Normal Accidents: Living with High-Risk Technologies. Charles Perrow. Princeton University Press, 41, William Street, Princeton, New Jersey 08540. 1999. 451 pp. Price: US$ 19.95.

Present-day life depends on systems like power, communication, transport and health to such an extent that any failure in these, leading to a simple discontinuity of service, becomes unbearable. These systems are complex and have catastrophic potential. The author, Charles Perrow, has concentrated on the risk aspects of systems. Questions like: 'How safe is safe enough?'; 'How much risk is acceptable?'; and 'What is the risk–benefit ratio?', are being raised and builders and managers of these systems are striving hard to provide risk-free service. However, as man is mortal, so are the products and services produced by him. What one tries is to build fail-safe systems so that unavoidable failures do not end up in catastrophes. Modern engineering and theoretical tools have made it possible to reduce the risk to a negligible level. But the risk remains, and the Three Mile Island (TMI) accident provided the author with a good subject to study in detail.

Perrow is with Yale University and is a specialist in organizational sociology. He was approached by the President's Commission to provide some inputs, and decided to undertake organizational analysis to understand the causes and effects of failures that lead to accidents.

After studying the TMI accident in depth, the author developed his Normal Accident Theory (NAT) and decided to see its applicability to accidents in other areas like petrochemical plants, aircraft and airways, marine transport, earthbound systems like dams, quakes, mines and lakes. He has even touched upon exotic areas like space, weapons, DNA and even Y2K.

Most complex systems are interactive and tightly coupled. In spite of best efforts to restrict unwanted interactions in tightly coupled systems, these do happen. The author has studied in depth the problems of complexity and coupling and their effects on accidents. He took a simple example in daily life of attending a job interview call. Unwanted errors happened and the person could not reach the place of interview. Where does the error lie? Does it lie in any or all of the following, namely human error, mechanical failure, environment, design of the system or the procedures used. In this simple case the failures were trivial but the interactions amongst them resulted in a loss of job opportunity. In frustration we invoke Murphy's Law – If anything can go wrong, it will! O'Toole, however, feels that Murphy is optimistic and he reframes the law thus: If anything is not expected to go wrong, it will go wrong.

The author defines accidents in his own way. He classifies disruptions due to failure at four increasing levels and he calls failures resulting in third- and fourth-level disruptions as accidents and other failures as incidents. He classifies victims of accidents also into four classes as follows. First – party victims are operators; second – party victims are non-operating personnel or system users such as passengers; third – party victims are innocent bystanders; and fourth – party victims are foetuses and future generations. First and second-party victims are voluntary and the others are involuntary. Most of the concern today is for fourth-party victims. The Nuclear Regulatory Commission (NRC) is aware of the intergenerational risk. However, it feels that there will be no problem if the risk of accidents is kept to a low of 1 in a million reactor-years. Perrow doubts this confidence displayed by NRC.

Perrow also defines component failure accidents as those involving one or more component failures that are linked in an anticipated sequence. System accidents involve unanticipated interactions of multiple failures. Interactions are also classified as linear and complex. Interactions in an expected sequence are linear and those in an unexpected sequence are complex or nonlinear. Irretrievably complex systems are those that transform raw materials rather than fabricate or assemble them. Transformation processes exist in nuclear power production, nuclear weapons, chemical plants, DNA technology and some aspects of space missions. The author feels that the existence of transformation processes without complete understanding characterizes, nuclear power. Recombinant DNA research is also fraught with gaps in knowledge. Limited knowledge allows unsuspected interactions and requires many control parameters and indirect sources of information.

Complex systems are characterized by proximity of parts or units not in production sequence, many common mode connections between components not in production sequence, unfamiliar or unintended feedback loops, many control parameters with potential reaction, indirect or inferential information sources and limited understanding of some processes. Linear systems have minimal feedback loops, fewer control parameters and direct information sources to reflect actual operation.

Linear systems are safer. However, we have to have complex systems as we do not have the knowhow to produce the required output through linear systems. If these complex systems have a catastrophic potential then, the author suggests, we should consider alternative ways of getting the product or else abandon the product itself. He considers nuclear power as one such activity. Complexity is inherent in some forms of production. It is not intrinsically undesirable. We need to welcome complexity in some bureaucracies and resist rationalization of our disorderly life because the unexpected interactions lead to innovations, amuse or interest us, or provide variety. However, if the system has catastrophic potential one cannot prevent propagation of incidents and intervene before an accident has occurred. The issue is a grave one. Loosely-coupled systems tend to have ambiguous or flexible standards, whereas ambiguity and flexibility in performance standards are not tolerated in tightly-coupled systems.

The author has also classified various systems based on complexity, linearity vs loose and tight coupling and portrays them on an interaction/coupling chart. There are four quadrants in this chart. The first quadrant includes systems with tight coupling and linear interactions; the second one includes systems with tight coupling and complex interactions; the third one includes systems with loose coupling and linear interactions; and the fourth one includes systems with loose coupling and complex interactions. The author has subjectively put nuclear plants, nuclear weapons, DNA, aircrafts, chemical plants, space missions and military early warning systems in the second most hazardous quadrant. He has placed systems such as junior colleges, assembly-line production, trade schools and motor vehicles in the third least hazardous quadrant. Both the chemical and nuclear industries have the best record in terms of injuries, fatalities and lost time accidents. The

author also puts aircrafts in the second quadrant. This industry has a virtually anonymous Air Safety Reporting System (ASRS). The author recommends a similar system for nuclear power and marine transport industries. Earth-bound systems like dams are linear but are tightly-coupled systems that have a catastrophic potential. This is a case of systems without interactive components but with a catastrophic potential.

