Appendix A
Glossary and Definition of Terms

Event tree analysis is an inductive analysis process that utilizes an event tree graphical construct that shows the logical sequence of the occurrence of events in, or states of, a system following an initiating event.

A *failure mode* is a way that failure can occur, described by the means by which element or component failures must occur to cause loss of the sub-system or system function.

Fault tree analysis is a systems engineering method for representing the logical combinations of various system states and possible causes which can contribute to a specified event (called the top event).

A *fragility curve* is a function that defines the probability of failure as a function of an applied load level.

A *hazard* is condition, which may result from either an external cause (e.g. earthquake, flood, or human agency) or an internal vulnerability, with the potential to initiate a failure mode. It is a source of potential harm or a situation with a potential to cause loss.

The *performance* of a system or component can be defined as its ability to meet functional requirements. The performance of an item can be described by various elements, such as flood protection, reliability, capability, efficiency, and maintainability. The design and operation of system affects this performance.

A *system* is a deterministic entity comprising an interacting collection of discrete elements and commonly defined using deterministic models. The word *deterministic* implies that the system is identifiable and not uncertain in its architecture. The definition of the system is based on analyzing its functional and/or performance requirements. A description of a system may be a combination of functional and physical elements. Usually functional descriptions are used to identify high information levels on a system. A system can be divided into subsystems that interact. Additional details in the definition of the system lead to a description of the physical elements, components, and various aspects of

This is a preliminary report subject to revision; it does not contain any final conclusions of the United States Army Corps of Engineers.

the system. Methods to address uncertainty in systems architecture are available and can be employed as provided by Ayyub and Klir (1996).

Reliability can be defined for a system or a component as its ability to fulfill its design functions under designated operating and/or environmental conditions for a specified time period. This ability is commonly measured using probabilities. Reliability is, therefore, the occurrence probability of the complementary event to failure.

Consequences for a failure event can be defined as the degree of damage or loss from some failure. Each failure of a system has some consequence(s). A failure could cause economic damage, environmental damage, injury or loss of human life, or other possible events. Consequences need to be quantified in terms of failure-consequence severities using relative or absolute measures for various consequence types to facilitate risk analysis.

Risk is the potential of losses for a system resulting from an uncertain exposure to a hazard or as a result of an uncertain event. Risk should be based on identified risk events or event scenarios. Risk can be viewed to be a multi-dimensional quantity that includes event-occurrence probability, event-occurrence consequences, consequence significance, and the population at risk; however, it is commonly measured as a pair of the probability of occurrence of an event, and the outcomes or consequences associated with the event's occurrence. Another common representation of risk is in the form of an exceedance probability function of consequences.

Probability is a measure of the likelihood, chance, odds, or degree of belief that a particular outcome will occur. A conditional probability is the probability of event occurrence based on the assumption that another event (or multiple events) has occurred.

Safety can be defined as the judgment of risk tolerance (or acceptability in the case of decision making) for the system. Safety is a relative term since the decision of risk acceptance may vary depending on the individual or the group of people making the judgment.

Risk analysis is the technical and scientific process to breakdown risk into its underlying components. Risk analysis provides the processes for identifying hazards, event-probability assessment, and consequence assessment. The risk analysis process answers three basic questions: (1) What can go wrong? (2) What is the likelihood that it will go wrong? (3) What are the consequences if it does go wrong? Also, risk analysis can include the impact of making any changes to a system to control risks.

Risk communication can be defined as an interactive process of exchange of information and opinion among stakeholders such as individuals, groups, and institutions. It often involves multiple messages about the nature of risk or expressing concerns, opinions, or reactions to risk managers or to legal and institutional arrangements for risk management. Risk communication greatly affects risk acceptance and defines the acceptance criteria for safety.

This is a preliminary report subject to revision; it does not contain any final conclusions of the United States Army Corps of Engineers.

A *scenario* is a unique combination of states that lead to an outcome of interest. A scenario defines a suite of circumstances of interest in a risk assessment. Thus there may be loading scenarios, failure scenarios or downstream flooding scenarios.

This is a preliminary report subject to revision; it does not contain any final conclusions of the United States Army Corps of Engineers.