International Journal of Occupational Safety and Ergonomics (*JOSE*) 2006, Vol. 12, No. 1, 79–93

Safety and Human Factors Considerations in Control Rooms of Oil and Gas Pipeline Systems: Conceptual Issues and Practical Observations

Najmedin Meshkati

Viterbi School of Engineering, University of Southern California, Los Angeles, USA

All oil and gas pipeline systems are run by human operators (called controllers*) who use computer-based workstations in control rooms to "control" pipelines. Several human factor elements could contribute to the lack of controller success in preventing or mitigating pipeline accidents/incidents. These elements exist in both the work environment and also in the computer system design/operation (such as data presentation and alarm configuration). Some work environment examples include shift hours, shift length, circadian rhythms, shift change-over processes, fatigue countermeasures, ergonomics factors, workplace distractions, and physical interaction with control system computers. The major objective of this paper is to demonstrate the critical effects of human and organizational factors and also to highlight the role of their interactions with automation (and automated devices) in the safe operation of complex, large-scale pipeline systems. A case study to demonstrate the critical role of human organizational factors in the control room of an oil and gas pipeline system is also presented.*

human factors pipeline control centers automation human error accidents safety

1. INTRODUCTION

Almost all major oil and gas pipeline systems are run by human operators (called *controllers*) who use computer-based workstations in control rooms to "control" pipelines. The National Transportation Safety Board (NTSB) is charged with the investigation of major accidents in five modes of transportation in the USA, including pipeline systems. Over the past 8 years, the NTSB has conducted 18 accident investigations on hazardous liquid, gas transmission, and local distribution companies' pipelines. Of those 18 accident investigations, the NTSB has identified 10 accidents where "controllers' actions, reactions or inactions, or the computer systems they use, were significant factors in detecting or contributing to the initial event, influencing recovery time or affecting the magnitude of an event" (p. 3) [1]. These 10 accidents which occurred between 1996 and 2000, totally released 11,474,530 L (3,031,250 gallons) of material to the environment and their overall monetary damages and cleanup costs amounted to be more than US $185 million [2, 3].

Human ingenuity can now create technological systems whose accidents rival in their effects the greatest of natural disasters; sometimes with even higher death tolls and greater environmental damage. A common characteristic of complex technological systems, such as chemical processing

In the analysis and writing of this research article, the author has greatly benefited from discussions with Professor Jens Rasmussen (Risø National Laboratory, Denmark), as well as his and Professor James Reason's (University of Manchester, UK) scholarly works. Contributions of the Research Assistant, Miss Priscilla Jorgensen, are highly appreciated.

Correspondence and requests for offprints should be sent to Najmedin Meshkati, Department of Civil/Environmental Engineering, Department of Industrial and Systems Engineering, Viterbi School of Engineering, University of Southern California, Los Angeles, CA 90089-2531, USA. E-mail: <meshkati@usc.edu>.

plants, nuclear power stations, and aircraft, is that they are under the centralized control of a few (control room or cockpit) operators. The effects of human error in these systems are often neither observable nor reversible; therefore, error recovery is often either too late or impossible. Complex technological systems' accidents, in the case of aircraft crashes, cause the loss of lives and property. In addition to these losses, in the case of chemical or nuclear plants, because of large amounts of potentially hazardous materials which are concentrated and processed at these sites, accidents pose serious threats with long-lasting health and environmental consequences for the workers, for the local public, and possibly for the neighboring region or country [5].

For the foreseeable future, despite increasing levels of computerization and automation, human operators will have to remain in charge of the day-to-day controlling and monitoring of these systems, since system designers cannot anticipate all possible scenarios of failure, and hence are not able to provide pre-planned safety measures for every contingency. According to Rasmussen [6], operators are kept in these systems because they are flexible, can learn and adapt to the peculiarities of the system, and because "they are expected to plug the holes in the designer's imagination" (p. 97). Thus, the safe and efficient operation of these technological systems is a function of the smooth and synchronized interaction among their human (i.e., people and organization) and engineered subsystems (e.g., automation in general and automated control devices such as "intelligent," expert or decision support systems in particular).

Many technological systems' failures implicated in serious accidents have traditionally been attributed to operators and their errors. Consequently, for the problem of technological systems safety, an engineering solution has been suggested [7]. For instance, many system designers postulate that "removing man from the loop" is the most convenient alternative for the reduction or even the elimination of human error and therefore, consider automation the key to the enhancement of system reliability. However, in many cases automation only aggravates the situation and becomes part of the problem rather than the solution. For example, in the context of aviation, automation is even more problematic because it "amplifies [crew] individual difference" [8], and "it amplifies what is good and it amplifies what is bad" [9]. Furthermore, the automated devices themselves still need to be operated and monitored by the very human whose caprice they were designed to avoid. Thus, the error is not eliminated, but only relocated. The automation system itself, as a technological entity, has a failure potential that could result in accidents. Once an automated system which requires human intervention fails, operators, because of being out-of-the-loop, are de-skilled in just those very activities which require their contributions.

The underlying rationale and the major objective of this article is to demonstrate the critical effects of human and organizational factors and to also highlight the role of their interactions with automation (and automated devices) in the safe operation of complex, large-scale technological systems. This is done in the following sections by (a) a brief analysis of well known accidents at such systems, (b) an overview of the most important problems and shortcomings of the present automated systems, and (c) a case study field work observations to demonstrate the critical role of human organizational factors in the safety of an advanced control room of an oil and gas pipeline system in the USA.

