

# Managing Modern Sociotechnical Systems: New Perspectives on Human-Organization—Technological Integration in Complex and Dynamic Environments

Haftay H. Abraha and Jayantha P. Liyanage

**Abstract** Modern sociotechnical systems (SSs) are becoming increasingly advanced, complex, boundary-less, and technology-dominant systems that have major economic, societal and environmental implications. Digital technologies are enabling us to develop systems with various levels of complexities and interconnections involving different elements. This creates new ways of organizing work, new work processes, for instance: creating closer cooperation across organizational and geographical borders and this trend is likely to increase. Complexities are associated not only with the large scale hardware and software infrastructures, but also with the even more complex issues involved in human and organizational behaviours and characteristics. This implies that there are many hidden risks under the modern systems development and deployment process, and subsequently the potential for serious events are considerable. A major area for study in this context is the establishment of a seamless connection between the characteristics of the individual components (at micro-level) and the macro-behaviour of the complex SSs. Given the complexity of the systems involved, use of classical/traditional approaches (e.g. linear relations of causality) alone to understand the behaviour and performance of these systems are quite challenging, if not extremely limited in use. We need new perspectives to understand the behaviours and interactions in wider context, so that the new perspectives can capture the complex issues that influence Human-Organization-Technological (HOT) conditions within such systems, can emerge. This paper elaborates on an approach that can provide the basis for micro-macro integration to reduce vulnerabilities based on a better awareness (i.e. system thinking) taking into account the dynamic and complex context from a new perspective.

**Keywords** Complex systems · Human error · Human-Organization-Technology · Unwanted events · Risk · Safety incidents · Sociotechnical system

---

H.H. Abraha (✉) · J.P. Liyanage  
University of Stavanger, Stavanger 4036, Norway  
e-mail: haftay.h.abraha@uis.no

## 1 Introduction

The stability, performance, and the survival of sociotechnical systems (SSs), as well as their ability to tolerate environmental disturbances, are dependent upon the nature, formation and interaction of the human, organizational, and technological subsystems. Modern SSs are becoming increasingly advanced, complex, boundary-less, and technology-dominant systems that have major economic, societal and environmental implications. Digital technologies are enabling us to develop systems with various levels of complexities and interconnections involving different elements. Complexities are associated not only with the large scale hardware and software infrastructures, but also with the even more complex issues involved in human [1] and organizational behaviours and characteristics. Hence there is a need to explore new ways of thinking to manage modern sociotechnical systems in faces of those new scenarios: system thinking as a complement to the traditional risk and safety analysis.

Given the complexity of the systems involved, use of classical/traditional approaches alone to understand the behaviour and performance of these systems are quite challenging, if not extremely limited in use [2]. Major accidents keep occurring that seem preventable and that have similar systemic causes. The following paragraph, for instance, is quoted from the Deepwater Horizon disaster investigation [3] to show the closely replication of many different disasters.

In many ways, this disaster (Macondo well blowout (2010)) closely replicates other major disasters that have been experienced by the offshore oil and gas industry. Eight months before the Macondo well blowout, the blowout of the Montara well offshore Australia in the Timor Sea developed in almost the same way-with very similar downstream effects.... Piper Alpha (North Sea) platform explosions and fires (1988)...followed roadmaps to disaster that are very similar to that developed during and after the Macondo well blowout. This disaster [Macondo well blowout] also has eerie similarities to the BP Texas City refinery disaster. These similarities include: (a) multiple system operator malfunctions during a critical period in operations,....., (c) neglected maintenance ,....., (e) inappropriate assessment and management of operations risks, (f) multiple operations conducted at critical times with unanticipated interactions, (g) inadequate communications between members of the operations groups, (h) unawareness of risks, (i) diversion of attention at critical times, (j) a culture with incentives that provided increases in productivity without commensurate increases in protection(safety), (k) inappropriate cost and corner cutting, (l) ....., and (m) improper management of change.

Part of the explanation for such replication of different disasters is that the current hazard analysis tools are not designed to analyze dynamic complexity of major incidents, which arise from the interaction between actors (social and technical) and the temporal and spatial gaps between actions and consequences. This is because most traditional causal analysis tools model events and causal factors linearly [4]. Besides, these traditional tools focus on events proximal to the loss.

Rasmussen [5] identified six levels in sociotechnical systems: (a) the government level-6, (b) the regulators and industry association level-5, (c) the management level-4, (d) the company level-3, (e) the staff level-2, and (f) the operation level-1.

