Comparison of four major industrial disasters from the perspective of human error factor

*Doru Costin Darabont**, *Daniel Onut Badea*, and *Alina Trifu*

National Research and Development Institute of Occupational Safety “Alexandru Darabont” – INCDPM, B-dul Ghencea 35A, Bucharest, Romania

Abstract. This paper presents the preliminary findings of a project still in progress at INCDPM regarding “Knowledge transfer partnership and research development in the assessment and prevention of occupational risks which may conduct to disaster”. After studying the major industrial disasters of our times, it become clear that even with technological advancement, human error is still the major cause of accidents and incidents. Analysis of human error and their role in accidents is an important part of developing systematic methods for reliability in the industry and risk prediction. To obtain data for predictive analysis is necessary to analyse accidents and incidents to identify its causes in terms of component failures and human errors. Therefore, a proper understanding of human factors in the workplace is an important aspect in the prevention of accidents, and human factors should be considered in any program to prevent those that are caused by human error. The comparison between four major industrial disasters (Chernobyl, Bhopal, Deepwater Horizon, Alpha Piper) was made using Human Factors Analysis and Classification System (HFACS), a modified version of "Swiss Cheese" model that describes the levels at which active failures and latent failures/conditions may occur within complex operations.

1 Introduction

During the industry history a series of devastating accidents with huge costs both economical and in human lives have happened. Piper Alpha disaster (1988), Bhopal Gas Plant disaster (1984), Chernobyl Nuclear Power Plant disaster (1986) and BP Deepwater Horizon Oil Spill disaster (2010) are examples of such accidents. Although these accidents happened in different places and time they all have in common, according to analyses and official reports of accident investigations, the role played by human error in triggering the disaster.

Analysis of human error and their role in accidents is an important part of developing systematic methods for reliability in the industry and risk prediction. A predictive analysis requires identifying the accident's causes in terms of component failures and human errors. Therefore, a proper understanding of human factors in the workplace is an important aspect

* Corresponding author: darabont_d@yahoo.com

in the prevention of accidents. The comparison between four major industrial disasters (Chernobyl, Bhopal, Deepwater Horizon, Alpha Piper) was made using Human Factors Analysis and Classification System (HFACS), a modified version of "Swiss Cheese" model that describes the levels at which active failures and latent failures/conditions may occur within complex operations and based on official investigation reports.

1.1 Human error factor

The term "human factors" was defined by Gordon in 1998 [1] as the study of the interactions between human and machine and also includes: management functions, decision making, learning and communication, training, resource allocation and organisational culture.

It has been widely acknowledged the role of human actions in major disasters, with studies concluding that the two types of human error, "active errors" and "latent errors", are responsible for approximately 80 per cent of accidents [2]. The effects of active errors are almost immediate and are more likely to be caused by frontline operators (control room crews, production operators etc.). The "latent errors" are caused by the less-visible organisational issues (time pressure, understaffing, inadequate equipment and fatigue) that accumulate over time.

1.2 Human Factors Analysis and Classification System (HFACS)

The methodology used in this paper is a broad human error framework called "The Human Factors Analysis and Classification System" (HFACS) and it was created to understand the underlying causal factors that lead to an accident without blaming the individuals involved.

The framework of the analysis uses four levels of deficiencies which lead to accident: 1) Unsafe acts, 2) Pre-conditions for unsafe acts, 3) Unsafe supervision and 4) Organisational failures. Within each level of HFACS, causal categories were developed to identify the active and latent failures that occur.

1. The Unsafe Acts level represents the unsafe acts of an operator leading to an incident/accident and is divided into two categories - errors and violations. Errors are unintentional behaviours, actions of the operator that fail to carry out the desired outcomes, and violations (routine violations, exceptional violations) are a wilful disregard of the rules and regulations.

2. The Preconditions for Unsafe Acts level and the first latent tier, is divided into three categories: environmental factors, condition of operators and personnel factors. Environmental factors (physical environment, technological environment) refer to the physical and technological factors that affect practices, conditions and actions of individual and which result in human error or an unsafe situation. Condition of operators (adverse mental state, adverse physiological state, physical/mental limitations) refers to the adverse mental state, adverse physiological state, and physical/mental limitations factors that affect practices, conditions or actions of individuals and result in human error or an unsafe situation. Personnel factors (crew resource management, personal readiness) refer to the crew resource management and personal readiness factors that affect practices, conditions or actions of individuals, and result in human error or an unsafe situation.

