Get To The Root Of Accidents

Systems thinking can provide insights on underlying issues not just their symptoms

By Nancy Leveson, Massachusetts Institute of Technology, and Sidney Dekker, Griffith University

Feb 27, 2014

An often-claimed "fact" is that operators or maintenance workers cause 70–90% of accidents. It is certainly true that operators are blamed for 70–90%. Are we limiting what we learn from accident investigations by limiting the scope of the inquiry? By applying systems thinking to process safety, we may enhance what we learn from accidents and incidents and, in the long run, prevent more of them.

MENTAL MODELS

Figure 1. Designers and operators necessarily view systems differently.

Systems thinking is an approach to problem solving that suggests the behavior of a system's components only can be understood by examining the context in which that behavior occurs. Viewing operator behavior in isolation from the surrounding system prevents full understanding of why an accident occurred — and thus the opportunity to learn from it.
We do not want to depend upon simply learning from the past to improve safety. Yet learning as much as possible from adverse events is an important tool in the safety engineering tool kit. Unfortunately, too narrow a perspective in accident and incident investigation often destroys the opportunity to improve and learn. At times, some causes are identified but not recorded because of filtering and subjectivity in accident reports, frequently for reasons involving organizational politics. In other cases, the fault lies in our approach to pinpointing causes, including root cause seduction and oversimplification, focusing on blame, and hindsight bias.

ROOT CAUSE SEDUCTION AND OVERSIMPILIFICATION
Assuming that accidents have a root cause gives us an illusion of control. Usually the investigation focuses on operator error or technical failures, while ignoring flawed management decision-making, safety culture problems, regulatory deficiencies, and so on. In most major accidents, all these factors contribute; so to prevent accidents in the future requires all to be identified and addressed. Management and systemic causal factors, for example, pressures to increase productivity, are perhaps the most important to fix in terms of preventing future accidents — but these are also the most likely to be left out of accident reports.

As a result, many companies find themselves playing a sophisticated “whack-a-mole” game: They fix symptoms without fixing the process that led to those symptoms. For example, an accident report might identify a bad valve design as the cause, and, so, might suggest replacing that valve and perhaps all the others with a similar design. However, there is no investigation of what flaws in the engineering or acquisition process led to the bad design getting through the design and review processes. Without fixing the process flaws, it is simply a matter of time before those process flaws lead to another incident. Because the symptoms differ and the accident investigation never went beyond the obvious symptoms of the deeper problems, no real improvement is made. The plant then finds itself in continual fire-fighting mode.

A similar argument can be made for the common label of “operator error.” Traditionally operator error is viewed as the primary cause of accidents. The obvious solution then is to do something about the operator(s) involved: admonish, fire or retrain them. Alternatively, something may be done about operators in general, perhaps by rigidifying their work (in ways that are bound to be impractical and thus not followed) or marginalizing them further from the process they are controlling by putting in more automation. This approach usually does not have long-lasting results and often just changes the errors made rather than eliminating or reducing errors in general.

Systems thinking considers human error to be a symptom, not a cause. All human behavior is affected by the context in which it occurs. To understand and do something about such error, we must look at the system in which people work, for example, the design of the equipment, the usefulness of procedures, and the existence of goal conflicts and production pressures. In fact, one could claim that human error is a symptom of a system that needs to be redesigned. However, instead of changing the system, we try to change the people — an approach doomed to failure.

For example, accidents often have precursors that are not adequately reported in the official error-reporting system. After the loss, the investigation report recommends that operators get additional training in using the reporting system and that the need to always report problems be emphasized. Nobody looks at why the operators did not use the system. Often, it is because the system is difficult to use, the reports go into a black hole and seemingly are ignored (or at least the person writing the report gets no feedback it even has been read, let alone acted upon), and the fastest and easiest way to handle a detected potential problem is to try to deal with it directly or to ignore it, assuming it was a one-time occurrence. Without fixing the error-reporting system itself, not much headway is made by retraining the operators in how to use it, particularly where they know how to use it but ignored it for other reasons.

Another common human error cited in investigation reports is that the operators did not follow the written procedures. Operators often do not follow procedures for very good reasons. An effective type of industrial action for operators who are not allowed to strike, like air traffic controllers in the U.S., is to follow the procedures to the letter. This type of job action can bring the system down to its knees.

**Figure 1** shows the relationship between the mental models of the designers and those of the operators. Designers deal with ideals or averages, not with the actual constructed system. The system may differ from the designer's original specification either through manufacturing and construction variances or through evolution and changes over time. The designer also provides the original operational procedures as well as information for basic operator training based on the
original design specification. These procedures may be incomplete, e.g., missing some remote but possible conditions or assuming that certain conditions cannot occur. For example, the procedures and simulator training for the operators at Three Mile Island nuclear power plant omitted the conditions that actually occurred in the well-known incident because the designers assumed that those conditions were impossible.

