CHEMICAL ENGINEERING TRANSACTIONS
VOL. 31, 2013
A publication of AIDIC
The Italian Association of Chemical Engineering
Online at: www.aidic.it/cet
Guest Editors: Eddy De Rademaeker, Bruno Fabiano, Simberto Senni Buratti

ISBN 978-88-95608-22-8; **ISSN** 1974-9791
DOI: 10.3303/CET1331069

On the Impact of Human and Organizational Archetypes on Human Failure Probabilities Used in Risk Analyses

Anna Letícia de Sousa*[a], Paulo Fernando Ferreira Frutuoso e Melo[b], Juliana Pacheco Duarte[c], Antonio Carlos de Oliveira Ribeiro[d]

[a] National Nuclear Energy Commission, CNEN, Rio de Janeiro, RJ, Brazil
[b] COPPE, Nuclear Engineering Program, Federal University of Rio de Janeiro, RJ, Brazil
[c] Polytechnic School, Department of Nuclear Engineering, Federal University of Rio de Janeiro, RJ, Brazil
[d] Bayer CropScience, Belford Roxo, RJ, Brazil
alsousa@cnen.gov.br

In a previous paper a radar diagram showing the influence of a set of ten features has been presented, discussed and their influence on human failure probabilities has been assessed. Among these, the most important features were management of change, control center design, and training. In this paper, we discuss the use of organizational archetypes in process plants in order to estimate human failure probabilities more realistically by bringing safety culture into stage. The analysis of archetypes is justified not only for the Tokaimura plant, as discussed in this paper, but also for most organizations, where safety efforts are credited to design, and safety restrictions accomplishment during operation is not trivial, even for those organizations with good safety standards. Generally, inadequate cost, schedule, and performance considerations lead to consequences with greater impact on deviations and incidents. The archetype analysis presented considers nonlinear interactions of factors that influence the maintenance of safety level. It produces good indicators of safety management plan improving during operation. This analysis becomes a relevant tool for facilities where safety culture is not strong.

1. Introduction

Strong evidence from accident investigations in hazardous process industries shows that 67 % of the notified accidents are caused by human failures (EC, 1993).
Particularly, in facilities that deal with dangerous technologies it is highly desirable to link the contribution of human factors to safety management through a holistic model (Bellamy et al, 2008). Safety is an emergent property of a system and cannot be determined or explained by the sum of its components alone. Compared to technical factors, the human and organizational components of a technological system are characterized by their multi-dimensional nature and intrinsic complexity due to nonlinear interactions that influence their behaviour (Zio, 2009).
Human Failure Probability (HFP) quantification in a facility or organization should be an individual approach. Many studies on human failure have been developed in last years (Gambetti et al, 2012). We can consider Reason (1990) as a precursor of these studies. The TMI nuclear accident was strongly influenced by human failures and in sequence Swain developed THERP (Swain and Guttman, 1983). HFP values from this technique are also used nowadays in semi-quantitative hazards analyses, like LOPA (AIChE, 2001). Other techniques have been proposed, like ATHEANA (NRC, 2000) and CREAM (Hollnagel, 1998). All of them take into account Performance Shaping Factors (PSFs) that contribute to adjust HFPs. Basically, HFP is an average of a number of observations and a probability density function (pdf) represents the uncertainties of these observations. PSFs are used to translate this average to the upper or lower limit from the pfd statistical confidence interval.

Please cite this article as: Sousa A.L., Frutuoso E Melo P.F., Duarte J.P. and Ribeiro A.C.D.O., 2013, On the impact of human and organizational archetypes on human failure probabilities used in risk analyses, Chemical Engineering Transactions, 31, 409-414 DOI: 10.3303/CET1331069

In a recent paper (Sousa et al, 2012), a methodology to incorporate human factors into HFPs, based on the OGP Model used in a CCPS guideline on human factors (AIChE, 2007) is discussed. An auditing check list was adapted from this guideline and it gives us a tool to create a factor for adjusting the existing data from the aforementioned techniques. Twelve features related to people, technology and organizational factors compose the check list. The global adjusting factor is composed by an auditing factor and three further weighting factors: 1) expert opinion; 2) a cognitive map created by the authors, based on systematic thinking theory (Senge, 1990) and system dynamics (Sterman, 2000); 3) past accidents (retrospective analysis).
The method presented in Sousa et al (2012) allows for a more detailed analysis of human and organizational features in a process plant. The objective of this paper is to go a step further in the discussion by considering archetypes (Marais and Leveson, 2006) for evaluating the impact of safety culture of organizations over human failure probabilities.

