Human Factors and the Impact on Plant Safety

Abstract

History is full of technology breakthroughs, all striving to increase productivity and efficiency, from the steam engine and the telegraph; we've seen technology changing the way we get things done, sometimes in a disruptive way.

Most recently mission critical computing systems have been introduced in manufacturing processes and automated tasks, resulting in increased safety and productivity during normal operation, but can these technologies help keep the plant safe during abnormal process conditions? That's where technology can support but not replace humans. The industry relies on human ability to respond to the unexpected, to handle the odd conditions and ask the right questions to fix the problems at hand.

Today, operators are loaded with numerous activities, is it reasonable to expect they'll be able to respond appropriately to all conditions, what are the human elements that should be taken in to consideration in the design and implementation of modern automation systems?

These issues and more will be addressed in this white paper.

Key words

Safety Instrumented System, Human Factors, Plant Safety, Process Safety, Risk Reduction

Author

Luis M. Duran
TUV FS Eng# 902/07
Product Marketing Manager Safety Systems
ABB
Houston, TX
e-mail: luis.m.duran@us.abb.com

What is the issue?

Start ups and shut downs remain the most tenuous time for any plant. The timing, technology, knowledge of technology, and adherence to procedures are vital.

Operating procedures should clearly lay down instructions for operation of the process plant. The procedure needs to represent a best practice that should occur at all times. Process operators should have guidance concerning the required operating philosophy to ensure they run the plant efficiently, comply with procedural requirements and properly identify abnormal conditions and respond accordingly. On top of that, adequate training should ensure operators are fully conversant with written procedures.

That is where people, process and technology all have to work in unison to make sure the plant starts or stops without incident. Yes, technology is always there to ensure the manufacturer has the correct tools and surely there is a process in place that earmarks the correct path. But what about the Human Factor? Just how does the human play into the impact on plant safety?

Technology is the key to any operation today, but humans factor into every aspect of the facility's lifecycle from design to operations and maintenance. But human factors analysis in the process industries found basic automated actions are reliable to one in several hundred thousand occurrences. To take it one step further, for certified safety systems the reliability is even higher at reliability levels approaching one failure in one million reoccurrences. But when it comes to manual actions, the reliability drops dramatically to 1 in 100 occurrences or less depending on environmental conditions such as mental stress during an abnormal event.

While through a concerted effort on process safety compliance via training, automation and enforcement there has been a dramatic drop in process safety incidents.

However, over the last five years, there has been a change. Incidents have not gone up, but rather there has been a plateau level where incidents remained low, but the infrequent incidents that do occur are more severe and costly. Root-cause analysis indicates in spite of the high degree of automation, operator training, and behavioral enforcement, error due to human judgment continues to be troubling.

These human failures are not the result of poor training, poor management systems, or unreliable machines or lack of information. In a large portion of the most recently reported process safety management incidents, these events occur with highly experienced operators. They just seem to make the one out of 100 errors in judgment which places them in the line of fire.

The question is, "If automation, training, knowledge and experience all in place, why is operator error most frequently identified as a significant contribution to the incident root cause?" One hypothesis is we have reached a saturation point between the operator, structured instruction and the automation systems. With saturation comes human overload. Add in additional environmental stress and you have a combination for failure.

Case in Point

To judge the importance of the human factor, take a look at the disaster at the BP plant in Texas City, TX, where 15 people died and 170 others suffered injuries in a massive explosion and fire during the start up of the isomerization process unit in March 2005.

Texas City had problems just about everywhere. They had antiquated equipment, corroded pipes about to burst, and safety alarms that didn't work. On top of that, there were three key pieces of instrumentation scheduled for repair, but it never happened. Add in the additional pressure to get the plant started up along with consistent lack of operating discipline, deviations from safe operating practices and complacency toward serious process safety risks.

While Texas City is a text book case of how technology, process and humans were not working on the same page, the idea that people could have prevented that catastrophe screams out beyond the headlines.

While well known, a little background shows that on March 23, 2005, a hydrocarbon vapor cloud explosion destroyed BP’s isomerization process unit. The Texas City Refinery was the second-largest oil refinery in the state, and the third-largest in the United States with an input capacity of 437,000 barrels per day. Reports suggest the direct cause of the accident was “heavier–than-air hydrocarbon vapors combusting after coming into contact with an ignition source. The hydrocarbons originated from liquid overflow from the F-20 blowdown stack following the operation of the raffinate splitter overpressure protection system caused by overfilling and overheating of the tower contents.”

