Process Safety Management, Jenga, Drift, and Preventing Process Industry Accidents

Paul Gruhn, P.E., CFSE
Global Functional Safety Consultant
aeSolutions, Houston, TX
paul.gruhn@aesolns.com

Abstract

There have been many well publicized process industry accidents over the last several decades. Much has been written about them, and many lessons learned have been proposed. Yet evidence would indicate there has not been a lessening of industry accidents. More recent realization of the complexity of modern processes, and the organizations responsible for designing, building, running, and maintaining them, has resulted in a broader understanding of accident causation, and what can be done to try and prevent further incidents. This paper will review the previous thinking process and recommendations, and offer an alternative approach and recommendations.

Have we learned from previous accidents?

There have been many well publicized process industry accidents over the last several decades. Articles and books have been written about many of these events. [1-3] Trevor Kletz's past suggestions have been for industry to do a better job with:

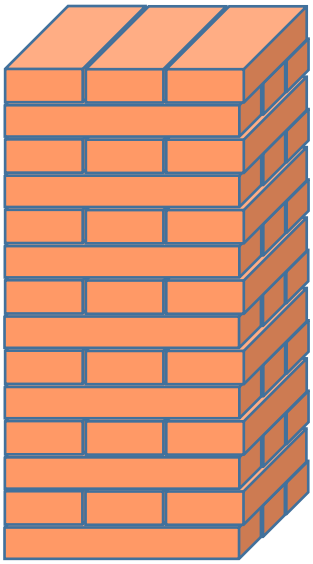
- Process hazards analysis
- Training
- Procedures
- Inspections and testing
- Control of management of change
- User friendly designs
- Better management

Kletz's recommendations are essentially now part of the OSHA Process Safety Management regulation (and similar other regulations worldwide). [4] However, most books essentially reviewed what happened the *day* of the particular accident. As interesting as that information might be, simply publicizing that has not helped industry significantly reduce the number of accidents. [5]

Engineers are trained in a classical style of thinking emphasizing Newtonian cause and effect. If there was an effect (i.e., an accident), there must have been a cause. We then hunt for the broken part, or the individual who made an error, and place blame. [6] The more serious the event, the more blame there must be. This is essentially the basis for the legal system, someone must be held responsible. However, knowing *what* happened the day of the event (a snapshot in time) has not proven to be as helpful as we might desire. Accidents, at least in the process industry, are *much* too complex to place blame in such a manner. In fact, doing so could actually be considered unethical. We need to understand *why* people were doing what they were at the time, how things *evolved* over time, and how such "normalization of deviance" became the new normal. The accident in Bhopal, India in 1984 is a classic example; the event was more than 5 years in the making. [7]

What process safety management and Jenga have in common

Figure 1 lists the 14 parts of the OSHA PSM regulation. Each part has subparts. Think of them as pieces of a Jenga tower/game as shown in the figure. But how many people and plants truly believe they have *all* the pieces in place, and that they are *all* 100% effective? Perhaps your facility is more like the tower on the right.



1. Trade secrets
2. Compliance audits
3. Emergency planning and response
4. Incident investigation
5. Management of change
6. Hot work permit
7. Mechanical integrity
8. Pre-startup safety review
9. Contractors
10. Training
11. Operating procedures
12. Process hazards analysis
13. Process safety information
14. Employee participation

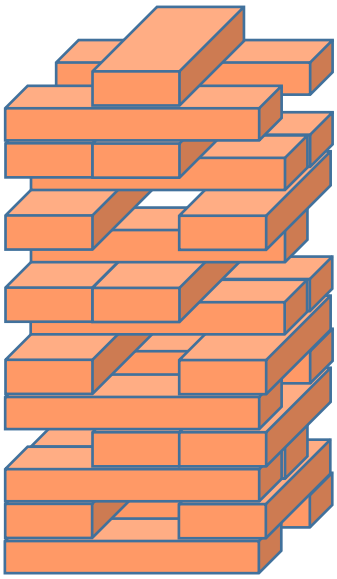


Figure 1: Process Safety Management and Jenga

What's deceptive is that the tower on the right is still standing. Everyone then naturally assumes they must be OK. Yet even a child would realize the tower is not as strong or as resilient as the one on the left. Langewiesche said "Murphy's law is wrong. Everything that can go wrong usually goes **right**, and then we draw the **wrong** conclusions." [6] Might we be able to measure, visualize, or judge the resiliency of the tower and determine if it were getting close to toppling?

