interscience.wiley.com.**]

deficiency where the company's safety training lacked the essential emergency evacuation component.

Finally, the CSB found that lessons from previous incidents were not being shared and learned throughout the company's facilities. A 2003 incident at the Formosa Baton Rouge facility and a 2004 incident at the same Illiopolis site identified the hazards associated with the bypassing of reactor bottom valves, yet corrective actions were not taken to prevent similar future incidents. All too often the CSB finds that companies who suffer a devastating incident had experienced similar incidents or near misses in the past that could have had the same results, had just one or two things gone differently. The BP Texas City explosion, which is briefly discussed later in this article, is one such additional example. There were eight serious isomerization unit blowdown drum incidents that preceded the 2005 explosion. Had the causes and potential risks of these incidents been fully investigated and lessons learned, the catastrophic 2005 incident may not have occurred. Previous incidents and near misses must be learned from—they provide a roadmap of where risks exist.

GIANT REFINERY EXPLOSION

The CSB also conducted an investigation of the Giant Industries refinery in Gallup, New Mexico, after the site experienced an explosion that seriously injured four maintenance workers. On April 8, 2004, highly flammable gasoline components were released as workers were removing a malfunctioning pump from a process unit to repair it. Unknown to personnel, a shut-off valve connecting the pump to a distillation tower was left in the open position, leading to the release of flammable material that found an ignition source and exploded.

Figure 2 depicts the shut-off valve thought to be closed. The horizontal bar coming off the valve stem, called the valve wrench, was used to manually open and close the valve.

The operator responsible for ensuring the valve was closed relied on the position of the valve wrench to determine the valve's status. It was common to use the valve wrench as an indicator of valve position—when the valve wrench was horizontal, as shown in Figure 2, the valve was thought to be closed. When it was vertical, the valve was considered open. The valve did have a position indicator that provided accurate information on the open/close state of the valve, but it was less visible than the valve wrench and, as such, was typically not used.

Seeing the valve in the horizontal position, the operator tagged and locked the valve in what he thought was the closed position. The valve, however, was actually open. Maintenance personnel, seeing the horizontal orientation of the valve wrench and the tags and locks in place assumed the valve was in its closed position. They also did not verify the valve's position by looking at the position indicator. They began unbolting the pump. The flammable material came out of the column and within 30–45 s the first of several explosions occurred.

Is this a case of more careless workers?

No. First of all, equipment was allowed to be used in a manner for which it was not designed. The shut-off valve was originally designed to be opened and closed by a gear-operated actuator. The gear-driver was removed and replaced with the two-foot-long valve wrench. No analysis or assessment of the safety implications of such a change was conducted. Over time, operators and maintenance personnel began to use an unofficial method of determining if the valve was open based on the orientation of the valve wrench position.

Yet, the valve wrench was not permanently affixed to the valve stem. And it was also common practice to remove the valve wrench and place it at the base of the pump—this allowed better clearance for personnel walking by. When the valve needed to be opened or closed, the wrench would be placed back into the valve stem. Before the incident, the wrench was likely placed back into the valve stem so that it operated opposite of the workers' expectations.

Additionally, the CSB found that maintenance at the site was not preventative. Remember, this incident occurred when workers were trying to repair a malfunctioning pump. The pump actually had a history of failures—23 work orders were submitted to repair the pump in the year previous to the incident. Yet each time a work order was submitted, the repairs were made without any further analysis to determine why the pump kept failing. Comparable with the act of continuing to bail water out of a leaking ship instead of just plugging the hole, the company continued to repair the pump without finding out the cause of the failure and rectifying it.

CAI/ARNEL MANUFACTURING PLANT EXPLOSION

On November 22, 2006, an explosion destroyed a local ink and paint manufacturing plant and damaged scores of nearby buildings. The explosion was the

result of solvents left stirring overnight in an unsealed mixing tank; flammable vapor slowly escaped out of the tank, accumulated and ignited.