2. Case Study

In Sousa et al (2012) the accident at Tokaimura was used as a case study. It was found that the final value of Tokaimura's HFP is 14 times the nominal HFP taken from elsewhere (NRC, 2000, Hollnagel, 1998). This shows that consideration of human and organizational factors provides a more realistic view of plant behavior.
An important contribution of the model is to allow seeing how features relate and how they influence HFP estimation, which allows directing efforts in the short and long term to reduce HFPs or even review the effectiveness of efforts being made to reduce them.
We can see in Figure 1 the influence of each feature on the estimated HFP for the Tokaimura event. It can be observed that features 1, 4, 5, 9 and 11 are the most important. This radar chart can be considered as a good tool to assist in directing resources and efforts to improve the safety function.

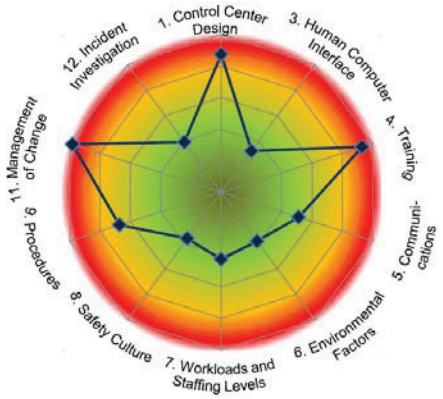

Figure 1: Radar chart of the relative influence of features on HFP estimation (Sousa et al, 2012).

One of the factors of the proposed model takes into account a retrospective analysis (by considering plant abnormal events) and it is able to highlight deficiencies, so that it is important to determine pathways starting from this analysis through the use of new tools, like system dynamics archetypes (Marais and Leveson, 2006).
Incidents are typically analyzed in such a descriptive way (focusing on `who', `what', `where' and `when') that only highly visible human and technical factors are unveiled. As pointed out by Lindsay (1992), to ensure that event investigations be detailed, they should include: (i) systems and organizational aspects, such as relevant policies, standards, rules and procedures, (ii) the work, including the premises, plant, substances and procedures in use and their effect on the employees concerned, (iii) the employees behavior, suitability and competence and the reasons for any performance deficiencies.
The use of archetypes allows one to incorporate non-linear elements that are known to influence unusual occurrences in process plants. Consideration of the influence of nonlinear factors will increase the accuracy of HEP estimation. Additionally, it is possible to structure the recommendations of post-accident investigations, highlighting the mechanisms or cause groups that led to accidents by considering gaps in the organization safety culture. A complementary assessment of safety archetypes can help those plants where it is impossible to perform a retrospective analysis.

3. The use of archetypes in the Tokaimura accident analysis context

3.1The Tokaimura accident

IAEA (1999) concluded that the Tokaimura nuclear fuel processing plant accident seems to have resulted primarily from human error and serious violation of safety principles, which together, led to a criticality event.

Tsuchiya et al (2008) conducted a detailed analysis of the Tokaimura accident and rose the causal factors that triggered it. For the authors, human failure is a behavior (an act or omission) that alone or in conjunction with another behavior can contribute to the cause of an event. However, the author points out that to attribute the cause of an event to human failure, without deeper explanations is of little or no use for the correction of causal factors or to address the implications. Human failure cannot be corrected, but rather its underlying causes, once they are known. The main causal factors of vulnerability are: (i) international price competition forcing to establishing management policies by JCO (Japan Nuclear Fuel Conversion Company) to increase efficiency; (ii) sale drops and a consequent reduction in the number of workers; (iii) impacts due to deregulation, facing an aggressive public opinion, and increasing commercial competition.

The results also highlight the influence of commercial success - sometimes even survival - in a competitive environment implying support and connivance to operate outside the usually accepted practice; consensus in exploring limits in critical situations, which involves taking the risk of crossing the boundaries of safe practices; inadequate awareness of risks by senior management of JCO, who are former executives or employees borrowed from its parent company, Sumitomo Metal Mining Company Ltd, which had no experience in the business beyond JCO nuclear plant; assuming that a nuclear criticality accident was impossible to occur, neglecting lessons learned from previous criticality accidents in other countries.