Each of these levels represents possible sources of “root causes”. The aftermath of most hazardous, large-scale technological systems’ accidents have serious and long-lasting economic, safety, health and environmental consequences. Hence, it is reasonable to analyze causes at all these levels to be identified so as to prevent recurrences effectively.

However, the analysis of systemic issues, especially those at company, regulators and industry associations, and government levels, (i.e., macro issues) are complex and dynamic. The complexity at these levels arises because causal factors are inter-related and decisions of actors and the corresponding effects are usually separated in time. Unfortunately, most causal analysis tools, such as those evaluated by [2, 6, 7], view cause and effect linearly and are not designed to model changes in the modern system across time. In other terms they are not designed to analyze the dynamic complexity of the emerging modern systems.

It is proposed in this paper that the traditional/classical causal analysis tools can be used to analyze the incident sequence and causal factors that are more immediate to the incident (micro issues). Key causal factors (macro issues) can then be further analyzed using tools designed to model dynamic complexity. The reason, as mentioned earlier, is that most major system accidents do not result simply from a unique set of proximal, physical events but from drift of the whole SS to a state of heightened risk over time as safeguards and controls are relaxed due to conflicting goals and tradeoffs. The challenge in preventing accidents, according to [8], is to establish safeguards and metrics to prevent and detect migration towards a state of unacceptable risk before accident occurs.

Some major thoughts (or rather motivational factors) for new perspectives would in this context be driven by;

- Safety remains the major concern regarding the design and use of modern and complex SSs in the context of rapidly changing technology.
- The increasing complexity in industrial SSs not only created by the latest developments in digital technologies, but also by other change phenomena related to organizational and human elements [1]
- Dynamic and complex environment (e.g. economic pressures, stringent human-safety-environment(HSE) regulations, etc.) has influences on safety of modern industries
- The decision settings of different stakeholders of complex systems have taken different turns involving multiple approaches and notably conflicting criteria

In light of this, it is important to devote some effort to examining our foundations before proposing some incremental improvement in what we do today (refer also [2, 6] for additional critical reviews on foundational safety issues). Re-examining some underlying assumptions and paradigms in safety is invaluable to identify any potential disconnects with the world as it exists today. The assumptions questioned in this paper involve: (a) definition of safety, (b) accident causal models, and (c) understanding on human and organizational error. Subsequently, alternatives based on system thinking are then proposed.

## 2 Assumptions Questioned and Alternative Approaches

Re-examining some underlying assumptions and paradigms in safety is invaluable to identify any potential disconnects with the world as it exists today. The assumptions questioned in this paper involve: (1) definition of safety, (2) accident causal models, and (3) understanding on human and organizational error.

### Assumption 1: Safety Is Enhanced by Increasing the Reliability of the Individual System Components

An MIT (Massachusetts Institute of Technology) professor, Leveson [9] argues that safety and reliability are different system properties: a system can be reliable and unsafe or safe and unreliable. This misperception is epitomized by HRO (high reliability organizations) researchers who suggest that ‘*organizations in which the system components<sup>1</sup> operate reliably will be safe*’ [10–13]. This belief is simply not true. In modern complex systems, accidents may result from interaction among perfectly functioning components.

Leveson explained this situation with an example:

The loss of the Mars Polar Lander was attributed to noise (spurious signals) generated when the landing legs were deployed during descent. This noise was normal and expected and did not represent a failure in the landing leg system. The on board software interpreted these signals as an indication that landing occurred (which the software engineers were told they would indicate) and shut the engines down prematurely, causing the spacecraft to crash into the Mars surface.

According to Leveson, the landing legs and the software performed perfectly (i.e., neither failed), but the accident occurred because the system designers did not account for all interactions between the leg deployment and the descent-engine control software.

In the past, the design of SSs was more intellectually manageable and the potential interactions among components could be thoroughly planned, understood, anticipated, controlled and guarded against [8]. Modern SSs, however, no longer satisfy these properties and system design errors are increasingly the cause of major accidents, even when all the components have operated reliably, i.e., have not failed.

Hence, *safety is system property*, not a component property like reliability [9]. Determining whether an offshore oil and gas plant is acceptably safe, for instance, is not possible by examining a BOP (blow out preventer) in the plant. Conclusions can be reached about the reliability of the BOP without referring to the context in which the BOP is used, but safety of the BOP can only be determined by the relationship between the BOP and the other plant components and its environment, i.e., in the context of the whole.

In systems theory, complex SSs are modeled as a hierarchy of organizational levels, each level more complex than the one below [5]. The levels are characterized

---

<sup>1</sup> Note: ‘component’ in this paper refers to both physical and human components of a SS.

by emergent properties that are irreducible and represent constraints on the degree of freedom of components at the level below. *Safety is an emergent property* and unsafe system behaviour is defined in terms of safety constraints on the behaviour of the system components.

