A conventional approach to safety is based on the concept of design events. A building code might say, for example, that a building should be able to survive a 7.0 earthquake. This approach has been basic to the regulation of nuclear reactors. As the interim report of the post-Fukushima NRC task force explains:

> [The regulation[also requires that design bases . . . reflect (1) appropriate consideration of the most severe of the natural phenomena that have been historically reported for the site and surrounding region, with sufficient margin for the limited accuracy and quantity of the historical data and the period of time in which the data have been accumulated, (2) appropriate combinations of the effects of normal and accident conditions with the effects of the natural phenomena, and (3) the importance of the safety functions to be performed. [p. 25]

The report points out two flaws with this approach. The first issue is selection of the design-basis event. At Fukushima, the design-basis tsunami was chosen too optimistically and without full consideration of the historical record. [p. viii] It is also difficult to ensure uniform treatment since the method for picking the design-basis event may vary between facilities. [p. 20] Selection of the design-basis event may be arbitrary. For instance, as Doug Kysar has explained, the planner for the New Orleans flood control system excluded some historic hurricanes from their calculations on the theory that those hurricanes were outliers.

Second, this approach does not encourage planning for the unexpected. As the Task Force explains:

> Whether through extraordinary circumstances or through limited knowledge of the possibilities, plants can be challenged beyond their established design bases protection. In such circumstances, the next layer of defense-in-depth, mitigation, is an essential element of adequate protection of public health and safety. Mitigation is provided for beyond-design-basis events and severe accidents, both of which involve external challenges or multiple failures beyond the design basis. [p.20]

Finally, use of the design-basis event may be misunderstood to imply that the facility is risk-free. It is notorious that communities often build up behind levees that are designed to

block the 100-year storm. The public believes that no breach can be expected for a century, whereas the standard actually means that there is a one-percent chance of flooding every year.

Design-basis planning is a crude tool. It may be adequate in some settings but not in major projects that are subject to potential catastrophic failures. The Task Force advises greater use of probabilistic risk analysis, to consider a broader range of risks, and also the use of “defense in depth” to deal with contingencies beyond the design-basis event. [p. 21] It would be wise to heed these recommendations, not only in the area of reactor safety, but also in other contexts such as flood planning for urban areas and deepwater drilling.