2. THE CRITICAL ROLE OF HUMAN AND ORGANIZATIONAL FACTORS IN THE SAFETY OF CONTROL ROOM-OPERATED PETROCHEMICAL AND NUCLEAR POWER PLANTS

According to foregoing NTSB studies, several human factor elements may have contributed to the lack of controller success in preventing or mitigating pipeline accidents/incidents. The summary list of elements provided by the NTSB indicated that elements exist in both the work environment and also in the computer system design/operation (such as data presentation and alarm configuration). Some work environment issue examples include shift hours, shift length, circadian rhythms, shift change-over processes, fatigue countermeasures, ergonomics factors, workplace distractions, and physical interaction with control system computers [1].

Most petrochemical and nuclear power plants around the world are operated by a group of human operators who use advanced computer-based devices from a centralized control room. A large number of accidents at these plants typically start with equipment malfunction, process upset or operator error; but they are aggravated and propagated through the system by a series of factors that could be attributed to human, organizational, and safety factors within the system. Also, most complex systems' accidents resemble an "unkind work environment"; that is, an environment in which once an error has been made, it is not possible for the person to correct the effects of inappropriate variations in performance before they lead to unacceptable consequences. This is because the effects of the errors are neither observable nor reversible [10]. As research has shown, in most cases, operator error is an attribute of the whole technological (plant) system—a link in a chain of concatenated failures—that could result in accidents. The most important lesson to be learned from past accidents is that the principal cause tends to be neither the isolated malfunctioning of a major component nor a single gross blunder, but the unanticipated and largely unforeseeable concatenation of several small failures, both engineered and human. Each failure alone could probably be tolerated by the system's defenses. What produces the disastrous outcome is their unnoticed and often mysterious complex interaction.

On many occasions, human error is caused by the inadequate responses of operators to unfamiliar events. These responses depend very much on the conditioning that takes place during normal work activities. The behavior of operators is conditioned by the conscious decisions made by work planners or managers. Therefore, the error and the resulting accidents are, to a large extent, both the attribute and the effect of a multitude of factors such as poor workstation and workplace designs, unbalanced workload, complicated operational processes, unsafe conditions, faulty maintenance, disproportionate attention to production, ineffective training, lack of motivation and experiential knowledge, non-responsive managerial systems, poor planning, non-adaptive organizational structures, rigid job-based pay systems, haphazard response systems, and sudden environmental disturbances, rather than being their cause [11]. Thus, attributing accidents to the action of front-line workers is an oversimplification of the problem.

According to Perrow [12], "the dangerous accidents lie in the system, not in the components" (p. 351), and the inherent system accident potential can increase in a poorly-designed and managed organization. The critical role of human and organizational factors in the safety of petrochemical plants has been highlighted in a survey by Meshkati [13]. The United States Environmental Protection Agency (EPA) has conducted a review of emergency systems for monitoring, detecting, and preventing releases of hazardous substances at representative domestic facilities that produce, use, or store these substances [14]. Among the findings in the EPA's final report was that the "prevention of accidental releases requires a holistic approach that integrates technologies, procedures, and management practices" (p. 3). Moreover, the report stated: "The commitment of management to accident prevention, mitigation, and preparedness is essential. Without such commitment, installation of the most advanced technologies will be an expensive, but ineffectual safeguard for preventing serious injury, death, or environmental damage....While accidents can occur in well-managed facilities, the lack of management commitment can lead to disaster.... The ultimate responsibility for safe design, operation, and maintenance of a facility rests with management" (p. 3).

The important role of human and organizational factors in the safety of nuclear power plants has been investigated in studies by Gertman, Haney, Jenkins, et al. [15]; Orvis, Moieni, and Joksimovich [16]; and Harber, O'Brien, Metaly, et al. [17]. These issues were also addressed and explored in the works of Gertman and Blackman [18]; Marcus and Nichols [19]; Wells and Ryan

[20]; Wu, Apostolakis, and Okrent [21]; and Mosleh, Grossman, and Modarres [22]. The critical role of human and organizational causes in the Chernobyl accident is encapsulated in the following statement which has appeared in the conclusion section of the International Atomic Energy Agency's (IAEA) report: "The root cause of the Chernobyl accident, it is concluded, is to be found in the so-called human element....The lessons drawn from the Chernobyl accident are valuable for all reactor types" (p. 6) [23].

Moreover, Valeriy A. Legasov (deceased), a former Soviet Academician, the First Deputy Director of the Kurchatov Institute in Moscow at the time of the Chernobyl accident, and the head of the Soviet delegation to the Post-Accident Review Meeting of the IAEA in August, 1986, "declared with great conviction": "I advocate the respect for human engineering and sound man–machine interaction. This is a lesson that Chernobyl taught us" (as cited in Munipov [24], p. 10).

These facts and other investigations led the IAEA to declare that "the Chernobyl accident illustrated the critical contribution of the human factor in nuclear safety" (p. 43) [25].

Finally, according to the IAEA, "the [Chernobyl] accident can be said to have flowed from deficient safety culture, not only at the Chernobyl plant, but throughout the Soviet design, operating and regulatory organizations for nuclear power that existed at the time....Safety culture...requires total dedication, which at nuclear power plants is primarily generated by the attitudes of managers of organizations involved in their development and operation" (p. 24) [26]. In a report by the International Nuclear Safety Advisory Group of the IAEA, safety culture is defined as "that assembly of characteristics and attitudes in organizations and individuals which establishes that, as an overriding priority, nuclear plant safety issues receive the attention warranted by their significance" (p. 4) [27].