Furthermore, the practice of the kaizen concept units resulted in ignoring certain design features established to avoid critical situations, but at the same time turned operations slower and more expensive. The revised company's operation manual violated the original instructions, which had been approved by the licensing authorities. Kaizen is a continuous improvement process that involves everyone taking small, incremental steps to pursue the goal relentlessly over extended time (Tsuchiya, 2001). In Japan, the concept of kaizen is so deeply rooted in the minds of both managers and workers that often they do not even realize that they are thinking kaizen. JCO had completed at least four kaizen campaigns and this "improvement" was the seventh. Since it is expected that all kaizen-based activities lead to greater customer satisfaction, it was natural that the kaizen emphasis in JCO had been on efficiency, cost reduction and quality improvement, not safety. Workers should take the initiative of kaizen, the manuals were often revised after workers had changed procedures and workers felt free to "improve" the production process, without official approval by supervisors. The famous Japanese kaizen tradition was conducted by workers with inadequate training, ultimately leading them to cross the boundaries of safe practices.

It is evident in the analysis of Tsuchiya et al (2008) that the criterion of perceived success by senior management is a factor to be considered in the degradation of the safety function. Another factor is the human resource. In the Tsuchiya et al (2008) approach both factors, reducing the number of workers as well the qualification of these are noted as relevant to maintain workers' competence. The little or no importance of safety organization is well evidenced in the analysis of Tsuchiya for their participation in decision-making. Complacency or deficiency of regulatory action is evident in both analyzes presented. The working procedure was modified in 1996 (three years before the accident) and regulators had not approved the new procedure.

3.2The use of archetypes of system dynamics

Effects are rarely proportional to causes and what happens locally in a system (near the current operating point) often does not apply in distant regions (other system states, so that one has to consider the so-called nonlinear interactions (Sterman, 2000). This is the case, for instance, with human probability failure estimations and safety level identification. Non-linear interaction and dynamic behaviour assign complexity to systems and these latter can be modelled by decomposing them into behavioural flow towards events, for which feedback mechanisms may be relevant.

Archetypes are used to develop dynamic models and treat these nonlinear interactions for describing organizational and systemic factors, that might contribute to an accident. Additionally, archetypes help clarify that safety-related decisions do not always result in the desired behavior, and how independent decisions in different parts of the organization may combine and result in an impact on safety.

Based on IAEA (1999) and Tsuchiya et al (2008), it is possible to recognize that the following archetypes (Marais and Leveson, 2006) can be helpful:

- Safety issues stalled in the face of technological advances;
- Decreased safety awareness;

- Fixing on symptoms and not the real causes;
- Unintended side effects of safety solutions;
- Eroding Safety.

The first archetype evaluates the stagnation of safety topics in the face of technological advances. It is possible to observe that technological advances result in an increase in performance in many areas, which in turn lead to further advances. Due to accelerated changes, safety understanding implications are left aside, leading to loss of safety function. Typically, organizations with a reasonable safety commitment have a low incidence of events associated with this archetype, and this fact is justified by the practice of performing safety analyses before implementing design changes. However, one must strengthen that management programs as well as design change management control are elements with great influence on the estimation of human error probabilities.

The second archetype (decreased safety awareness) takes into account that whenever a safety program reaches fullness and success is realized by organization's top management staff sets up a dynamics that can eventually get a decrease in safety. The perception of success pushes boundaries, and increases pressures and expectations of better performance by reducing the safety priority. Another consequence is the reduction in safety resources allocation. According to Rasmussen (1997), a system super performance leads to new risks that may materialize in the form of disastrous accidents.

In most organizations the fixation on symptoms illustrates the stress between the appeal of short-term symptomatic solutions and long-term impact of fundamental solutions. Symptomatic solutions are usually easier, faster and cheaper to implement than fundamental long-term solutions.

The archetype that shows the competition between the symptomatic solutions and fundamental solutions is based on the fact that in most organizations positive results of symptomatic solutions are immediately seen, since the visible symptoms are eliminated. Once a symptomatic solution has been successfully applied, the pressure to implement a basic solution tends to decrease. Solutions may become less effective over time or different symptoms of the underlying problem may arise, and in response new symptomatic solutions are designed and implemented.

A significant number of reports of root cause analysis is restricted to the immediate removal of causes and causal factors. This approach (correct only the immediate cause) is a simplistic approach that may prevent a similar incident to occur again in the same place, but will not prevent similar incidents. Another problem arising from this approach is the occurrence of unintended side effects. This archetype shows some situations where the fundamental problem is not understood, or when solutions to the fundamental problem are not appropriate or are improperly implemented.