The steam valve to the tank was either inadvertently left open overnight by an operator or it malfunctioned.[2] As a result, the steam continued heating the tank mixture, causing the flammable solvent within to boil. Flammable vapor created from this heating escaped through the unsealed tank into the building and accumulated inside. It eventually found an ignition source. The resulting explosion not only demolished the manufacturing plant, but also heavily damaged dozens of nearby homes and businesses, many of which were completely destroyed. Amazingly, there were no fatalities, but a number of individuals were treated for cuts and bruises.

Once more, the question is raised: Was the operator the cause of the accident?

No, many other higher level safety system deficiencies created an environment ripe for catastrophe. Not only is processing flammables inside buildings considered an unsafe work practice, but CAI's flammable liquids storage inside the building did not conform to OSHA and Massachusetts fire code requirements. Massachusetts fire regulations require that flammable liquid storage equipment located inside buildings be vented to the outside and have approved automatic shutoff valves. However, neither of these required safeguards was in place.

In response to the neighboring residents' complaints about excessive noise and to reduce heat loss from the building, CAI turned the building's ventilation system off nightly; this goes against both state and federal fire safety regulations that require adequate building ventilation to prevent flammable vapors from accumulating to dangerous concentrations. Additionally, the company did not use checklists or formal written procedures to help ensure the correct sequence of operator actions. Finally, there were no automatic alarms, shutdown systems, or interlocks to prevent overheating of the mixing tank. Yet, when hazardous processes are intended to be left running unattended, it is particularly important to use multiple safeguards, called layers of protection, to prevent catastrophic accidents.

BP TEXAS CITY REFINERY EXPLOSION

Finally, this article highlights some of the higher level safety system issues of the BP Texas City refinery explosion that occurred on March 23, 2005. It is interesting to note that many of the safety deficiencies of the incidents described above were also found to be causal in the BP incident.

The BP Texas City accident occurred during the start-up of a distillation tower that processed large quantities of hydrocarbons. During the start-up, the tower and associated piping were overfilled and overpressured. As a result, flammable liquid vented from the tower to a relief disposal system (blowdown drum with a stack open to atmosphere) that also filled completely with flammable liquid. Vapor and liquid erupted out of the top of the stack. A large flammable vapor cloud developed at ground level, found an ignition source, and exploded. Fifteen individuals in the area where the cloud formed were killed and 180 others were injured.

After the incident, much attention was immediately given to the operators of the distillation process unit. And many individuals were quick to point out that procedures were deviated from, that errors were made that should not have been, and that perhaps the operators were being careless. But this was not the case.

Through extensive analysis and reconstruction of the incident, the CSB was able to conclude that operators were doing what they believed was necessary to start up the unit. They were following practices they often did. And their actions that day were in response to management decisions made hours, days, months, and even years before the incident.

Indeed, the investigation team found numerous underlying conditions and safety system deficiencies that influenced operators' decisions and actions leading up to the BP Texas City incident, including a history of procedural deviations that were allowed to repeatedly occur without investigation as to why the deviations were taking place. Various process data were collected by the control board system but not systematically reviewed for deviations to process parameters. Additionally, the procedural review process was not being upheld or managed to ensure that procedures reflected actual and safe work practices.

These higher-level safety system deficiencies became apparent to the CSB when, in addition to examining the startup on March 23, 2005, the agency reviewed the data from the 18 previous startups of this specific distillation unit. The agency found that in 15 of these 19 startups, the tower was filled with liquid hydrocarbons to a level that was above the range of the tower's level transmitter. When the liquid goes beyond the transmitter's range of measurement, operators have no means to determine how much liquid is in the tower; for obvious reasons, this made overfilling the tower much more likely. Additionally, in 18 of the 19 startups, the tower experienced dramatic swings in liquid level, where the liquid in the tower would drop and rise rapidly; this made controlling the startup difficult. Operators knew that swings in the liquid level could result in a loss of flow out the bottom of the tower. This loss of flow could damage the furnace tubes and potentially result in an emergency shutdown of the unit. Operators filled the tower with liquid hydrocarbons above the transmitter—contrary to the procedures—because doing so reduced the likelihood of a loss of flow out the bottom of the tower. The actions taken that day by operations were done with protection of the unit in mind.

