# Management by Hierarchical Control versus Mindfulness

#### **<u>G. Lintern<sup>1</sup></u> and P. N. Kugler<sup>2</sup>**

<sup>1</sup>Monash University Accident Research Centre, Building 70, Monash University, Victoria 3800, Australia, Email: <u>glintern@CognitiveSystemsDesign.net</u>

<sup>2</sup>Contract Engineer, Brewster, MA 02631, USA

**Abstract:** Hierarchical control, as developed within systems engineering, and mindfulness, as developed within management science, offer contrasting approaches to organizational management for sociotechnical systems. The hierarchical control model proposes that the social and organizational processes within a sociotechnical system conform to a multi-level, hierarchical control structure. The model posits that the various levels of management and operations are connected by communication and control links, with a descending path propagating management decisions down the hierarchy and an ascending path propagating information about work-related processes up the hierarchy. These communication links between levels constitute interdependencies that are viewed as critical to the functioning of an effective system

Although it would seem to capture the essential multilevel character of complex sociotechnical systems, the between-level transactions promoted by the hierarchical control model have a formal and rational character. Those promoting this model appear to be ignoring the essential cognitive processes that make contemporary knowledge systems work. Following Weick and Sutcliffe (2001), we characterize those cognitive processes as elements of mindfulness; the cognitive state of being alert to and inquiring continuously about subtle and changing situational complexities. Those who are mindful understand that operational work has many subtle and complex details, they remain sensitive to operational demands, they defer to expertise, and they reflect zealously on the potential for failure.

As implied by the topic statement for this session, the design and management of large-scale sociotechnical systems pose significant challenges. In part, we continue to struggle with this because we do not have a comprehensive functional model that takes account of the essential melding between the socio and the technical. Here we propose that a hierarchical structure, when complemented with insights relating to organizational mindfulness, offers an innovative model that can guide us towards resolving that challenge.

Keywords: System design, organizational factors, organizational cognition

## 1. INTRODUCTION

On 11 March 2011, a violent earthquake off the East coast of Japan created a tsunami that surged over the seawall of Fukushima Dai-Ichi nuclear power station, resulting in a multiple core meltdown. Over the following days, Tokyo was threatened with irradiation, raising the possibility of mass evacuation from the city and threatening the economic future of Japan (Willacy, 2013). With historical records suggesting that a tsunami of that magnitude and destructive power could be anticipated every 800 years or so, the failure to build an adequate seawall, and to protect backup systems against earthquake and flooding, seems grossly neglectful.

On 20 April 2010, an oil drilling rig, Deepwater Horizon, blew out in the Gulf of Mexico. Eleven workers perished that day and subsequently, over a period of three months, the damaged well released almost five million barrels of oil into the Gulf of Mexico. As reported by the National Commission on the BP Deepwater Horizon Oil Spill and Offshore Drilling (2011), diverse safety systems and backup safety systems failed at critical times. In addition, poor planning by off-rig management and poor coordination between on-rig teams contributed to the accident and exacerbated its severity.

These are just two of the many industrial accidents we have witnessed over recent decade that can be classified as major disasters. In retrospect, the system fragilities that contributed to these enormous losses seem trifling, even inconsequential, thereby conforming to the idea that highly-coupled systems allow the effects of some types of events to cascade through the system, expanding the magnitude of the catastrophe (Perrow, 1984). Nevertheless, despite all that has been written on large-scale industrial accidents with catastrophic potential, we can have no confidence that we have resolved the general problem; that we have eliminated similarly fragile design features lurking within other large-scale industrial complexes with catastrophic potential.

#### 2. SAFETY MANAGEMENT

Proactive safety management of large-scale sociotechnical systems remains a challenge. Two different approaches, the hierarchical control model as developed in extensive detail by Leveson (2011), and mindfulness as discussed by Weick and Sutcliffe (2001), offer promise in this area. Safety management for large socio-technical systems is typically retroactive. While there is much to be gained from a retroactive analysis of major accidents, we have many systems with such catastrophic potential that they must be made safe for their entire working life. Both hierarchical control and mindfulness underpin approaches to proactive safety management (Lintern & Kugler, 2017). In this paper, we outline each approach and review a selection of the related safety management issues.