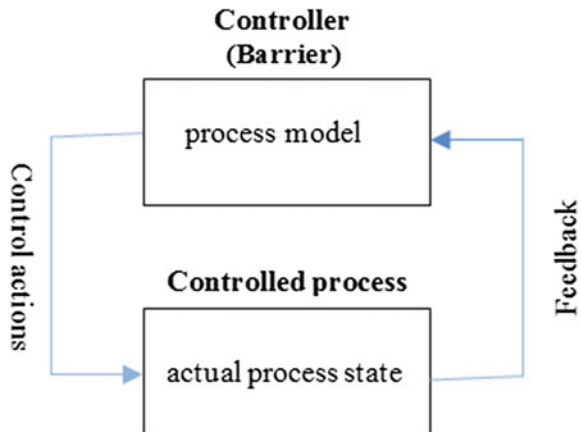
Safety should then be viewed, using systems thinking and systems theory, as a *control problem* (problem of enforcing the safety constraints) rather than a failure or reliability problem [9]. Safety incidents occur when component failures, external disturbances, and/or potentially unsafe interactions among system components are inadequately controlled (managed). In basic systems theory, in order to provide adequate control, the *controller (barrier)* must have an accurate model of the *process* it is controlling (see Fig. 1). For both automated and human controllers, the *process model* (for human controllers, this model is commonly called the mental model) is used to determine what control actions are necessary to keep the system operating effectively.

The process model includes assumptions about how the controlled process operates and about the current state of the controlled process. Safety incidents in complex systems often result from inconsistencies between the model of the process used by the controller (barrier) and the actual process state [3]. For instance: the local BP manager on the Deepwater Horizon disaster [3] thought the cement had properly sealed the annulus (he did not notice the positive pressure test) and ordered the mud to be removed; the operators at Texas City [14] thought the level of liquid in the isomerization unit was below the appropriate threshold.

Usually, these process models of the controlled system become incorrect due to missing or inadequate feedback and communication channels. The effectiveness of the safety control structure is greatly dependent on the accuracy of the information about the actual state of the controlled system each controller has, often in the form of feedback from the controlled process.

In modern SSs major accidents rarely have a single root cause but result from an adaptive feedback function that fails to maintain safety as performance changes

**Fig. 1** ‘Controller-Controlled process’ relationship to determine what actions are needed (modified from [9])



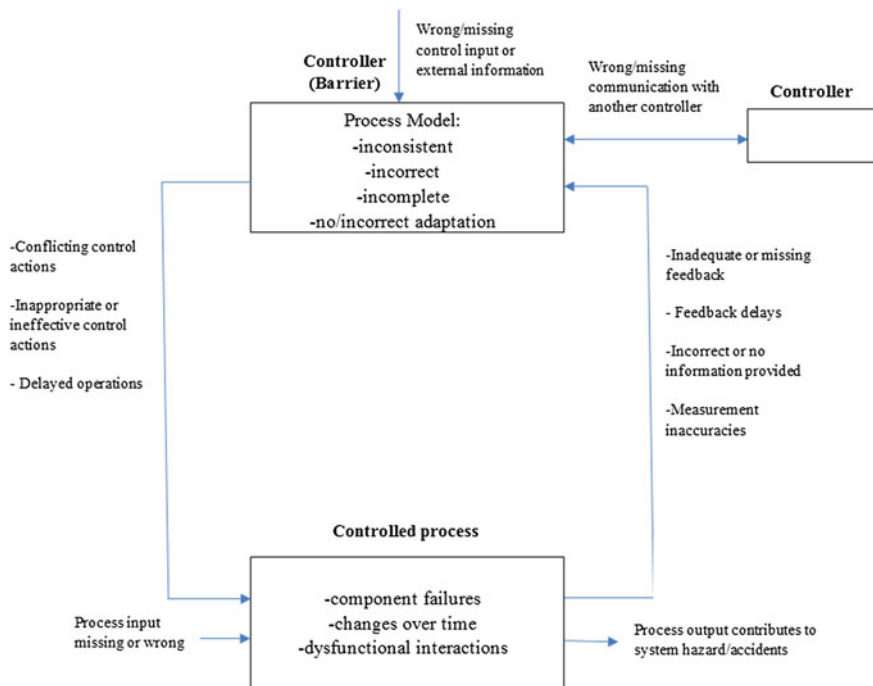


Fig. 2 Some generic factors involved in unsafe control

over time to meet a complex and changing set of goals and values. Figure 2, for instance, shows some of the generic factors involved in unsafe control. Also, as shown in Fig. 2, more than one controller may participate in the safety control structure, with the controllers of the components having individual responsibilities for ensuring that the controlled processes or components are fulfilling their safety responsibilities.