The recurring procedural deviations and abnormal tower levels experienced in previous startups were not investigated to correct the underlying problems, nor were deviations typically subjected to any hazard review or assessment, which was contrary to BP's

[2]The operator on duty believes he closed the valve. Because of the severity of the explosion, any evidence to determine if the valve malfunctioned was destroyed.

own policy. Just like in the Giant case, where over time an unsafe method for determining valve position became the norm, here too unsafe deviations to the startup procedures became common practice.

BP Texas City workers also had inadequate training that focused on computer-based memorization of facts without much training on abnormal situation management. The human's role in most modern technology is as a "monitor," employed to ensure that the system functions as planned. These individuals are expected to be there in case the technology fails. Yet the CSB found that the training the operations staff received often did not focus on handling infrequent and abnormal scenarios, yet these were the very situations where operators would be expected to take action and make decisions above-and-beyond the limits of the technology.

The distillation unit, and its respective control room, also had insufficient staffing and supervision during startup. It is a well-known fact that unit startup is an especially hazardous time in a refinery [3]. BP recognized this fact and had policies recommending additional assistance from supervisors or technically trained personnel during startup. However, the one supervisor who had work experience in the unit left the refinery that morning for a family emergency and there was no replacement assigned, as required by BP policy. It is during abnormal and non-routine tasks that additional assistance and supervisory support is needed; like the Tosco and Formosa incidents, operators typically made significant decisions without the benefit of input from a knowledgeable authority. Clear role responsibilities, and additional supervision and/or staffing of technically-trained personnel are particularly needed during abnormal and safety-critical tasks.

On top of those issues, operators also had fatiguing work schedules; each had been working 12-h shifts for 29 or more consecutive days. Fatigue can increase errors, delay responses, and cloud decision-making [4,5]. BP had no fatigue prevention policy in place or any limit on maximum allowable work hours at its Texas City site. In fact there are no widely-used fatigue prevention guidelines or restrictions on hours and days of work throughout the US refining industry, even though fatigue is recognized as a serious safety issue in other hazardous sectors like transportation, health care, and the nuclear industry.

These are just some of the many underlying conditions that existed in the BP Texas City work environment that led the operators to make the decisions and take the actions that they did during the unit startup.[3] Multiple safety system deficiencies created a workplace where the eventual error by a frontline employee would result in devastating consequences. One could say it was only a matter of time.

[3]Please see Section 3 of the US Chemical Safety and Hazard Investigation Board (March 2007). Refinery Explosion and Fire: BP for further information.

CONCLUSION

It is clear that stopping at the human error level of accident causation is not enough for true accident prevention. Companies that are serious about keeping their facilities safe must dig deep and go further in their investigations of incidents and near misses. The human machinery of any complex high-hazard system is apt to fail just as much as any piece of technology. Companies must stop treating the symptom of human error, and instead focus on remedying the underlying illnesses in their safety systems.

LITERATURE CITED

1. S. Dekker, The Field Guide to Understanding Human Error, Ashgate Publishing Group, Burlington, VT, 2006.
2. BP Refinery Explosion and Fire, U.S. Chemical Safety and Hazard Investigation Board, Washington, DC 2007.
3. Institute of Chemical Engineers. BP Process Safety Series: Safe Ups and Downs for Process Units, Rugby, UK, 2005.
4. Validation and Development of a Method for Assessing the Risks Arising from Mental Fatigue, Report 254, Defence Evaluation and Research Agency Centre for Human Services, for the HSE, U.K. 1999.
5. Managing Fatique Risks. Inspectors Toolkit: Human Factors in the Management of Major Accident Hazards, HSE, U.K., 2004, Available at: **http://www.hse.gov.uk/humanfactors/comah/toolkit.htm**, Accessed on March 1, 2006.