3. The Unsafe Supervision level deals with performances and decisions of supervisors and managers that can affect the performance of operators in the frontline and is categorized into four categories: *inadequate supervision* (includes those times when supervision either fails to or provides inappropriate or improper guidance, oversight, and/or training), *plan inappropriate operation* (involves those situations when supervisors fail to evaluate the risk associated with a task, thereby placing employees at an unacceptable level

of risk; these include improper staffing, mission not in accordance with rules/regulations, and inadequate opportunity for crew rest), *fail to correct known problem* (refers to those instances where unacceptable conditions of equipment, training or behaviours are identified, yet actions or conditions remain uncorrected, meaning supervisors fail to initiate corrective actions or report such unsafe situations), *supervisory violation* (the wilful disregard of the established rules and regulations by those in positions of leadership).

4. The Organisational Influences level, and the final latent tier, is divided into three categories: *resource management* (includes top management decisions related to the allocation of such resources as equipment, facilities, money, and personnel), *organisational climate* (refers to those variables, such as the organizational structure, culture, and policies, which affect worker performance), *organizational process* (refers to the decision-making that governs the day-to-day operations of an organization, such as operations, procedures, and oversight).

2 Major industrial disasters

2.1 Chernobyl

2.1.1 Short description of the accident

On April 26, 1986, the Chernobyl Nuclear Power Plant in Ukraine exploded, creating what was considered the worst nuclear disaster the world has ever seen. The Chernobyl plant used four Soviet-designed RBMK-1000 nuclear reactors — a design that's now universally recognized as inherently flawed. RBMK reactors were of a pressure tube design that used an enriched U-235 uranium dioxide fuel to heat water, creating steam that drives the reactors' turbines and generates electricity. The accident occurred during a test executed before the unit shutdown for the planned maintenance. The test aimed to study the possibility of utilization of the mechanical energy of a turbo-generator after cut-off of steam supply, practically to check the possibility of powering the main reactor coolant pumps from one of the turbo-generators for a few seconds while it was slowing down under its inertia in the event of loss of offsite power, thereby providing additional time for emergency takeover by the diesel generators. This test was performed neither under the planned conditions nor in compliance with reactor operating procedures. In particular, several safety systems were disabled [3]. According to the Soviet experts the prime cause of the accident at the Chernobyl nuclear power plant was "...an extremely improbable combination of violations of instructions and operating rules committed by the staff of the unit". This conclusion sets a full responsibility for the accident at the Chernobyl on its staff.

2.1.2 Contributory factors of accident distributed according to HFACS' levels

Organizational Influences

1. Training of personal was insufficient and totally inconsistent with absence of passive safety features in the reactor design. Not knowing much about the behaviour of the reactor core, they were unable to appreciate the implications of the decisions they were making, and their situation was even more dangerous in that the test was being done at low power and in violation of standing orders. 2. Safety procedures not in place. 3. The culture of secrecy, imposed compartmentalization of knowledge: no single person was allowed to see the big picture and to integrate all aspects of the safety of the operation. 4. Political issues. The scientists and engineers worked under one guideline: to produce plutonium - as much as possible and as quickly as possible.

Unsafe Supervision

1. The operating instructions, both the standing orders and the specific instructions for the test, were incomplete and imprecise. 2. Bad communication not only between the operators, but also with authorities and government.

Preconditions for Unsafe Acts

1. A flaw in the reactor design that makes the RBMK reactor core is unstable below 700 Megawatts-thermal, about a quarter of full power, meaning that at low power the reactor is difficult to control and any tendency toward a runaway chain reaction is automatically and rapidly amplified. 2. The insertion of the control rods is too slow, taking about 20 seconds to full insertion while it takes less than 2 seconds in other reactors throughout the world. This is much too slow to prevent runaway of the core while it is operating in the unstable mode. 3. Lack of emergency control rods with fast insertion. The tips of control rods, when inserted, first increase the reactivity. 4. No safeguards that controls the number of rods.

Unsafe Acts Operation

1. The number of reserve control rods in the reactor core was drop below permissible levels, 2. The automatic controls for the reactor's power level were shut off, 3. Both the main water-circulation pumps and the backup pumps were turned on at the same time, forcing the coolant to flow too quickly, 4. Cutting off automatic blocking devices that would have shut off the reactor when steam failed to reach the generator, 5. Switching off systems that controlled water level and steam pressure, 6. Turning off "the most sacred thing" - the emergency safety cooling system for the reactor.

2.2 Bhopal

2.2.1 Short description of the accident

Bhopal accident was the spillage of a very toxic substance - methyl isocyanate (MIC) - to the atmosphere in large quantities from a pesticide plant. It led to the dead of more than 5000 people. The methyl isocyanate (MIC) was stored in three underground tanks made of stainless steel that have to be kept refrigerated so that the temperature of content to be close to 0°C. To prevent release of methyl isocyanate in the atmosphere, after the tank there was a vent gas scrubber that would neutralize the MIC by spraying alkali. Also, then there was a flare tower to burn the remaining gases going from the vent gas scrubber. The plant was shut down for maintenance two months prior to the accident. Due to a series of errors, lack of knowledge and delays in response of operators and supervisors 40 to 45 tonnes of MIC escaped, part of which got decomposed into hydrogen cyanide.