BP and the Chemical Safety and Hazard Investigation Board (CSB) identified technical and organizational problems at the refinery and within corporate BP. Organizational failings contributed to the human factor in the incident with corporate cost-cutting, a failure to invest in the plant infrastructure, a lack of corporate oversight on the safety culture and major accident prevention programs, a focus on occupational safety and not process safety, a defective management of change process, the inadequate training of operators, a lack of competent supervision for start-up operations, poor communications between individuals and departments and the use of outdated and ineffective work procedures which were often not followed. There were technical failings as well, including a blowdown drum that was of insufficient size (which would have been identified in the HAZOP procedure), a lack of preventive maintenance on safety critical systems, inoperative alarms and level sensors in the ISOM process unit and the continued use of an outdated blowdown drum and stack technology when replacement with the safer flare option had been a feasible alternative for many years.

There is no doubt Texas City was a combination of human factors, but that disaster was an end point that started long before that fateful day. Other organizations in the industry face that same scenario every day where features and procedures that operators should follow to properly run the system ended up bypassed – not out of negligence, but out of expediency. With the proper systems in place reinforcing a solid safety culture, you could most likely erase one disaster from the record books.

It would be possible for humans to eliminate errors by keeping a vigilant eye toward asset optimization where the user could right click and get access to procedures and configuration guidelines. In addition, through an integrated control and safety system it would be likely to catch alarm failures and the lack of adequate safeguards and use of outdated process design.

In addition, a warning or event indication would be able to alert the operator or maintenance workers if there was a recirculation automated level control valve left closed during startup or if there were failures or breakdowns not attended where a work order ended up closed without job the completed.

Humans are Fallible

Hardware and software systems have improved immensely over the past 30 or 40 years through the use of automated procedures, proper audit trails, management of change process, alarm management, situation-based displays, human-centered HMIs and control room design, but with humans still in the loop either in the design, operation or maintenance there has to be an understanding that mistakes will happen. Humans are fallible and they make high degree of errors and that has to be taken into account which means there has to be a very robust system.

That is where process safety and integrity management can come together. Process safety is the prevention of unplanned and uncontrolled loss of containment from plant and process equipment that might cause harm to people or the environment. That definition works hand in hand with integrity management which is the assurance that plant and equipment are fit and ready to go by establishing competent people, effective systems and dependable assets.

Benefits from integrated safety and integrity management include:

- Being in control, resulting in improved health, safety and environmental performance; full regulatory compliance, and business performance benefits, including higher plant availability, improved output and more reliable customer provision
- Reduced costs, including maintenance costs
- Compliance with the ability to reliably meet ever more demanding regulatory requirements
- Technology backbone to a culture that ensures safety and integrity are integral parts of day to day operations.

Delivery of performance which means a more proactive approach and managing improved performance sustainably.

Risk Reduction

In an industrial facility, it is all about reducing risk and to do that a manufacturer has to design in inherently safe processes. Industrial processes have a built in danger and that means accidents should always be at the forefront of everyone’s mind. But with a strong safety culture, the potential for accidents can significantly lower through a constant assessment of the significance of safety events and issues to ensure each receives the appropriate level of attention.

Part of those assessments will include the idea that system design must follow safety standards that include an ongoing continuous improvement cycle based on periodic Hazard Analysis or HAZOP.

Also, asset management systems must undergo regular testing and maintenance in accordance with safety procedures. Proper asset management must include an alarm management strategy with warning or event indication to alert the operator and maintenance when maintenance is due.

Integrated safety systems to plant automation are an important technology trend across the industry seamlessly displaying critical information or alarms. Utilizing common reporting tools for safety and basic process control systems (BPCS) creates an environment for consistent analysis and breeds familiarity with safety systems for the operator.

Operator effectiveness needs to be taken into account. Effective operator ergonomics will improve the work environment which will have a positive impact on alertness, which removes the potential to miss critical information due to fatigue. With extended operator workplaces with interactive personal large display, the operator has a greater overview of the complete process; better working height and viewing angle; increased sitting comfort and legroom; better ambient lighting; reduced noise level and traffic, and console proximity to communications and collaboration.