According to the author's analyses of large-scale technological systems' accidents, there were two main categories of human and organizational factors causes: lack of human and organizational factors considerations at the system's (a) design stage; and (b) operating stage [5]. Notwithstanding the overlapping domains and intertwined nature of these two stages, the former, using Reason's [28] characterization, refers primarily to "latent errors"—adverse consequences that may lie dormant within the system for a long time, only becoming evident when they combine with other factors to breach the system's defenses. In the context of this article, they include the control room, workstation, and display/control panel design flaws causing confusion and leading to design-induced errors; problems associated with lack of foresight in operators' workload estimation leading to overload (and stress); inadequate training; and organizational rigidity and disarrayed managerial practices. The final factor, which is associated with the performance of the front-line operators immediately before and during the accident, includes sources and variations of "active errors" such as misjudgments, mistakes, and wrong-doings. In order to prevent accidents in chemical and nuclear plants, an integrated systemic approach should be taken to the design and operation as attentive to both technical elements and human and organizational factors [5, 29]. This approach should be based on a thorough and integrated analysis of plants' processes, workstations, procedures, management, and supervisory systems.

3. THE PROBLEMS OF AUTOMATION IN CONTROL OF COMPLEX SYSTEMS

Most complex, large-scale, technological systems have been both "tightly coupled" and "complexly interactive" [12]. The characteristics of a tightly coupled system include processing delays that are unacceptable; production sequences that are relatively invariant; relatively few ways of achieving a particular goal; little slack permissible in supplies, equipment, and personnel; and buffers and redundancies deliberately designed into the system. Interactive complexity can be described by one or a combination of features such as the close proximity of components that are not linked together in a production sequence; the presence of many common-mode connections (i.e., many components whose failure can have multiple effects "down-stream"); the fact that there is only a limited possibility of isolating failed components; that, due to the high degree of specialization, there is little chance of substituting or reassigning personnel (the same lack of interchangeability could also be true for material and supplies); unfamiliar or unintended feedback loops; the many control parameters that could potentially interact; the fact that certain information about the state of the systems must be obtained directly, or inferred; and the characteristic that there is only a limited understanding of some processes, particularly those involving transformations. Tight coupling requires centralization to ensure immediate response to failures by those who are in charge and in a position to understand the problem and determine the correct course of action. Interactive complexity, on the other hand, mandates decentralization to handle the unexpected interaction of different functions, decisions, and errors.

As the task uncertainty increases, which is the case in the "non-normal" or emergency situations at complex technological systems, the number of exceptions also increases until the organizational hierarchy is overloaded, at which time the organization must use another mechanism to reconfigure itself. Furthermore, the "normal function" of tightly coupled technological systems is to operate on the boundary to loss of control. That is, people are involved in a dynamic and continuous interaction with the failure and hazard [30]. Thus, "touching the boundary to loss of control is necessary (e.g., for dynamic 'speed–accuracy' trade-offs)" (p. 150) [31]. This is a rapidly changing environment, and in order to survive it, the system should be able to respond in a safe and effective manner. Occasionally, it may require an improvised response from the operator(s), but it should certainly be coordinated and in concert with others' activities and stay within the boundaries or "space" of acceptable work performance [30]. Otherwise, it would be just "noise" in the control of the system and could lead to errors.

It is the nature of complex, tightly coupled, and complexly interactive systems, according to Reason [32], to spring "nasty surprises." As case studies repeatedly show, accidents may begin in a conventional way, but they rarely proceed along predictable lines. Each accident is a truly novel event in which past experience counts for little, and where the plant is returned to a safe state by a mixture of good luck and hard, knowledge-based effort. Accident initiation and its propagation through possible pathways and branches within the system is a highly complex and hard to foresee event. It is analogous to the progression of a crack in an icy surface, which can move in several directions, hit different levels of thickness, and if not stopped, can cause the surface to break up and open ("uncover the core" and break the system).

The interactions between automation and system complexity as well as the role of human factors in such environment have been succinctly addressed by Karwowski [33]. As he noted, automation may often lead to an increase in the experience of difficulty and frustration when interacting with the added functionality provided by automation. Such incremental complexity cannot be avoided when functions are added, and according to Karwowski, "can only be minimized with good design that follows natural mapping between the systems elements (e.g., the control-display compatibility)" [34] (p. 582). In other words, "as system complexity increases, the incompatibility between the system elements, as expressed through their ergonomic interactions at all system levels, also increases, leading to greater ergonomic (non-reducible) entropy of the system and decreasing the potential for effective ergonomic intervention" (p. 456) [33].

Operators' control of complex, large-scale technological systems can be termed *coordination by pre-planned routines* [35]. However, coordination by pre-planned routines is inherently "brittle." Because of both pragmatic and theoretical constraints, it is difficult to build mechanisms into pre-planned routines that cope with novel situations, adapt to special conditions, or recover from human errors in following the plan. When pre-planned routines are rotely invoked and followed, performance breaks down in the light of under-specified instructions, special conditions or contexts, violations of boundary conditions, human execution errors, bugs in the plan, multiple failures, and novel situations (incidents not planned for) [35]. This is the problem of unanticipated variability which happens frequently during emergencies at complex technological systems. Moreover, in virtually every significant disaster, or near-disaster, in complex systems, there have been some points where expertise beyond the pre-planned routines was needed. This point involves multiple people and a dynamic, flexible, and problem-solving organization. Handling unfamiliar events (e.g., emergencies) also requires constant modification of the design of the organization, coordination, and redeployment of resources [36]. However, as it has been observed and reported many times, usually the pre-programmed routines of decision support in expert computing systems sets the organization in a static design [37].

