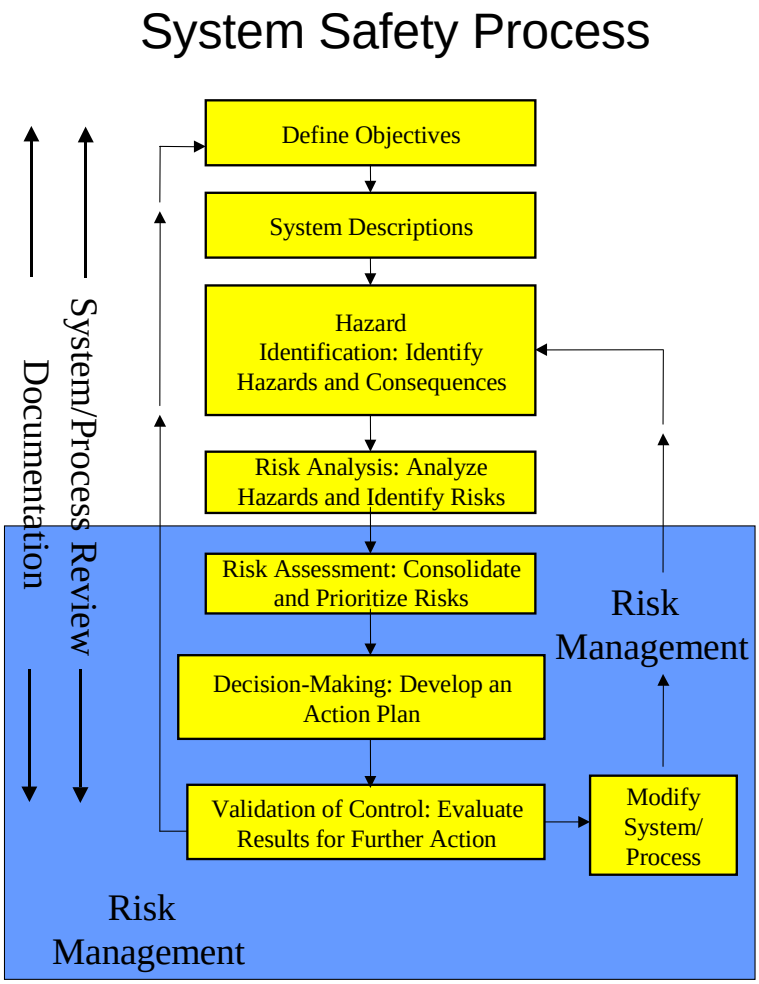
System Safety Process Steps

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.



1. Define Objectives

The first step in the System Safety process is to define the objectives of the system under review. These objectives are typically documented in business plans and operating specifications

2. System Description

A description of the interactions among people, procedures, tools, materials, equipment, facilities, software, and the environment. This also includes descriptions of data available

3. Hazard Identification: Identify Hazards & Consequences

Potential hazards may be identified from a number of internal and external sources. Generally, hazards are initially listed on a Preliminary Hazard List (PHL), then grouped by functional equivalence for analysis. Prior to risk analysis you must also include the consequence (undesired event) resulting from the hazard scenarios. Hazard scenarios may address the following: who, what where, when, why and how. This provides an intermediate product that expresses the condition and the consequences that will be used during risk analysis.

4. Risk Analysis: Analyze Hazards and Identify Risks

Risk analysis is the process whereby hazards are characterized for their likelihood and severity. Risk analysis looks at hazards to determine **what** can happen **when**. This can be either a qualitative or quantitative analysis. The inability to quantify and/or the lack of historical data on a particular hazard does not exclude the hazard from the need for analysis. Some type of a Risk Assessment Matrix is normally used to determine the level of risk (see an example contained in Attachment 1)

5. Risk Assessment: Consolidate & Prioritize Risks

Risk Assessment is generally defined as the process of combining the impacts of risk elements discovered in risk analysis and comparing them against some acceptability criteria. Risk Assessment can include the consolidation of risks into risk sets that can be jointly mitigated, combined, and then used in decision making.

6. Decision Making: Develop Action Plans

This step begins with the receipt of a prioritized risk list. Review the list to determine how to address each risk, beginning with the highest prioritized risk. The four options that may be chosen for a risk are transfer, eliminate, accept, or mitigate (T.E.A.M). Generally, design engineering follows the “safety order of precedence”: 1) Design for minimum risk, 2) Incorporate safety devices, 3) Provide warning devices, or 4) Develop procedures and training. This may result in alternative action plans.

7. Validations and Control: Evaluate Results of Action Plan for Further Action

Validation and control begins with (1) the results of scheduled analyses on the effectiveness of actions taken (this will include identification of data to be collected and identification of triggering events if possible; then developing a plan to review the data collected) and (2) the current status of each prioritized risk. If the residual risk is acceptable, then documentation is required to reflect the modification to the system, and the rationale for accepting the residual risk. If it is unacceptable, an alternate action plan may be needed, or a modification to the system/process may be necessary.

8. Modify System/Process (if needed)

If the status of a risk should change or the mitigating action does not produce the intended effect, a determination must be made as to why. It may be that the wrong hazard was being addressed, or the system/process needs to be modified. In either case, one would then re-enter the system safety process at the hazard identification step.

Attachment 1

Example Risk Assessment Matrix

RISK ASSESSMENT MATRIX				
	Severity			
Likelihood	Negligible	Marginal	Critical	Catastrophic
Frequent				
Probable				High
Occasional			Serious	
Remote		Medium		
Improbable	Low			

Severity Scale Definitions	
Catastrophic	Results in fatalities and/or loss of the system.
Critical	Severe injury and/or major system damage.
Marginal	Minor injury and/or minor system damage.
Negligible	Less than minor injury and/or less than minor system damage.

Likelihood Scale Definitions		
Frequent	Individual	Likely to occur often.
	Fleet	Continuously experienced.
Probable	Individual	Will occur several times.
	Fleet	Will occur often.
Occasional	Individual	Likely to occur some time.
	Fleet	Will occur several times.
Remote	Individual	Unlikely to occur, but possible.
	Fleet	Unlikely but can reasonably be expected to occur.
Improbable	Individual	So unlikely, it can be assumed it will not occur.
	Fleet	Unlikely to occur, but possible.