A Definitions

People have been arguing about them for decades, so it is unlikely that everyone will agree with all (or perhaps even any) of the following definitions. They reflect, however, the use of these terms in this book.

Accident An undesired and unplanned event that results in a loss (including loss of human life or injury, property damage, environmental pollution, and so on).

Hazard A system state or set of conditions that, together with a particular set of worst-case environment conditions, will lead to an accident (loss).

Hazard Analysis The process of identifying hazards and their potential causal factors.

Hazard Assessment The process involved in determining the hazard level.

Hazard Level A function of the hazard *severity* (worst case damage that could result from the hazard given the environment in its most unfavorable state) and the *likelihood* (qualitative or quantitative) of its occurrence (figure A.1).

Risk Analysis The process of identifying risk factors and their potential causal factors.

Risk Assessment The process of determining the risk level (quantifying risk).

Risk Factors Factors leading to an accident, including both hazards and the conditions or states of the environment associated with that hazard leading to an accident.

Risk Level A function of the hazard level combined with (1) the likelihood of the hazard leading to an accident and (2) hazard exposure or duration.

Safety Freedom from accidents (loss events).

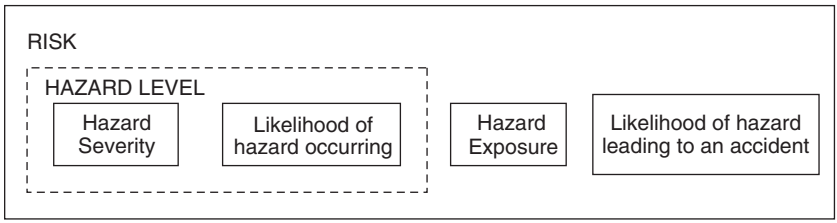

Figure A.1
The components of risk.

System Safety Engineering The system engineering processes used to prevent accidents by identifying and eliminating or controlling hazards. Note that hazards are not the same as failures; dealing with failures is usually the province of reliability engineering.