Furthermore, it has been empirically validated that experts in high stress demanding situations do not usually operate using a process of analysis. Even their rules of thumb are not readily subjected to it; whereas most of the existing artificial intelligence-based automated systems always rely on analytical decision process. If operators of complex systems relied solely on computers' analytic advice, they would never rise above the level of mere competence—the level of analytical capacity—and their effectiveness would be limited by the inability of the computer systems to make the transition from analysis to pattern recognition and other more intuitive efforts [38].

The issue of operators trusting automated systems is another major factor limiting the application and effectiveness of these systems. Trust between humans and machines is a very complex issue which, among others, is a function of the machine's behavior and the stability of its environment [39, 40].

In summary, in employing automation for the control of complex technological systems, system designers and managers should always remember that one can—and should—not replace the other: "Men and machines are not comparable, they are complementary....Men are good at doing what machines are not good at doing and machines are good at doing that at which men are not good at doing" (p. 203) [41].

4. OBSERVING SAFETY AND HUMAN PERFORMANCE ISSUES IN AN OIL AND GAS PIPELINE SYSTEM'S CONTROL ROOM

According to a study of 500 incidents involving pipework failure and subsequent chemical release (in the United Kingdom, the USA, the Netherlands, and Finland) for the UK's Health and Safety Executive, "responsible in 30.9% of the incidents, operator error was the largest contributor to pipework failures among known direct causes" (p. 68) [4]. This study has concluded and recommended "human factors reviews of maintenance and operations personnel and functions" (p. 69) as one of the four critical areas where management of oil, gas, and chemical companies should concentrate their efforts.

4.1. General Observations and Findings

The following is a summary of relevant and pertinent human, organizational and safety factors affecting operators' performance while using advanced automated systems in a pipeline control room. From this control room, a sophisticated network of oil and gas pipeline systems in the Western USA is controlled.

4.1.1. Human factors considerations

Workstation and interface (displays)

Alarms are incoming signals from different active and inactive pipeline systems which operators need to acknowledge.

- Alarms were not prioritized.
- In responding to different alarms for a pipeline system, the operator had to spend significant amounts of time in identifying the alarm.
- All manual valves were usually not presented on the display, whereas remotely controlled valves were all presented. A manual valve was only displayed when it connected two lines.

Workload and its sources

Normal conditions and the nature of the workload

The major contributing (task) loading factors or categories of the operators' (mental) workload during normal or routine times, included the following.

- Information processing—e.g., performing a number of concurrent tasks, valve alignments, responding to alarms, and other mental tasks.
- Communication—e.g., on a routine basis talking with field workers, maintenance, and other operators; answering phone calls.
- Data recording—e.g., filling out paperwork and incident logs.
- A workload which, of course, was proportional to the number of pipeline systems that were controlled by the operator. In this control room, 7–9 pipelines, on the average, were simultaneously controlled by a single operator. The workload could have intensified because of time pressure, time of the day, and activities in the field (such as maintenance) that affected the control room operators.

Abnormal conditions, workload, and leak detection

Workload substantially increased as a result of system upset, such as a leak or equipment malfunction (valve or pump breakdown).

Leak detection required a good understanding of the physical characteristics of the product, the "profile" of the pipeline system and its hydraulic characteristics (pressure and flow), the terrain, and environmental conditions (temperature).

A leak, therefore, was an unannunciated event in the control room and leak detection was a diagnostic effort.

During an emergency, the pipeline system control room was the focal point of communication with state and local agencies.

- Leak detection was typically done through periodic checks of (the trend of) temperature, pressure, flow rate, meter accumulator, or tank gauge.
- During the leak detection and handling, the operator needed to continue performing other control functions.

4.1.2. Safety-related considerations

Reported causes of errors and performance obstacles

There were two basic types of errors: pipeline valve alignment and paperwork-related.

Misalignment errors were primarily caused by lack of concentration (interruption, distraction, and omission caused by heavy workload), failure to check the pipeline map thoroughly for all valves, and discrepancy between map and computer data.

Other sources of errors were lack of familiarity with the particular pipeline system, not asking for help from other operators, and relying on the information given only by one source, either the sending or receiving party.

Other errors were caused by not keeping track of the required entries for the paperwork and not balancing the product movement.

- There were non-essential interruptions resulting from calls to the pipeline system control room.
- There were discrepancies between the valves' positions on the pipeline blueprint (map) version and its computer version.
- When all valves on a pipeline were remotely controlled valves, it took a fraction of an hour to align the system; for pipelines with manual valves, it took up to 10 times that long.

4.1.3. Organizational-related factors

Performance obstacles

- Operators perceived a lack of sufficient support and appreciation from within the company; affecting morale and motivation.
- Operators perceived very limited opportunities for advancement and promotion.
- Operators perceived a disproportionate amount of input from other units within the company in their performance review.

4.2. Analysis

A primary goal of this case study was to identify error-inducing conditions as well as human and organizational causes of errors, while using automated systems at the pipeline control room. This section attempts to further elaborate these issues by addressing the potential for human–task mismatch, because errors are caused by human–machine or human–task mismatches. Operators' errors should be seen as the result of human variability, which is an integral element in human learning and adaptation [42]. This approach considers the human–task or human–machine mismatches as a basis for analysis and classification of human errors, instead of solely tasks or machines [43]. These mismatches could also stem from inappropriate work conditions, lack of familiarity, or improper (human–machine) interface design. The use of off-the-shelf general training, increased number of procedures, and stricter administrative controls is less effective than utilizing real counter-measures against these modes of mismatches or misfits. Thus, human error occurrences are defined by the behavior of the total human–task system. Frequently, the human–system mismatch will not be due to spontaneous, inherent human variability, but to events in the environment which act as precursors.