The biological community and chemical and aerospace engineers look upon engineers in the nuclear industry as bungling dropouts from the truly scientific world. But the truth is that these complex systems go beyond the capacities of engineers and designers in all areas. The biological researchers in both university and commercial laboratories feel that they know what they need to know about the risks of technology. They feel that genetic materials will either do what they are supposed to do when they are displaced, or do nothing at all. The author feels this confidence is unfounded. One can ask the question which Nobel laureate Sczent Gorgy once asked, 'What do we know about what we do not know?'

The author classifies the systems into three categories. The first includes systems that are hopeless and need to be abandoned in view of the inevitable risks that outweigh any reasonable benefits (nuclear weapons and power). The second category has systems that we are either unlikely to be able to do without, but which could be made less risky with considerable effort (some marine transport), or where the expected benefits are so substantial that some risks should be run, but not as many as we are now running (DNA research and production). Finally, the third group includes those systems which while hardly self-correcting in all respects, are self-correcting to some degree and could be further improved with quite modest efforts (chemical plants, airlines and air traffic control, and a number of systems we have not examined carefully but should mention here, such as mining, fossil fuel power plants, highway and automobile safety). The author feels that his recommendations are consistent with public opinion.

The science of risk assessment has developed to such an extent that no new project is now undertaken and old continued without risk assessment. Mathematical models are developed to assess risk/benefit ratio. ALARA (As Low As Reasonably Achievable) criteria are developed and acceptable risk need be less but not under any circumstances more than what we have accepted so far. One more argument in favour of entire development is based on taking calculated risk. Active risk is classified as voluntary and passive is classified as involuntary. We must be aware that the method of cathetering in medicine is the result of the voluntary risk taken by German Nobel Laureate scientist Dr Forssman.

We will have to live with activities with potentially high risk. However, the government has to step in to regulate such activities. Recognizing the risk involved in nuclear activity, the US government established a high power body called Nuclear Regulatory Commission. A similar commission is required for regulating chemical and bio-technical activities.

The book was first published in 1984. Since then catastrophes like Bhopal, and Challenger happened. The problem of Y2K was also thought of as a potential catastrophe. The author has tried to apply his NAT to the Bhopal and Challenger scenario in his recent published edition. The author has dealt in detail with Bhopal. A few hundred plants with this potential level of catastrophe are operating for a number of years. But it takes just the right combination of circumstances to produce a catastrophe. He calls this the 'Union Carbide Factor'.

Normally one feels that a safety and reliability culture is enough to handle high-risk systems. However, in case of complex and tightly-coupled systems this is not enough. A detailed risk analysis is a must, taking into account error-inducing and error-avoiding systems.

Y2K was thought to create a catastrophe of an unprecedented level. It was thought by pessimists that engineers and software technologists will not be able to manage the crisis. However, the pessimists have been proven wrong.

HIV/AIDS is presently seen as a menace leading to catastrophe. Its spread depends on temporary tight coupling and the author needs to analyse this scenario using NAT.

The author has investigated the accidents with catastrophic potential in detail and has tried to use NAT to explain the scenario. He, however, feels that the engineers who design, operate, maintain and regulate the systems are not competent enough to control and avoid the catastrophe. The fact that a very large number of systems with catastrophic potential are operating and only a few catastrophic accidents have occurred proves that scientists and engineers are not only competent but socially conscious of their duty to society in developing and managing the new developments such as nuclear energy, aerospace industry, telecommunications, information technology, and marine and road transport technology. These developments have really improved the quality of life of common man. Ordinary people identify scientists and technologists with the creator (*Brahma*) and not the destroyer (*Yama*). Productivity, Quality, Reliability, Safety and Testability (PQRST) are criteria for the viability of any enterprise today. The human cardiogram is called PQRST and if this is all right, the human heart is healthy. Similarly, technological PQRST indicates the health of any present and future industry. There is no need to decry nuclear energy. France has 75% of its electrical energy flowing through a nuclear source. Society can definitely live with nuclear energy. Rare accidents need not cast doubts on the competence of the bulk of scientists and engineers. Scientists and engineers have professional pride and they will not do anything to undermine the confidence the society reposes in them. Moreover, professional bodies like ASME, IEEE, ANS and international bodies of UN, namely IAEA, ISO, IEC and WHO are overseeing and regulating the technology. Non-governmental bodies and learned persons like the author also help to keep the scientists and engineers on their toes.

Lastly, I would like to mention that perfection means stagnation. There is a scope for improvement with imperfection. This is the theme of the book entitled *In Praise of Imperfection* by Nobel laureate Rita Levi-Montalcini.

D. V. PETKAR

S-C-6 Central Park,
Agashi Road, Virar West,
Mumbai 401 303, India