Even with multiple technology protective layers, manufacturers need to enforce a strong safety culture that reaches every level -- and it has to start at the top.

Technology and Training

Systems can undergo a design to react properly to an incident, but it can't just stop there. Operators will need proper training. The system cannot prevent every little discrepancy, but the right problem solvers in the right culture with the right technology will solve problems before they escalate.

One way to ensure a safe environment is to implement lifecycle management that will not only allow the user to work with issues that are known today, but also tackle those that appear down the road.

When looking at the human factors, think about the entire lifecycle. When the designers created the system, did they understand the risks? Did they use reasonable levels of probability? How about the consequences? Did they mitigate those factors?

Equipment will continue working for years, but other factors intervene. Just how sure is everyone that valves that have been in place for 20 years or so will open or close as they should during an emergency situation? Have they been tested and how do you know they will work?

Technology will not fix a problem unless the right processes and the right best practices are in place. Technology will help enable people to make the right decision. But the culture has to be there to enforce them to make the decision in the first place.

Human Factor Squeeze

One idea where technology may advance to the point where manufacturers may be able to tighten up the human factor is using a combination of software and wireless to improve manual operations.

This is where the manufacturer can eliminate human interfacing in a manual safety setting by using computer integration techniques to combine manual procedures with automated equipment.

One example would be the frequent case of loading or offloading a truck with a chemical at a facility. In that procedure there are a number of valves and pumps and not all of them are automated. In most cases users do not have automation on the valves that line up equipment from one tank to another and from one line to another, so that ends up being a manual procedure to "lock this" and "turn on that" to control the actions. What if the workflow to those manual actions used mobile technology and checklists? In this case, the operator does his manual task by checking the box in the mobile device and that sends a signal back to the control system which provides interlocks to the flow control and pumps and switches so it assures the operational state or readiness. It integrates the manual task with the automated action.

This future technology shift error proofs the manual action that does not have I/O and still needs the human to initiate the task. It automates the workflow and allows the completion of the workflow with the automation system.

Addressing the Human Factor

Technology does go a long way toward handling safety issues that can arise, but humans do remain the vital part of a safety solution.

The following are some recommendations to keep everyone tuned into plant safety:

- Use check lists: Create a check list and then have a co-worker verify the checklist. With tablets becoming more commonplace, that will be a big assist.
- Fool proofing: Recognize some operations are highly critical and sit down and make sure everyone understands that and then find the answer to the question of how can we make this foolproof in the human interaction.
- Flag changes: Operators and maintenance users get a flag that tells them when systems end up moved off automatic and into manual. Flagging should make workers aware when others make changes and what that means to the safety of the plant.
- Communication: Workers need to cross check and talk through an issue; create a collaboration table where people can have a look at the plant digitally where they can cross check and look at diagrams and understand the ramifications behind any decisions.

Near Misses

One area manufacturers need to focus on is not just reacting to a problem, but also assessing near misses. All factors should come into play in a true safety lifecycle management program. A cycle for continuous improvement in safety performance also should be in place to track any near misses, analyze them for root causes, and use the results to further improve safety system performance. This is another area where technology (such ICSs) can help an operator track the right KPIs that plant management already established.

In the case of Texas City, not calibrating the instruments properly may seem like a small issue, but after a period of time of ignoring a seemingly small issue, that may have caused a slight performance blip which ended up starting the countdown to a disaster.

Proper management of the safety lifecycle requires trained and certified workers. Along those lines, maintenance of safety-related equipment often goes overlooked and that means operations and maintenance personnel need training and certification in testing safety systems.

Better adherence to maintenance practices is a must. Asset integrity management systems can help bring about a more proactive maintenance strategy and can even reduce maintenance costs.

Standards Set the Tone

In short, safety often relies upon adhering to a company's standards or the industry standards like IEC's 61508 and 61511 standards. What is interesting to note, and something most manufacturers should keep a vigilant eye on, is just about 66 percent of safety instrumented systems in use today predate these standards.

