## 7.3 Safety Concerns

There are two coupled, major concerns for the designer, manufacturer and operator of a nuclear power station. The first of these is to avoid any hazard associated with uncontrolled criticality of the reactor and the second is to eliminate any possible release of radioactive material to the environment surrounding the plant. The designer, manufacturer and operator seek to minimize the likelihood of any accident and this requires not only constant vigilance but also continuing improvement in the monitoring instrumentation and in the training of the plant operators.

Over the years, partly because of both the major and lesser accidents that have occurred at nuclear power stations, a great deal of time and effort has gone into examining every conceivable failure (both mechanical and human) that might lead to a departure from controlled operation of a nuclear reactor power station (USAEC 1957, 1973). Fault trees (Bodansky 1996) have been exhaustively explored in order to try to eliminate any combination of malfunction and/or operator mismanagement that might have serious consequences. Experience, for example during the Three Mile Island accident, has shown that a relatively minor equipment failure combined with human operator error can lead to a serious accident, even to a release of radioactivity.

Moreover, technical and operational analyses must be carried well beyond the initial failure and until a safe and controlled state has again been established. Thus the failure trees must postulate quite unlikely initial failures and then follow the progression of events that necessarily unfold in the seconds, minutes, hours and weeks that follow. Thus, for example, much attention has been given to the hypothetical *loss of coolant accident* (LOCA) (see sections 7.6.2 and 7.6.3) that would occur if part of the primary coolant circuit were to fail so that coolant were to escape into the secondary containment and the heat produced in the reactor were no longer being removed by the coolant. The subsequent build-up of heat within the reactor could lead to a meltdown of the core and its containment, a scenario that became popularized by the movie *The China Syndrome* (see, for example, Lewis 1977, Okrent 1981, Collier and Hewitt 1987). The likelihood that such a meltdown would also lead to a release of radioactive material led to exhaustive study of this particular developing fault path.

These explorations of conceivable fault trees and accidents led to the installation of equipment designed to mitigate the effects of these unlikely events. Indeed, to minimize the potential of human error it is also desirable that these safety systems be *passive* (not requiring human or mechanical intervention and not requiring power) though this is not always possible. The next section provides information on some of the installed safety systems, with particular focus on those systems designed to mitigate the consequences of a loss of coolant accident.

Another class of concerns is the vulnerability of nuclear reactors to large external events and forces, such as earthquakes, tsunamis, volcanoes, hurricanes, power outages, and terrorist attacks. Many of these involve the choice of the site of a nuclear power plant. Particularly in California, a great deal of atten-

tion has been given to the proximity of earthquake faults and the need to ensure that the reactor, its containment structures and emergency power systems are as impervious as possible to a major earthquake (Bodansky 1996, Okrent 1981). Moreover, these power plants require copious external cooling water and are therefore often sited close to the ocean. The Fukushima accident (see section 7.5.3 below) demonstrated that more thought should have been given to protecting the plant and its surrounding auxiliary facilities from the tsunami danger. Another scenario that needed to be examined in the aftermath of the 9/11 disaster in 2001 was the possibility of a direct hit by a fully loaded airliner. Analyses and tests have shown that under no circumstances would there be any penetration of the containment building; the airliner would simply disintegrate.

Of course, public imagination conjures up the possibility of an even more drastic accident, namely a nuclear explosion. It is, however, contrary to the fundamental laws of physics for any commercial nuclear reactor containing fuel enriched to less than 5% to explode like a nuclear bomb. It is also important to emphasize that, apart from the Chernobyl accident, *no one* (neither a member of the public nor a plant worker) has ever died as a result of exposure to a commercial nuclear reactor incident. Moreover, as discussed below, the world has put any future Chernobyl incident beyond the realm of possibility.