Nature and categories of errors in the pipeline system control room

An important category of errors within the context of the pipeline system control room, wherein the operators typically engage in monitoring and supervising the system and have to respond to changes in system operation with corrective actions, is called *systematic errors*. In this context, two types of systematic errors are important and should be considered [28].

- Research has shown that operators' responses to changes in a technological system will be systematically wrong if the task demands exceed the limits of capability. In the case of pipeline system operator, job demands and capability may conflict due to several aspects of a task, such as the time required and the availability of needed information and background knowledge on system functioning.

The mental workload of operators working in the pipeline system control room was highly variable and could have reached extremely high levels. This is synonymous with having or lacking balance between task demands and an operator's capabilities. According to Tikhomirov [44], high or unbalanced mental workload causes

- a narrowing span of attention,
- inadequate distribution and switching of attention,
- forgetting the proper sequence of actions,
- an incorrect evaluation of solutions,
- slowness in arriving at decisions.

In addition to occasional unbalanced workloads, human factors related-problems with the computer workstation, such as a mismatch between computer and map data on valves or lack of alarm prioritization, could cause a good portion of errors in the pipeline system control room. These types of errors, the so-called design-induced or system-induced errors, are forced upon operators.

- Systematic operator error may be caused by several kinds of "procedural traps" [45]. During normal working conditions, human operators are generally extremely efficient because of effective adaptation to convenient, representative signs, and signals that they receive from the system. This is a very effective and mentally economical strategy during normal and familiar periods, but leads the operator into traps when changes in system conditions are not adequately reflected in his/her system of signs. Such mental traps often significantly contribute to the operator's misidentification of unfamiliar and complex system states. This misidentification, in turn, is usually caused by the activation of "strong-but-wrong" rules, where the "strength" is determined by the relative frequency of successful execution. When abnormal conditions demand counter-measures from the operator, a shift in the mental work strategies is needed by the operators. However, it is very likely that familiar associations based on representative, but insufficient, information will prevent the operator from realizing the need to analyze a complex and/or unique situation. He/she may more readily accept the improbable coincidence of several familiar faults in the system, rather than the need to investigate one new and complex "fault of low probability." In this case, the efficiency of the human operator's internal mental model allows him/her to be selective and, therefore, to cope effectively with complex systems in familiar situations, which at the same time may lead him/her into traps that are easily seen after the fact.

Errors during normal conditions

Usually, those errors which occur during normal conditions at the pipeline system control room, such as failing to open a valve when preparing a pipeline, are slips or lapses, rather than mistakes. Slips and lapses are associated with failures at the more subordinate levels of action selection, execution, and intention storage, whereas mistakes occur at the level of intention, formation and planning [28].

According to research findings, a necessary condition for the occurrence of a slip or lapse is the presence of "attention capture" associated with either distraction or preoccupation. Another type of slip that happens at the pipeline system control room could stem from what is called "inappropriately timed check." Like omitted checks, inappropriate monitoring is associated with attention capture. Mis-timed monitoring is most likely to occur immediately following a period of "absence" from the task in mind, caused by interruptions [28].

In addition to the general factors that promote absent-minded slips and lapses (the execution of routine tasks while preoccupied or distracted), the following are a number of task factors in the pipeline system control room that are likely to increase the probability of making an omission error. Even the most experienced operators can not escape the negative effects of these factors (based on Reason's [28] framework):

- The larger the number of discrete steps in a sequence of actions (e.g., having many valves on the pipeline), the greater the probability that one or more of them will be omitted.
- The greater the informational loading of a particular procedural step (e.g., preparing a pipeline with many complicated pipeline valve stations having several manual valves), the more likely it is that items within that step will be omitted.
- Procedural steps that are not obviously cued by preceding actions or those that do not follow in a direct linear sequence from them are likely to be omitted.
- When instructions are given verbally and there are more than five simple steps, items in the middle of the list of instructions are more likely to be omitted than those either at the beginning or the end.
- When instructions are given in a written form, isolated steps at the end of the sequence (e.g., replacing caps or brushes after maintenance, removing tools) have a reasonably high probability of being omitted.
- In a well-practiced, highly automated task, unexpected interruptions (e.g., during valve alignment task, receiving alarm and phone calls) are frequently associated with omission errors, either because some unrelated action is unconsciously "counted in" as part of the task sequence, or because the interruption causes the individual to "lose his/her place" on resumption of the task (i.e., he/she believes that he/she was further along in the task prior to the interruption than he/she actually was). Such routine tasks are also especially prone to premature exits—moving on to the next activity before the previous one is completed, thus omitting some necessary final steps (e.g., without opening a valve, moving to the next one on the pipeline). This is particularly likely to happen when the individual is working under time pressure or when the next job is near at hand (e.g., preparing a pipeline and having to fill out the corresponding paperwork).

Errors during abnormal conditions

The aforementioned systematic errors are significant contributors to technological systems' failures. According to research findings, the failure of human operators to identify abnormal states of a system, because of the foregoing systematic errors, plays an important role in accidents and incidents in complex technological systems. Even if the state of the system is correctly identified, the operator may still be caught in a procedural trap [45]. It has been argued that a familiar, stereotyped sequence of actions may be initiated from a single conscious decision or association from the system state. If the corresponding procedure takes some time, e.g., it is necessary to move to another place to perform it, the mind may return to other matters, making the workings of the subconscious vulnerable to interference, particularly if part of the sequence is identical to other heavily automated sequences. Systematic human errors in unfamiliar tasks are typically caused by interference from other more stereotyped situations and, therefore, the potential for systematic errors depends very much upon the level of the operator's skill. "The fact that operators can control the system successfully during a commissioning and a test period is not proof that operators will continue to do so during the system life cycle" (p. 364) [45].