Note that when we say ‘control’ in our case, it is not only about the controls provided by engineered systems (e.g. interlocks, BOP or various types of barriers and fault tolerance features) and direct management and operational interventions, but also indirectly by policies, procedures, shared values, and other aspects of the organizational culture. Therefore, an accident results not simply from components failure or human error, but from the *inadequate control* of the safety-related constraints on the development, design, construction, management and operation of the entire SS.

Figure 3 below shows the safety control structure existing at the time of the Macondo well system accident. Each component has specific assigned responsibilities for maintaining the safety of the entire SS. For instance, the mud logger is responsible for creating a detailed record of a borehole by examining the contents of the circulating drilling medium, the cementer is responsible for properly sealing off a wellbore, and local management has responsibilities for overseeing that these and other activities are carried out properly and safely. The government oversight

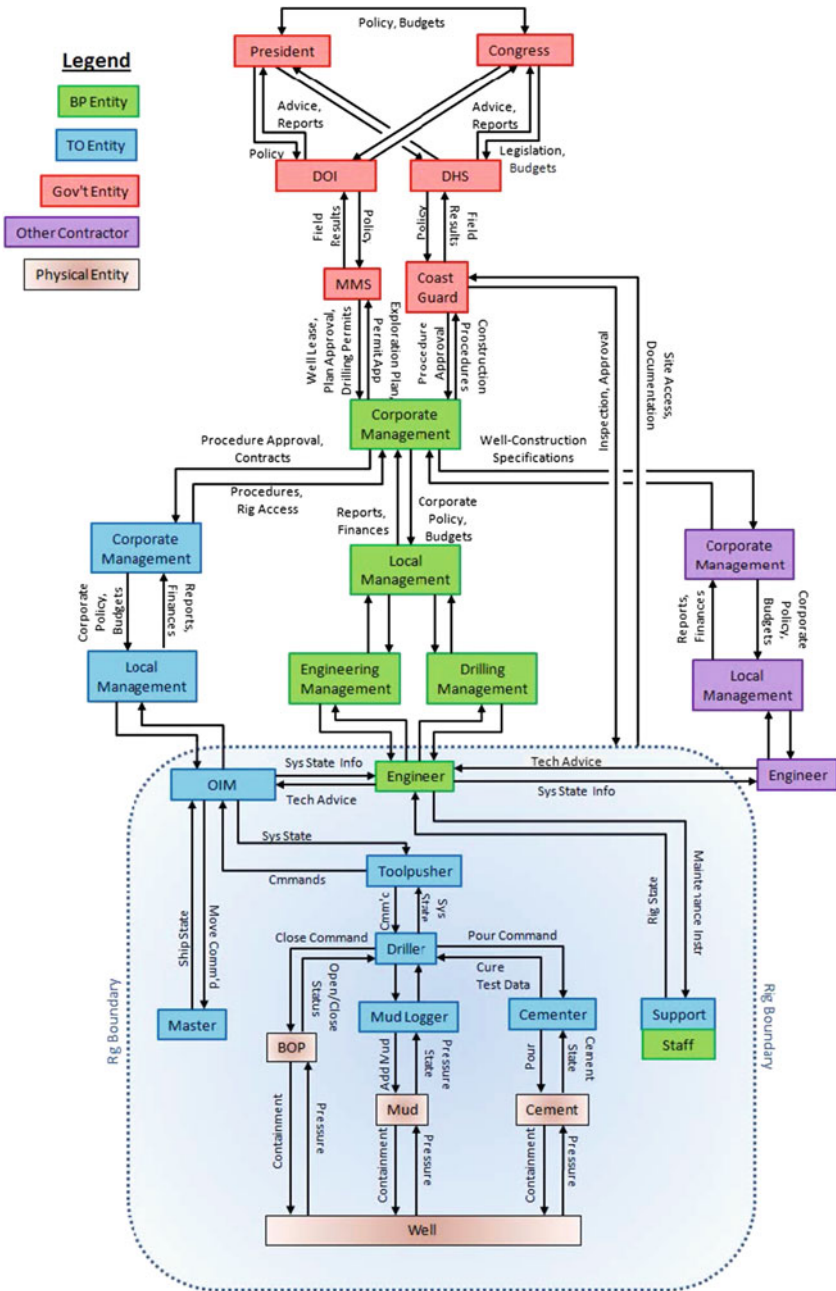


Fig. 3 Safety control structure existing at the time of Macondo blowout (adapted from [8])

agency may be responsible for ensuring that safe practices are being followed and acceptable equipment being used, and so forth and so on.