#### 2.1. Hierarchical Control

Leveson (2011) offers a hazard analysis technique that is based on the view of an organization as a hierarchical control structure. Within this hierarchical structure, organizational entities with different management responsibilities are arranged in layers as shown in figure 1. The controlling executive is represented at the highest level with lower levels in the hierarchy responsible for operations management and, at the lowest level, plant operations. The organization is seen to function as a coherent system by virtue of control and communication links between levels; a downward reference channel that exerts control over operational behavior by transmitting instructions and constraints from the top management level through intermediate levels to the bottom operational level, and an upward reference channel that passes operational assessments through intermediate levels to the top level about the efficacy of management instructions and constraints for controlling operational behavior at the bottom level.

Hierarchy is the most popular and intuitively appealing conception of organizational structure. It has those at the highest level in charge and those at



Figure 1. An organization viewed as a hierarchical control system (adapted from Leveson, 2011).

progressively lower levels being accorded degrees of authority and control as delegated from the level above. Accident analyses guided by the hierarchical model typically attribute flaws in safety management to failure associated with the descending and ascending communication channels (Leveson, 2011; Vicente and Christoffersen, 2006). Safety is jeopardized when the control exerted via the descending communication channel is loose and when the feedback arriving at the higher levels about lower-level functions and processes is imprecise, unreliable, or incomplete.

Hierarchical control theory is relevant to the analysis of the Deepwater Horizon accident in which there was no sustained effort by upper-level management to ensure that on-rig operations conformed to a rather extensive set of guidelines and instructions. In contrast, the Fukushima accident resulted from a design flaw rather than from operational errors, but Leveson's System-Theoretic Process Analysis allows a hierarchical control structure for design that links with the hierarchical control structure for system operations (see Leveson, 2011, page 82), thereby accommodating design issues within the framework.

## 2.2. Mindfulness

Karl Weick and his colleagues forward an argument that socio-technical systems become safe, effective, and adaptive in their management of complex, ill-structured contingencies by integrating orderly cognitive functions and processes with variations in routine activities (Weick, Sutcliffe and Obstfeld, 1999; Weick and Sutcliffe, 2001). The central cognitive construct in this work is that of mindfulness and the central challenge is that of adapting to situated contingencies where effects combine in unusual and unexpected ways to generate new and unanticipated problems.

Mindfulness is the cognitive state of being alert to and inquiring continuously about changing situational complexities. Those who are mindful are fully committed to system resilience. They understand that operational work has many subtle and complex details, they remain sensitive to operational demands, they defer to expertise, and they reflect zealously on the potential for failure. Mindfulness encompasses perceiving, understanding, and acting and might be viewed as an attentive process of building situation awareness (Endsley, 2015) integrated with a similarly attentive process of mental simulation as undertaken in naturalistic decision making (Klein, 1998). Mindfulness encourages ongoing scrutiny of existing expectations combined with continuous refinement and differentiation of expectations based on new experiences (Weick & Sutcliffe, 2001). It also encourages a willingness and a capability to invent new expectations that make sense of unprecedented events, a more nuanced appreciation of context and ways to deal with it, and identification of new dimensions of context that improve foresight and current functioning.

Mindfulness is viewed as crucial to the effective functioning of complex, hierarchical human organizations. Failures in organizational effectiveness, which include lapses in safety, are typically attributed to lack of mindfulness at one or more levels of an organization. Here, we propose that mindfulness is the opposite of neglectfulness, which was pervasive at both management and operational levels in the Deepwater Horizon accident and was a factor in design of safeguards against flooding at Fukushima.

#### 3. HIERARCHICAL MANAGEMENT

Executive, management, and operational functions are undertaken at different organizational levels (Figure 1). In any organization, there are information transactions across the levels that impact how work is done at each of the levels and some sort of transactional exchange between levels is essential. The two theories, hierarchical control and mindfulness, characterize these exchanges in contrasting ways. With hierarchical control, they are control loops involving instructions from above and feedback from below. With mindfulness, they involve zealous reflection on the potential for failure within and between levels, accompanied by constant vigilance for, and constant readiness to respond to signs that anticipate hazardous events.

