SAFETY SCIENCE Monitor

Safety in Action
25-28 February 1998

Special Edition 1999

Philosophy of Safety
Article 1

VOL 3

THE CONCEPT OF HUMAN ERROR: IS IT USEFUL FOR THE DESIGN OF SAFE SYSTEMS?

JENS RASMUSSEN, EMERITUS PROFESSOR

Analyses of industrial accidents have often concluded that 'human error' is a determining factor in 70-80% of the cases. Furthermore, multiple contributing errors and faults are normally found, because several defenses against accident have been used to protect a hazardous process. Typically, it is also concluded that the 'root cause' of the accident was a human error on part of a person involved directly in the dynamic flow of events, a pilot, a process operator, or a train driver.

Consequently, great effort has been spent to improve safety by better training schemes, by safety campaigns motivating the work force to be safety conscious, and by improved work system design to prevent human errors. In addition, considerable resources have been spent on human error research and comprehensive programs are established to define and categorize human behaviour fragments in terms of errors without any significant success; 'human error' data bases still do not exist.

The concept of human error is very elusive. At a closer look, the frequent allocation of accidental causes to human error appears to be subjective and guided by the tool box of the analyst. This is a simple reflection of the nature of causal analysis and the fact that no objective stop rule exists to terminate the causal back tracking in search of a root cause. The search stops when an event is found for which a cure is known to the analyst.

A deeper analysis of accident causation indicates that the observed coincidence of multiple errors cannot be explained by a stochastic coincidence of independent events. Accidents are more likely caused by a systematic migration toward accident by an organization operating in an aggressive, competitive environment. Commercial success depends on exploitation of the benefit from operating at the fringes of the usual, accepted practice. Closing in on and exploring the boundaries of established practice during financial crises necessarily imply the risk of crossing the limits of safe practices. Court reports from several accidents such as Bhopal, Flixborough, Zeebrügge, and Chernobyl demonstrate this effect.

This effect seems now to be increasingly critical, since we are facing some changes of the conditions of industrial risk management:

- Companies live in an increasingly aggressive and competitive environment.
- A very fast pace of change of technology is found at the operative level of society, faster than the pace of change found in management structures and regulatory rules.

- A high degree of integration and tight coupling of systems - one single decision can have dramatic effects that propagate rapidly and widely through the global society.
- An increasing scale of industrial installations with a corresponding potential for large-scale accidents. A very low probability of accidents have to be demonstrated to have operation accepted by society.

This situation creates several basic research and design problems:

Need for vertical analyses of dynamic organizations

Injuries, contamination of environment, and loss of investment all depend on loss of control of a physical processes capable of injuring people or damaging property. Safety, then, depends on the control of work processes so as to avoid accidental side effects causing harm to people, environment, or investment.

The socio-technical system involved in risk management is normally decomposed according to organizational levels, and the levels, government, authorities, management, and operating staff, are the subject of study within separate disciplines. Furthermore, research usually has a 'horizontal' orientation across the types of technological hazard sources. Management theories for instance tend to be independent of the substance matter context of a particular organization. We need more studies of the 'vertical' interaction among the levels of socio-technical systems with reference to the nature of the technological hazard they are assumed to control.

Models of adaptive systems in terms of behaviour shaping features

Human behaviour in any work system is shaped by objectives and constraints which must be respected by the actors for work behaviour to be successful. Many degrees of freedom are, however, left open which will be closed by the individual actor in an adaptive search guided by local and subjective criteria such as work load, cost effectiveness, or risk of failure. Consequently, in a dynamic society, modeling of work behaviour in terms of tasks, decisions, acts, and errors is no longer a reliable approach.

We have to model work systems in terms of the mechanisms that generate behaviour in the actual, dynamic work context. That is, we need a representation in terms of the relational structure of the work space, the objectives and constraints present, and the boundaries of acceptable performance. The likely behavioural trace can only be predicted when the situational and subjective performance criteria that guide navigation in this work space are known. This is a cross-disciplinary issue, involving technical as well as human sciences.

Control of system performance

This change in approach to modelling accident causation also invites a new approach to the control of system performance. Rather than striving to control behaviour by-fighting *deviations* from a particular pre-planned path, the focus should be on the control of behaviour by *making the boundaries explicit and known* and by giving opportunities to develop *coping skills at boundaries.*

Accidents appear to be caused by side effects of decisions made by different actors distributed in different organizations, at different level of society, and during activities at different points in time. These decision makers are deeply emerged in their normal, individual work context. Their daily activities are not coupled in any functional way, only an accident as observed after the fact connects their performance into a particular coupled pattern. By their various, independent decisions and acts, they shape a causal path through the landscape along which an accidental course of events sooner or later may be released, very likely by yet another *quite normal variation* in somebody's work performance - which very likely then will be judged the 'root cause' after the accident.

A basic way to improve safety of complex systems then is to create a shared work support system which makes the 'deep structure' of the work space directly visible to the individual decision maker together with the boundaries of safe operation - including the dependence of the boundaries upon decisions made by other decision makers. The Human Factors problem is *not* to design interfaces that match the users' mental models, but to create interfaces that generate and maintain in decision makers effective and safe mental models. This approach has been called 'ecological interface design' focused on design of human-work interfaces, not human-computer interfaces.

Cross-disciplinary research

The problem of risk management in a dynamic society opens up a cross-disciplinary research arena. Fortunately, information processing metaphors have influenced modelling in human sciences in general and prepared the ground for a convergence of research paradigms. The paradigms of 'management,' 'decision making,' and 'cognitive control' appear to merge in a fruitful way that will facilitate the design of work support systems.

REFERENCES

Rasmussen, J. (1990): Human Error and the Problem of Causality in Analysis of Accidents. Phil. Trans. R. Soc. Lend. B 327, 449-462.

Rasmussen, J. (1990): Role of Error in Organizing Behavior. Ergonomics, 1990, vol. 33, nos 1 0/1 1, 1185-1190.

Rasmussen, J. (1993): Market Economy, Management Culture and Accident Causation: New Research Issues? Invited lecture; Proceedings Second International Conference on Safety Science. Budapest: Meeting Budapest Organizer Ltd.

Rasmussen, J. (1994): Risk Management, Adaptation, and Design for Safety. Invited contribution to: Sahlin, N. E. and B. Brehmer (Eds.): Future Risks and Risk management. Dordrecht: Kluwer.

Rasmussen, J. (1997): Merging paradigms: Decision Making, Management, and Cognitive Control. In: Flin, R., Salas, E. Strub, M. E., Marting, L.: Decision Making under Stress: Emerging Paradigms and Applications. Aldershot: Ashgate

Rasmussen, J. (1997): Risk management in a Dynamic Society: A Modeling Problem. *Safety Science, 27, 183-213.*

Rasmussen, J. and Pejtersen, A. M. (1 994): Virtual Ecology of Work. In: J. Flach, P. Hancock, J. Caird, and K. Vicente (Eds.): Ecology of Man-Machine Systems: A Global Perspective. Hillsdale, NJ.: Lawrence Erlbaum

Rasmussen, J., Pejtersen, A. M. and Goodstein, L. P. (1994): Cognitive Systems Engineering. New York: Wiley.

Vicente, K. J. and Rasmussen, J. (1992): Ecological Interface Design: Theoretical Foundations. IEEE Trans. SMC, Vol. 22, No. 4, pp 589- 607, July/Aug 1992.