The archetype that analyzes eroding safety shows how safety objectives can be eroded or become subverted over time. Often this declining trend is difficult to observe because change tends to happen gradually. On reduced time scales, changes may be imperceptible. Usually, only after the occurrence of an accident the scale of change is noticed in its entirety.

Usually, root cause analyses generate a large number of recommendations over time and these measures are not part of an action plan, so that the organization loses the potential benefits of preventing the occurrence of new adverse events.

Another contributing factor, is the apparent lack of or inappropriate judgment of a safety threat for oversight may seem draconian and unnecessarily costly. Coupled with budgetary pressures, this anti-regulation feeling creates pressure to decrease oversight, which is manifested on one hand by less training and fewer or less strict certification requirements, and on the other hand, by decreased inspection and monitoring. A decrease in these activities eventually leads to an increase of the eroding safety phenomenon.

For modern organizations, safety programs design is usually established or idealized supposing or assuming some conditions. However, one must be aware of the fact that systems are not static and experience changes all the time and certainly some changes will violate pre-established conditions.

According to Leveson (2011), variations usually occur in all parts of the system:

- ••Physical changes: the equipment may degrade or is not properly maintained;
- ••Human changes: human behavior and priorities usually change over time;
- ••Organizational changes: change is a constant in most organizations, including changes in the safety control structure itself.

The system ability to adjust its operation so that it can sustain performance in all conditions (expected or not) is known as resilience. Therefore, despite a safety managing plan, resilience gives it a dynamic behavior that is reflected on safety. The safety plan shall establish controls to reduce the risk associated with the above three types of system variations.

The results presented in Figure 1 and the additional application of the above discussed archetypes for the Tokaimura plant safety show that it is important that the safety management plan is reviewed with a focus on at least the following aspects:

The culture-driven problem correction focus must be shifted to a learning-oriented culture focus, where causes are included in the systematic search for the source of safety problems.

It is important to implement a mechanism for continuous improvement and learning. Identified gaps should not be simply corrected: they must be inserted into a program to improve the safety control structure.

During the system operational phase, failures occur due to defects in physical systems, human errors or failures in the assumptions set out to design the safety plan. The safety management plan must be able to:

- Detect flaws in system design and control safety structures, anticipating further losses;
- Determine errors in the development process, which could allow failures to occur and improve the process to prevent recurrence;
- Determine if the identified shortcomings in the process can make the system vulnerable.

Something needs to be done to ensure safety constraints for systems that are in a dynamic process in their environment. So, Managing Change is required.

Before any planned changes are made, their impact on safety must be evaluated. Most organizations include such controls, by means of management of change procedures. Additionally, it is imperative that responsibility needs to be assigned for ensuring compliance so that change analyses are conducted and the results are not ignored.

While dealing with planned changes is relatively straightforward (even if difficult to enforce), unplanned changes that move systems toward states of higher risk are less straightforward. Procedures to prevent or detect changes that impact the ability of safety control structure operations and the designed controls to enforce safety constraints need to be established (Leveson, 2011).

As shown earlier, in the analysis of the Tokaymura accident, Tsuchiya (2008), people tend to optimize their performance over time to meet a variety of goals. If an unsafe change is detected, it is important to respond quickly.

Here, it is important to be aware of the fact that often an unsafe modification is seen by workers and managers as a manufacturing process optimization. Not to mention that one cannot ignore that the ability to change is a systemic feature. So, managing unplanned modifications must allow modifications that do not violate basic safety restrictions.

Regarding the management changes the Safety Management Plan must have mechanisms to allow flexibility in how safety objectives will be achieved without allowing a flexibility level that could violate these goals.

Training should not be a onetime event, it should be continuous.

For Tokaymura, as for other process facilities, while most of the discussions focused on the design and quality during construction, attention was not sufficient paid to safety during operation and in relation to human performance failures and organizational factors. This shift in focus from design to operation implies that both managers and operators need to understand the risk they are taking due to the decisions they make.

Further understanding the safety rationale, that is, the why, behind the system design will also have an impact on combating complacency and unintended changes leading to hazardous states (Leveson, 2011).

The Organizational Culture should encourage information sharing.

Between 1953 and 1997 there were at least 21 criticality accidents in JCO similar plants and yet managers assuming that a nuclear criticality accident was impossible to install, neglected the lessons learned from previous accidents. The inaccurate risk perception by management led to not taking the necessary control actions.

Additionally, workers were pressured by company to operate more efficiently (kaizen). This is a nonlinaer interaction that induces the violation of safety margins and operation in adverse conditions by seeking process improvements even though it results in safety corrosion.