And while the U.S. implementation of IEC 61511, or ANSI/ISA 84, includes a "grandfather clause" for older systems, its insistence that operating companies ensure safety systems end up "designed, maintained, inspected, tested, and operating in a safe manner" leaves no room for less-than-rigorous safety system discipline.

While the IEC Safety Instrumented Systems (SIS) standards are not legal requirements such as in the United States, their growing acceptance as descriptors of industry best practices means that non-compliance may have very real liability implications in the event of an incident. And in some regions and industries, compliance already carries the force of law like in the United Kingdom, Germany and Australia. One economic plus is if manufacturers can prove compliance, it may help operating companies reduce insurance premiums.

Purposely non-prescriptive in nature, the IEC safety standards outline a holistic methodology for managing every stage of a safety systems' lifecycle — from risk analysis and design engineering through operations, management of change and decommissioning.

Elements relevant to safety systems performance assessment include adherence to accepted risk evaluation and mitigation methodologies such as process hazards analysis (PHA), hazards and operability (HAZOP) analysis, and layers of protection analysis (LOPA).

Risky Business Means Accidents

Even when precautions are in place to reduce the risk of accidents, they will happen. Nearly 3 million nonfatal workplace injuries and illnesses ended up reported by private industry employers in 2011, resulting in an incidence rate of 3.5 cases per 100 equivalent full-time workers, according to the U.S. Bureau of Labor Statistics.

In addition, there were 4,693 fatal work injuries recorded in the U.S. alone in 2011, compared to 4,690 fatal work injuries in 2010, according to the Occupational Safety and Health Administration (OSHA).

A majority of the industrial accidents that occur every year are a result of human error. Those incidents occur as a result of improper training of personnel. Systems can have the right design to react properly to an incident, but manufacturers need properly trained workers to ensure the safe handling of a problem.

Manufacturers need to have an action plan of best practices to ensure a safe environment. They need to:

- Set up procedures for reducing incidents that include proactive asset management and written standard operating procedures.
- Perform comprehensive hazard assessment after every incident or accident to ensure equipment meets baseline protection levels at minimum.
- Manage process safety as an all-inclusive effort where all parties (including third-party contractors) possess appropriate process safety knowledge and expertise. Root cause analysis of incidents leverages lessons learned and adds to the overall body of knowledge.
- Consider an integrity management system to gain more knowledge of the current state of all plant equipment as it relates to safe operations.
- Do retrospective HazOp implementing “what if” scenarios. If the plant has been running 10 to 15 years, every five years the plant should do a HazOp test to make sure everything is working.
- Layers of protection analysis (LOPA). This is to overcome human factors where plants undergo changes over the years. People have modifications like add ons or close offs. This type of analysis would inform what was working and what was not.
- Asset integrity management. This is for the mechanical items on a production plant. Make sure the control valves, the emergency relief valves, piping and pressure vessels, etc. undergo inspections at defined frequencies.
- Alarm management. A root cause of the Three Mile Island nuclear plant incident was the operators ended up swamped with alarms. Operators had dozens of flashing lights and they couldn’t tell the wood from the trees. Alarms need to be put into context. Now there are emergent standards coming out that allows for a certain amount of alarms in 10 minutes.

Safety goes beyond just ensuring processes remain stable. By having a solid plant and ensuring a strong safety culture where all users remain involved at all times, safety does have a direct link to increases in production and decreases in incidents. The issue is not enough manufacturers are looking at the big picture and realizing just what a strong safety program brings to the bottom line.

As Trevor Kletz, an adjunct professor of the Texas A&M University Artie McFerrin Department of Chemical Engineering, said during the CSB investigation of the Texas City Disaster, “If you think safety is expensive, try an accident. Accidents cost a lot of money; not only in the damage to a plant and in claims of injury, but also in the company’s reputation.”

Sources:

Conning, Tony (ABB). Personal Interview. August 2013
Williams, Mike (The Dow Chemical Company). Personal Interview. August 2013
www.CSB.gov
http://www.cbsnews.com/8301-18560_162-2126509.html
http://www.bp.com/liveassets/bp_internet/globalbp/globalbp_uk_english/SP/STAGING/local_assets/assets/pdfs/Baker_panel_report.pdf
http://www.bls.gov/news.release/pdf/osh.pdf
http://www.bls.gov/news.release/cfoi.nr0.htm