The main idea that we can draw from this structure is that safety incidents are rarely the result of unsafe behaviour by only one of the components but usually the result of unsafe interactions among and behaviour by all or most of the HOT components in the control structure. A systems thinking approach (such as causal loop diagrams [4], STAMP- Systems-Theoretic Accident Model and Processes [8]) allows capturing the non-linear dynamics of interactions between human, organization and technological (HOT) components of a SS and anticipating the risk-related consequences of change and adaptation over time.

### **Assumption 2: Accidents Are Caused by Chain of Directly Related Failure Events**

This assumption implies that investigating backward from the loss event and identifying directly related predecessor events (usually technical failures or human errors) will identify the “root cause” for the loss. The solution to this approach is then either the “root cause” event is eliminated or an attempt is made to stop the propagation of events by adding barriers between events, by preventing individual failure events in the chain, or by redesigning the system so that multiple failures are required before propagation can occur.

The problem with the chain-of-events model of accident causation is that it oversimplifies causality and the accident process and excludes many of the systemic factors in accidents and indirect or non-linear dynamic interactions among events. It also does not hold for accidents where the cause(s) lies in the interaction among HOT-factors of modern SSs, none of which may have failed.

To hold systemic factors and non-linear dynamic interactions among the HOT factors in modern SSs, the accident causation can be viewed as involving three hierarchical levels, as proposed in Fig. 4. Level 1 is the basic proximate event chain; Level 2 represents the conditions that allowed the events to occur; Level 3 contains the systemic factors that contribute to the conditions and events. The levels are annotated in the figure with the proposed approach to managing modern systems i. e., using systemic thinking approaches (for macro issues) and classical approaches (for micro issues) in a seamless integration.

Classical approaches will help to present facts of the proximal events leading to the loss. The key causal factors (macro factors) can then be further analyzed using systemic thinking approaches. For instance in Macondo blowout: the regulators and the government, each seemed to be doing the “right” thing in view of the pressures that each was facing. However, unintentionally, each actor contributed to the poor safety culture and the worsening of the situation that finally resulted in the blowout. Understanding systemic structure as a whole will help organizations understand the possible negative consequences of their decisions on safety culture and result in the design of more effective safety management strategies. A systems perspective also helps to reduce the tendency to blame a particular group or organization for the incident/accident, thereby increasing the chances of identifying effective proactive measures.



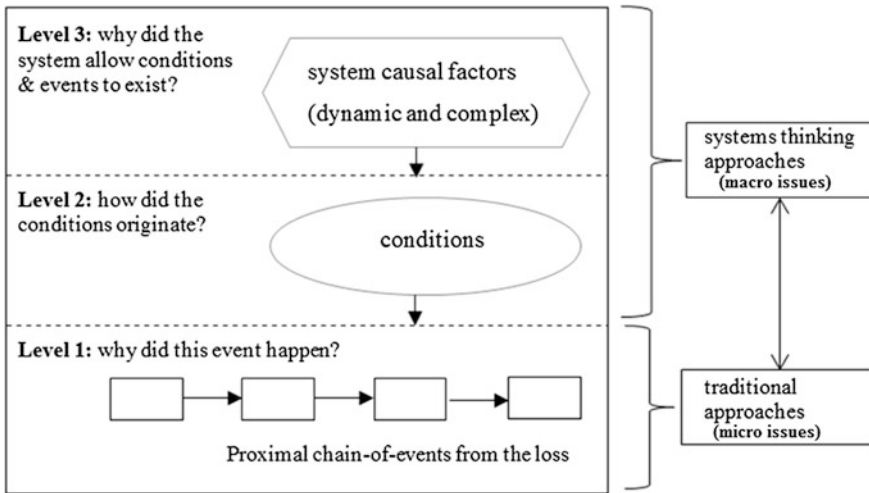


Fig. 4 Macro-micro integration to identify the root cause(s)

The potential advantage of systems thinking is basically to facilitate a more effective way of seeing reality and summarizing dynamically complex situations.