Yet process safety, much like physical heath, or the stability of a Jenga tower, is not a binary state. No process or person is 100% healthy, or 100% unhealthy. It's difficult, if not impossible, for your doctor to say that you're going to die *tomorrow*. (Yet the author's eldest brother saw his doctor recently because he was feeling sluggish. His doctor hospitalized him immediately, and he had a pacemaker put in the very next day. His doctor said he would have been dead within a *week*.) Are you willing to tolerate having mildly high cholesterol? Are you willing to tolerate being obese and type II diabetic? If so, for how long? Will it take having a limb amputated to finally make you realize the danger (as was the case with one of the author's in-laws)? What would it take to make you or your company change and take the health of your process safety program seriously? How many Jenga pieces are you willing to tolerate as missing? After all, people and organizations are resistant to change and will usually only change when their leadership makes it a priority. Unfortunately, history indicates that it usually takes a major accident, or an update in regulations to get companies to initiate a change. The Titanic met the lifeboat regulations at the time. Yet, that single accident changed regulations worldwide.

Take note, not all Jenga towers, process facilities, or human bodies are the same. Imagine some towers as tall and slender, others as short and squat. Some are more 'resilient' than others. Some may be able to tolerate 50% of the pieces missing, others may be more 'brittle' and topple if just 10% are removed.

Conflicting goals

Process plants obviously aren't as simple as a Jenga tower. Organizations are complex, messy, and usually have conflicting goals. For example, NASA's motto was actually "Faster, Better, Cheaper" in the nineties. As wonderful as that may initially sound, can any organization actually be all three? How much can you sacrifice one goal to achieve the other two? Such decisions are rarely clear. Organizations must adapt to unruly technology, along with pressures of scarcity (i.e., finances, personnel, equipment) and competition. Jens Rasmussen wrote how complex systems are bounded by three constraints, as shown in Figure 2. [8]

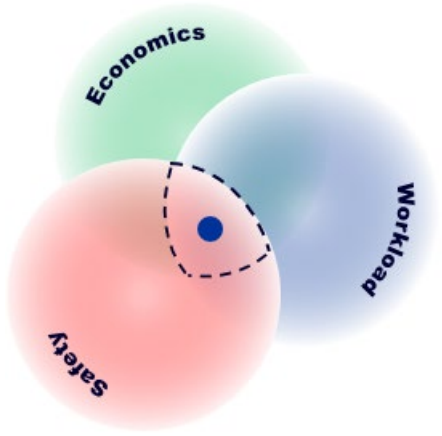


Figure 2: Organizational Constraints

Beyond the **economic** boundary, the system cannot sustain itself financially. Beyond the **workload** boundary, the people or technology cannot perform the tasks they are supposed to. Beyond the **safety** boundary, systems will functionally fail.

The goal is to remain in the space bound by all three (i.e., the dot bounded by the dotted line). Yet the three areas may overlap a lot, resulting in a lot of slack (i.e., a resilient organization), or they may overlap very little, meaning even a small change can trigger a major breakdown (i.e., a brittle organization).

Keep in mind that the circles and the dot move over time. Organizations are never static. They drift. And as Sidney Dekker wrote, they may drift into failure. [6]

How control theory could help

Control theory could be used to help determine if a facility were inside the 'sweet spot' or not. It could even be possible to visualize this, show the values changing over time, and provide it as a tool to management. Many leading and lagging indicators were published by the American Institute of Chemical Engineers Center for Chemical Process Safety and the American Petroleum Institute. [9, 10] A *partial* list of items to track could include the following:

- **Safety factors**: # of safety loops in bypass, # of safety loops past proof test intervals, % of actual failure rates greater than assumed rates, % of demand rates on safety functions higher than assumed, # of near hits, # of toxic and combustible gas releases, etc.
- **Workload factors**: Staff vacancies, maintenance backlog, % of hazard assessment recommendations not closed out, known reliability problems, not meeting projected equipment efficiencies, not meeting projected production quotas, etc.
- **Economic factors**: Meeting budget or not, making a profit or not, etc.

If the above factors are *not* monitored regularly, a one-time compliance audit could yield similar results at that particular point in time. However, the 'tipping point' of the Jenga tower cannot be clearly predicted. As mentioned earlier, process safety, like health, is not a binary proposition. Some things may impact you more than others. Just as it took doctors years of research to determine healthy vs.

unhealthy levels of cholesterol and blood sugar, it will either take years to determine such factors in the process industry, or management will simply have to decide what percentage of missing PSM Jenga pieces they are willing to tolerate from a risk perspective. How comfortable would you be telling your insurance carrier, or an OSHA inspector, "Yes, we realize we were only 70% compliant with the regulations and standards, but we were comfortable with that. We generally do what we intend to do in our procedures and processes."

Additional ways of preventing accidents

Diversity of thought and experience. High reliability organizations (e.g., aircraft carriers, nuclear power plants) consist of people and groups who have the authority, credibility and courage to stand up and say "no". The chief engineer of Morton Thiokol (the manufacturer of the solid rocket boosters for the space shuttle) voted "no" for the launch of the Challenger due to the unprecedented cold weather. Yet he was pressured by others and reluctantly consented to the launch. Managers should avoid being surrounded by 'yes' men, and bad news needs to be able to go up within an organization. It does an organization no good to be staffed by clones that all think alike, are afraid to speak up, and easily succumb to group-think. Engaging in industry associations or utilizing trusted consultants to gain outside insight for some important decisions is one way of imparting diversity.