In contrast, operators must deal with the actual constructed system and the conditions that occur, whether anticipated or not. They use operational experience and experimentation to continually test their mental models of the system against reality and to adjust the procedures as they deem appropriate. They also must cope with production and other pressures such as the desire for efficiency and “lean operations.” These concerns may not have been accounted for in the original design.

Procedures, of course, periodically are updated to reflect changing conditions or knowledge. But between updates operators must balance between:

1. Adapting procedures in the face of unanticipated conditions, which may lead to unsafe outcomes if the operators do not have complete knowledge of the existing conditions in the plant or lack knowledge (as at Three Mile Island) of the implications of the plant design. If, in hindsight, they are wrong, operators will be blamed for not following the procedures.

2. Sticking to procedures rigidly when feedback suggests they should be adapted, which may lead to incidents when the procedures are wrong for the particular existing conditions. If, in hindsight, the procedures turn out to be wrong, the operators will be blamed for rigidly following them.

In general, procedures cannot assure safety. No procedures are perfect for all conditions, including unanticipated ones. Safety comes from operators being skillful in judging when and how they apply. Safety does not come from organizations forcing operators to follow procedures but instead from organizations monitoring and understanding the gap between procedures and practice. Examining the reasons why operators may not be following procedures can lead to better procedures and safer systems.

Designers also must provide the feedback necessary for the operators to correctly update their mental models. At BP’s Texas City refinery, there were no sensors above the maximum allowed height of the hydrocarbons in the distillation tower. The operators were blamed for not responding in time although they had no way of knowing what was occurring in the tower due to inadequate engineering design.

FOCUSBNG ON BLAME
Blame is the enemy of safety. "Operator error" is a useless finding in an accident report because it does not provide any information about why that error occurred, which is necessary to avoid a repetition. There are three levels of analysis for an incident or accident:

• What — the events that occurred, for example, a valve failure or an explosion;

• Who and how — the conditions that spurred the events, for example, bad valve design or an operator not noticing something was out of normal bounds; and

• Why — the systemic factors that led to the who and how, for example, production pressures, cost concerns, flaws in the design process, flaws in the reporting process, and so on.

Most accident investigations focus on finding someone or something to blame. The result is a lot of non-learning and a lot of finger pointing because nobody wants to be the focus of the blame process. Usually the person at the lowest rung of the organizational structure (the operator) ends up shouldering the blame. The factors that explain why the operators acted the way they did never are addressed.

The biggest problem with blame, besides deflecting attention from the most important factors in an accident, is that it creates a culture where people are afraid to report mistakes, hampering accident investigators’ ability to get the true story about what happened. One of the reasons commercial aviation is so safe is that blame-free reporting systems have been established that find potential problems before a loss occurs. A safety culture that focuses on blame will never be very effective in preventing accidents.
Hindsight bias permeates almost all accident reports. After an accident, it is easy to see where people went wrong and what they should have done or avoided or to judge them for missing a piece of information that turned out (after the fact) to be critical. It is almost impossible for us to go back and understand how the world appeared to someone who did not already have knowledge of the outcome of the actions or inaction. Hindsight is always twenty-twenty.

For example, in an accident report about a tank overflow of a toxic chemical, the investigators concluded “the available evidence should have been sufficient to give the board operator a clear indication that the tank was indeed filling and required immediate attention.” One way to evaluate such statements is to examine exactly what information the operator actually had. In this case, the operator had issued a command to close the control valve, the associated feedback on the control board indicated the control valve was closed, and the flow meter showed no flow. In addition, the high-level alarm was off. This alarm had been out of order for several months but the operators involved did not know this and the maintenance department had not fixed it. The alarm that would have detected the presence of the toxic chemical in the air also had not sounded. All the evidence the operators actually had at the time indicated conditions were normal. When questioned about this, the investigators said that the operator “could have trended the data on the console and detected the problem.” However, that would have required calling up a special tool. The operator had no reason to do that, especially as he was very busy at the time dealing with and distracted by a potentially dangerous alarm in another part of the plant. Only in hindsight, when the overflow was known, was it reasonable for the investigators to conclude that the operators should have suspected a problem. At the time, the operators acted appropriately.

In the same report, the operators are blamed for not taking prompt enough action when the toxic chemical alarm detected the chemical in the air and finally sounded. The report concluded that “interviews with personnel did not produce a clear reason why the response to the … alarm took 31 minutes. The only explanation was that there was not a sense of urgency since, in their experience, previous … alarms were attributed to minor releases that did not require a unit evacuation.” The surprise here is that the first sentence claims there was no clear reason while the very next sentence provides a very good one. Apparently, the investigators did not like that reason and discarded it. In fact, the alarm went off about once a month and, in the past, had never indicated a real emergency. Instead of issuing an immediate evacuation order (which, if done every month, probably would have resulted in at least a reprimand), the operators went to inspect the area to determine if this was yet another false alarm. Such behavior is normal and, if it had not been a real emergency that time, would have been praised by management.

