System Safety Process Steps

The System Safety discipline is defined as the application of special technical and managerial skills to the systematic, *forward-looking* identification and control of hazards throughout the life cycle of a project, program, or activity. The primary objective of System Safety is accident prevention. Proactively identifying, assessing, and eliminating or controlling safety-related hazards, to acceptable levels, can achieve accident prevention. A hazard is a condition, event, or circumstance that could lead to or contribute to an unplanned or undesired event. Risk is an expression of the impact of an undesired event in terms of event severity and event likelihood. Throughout this process, hazards are identified, risks analyzed, assessed, prioritized, and results documented for decision-making. The continuous loop process provides for validation of decisions and evaluation for desired results and/or the need for further action.

The System Safety process steps are depicted graphically in the following figure. It is a formal and flexible process that generally follows the steps in the FAA's *Safety Risk Management Order, 8040.4.* A systematic approach to process improvement requires proactively searching for opportunities to improve the process at every step, not simply identifying deficiencies after an undesired event. Risk Management has been defined as the process by which Risk Assessment results are integrated with political, social, economic, and engineering considerations for decisions about need/methods for risk reduction.