Hierarchical control manages safety proactively by implementing inter-level control structures for hazards that are identified through detailed and systematic analysis. To the extent that the analysis is comprehensive, nothing can happen that is unexpected. In contrast, mindfulness assumes that no analysis can anticipate all possibilities and that safety-critical organizations must prepare to cope with the unexpected. Mindfulness theory addresses hazard management proactively by promoting an organizational culture that reflects zealously on the potential for failure, develops sensitivity to information that presages hazardous conditions, and builds an adaptive capacity to respond to hazardous situations.

The most salient difference between the two is that hierarchical control promotes tight specification of operational procedures while mindfulness promotes tight social coupling around core cultural values accompanied by loose coupling around the means for realizing those values. For Leveson (2011), system safety

is promoted by controls that enforce the essential constraints while Weick et al (1999) argue for structural under-specification that does not lock all system constraints.

#### 4. **DISSENSIONS**

#### 4.1. Hierarchical Control

The foundational image for hierarchical control is a feedback control system or servomechanism in which a process responds to a command derived from an intention. Execution of the process results in an output which is looped back as feedback to be compared to the intention. Any mismatch between feedback and intention stimulates more processing aimed at reducing the discrepancy. In the hierarchical control model, the feedback control spans adjacent levels, with the processing undertaken in the lower level and the comparison of feedback and intent undertaken in the upper level.

The servomechanism image does not capture the full implications of *control* as that term is used in the hierarchical control model. Control can also be viewed as the action taken to achieve stability in a dynamic system. To illustrate, the balance point for a predator-prey system is an emergent property of the carrying capacity for each of the two species; the carrying capacity of the natural environment for the prey (primarily, food and shelter), which in turn, establishes the carrying capacity (food) for the predator.

A dynamic system has a control parameter. To adjust the balance point of a predator-prey system (e.g., more or fewer predators) we might adjust the food supply and shelter for the prey. On its own, direct action on predators is unlikely to have a long-term effect. Furthermore, the control parameter for a dynamic system is not always obvious. For example, we may intuit that our home pet (dog or cat) sheds its coat as winter closes in response to warmer weather. The shedding mechanism is, however, controlled by the lengthening period of daylight (wikipedia.org, 2017). Similarly, natural sequence farming seeks to restore organic matter to depleted soil by rehabilitation of ground water flows rather than by direct cultivation of the soil (Williams, 2010).

This raises a concern for a hierarchical control analysis; even when a hazard is identified, the defense may not be self-evident. In the terms of dynamic systems, we need to know how the system works to ensure we adjust the right control parameter and to ensure we adjust it in a way that achieves the stable point we want. Mindfulness does not negate the need for control but rather, helps workers and management become attuned to how they should go about controlling a system they do not fully understand and how they should assess whether their control actions are having the desired effect.

#### 4.2. System Design

Hazard management is both an analysis problem and a design problem. There is, however, as sense within the safety literature that design for hazard management is straightforward once the hazard is identified; that the nature of the solution is obvious from the description of the problem. The poverty of this view is illustrated in the work of Iedema, Jorm, Braithwaite, et al (2006) who reported on a safety investigation of a morphine overdose in a healthcare setting. They found that the clinical team undertaking the investigation could not distinguish correct from incorrect ways of doing healthcare work. The clinical team grappled with the problem of imposing procedural solutions on contexts and practices they knew to be uncertain and contradictory, observing that the complexity and ambiguity of healthcare work demanded participatory or cultural solutions that promoted heedfulness and interactive flexibility. We take heedfulness as introduced by Iedema, et al (2006) to be like, or possibly even equivalent to mindfulness as discussed by Weick and his associates.