At 2,30 in the morning MIC vapours started affecting people in the vicinity, and a large number of people started running out of the houses. On the morning of 3 December, the local hospital had about 12000 persons. Again on the night of 3/4 December, MIC from the atmosphere recondensed and more people were affected. On the 4 December 1984 Hamidia Hospital had to handle about 55000 people [4].

2.2.2 Contributory factors of accident distributed according to HFACS' levels

Organizational Influences: 1. Carrying out plant modifications in hazardous facilities without hazard and operability studies; 2. Storing 55 tonnes of MIC while usage daily was 5 tonnes; 3. Neglecting safety management at the unit; 4. No action on earlier accident

analysis reports; 5. Heavy reliance on inexperienced operators; 6. decision to reduce operating and maintenance staff in control room/plant;

Unsafe Supervision: 1. using a non-trained superintendent for the plant; 2. failure to recognize that the pressure rise was something abnormal; 3. failure to use the empty MIC tank to release the pressure.

Preconditions for Unsafe Acts: 1. Refrigeration plant was not operational; 2. pressure indicator and temperature indicator not working; 3. flare tower was disconnected; 4. vent gas scrubber not in active mode; 5. plant modification; 6. use of iron pipelines for MIC; 7. no indicator for monitoring position of valves in control room.

Unsafe Acts: 1. Repressurizing the tank when it failed to get pressurized once; 2. failure of shift operator to communicate information on pressure increase to the next operator; 3. issuing orders for washing when methyl isocyanate tank failed to get pressurize; 4. not following the safety precautions while washing MIC lines; 5. failure to recognize the seriousness of the leak; 6. failure to inform Works Manager as soon as the leak started.

2.3 Deepwater Horizon

2.3.1 Short description of the accident

Deepwater Horizon was an ultra-deep water, dynamically positioned, semi-submersible offshore drilling rig owned by Transocean and leased to British Petroleum. On 20 April 2010, while drilling at the Macondo Prospect, an uncontrollable blowout caused an explosion on the rig that killed 11 crewmen and ignited a fireball visible from 64 km away. The fire was inextinguishable and, two days later, on 22 April, the Horizon sank, leaving the well gushing at the seabed and causing the largest oil spill in U.S. waters. Every one of the *Deepwater Horizon's* many defences failed—some were never engaged, some were engaged too late, and some simply did not work as designed. The chain of events between February and the disaster could have been interrupted at many points, but a lack of preparation and experience and an unclear chain of command prevented key decisions at every step [5].

2.3.2 Contributory factors of accident distributed according to HFACS' levels

Organizational Influences: 1. Decision to proceed to temporary abandonment of the exploratory well, 2. Changing key supervisory personnel on the Deepwater Horizon just prior to critical temporary abandonment procedures, 3. Time pressure, 4. Communication was poor among and between rig crew members who worked for multiple companies and shore superiors and middle and top management, 5. Financial pressures to complete the operation quickly, 6. Lack of sufficient training.

Unsafe Supervision: 1. Oversimplified instructions, 2. Last minute changes in procedures, 3. Last minute changes of personnel, 4. Insufficient experience

Preconditions for Unsafe Acts: 1. The Macondo prospect presented a number of technical challenges from the start, such as deep water, high formation pressures and temperatures, and the need to drill through multiple geologic zones. 2. Valve failure, allowing oil and gas to travel up the pipe towards the surface. 3. Leak not spotted soon enough - whether a well is under control or not, the crew at the surface should be able to detect a flow of oil and gas towards the surface by looking for unexpected increases in pressure in the well. 4. No battery for blowout preventer - the explosion destroyed the control lines the crew were using to attempt to close safety valves in the blowout preventer.

Unsafe Acts or Operation: 1. Attempting to cement the multiple hydrocarbon and brine zones encountered in the deepest part of the well in a single operational step, despite the

fact that these zones had markedly different fluid pressures. 2. Using the wrong cement formula - The cement at the bottom of the borehole did not create a seal, and oil and gas began to leak through it into the pipe leading to the surface. 3. Overwhelmed separator - The crew had the option of diverting the mud and gas away from the rig, venting it safely through pipes over the side. Instead, the flow was diverted to a device on board the rig designed to separate small amounts of gas from a flow of mud. 4. Pressure test misinterpreted - The crew carried out various pressure tests to determine whether the well was sealed or not. The results of these tests were misinterpreted, so they thought the well was under control. 5. Failure to observe and respond to critical indicators.