Hindsight bias is difficult to overcome. However, it is possible to avoid it (and therefore learn more from events) with some conscious effort. The first step is to start the investigation of an incident with the assumption that nobody comes to work with the intention of doing a bad job and causing an accident. The person explaining what happened and why it happened needs to assume that the people involved were doing reasonable things (or at least what they thought was reasonable) given the complexities, dilemmas, tradeoffs and uncertainty surrounding the events. Simply highlighting their mistakes provides no useful information for preventing future accidents.

Hindsight bias can be detected easily in accident reports (and avoided) by looking for judgmental statements such as “they should have …”, “if they would only have …”, “they could have …” or similar. Note all the instances of these phrases in the examples above from the refinery accident report. Such statements do not explain why the people involved did what they did and, therefore, provide no useful information about causation. They only serve to judge people for what, in hindsight, appear to be mistakes but at the time may have been reasonable.

Only when we understand why people behaved the way they did will we start on the road to greatly improving process safety.

Escaping the Whack-A-Mole Trap
Systems are becoming more complex. This complexity is changing the nature of the accidents and losses we are experiencing. This complexity, possible because of the introduction of new technology such as computers, is pushing the limits that human minds and current engineering tools can handle. We are building systems whose behavior cannot be completely anticipated and guarded against by the designers or easily understood by the operators.

Systems thinking is a way to stretch our intellectual limits and make significant improvement in process safety. By simply
blaming operators for accidents and not looking at the role played by the encompassing system in why those mistakes occurred, we cannot make significant progress in process safety and will continue playing a never-ending game of whack-a-mole.

REFERENCES

NANCY LEVESON is professor of aeronautics and astronautics and professor of engineering systems at the Massachusetts Institute of Technology, Cambridge, Mass. SIDNEY DEKKER is professor of social science and director of the Safety Science Innovation Lab at Griffith University, Brisbane, Australia. E-mail them at leveson@mit.edu and s.dekker@griffith.edu.au.

What are your comments?
You cannot post comments until you have logged in. Login Here.

Comments

- Submitted by Paul Burnett on Thu, 03/06/2014 - 10:31
  The "Mental Model" figure reminds me of the famous cartoon "How Projects Really Work" or "What the customer really wanted" - http://www.edugeek.net/attachments foraums/general-chat/15350d1348823969-why-do-projects fail-6a00d8345f25369e20120a513810c970b-800wi.jpg
  The cartoon and the article show that communication between the very different worlds of management, engineers and operator / maintenance personal can be almost impossible. This almost always leads to blaming the lowest ranking individual involved in an accident - a time-honored but fault-laden custom.
  In addition to improving communication, I would put more emphasis on "near-miss" reporting. By finding and eliminating the root causes (almost never a single root cause) of near misses, actual hits - accidents - can be prevented. Been there, done that.
  Reply

- Submitted by Traci Purdum on Thu, 03/06/2014 - 10:53
  Thanks for your comment Paul. You might want to read the article "Learn More from Near-Misses" >> http://www.chemicalprocessing.com/articles/2014/risk-management-learn-more-from-near-misses/
  And we love the cartoon.
  Regards,
  Traci Purdum
  Senior Digital Editor
  Reply

RSS feed for comments on this page | RSS feed for all comments

- Member Login
- Become a Member
Related Content You May Like
If you enjoy this article, our editors think you may enjoy this related reading.

- Key Steps Spur More-Effective Root Cause Analyses
- Achieve Effective Process Safety Management
- Process Safety Begins in the Board Room
- Orchestrate an Effective Safety Culture
- Fight Over-Confidence
- Make Safety Second Nature

Most Popular
Check out the most popular content, as determined by our visitors.

1. #1 Compressed Air Systems: The Secret is in the Pipe
2. #2 Shell-and-Tube Heat Exchanger: Pick the Right Side
3. #3 Spotlight Shines on Plant Safety
4. #4 Isobutene Process Progresses
5. #5 Optimize Batch Distillation

FAQ Series: Reliability Engineering
This guide answers 9 of the questions most frequently asked of reliability engineers.
ChemicalProcessing.com's Podcast Library contains a wealth of audio interviews conducted with some of the biggest names in the chemical processing and related industries.

Featured Sponsors

Ask the Experts
A roster of leading authorities in many fields to help you address technical issues.

Federal Equipment Company
We Buy and Sell Used Equipment
800.652.2466 • www.fedequip.com

It's fast, easy and we don't ask for your mother's cousin's dog's groomer's name.

- Subscribe to E-Newsletters »
- Subscribe to the Magazine »
- Get the Article RSS Feed »