For Leveson (2011), hazards are identified and then resolved by enforcement of procedural constraints. The situation with access to commercial aviation cockpits underscores the problems that arise with an exclusively rule-based approach. Prior to September 11, 2001, commercial aircrew cooperated with terrorists, allowing them access to the cockpit, in expectation that the lives of passengers and crew could be saved by patient negotiation. The September 11, 2001attack changed that. The procedures in place were not set up to cope with a suicide mission. After that attack, heavy-duty doors locks were installed to prevent access to the cockpit by unauthorized passengers. However, this new system enabled the destruction by the second officer of Germanwings Flight 9525 in March 2015. Apparently, the first officer left the cockpit for a brief time and the second officer would not let him back. This sort of crash by suicide would not have been possible under the system in place before the September 11, 2001 attack. More generally, a rule may plug one vulnerability but create another.

Following Rasmussen (1986), Lintern and Motavalli (submitted) argue that procedures should be used judiciously and that a comprehensive design strategy will employ a well-integrated mix of knowledge- and

skill-based strategies along with the rule-based strategies. Rules are an obvious, conceptually easy solution, but are brittle to changes in context. Particularly in an adversarial situation, a clever and adaptable enemy will exploit our rule sets to their advantage.

There is, however, a more general problem in system development; many take a detailed and systematic approach to analysis but take an ad hoc approach to design, while others take a detailed and systematic approach to design but an ad hoc approach to analysis. Bennet and Flach (2011) offer one of the few treatments of the design problem that brings these together in a meaningful way. In a similar vein, Lintern (2013) has demonstrated how to follow a detailed and comprehensive analysis with explicit and systematic design strategies.

## 4.3. Complacency

Organizational complacency has been a factor in many major accidents. Leveson (2011, page 34) notes the dangers of organizational complacency when she discusses the loss of the steamship, Titanic, which she attributes in part to the fact that a widespread belief in the unsinkability of the Titanic induced behaviors that were inconsistent with best safety management practice. Although every major accident is different in its specifics, the most pervasive similarity is the neglect of crucial issues that, in retrospect at least, seem to have been obvious. In that this was evident in the chemical spill at Bhopal, India decades ago (Lapierre & Moro, 2002), and in the Deepwater Horizon Gulf Oil Spill (National Commission on the BP Deepwater Horizon Oil Spill and Offshore Drilling, 2011) and the Fukushima Dai-Ichi nuclear power station accident (Willacy, 2013) in the current decade, this seems to be a pervasive and continuing problem.

For Leveson (2011), the solution to organizational complacency is to enforce procedural compliance. For Weick, et al (1999) and Weick and Sutcliffe (2001), the solution lies in developing a culture of organizational mindfulness. Notably, in expressing her concern for the dangers of organizational complacency, Leveson appears to argue for a social process that is something like mindfulness. Nevertheless, she explicitly rejects Weick's concept of mindfulness and other associated ideas on high-reliability organizations as misleading to the enterprise of safety management (Leveson, 2011; Lintern & Kugler, 2017).

Problematically, it is difficult to see how a complacent organization can be motivated to change its behavior. In implementing crew resource management, commercial aviation made the transition, motivated by an accumulation of highly visible disasters that revealed the problems associated with the then current model of crew interaction. Somehow, commercial aviation abstracted useful lessons from those disasters (Lintern & Kugler, 2017). In contrast, is not clear that the relevant industries have abstracted useful lessons from Bhopal, Fukushima, or Deepwater Horizon. If those disasters were not sufficiently noteworthy to force a revision of strategy, it is unclear what type of experience will.

#### 4.4. Organizational Dysfunction

The team and management problems that contributed to the Deepwater Horizon accident were self-evident, at least after the accident. Management was disengaged with operations and operational teams downplayed the significance of warning signs. It would not have taken much effort to identify these issues proactively and Leveson's form of hazard analysis, if undertaken by diligent and competent professionals, would almost certainly have served the purpose. It would not be overly harsh to characterize the Deepwater Horizon problem as chronic organizational dysfunction.

Westrum (2009) points to an opposing problem; that managers can exhibit a pathological emphasis on authority and a bureaucratic emphasis on rules, order and accountability. They can, in other words, fall into the trap of micro-management. Weick and Sutcliffe (2001) outline the problems that ensued after two US companies, Union Pacific Railroad and Southern Pacific Railroad, merged in 1996. In a well-intentioned attempt to improve efficiency and productivity of the merged entity, management imposed new operational procedures without understanding or appreciating the complex, situated details of the work. This micro-management disrupted operations and appear to have led to several accidents.