2.4 Piper Alpha

2.4.1 Short description of the accident

The Piper Alpha disaster happened on July 6, 1988. In the explosion and subsequent fire on the oil platform, 167 workers died, while only 61 survived. The death toll was the highest of any accident in the history of offshore operations. The Piper Alpha rig, started initially in 1976 with oil production, being converted to gas recovery in 1980. Unfortunately, this repurposing was poorly made from the point of view of safety (for example, the gas compression units were installed next to the central control room) and wherein lies one of the causes of the disaster. The series of constructions, maintenance and upgrade works diluted the safety features of the four modules of Piper Alpha which were initially separated by firewalls with the most dangerous operations distant from the personnel areas. A lack of communication between operators causes to operate a pump being under maintenance and having a safety valve dismantled. As a result, an important gas leakage occurred. Although six gas alarms were triggered the gas ignited before anyone could act. Further compromises in the safety system were facilitated by further explosions resulting in the gas line melting, which released 15-30 tonnes of gas every second into the fire. The fire was soon being fed by oil from two separate rigs that shared a communal oil pipe. When the platform blew out 167 of 228 workers died. The platform was completely destroyed and it took almost three weeks for the fire to be brought under control [6].

2.4.2 Contributory factors of accident distributed according to HFACS' levels

Organizational Influences: 1. The decision of owners to keep the platform producing oil and gas as it set about a series of construction, maintenance and upgrade works; 2. Lack of training; safety procedures not in place; 3. Insufficient number of crew members.

Unsafe Supervision: 1. Communication breakdown for permit to work PTW; 2. Shift change procedure not properly functioned.

Preconditions for Unsafe Acts: 1. Improper restructuring of platform - the gas compression units were installed next to the central control room; 2. Improper installation of pressure safety valves; 3. Undetected gas release

Unsafe Acts Operation: 1. Placing a vital document in the wrong place; 2. Restarting of a pump in maintenance; 3. Command system failed in emergency.

3 Results and discussions

Table 1 presents a synthesis of the contributory factors of the above analysed accidents. The results indicate that 50% of the contributing factors identified in each of the four accidents reviewed are latent failure in level 2 and level 4. There are environmental factors,

conditions of the operator, personnel factors, resource/acquisition management, organizational climate, and organizational process that shows that is possible for the failures created at higher level to remain in the system for a considerable time without being noticed, thereby creating conditions for accidents to occur during operations.

Table 1. Contributory factors of the analysed accidents

Level of HFACS	Accidents			
	Piper Alpha	Chernobyl	Deepwater	Bhopal
Level 4. Organizational Influences	3	4	5	8
Level 3. Unsafe Supervision	3	2	4	3
Level 2. Preconditions for Unsafe Acts	3	4	4	7
Level 1. Unsafe Acts	3	6	5	6

4 Conclusions

After studying the major industrial disasters of our times, it become clear that even with technological advancement, human error is still the major cause of accidents and incidents. Analysis of human error and their role in accidents is an important part of developing systematic methods for reliability in the industry and risk prediction. To obtain data for predictive analysis is necessary to analyse accidents and incidents to identify its causes in terms of component failures and human errors. Therefore, a proper understanding of human factors in the workplace is an important aspect in the prevention of accidents, and human factors should be considered in any program to prevent those that are caused by human error.

Also, the comparison between four major industrial disasters made in this paper indicates that 50% of the contributing factors identified in each of the four accidents reviewed are latent failure in level 2 and level 4. There are environmental factors, conditions of the operator, personnel factors, resource/acquisition management, organizational climate, and organizational process that shows that is possible for the failures created at higher level to remain in the system for a considerable time without being noticed, thereby creating conditions for accidents to occur during operations and supports the view that all human initiated disasters ultimately can be traced back to deficiencies in the management of the systems at the corporate level. Yet in major accident assessment and prevention, these deficiencies are often overlooked or very inadequately addressed.

References

1. R. Gordon The contribution of human factors to accidents in the offshore oil industry, *J Reliability Engineering and System Safety* **61** (1998) 95-108
2. A. Aas, The human factors assessment and classification system (HFACS) for the oil & gas industry. *Paper presented at the International Petroleum Technology Conference* (2008).
3. INSAG-7 The Chernobyl Accident. A report by the International Nuclear Safety Advisory Group, International Atomic Energy Agency Vienna, 1992
4. Delhi Science Forum Report: Bhopal Gas Tragedy, *J Social Scientist*, **13**, 32-53, (1985)
5. U.S. Chemical Safety and Hazard Investigation Board Investigation report vol 3, Drilling rig explosion and fire at the Macondo well, Report no. 2010-10-i-os, (2016)
6. Departament of Energy, The public Inquiry into the Piper Alpha Disaster, vol 1, November 1990