**Assumption 3: Most Accidents Are Caused by Human Error**

Human behaviour is influenced by the context in which it takes place [15] and hence, changing that context will be more effective in reducing accidents than blaming the human for doing errors. The irony in here is that systems are designed in which human error is unavoidable and then blame the human. Moreover, the present digital, complex and large-scale technological systems (with their dynamic environment) pose additional demands and new requirements on the human operators. Modern SSs require human operators to constantly adapt to new and unforeseen system and environmental demands. Furthermore, there is no clear cut distinction between system design and operation, since the operator will have to match system properties to the changing demands and operational conditions. In other words, according to [16, 17], operators must be able to handle the ‘non-design’ emergencies, because the system designers could not foresee all possible scenarios of failures and are not able to provide automatic safety devices for every contingency.

Thus, the role of the human operator responsible for such systems has changed from a manual controller to a supervisory controller who is responsible for overseeing one or more computer controllers who perform the routine [15]. In supervisory control systems, the human operator’s role is primarily passive, i.e., monitoring of change in the system state. The operator’s passive role, however, changes to one of active involvement in cases of unexpected systems events, emergencies, alarm alerts, and/or system failures.

Mental models play a significant role here. The ability to adapt mental models through experience in interacting with the operating system is what makes the

human operator so valuable (see Fig. 5). Designers deal with ideal (or average) systems, and they provide procedures to operators with respect to this ideal. Systems may deviate from the ideal through manufacturing and operation variances or through evolution and changes over time. Operators must deal with the existing system and change their operational procedures using operational experience and experimentation [8]. While procedures may be updated over time, there is usually a time lag in this updating process and operators must deal with the existing system state.

Based on current information, the operators' actual behavior may differ from the prescribed procedures. The irony is that when the deviation brings fortunate results at that particular instant in time, then the operators are considered to be doing their job (and rewarded). However, the operators are often blamed for any unfortunate results, even though their incorrect actions may have been reasonable given the information they had at the time.

Flawed decisions may also result from limitations in the boundaries of the model used, but the boundaries relevant to a particular decision maker may depend on activities of several other decision makers found within the complex modern SS. Safety incidents may then result from the interaction of the potential side effects of the performance of the decision makers during their normal work. It is difficult if not impossible for any individual to judge the safety of their decisions when it is dependent on the decisions made by other people in other departments and organizations [5].

Part of the problem to blaming operators also stems from the linear and deterministic approach to accident investigation where it is usually difficult to find an

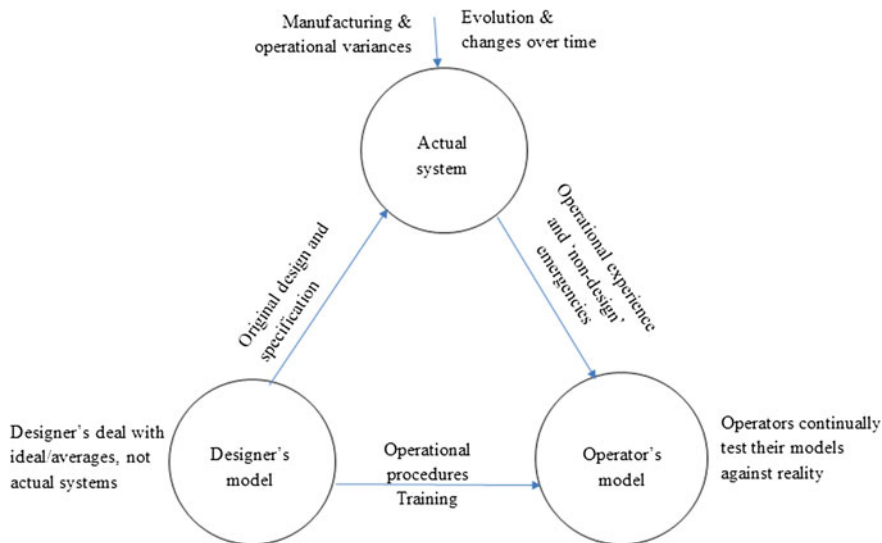


Fig. 5 The role of mental models in operations (modified from [8])

“event” preceding and causal to the operator behaviour [9]. If the problem is the system design, there is no proximal event to explain the error. Even if a technical failure precedes the human action, the tendency is to put the blame on an inadequate response to the failure by an operator. Perrow [11] cites a U.S. Air Force study of aviation accidents that concludes that the designation of a pilot error is a convenient classification for mishaps whose real cause is uncertain, complex, or embarrassing to the organization.

As argued by Reason and others [2, 5, 16–18, etc.], devising more effective accident causality models requires shifting the emphasis in explaining the role of humans in accidents from error (deviations from normative procedures) to focus on the mechanisms and factors that shape human behavior, i.e., the performance-shaping mechanisms and context in which human actions take place and decisions are made. Modeling behavior by decomposing it into decisions and actions (i.e., events) and studying it as a phenomenon isolated from the context in which the behavior takes place is not an effective way to understand behaviour.