It might initially seem that management must balance competing demands, walking a tightrope between pathological micro-management and pathological disengagement. However, we might find a solution in the idea from Weick et al (1999) that we need tight social coupling around core cultural values (e.g., efficiency, productivity) and loose coupling around the means for realizing those values; in other words, an emphasis on organizational priorities but a relaxed attitude about how operational work is executed. More generally, Weick et al (1999) promote structural under-specification that does not lock all system constraints. They argue for a

hybrid system in which relaxed hierarchical structures promote an essential level of orderliness but are sufficiently loose to encourage flexible action and collaborative problem solving.

### 5. DISCUSSION

### 5.1. The challenge

Leveson's (2011) strategy of hazard analysis is detailed and comprehensive and, in going beyond the purely technical aspects of a sociotechnical system to take account of human interactions, adds an important dimension to traditional strategies of hazard analysis. This analysis typically identifies scores of frailties, thereby implying that control needs to be exerted over scores of hazards. At first glance, the hazards and the procedural defenses seem obvious and incontestable. However, if they are indeed obvious and incontestable, we might ask why they were not covered proactively in the systems Leveson analyzed. While that analysis is undoubtedly useful, it does not add any level of protection for hazards that are already evident but ignored.

Nor does it add any level of protection for hazards not revealed by the analysis. Whether an analysis does identify and then resolve all significant hazards will inevitably depend on the expertise and rigor applied to the analysis and the system design. For example, a risk analysis conducted during development of the Fukushima Dai-Ichi nuclear power station identified the possibility of flooding from a typhoon-induced sea surge but not from a tsunami of a size found in historical records for that area (Willacy, 2013). Furthermore, given that the risk analysis had identified the possibility of flooding, it is disconcerting that the backup power generators were not protected against its potential effects.

Inevitably, no strategy of hazard analysis can be assumed to uncover or respond appropriately to all significant hazards. If these become evident during system operation, safe recovery will depend on the attentiveness and expertise of the workforce. In reprise of Iedema, et al (2006), it seems that proactivity demands something other than a list of vulnerabilities and procedural solutions; it needs some sort of participatory or cultural response that promotes mindfulness.

#### 5.2. System Orderliness

One implication of Leveson's argument is that sociotechnical systems must be designed to be orderly. That would seem, in fact, to be the purpose of the extensive complement of standards and protocols that emerge from her form of hazard analysis. As noted by Vincent and Amalberti (2016), safety within orderly sociotechnical systems in which activities are highly standardized can benefit from a detailed set of standards and protocols. However, not even the most standardized of sociotechnical systems can avoid the unexpected entirely, as was evident at Fukushima and Bhopal. Commercial aviation is possibly the most standardized of industries. It has a creditable safety record in the face of countless opportunities for disaster, yet even here, strict standardization has been complemented with an emphasis on mindful interactions between crew members in the cockpit (Lintern & Kugler, 2017).

Furthermore, some sociotechnical systems are inherently disorderly and do not lend themselves well to control or management predominantly by use of standards and protocols (Vincent and Amalberti, 2016). They do benefit from use of a sparse and carefully targeted set of standards and protocols, but for sociotechnical systems in which unpredictable perturbations place unavoidable demands on the professional judgement and flexibility of the workforce, organizational mindfulness would appear to be crucial.

#### 6. CONCLUSION

Rather than an outright rejection of one safety management approach versus the other, we need a structured approach, such as offered by a hierarchical model, to be complemented with the principles of mindfulness. The balance between procedural control and mindful management will, to some extent, be based on the predictably and orderliness of the system but, if we are to take the mindfulness arguments seriously, the use of standards and protocols in disorderly systems should be minimally judicious.

The occasional references to hierarchical structure in the mindfulness literature are typically implicit rather than explicit. There is value for safety management in a more explicit treatment of how mindfulness can function within a hierarchical management structure. Although building on the work of others, Leveson's (2011) treatment of hierarchical management structure in sociotechnical systems is far more detailed and extensive than anything before it. In that respect, her treatment motivates further consideration of how social processes either detract from or enhance safety.