A basic problem when dealing with systematic erroneous responses to unfamiliar situations is the low probability of such complex situations. In a properly designed system, there should be a reverse relation between the probability of occurrence of an abnormal situation and its potential effects in terms of losses and damage. In modern centralized control rooms, the consequence of faults can be very serious and, as a result, the effects of human error in situations of extremely low probability must be considered. In such cases, as in the pipeline system control room, the potential for systematic errors cannot be identified from experience. The skills developed and gained during normal operations are not a satisfactory basis for infrequently needed improvisation to handle unfamiliar events [6]. Instead, the operator's task and work organization should be restructured to ensure that he/she has the necessary knowledge available when abnormal situations demand an understanding of the system's physical functioning. Only through a systematic functional analysis of realistic scenarios and their decomposition to the sub-task level, can the error-inducing conditions be exposed.

Furthermore, we cannot rely solely on the operators' experience level to avoid accidents. In fact, "in accident avoidance, experience is a mixed blessing" (p. 86) [28]. Operators learn their avoidance skills not so much from real accidents as from near-misses. It has even been said, "if near-accidents usually involve an initial error followed by an error recovery, more may be learned about the techniques of successful error recovery than about how the original error might have been avoided" (p. 86) [28].

The aforementioned types of problems cannot be effectively counteracted by administrative measures or by better training. In complex systems, such as the control room of the oil and gas pipeline system, we also have to consider rare events for which operators cannot be prepared by training on the use of procedures. In such cases, operators have to generate proper procedures on-line by functional evaluation and causal reasoning, based on knowledge about system properties. This suggests that it is necessary that more than one operator be involved in problem-solving during rare events, and the whole crew of the pipeline system control room should be able to work as a team. Studies on *team mind* consider the team as "an emergent entity;" postulating that the "team acts as does a person" and contend that a smoothly functioning team mind is "anticipating the needs of others, synchronizing actions, and feeling free to improvise" (p. 3, 6) [46].

4.3. Conclusions and Recommendations

Based on the analysis, recommendations for considering human, organizational, and safety factors in pipeline system control room were made. There were two sets of such recommendations, one each for both short- and long-term considerations.

4.3.1. Short-term human, organizational and safety considerations

In the short term, it was concluded that human factors and safety considerations should include simplifying tasks, and improving the physical control center and interface-related factors. It was recommended that attempts should be made to do the following.

- Minimize interruptions.
- Prioritize incoming alarms, queue, and batch process the low-priority ones.
- Balance the workload.
- Redesign and simplify paperwork and revise procedures for filling it out.
- Upgrade computer databases of pipeline parts, components, valves, and routes and make them consistent with maps.
- Develop a system for on-line updating of the preparation of the pipeline system and progress of maintenance activities.
- Make sure all pipeline system control room equipment and systems (computer and communications) work properly.
- Develop and provide operators with decision aids and memory aids. Decision aids are designed to minimize failures when a human operator formulates his/her action or plan, while memory aids support the performance during plan storage and execution [28].
- Develop a paper or electronic checklist for every pipeline system. These checklists should cover all steps needed for the alignment of all manual and remotely controlled valves on any pipeline system.

In the short term, it is suggested that the organizational-related factors should include and should attempt to do the following.

- Educate employees working for other areas in the company about the pipeline system control room and the full range of operators' jobs and responsibilities.
- Set performance goals with input from the operators.
- Review the career opportunities and promotion possibilities of operators within the company. Openly communicate this information to the existing and future crew members of the control room.
- Clearly identify career aspirations (career concepts) of each operator.
- Integrate and synchronize the personnel requirements of the support staff and other supporting departments with the control room.
- Develop a context-specific and skill-based performance review system for the pipeline system control room. The corresponding form should not be generic or job-based. Factors such as skill versatility, analytical abilities, and information integration and differentiation abilities should be included as they are important contributors to keeping the system in a normal operating mode and bringing it back from an upset mode in the case of a failure. This form should address all the performance-related factors of the control room crew as specifically as possible.
- Develop a team or collective performance evaluation plan and an accompanying mechanism, in addition to any individual performance review, to encourage, recognize, and reward the much needed teamwork.

It is noteworthy that one of the most important considerations, with far-reaching effects for human, organizational, and safety areas, is the inclusion of the operators in the decision-making process. The operators' input may point out areas with a high potential for error within the system that might otherwise be overlooked.

4.3.2. Long-term human, organizational, and safety considerations

It was recommended that the long-term human factors considerations should include the incorporation of several human factors issues in the design of software and (new) display systems for the control room.

Moray et al.'s [47] findings have important implications for the new generation of control room, computer-generated, animated, and direct perception displays. According to this study, "recall and diagnosis should be better for an integrated display than for a traditional single-sensor-single-indicator display (SSSI)....Even experts can only exercise their skills and expertise optimally if the pattern in which information is displayed matches their models of the dynamics of the problem….The advantage of direct perception interfaces should be particularly strong when the operators have advanced levels of expertise." Computer-generated "displays should not merely transfer *data* to the observer: they should transfer *goal-relevant information*, which will most easily arouse the operator's expertise in the relevant task domain. To evaluate interfaces requires us to evaluate the extent to which they perform this task." These findings were further corroborated by Meshkati, Buller, and Azadeh [48], where uses of the ecological interface resulted in significantly more accurate event diagnosis and recall of various plant parameters, faster response to plant transients, and higher ratings of operators' preference.