Utilize Professional Engineers. Not all Engineers are licensed; the "industrial exemption" still remains. Licensed Engineers are held to a higher standard of professionalism and ethics. When there's a catastrophic accident, there are often calls to change regulations and demand that Professional Engineers (PEs) be involved in, or at least oversee, all such future work (e.g., Deepwater Horizon, 2018 Massachusetts pipeline explosions). This is actually what brought about many of the state PE regulations upwards of 100 years ago. While PEs are obviously not infallible, their use would represent a helpful level of diversity of thought and experience.

Involve outsiders in management of change activities. Effective management of change is required by regulations worldwide. Many accidents were not the result of a single, simple change. Bhopal was a classic example of many changes, made over many years, by many different people, all operating with the best of intentions. While the impact of a single change may appear to be insignificant, the combined impact of many changes over time may allow an organization to drift into failure. Again, outsiders may provide a fresh perspective of changes. Outsiders do not necessarily have to come from outside the *company* (i.e., they could be from a corporate support office), but such diversity can be beneficial. Outsiders may think very differently about a proposed change than insiders might. Outsiders may help insiders calibrate what is "normal" in the rest of industry.

Utilize outsiders for assessments. While a one-time assessment can't reveal *everything* about a complex system/organization (and the potential result of all the possible interactions), it can help an organization realize how off-center they might actually be. Someone once said, "It's best to have an outside audit because you can't smell a dead rat in your own house." The rat may have died years ago, but everyone in the household slowly got used to the smell and no longer even notices. Yet that's likely the first thing an outsider would notice stepping into the home. It's similar to going to a doctor for a yearly checkup. You might feel fine, but the doctor might find significant things that you should be aware of. Some people apparently don't want to visit a doctor for that very reason. But ignoring the problem and burying your head in the sand like an ostrich is not going to make the problem go away.

Conclusions

- Traditional accident investigations and their conclusions have not been as helpful as desired. Searching for the single root "cause" of an accident, and then trying to somehow place blame, does not account for the complexity of modern systems, and the many small changes that occur over time within all organizations, which may result in an organization drifting into failure.
- Process safety management is much like a Jenga tower. There are many individual pieces that all contribute to the stability of the organization. If enough pieces are removed, the organization may experience an accident. Yet process safety, like personal health, is more than just a binary state. There are many stages of both personal and organizational health. How unhealthy might you or your organization need to be in order to accept the need for change?
- Control theory could be used to monitor the health of an organization. Various *leading* indicators representing economics, workflow, and safety factors could be tracked, monitored, and controlled to help keep an organization in the sweet spot of all three. This could help prevent the organization from drifting into failure.
- Accidents could be prevented if industry would incorporate certain aspects of recognized high reliability organizations. Departments and people should have the authority, credibility and courage to stand up and say "no" when they are aware of, or asked to consider, unsafe practices.
- Accidents could be prevented if industry would incorporate greater diversity of opinion in their decisions, management of change, and gap assessments. Outsiders can provide greater diversity of opinion, and often greater experience, than insiders.

References:

1. "What Went Wrong? Case Histories of Process Plant Disasters", Trevor A. Kletz
2. "An Engineer's View Of Human Error", Trevor A. Kletz
3. "Learning from Accidents", Trevor A. Kletz
4. "Process safety management of highly hazardous chemicals", 29 CFR 1910.119
5. "The 100 Largest Losses 1974-2015, large property damage losses in the hydrocarbon industry, 24th edition", 2016, Marsh Ltd.
6. "Drift into failure", Sidney Dekker
7. "Rethinking Bhopal", Kenneth Bloch
8. "Cognitive Systems Engineering", Rasmussen and Pejtersen
9. "Process Safety Metrics: Guide for Selecting Leading and Lagging Metrics", AIChE CCPS
10. "Process Safety Performance Indicators for the Refining and Petrochemical Industries", API RP 754
11. "Engineering a Safer World: Systems Thinking Applied to Safety", Nancy G. Leveson
12. "Streetlights and Shadows", Gary Klein

Author bio:

Paul Gruhn is a Global Functional Safety Consultant with aeSolutions in Houston, Texas. Paul is an ISA (International Society of Automation) Life Fellow, a 25+ year member and co-chair of the ISA 84 standard committee (on safety instrumented systems), the developer and instructor of ISA courses on safety systems, the author of two ISA textbooks, and the developer of the first commercial safety system modeling software. Paul has a B.S. degree in Mechanical Engineering from Illinois Institute of Technology, is a licensed Professional Engineer (PE) in Texas, a member of the Control Systems Engineering PE exam committee, and both a Certified Functional Safety Expert (CFSE) and an ISA 84 Safety Instrumented Systems Expert. Paul is the 2019 ISA President.