#### REFERENCES

Bennett, K.B. and Flach, J.M. (2011). *Display and Interface Design: Subtle Science, Exact Art.* Boca Raton, FL, CRC Press, ISBN-13: 978-1-4200-6439-1 (Ebook-PDF).

Endsley, M.R. (2015). Situation awareness: operationally necessary and scientifically grounded. *Cognition Technology and Work*, 17, 163–167.

Iedema, R.A. M., Jorm, C., Braithwaite, J., Travaglia, J. and Lum, M. (2006). A root cause analysis of clinical error: Confronting the disjunction between formal rules and situated clinical activity. *Social Science and Medicine* 63, 1201-1212.

Klein, G. (1998). Sources of power: how people make decisions. Cambridge, Massachusetts: MIT press.

Lapierre, D. and Moro, J. (2002). *Five past midnight in Bhopal: the epic story of the world's deadliest industrial disaster*. New York: Warner Books ISBN 0-446-53088-3.

Leveson, N.G. (2011). *Engineering a Safer World. Systems Thinking Applied to Safety*. Cambridge, MA: MIT Press.

Lintern, G. (2013). *Joker One: A Tutorial in Cognitive Work Analysis*. Melbourne, Australia: Cognitive Systems Design. http://www.cognitivesystemsdesign.net/Downloads/Cognitive Work Analysis Joker One Tutorial.pdf, Accessed August 1, 2013.

Lintern, G. and Kugler, P.N. (2017). Sociotechnical System Safety: Hierarchical Control versus Mindfulness. *Syst Eng.* Wiley Online Library, dx.doi.org/10.1002/sys.21396.

Lintern, G. and Motavalli, A. (submitted). Healthcare Information Systems: The Cognitive Challenge. *BMC Medical Informatics and Decision Making*.

National Commission on the BP Deepwater Horizon Oil Spill and Offshore Drilling (2011). *Deep Water: The Gulf oil disaster and the future of Offshore Drilling*. https://www.nrt.org/sites/2/files/GPO-OILCOMMISSION.pdf. Accessed 18 May 2017.

Perrow, C. (1984). Normal Accidents: Living with High Risk Technologies. New York: Basic Books.

Rasmussen J. *Information processing and human machine interaction: an approach to cognitive engineering.* New York: science publishing, North Holland series in system science and engineering, 1986;12. ISBN 0-444-00987-6.

Vincent C., Amalberti R. (2016). Safer healthcare: Strategies for the real world. New York, NY: Springer Open, ISBN 978-3-319-25557-6, ISBN 978-3-319-25559-0 (eBook), DOI 10.1007/978-3-319-25559-0

Vicente, K.J. and Christoffersen, K. (2006). The Walkerton E. coli outbreak: A test of Rasmussen's framework for risk management in a dynamic society. *Theoretical Issues in Ergonomics Science*, 7, 93–112.

Weick, K.E. and Sutcliffe, K.M. (2001). *Managing the unexpected: assuring high performance in an age of complexity*. San Francisco: John Wiley.

Weick, K.E., Sutcliffe, K.M. and Obstfeld D. (1999). Organizing for High Reliability Processes of Collective Mindfulness. *Research in Organizational Behavior*, 21, 81-123.

Westrum, R. (2009). Information Flow and Problem Solving. In Croskerry, P., Cosby, K.S., Schenkel, S.M., and Wears, R.L (eds), *Patient Safety in Emergency Medicine*. Philadelphia: Lippincott Williams and Wilkins, Ch 6, pp 34-39.

Wikipedia (2017). Coat (Dog). https://en.wikipedia.org/wiki/Coat\_(dog). Accessed July 14, 2017.

Williams, J. (2010). The principles of Natural Sequence Farming. Int. J. Water, 5 (4), 396-400.

Willacy, M. (2013). Fukushima: Japan's Tsunami and the inside story of the nuclear meltdown. Sydney: Macmillan Australia.