As mentioned before, errors are caused by human–machine or human–task mismatches. These mismatches could stem from inappropriate working conditions, lack of familiarity with the system, or improper (human–machine) interface design. To reiterate, using general training, a large number of procedures, and stricter administrative controls is less effective than utilizing real counter-measures against these modes of mismatches or misfits. Whatever the cause of the specific individual error—a change in working conditions, a spontaneous slip of memory, high workload, distraction, etc.—the resulting margin of mismatch between situation and the human can be decreased by providing the operator with better access to information about the underlying causal net so as to improve improvisation and recall. In particular, the margin can be decreased by making the effect of the operator's activity directly observable. Interface design should aim at making the boundaries of acceptable performance visible to the users while their effects are still observable and reversible. This can be done by designing readily visible feedback to support functional understanding of the system. It was recommended that to assist operators in coping with unforeseen situations, the designer should provide them with tools to make experiments and test hypotheses without having to do these things directly upon potentially irreversible pipeline systems.

Another prudent and innovative approach for human factors analysis in this context could take advantage of the powerful Activity Theory concept which addresses the interdependencies and mutual influence of internal mental and external motor activity [49]. Moreover, as suggested by Rasmussen [30], causal reasoning in a complex functional network, such as a pipeline with many pipeline valve stations, places excessive demands upon limited working memory resources. Information should be embedded in a structure that can serve as an externalized mental model. It was recommended that this representation (for the operators) should not only aim at identifying a specific problem solution, but should also aim at indicating an effective strategy (i.e., a category of possible solutions).

The inclusion of organizational and safety factors into the design and operation of a pipeline system control room results in better operator–task and operator–workstation matches. Thus, it will certainly contribute to a reduction of human error potential and enhancement of the total system's reliability.

REFERENCES

1. Department of Transportation. Pipeline and Hazardous Materials Safety Administration. Pipeline safety: Controller Certification Pilot Program (CCERT) (Docket No. RSPA-04-18584; Notice 1) [Federal Register, April 2005]. Retrieved February 21, 2006, from: http://ops.dot.gov/new/New_2005/Controller%20Cert%20-%20April%202005.pdf
2. National Transportation Safety Board (NTSB) (2005). Pipeline Accidents, http://www.ntsb.gov/Publictn/P_Acc.htm
3. Pipeline Safety Improvement Act of 2002 (PSIA), signed into law on December 17, 2002, H.R. 3609.
4. Geyer TA, Bellamy LJ, Astley JA, Hurst NW. Prevent pipe failures due to human error. Chemical Engineering Progress. 1990;November:66–9.
5. Meshkati N. Human factors in large-scale technological systems' accidents: Three Mile Island, Bhopal, Chernobyl. Industrial Crisis Quarterly. 1991;5:133–154.
6. Rasmussen J. What can be learned from human error reports? In: Duncan KD, Gruneberg MM, Wallis D, editors. Changes

in working life. New York, NY, USA: Wiley; 1980. p. 97–113.

7. Perrow C. Complex organizations: a critical essay. 3rd ed. New York, NY, USA: Random House; 1986.
8. Graeber RC. Integrating human factors knowledge into automated flight deck design [unpublished invited presentation at the International Civil Aviation Organization (ICAO) Flight Safety and Human Factors Seminar, Amsterdam, The Netherlands, May 18, 1994].
9. Wiener E. Integrating practices and procedures into organizational policies and philosophies [unpublished invited presentation at the International Civil Aviation Organization (ICAO) Flight Safety and Human Factors Seminar, Amsterdam, The Netherlands, May 18, 1994].
10. Rasmussen J. Information processing and human–machine interaction: an approach to cognitive engineering. New York, NY, USA: North-Holland; 1986.
11. Meshkati N. An integrative model for designing reliable technological organizations: The role of cultural variables [unpublished invited position paper for the World Bank Workshop on Safety Control and Risk Management in Large-Scale Technological Operations, World Bank, Washington, DC, USA, October 18–20, 1988].
12. Perrow C. Normal accidents. New York, NY, USA: Basic Books; 1984.
13. Meshkati N. Critical human and organizational factors considerations in design and operation of petrochemical plants (Paper No. SPE 23275). In: Proceedings of the First International Conference on Health, Safety & Environment in Oil and Gas Exploration and Production, 11–14 November 1991. The Hague, The Netherlands: Society of Petroleum Engineers (SPE); 1991. vol. I, p. 627–34.
14. Environmental Protection Agency (EPA). Review of emergency systems (Report to Congress). Washington, DC, USA: EPA, Office of Solid Waste and Emergency Response; 1988.
15. Gertman DI, Haney LN, Jenkins JP, Blackman, HS. Operational decision making and action selection under psychological stress in nuclear power plants (NUREG/CR-4040). Washington, DC, USA: U.S. Nuclear Regulatory Commission (NRC); 1985.
16. Orvis DD, Moieni P, Joksimovich V. Organizational and management influences on safety of nuclear power plants: use of PRA techniques in quantitative and qualitative assessment (NUREG/CR-5752). Washington, DC, USA: U.S. Nuclear Regulatory Commission (NRC); 1993.
17. Haber SB, O'Brien JN, Metlay DS, Crouch DA. Influence of organizational factors on performance reliability (NUREG/CR-5538). Washington, DC, USA: U.S. Nuclear Regulatory Commission (NRC); 1991.
18. Gertman DI, Blackman HS. Human reliability and safety analysis data handbook. New York, NY, USA: Wiley; 1994.
19. Marcus AA, Nichols ML. Assessing organizational safety in adapting, learning systems: empirical studies of nuclear power. In: Apostolakis G, editor. Probabilistic safety assessment and management. New York, NY, USA: Elsevier; 1991. p 165–70.
20. Wells JE, Ryan TG. Integrating human factors expertise into the PRA process. In: Apostolakis G, editor. Probabilistic safety assessment and management. New York, NY, USA: Elsevier; 1991. p. 577–82.
21. Wu JS, Apostolakis G, Okren, D. On the inclusion of organization and management factors into probabilistic safety assessments of nuclear power plants. In: Apostolakis G, editor. Probabilistic safety assessment and management. New York, NY, USA: Elsevier; 1991. p. 619–24.
22. Mosleh A, Grossman N, Modarres M. A method for evaluation and integration of safety performance indicators. In: Apostolakis G, editor. Probabilistic safety assessment and management. New York, NY, USA: Elsevier; 1991. p. 43–8.
23. International Atomic Energy Agency (IAEA). Summary report on the post-accident review meeting on the Chernobyl accident (Safety Series No. 75-INSAG-1). Vienna, Austria: IAEA; 1986.
24. Monipov VM. Chernobyl operators: criminals or victims? Appl Ergon. 1992; 23(5):337–42.