### 3 Analyses and Discussion

Much effort has been done to avoid safety incidents, but they still occur. The problem is that no engineering process is perfect, and every SS and its environment evolve and are subject to change over time. However, our analysis tools are more of static and deterministic (i.e., they model cause and effect linearly and focus on events proximal to the loss).

In general, the causes for safety incidents in modern SSs:

1. May arise in the development and implementation of the system,
2. May reflect management and cultural deficiencies,
3. May arise in operations

#### 3.1 *Development and Implementation*

- Inadequate safety incident analysis (assumptions about the system hazards or the process used to identify them do not hold)
  - Safety incident analysis is not performed(or is not completed)
  - some safety incidents are not identified or are not handled because they are often assumed to be “sufficiently unlikely”
  - safety incident analysis is incomplete (important causes are omitted)
- Inadequate identification and design of control and mitigation measures for the hazards (e.g., due to inappropriate assumptions about operations)
- Inadequate construction of control and mitigation measures

### ***3.2 Management and Cultural Deficiencies***

- The design of the safety control structure is flawed
- The safety control structure does not operate the way it was designed to operate
  - one general cause may be the safety culture, i.e., the goals and values of the organization with respect to safety, degrades over time
  - the behavior of those in the safety control structure may be influenced by competitive, financial or other pressures

### ***3.3 Operations***

- Controls that designers assumed would exist during operations are not adequately implemented.
- Changes over time violate the assumptions underlying the design and controls [8]
  - New hazards(arise with changes over time) were not anticipated during design and development or were dismissed as unlikely to occur
  - Physical controls and mitigation measures degrade over time in ways not accounted for in the analysis and design process
  - Components (including humans [1] ) behave differently over time (violate assumptions made during design and analysis)
  - The system environment changes over time (violates assumptions made during design and analysis)

To adequately control (manage) safety incidents of modern SSs, we propose systems thinking approaches to work in seamless integration with traditional investigation and causal analysis methods (see Fig. 4). However, the potential advantages of systems thinking approaches to seeing reality and summarizing dynamically complex situations in more effective way depend on the people to adapt a systems-oriented paradigm.

To understand the cause of accidents and to prevent future ones, the system's hierarchical safety control structure (see Fig. 4) must be examined to determine why the controls at each level were inadequate to maintain the constraints on safe behaviour at the level below and why the events occurred. To get a deep enough understanding of the causal factors in an accident such as the Macondo blowout, the reasons for the events and the conditions leading to those events as well as systemic causes need to be identified.

The first step in the safety incident analysis is, hence, to understand the physical proximal factors (micro issues) involved in the loss, including:

- the limitation of the physical system design (e.g., The BOP system was neither designed nor tested for the dynamic conditions that most likely existed at the time that attempts were made to recapture well control),

- the failures and dysfunctional interactions among the physical system components (e.g., the operator at Macondo blow out did not notice the positive pressure test), and,
- environmental factors (e.g., deep water, high temperature, high pressure-HTHP) that interacted with the physical system design

Most classical accident analyses include this information, though they usually omit dysfunctional interactions and look only for component failures. Understanding the physical factors leading to the loss is only the first step in understanding why the accident occurred.

The next step is, understanding how the engineering design practices contributed to the accident and how they could be changed to prevent such an accident in the future. Why was the hazard (e.g., blowout as a result of spills) not adequately controlled in the design? Some controls were installed to prevent this hazard (for example, the BOP and the assignment to see pressure test), but some controls were inadequate or missing.

Many of the reasons underlying poor design and operational practices stem from management and oversight inadequacies due to conflicting requirements and pressures. Identifying the factors lying behind the physical design starts with identifying the safety-related responsibilities assigned to each component in the hierarchical safety control structure along with their safety constraints [8]. Using these safety-related responsibilities, the inadequate control actions for each of the components in the control structure can be identified. In most major accidents, there is inadequate control exhibited throughout the structure, assuming an adequate control structure was designed to begin with (see Fig. 2). But simply finding out how each person or group contributed to the loss is only the start of the process necessary to learn what needs to be changed to prevent future accidents. We must first understand why the “controllers” (see Fig. 1) provided inadequate control. The analysis process must identify the systemic factors in the accident causation, not just the symptoms.

To understand why people behave the way they do, we must examine their mental models and the contextual factors affecting their decision making. All human decision-making is based on the person’s mental model of the state and operation of the system being controlled (see Fig. 5). Preventing inadequate control actions in the future requires not only identifying the flaws in the controllers’ process models (including those of the management and government components of the hierarchical safety control structure) but also why these flaws existed.

