RISK MANAGEMENT OF COMPLEX TECHNOLOGICAL SYSTEMS: TOWARDS A SOCIO-ENGINEERING APPROACH

Ab van Poortvliet[1], Jos A. Rijpma[2], Giampiero E.G. Beroggi[1], John A.A.M. Stoop[1], and Wil A.H. Thissen[1]
[1]School of Systems Engineering, Policy Analysis, and Management
Delft University of Technology
P.O. Box 5015, 2600 GA Delft, The Netherlands
[2]Department of Social Sciences
University of Leiden
P.O. Box 9555, 2300 RB Leiden, The Netherlands

ABSTRACT

Engineers and social scientists have addressed risk management of technological systems in many different ways. In this paper we will argue that all of these approaches offer significant insights, but that there are also shortcomings when safety issues are approached within only one discipline. The ever increasing complexity of large-scale problems calls for a more comprehensive approach to safety management. One-dimensional thinking cannot cope with the intricate interconnections among various decision makers and levels of decision making, diverging value-systems of different stakeholders, and hazardous (complex) operations.

This paper discusses an influence diagram and a multi-level model for disaster analysis applied to an integrated whole of both engineering and social concepts. This approach provides more understanding of the causes of disasters than the single-disciplinary approaches, which is necessary to come to improved risk management of complex technological systems. The concept is illustrated by analysing the Zeebrugge ferry disaster.

INTRODUCTION

Complex man-made disasters have been studied many times. Most studies are characterized by a single-discipline approach. So are the results of those studies. In this paper, an effort is made to show advantages of an interdisciplinary approach for analysing disasters involving complex technological systems. As an example, the causes of the Zeebrugge ferry disaster will be analyzed from both engineering and social science points of view. The engineering perspective includes both a quantitative risk assesment model and the design of the particular vessel. The social science approaches consider psychological and organisational aspects. All perspectives will be used to determine causes that lead to the accident. In order to get a clear view on the overall causes of this complex accident, the different perspectives have to be integrated. Useful integrative work which has been done recently is discussed. System approaches seem suitable for further integration. They will be discussed in general briefly. For the purpose of understanding the accident, Perrow's 'normal accident' concept is used. An influence diagram and a multi-level approach are proposed and appear to be very useful for our aim: structuring and explaining the variety of causes that lead to the accident. The paper ends with conclusions for risk management of complex technological systems.

entire statistics. Another problem is the risk measure used: 'total loss' does not express the number of lethalities, injured, and degree of personal damage.

Design of Ro-Ro vessels

Instability leading to capsize is generally seen as one of the major threats for passengers on a Ro-Ro vessel. Unobstructed vehicle decks imply a total lack of subdivisions above the bulkhead deck (uppermost deck up to which transverse watertight bulkheads are carried). This is the principal difference between Ro-Ro passenger ferries and conventional ferries.

Collisions, operational errors, and fire extinguishing operations can lead to large quantities of water on the decks. I.M.O. (the International Maritime Organization) Regulations on Subdivisions of Passenger Ships 1984 require little initial stability (only 0.05 m metacentric height) and very little freeboard (0.076 m) for ships in damaged condition. Applied to Ro-Ro passenger ferries it is clear that the chances of surviving in such a situation are non-existent [3]; the dynamics of the water (including waves), strong winds (possibly combined with current) or just giving rudder can all lead to a small (extra) heeling, allowing water to flow above the bulkhead deck.

The static analysis which has been used successfully for conventional passenger vessels does not apply to Ro-Ro vessels. In the latter case water is not restricted to small areas and thus allowed to run freely over the whole deck, which destabilizes the vessel enormously. Even small amounts of water on the upper decks can lead to a rapid capsize.

The 1984 Regulations did not express the fact that a Ro-Ro ship is, by its basic design, a special ship. Further, the regulations are restricted to the system 'ship'. In this paper it will be pointed out that, for assessing safety, it may be better to define the system as 'shipping'. Not fail-safety of a ship, but safety of the whole shipping system is the real issue.

APPROACHES FROM SOCIAL SCIENCES

Psychological perspective

Human-error as a cause for accidents has been studied extensively and is said to be a crucial cause in 90% of marine accidents [4]. The normative model of human decision making, which assumes a deliberate exploration of alternatives and their consequences, is not applicable to the actual behaviour of people about to be engaged in accidents. Routine behaviour is preprogrammed to such an extent that it occurs without any explicit consideration of risk (assistant bosun going to sleep, and bosun, loading officer and captain not checking whether doors are closed or not).

Recent research has shown that false hypotheses are the prevalent factor in the human-error induced accident causation process [4].

These findings are very interesting. However, relevant questions like 'Why are people diagnosing their situation incorrectly?', 'Which human-errors lead under what conditions to accidents?' and 'What determines the magnitude of the accident?' cannot be answered from a psychological perspective only.

Organisational perspective

According to Turner, events occur in the phase immediately preceding an accident that indicate differences between reality and planned reality [5]. He calls this phase the 'incubation period'. Due to rigidities in perception and beliefs, these events remain unnoticed or are wrongly interpretated.

In the case of the Herald there were many events which indicated unsafety, as is clear from the warnings given by the captains and addressed to management. However, management did not believe in the vulnerability of the ferry system and simply gave priority to low cost over increased safety. Maximizing the profits caused very tight schedules, which caused a time-pressure to such an extent that many operating

breakdown of the system, what he calls a 'normal accident'. The more complex and the more tightly coupled a system is, the more unexpected and linked the events are; the more it is prone for normal accidents.