25. International Atomic Energy Agency (IAEA). Nuclear safety report for 1987. Vienna, Austria: IAEA; 1987.

26. International Atomic Energy Agency (IAEA). The Chernobyl accident: updating of INSAG-1 (Safety Series No. 75-INSAG-7). Vienna, Austria: IAEA; 1992.

27. International Atomic Energy Agency (IAEA). Safety culture: A report by the International Nuclear Safety Advisory Group (Safety Series No. 75-INSAG-4), Vienna: IAEA. Vienna, Austria: IAEA; 1991.

28. Reason J. Human error. New York, NY, USA: Cambridge University Press: 1992.

29. Meshkati N. Preventing accidents at oil and chemical plants. Prof Saf. 1990;35(11): 15–8.

30. Rasmussen J. Human error and the problem of causality in analysis of accidents [unpublished invited paper for Royal Society meeting on Human Factors in High Risk Situations, 28–29 June, 1989, London, UK].

31. Rasmussen J, Pejtersen AM, Goodstein LP. Cognitive systems engineering. New York, NY, USA: Wiley; 1994.

32. Reason J. Cognitive aids in process environments: prostheses or tools? Int J Man Mach Stud. 1987;27:463–70.

33. Karwowski W. Ergonomics and human factors: The paradigms for science, engineering, design, technology and management of human compatible systems. Ergonomics. 2005;48(5):436–63.

34. Karwowski W. Cognitive ergonomics: requisite compatibility, fuzziness, and nonlinear dynamics. In: Proceedings of the IEA 2000/HFES 2000 Congress. July 29–August 4, 2000, San Diego, California USA. Santa Monica, CA, USA: Human Factors and Ergonomic Society; 2000. vol. 1, p. 580–3.

35. Woods DD. Commentary: cognitive engineering in complex and dynamic world. Int J Man Mach Stud. 1987; 27:571–85.

36. Meshkati N. Integration of workstation, job, and team structure design in complex human–machine systems: A framework. Int J Ind Ergon. 1991;7:111–22.

37. Sloane SB. The use of artificial intelligence by the United States Navy: case study of a failure. AI Magazine. 1991;Spring:80–92.

38. Dreyfus HL, Dreyfus SE. Mind over machine. New York, NY, USA: The Free Press; 1986.

39. Muir BM. Trust between humans and machines, and the design of decision aids. In: Hollnagel E, Mancini G, Woods DD, editors. Cognitive engineering in complex dynamic worlds. New York, NY, USA: Academic Press; 1988. p. 71–83.

40. Sheridan TB. Computer control and human alienation. Technol Rev. 1980;October: 61–73.

41. Jordan N. Themes in speculative psychology. London, UK: Tavistock; 1968.

42. Rasmussen J. Trends in human reliability analysis. Ergonomics. 1985;28(8):1185–95.

43. Rasmussen J, Duncan K, Leplat J, editors. New technology and human error. New York, NY, USA: Wiley; 1987.

44. Tikhomirov OK. The psychology of thinking (Translated from the Russian by Natalia Belskaya). Moscow, USSR: Progress Publishers; 1969.

45. Rasmussen J. Notes on human error analysis.: In Apostolakis G, Garribba S, Volta G, editors. Synthesis and analysis methods for safety and reliability studies. New York, NY, USA: Plenum; 1980. p. 357–89.

46. Thordsen ML, Klein GA. (1989). Cognitive processes of the team mind. In: Proceedings of the IEEE Conference on Systems, Man and Cybernetics. New York, NY, USA: IEEE; 1989. p. 46–9.

47. Moray N, Jones BJ, Rasmussen J, Lee JD, Vicente KJ, Brock R, et al. A performance indicator of the effectiveness of human–machine interfaces for nuclear power plants (NUREG/CR-5977). Urbana, IL, USA: University of Illinois, Urbana-Champaign, Department of Mechanical and Industrial Engineering; 1993.

48. Meshkati N, Buller BJ, Azadeh MA. Integration of workstation, job, and team structure design in the control rooms of nuclear power plants: experimental and simulation studies of operators' decision

styles and crew composition while using ecological and traditional user interfaces (Grant report prepared for the U.S. Nuclear Regulatory Commission; grant NRC-04-91-102). Los Angeles, CA, USA: University of Southern California; 1994. vol. I.

49. Bedny GZ, Karwowski W. Activity theory as a basis for the study of work. Ergonomics. 2004;47(2):134–53.