## 4 Conclusions

Two conclusions may be drawn from the study. One conclusion is related to the critical review on some key assumptions (such as assumptions on: safety vs. reliability; accident causation models; human and organizational error) and the

important of defining safety as: a control problem; system property (i.e., safety deals with systems as a whole, not just components, knowing that many accidents occur because of interactions among HOT subsystems); an emergent property.

The second conclusion is related the proposed approaches (i.e., using systemic thinking approaches as a complement to the classical approaches) to managing risk & safety incidents of modern and dynamic SSs. This approach could remove hindsight bias views and conduct a modern SS towards foresight views.

In the future human, organization and technology (HOT) subsystems will be even more coupled and interdependent, and the boundaries between them will be more blurred. Complex and dynamic interactions, an ever advancing digital technology, trust (both in the technology and human), and common situational awareness among the people at different locations are some of the issues that are more likely to become more important in the future.

Even though traditional causal analysis tools are useful and necessary, they model cause and effect linearly and they are less effective in representing the complex and dynamic interactions between multiple actors and factors across time. It is therefore proposed that systems thinking approaches (methods, tools) should be employed in the analysis of macro-issues in a seamless integration with the traditional tools (which deal with proximal-to-the-loss events/micro issues) so that the systemic structure that contributed to the incident can be more readily understood. The use of systemic thinking approaches could facilitate the early identification of emerging problems in modern industries so as to introduce proactive measures that improve safety and risk management capacity rather than event-level interventions. In addition, it is believed that more research and application of systems thinking concepts will improve the overall effectiveness of safety, health and environment management.

## References

1. Liyanage JP (2012) Human-An asset or a liability: The real deal with modern humans in intelligent systems and complex operations, Daejeon, WCEAM2012, accepted
2. Abraha HH, Liyanage JP (2012) Review of theories and accident causation models: Understanding of the human-context dyad towards the use in modern complex systems, Daejeon, WCEAM2012, accepted
3. Deepwater Horizon Study Group, DHSG (2011) [online]. Retrieved from <[http://ccrm.berkeley.edu/pdfs\\_papers/bea\\_pdfs/dhsgfinalreport-march2011-tag.pdf](http://ccrm.berkeley.edu/pdfs_papers/bea_pdfs/dhsgfinalreport-march2011-tag.pdf)> [accessed: 03 FEB 2013]
4. Goh YM, Brown H, Spickett J (2010) Applying systems thinking concepts in the analysis of major incidents and safety culture. *Saf Sci* 48(3):302–309
5. Rasmussen J (1997) Risk management in a dynamic society: a modeling problem. *Saf Sci* 27 (2):183–213
6. Abraha HH, Liyanage JP (2012) Review of theoretical foundations for risk minimal operations in complex socio-technical systems: The role of human error, Daejeon, WCEAM2012, accepted
7. Sklet S (2004) Comparison of some selected methods for accident investigation. *J Hazard Mater* 111(1–3):29–37

8. Leveson NG (2013) A systems thinking approach to leading indicators in the petrochemical industry: ESD working paper series. Retrieved from <<http://esd.mit.edu/wps/2013/esd-wp-2013-01.pdf>> [accessed: 15 May 2013]
9. Leveson N (2011) Risk Management in the oil and gas industry [online]. Retrieved from <<http://mitei.mit.edu/news/risk-management-oil-and-gas-industry>> [accessed: 10 FEB 2013]
10. LaPorte TR, Consolini PM (1991) Working in practice but not in theory: theoretical challenges of "high-reliability organizations". *J Public Admin Res Theory: J-PART 1(1)*:19-48. Oxford Journal of Public Administration Research and Theory, Inc
11. Perrow C (1999) Y2 K as a normal accident. International Conference on Disaster Management and Medical Relief, June 14-16, Amsterdam
12. Roberts KH (1990) Managing high reliability organizations. *Calif Manag Rev* 32(4):101-114
13. Weick Karl E, Sutcliffe K, Obstfeld D (1999) Organizing for high reliability. *Res Org Behav* 21:81-123
14. CBS(2005) Chemical Safety Board (2007). Investigation report: Refinery explosion and fire, BP Texas City, March 23
15. Dekker S (2006) *The field guide to understanding human error*. Ashgate, Aldershot
16. Reason J (1990) *Human error*. Cambridge University Press, Cambridge
17. Reason J (1997) *Managing the Risks of Organizational Accidents*. Ashgate, England
18. Rasmussen J (1986) *Information processing and human-machine interaction: an approach to cognitive engineering*. North-Holland, New York