As has been noticed in the previous sections, there are many important decisions directly concerned with safety that are taken ashore by management. Further, the harbour situation causes the need for trimming the ship which is a crucial factor in the accident causation process. Therefore it makes sense to take broader system boundaries than Perrow: the system to be studied is 'Ro-Ro shipping' more than 'Ro-Ro ship Herald of Free Enterprise'. Within these new boundaries the different monodisciplinairy perspectives can be incorporated.

Procedures carried out too hastily or at sea instead of ashore, using parts of the ship differently than designed for, make the system more complex than is perceived at first sight. The trimming of the ship is necessary for loading the upper deck in other constructed berths than the berth for which the ship has been designed. Time-pressure forces captains to untrim the ship at sea because the pumps do not have by far enough capacity to empty the ballast tanks in the minutes after loading. However, the properties of a ship, including stability, do change by trimming. Captains may accelerate ships that are significantly trimmed and overloaded more quickly than normal in order to gain time back, regardless of the possible hydraulic aspects. Bow doors are used for ventilation. However, there are no indicators that tell the captain whether those doors have been closed or not after the ventilation procedure. S/he relies upon the negative checking system, which assumes everyone does his/her duty. However, crews are 24 hours on board, and officers do not always communicate explicitly when it is not required. There is much other work to be done in the many quick crossings of one of the world's busiest fairways. Meanwhile, Ro-Ro ships still have the potential for a rapid capsize.

As mistakes at sea do not have to be reported, the authorities were not fully aware of the circumstances within the system and thus not able to maintain the regulations that deal with proper safety management and good seamanship.

So the Ro-Ro ferry system can be considered as complex and coupled, not because sailing a ship itself is that complex and coupled, but because an error-inducing culture, arisen due to time-pressure and lack of external control, makes shipping more complex and coupled than technologically necessary. According to Perrow such a system is prone for normal accidents. Such an accident occurred at Zeebrugge on 6th March 1987.

Influence diagram

Influence diagramming is an easy way to describe the factors that influence safety and their (causal) relations. Nevertheless, it is very useful as the method is very effective in showing the wholeness of the system and the limitations of the ranges of monodisciplinary perspectives. Figure 1 illustrates such a diagram. The aspects that influence the safety of the Ro-Ro shipping system have been placed along the different life-cycle phases of the system until the accident occurred. Each of the monodisciplinary perspectives concentrates mainly on one phase: the psychological perspective on the daily operations, the organisational perspective on management, engineering on basic design and hardware development. The diagram shows that relevant decisions made at different times and in different phases do influence each other, and that interdisciplinarity is necessary for tuning these decisions. Unsafety appears to be an evolutionary process in which operator errors are the last stage before the accident happens. Theadvantage of seeing unsafety as an evolutionary process are: (i) safety can be improved by taking safety measures in other stages than the daily operational stage (ii) improved predictions of probability and magnitude of major accidents seem possible.

At the individual system level the most important factors are personal interests, legislation from policy level, company orders from organisational level, and working environment. The working environment can be complex due to decisions made on the organisational level (like in the case of the Herald) or on the policy level. The complexity of daily operations can lead to false hypotheses which are important causes of human-error. Further, personal interests like making a career or working pressure can force individuals to perform unsafe acts (although forbidden by legislation).

The advantage of a multi-level model is that it explicitly shows the relevance to safety of decisions at all levels. In addition, the interactions between the levels are stated. These interactions seem to explain the (un)safety of a system. Besides a better overall understanding of the causes of disasters, this approach offers the possibility to (re)design complex systems effectively by tuning the decisions made at each level.

CONCLUSIONS

Safety of complex technological systems is concerned with both engineering and social sciences. Approaches to safety of such systems made within the different disciplines provide much insights. However, risk management of the ever increasing and ever more complex large-scale systems calls for a more integrated approach. To analyze a disaster in or assess the safety of such a system, an influence diagram and a multi-level model are very useful. An influence diagram shows how unsafety of a system develops in time, and the need for interdisciplinarity for effective risk management. A multi-level model will explicitly show the trade-offs being made at each level, as well as their consequences at other levels. The discussion to what extent accidents can be anticipated remains open. But by applying appropriate approaches we know at least what underlying causes may lead to accidents, as has been illustrated with the Zeebrugge tragedy.

Further development of the integrated approaches is necessary. The economic aspect is supposed to have much influence on the safety of a system. Therefore, it should be studied more thoroughly. Other important research topics are the relations between meso and macro level. Approaches considering these relations and good multiple case study research are required for sharpening or redefining concepts, definitions, and models in order to make these models operationally useful.

REFERENCES

[1] Glansdorp, Traffic Investigation in European Waters, COST 301 Symposium, 1986.

[2] Det Norske Veritas, Safety of RoRo-vessels, RoRo Casualty statistics, DNV, Hovik, 1981.

[3] Report of Formal Investigation: Sheen report, The Merchant Shipping Act. MV Herald of Free Enterprise, Report of Court No. 8074, HMSO, London, 1987.

[4] Willem A. Wagenaar & Jop Groeneweg, Accidents at sea: Multiple causes and impossible consequences, Int. J. Man-Machine studies 27, 1987, p587-598.

[5] Barry A. Turner, Man-made Disasters, Wykeham Publications Ltd., London, 1978.

[6] J.T. Reason, R. Shotton, W.A. Wagenaar & J. Groeneweg jr., TRIPOD. A principled basis for safer operations. Report prepared for Shell Internationale Petroleum Maatschappij, Exploration and Production, 1989.

[7] Charles Perrow, Normal Accidents, Basic Books, U.S.A., 1984.