Chapter

13

Hazard Analysis

The argument that the same risk was flown before without failure is often accepted as an argument for the safety of accepting it again. Because of this, obvious weaknesses are accepted again and again, sometimes without a sufficiently serious attempt to remedy them, or to delay a flight because of their continued presence.

—Richard Feynman
Personal Observations on Reliability of Shuttle [1]

Unfortunately, everyone had forgotten why the branch came off the top of the main and nobody realized that this was important.

—Trevor Kletz
What Went Wrong?

Hazard analysis is at the heart of any effective safety program, providing visibility and coordination (see Figure 13.1). Information flows both outward from and back into the hazard analysis. The outward information, for example, helps designers perform trade studies and eliminate or mitigate hazards and helps quality assurance identify quality categories, acceptance tests, required inspections, and components that need special care. Any changes or additional information must flow back through the analysis so that (1) solutions or corrections can be integrated into the design and (2) the overall conceptual system model and approach to safety is maintained.

Although hazard analysis alone cannot ensure safety, it is a necessary first

[1] Appendix F of the Rogers Commission report [295]