To maintain a strong safety culture, an appropriate information system is very important. Sometimes, cultural problems interfere with the feedback about the state of the controlled process. If the culture does not encourage sharing information, it is imperative that both, managers and operators, understand the importance of safety in organizational goals.

A businesslike safety management plan is needed.

To guide the operational safety control it is needed to establish and implement a safety management plan. The safety management plan can help the organization maintain the safety levels despite the dynamic behavior of the organization.

4. Conclusions

The analysis of archetypes was justified not only for the Tokaymura plant, but also for most organizations, where safety efforts are credited to design, and safety restrictions accordance during the operation is not trivial, even for those organizations with good safety standards. Generally inadequate considerations of cost, schedule, and performance lead to consequences with greater impact on deviations and incidents. Often, managers are tempted to satisfy the above three objectives (cost, schedule, and performance) at the expense of safety, since these factors that take part in the dynamic behavior usually are not considered in decisions and safety analyzes.

The archetype analysis presented here considers nonlinear interactions of factors that influence the maintenance of safety level. The analysis by means of archetypes produces good indicators of safety management plan improving during operation. The work developed in this paper should go further in order to implement the findings on organizational safety culture in Human Failure Probability estimations. This type of analysis becomes a relevant tool for facilities where the safety culture is not strong, usually labeled as safety culture driven by compliance and standards.

References

AIChE, American Institute of Chemical Engineers, 2001, Layer of Protection Analysis: Simplified Process Risk Assessment. Wiley, New York, USA.

AIChE, American Institute of Chemical Engineers, 2007, Human Factors Methods for improving Performance in the Process Industries. Wiley, New York, USA.

Bellamy, L. J., Geyer, T. A. W., Wilkinson, J., 2008, Development of a functional model which integrates human factors, safety management systems and wider organizational issues, Safety Science, 46, 461–492.

Gambetti, F., Casalli, A. and Chisari, V., 2012, The Human Factor in Process Safety Management, Chemical Engineering Transactions, 26, 279-284, DOI: 10.3303/CET1226047

Hollnagel, E., 1998 Cognitive Reliability and Error Analysis Method (CREAM). Elsevier, Oxford UK.

IAEA, 1999, Report on the preliminary fact finding mission following the accident at the nuclear fuel processing facility in Tokaimura, Japan. Vienna, Austria.

N. Kawka, C. Kirchsteiger, 1999, Technical note on the contribution of sociotechnical factors to accidents notified to MARS. Journal of Loss Prevention in the Process Industries 12 (1999) 53–57.

Leveson, N. G., 2011, Engineering a Safer World – Systems Thinking Applied to Safety-Draft, Massachusetts.

Lindsay, F. D., 1992, Successful health & safety management.The contribution of management towards safety. Safety Science. 15, 387-402.

Marais, C., Leveson, 2006, N. Archetypes for Organizational Safety. Safety Science, 44, 565-582;

NRC, NUREG-1624, 2000, Technical Basis and Implementation Guidelines for A Technique for Human Event Analysis (ATHEANA). Washington, DC, USA.

Rasmussen, J., 1997, Risk Management in a Dynamic Society: A Modelling Problem. Safety Science, 27 (2/3), 183-213.

Reason, J., 1990, Human Error, Cambridge University. Cambridge, MA, USA.

Senge, Peter M. A, 1990, The Fifth Discipline. Random House Inc. New York, USA.

Sousa, A. L., Ribeiro, A., Frutuoso e Melo, P. F. F., Duarte, J. P., 2012, Quantifying human error probability through a human factors assessment too. Proceedings of CCPS 4Th Latin Conference on Process safety, Brazil.

Sterman, John D., 2000, System Dynamics: Systems Thinking and Modeling for a Complex World, Proceedings of the ESD Internal Symposium, MIT, Cambridge, MA, USA.

Swain, A. D. and Guttman, H. E., 1983, Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications. U. S. Nuclear Regulatory - NUREG/CR-1278, Washington, DC.

Tsuchiya, S., Tababe, A., Naruchima, T, Ito, K. and Yamazaki, K., 2001, An Analysis of Tokaimura Nuclear Criticality Accident: A Systems approach, The 19th International Conference of The System Dynamics Society, USA.

Tsuchiya, S., Narushima, T., Inanobe, M., 2008, Knowledge Management Aspect of JCO Nuclear Accident, Chiba Institute of Technology.

Zio, E., 2009, Reliability engineering: old problems and new challenges, Reliability Engineering and System Safety, 94, 125–141.